Hacker Highschool
SECURITY AWARENESS FOR TEENS

LESSON 1
BEING A HACKER

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

"License for Use" Information

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the Hacker Highschool web page at www.hackerhighschool.org/license.

The HHS Project is a learning tool and as with any learning tool, the instruction is the influence of the instructor and not the tool. ISECOM cannot accept responsibility for how any information herein is applied or abused.

The HHS Project is an open community effort and if you find value in this project, we do ask you support us through the purchase of a license, a donation, or sponsorship.

Table of Contents

Contributors

Pete Herzog, ISECOM

Chuck Truett, ISECOM

Marta Barceló, ISECOM

Kim Truett, ISECOM

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

1.0 Introduction

Welcome to the Hacker Highschool program! This program is designed to encourage you to be well-rounded and resourceful. The core instruction theme is to harness the hacker curiosity in you and to guide you progressively through your hacker education to help you grow into a responsible role, capable of determining security and privacy problems and making proper security decisions for yourself.

While there is a thrill to hacking partly because of the illegal nature of computer trespass, we want to show you that it is just as big a thrill to alert others about lapses in security and make them public without worrying about going to jail over it. As a citizen of most countries, it is not only your right, but your responsibility, to report security and privacy leaks to the proper authorities. You do this not because you can, but because many other people can't. You are helping those who can't help themselves. This is what watchdog groups do. This is what you will learn to do.

1.1 Resources

This lesson is about how to learn – a critical skill for a hacker. Hacking, in reality, is a creative process that is based more on lifestyle than lesson. We can't teach you everything that you need to know, but we can help you recognize what you need to learn. This is also true due to the constant advances in the computer sciences. What we teach today may not be relevent tomorrow. It is much better for you to embrace hacker learning habits, which are probably the most vital part of hacking and will separate you from the script kiddie (a person who runs hacking tools without knowing how or why they work).

Words and concepts you don't understand in this workbook may require research on the web or in a library. If you don't understand a word or a topic, it is essential you look it up. Ignoring it will only make it difficult for you to understand concepts in other workbooks. The other workbooks may ask you to investigate a topic on the web and then expect you to use the information that you find on the web to complete the exercises in that workbook – but those workbooks won't explain to you how to do this research. This workbook is the only one with a thorough explanation of how to research built into it, so be sure to spend as much time as you need to learn how to research using the various resources available to you.

Don't just limit yourself to computers, hacking, and the internet. Great hackers are well-rounded and creative. Many of them are painters, writers, and designers. Hacking skills can also be applied to other fields, such as Political Science (see *The Prince* by Machiavelli for an example).

Besides being interested in other fields, you should be interested in how other businesses operate. Reading books on everything from psychology to science fiction will make you a much more versatile and functional hacker. Remember, hacking is about figuring out how things work regardless of how they were designed to work. This is how you expose insecurities, vulnerabilities, and leaks.

1.1.1 Books

Books are a great way to learn the foundation and factual science of all that you are willing to explore. Want to know something about the fundamentals of a science, like the hardware details of your PC? Nothing will help you more than reading a current book on the subject. The main problem with books for computers is that they quickly become old. The secret is to learn to see the fundamental structure underneath the thin skin of details. MS-DOS and Windows are clearly different, but both are based on principles of Boolean logic that have driven computers since Ada, Countess of Lovelace, wrote the first computer programs in the nineteenth century. Security and privacy concerns may have changed in the last 2,500 years, but *The Art of War* by Sun Tzu covers fundamental principles that still apply today.

Even though information found in books may not be as 'up to date' as information that comes from other sources, you will find that the information you find in books is more likely to be factually accurate than that which comes from other sources. A writer spending a year writing a book is more likely to check facts than someone who is updating a blog six times a day. (See *Section 1.1.3 Zines and Blogs* for more information.) But remember – accurate does not mean unbiased.

It's not necessary to start a library of your own, but you may want to write notes in margins or otherwise mark what you read, and this is something you can only do in your own books.

Finally, don't look at a book and give up before you even start just because of the size and complexity. Most of these massive tomes that you see sitting around are not read from cover to cover. Think of them as prehistoric web pages. Open one up to random page and begin

to read. If you don't understand something, go backward and look for the explanation (or skip forward to something that does make sense). Jump through the book, backwards and forwards, just as you would bounce from link to link in a web page. This type of non-linear reading is often much more interesting and satisfying for hackers, as it's about satisfying curiosity more than it is about "reading".

1.1.2 Magazines and Newspapers

The use of magazines and newspapers is highly encouraged for providing concise, timely information. However, magazines are usually short on details and often focus too much on the zeitgeist of the community. This is something that a hacker needs to know – social engineering and password cracking, in particular, are more effective if you have a solid grounding in pop culture – but you also need to know that 'pop journalism' isn't always 'accurate journalism'.

Another issue you should consider is the topic or theme of the magazine. A Linux magazine will attempt to down-play Microsoft Windows, because it is a conflicting theme and that is what their main readers want to read.

The best way to combat these two flaws is by being well and widely read. If you read an interesting fact in a magazine, look into it further. Pretend that you believe it, and look for confirmations, then pretend that you don't believe it, and look for rebuttals.

Exercises:

A. Search the Web for 3 online magazines regarding Security.

B. How did you find these magazines?

C. Are all three magazines about computer security?

1.1.3 Zines and Blogs

Zines are small, often free magazines that have a very small distribution (less than 10,000 readers) and are often produced by hobbyists and amateur journalists. Zines, like the famous *2600* zine or *Phrack Hacking* web zine, are written by volunteers and the producers do not edit the content for non-technical errors. This means the language can be harsh for those not anticipating such writing. Zines have a very strong theme and are very opinionated. However, they are more likely to show and argue both sides, as they do not care to nor have to appease advertisers and subscribers.

Blogs are a modernization of the zine. Blogs are updated more often and use communities to tie in very strong themes. Like zines, however, anyone may criticize a story and show an opposing opinion. For blogs, it is important to read the commentary just as much as the story.

Exercises:

A. Search the Web for 3 zines regarding computer security.

B. How did you find these zines?

C. Why do you classify these as zines? Remember, just because they market it as a zine or put "zine" in the title does not mean it is one.

D. Search the Web for 3 blogs regarding computer security.

E. What communities are these associated with?

1.1.4 Forums and Mailing Lists

Forums and mailing lists are communally developed media, much like a recording of a series of conversations at a party. The conversations shift focus often, and much of what is said is rumor, and, when the party is over, no one is certain who said what. Forums and mailing lists are similar, because there are many ways for people to contribute inaccurate information – sometimes intentionally – and there are also ways for people to contribute anonymously. And, since topics and themes change quickly, it's important to read the whole thread of comments and not just the first few in order to get the best information.

You can find forums on almost any topic and many online magazines and newspapers offer forums for readers to write opinions regarding published articles. For this case, forums are invaluable for getting more than one opinion on an article, because, no matter how much you liked the article, there is certain to be someone who didn't.

Many mailing lists exist on special topics, but these are hard to find. Often times, you must look for an idea before you find a mailing list community supporting it.

For a hacker, what is most important to know is that many forums and mailing lists are not searchable through major search engines. While you might find a forum or a list through a topic search in a search engine, you may not find information on individual posts. This information is called "the invisible web" as it contains information and data that is invisible to many since a very specific search is needed, often through meta-search engines or only directly on the website of the forum.

Exercises:

A. Find 3 computer security forums.

B. How did you find these forums?

C. Can you determine the whole theme of the website?

D. Do the topics in the forums reflect the theme of the website hosting them?

E. Find 3 computer security mailing lists.

F. Who is the "owner" of these lists?

G. On which list would you expect the information to be more factual and less opinionated and why?

1.1.5 Newsgroups

Newsgroups have been around a long time. There were newsgroups long before the Web existed. Google purchased the entire archive of newsgroups and put them online at http://groups.google.com. You will find posts in there from the early 1990s. This archive is important for finding who is the original owner of an idea or a product. It is also useful for

finding obscure information that is perhaps too small a topic for someone to put on a web page.

Newsgroups are not used less today than they were years ago, before the web became the mainstream for sharing information. However, they also haven't grown as their popularity is replaced by new web services like blogs and forums.

Exercises:

A. Using Google's groups, find the oldest newsgroup posting you can about security.

B. Find other ways to use newsgroups - are there applications you can use to read newsgroups?

C. How many newsgroups can you find that talk about computer hacking?

1.1.6 Websites

The *de facto* standard for sharing information is currently through a web browser. While we classify this all as "the web" the real term is "web services," as not everything on the web is a website. If you check e-mail using a web browser, you are using a web service. Often times, web services require privileges. This means you need a login name and password to gain access. Having access and the legal right to access is known as having "privileges". Hacking into a website to allow you to change the page may be having access, but since it is not your legal right to do so, it is not privileged access. We are only concerned with having privileged access, but as your experience grows with using the web, you will find many places give access to privileged areas by accident. As you find this, you should get into the habit of reporting this to the website owner.

Websites are searchable through a large number of search engines. It's even possible to make your own search engine, if you have the time and hard drive space. Often, it's the search engines who get privileged access and pass it on to you. Sometimes it is in the form of *cache*. A *cache* is an area of memory on the search engine's server where the search engine stores pages that matched your search criteria. If you click on the link that says *cached*, instead of the actual link, then you will see a single page that shows what the search engine found during its search. The search engines save this information to prove that the search was valid – if, for instance, a page goes down or is changed between the time that you initiated your search and the time that you try to access the page that was returned – but you can also use the cached pages for other purposes, such as bypassing a slow server.

One of the most useful public caches is at http://www.archive.org. Here you will find cached versions of whole websites from over the years.

One final note on websites, do not assume you can trust the content of the websites you visit just because they appear in a search engine. Many hacker attacks and viruses are spread just by visiting a website or downloading programs to run. You can safeguard yourself by not downloading programs from untrusted websites and by making sure the browser you use is up-to-date on security patches.

Exercises:

A. Using a search engine, find sites that may have mistakenly given privileged access to everyone. To do this, we will look for directory listings which are accessible when you don't go

directly to the right web page. To do this, we will go to http://www.google.com and enter this into the search box:

```
allintitle:  "index of" .pdf
```

Click on a link in the results and you should find one that looks like a directory listing.

This type of searching is also known as *Google Hacking*.

B. Can you find other types of documents in this way using Google? Find 3 more directory listings which contain .xls files and .avi files.

C. There are many search engines out there besides Google. A good researcher knows how to use them all. Some websites specialize in tracking search engines, such as http://www.searchengine.com. However, there are many more and you can generally find them by using search engines. There is even a search engine for "the invisible web". Find 10 search engines which are NOT meta search engines.

D. Search for "security testing and ethical hacking" and list the top 3 answers.

E. Search for the same without the quotes and give the top 3 answers. Are they different?

F. It is very different to search for a topic than it is to search for a word or phrase. In exercise D, you searched for a phrase. Now you will search for an idea. To do this, you need to think about what you want and how you want to find it. For example, you want to find an online resource of magazines for ethical hacking. If you enter *online resource of magazines for ethical hacking* into a search engine, you will get a number of opinions about the topic. This is helpful but not as helpful as actually getting the resource. Instead, you need to think, "If I was to make such a resource, what information would be in there and what key words could I pick from that information?" Put the following words and phrases into a search engine and find out which provides the best results for your search:

1. my favorite list of magazines on ethical hacking

2. list of ethical hacking magazines

3. resources for ethical hackers

4. ethical hacking magazine

5. magazines ethical hacking security list resource

G. Find the oldest website from Mozilla in the Internet Archive. To do this you need to search on "www.mozilla.org" at the http://www.archive.org website.

H. Now to put it all together, let's say you want to download version 1 of the Netscape web browser. Using search engines and the Internet Archives, see if you can locate and download version 1 (but don't install it).

1.1.7 Chat

Chats, also known as Internet Relay Chat (IRC), as well as Instant Messaging (IM), are very popular modes of quickly communicating with others.

As a research source, chat is extremely inconsistent, because you will be dealing with individuals in real time. Some will be friendly, and some will be rude. Some will be harmless pranksters, but some will be malicious liars. Some will be intelligent and willing to share information, and some will be completely uninformed, but no less willing to share. It can be difficult to know which is which.

However, once you get comfortable with certain groups and channels, you may be accepted into the community, and you will be allowed to ask more and more questions, and you will learn who you can trust. Eventually you will be able to learn the very newest security information (also known as *zero day,* which implies that it was just discovered) and advance your own knowledge.

Exercises:

A. Find 3 chat programs to use for instant messaging. What makes them different? Can they all be used to talk to each other?

B. Find out what IRC is and how you can connect to it. Once you are able to connect, enter the ISECOM chat room as announced on the front page of http://www.isecom.org.

C. How do you know which channels exist to join in IRC? Find 3 computer security channels and 3 hacker channels. Can you enter these channels? Are there people talking or are they "bots"?

1.1.8 P2P

Peer to Peer, also known as P2P, is a network inside the Internet. Instead of many local computers communicating with each other through a centralized, remote computer, the computers in a P2P network communicate directly with each other. Most people associate P2P with the downloading of mp3s and pirated movies, however, many other P2P networks exist – both for the purposes of exchanging a wide variety of information and as a means to conduct research on distributed information sharing. One website dedicated to teaching about this, http://infoanarchy.org, is based on the premise that information should be free. On the Infoanarchy website, you can find a listing of available P2P networks and clients.

The problem with P2P networks is that, while you can find information on just about anything on them, some of that information is on the network illegally. The Hacker Highschool program doesn't condone the use of P2P to illegally download intellectual property, but there is no question that P2P networks can be a vital resource for finding information. Remember: there is nothing illegal about P2P networks – there are a lot of files that are available to be freely distributed under a wide variety of licenses – but there are also a lot of files on these networks that shouldn't be there. Don't be afraid to use P2P networks, but be aware of the dangers.

1.2 Further Lessons

Now you should practice to master the skill of researching. The better you get at it, the more information you can find quickly, and the faster you will learn. To help you become a better researcher for the Hacker Highschool program, here are some additional topics and terms for you to investigate:

Meta Search

The Invisible Web

Google Hacking

How Search Engines Work

The Open Source Search Engine