

# Module 42

# Hacking Database Servers

- In the CEHv6 Labs CD-ROM, navigate to Module 42
- Open the Hacking SQL Server.pdf file and read the content



- In the CEHv6 Labs CD-ROM, navigate to Module 42
- Open the **HackingProject.pdf** file and read the content

HackingProject.pdf - Adobe Reader	
e Edit View Document Tools Window Help	,
🖻 💌 100% - 🛛 拱 🚼 🛛 Find -	
Project 1: Hacking Database Network Protocols	
2 General Description	
Database servers today are the most critical assets of an organization. In recent years,	
these servers have become the target of hackers employing three types of attack	
techniques: low level network attacks against the operating system that hosts the database	
server, SQL injection attacks through application servers and direct SQL based attacks.	
All techniques have been widely explored and studied and commercial tools are available	

to protect databases against such techniques. As a consequence hackers have started to explore a new technique – network level attacks against the protocol used by the database server.

All commercial database vendors (Oracle, Microsoft, IBM, Sybase) use propriety and obscure protocols to communicate between client and database server. These protocols have been proven to contain security related vulnerabilities, some of which became public recently.

#### Requirements

In this project, students will be given protocol documentation for a specific database and 8.50 x 11.00 in

Ø

- In the CEHv6 Labs CD-ROM, navigate to Module 42
- Open the An Introduction to SQL Injection Attacks for Oracle Developers.pdf file and read the content

🔁 An	Introduction to SQL Injection Attacks for Oracle Developers.pdf (SECURED) - Adobe Reader	
File Ec	lit View Document Tools Window Help	×
9	🔊 90% 💌 📷 🚰 🛛 Find 💌	
â	SQL Injection: Oracle versus Other Databases	~
Ē	Oracle has generally faired well against SQL injection attacks as there is no multiple SQL statement support (SQL Server and PostgreSQL), no EXECUTE statement (SQL Server), and no INTO	-
	OUTFILE function (MySQL). Also, use of bind variables in Oracle environments for performance reasons provides strong protection against SQL injection attacks.	
?	An Introduction to SQL Injection Attacks for Oracle Developers 4	
	Oracle may provide stronger and more inherent protections against SQL injection attacks than other database, however applications without proper defenses against these types of attacks can be vulnerable. Despite these advantages many web applications are vulnerable to SQL injection attacks.	
	Application Development	
~	Applications can be developed using many methods for connecting to an Oracle database – some of	
Ø	these methods are more vulnerable to SQL Injection attacks than others. This paper will focus on	
	just a few programming languages and application architectures commonly used for web-based	
-	applications, although, the techniques described in this paper should be relevant for most	~
	8.50 x 11.00 in	>

- In the CEHv6 Labs CD-ROM, navigate to Module 42
- Open the **sql.pdf** file and read the content



- In the CEHv6 Labs CD-ROM, navigate to Module 42
- Open the AppRadar\_Datasheet.pdf and read the content





# Module 43

# Cyber Warfare- Hacking, Al-Qaida, and Terrorism

- In the CEHv6 Labs CD-ROM, navigate to Module 43
- Open the **Computer Attack and Cyber Terrorism.pdf** and read the content

🔁 Com	puter Attack and Cyber Terrorism.pdf - Adobe Reader	
<u>File E</u> dit	: <u>V</u> iew <u>D</u> ocument <u>T</u> ools <u>W</u> indow <u>H</u> elp	×
	90% • 😸 🚱 Find •	
Û	Definition of Cyber Terrorism	
?	It is first important to note that no single definition of the term "terrorism" has yet gained universal acceptance. Additionally, no single definition for the term "cyber terrorism" has been universally accepted. Also, labeling a computer attack as "cyber terrorism" is problematic, because it is often difficult to determine the intent, identity, or the political motivations of a computer attacker with any certainty until long after the event has occurred.	-
I	There are some emerging concepts, however, that may be combined to help build a working definition for cyber terrorism. Under 22USC, section 2656, terrorism is defined as premeditated, politically motivated violence perpetrated against noncombatant targets by sub national groups or clandestine agents, usually intended to influence an audience. The term "international terrorism" means terrorism involving citizens or the territory of more than one country. The term "terrorist group" means any group practicing, or that has significant subgroups that practice, international terrorism. <sup>14</sup>	
I	The National Infrastructure Protection Center (NIPC), now within DHS, defines cyber terrorism as "a criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies." <sup>15</sup>	
0	By combining the above concepts, "cyber terrorism" may also be defined as the politically motivated use of computers as weapons or as targets, by sub-national groups or clandestine agents intent on violence, to influence an audience or cause a government to change its policies. The definition may be extended by noting that DOD operations for information warfare <sup>16</sup> also include physical attacks on computer facilities and transmission lines.	*
	8.50 x 11.00 in <	>

- In the CEHv6 Labs CD-ROM, navigate to Module 43
- Open the Cyber Operations and Cyber Terrorism.pdf and read the content



- In the CEHv6 Labs CD-ROM, navigate to Module 43
- Open the Terror's Digital Jihad.pdf and read the content



- In the CEHv6 Labs CD-ROM, navigate to Module 43
- Open the **Computer Attack and Cyberterrorism 1.pdf** and read the content

🔁 Comp	puter Attack and Cyberterrorism 1.pdf - Adobe Reader	
<u>F</u> ile <u>E</u> dit	: <u>V</u> iew <u>D</u> ocument <u>T</u> ools <u>W</u> indow <u>H</u> elp	×
	100% • 🛃 🔂 Find •	
٥	Three Methods for Computer Attack	<u>^</u>
3	A computer attack may be defined as actions directed against computer systems to disrupt equipment operations, change processing control, or corrupt stored data. Different attack methods target different vulnerabilities and involve different types of weapons, and several may be within the current capabilities of some terrorist groups. <sup>5</sup> Three different methods of attack are identified in this report, based on the effects of the weapons used. However, as technology evolves, distinctions between these methods may begin to blur.	-
	<ul> <li>A physical attack involves conventional weapons directed against a computer facility or its transmission lines;</li> <li><sup>5</sup> All methods of computer attack are within the current capabilities of several nations. See CRS Report RL31787, <i>Information Warfare and Cyberwar: Capabilities and Related Policy Issues</i>.</li> </ul>	
		_
Ø	CRS-3	
<b>%</b>	• An electronic attack (EA) involves the use the power of electromagnetic energy as a weapon more commonly as an 8.50 x 11.00 in	>

- In the CEHv6 Labs CD-ROM, navigate to Module 43
- Open The Cyberterrorism Threat.pdf and read the content

🔁 The	Cyberterrorism	Threat.pdf - Adobe Reader				
File Edi	it View Document	Tools Window Help	×			
	125% -	Find The second				
Ē		Cyberterrorism—What Is It and Who Does It?	<u>^</u>			
2		In general, terrorism proves a difficult topic to set boundaries around. One	-			
		common approach to defining cyberterrorism is broad inclusiveness in				
		addressing the actors, means and goals involved. My approach endeavors to				
		delineate the threat in terms of factors relevant to evaluating US policy and				
		organizational responses. Definitions and boundaries prove critical in				
	establishing policy, defining organizational responsibilities and addressing					
	resource allocation. So while arguably an artificial exercise, we will begin by					
	answering two key questions—"What types of acts constitute cyberterrorism?"					
	and "Who conducts cyberterrorism?"					
		This analysis of cyberterrorism centers on the activities of organized,				
		non-state actors pursuing political or systematic objectives against the US <sup>6</sup> The	e			
	activities of states conducting hostile activities in cyberspace against the US fall					
	outside the realm of cyberterrorism into areas which can be labeled information					
		warfare, espionage, or public diplomacy. However, we will consider the				
Ø		possibility that states may be associated with non-state actors in the furtherance	2			
-		of cyberterrorism. I also do not consider activities of individuals in the				
Storget.	8.50 × 11.00 in		> ×			

- In the CEHv6 Labs CD-ROM, navigate to Module 43
- Open the Cyberterrorism.pdf and read the content



- In the CEHv6 Labs CD-ROM, navigate to Module 43
- Open the Cyberterrorism-The Bloodless War.pdf and read the content



- In the CEHv6 Labs CD-ROM, navigate to Module 43
- Open the Cyberterrorism-How Real Is the Threat.pdf and read the content



- In the CEHv6 Labs CD-ROM, navigate to Module 43
- Open the **1yberterrorism 1.pdf** and read the content

🔁 cyberterrorism1.pdf - Adobe Reader	
File Edit Vie	w Document Tools Window Help 3
1	25% • 🛛 🛃 🛛 Find •
	Pure cyberterrorism
?	The concept of 'pure' cyberterrorism — that is, terrorism activities that are carried out entirely (or

primarily) — in the virtual world is an interesting one. The Internet provides many different ways of anonymously meeting with 'like minded' individuals in a (comparatively) safe way. Furthermore, a successful cyberterrorism event could require no more prerequisite than knowledge — something that is essentially free to the owner once acquired, and an asset that can be used over and over again. Thus, it would be possible that such an environment could facilitate the creation of entirely new terrorist groups — no monies would be required for actions, and members could organize themselves quickly and easily in the anonymity of cyberspace. This is very different from certain examples given above, where the computer can aid the task of the terrorist, but 'real' resources are still required to execute the plan. It is this pure cyberterrorism that most writers mean when they discuss the dangers posed by the cyberterrorist, and this compartmentalization poses a significant barrier to our ability to protect ourselves.

One question that has not been adequately addressed in the literature is what might this terrorism look like. At this time, there is much confusion, based largely upon lack of agreement in definitions. However, using 'traditional' terrorism models should help make the situation more suited to analysis, and this is certainly a topic for future research.

Terrorism as theater?

8.50 × 11.00 in 🛛 <

Ø

>



# Module 44

# **Internet Content Filtering Techniques**

### Lab 44-01

#### Objective:

Use **Ad Cleaner** to block adware and popups.

- In the CEHv6 Labs CD-ROM, navigate to Module 44
- Install and launch AdCleaner program

AdCleaner (unregister version)				
Popup Ads         New form Ads         Adwares and Spywares           Settings         White List         Block history         About AdCleaner				
AdCleaner , The professional IE advertisements clean tool eEriEsoft Inc. 2003-2004				
AdCleaner Version 1.21 Copyright (c) 2003-2005 eEriEsoft, Inc.				
Web: <u>www.eEriEsoft.com</u>				
You can try AdCleaner 1.21 for free until 2008-1-25, and then please register AdCleaner at eEriEsoft, Inc. Register Code:				
You can get register code at Owerks, Inc. Register(R)				
OK Cancel				

- Go to Settings tab. Set the required IE settings and Options by enabling the check boxes

AdCleaner (unregister version)						
Cleaner (unregister version)       Image: Cleaner (unregister version)         Popup Ads       New form Ads       Adwares and Spywares         Settings       White List       Block history       About AdCleaner         IE Settings       Image: Cleaner       Image: Cleaner       Image: Cleaner         Image: Cleaner       Image: Cleaner       Image: Cleaner       Image: Cleaner         Image: Clea					r	
	animations e script debugge	r	Res	tore Defa	ults	
Skin You can select three difference skins here SKIN_BLUE						
Options Add to IE context menu Enable Tips Keep history logs						
			0	к	Cancel	

• Go to **Popup Ads** tab and check the required options to block popup ads

AdCleaner (unregister version)				
Settings White List Block history About AdCleaner Popup Ads New form Ads Adwares and Spywares				
General          General         Auto block popup Ads         Auto block unfathered popup Ads         Auto block ModelessDialog popup Ads				
Hotkey Temporarily disable AdCleaner by holding down:				
Notification When a popula (id is blocked)				
✓ Display message in status bar     Sound File       ✓ Beep via PC speaker				
Play default sound  Play sound file				
OK Cancel				

 Go to White List tab and click Add button to add websites for which you want the popups to be allowed

AdCleaner (unregister version)
Popup Ads       New form Ads       Adwares and Spywares         Settings       White List       Block history       About AdCleaner         The white list contains websites where popups are allowed.       Address of website to add:       Image: Common State Stat
✓ Enable white list
OK Cancel

• Go to New form Ads tab to block the new form of ads. Check the required options and click OK.

AdCleaner (ı	ınregister ve	rsion)			?	×
Settings Popup Ads	White List New for ds.Flash Ads.Anir	Block his rm Ads mated Ads -	story Adw	About Ado ares and Spy	Cleaner wares	
AdCleane Animated website in	r can automatica Ads. These Ads istead of popup /	lly block Flo are used m Ads.	ating Ad ore and i	s,Flash Ads a more in some	ind	
Auto t 🔽 Auto t	block Floating Ad block Flash Ads y message in sta	s 🔽 Aut 🔲 Blo tus bar whil	:o block # ck uncaci le blockin	Animated Ads hed images 1g a floating A	: Ad	
You can manually hide all Flash Ads and Animated Ads with the following shortcut:						
Press sho	rtcut key(s): No	ne				
Script Block resize by script						
			Ŕ	<u></u>	Cancel	

Open a site in IE, the adware and pop-ups will be blocked



### Lab 44-02

#### Objective:

Use AdsGone Popup Killer to avoid hazardous popup and banner advertisements.

- In the CEHv6 Labs CD-ROM, navigate to Module 44
- Install and launch AdsGone Popup Killer program

AdsGone Spyware Blocker and Popup Killer 2008	×
File Help	
AdsGone Spyware Blocker and Popup Killer Spyware Blocker	ter Popup Killer Settings Statistics Buy/Register   About   Help
Spyware Scan         Ignored Items         Quarantine       Last Scan Run         Sunday, November 26, 2006 at 1:00:33 PM         © Memory locations scanned, 0 Infected.         © Negistry locations checked, 0 Infected.         © Files checked, 0 Infected.         © Cookies scanned, 0 Infected.	Quick Statistics Spyware Database Definitions: 0 Spyware Detected on this Computer: 0 Spyware Quarantine Files: 0 Spyware Ignored: 0 Spyware Deleted : 0
0 Spyware Threat(s) Detected	
Review all Ignored threats Review all items Quarantined Spyware Definitions Database Version :	SCAN NOW

•



Click on the **Settings** button. **General** settings are displayed by default.

🗹 AdsGone Spyware Blocker and Popup Killer 2008 🛛 🛛 🛛 🔀
File Help
AdsCone Spyware Blocker and Popup Killer Spyware Blocker Popup Killer Spyware Blocker Popup Killer
Settings Buy/Register   About   Help
General       Ceneral         Advanced       Startup £ Setup Options:         Admin Settings       Start when windows starts         Activate only when internet explorer is running set this ONLY if you use internet explorer!         Display the settings button on the internet explorer tool bar         Automatically "Quarantine" when threats are found         Automatically update when new spyware threats are found         Load spiware definitions when startup         Load splash screen on startup
<ul> <li>Automatically download ad blocking and spyware blocking definitions from the server (every few days)</li> <li>Hide detailed update progress window</li> <li>Download latest ad blocking, and spyware definitions from the internet now!</li> </ul>
Download

•

Click **Advanced** link to configure advanced settings.

AdsGone Spyware Blocker	r and Popup Killer 2008	
File Help		
AdsC Spyware Blocker	and Popup Killer Spyware Blocker Popup Killer Settings Statist	tics
Settings	Buy/Register   About   H	lelp
General Advanced Admin Settings	Advanced  Popups and Banners: Block Internet Explorer Popup Ads Block ALL new Internet Explorer popup windows (maximum protection) Block Banner Ads and Many Popup Ads (using the list of known ad servers) host list Disable messenger service popup ads.  Lick here to block Web Page Dialog' popup ads (by window title)  Internet Explorer Options: Disable Script Debugging Show Script Debugging Disable Macromedia Flash Ads Play Animation in Web Pages	

• Click on Admin Settings link to configure administrative settings and explore various options.

AdsGone Spyware Blocker and Popup Killer 2008
e Help
Spyware Blocker and Popup Killer Spyware Blocker Popup Killer Settings Statistics
Settings Buy/Register   About   Help
General       Admin Settings         Advanced       Administrator Settings Password:
Download     Download latest ad blocking and spyware definitions from the Internet Ad Blocking Server.     Reset your ad blocking statistics to zero.       Download     Reset
Test your connection to the ad blocking data server.         Connect    See if there is a newer version of this software. Just Download and install.          New



Click **Popup Killer** button to configure the popup killer.

AdsGone Spyware Blocker	and Popup Killer 2008			X
File Help				
Adsc Spyware Blocker	ONE and Popup Killer	Spyware Blocker	Popup Killer Set	tings Statistics
Popup Killer	•		Buy/Reg	gister   About   Help
Allow Whitelist Block Blacklist Hot Key	Allow Whitelist Allow Popup/Ads by	Ad Server Name	Window Title	URLWhitelist
Sound	No ads have been blocked by 'Ad	Server Name' yet.		
Click here to ALLOW all content	rom the named ad server (domain). You If you are having the software block ba can ALLOW any content blocked by c	can add and remove	Allow Ads I server content blocked	ads.someserver.com) by AdServer d is shown here. You

 Go to Ad server Name tab and click on No ads have been blocked 'Ad Server' Name Yet link

AdsGone Spyware Blocker	and Popup Killer 2008 🛛 🔀
File Help	
Adso Spyware Blocker	ONE and Popup Killer Spyware Blocker Popup Killer Settings Statistics
Popup Killer	Buy/Register   About   Help
Allow Whitelist Block Blacklist	Allow Whitelist Allow Popup/Ads by Ad Server Name Window Title URLWhitelist
Hot Key Sound	No ads have been blocked by 'Ad Server Name' vet.
Click here to ALLOW all content i	rom the named ad server (domain). You can add and remove domains to block (i.e. ads.someserver.com)
	Allow Ads by AdServer
	If you are having the software block banner ads, the last ad server content blocked is shown here. You can ALLOW any content blocked by clicking above.

•

#### Enter the ad server name and click Add to List.

Block or Allow all content from ad server domains.	
<ul> <li>To allow an ad server, find it on the list to the left and move it to the allowed server list to the right:</li> <li>This software has a default list of all known ad servers. These are listed in the left column. If you are trouble with a site and need to "Un-Block" that site, click on it in the list and use the =&gt; button to mo</li> <li>'Allowed Servers' list. You can move entries back and forth. Any ads or pages served from the sites 'Allowed Servers' list will not be blocked.</li> </ul>	e having we it to the in the
Search for: 0 Allowed (unblocked) Ad Servers	
Blocked Ad Servers: Allowed Ad Servers:	
actionsplash.com ads.x10.com images.x10.com adserv.internetfuel.com popme.163.com servedby.advertising.com specialoffers.aol.com whenushop.whenu.com www.popupnation.com	
Add Additional Ad Servers to Block: 2 Server: www.certifiedhacker.com Add to List Delete from List Www.certifiedhacker.com WARNING: All content from that server/doma blocked. There is no way to specify something 'www.cert.com/cgi-bin/ads/*'. AdsGone 2000 faster this way at the expense of less flexibility, names are allowed here (e.g. 'www.SomeAdStrict)	erving just and click in will be g like 8 is much Only domain erver.com').
3 Click Here to have this software close Any window based on its Window Title Cancel	ОК
<ul> <li>Try to open blocked site.</li> </ul>	
http://www.certifiedhacker.com/ - Windows Internet Explorer	
Image: Second Secon	^
Chttp://www.certifiedhacker.com/	★
AdsGone 2008 Blocked HTML Ad	
ione 🛛 🤯 😜 Internet	🔍 100% 🔹

# Lab 44-03

#### Objective:

Use **AdSubtract** to block banner ads, contextual ads, Pop-ups, animations on web pages, background sounds and ad server cookies.

- In the CEHv6 Labs CD-ROM navigate to Module 44
- Install and launch AdSubtract program

😫 AdSubtr	act PRO 3						
AdSul	btract*	<b>V</b> Buy	() About	Ø Options	<b>D</b> Test	() Help	
Block	Ad Blocking Ad	Subtract Filtering	is:		Scorebo A	ard ds Subtracted	d Since 1-19-2008 :
<b>P</b> Search		OFF				Ban	20 Iner Ads
Sanity		nable Filterin	5			Рор	<b>7</b> -Up Ads
Cookies & Clean Up	Total Ads Block	ted otracted by AdSu	ibtract Use	dh) rs:		Sea	0 Irch Ads
Stats	Updates	00 Marrian 2.05					
Themes	<ul> <li>AdSubtract Pr</li> <li>Ad Definitions</li> </ul>	Version 1.40					Check for Updates
Main		Yo	u have 28	days rema	aining in y	your trial	🛞 Activate 🛛 OK



Click **Search Sanity** 💏 icon to block sponsored and paid ads in popular search engines.



Page | 791

Click Cookies & Clean Up to cleanup cookies and check the required Clean up options.

AdSubtract PRO 3 ٦ 0 0 50 AdSubtract<sup>®</sup> Buy About Options Test Help INTERMUTE<sup>\*\*</sup> Cookies Clean Up Options Some Internet cookies are used to remember your Web site Select preferences and settings. But "profiling" cookies (shown in RED) Block may be used to track your web surfing history. Keep the cookies Cookies you trust. Let AdSubtract regularly delete the others. Browser Cache F, Search Cookies to remove **Trusted Cookies** 뉙 Browser History 192.168.0.2 Sanity 192.168.0.2 7 Search History 192.168.0.2 11 208.106.153.175 Temporary Files ad.yieldmanager.com Cookies & Document History admagnet.net Clean Up ads.ozonemedia.co.in Run History atdmt.com 5 au.real.com Recycle Bin Stats c.msn.com AdSubtract Stats classified.tnonline.com cookie.monster.com cookie.monster.com Themes ehg-techtarget.hitbox.com 🔽 Return To Main Panel selected items at start-up Clean Up Now OK Click **Main** icon to return to the main screen. AdSubtract PRO 3 -V 6 0 J 0 AdSubtract<sup>®</sup> Options Buy About Test Help INTERMUTE" Ad Blocking Scoreboard AdSubtract Filtering is: Ads Subtracted Since 1-19-2008 : Block 20 50 Banner Ads Search Enable Filtering Sanity 7 Pop-Up Ads 1 Pa Total Ads Blocked Cookies & 0 Clean Up Total Ads Subtracted by AdSubtract Users: Search Ads 9 -Updates-Stats AdSubtract PRO Version 3.05

Ad Definitions Version 1.40 Check for Updates
You have 28 days remaining in your trial
Activate OK

Theme

ł

Main



Click Enable Filtering to start filtering.

To cloak an image in the browser select the image, right click and select **AdSubtract: Cloak image** 

C IndiaP	Open Link	ia for Boards & University Exam Results, Admission Notificatio - Micr 🔳 🗖 🔀
$\mathbf{G}$	Open Link in New Tab	com/ 🔽 🐓 🗙 Google
File Edil	Open Link in New Window	elo
AdSul	Print Target	7 Pops: 9
🖈 🏟	Show Picture Save Picture As	ndia for Boards & Univer
Total 88. in IIT- Ph: 0744-32	E-mail Picture Print Picture Go to My Pictures Set as Background	Doards Universities comp. exams recruitments Initiatives its :: Poils     ER) Examination Schedule - 2008 rkow     National Anthem sti     Us to worship mothe     VTU) BE III Sem Supplementary Result 2007 more :: rkow     VYes
-	Cut Copy Copy Shortcut	BEB) Middle Examinations - 2008 Date Sheet New       Image: Comparison of the sheet New         OK) M Sc Final Mathematics Exam Result more :: New       Image: New         BSE) Exam Schedule: SSC & HSC Examinations - 2008 New       Image: Can't Say         BSE) Exam Schedule: All India Sec & Sr Sec Exams-2008       Image: Can't Say
- Ahmedat	Add to Favorites AdSubtract: Bypass Site AdSubtract: Cloak Image	he Indian School Certification Exam. ol Education Board gher Secondary Education, Orissa
& Aer Ph: +91-99	Adg ptract: Report Site Properties	Education and Examination Board Examination Results ediate Education Council Most of the MNCs require no Prior Exp. Submit y Free Now! MonsterIndia.com
Poor College 98292-551	Stribut of gunsering of Engg. Jaipur 105/55106 Grad Board Board of I Board of S Jammu & K HP Board of Uttarancha West Beng	of Sec. and Higher Secondary Education itermediate Education, Andhra Pradesh econdary Education Rajasthan (ashmir State Board of School Education if School Education, Dharamshala I Education and Examination Board al Examination Results
		😧 😧 Internet 🔍 100% 🗸 🕫

The site after blocking the images

Ethical Hacking and Countermeasures v6 Lab Manual

🦉 IndiaResults : No 1 Portal in India for Boards & University Exam Results	s, Admission Notificatio - Micr 🔳 🗖 🔀
🚱 🕞 👻 http://www.indiaresults.com/ 💌 🐓	Coogle
File Edit View Favorites Tools Help AdSubtract Stats 🔊 Ads: 27 Pops: 9	
🙀 🏟 🌈 IndiaResults : No 1 Portal in India for Boards & Univer	🏠 🔹 🔝 👘 🖶 🔹 🔂 Page 👻 🎯 Tools 📼 🎽
INDIARESULTS.COM	Forums Profile Select State
Notifications ::	VITEEE-2008 A
Advertisements ::	Certificate course in Aviation Mar
Hot Results boards universities comp. exa	ams recruitments 🥰 IndiaResults :: Polls
Total 883* Selections in IIT-JEE 2007         21/01/2008 (RUHS Medical Univ.) Pre PG (Medical) Exam           Ph: 0744-3291927,3237127         21/01/2008 (RUHS Medical Univ.) Pre PG (Dental) Exam           19/01/2008 (CISCE) ISC (XII) Exam - 2008 Date Sheet	Result more :: NEW: More :: NEW: More :: NEW: More :: NEW: National Anthem sti us to worship mothe O Yes O No.
19/01/2008 (BSER) Examination Schedule - 2008 NEW!	Can't Sav
19/01/2008 (CSVTU) BE III Sem Supplementary Result 2 18/01/2008 (PSEB) Middle Examinations - 2008 Date She	eet NEW!
BOARDS	
http://ads.indiaresults.com/adv/banners.asp?id=901	😜 Internet 🛛 🍕 100% 🝷 🏢

To set themes, Click Themes 😂

😫 Ad Subtra	act PRO 3						
AdSub	otract <sup>®</sup>	Buy	(1) About	options	🗊 Test	(C) Help	
Block Block Search Sanity Cookies & Clean Up Stats Stats Themes Main	Sounds Choose a sound So @ B @ P @ S @ A @ C Custom Remove	scheme for A unds Off anner Ad Sound op-Up Sound earch Ad Sound d Rotator Sound sound Schen Sound Schen	dSubtract		Color Sc Choc Backgrou Choose a program:	heme base a color so Blu und Image a background Default Cance	theme for AdSubtract: e  • image for the AdSubtract Browse I Apply OK

To view statistics, Click Stats <sup>3</sup>

Ethical Hacking and Countermeasures v6 Lab Manual

😫 Ad Subtra	act PRO 3							×
AdSub	otract	Buy	About	options	<b>)</b> Test	(C) Help		
	Stats	е		Ads		Pop-Ups	Cookies	
Customize	your filter settings, including	how you blo	ick	3		0	0	
	ad.yieldmanager.com			1		1	0	
Search	ads.ozonemedia.co.in			1.		1	0	
Sanity	d2.zedo.com			1		0	0	
Cookies & Clean Up	www.indiaresults.com			4		0	0	
Stats								-
Themes	Total			10		2	0	
Main						Â	Reset OK	

To bypass a website, Click **Block→ Bypass→ Add** 

Sub	tract <sup>®</sup>	About	Options	<b>D</b> Test	(C) Help	INTERMU'
. [	Filtering Options			Bypass • C	loak • RedirectF	Protect
ock	Block Annoyance		1	"Bypass" le AdSubtract	ets specified We filtering.	b sites avoid
2	Pop-Ups			Remo	ve Site	
rch nity	<ul> <li>Intelligent Filtering</li> <li>Aggressive Filtering</li> </ul>				login.yaho	oo.com
	Banner Ads					
2	Contextual Ads					
es& iUp	Cookies (Ad Server	Cookies (Ad Server/Profiling)				
	✓ Windows Messenge	er Pop-Ups				
te l	Animations					
	E Background Sound	5				
	✓ Flash				and B	emove
nes	External JavaScript					
3					A	

Enter the site address, Click Add

.

.

Ethical Hacking and Countermeasures v6 Lab Manual



To hide specific unwanted images, Click Cloak


# Lab 44-04

## Objective:

Use Anti AD Guard program to block commercial banners loaded by the browsers.

- In the CEHv6 Labs CD-ROM navigate to Module 44
- Install and launch Anti-AD Guard program
- Click **Start** to Start Anti Ad Guard

🚯 Anti-AD C	iuard 2.1 📃 🗖 🔀
Anti-AD Gua	ard 2.1 (signatures: 11095, build: 2127)
	Anti-AD Guard is a powerful program that blocks commercial banners from being loaded by browsers.
Total check	ed items: 646
Total block	ed items: 17
Owner: Personal-ID: Web: Support:	PYmS3f+2bBz8bxWwsTg+jw== www.pcguardsoft.com support@pcguardsoft.com
URL	

Browse any site

Ethical Hacking and Countermeasures v6 Lab Manual

e	EC-Counc	il Security Certifica	ation - Windows	Internet Explore	er		
G	🕥 🗸 🖪 http:	://www.eccouncil.org/		<ul><li>✓ €•</li></ul>	× Live Search	1	<b>P</b> -
🚖 🐗	🕅 🖻 E	C-Council Security Certif	fication		🙆 • 🔊 ·	🖶 🔹 🔂 Page 🔹	
	2						
	🛃 Home	Pressroom	E Certification	Education	FAQ	🛃 ATP	💽 In:
	1			nonor   EC-C		sity   EC-Counc	
<u>×</u>	• 		IT.		👵 😜 Internet		► 100% ▼

• Check the blocked pop-ups

Ethical Hacking and Countermeasures v6 Lab Manual

😻 Anti-AD G	iuard 2.1	
Anti-AD Gua	rd 2.1 (signatures: 11079, build: 2127)	
	Anti-AD Guard is a powerful program that blocks commercia from being loaded by browsers.	al banners
Total check	ed items:	19
Total blocke	ed items:	2
Owner: Personal-ID: Web: Support:	Trial User (license expired on 5/28/2008) u9Y3iGquGuPSQquriyVnyA== www.pcguardsoft.com support@pcguardsoft.com	
URL		
🕘 http://ads1	1.msn.com//dap.js	
() http://www	w.eccouncil.org//rotating%20banners.swf	
Pause	Statistics	Settings

# Lab 44-05

Objective:

Use **KDT site blocker** to block the desired web pages by adding the link.

- In the CEHv6 Labs CD-ROM navigate to Module 44
- Install and launch **KDT site blocker** program

Ethical Hacking and Countermeasures v6 Lab Manual

🔓 KDT Site Blocker	
la-	Admin Options
Site Blacker	Change Your Password
	🗔 Uninstall This Software
⊂Blocked Sites	
N	
Type a website here and click "Add".	👍 Add 🛛 🔊 Edit 🕵 Del
NOTES: Include the 'www' portion if applicat Only domains (i.e. websites) can be	le (e.g. www.google.com). blocked; not individual pages.
Changes take effect when you save Unblocking sites may require clearing	changes and restart your browser. g your Temporary Internet Files
Save Change	s and Exit

• Enter the site address to be blocked and click on **Add** button.

🔓 KDT Site Blocker	
Admin Opt	tions
Site Blacker	ige Your Password
	tall This Software
- Blocked Sites	
www.google.com	🕼 Edit 🕵 Del
NOTES: Include the 'www' portion if applicable (e.g. www.g Only domains (i.e. websites) can be blocked; not in	oogle.com). dividual pages.
Changes take effect when you save changes and re Unblocking sites may require <u>clearing your Tempor</u>	estart your browser. <u>ary Internet Files</u>
🕞 Save Changes and Exit	

 -	
 <b>n</b>	 
	CIII.
	_
~~	

Click Save

## Changes and Exit button

•

Admin Options  Admin Options  Change Your Password  Uninstall This Software  Blocked Sites  www.google.com
Kpr       Site Blocker          Site Blocker        Uninstall This Software         Blocked Sites       www.google.com
Blocked Sites
Blocked Sites
Www.google.com
www.google.com
🔂 Add 🕞 Edit 🕵 Del
NOTES: Include the 'www' portion if applicable (e.g. www.google.com).
Only domains (i.e. websites) can be blocked; not individual pages.
Unblocking sites may require <u>clearing your Temporary Internet Files</u>
Save Changes and Exit

Open the site, 'This website has been BLOCKED from viewing' message appears Slocked by KDT Site Blocker - Microsoft Internet Explorer 🖌 🐓 🗙 Google p. 🕒 🐑 👻 🙋 http://www.google.com/ View Favorites Tools Help Edit File 🟠 🔹 🔝 🔹 🖶 🔹 🔂 Page 🔹 🎯 Tools 🔹 \* \* 🔏 Blocked by KDT Site Blocker This website has been **BLOCKED** from viewing By **k**<sub>D</sub>T Site Bløcker 💊 2 😜 Internet 100% Done

# Lab 44-06

Objective:

Use **Stop-the-Pop-Up Lite** to block pop-up windows from appearing as you surf the web.

- In the CEHv6 Labs CD-ROM navigate to Module 44
- Install and launch Stop-the-Pop-Up Lite program

Ethical Hacking and Countermeasures v6 Lab Manual

Stop-the-Pop-Up Lite     Image: Stop-the-Pop-Up Lite       Image: Litre
STOP-THE-POP-UP
🗖 Disable pop-up killer.
🔽 Start automatically after reboot.
T Aggressive mode.
5 pop-ups killed so far.
Visit Sureshot! Advanced settings
Press Ctrl, Shift or 'a' to allow pop-ups.
Test your pop-up killer here
Minimize Help

• To disable blocking popups, check the option **Disable pop-up killer** in the control panel

Stop-the-Pop-Up Lite
STOP-THE-POP-UP © SURESHOT
Disable pop-up killer. Start automatically after reboot. Aggressive mode. 5 pop-ups killed so far.
Visit Sureshot! Advanced settings
Disabled. Pop-ups are allowed.
Test your pop-up killer here
Minimize Help



• As the popups are disabled the popup window opens

🏉 ICICI Bank Online : Cards : (	Credit Card - Microsoft	Internet Explorer			
💽 🗸 🖉 https://infinity.icid	ibank.co.in/web/esourcing/js	p/esourcingSti 🗙 🔒 🛃	Google	<b>P</b> -	
File Edit View Favorites Too	ls Help				
🚖 🕸 🌈 ICICI Bank Online : Ca	ards : Credit Card		🚹 🔹 🔝 👘 🖶 🔹 🔂 Pag	e 🔹 🍈 Tools 🔹 🎇	
				<u>^</u>	
<b>VICICI Ba</b>	nk				
	Important Guidelines f	for filling the Credit Ca	ard application form		
Most Important Terms & Con	ditions				
1. Please fill all details marked	mandatory.				
<ol> <li>The correct PAN number has PAN number of only individual</li> </ol>	2. The correct PAN number has to be filled. Applications without PAN number can not be submitted. PAN number of only individuals is acceptable. PAN of HUF or corporates is not acceptable.				
3. ICICI Bank credit card is avai	ilable in selected cities.	The list of cities is availa	able in the drop down box of the	e Present addre	
4. All details to be filled correct	ly and completely.	Ν			
5. Eligibility and Age Criteria					
	Eligibility Criteria				
Cards	Eligibilit	y Criteria			
	Salaried	Self Employed			
All ICICI Bank Silver Credit Card	Rs. 96,000/- p.a.	Rs. 1,00,000/- p.a.			
All ICICI Bank Gold Credit Card	Rs. 1,20,000/- p.a.	Rs. 1,00,000/- p.a.			
ICICI Bank AMEX Gold	Re 2.50.000/- n.a	Re 2.50.000/- n.a		~	
				>	
			😜 Internet	🔍 100% 🔹 💡	

#### **EC-Council**

To enable the

blocking popup uncheck the option **Disable pop-up Killer** in the control panel

📕 Stop-the-Pop-Up Lite
STOP-THE-POP-UP
Disable pop-up killer. Start automatically after reboot. Aggressive mode. 5 pop-ups killed so far.
Visit Sureshot! Advanced settings Press Ctrl, Shift or 'a' to allow pop-ups.
Test your pop-up killer here Minimize Help

#### Now, Browse

the site in the IE browser



skipped resulting the next window

Popup window

Ethical Hacking and Countermeasures v6 Lab Manual

#### **EC-Council**

🖉 B.Tech. III Year I Sem	. Reg. Nov-2007 Results	<ul> <li>Microsoft Internet Explo</li> </ul>	orer	
🔆 🔁 🗸 🖉 🖉	w5.indiaresults.com/Andhra_Pra	adesh/JTBT3Y1S/rollquery.htm	Google	P •
File Edit View Favorites	s Tools Help			
🚖 🏟 🔘 B.Tech. III Yea	ar I Sem. Reg. Nov-2007 Result:	5	🟠 • 📾 - 🖶 • 🗄	Page 🕶 🎯 Tools 👻 🎇
	●M	Home   E IIIMM © Balaji Institute of Nedern Managenere Among Too J B S-Schools in India BIMMpune.com	mail Alerts   Jobs @ IRC   Adve We accept CAT / MAT / XAT / ATMA ex Haven't applied to any, Apply ATM/	click here am scores. Feedback - Ads by C
EGreetings Games	s Forums Profile	Shopping Search:	Site 🔽 🚭	Select State
Notifications ::			(Goverment Of	Kerala) Comman-
Core 2 Dun	YOU	R MUBILE ENTERTAINME Compan	NT ION	vse gree
Advertisements ::			Certificate cour	se in Aviation Mar
CLICK HERE TO APPLY 12 9314881683, 9829058655	Jawahar B.Te	lal Nehru Technol ch. III Year I Sem. Reg.	ogical University Nov-2007 Results	PJFoundat Poornima- JI Educational Found: Nob: 9829255105/98295
REG SUPPLY BATCHES SURE SHOT SUCCESS ADMISSION OPEN B.Tech Tutions 92451177 / 040-66327577	To get your results e.g. JNTUBT	on SMS type JNTUBT3 send to 5676750 3 <b>Y1S 01371A1229</b> sei	Y1S <hallticketno> &amp; and to <b>5676750</b></hallticketno>	B.E / BTeo B Pharma BHMCT Ph.No. 9314088
<				2 4000
			👹 Internet	☜ 100% ▾ 🧰

popups blocked is shown on the control panel

Stop-the-Pop-U	p Lite 📃 🗖
STOP-TI	1F-POP-UI
Disable pop-up	killer.
🔽 Start automatic	ally after reboot.
Aggressive mod	le.
6 pop-ups killed so	far.
Visit Sureshot!	Advanced settings
Press Ctrl, Shift or 'a	a' to allow pop-ups.
Testusur	non un killer here
<u>Test your</u>	pop-up killer here
M	inimize Help

The number of

## Objective:

Use **Super Ad Blocker** to prevent the ads such as Pop-Up and Pop-Under, Flash and Rich Media Ads, Fly-in and Slide-in Ads, Common Ad Banners, Web Page Dialog Ads, Desktop Messenger Ads, Spyware/Adware Ads, etc.

- In the CEHv6 Labs CD-ROM navigate to Module 44
- Install and launch Super Ad Blocker program

Super Ad Blocker
SUPERAdBlocker.com
General Options Ad Blocking Ad Management History Cleaning Cookie Cleaning Notification Statistics Help
General General program options including starting with Windows and browser specific options.
Start-Up Options Automatic Updates
Start Super Ad Blocker when Windows starts  Automatically check for program updates  Show splash screen on startup Use Windows XP style menus  Finable HotKeys for Super Ad Blocker  Automatic updates are safe and secure. No
Internet Explorer Specific Options our servers.
Display Super Ad Blocker Toolbar     SUPERAntiSpyware Scanner       Configure Toolbar     Scan your computer for harmful software.
Disable script error display in Internet Explorer       Scan your Computer         Add Super Ad Blocker Menu to Internet Explorer       Image: Computer Compute
Close

## • Go **General Options** tab and check the desired options

Super Ad Blocker	$\mathbf{X}$
SUPERAdBlocker.com	
General General program options including starting with Windows	and browser specific options.
Start-Up Options  Start Super Ad Blocker when Windows starts  Show splash screen on startup Use Windows XP style menus  Enable HotKeys for Super Ad Blocker  Internet Explorer Specific Options Display Super Ad Blocker Toolbar  Configure Toolbar  Disable script error display in Internet Explorer  Add Super Ad Blocker Menu to Internet Explorer	Automatic Updates  ✓ Automatically check for program updates  Check for Updates  Automatic updates are safe and secure. No personal information is ever communicated to our servers.  SUPERAntiSpyware Scanner  Scan your computer for harmful software.  Scan your Computer  ✓ Enable Real-Time Spyware Protection
	Close

Go to Ad Blocking tab and explore various options



Open a site in

the IE browser



Write click on

an image and click on Block Image from eccouncil.org



• Again open the same site and check blocked image

EC-Council Security Certification - Mozilla Firefox	
Eile Edit View Higtory Bookmarks Iools Help	0
	Q
Firefox will now always block images from eccouncil.org.	
Mission   Members   Roll of Honor   EC-Council University   EC-Council Global Services (	EGS)
Attend Hacker Halted 2008 Security Event in USA May 29th - June 4th 2008, Myrtle Beach Halted	тя 1
	>
Done	1

# Lab 44-10

Objective:

Use **iProtectYou** software for internet content filtering to protect children from accessing harmful information on the Internet.

- In the CEHv6 Labs CD-ROM navigate to Module 44
- Install and launch i Protect You program

Ethical Hacking and Countermeasures v6 Lab Manual

Ethical Hacking and Countermeasures v6 Lab Manual

#### **EC-Council**



## Click Internet

## Timetable to set time table



Thursday Friday

Saturday

Permit All

**EC-Council** 

То

•

disable



Click on "Forbid All" to disable Internet access completely for

Daily Time Limits

## internet access continuously for a group, Click Forbid All

The color

**?** 

For example 10 means from 10:00 to 10:59

changes after disabling the internet access

the selected group.

rbid All



Page | 818

Access

restriction message will appear while browsing a site



# Lab 44-11

## Objective:

Use **Block Porn** to block anti pornography material or adult material on the Internet by adopting advanced interception technology.

- In the **CEHv6 Labs CD-ROM** navigate to **Module 44**
- Install and launch Block Porn program

#### Ethical Hacking and Countermeasures v6 Lab Manual





To set the website restrictions, Click **Block Set**

🖀 MpSoft Block	Porn(V4.1 Stadard)	
About BlockSet System Help Help Register	Select Mode       User Add       Fault tolerance       Remote update       History record            • Web site restrict mode(cannot accessing restricted site)           • Web site lock mode(can accessing following list site only)             • Web site lock mode(can accessing following list site only)           • Add             • Web site lock mode(can accessing following list site only)           • Add             • Web site lock mode(can accessing following list site only)           • Remove	
📣 Ex	t 🗳 Save 🛐 Hid	3

• To add website, Click Add

🖀 MpSoft Block	Porn(V4.1 Stadard)	
About About BlockSet System Help Help Register	Select Mode       User Add       Fault tolerance       Remote update       History record         Image: Web site restrict mode(cannot accessing restricted site)       Image: Web site lock mode(can accessing following list site only)         Image: Web site lock mode(can accessing following list site only)       Image: Web site lock mode(can accessing following list site only)         Image: Web site lock mode(can accessing following list site only)       Image: Web site lock mode(can accessing following list site only)         Image: Web site lock mode(can accessing following list site only)       Image: Web site lock mode(can accessing following list site only)	
, <b>⊄≫</b> E×	it 🔤 Hid	e

ebsite address and cl	ck <b>OK</b>	Enter
Add web site		
Enter web site add	ess www.google.com	
	R <sup>®</sup> ∕ ok*	Cancel
anges, Click <b>Save</b>		To a
MpSoft Block Po	n(V4.1 Stadard)	
Se	ct Mode User Add Fault tolerance Remote update History record	
About	Web site restrict mode(cannot accessing restricted site)	
BlockSet	• Web site look mode(can accessing following list site only)	
<b>N</b>	GOOGLE.COM	
System	🕱 Edit	
Help	Remove	
Register		
<b>d≱</b> Exit	By Save	lide
rompting message ar	pears Click <b>OK</b>	When

 System prompt
 Image: System prompt

 Image: Wour setup save successfully, current configuration will take effect at new IE window!

 Image: Wour setup save successfully, current configuration will take effect at new IE window!

Page | 822

.

#### **EC-Council**

Select the site

other than one added to the list in the browser

C ERROR PAGE - Microsoft Internet Explorer		
C:\pornview.htm	🗙 😽 🗙 Google	<b>₽</b> -
File Edit Vi 🖉 http://www.microsoft.com/	7	
🚖 🏟 🌈 ERROR PAGE		🖶 🔹 🔂 Page 👻 🍈 Tools 👻 🎽
ERROR - Warning! Oops You can see this page, maybe contains porno or other ins it was forbbi Otherwise, Please repo T	s~~ So Sorry! is because you visited webpage ggraphy material, adult material appropriate material, den by administrator. ort this problem to administrator. hank you!	
	Back	
		http://www.mpinfo.net
	😏 My Com	puter 🔍 100% 🔻 💡

It displays an

## error message as shown



The site added

to list can be accessed without any restrictions



- In the CEHv6 Labs CD-ROM navigate to Module 44
- Open the **ContentFiltering.pdf** and read the content

Ethical Hacking and Countermeasures v6 Lab Manual

#### **EC-Council**



- In the CEHv6 Labs CD-ROM navigate to Module 44
- Open the **Investigating large-scale Internet content filtering.pdf** and read the content



- In the CEHv6 Labs CD-ROM navigate to Module 44
- Open the filtereffectiveness.pdf and read the content



- In the CEHv6 Labs CD-ROM navigate to Module 44
- Open the Internet Content Filtering Solution.pdf and read the content

🔁 Int	ternet	Conten	t Filte	ering	Sol	ution	.pdf	- A do	be R	eade	ſ											
File E	Edit Vie	w Docu	iment	Tools	s W	indow	Help															×
0	• 80	)% •		<b>↓</b>	÷	Fin	3		•													
Ē				Inte	ern	et C	onte	ent F	ilte	ering	g S	olı	utic	n								<b>^</b>
?	L			Info The com and to ce	Orm Child plian tech	dren's ice wi nology n visu	Inter th thi mea al dep	acke net Pr s legis sures piction	otec latio in pl	tion A n, pu lace to	Act ( blic o blo	(CIP sch ock	PA) b nool d or fi	ecam Jistric ilter	e lav cts m Interr	v on / ust ce net ac	April 20 ertify t coess f	), 200 hat th or bot	1. In o ey ha h min	order t ve the ors and	to be in policies d adults	
	L			The cont Web Act	Offi ent sens (CIP#	ce of filteri e, has ().	Tech ng in beer	inolog its s impl	y Se choo emer	rvices Is and nted i	s of d di: in or	An istri rder	nders ict o r to	on S ffice. comp	chool . The Iy wi	Dist Inte th th	rict Fo rnet c e Chilo	our ha onten Iren's	s ena t filte Interr	bled I ring s net Pro	Internet olution, otection	
				We	bsit	e Ca	tego	ries h are l	heind	a bloc	ked :	are	a ac fe	allow	<b>c</b> •							
				me	cate	• A	dult	Conter	nt	s bloc	Keu i	are	asi	buow	5.							
						• 1	ludity	1														
						• 5	ex															
						• -	inger	le and	Swir	msuit												
							AD3	1 Drug	>													
						. (	Gambl	ine														
						• (	Sames	5														
						•	llegal	/Ques	tiona	able												
						• •	lackir	ig														
						• •	Veb C	hat	2,1227													
D							Antitar	ICY / E	xtre	mist												
Ø						• P	erson	als/D	ating													
						• 1	astel	ess														
						• \	/iolen	ce														
	10					• 1	Veapo	ons														~
	8.5	0 x 11.00	) in	<										Ш								>

- In the CEHv6 Labs CD-ROM navigate to Module 44
- Open the **The Filtering Matrix.pdf** and read the content





# Module 45

# Privacy on the Internet

# Lab 45-01

Objective:

Use **HistoryKill** to securely delete history traces on computer with the File Shredder.

- In the CEHv6 Labs CD-ROM navigate to Module 45
- Install and launch "History Kill" program

👼 HistoryKill 2007 - Pr	otecting Your Privac	y Since 1997!			×
Menu Auto-Kill Help					
	Kill 20 Net privacy to	)07 ol" - CNN			
Mozilla Firefox	AOL	File Shredder			
Internet Explorer	Windows	Auto-Kill	Boss Key! Setup		
URL address di URL address di Internet Histor Temp Internet AutoComplete index.dat All of the above	op-list box □ Go y file □ Se Files ☑ Co Cho e day(s)	oogle Toolbar history earch Button history bookies <b>Dose which cookies to</b> Cookie Manager	• keep:		
Help File Shredde	Purchase HistoryKill M	has killed 0 history tr	Kill Now!		

## Click on Internet Explorer

🙀 HistoryKill 2007 - Protecting Your Privacy Since 1997! 🛛 🛛 🗙
Menu Auto-Kill Help
History Kill 2007 "TOP INTERNET PRIVACY TOOL" - CNN
Mozilla Firefox AOL File Shredder
Internet Splore: Windows Auto-Kill Boss Key! Setup
Internet Explorer / MSN Privacy       Image: Complex of the story         URL address drop-list box       Google Toolbar history         Internet History file       Search Button history         Internet Files       Cookies         AutoComplete       Index.dat         Index.dat       Cookie Manager
Evaluation expires in 15 day(s)
Help File Shredder Purchase Kill Now!
http://www.historykill.com HistoryKill has killed 0 history traces since installation.

• Select the required Options from the list

🙀 HistoryKill 2007 - Pi	otecting Your Privac	y Since 1997!	<u>x</u>
Menu Auto-Kill Help			
History "TOP INTER	Kill 20 Net privacy to	)07 01″ - M	
Mozilla Firefox	AOL	File Shredder	]
Internet Explorer	Windows	Auto-Kill	Boss Key! Setup
Internet Capiton         Internet Histor         Internet Histor         Temp Internet         AutoComplete         index.dat         All of the abov         Evaluation expires in 15         Help         File Shredd         http://www.historykill.com	rop-list box Go y file 56 Files CC c day(s) ar Purchase MistoryKill f	ogle Toolbar history arch Button history ookies oose which cookies to Cookie Manager	to keep: Kill Now!
• Click on **Kill Now** to remove the Internet traces

istoryKill 2007 - Pr Menu Auto-Kill Help	otecting Your Privac	/ Since 1997!	_		×
	Kill 20	07 DL" - CN			
Mozilla Firefox	AOL	File Shredder	1		
Internet Explorer	Windows	Auto-Kill	Boss Key! Setup		
Internet Explore	er / MSN Privacy 📷	HistoryKill - Protecting S	ince 1997!	X	
URL address di AltoComplete and AltoComplete Alt of the above Evaluation expires in 15 Help File Shredde http://www.historykill.com	rop-list box [ y file [ Files [ e day(s) e HistoryKill ha	Removing your Inter ling Internet Explorer's cooki ling Windows Recent Docur ling Windows Recycle Bin uccessful! Your privacy is provide a state of the state	rnet traces Now ies ments list otected. issince installation.		

#### **EC-Council**

Click on Windows

•

👹 HistoryKill 2007 - Protecting Your Privacy Since 1997!	×
Menu Auto-Kill Help	
History Kill 2007 "TOP INTERNET PRIVACY TOOL" - CNN	
Mozilla Firefox AOL File Shredder	
Internet Explorer Auto-Kill Boss Key! Setup	
✓ Windows Media player recent URL/file list         ✓ Windows Recycle Bin         ✓ Windows Recent Documents list         ✓ Windows Temp Folder         ✓ Windows File Fragments (*.CHK)         ✓ Windows Start, Run drop-list         ✓ MS Office Recent File List	
Evaluation expires in 15 day(s)       Help       File Shredder       Purchase       Kill Now!	
http://www.historykill.com HistoryKill has killed 10 history traces since installation.	

• Click on **Kill Now** to remove the Internet traces

Menu Auto-Kill 2007 - Pr	otecting Your Privac	cy Since 1997!
History "TOP INTER	<b>Kill 2</b> 0	007 OL" - CNN
Mozilla Firefox	AOL	File Shredder
Internet Explorer	Windows	Auto-Kill Boss Keyl Setup
Windows Privac	у 👩	HistoryKill - Protecting Since 1997
Windows Me     Windows Re     Windows Re     Windows Ter     Windows File     Windows Sta     MS Office Re     All of the abo	dia player recent UF cycle Bin cent Documents list mp Folder e Fragments (*.CHK) art, Run drop-list ecent File List	Removing your Internet traces Now
Evaluation expires in 15	dav(s)	
Help File Shredde	er Purchase	Kill Now!
http://www.historykill.com	n HistoryKill h	as killed 15 history traces since installation.

• Click on Auto-Kill

🔯 HistoryKill 2007 - Prote	cting Your Privacy Since 1	997!				>
Menu Auto-Kill Help						
History "TOP INTERNE	KIII 2007 T PRIVACY TOOL" - (	ME				
Mozilla Firefox	AOL File 9	Shredder				
Internet Explorer	Windows 🏼 🏹	to-Kill	Boss Keyl Setup	p [		
Auto-Kill on Window     Auto-Kill on Last Bro     Auto-Kill every: 15     What to show when	s startup wser Window close Minutes	Auto-Killing Setti	ings			
C Stealth Mode - Aul	o-Kill with HistoryKill hidden w Progress Window During Au Hide Tray Icon (ALT-Z to Shov	uto-Kill w HistoryKill)				
Evaluation expires in 15 day	(\$)					
Help File Shredder	Purchase	🄖 Ki	ll Now!			
http://www.historykill.com	HistoryKill has killed 1	15 history trace	s since install	lation.		

#### **EC-Council**

Click on Auto-Killing Settings

🙀 HistoryKill 2007 - Prot	ecting Your Privacy S	ince 1997!			×
Menu Auto-Kill Help					
History "TOP INTERN	KIII 200	)7 ″ - M			
Mozilla Firefox	AOL	File Shredder			
Internet Explorer	Windows	Auto-Kill	Boss Key! Setup		
<ul> <li>✓ Auto-Kill on Window</li> <li>✓ Auto-Kill on Last Br</li> <li>☐ Auto-Kill every: 15</li> </ul>	vs startup owser Window close i Minutes	Auto-Killin	Settings		
What to show when C Stealth Mode - Au Display Mode - St	Killing: ito-Kill with HistoryKill hido now Progress Window Du	len Iring Auto-Kill			
Complete Stealth	- Hide Tray Icon (ALT-Z t	o Show HistoryKill)			
Evaluation expires in 15 da Help File Shredder http://www.historykill.com	y(s) Purchase HistoryKill has k	killed 15 history	Kill Now!		

• Select the options and click on **Save** 

	Kill 2007 HistoryKill Auto-Kill Setup	
Mozilla Firefox At Internet Explorer pr	uto-Kill is a feature of HistoryKill that automatically clears the below privacy problems immediately after you lose your web browser, or at the start up of Windows. Auto-Kill is essential in always maintaining your rivacy on your computer. Put a Checkmark next to the Internet trace to automatically Kill during Auto-Kill:	
When to Kill: Auto-Kill on Winc Auto-Kill on Last Auto-Kill every: What to show wh C Stealth Mode - C Display Mode -	Internet Explorer / MSN Privacy	
Evaluation expires in 15       Help       File Shredde	Help Default Cancel Save the above settings Save the above settings HistoryKill has killed 15 history traces since installation.	

• Click on **Kill Now** to remove the Internet Traces

<mark>e HistoryKill 2007 - Protect</mark> i Menu Auto-Kill Help	ing Your Privacy S	ince 1997!					X
Historyk "TOP INTERNET	GII 200 PRIVACY TOOL	)7 "- (N)					
Mozilla Firefox	AOL	File Shredder	1				
Internet Explorer	Windows	Auto-Kill	Boss Keyl Setu	p			
Auto-Kill Settings 🔲 Dis	able Auto-Kil 🔯 His	toryKill - Protec	ting Since 1997!		×		
When to Kill:         Auto-Kill on Windows sl         Auto-Kill on Last Brows:         Auto-Kill every:         Auto-Kill every:         15 Mir         What to show when Kill         C Stealth Mode - Auto-K         Display Mode - Show	tartup er Window cl nutes ing: Killing Killing Killing Killing Killing Killing Killing	Removing your Internet Explorer's Windows Recent Windows Media I Windows Media I Windows Recycl Windows TEMP essfull Your privad	r Internet traces No s cookies t Documents list Player recent lists e Bin folder cy is protected.		ĸ		
Evaluation expires in 15 day(s)	de Tray Icon (ALT-Z )	o Show HistoryKill)	k V				
Help File Shredder	Purchase		Kal Now!				
			THESE SHIES HISIO	inition.			

Click on File Shedder

🙀 HistoryKill 2007 - Protecting Your Privacy Since 1997!
History Kill 2007 "TOP INTERNET PRIVACY TOOL" - CNN
Mozilla Firefox     AOL       Internet Explorer     Windows       Auto-Kill     Boss Key! Setup
Auto-Kill Settings       Disable Auto-Kill (Not Recommended)       > Test Auto-Kill Now         When to Kill:           ✓ Auto-Kill on Windows startup       Auto-Killing Settings         ✓ Auto-Kill on Last Browser Window close       Auto-Killing Settings         ✓ Auto-Kill every:       15 Minutes         ✓ What to show when Killing:
Evaluation expires in 15 day(s) Help File Shredder Purchase Kill Now! http://www.historykill.com HistoryKill has killed 22 history traces since installation.

• Save the Changes

🙀 HistoryKill 2007 - Prot	ecting Your Privacy	Since 1997!						
History "TOP INTERN	Kill 20 et privacy too	07 L'' - CN						
Internet Explorer Mozilla Firefox	Windows AOL	Auto-Kill File Shredder	Boss Key! Setup					
Remember! Man will i soft HistoryKill will secure or recovered by oth your Internet histor Overwrite y Saved! Tra	Remember! Manually deleting your history traces on your computer will NOT protect you from someone using UNDELETE software to recover your history traces!         HistoryKill will securely delete Internet traces so that they can NOT be undeleted or recovered by others. Below you can set how many times HistoryKill overwrites your Internet history traces with completely random data:         Overwrite your Internet traces       Image: Traces will be overwritten 7 times!							
Evaluation expires in 15 da	y(s)							
http://www.historykill.com	HistoryKill has	killed 22 history tra	Kill Now! races since installation.					

#### Objective:

Use NetDefender Firewall to block all referring traffic.

- In the CEHv6 Labs CD-ROM navigate to Module 45
- Install and launch "NetDefender Firewall" program

<mark>60</mark> Fil	NetDefender e Tools Help									
	Start Stop	Block All Allow Al	Block Ping   App I	nfo Port Scan Ab	out					
	Belo	w are the rules that	are currently regis	stered by Netdefend	er.					
	SOURCE IP	DESTINATION IP	SOURCE PORT	DESTINATION PORT	PROTO					
			k,							
	<b>Ⅰ</b>									
	🔂 Add New Rules 📝 Edit Rule 😹 Remove Rule 📚 Re-Register Rules									
For	r Help, press F1			NU	м 📃 🥥 🍑					

**EC-Council** 

Click on Start

	) ile	jetDefender Start the Netc	tefender			_ 🗆 X					
		Start Une Wett	Block All Allow A		nfo Port Scan Ab	out					
	[	Belo	w are the rules tha	t are currently regi	stered by Netdefend	er.					
		SOURCE IP	DESTINATION IP	SOURCE PORT	DESTINATION PORT	PROTO					
	1										
		•				Þ					
	Add New Rules I Edit Rule Edit Rule Remove Rule Re-Register Rules										
F	or H	lelp, press F1			NU	м 📃 🍚 🥥					

Click on **Tools** and **Select Port Scanner**

🛞 NetDefende	:r									
File Tools He	lp									
Port	Scanner			<b></b>						
🛛 🕻 😋 <u>B</u> lock	🛛 🔄 🔤 🛃 🗸 🖉 🖉									
Searc		Allow A	Block Ping    App I	nfo Port Scan	About					
	Dolow	are the rules that	are currently regis	stored by Notda	fondor					
					DODT	PPOTO				
		ESTINATION IF	JUDICE FUNT	DESTINATION	-UNI	rhoro				
91 S										
-										
Add New	Hules	<u>E</u> dit Ru	ule <u>×</u> <u>R</u> emov	ve Hule	🏂 He-Heg	gister Hules				
Port Scanner for	scanning	g open port in a sys	tem		NUM	- I I I I I I I I I I I I I I I I I I I				

Ethical Hacking and Countermeasures v6 Copyright © **EC-Council** All Rights Reserved. Reproduction Strictly Prohibited.

**EC-Council** 

Ethical Hacking and Countermeasures v6 Lab Manual

• Write the **IP Address** and **Range of Ports** 

<b>W</b> NetD	🛾 Port Scanne	r				× ×
File To	IP address	of the remote a single port a range of ports er of attempts:	machine: 1 1 due 2 1	92 . 168 .	0 . 12	
	Result of sc	anning:				
	IP address	Port number	Port Status	Attempts	Remarks	
I						
<u>ο</u> Αα						Rules
For Help,	Ready					

• Click on **Start** and check the **Result of Scanning** 

8	NetD	C Port Scanner	r				×	. 🗆 🗙
File	е То С	IP address	of the remote r	nachine: 1	92 . 168 .	0.12		
	Start	O Scan a	i single port	1 duo 2				
		Numbe	er of attempts:	1 1	~	Start Sto	2P	
	<u> </u>	Result of sca	anning:			hç		
		IP address	Port number	Port Status	Attempts	Remarks		
		192.168.0.12	1	Close	1			
		192.168.0.12	2	Close	1			
		192.168.0.12	3	Close	1			
		192.168.0.12	4	Close	1			
		192.168.0.12	5	Close	1			
		192.168.0.12	5	Close	1			
		192 168 0 12	8	Close	1			
	<u> A</u> c		-					Rules
For	Help,	Ready						00

Ethical Hacking and Countermeasures v6 Copyright © **EC-Council** All Rights Reserved. Reproduction Strictly Prohibited.

**EC-Council** 

Ethical Hacking and Countermeasures v6 Lab Manual

Click on Tools and Select on BlockScanner

1	etDefender					<u> </u>
File	Took Help	,				
(	Ort Scan					
			I Door Lind Lubb 1	Port Starr	About	
	Belo	w are the rules that	are currently regis	tered by Netdef	ender.	
	SOURCE IP	DESTINATION IP	SOURCE PORT	DESTINATION P	ORT	PROTO
						5 2
	•					Þ
6	🗋 Add New Rule	s 📝 <u>E</u> dit Ru	ile 🔀 <u>R</u> emov	/e Rule	} Re-Reg	ister Rules
List o	of Applications Acc	cessing Network			NUM	- 0

Check on Running Application

Running / Running The A to net	Application Application Application Application twork.	nefender ons ns : ons listed Below a	are those which a	are currently ru	inning on your syst	em and trying t	x connect
Proto	Pid	Process Name	Local Address	Local Port	Remote Address	Remote Port	State
😻 ТСР	1772	apache.exe	0.0.0	80	0.0.0.0	-	LISTENING
🔮 ТСР	1132	svchost.exe	0.0.0	135	0.0.0.0	-	LISTENING
🔮 ТСР	1772	apache.exe	0.0.0	443	0.0.0.0	-	LISTENING
🔮 ТСР	4	System	0.0.0.0	445	0.0.0.0	-	LISTENING
🔮 ТСР	1896	mysqld-nt.exe	0.0.0	3306	0.0.0.0	-	LISTENING
🔮 ТСР	2836	alg.exe	127.0.0.1	1031	0.0.0.0	-	LISTENING
🔮 ТСР	3852	firefox.exe	127.0.0.1	1048	127.0.0.1	1049	ESTABLISHE
🔮 ТСР	3852	firefox.exe	127.0.0.1	1049	127.0.0.1	1048	ESTABLISHE
🔮 ТСР	3852	firefox.exe	127.0.0.1	1050	127.0.0.1	1051	ESTABLISHE
TCP	3852	firefox.exe	127.0.0.1	1051	127.0.0.1	1050	ESTABLISHE
	Lor Holo	proce h1				ОК	Cancel
	For Help,	, press H1					

**EC-Council** 

## Lab 45-03

Objective:

**Privacy Eraser** is an Internet **Eraser** that protects Internet **privacy** by cleaning up all the tracks of Internet and computer activities.

- In the CEHv6 Labs CD-ROM navigate to Module 45
- Install and launch "Privacy Eraser" program

🥜 Privacy Eraser Pro (Unregistered - 14 Days Left)	<b>- - ×</b>
Main Windows Browsers Plug-Ins File Shredder Drive Ops Advanced Schedule Misc. /	About
Profes	SET ssional PRMACY Its Reserved.
Quick Clean & Reboot ▼ Stop Tasks <u>H</u> elp	<u>E</u> xit
	^
k,	
<li></li>	>

**EC-Council** 

Click on Quick Clean



**EC-Council** 

Privacy Eraser Pro is Initializing

🥜 Privacy Eraser Pro (Unregistered - 14 Days Left) 💿 💽 💽
Main Windows Browsers Plug-Ins File Shredder Drive Ops Advanced Schedule Misc. About
Professional         Copyright(C) 2002-2007 PrivacyEraser Computing, Inc. All Rights Reserved.
Quick Clean & Reboot 🔻 Stop Tasks Help Exit
Initalizing Privacy Eraser Pro Computer Name: EC-A50783B2565A Current Username: Admin Windows Type: Microsoft Windows XP Windows Version: 5.1 (Build 2600) Service Pack 2 Windows Main Directory: C:\WINDOWS Windows System Directory: C:\WINDOWS\system32 Windows Temporary Files Directory: C:\DocUME~1\Admin\LOCALS~1\Temp Internet Explorer Cache Directory: C:\DocUments and Settings\Admin\Local Settin( Internet Explorer Cache Directory: C:\Documents and Settings\Admin\Local Settin; Internet Explorer History Directory: C:\Documents and Settings\Admin\Local Sett: Privacy Eraser Pro Ready
< >

Tracks for the Internet and Computer Activity are erased

🥜 Privacy Eraser Pro (Unregistered - 14 Days Left)
Main Windows Browsers Plug-Ins File Shredder Drive Ops Advanced Schedule Misc. About
Professional         Copyright(C) 2002-2007 PrivacyEraser Computing, Inc. All Rights Reserved.
Quick Clean & Reboot 🔻 Stop Tasks Help Exit
Internet Explorer History Directory: C:\Documents and Settings\Admin\Local Sett:
Privacy Eraser Pro Ready
Erasing Windows Recent Document List Windows Recent Document List Erased.
Erasing Windows Run History Windows Run History Erased.
Erasing Windows Find Computer History Windows Find Computer History Erased.
Erasing Windows Find Files/Folders History Windows Find Files/Folders History Erased.
Erasing Windows Open/Save History Windows Open/Save History Erased.
Erasing Windows Clipboard Windows Clipboard Erased.
Erasing Windows Paint Recent File List

Objective:

Use **Sunbelt Personal Firewall** to protect and control your Internet connection.

- In the CEHv6 Labs CD-ROM navigate to Module 45
- Install and launch "Sunbelt Personal Firewall" program

🜆 Sunbelt Personal Firewal	II		
Personal Firewall 4	Connections Statistics	Preferences License	
Overview       Image: Overv	Local Point Remote Point	Protocol Speed In S TCP, UDP TCP TCP UDP, 255 TCP, UDP TCP TCP	peed Out
Logs & Alerts         Utgoing:       0.98 KB/s         Dutgoing:       0.99 KB/s         Stop all traffic	k 		
	Connected in: 6     Connected out: 6	S Listening: 19	Þ
	Register	Help OK Cancel	Apply

## • Check the **Overview** of the System

퉳 Sunbelt Personal Firewa	ll			
Personal Firewall 4	Connections	Statistics	Preferences	License
Overview	Local Point	Remote Point	Protocol	Speed In Speed Oul
	🖃 🥘 Firefox		тср	
Network Security	📫 All: 1049	localhost: 1048	TCP	
	🕩 All: 1051	localhost: 1050	TCP	
Intrusions	🔃 localhost: 1048	localhost: 1049	TCP	
	🔃 localhost: 1050	localhost: 1051	TCP	
🔔, Web	📃 🖃 Application Layer Gates	way Service	ТСР	
	📙 localhost: 1031		TCP	
Logs & Alerts	🗉 🖃 LSA Shell (Export Versio	n)	UDP, 255	
	S All	All	255	
	S All: 4500		UDP	
	S All: isakmp		UDP	
	🖃 🔲 Generic Host Process fo	r Win32 Services	TCP, UDP	
	All: 1597		UDP	
Outgoing: 0.00 KB/s	All: 1025		UDP	
Incoming: 0.25 KB/s	All: romap		TCP	
5 Stop all traffic	S localfièst: 1900		UDP	
	S localhost: ntp		UDP	
	5 192.168.0.12: 1900		UDP	
	5 192.168.0.12: ntp		UDP	
	🗄 🔪 Apache HTTP Server		TCP	
	🗄 🛄 mysqld-nt		ТСР	
	•			Þ
	🐠 Connected in: 6 🛛 🙀 C	Connected out: 6	🖕 Listening: 19	
L				
		Register	Help OK	Cancel Apply

## Click on Network Security

Sunbelt Personal Firewall	Applications	Predefined	Trusted area	Advanced
Overview         Network Security         Intrusions         Web         Logs & Alerts         Outgoing:       0.00 KB/s         Incoming:       0.15 KB/s	<ul> <li>Enable Network security module</li> <li>Description         <ul> <li>wcescomm</li> <li>wcesmgr</li> <li>rapimgr</li> <li>ceappmgr</li> <li>Internet Explorer</li> <li>LSA Shell (Export Version)</li> <li>Windows NT Logon Appl</li> <li>Userinit Logon Application</li> <li>Generic Host Process fo</li> <li>avgemc</li> <li>AVG Update downloader</li> <li>Microsoft File and Printe</li> <li>Any other application</li> </ul> </li> </ul>	In     Out       X     deny     permit       X     deny     permit	Internet In Out Control Out Out Out Out Out Out Out Out	Log         Alert           -         - </th
Stop all traffic	Edit Remove	Register	Pao Help OK	tket filter Refresh

## Click on **Instructions** and Select the tabs



#### • Click on **Web** and Select the Tabs

🌆 Sunbelt Personal Firewa		J
Sunbelt Personal Firewall 4	Ad blocking Privacy Site exceptions	
Overview	C Enable web filtering	
Network Security	Advertisements       Image: Block advertisements     Set	
	Popups	
Web	Block pop-up and pop-under windows	
Logs & Alerts	Temporarily override by pressing down the Ctrl 💌 key	
	Web content	
	Block JavaScripts Block VBScripts	
	Block ActiveX	
Incoming: 0.00 KB/s		
Stop all traffic		
	Register Help OK Cancel Apply	

#### Click on Logs and Alerts

	Line	Co	Date	Method	URL	Subject	Value 🛃
	1251	1	21/Jan/2008 11:55:08	GET	192.168.0.2/vo/groupAdmin.do?mo	referer	http://19
Network Security	1252	1	21/Jan/2008 11:55:24	GET	192.168.0.2/vo/jsp/hide.jsp	referer	http://19
	1253	1	21/Jan/2008 11:55:25	GET	192.168.0.2/vo/desktop.do	referer	http://19
Intrusions	1254	1	21/Jan/2008 11:55:49	GET	192.168.0.2/vo/mailFrame.do?&use	referer	http://19
angebanan sa	1255	1	21/Jan/2008 11:55:49	GET	192.168.0.2/vo/jsp/subFrame.jsp?c	referer	http://19
Mab	1256	1	21/Jan/2008 11:55:49	GET	192.168.0.2/vo/jsp/mailFrame.jsp?s	referer	http://19
web	1257	1	21/Jan/2008 11:55:50	GET	192.168.0.2/vo/mailTab.do?show=/	referer	http://19
	1258	1	21/Jan/2008 11:55:50	GET	192.168.0.2/vo/mtree.do?accountI	referer	http://19
.ogs & Alerts	1259	1	21/Jan/2008 11:55:50	GET	192.168.0.2/vo/tree.do?accountId	referer	http://19
	1260	1	21/Jan/2008 11:55:52	GET	192.168.0.2/vo/jsp/mailCount.jsp?a	referer	http://19
	1261	1	21/Jan/2008 11:56:06	GET	192.168.0.2/vo/mail.do?order=dow	referer	http://19
	1262	1	21/Jan/2008 11:56:06	GET	192.168.0.2/vo/jsp/lang_en.jsp	referer	http://19
	1263	1	21/Jan/2008 11:56:12	POST	192.168.0.2/vo/mail.do	referer	http://19
: 0.00 KB/s	1264	1	21/Jan/2008 11:57:09	GET	192.168.0.2/vo/jsp/lang_en.jsp	referer	http://19
: 0.00 KB/s	1265	1	21/Jan/2008 11:57:09	POST	192.168.0.2/vo/tree.do?accountId	referer	http://19
	1266	1	21/Jan/2008 11:57:13	POST	192.168.0.2/vo/readMail.do	referer	http://19
top all traffic	1267	1	21/Jan/2008 12:04:24	POST	192.168.0.2/vo/tree.do?accountId	referer	http://19
	1268	1	21/Jan/2008 12:04:29	POST	192.168.0.2/vo/readMail.do	referer	http://19
	1269	1	21/Jan/2008 12:04:39	POST	192.168.0.2/vo/readMail.do	referer	http://19
	1270	1	21/Jan/2008 12:04:44	GET	192.168.0.2/vo/jsp/subFrame.jsp?c	referer	http://19
	1271	1	21/Jan/2008 12:05:14	GET	192.168.0.2/vo/desktop.do?show= <u>.</u>	referer	http://19
		etwork		HIPS	Behavior Web /		التد

• To stop all traffic , Click on **Stop all traffic** 

Line	Co	Date	Method	URL	Subject	Value
1251	1	21/Jan/2008 11:55:08	GET	192.168.0.2/vo/groupAdmin.do?mo	referer	http://1
rity 1252	1	21/Jan/2008 11:55:24	GET	192.168.0.2/vo/jsp/hide.jsp	referer	http://1
1253	1	21/Jan/2008 11:55:25	GET	192.168.0.2/vo/desktop.do	referer	http://1
1254	1	21/Jan/2008 11:55:49	GET	192.168.0.2/vo/mailFrame.do?&use	referer	http://1
1255	1	21/Jan/2008 11:55:49	GET	192.168.0.2/vo/jsp/subFrame.jsp?c	referer	http://1
1256	1	21/Jan/2008 11:55:49	GET	192.168.0.2/vo/jsp/mailFrame.jsp?s	referer	http://1
1257	1	21/Jan/2008 11:55:50	GET	192.168.0.2/vo/mailTab.do?show=/	referer	http://1
1258	1	21/Jan/2008 11:55:50	GET	192.168.0.2/vo/mtree.do?accountI	referer	http://1
1259	1	21/Jan/2008 11:55:50	GET	192.168.0.2/vo/tree.do?accountId	referer	http://1
1260	1	21/Jan/2008 11:55:52	GET	192.168.0.2/vo/jsp/mailCount.jsp?a	referer	http://1
1261	1	21/Jan/2008 11:56:06	GET	192.168.0.2/vo/mail.do?order=dow	referer	http://1
1262	1	21/Jan/2008 11:56:06	GET	192.168.0.2/vo/jsp/lang_en.jsp	referer	http://:
1263	1	21/Jan/2008 11:56:12	POST	192.168.0.2/vo/mail.do	referer	http://1
1264	1	21/Jan/2008 11:57:09	GET	192.168.0.2/vo/jsp/lang_en.jsp	referer	http://1
B/s 1265	1	21/Jan/2008 11:57:09	POST	192.168.0.2/vo/tree.do?accountId	referer	http://:
1266	1	21/Jan/2008 11:57:13	POST	192.168.0.2/vo/readMail.do	referer	http://:
1267	1	21/Jan/2008 12:04:24	POST	192.168.0.2/vo/tree.do?accountId	referer	http://:
1268	1	21/Jan/2008 12:04:29	POST	192.168.0.2/vo/readMail.do	referer	http://:
1269	1	21/Jan/2008 12:04:39	POST	192.168.0.2/vo/readMail.do	referer	http://:
1270	1	21/Jan/2008 12:04:44	GET	192.168.0.2/vo/jsp/subFrame.jsp?c	referer	http://:
1271	1	21/Jan/2008 12:05:14	GET	192.168.0.2/vo/desktop.do?show= <u>.</u>	referer	http://1
	Network	ά NIPS ά	HIPS	Behavior Web	1	
			1000000			

## Objective:

Use **TraceEraser Pro** to delete internet history tracks and to protect privacy.

- In the CEHv6 Labs CD-ROM navigate to Module 45
- Install and launch "TraceEraser Pro" program

Tracks Eraser Pro(Unregistered)	? ∈ x
Tracks Eraser Cover Your Tracks	Erase Now
WWW.RESSOFT.RET	Iest Now
Task Sta	atus 🔺 Eraser <u>S</u> ettings
E Address Bar E Cookies	 
E History	File Shredder
IE Plualns	Log
	About
	Help
	Exit
Last Era, 30 at:	

• Click on **Erase Now** to erase all tracks



Click on **OK**

#### **EC-Council**

Ethical Hacking and Countermeasures v6 Lab Manual



#### Objective:

Use Cookie Pal to protect privacy on Internet.

- In the **CEHv6 Labs CD-ROM** navigate to **Module 45** Install and launch "**Cookie Pal**" program •

🙁 Cookie Pal 1.7c (	(Unregistered)			_	
🥳 Session 📳 I	Filters 🛛 😳 Cook	ies 🕅 Sounds	Configure		
The list below d	isplays web sites f current ses	rom which cookie sion. Click Help fo	s have been accep or more information.	oted or rejected for t	he
Server		# Accepted	# Rejected	Time -	
		ţ			
Accepted: 0 Rejected: 0	Always accep	t Always rej	ect Clea	r 🛛 🖲 Summ	iary
Total: 0				──── ○ Detail	
Ordering	Register	]	About	Help	

• Click on **Session** to accept or reject cookies for current session

🥴 Cookie Pal 1.7c (Unregistered)								
🥳 Session 📰 Filters 🙄 Cookies 🕅 Sounds 🗐 Configure								
The list below displays web sites from which cookies have been accepted or rejected for the								
	current session. Click Help for more information.							
	Server		Expires		Name	Value		
	•						<b>F</b>	
	Accepted:	0						
	Rejected:	0	Always accept	Always	reject	Clear	Contail	
	Total:	0					2 Source	
		1				1		
	Urdering		Hegister			About	Help	

• Click on **Filter** to provide information to accept and reject cookies

😬 Cookie Pal 1.7c (Unregistered	)					
🛞 Session 🔛 Filters 🕥 Cod	okies 🕅 Sound	ds 🗐 Configure				
Accept cookies from :		Reject cookies from :				
	~					
New Delete		New Delete				
Reject third-party cookies (If	5 6 and later only)					
Cookies from unknown servers: -						
Accept cookies that expire in the current browser session 🔽 🗖 Override Filters						
Ordering Register		About Help				
Back						

• Click on **New** and write the name of server from which to accept cookies

🙁 Cookie Pal 1.7c (Unregistered	)				
🛞 Session 🔛 Filters 🙆 Coo	okies 🕅 Sounds 🗐 Configure				
Accept cookies from :	Reject cookies from :				
New Filter	X				
Enter the na	ame of a server from which you wish to accept cookies:				
Server name	, ecc				
Reject third OK	Cancel Help				
Cookies from un <del>known servers.</del>					
O Reject all	C Accept all       Ask for confirmation				
Accept cookies that expire in the current browser session 💌 🗖 Override Filters					
Ordering Register	About Help				

#### **EC-Council**

Ethical Hacking and Countermeasures v6 Copyright © **EC-Council** All Rights Reserved. Reproduction Strictly Prohibited.

**EC-Council** 

• Click **New** and write the name of server from which to reject cookies

🙁 Cookie Pal 1.7c (Unregi	stered)					
∰ Session 🔛 Filters I	🙄 Cookies 🕅 Si	ounds 🗐 Configure				
Accept cookies from :		Reject cookies from	:			
ecc						
New Fi	lter		×			
En	er the name of a serv	er from which you wish to				
	reject c	ookies:				
Ser	er name		-			
	er name					
New		R.	II [			
🔽 Reject third-	OK Ca	ncel Help				
Cookies from un <del>known s</del>	ervers.					
C Reject all	C Accept a	il 💿 i	Ask for confirmation			
Accept cookies that expire in the current browser session 💌 🗖 Override Filters						
Ordering	egister	About	Help			

- In the CEHv6 Labs CD-ROM navigate to Module 45
- Open the Online Privacy and a Free Internet.pdf and read the content



- In the CEHv6 Labs CD-ROM navigate to Module 45
- Open the **Privacy\_Policy.pdf** and read the content



- In the CEHv6 Labs CD-ROM navigate to Module 45
- Open the spyware2005.pdf and read the content


## Lab 45-10

- In the CEHv6 Labs CD-ROM navigate to Module 45
- Open the **Spyware a Hidden Threat.pdf** and read the content



## Lab 45-11

- In the CEHv6 Labs CD-ROM navigate to Module 45
- Open the Privacy Preserving Web-Based Email.pdf and read the content



Ethical Hacking and Countermeasures v6 Lab Manual



# Module 46

# Securing Laptop Computers

## Lab 46-01

### Objective:

Use **Connection Manager Pro** to manage available network connections.

- In the CEHv6 Labs CD-ROM navigate to Module 46
- Install and launch BVRP Connection Manager Pro program

BVRP Connection Manage	er Pro 🛛 ? 📃 🗙
Profile:Local Area Network Status:OK	About-
Type:Local Area Network Status:Connected Duration:00:06:15 Speed:100.0 Mbits/s Received:132.55 Kbytes Sent:106.03 Kbytes	
	BVRP

• To setup a profile click on and click profile name (e.g. office)



• The List of Profiles is as shown

🐷 BVRP Conn	ection Manage	er Pro				
File Edit View	Action Help					
🚨 New	▼ Select	- SX Delete	Properties	Broups	Frofiles	° 😵
Create new p	rofile					
2						
New profile						
	2					
Local Area Ne	twork					
Local Area Network	office					
Ready	Lo	ocal Area Network is a	ctive			<ul> <li>Image: Control of the second se</li></ul>

■ To create a profile Using Wizard, click on File→New→Profile→Using Wizard

📴 BVRP Connection M	anager Pro				
File Edit View Action I	Help				
New 🕨	Profile 🕨 🕨	Using Wizard	Ctrl+N	Profiles	:02
Import Ctrl+I Export Ctrl+E	Group	Using current configuration		and Provides	200 F
Rename F2					
Delete Ctrl+D					
Duplicate Ctrl+U					
Properties					
Close					
Local Area office Network					
Creat <mark>e a new profile assisted</mark>	by • Local Area Netwo	rk is active			0

• Enter the profile information and click **Next** 

📴 Profile wizar	d								
Profile configuration Set the profile name, its description and choose an icon									
Enter the name a associated icon. Profile name: Icon: Description:	and a brief description you wish to give this profile and select the								
Group:	No group								

To create a New Group click on **File→New→Group** 

🐷 BVRP Con	nection N	lanager Pro			
File Edit Viev	v Action	Help			
New	×	Profile	te <b>De</b> Propertie	s Groups	:22
Import Export	<b>Ctrl+I</b> Ctrl+E	Group	0.3		 
Rename Delete Duplicate	F2 Ctrl+D Ctrl+U				
Properties					
Close					
Local Area Network	office	9			
		Local Area Networ	k is active		0
		inder and the leaf			

To connect to the wireless network click on

•

Ethical Hacking and Countermeasures v6 Copyright © **EC-Council** All Rights Reserved. Reproduction Strictly Prohibited.



To Monitor Data Transmission and Receiving click on



• To check statistics of the received data click on **Received** 

🔤 BVRP Conne	ction Manager Pro monitor	
🔣 Realtek RTL8	139 Family PCI Fast Ethernet NIC	
Connection		
Statistics		
Received	Transmitted	Kbits/s
6-		
4-		
received: 18.	81 Kbytes , sent: 14.52 Kbytes	
Status		
Status:	Connected	
Duration:	00:02:16	
Speed:	100.0 Mbits/s	
	Internet Protocol	(TCP/IP)
		Close

• To check the statistics of transmitted data click on **Transmitted** 

BVRP Connection	on Manager Pro monito	r 💶 🗖 🔀
属 Realtek RTL8139	Family PCI Fast Ethernet NIC	
Connection		
Statistics		
Received Tran	nsmitted	Kbits/s
	- 41	
6-		
2		
received: 20.54 k	(butes sent: 16.91 Kbutes	
Status:	Connected	
Duration:	00:02:31	
Speed:	100.0 Mbits/s	
	(Julawa) Desta	
	Internet Protoc	cor(TCP7IP)
		Close



To set the settings click on

•

,click on Main Screen Settings



**EC-Council** 



To set properties for a profile click on **Current profile properties** 



■ To set General settings click on **General**→**Configure** 

📴 Edit 'Local Area Network' profile settings 🛛 🔀									
General Connections Printer Internet settings Share Security									
Enter the name you wish to give this profile and select the associated icon.									
Profile name: Local Area Network									
Icon: Change icon									
Description:									
Group: No group									
Network identification									
Select the type and the name of workgroup or the main to which the computer belongs in this profile.									
Location									
Select the location that will be used in this profile. Configure									
Apply this profile now OK Cancel									

■ To View the network connections and adding click **connections** → **Add** 

8	Edit 'L	ocal Area N	letwork' profile :	settings			×
ſ	General	Connections	Printer Internet se	ttings Share	Security		
	The list compute	لک below displays er.	the network connect	ion types that a	are configur	ed on your	
	Select t	he connection	to use in this profile:	🗹 Show pr	esent conn	ections only	
	Conn	ection	Туре	Ada	pter name		
							28
	Add	Dele	te Configure	Add to Bla	ack List	Bescan	
						nosodn	
L							
	Apply the	nis profile now			ОК	Cancel	

• To Set the internet settings click on **Internet settings** 

📴 Edit 'Local Area Network' profile settings	×
General Connections Printer Ingranet settings Share Security	_
Email	
Applications Select the applications to launch after applying this profile. Configure	
Ргоху	
Use a server proxy that will be used to access to Internet. Configure	
Apply this profile now OK Cancel	

• Go to Security tab. Click on **Settings** to set the Security Settings.

📴 Edit 'Local Area Network' profile settings	
General Connections Printer Internet settings Share       Security         Internet connection firewall       Protect my computer and the network by limiting access to this computer from Internet         Settings	
Apply this profile now	Cancel

To set the profile preferences click on → click on Profile Preferences



# Lab 46- 02

Objective:

Use **Cryptex** tool is to secure information on a PC, by creating a vault

- In the CEHv6 Labs CD-ROM navigate to Module 46
- Install and launch Cryptex program

🔂 Cryptex							🛛
Vaults Edit View	Tools Help						
				Q			
Create	Unlock	Lock	Launch explorer	View	Encrypt files	Email files	
Veed more space?	a Recommend a	friend					
Ready							NUM

Ethical Hacking and Countermeasures v6 Lab Manual

**EC-Council** 



•

icon to create a vault

🔒 Cryptex							
Vaults Edit View	Tools Help						
<b>ö</b> Need more space?	🥞 Recommend a	friend					
R.			<b>V</b>	Q			
Create	Unlock	Lock	Launch explorer	View	Encrypt files	Email files	
Ready							NUM .:

• Select a drive for creating a vault

🗧 Add a new encr	ypted vault 📃 🗖 🔀
-Step 1 of 3: Select th	e drive letter and the location to store the image file
Drive letter:	
	e location to store the data to:
Can P:	Previous Next
0: N: M: L: K:	
J: I: H: G:	

Browse a file from a particular location

Browse For Folder	?×
<ul> <li>Desktop</li> <li>My Documents</li> <li>My Documents</li> <li>My Music</li> <li>My Pictures</li> <li>My Virtual Machines</li> <li>OneNote Notebooks</li> <li>My Computer</li> <li>My Network Places</li> </ul>	
Make New Folder OK Can	cel

Click **OK**

Browse For Folder	? 🗙
<ul> <li>Desktop</li> <li>My Documents</li> <li>demo</li> <li>My Music</li> <li>My Pictures</li> <li>My Virtual Machines</li> </ul>	
My Computer My Network Places Make New Folder	cel

Click Next

😚 Add a new encrypted vault
Step 1 of 3: Select the drive letter and the location to store the image file
Drive letter:
Please enter the location to store the data to:
C:\Documents and Settings\Admin\My Documents\demo\"
Cancel Previous Next

Enter a password and click Next

🗟 Add a new encrypted vault 📃 🗖 🔀								
Step 2 of 3: Select a p	Step 2 of 3: Select a password for your drive							
Please enter a local	Please enter a local password for your vault							
Type password:	•••••							
Confirm password:	••••••							
You may enter the same password as the master password								
Cancel	Pr	evious Next						

• Select desired encryption algorithm

🗟 Add a new encrypted vault						
Step 3 of 3: Cho	ose your drive size and encryption:					
Drive size(MB):	10 Max size(MB): 6000					
Method:		information				
Key length:	Blowfish Triple DES					
The key length	must be divisible by 64					
Format this drive manually (Advanced)						
Cancel	Previous	Finish				

Click Finish

😼 Add a new encrypted vault
Step 3 of 3: Choose your drive size and encryption:
Drive size(MB); 6000 Max size(MB): 6000
Method: Blowfish Vore information
Key length: 128 Min key length: 8 Max key length: 448
The key length must be divisible by 8
Format this drive manually (Advanced)
Cancel Previous Finish

• The Removable drive is created



Select a document to be encrypted



Select a document and click on Encrypt files



🔒 Cryptex								
Vaults Edit View	Tools Help							
📢 Need more space?	a Recommend a	friend						
<b>R</b>			<b>N</b>	Q				
Create	Unlock	Lock	Launch explorer	View	Encrypt Siles	Email files		
		demo.docx	1					
							NUM	

• Select a location to save the encrypted file

Save As							? 🛛
Save AS Save in: My Recent Documents Desktop My Documents	My Document: My Recent Do Desktop My Compute Local Disk Local Disk Local Disk CD Drive ( Removabl Shared Do My Docum System17: My Network	s cuments r .(C:) .(D:) .(E:) F:) e Disk (H:) pouments nents s Documents Places	×,	© (	3 🔊	••••	
	File name:	Cryptex-demo			*	(	Save
My Network	Save as type:	Self-extracted files(*.exe)			*		Cancel

Ethical Hacking and Countermeasures v6 Copyright © **EC-Council** All Rights Reserved. Reproduction Strictly Prohibited.

Click Save

Save As						? 🔀
Save in:	🗢 Removable Di	sk (H:)	~	G 🤌	• 📰 🕈	
My Recent Documents						
Desktop						
My Documents						
My Computer						
	File name:	Cryptex-demo			~	Save
My Network	Save as type:	Self-extracted files(	<sup>×</sup> .exe)		*	Cancel

• Enter the Password for Encryption and click **Ok** 

Cryptex - Encrypt files							
This option allows you to select a file from your vault and automatically encrypt it into a self extracting executable. The file will only be able to be opened with the correct password.							
Select file path:							
H:\Cryptex-demo.	exe						
Password:	•••••						
Confirm password:	••••••						
Self extracting EXE file O Protected ZIP archive							
Selected files will be encrypted with given password and saved as executable file in the specified directory.							
Cancel QX							

# • The file encrypted is as shown

🔒 Cryptex							
Vaults Edit View	Tools Help						
G Need more space?	in the commend a contract of the contract of t	friend					
<b>N</b>			Ń	Q			
Create	Unlock	Lock	Launch explorer	View	Encrypt files	Email files	
		Cryptex-der .exe		Ŀ,			
Ready							NUM

■ To decrypt the file Click on **Tools** → **Decrypt** 

🔒 Cryptex		
Vaults Edit View	Tools Help	
Veed more space?	Image: Construction of the second	
	Cryptex-demo .exe	
		NUM 🔡

Browse the file from the location and click **Open** 

Open							?	×
Look in:	🖙 Removable Di	sk (H:)	*	G	ø	ø		
My Recent Documents Desktop	Cryptex-demo							
My Documents								
My Computer								
	File name:	Cryptex-demo				~	Qpen	
My Network	Files of type:	Self-extracted files(*.exe)				*	Cancel	

• Enter the password and click **Extract** 

🗧 Cryptex - Self extracting encrypted	vault 📃 🗖 🔀
Self extracting encrypted vault Please enter your password: *******	
Please enter the path to extract into:	
	Cancel Extract

• The file after decryption is as shown

🔒 Cryptex							
Vaults Edit View	Tools Help						
📢 Need more space?	in the commend a contract of the contract of t	friend					
<b>R</b>			Ń	Q			
Create	Unlock	Lock	Launch explorer	View	Encrypt files	Email files	
		Cryptex-den .exe	demo.docx				
Ready							NUM

• The Content in the decrypted file



Ethical Hacking and Countermeasures v6 Copyright © EC-Council All Rights Reserved. Reproduction Strictly Prohibited.

To lock a particular drive, select a particular drive and click on Lock button

🔂 Cryptex							
Vaults Edit View	Tools Help						
📢 Need more space?	in Recommend a	ı friend					
		2	<b>V</b>	Q			
Create	Unlock	Lock	Launch explorer	View	Encrypt files	Email files	
		Cryptex-de	demo.docx				
Ready							NUM

• The drive locked is as shown



To unlock a drive click on Unlock button

🔒 Cryptex							
Vaults Edit View	Tools Help						
Veed more space?	in the commend a commend a commend a commence of the commence of the commend a commend	friend					
			T <sub>N</sub>	Q			
Create	Unlock	Lock	Launch explorer	View	Encrypt files	Email files	
							NUM

• Enter Password and click **Ok** 

Cryptex - Unlock vault	×
Please enter your password to unlock the drive	
••••••	

• The drive unlocked is as shown

🔒 Cryptex								
Vaults Edit View	Tools Help							
📢 Need more space?	in the commend a commend a commend a commence of the commence of the commend a commend	friend						
<b>R</b>		X	TA I	Q				
Create	Unlock	Lock	Launch explorer	View	Encrypt files	Email files		
		Gryptex-de	emo.docx			<b>I</b> ≩		
Ready							NUM	1.5

■ To delete a Vault click on Vaults→Delete Vault

8	Cryptex							
Vau	ts Edit View Tools	s Help						
S.	<sup>0</sup> ⊆reate							
	Open	immend a	friend					
0	<u>U</u> nlock			VQ.	Q	à		
*	Lock	bek	Lock	Launch explorer	View	Encrypt files	Email files	
	<u>R</u> ename		0	(in the second s		2		
	Change Password							
	Properties		Cryptex-de	. demo.docx				
ø	Delete vault							
	<u>E</u> ×it							
								NUM

• Click **Yes** to delete the vault



• After deleting the Vaults

🔒 Cryptex								
Vaults Edit View	Tools Help							
😡 Need more space?	in the commend a commend a commend a commence of the commence of the commend a commend	friend						
<b>R</b>			Ta and the second secon	Q				
Create	Unlock	Lock	Launch explorer	View	Encrypt files	Email files		
				Δ,				

Page | 901

Ethical Hacking and Countermeasures v6 Copyright © **EC-Council** All Rights Reserved. Reproduction Strictly Prohibited.

## Lab 46-03

### Objective:

Use **Data Protection Software** is to provide security and confidentiality for data on a removable medium.

- In the CEHv6 Labs CD-ROM navigate to Module 46
- Install and launch Data Protection Software program

💽 Data Pro	otection S	oftware ma					
File Service	Help						
Create	Nount	Sector 2000 - Unmount	- 🚺 - Unmount all P	assword Settings	Delete		
Description				Creation time	Last access time	Status	Mount point
				k			
				0			



to create a new container

🚱 Data Protection Software manager						
File Service Help						
Character a new container mount Unmount all Password Settings Delete						
Description	Creation time	Last access time	Status	Mount point		

.

• Select a desired location to save the container, click **Browse** 

🚱 Create container	
Path to SVD container	Browse
Container size: 1 KB  Container description:	it point: G:\ 💽
Type password:  Type password: Re-type password:	?? Cancel

• Enter the file name and click **Save** 

Save As		? 🗙
Save in:	🖙 Local Disk (E:) 💽 🔶 📑 📰 🕶	
My Recent Documents Desktop	Euns Softwares songs Traning session documents	
My Documents		
My Computer		
My Network Places	File name:     test       Save as type:     ????? ??????? (*.svd)	Save Cancel

• Click on 코 , select the desired size of the container

🚱 Create container	×
Path to SVD container E:\test.svd	Browse
Container size: 1 KB Default mour KB KB KB Container description: MB GB	ıt point: G:\ ▼
Type password:     ************************************	?? Cancel

• Click on , select the desired drive to set the Default mount point

🚱 Create container	
Path to SVD container	
E:\test.svd	Browse
Container size: 100 MB 🗸 Default moun	t point: G:\
Container description:	G:\ \\ H:\
l ype password:	N:X 💌
Re-type password:   ***********************************	Cancel

Click on ?? button to create a container

E. 11851.570		Browse
Container size: 100	◆ MB ▼	Default mount point: H:\
Container description:		
test container		

■ To import a created container click on **File→Import** 

🔉 Data Protection Software manager 📃						
File Service Help		_				
Kreate Mount Import		Unmount all	assword Settings	Delete		
Safe unmount drive Fast unmount drive	Ctrl+U		Creation time	Last access time	Status	Mount point
Safe unmount all drives Fast unmount add drives	; Ctrl+A					
Format Delete	Ctrl+F Ctrl+E					
Exit	Ctrl+X					
1				1		
Click Browse



Browse the file and click **Open** 

Open		? 🗙
Look in:	🖙 Local Disk (E:) 💽 🖛 🗈 💣 🏢 -	
My Recent Documents Desktop My Documents	<ul> <li>Funs</li> <li>Softwares</li> <li>songs</li> <li>Traning session documents</li> <li>test.svd</li> </ul>	
My Computer		
My Network Places	File name:     test       Files of type:	Rpen Cancel

Ethical Hacking and	Countermeasures v6	Lab Manual
---------------------	--------------------	------------

## **EC-Council**

•	Click on	??
		💁 Input container to the mount list
		Path to SVD container:
		E:\test.svd
		?? Cancel

Enter Password Click **Ok**

Password	
Password:	
*****	
ОК	Cancel

File imported

💽 Data Pro	tection S	oftware m	anager				
File Service	Help						
Create	Nount	Sector Unmount	- 힌 - Unmount all	Password Settings	- Carlos Contractor Co		
Description				Creation time	Last access time	Status	Mount point
test container				3.1.2008 17:39:18	***	Unmounted	< H:\>
						Mount List. Here pr	esents all containers to t
				N			

• To mount the imported container, Right click and select Mount

💽 Data Pro	tection S	oftware m	anager				
File Service	Help						
Create	Nount	Sector Unmount	- 🚺 - Unmount all	Password Settings	- Carlo Delete		
Description				Creation time	Last access time	Status	Mount point
test container				3.1.2008 17:39:18	***	Mount	12003
						Safe unmount Safe unmount	drive all drives
						Fast unmount	drive all drives
						Format drive Change contai	ner properties
						Delete contain	er from mount list
Container info:				test container		Unmounted	< H:\ >

• Select the Mount point click **Ok** 

💁 Mount container	
Mount point: G:\ -	ОК
🔲 Read only	Cancel

• Enter password click **Ok** 

Password	
Password:	
*****	
OK D	Cancel

💽 Data Protection Sof	tware ma	nager				
File Service Help						
Vをreate Mount Import		Unmount all	assword Settings	- C		
Safe unmount drive	Ctrl+U		Creation time	Last access time	Status	Mount point
Fast unmount drive			3.1.2008 17:39:18	3.1.2008 17:39:18	Mounted	G:V
Safe unmount all drives Fast unmount add drives	Ctrl+A					
Format	Ctrl+F					
Delete	Ctrl+E					
Exit	Ctrl+X					
Container info:			test container		Mounted	G:\

■ To format the mounted container, click on **File**→**Format** 

• Click on , select the desired file system to format the drive, Click **Begin** 

🚱 Format dialog	×
Mount point:	
G:\	
Disk size:	
File system type:	
FAT	R
FAT FAT32	Ĩ
NTFS	
0%	_
Begin Cancel	

•

To unmount the drives, select the items in the list, right click and select **Fast unmount all drives** 

💽 Data Pro	tection S	oftware m	anager					
File Service	Help							
Create	Nount	Sector Unmount	• 힌 • Unmount all	Password -	Settings -	C Delete		
Description				Creation time	1	Last access time	Status	Mount point
test container				3.1.2008 17:	39:18	3.1.2008 17:39:18	Mount Safe unmount drive Safe unmount all drive Fast unmount all drive Fast unmount all drive Format drive Change container pro	s perties
							Delete container from	mount list
Container info				test container			Mounted	G:\

To delete a container click **Delete** 

🚱 Data Protection Software manager 📃 🗖 🔯									
File Service	Help								
Create	Nount	Sector Unmount	- 힌 - Unmount all	Password -	Settings				
Description				Creation tir	me	Last access time	Status	Mount point	
test container				3.1.2008 1	17:39:18	***	Unmounted	< H:\>	
Container info:				test contair	her		Unmounted	< H:\ >	

Browse the file and Click **Ok** 

Delete container	
Path to SVD container:	
E:\test.svd	Browse
Ск	Cancel

Ethical Hacking and Countermeasures v6 Copyright © EC-Council All Rights Reserved. Reproduction Strictly Prohibited.

## Lab 46 -04

## Objective:

Use Net Profile switch Tool to store and switch between two or more network configuration sets.

- In the CEHv6 Labs CD-ROM navigate to Module 46
- Install and launch Net Profile Switch program

🔹 Net Profile Switch	×
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>H</u> elp	
Net Profile Switch switching between networks	
New profile Activate 📸 Edit 🔚 Save changes 🚺 Settings	125
ka la	
Profile "office" activated. Net Profile Switch can be closed.	

• To create a new profile click on **New Profile** 



• To set an icon for a profile, Enter the profile name select a profile icon



• click **OK** 



Ethical Hacking and Countermeasures v6 Copyright © EC-Council All Rights Reserved. Reproduction Strictly Prohibited. • To set the network settings go to **Network** tab

🖉 office - edit profile				×
General Network Proxy Firewall	Net drives & shares	Printer 1	VPN & Dial-up St 🔹	>
Available network interfaces in your	system (click to edit):			
🔍 [00000001] Realtek RTL8139	Family PCI Fast Ethern	net NIC		
1				
Settings for [00000001] Realtek R	TL8139 Family PCI Fas	st Etherne	et NIC	
[00000001] Realtek RTL8139	Family PCI Fast Ether	rnet NIC		
	·			
Change this network-interface	e's settings when the pr	rofile is ac	ctivated	
🗹 Obtain an IP address aut	omatically			
IP Address:	0.0.0.	0	view current IP	
Subnet Mask:	255 . 255 . 255 .	0	settings for this	
Default gateway:	0.0.0.	0	network card	
Obtain DNS server addre	ss automatically			
Preferred DNS server:	0.0.0.	0		
Alternate DNS server:				
AVENC SERVICE				
WINS server:				
			K Cancel	Ъ

• To set the firewall settings click on **Firewall** 



• To set Net drives & shares settings click on **Net drives & shares** 

🖉 office - edit profile 🛛 🗙
General Network Proxy Firewall Netdrives & shares Printer VPN & Dial-up St
Network drive mappings and network shares for this profile Add these drive mappings after activating the profile:
Add Remove
Import current     Disconnect previous network drives first
Add these network shares after activating the profile: Add Remove
Import current Disconnect previous network shares first
OK Cancel

•

## To set the printer settings click on **Printer**



■ To set the workgroup settings click on **work group→Ok** 

ą	office - e	dit profile	
	Net drives &	shares Printer VPN & Dial-up SMTP Scripting Workgroup	< >
	<u>.</u>	Change workgroup	
		Join a workgroup after activating this profile (requires Windows XP or higher)	
		Workgroup to join:	
		ОК	Cancel

# Lab 46-06

Objective:

Use **Private Disk Multifactor** to provide data confidentiality on Laptops.

- In the CEHv6 Labs CD-ROM navigate to Module 46
- Install and launch **Dekart Private Disk Multifactor** program

🎼 Dekart	Private Disk Multifactor	
Disk O	otions Recovery Customize Key Reader	
<u>Q</u>	Mounts a virtual encrypted disk in the operating system.	Connect
f	Creates, activates and formats a new virtual encrypted disk.	Create
<b>\$</b>	Erases a virtual encrypted disk.	Delete
	Allows to view and change some virtual encrypted disk properties.	Properties
About		Close

■ To create a virtual encrypted disk , Click on **Disk**→ **Create** 

X	Dekart I	Private Disk Multifactor	
D	isk Op	tions Recovery Customize Key Reader	
	<u>@</u>	Mounts a virtual encrypted disk in the operating system.	Connect
		Creates, activates and formats a new virtual encrypted disk.	Reate
	<b>\$</b>	Erases a virtual encrypted disk.	Delete
		Allows to view and change some virtual encrypted disk properties.	Properties
	About		Close

•

# Select the desired drive to be created

🕅 New Priv	ate Dis	k 🛛 🔀
File ima	ge:	Browse
Disk letter:	Z:	Disk size: 50 🔅 MBytes
🗹 Removat	H: l: .l:	Read Only Disk
Hidden Fi	с. К: L:	Connect on System start
Save and	M: N:	hares automatically
Clear the	0: P:	ss time of the File-Image
	Q: R: S: T:	Restore Defaults
Quick cre	U: V: W:	ot fill up the file-image with random data)
	X: Y: Z:	Create Cancel

• Select the location to save a particular drive, click on **Browse** 

🕅 New Private Disk 🛛 🛛 🗙		
File image: Browse		
Disk letter: H Disk size: 50 S MBytes		
Removable Disk		
Hidden File-Image		
Save and restore shares automatically		
Clear the last access time of the File-Image		
Restore Defaults		
Quick create (Do not fill up the file-image with random data)		
Create		

• Enter disk name, click **Save** 

## **EC-Council**

## Ethical Hacking and Countermeasures v6 Lab Manual

📕 Private Disk	File image					? 🔀
Save in:	👄 Local Disk (	E:)	~	G	1 🖻 🖬	J•
My Recent Documents Desktop	Funs Softwares songs Traning sessi	on documents				
My Documents My Computer						
No. Natural	Charmen	Pid				
Places	Save as type:	Private Disk files (*.dpd)			~	Cancel

Click Create

🕅 New Private Disk 🛛 🔀		
File image: E:\Disk.dpd Browse		
Disk letter: H: V Disk size: 50 S MBytes		
Removable Disk Read Only Disk		
Hidden File-Image Connect on System start		
Save and restore shares automatically		
Clear the last access time of the File-Image		
Restore Defaults		
Quick create (Do not fill up the file-image with random data)		
Create Cancel		

• To set the password Enter the password and click **OK** 

🕅 Encryption password 🛛 🔀				
E:\Disk.dpd				
Password:				
Confirmation:				
Password quality:				
19%				
ОК	Cancel			

• When the formatted message appears, click on **start** 

🕅 Format	?×
Capacity:	
50.0 MB	~
File system	
NTFS	~
Allocation unit size	
Default allocation size	*
Volume label	
- Format options	
🗹 Quick Format	
Enable Compression	
Create an MS-DOS startup disk	
Start Ck	ose

• To mount a disk into the virtual operating system click on **Connect** 

🛤 Dekart	Private Disk Multifactor	
Disk O	otions Recovery Customize Key Reader	
<u>@</u>	Mounts a virtual encrypted disk in the operating system.	Connect
<b>P</b>	Creates, activates and formats a new virtual encrypted disk.	Create
	Erases a virtual encrypted disk.	Delete
	Allows to view and change some virtual encrypted disk properties.	Properties
About	Help	Close

Browse the disk, Click **Open** 

K Connect Pri	vate Disk					? 🗙
Look in:	🍛 Local Disk (E:	)	~	G 🦻	ج 🔁	
My Recent Documents Desktop My Documents My Computer	Funs Softwares songs Traning session	i documents				
My Network Places	File name: Files of type:	Disk Private Disk files (*.dp Open as read-only	od)		¥ ¥	Open Cancel

• Enter Password, click **Ok** 

X Decryption password	×
E:\Disk.dpd	
Password:	
OK Cancel	

To explore content of virtual disk click **Explore**



The Explored Virtual disk

😂 Removable Disk (H: )		
File Edit View Favorites Tools	Help	
🕝 Back - 🕥 - 🏂 🔎 Se	arch 😥 Folders 🛄 -	
Address 🗢 H:\		💌 🄁 Go
Folders     ×       Image: Construction of the state of the	Demo K	

• To view the list of programs those are allowed to access the disk, click on H:\-->Disk Firewall

📕 Dekart I	Private Disk Multifactor	
H:\ Di	sk Options Recovery Customize Key Reader	
2	Unmounts the encrypted disk from the operating system.	Disconnect
ß	Explores content of the virtual encrypted disk.	Explore
	Shows and edits the list of programs that are allowed to access the disk.	Disk Firewall
	Shows and edits the list of programs that will be run automatically on disk connecting.	Autorun
<b>S</b>	Shows and edits the list of programs that will be run automatically on disk disconnecting.	Autofinish
<b>S</b>	Shows some properties of connected encrypted disk.	Information
About		Close

#### **EC-Council**

- To add the program that are able to access the disk, click on  $\mathbf{Add} \! \rightarrow \mathbf{Ok}$  , check the **Enable Disk Firewall** box

Allowed programs		
List of allowed programs		Add
	ОК	Cancel

• To view and edit the list of programs running automatically after disk connecting, click on **Autorun** 



■ To add list of programs Click Add→Ok

🕅 Autorun programs	
List of programs to autorun  Enable Autorun	Add Delete
<u> </u>	Cancel

• To view and list of programs that run automatically on disk disconnecting, click Autofinish

🕅 Dekart Private Disk Multifactor	
H:\ Disk Options Recovery Customize Key Reader	
Unmounts the encrypted disk from the operating system.	Disconnect
Explores content of the virtual encrypted disk.	Explore
Shows and edits the list of programs that are allowed to access the disk.	Disk Firewall
Shows and edits the list of programs that will be run automatically on disk connecting.	Autorun
Shows and edits the list of programs that will be run automatically on disk disconnecting.	Autofinish
Shows some properties of connected encrypted disk.	Information
About Help	Close

• Add the programs and click **Ok** 

🕅 Autofinish programs	
List of autofinish programs	
	Add
	Delete
С СК С	Cancel

• To view the disk information, click on **Information** 

🛤 Dekart Private Disk Multifactor	
H:\ Disk Options Recovery Customize Key Reader	
Unmounts the encrypted disk from the operating system.	Disconnect
Explores content of the virtual encrypted disk.	Explore
Shows and edits the list of programs that are allowed to access the disk.	Disk Firewall
Shows and edits the list of programs that will be run automatically on disk connecting.	Autorun
Shows and edits the list of programs that will be run automatically on disk disconnecting.	Autofinish
Shows some properties of connected encrypted disk.	La Information
About Help	Close

## **EC-Council**

• The Disk information is as shown

M Disk Information	
Disk Information         Connect on System start:       No         Save and restore shares automatically:       No         Key length:       256 bits         Clear the last access time of the File-Image:       No         List of allowed programs ( Disabled ) : <empty>       List of programs to autorun ( Disabled ) :         <empty>       List of autofinish programs ( Disabled ) :         <empty>       List of autofinish programs ( Disabled ) :         <empty>       List of autofinish programs ( Disabled ) :         <empty>       List of autofinish programs ( Disabled ) :</empty></empty></empty></empty></empty>	
ок	

• To set the options click on **options**, check the desired dialog boxes

🕅 Dekart Private Disk Multifactor	
H:\ Disk Options Recovery Customize Key Reader	
ドロ Run automatically on System start	
Check if a new version of Dekart Private Disk Multifactor is available	
Closing the window will minimize the program to System taskbar	
Enable error and operation logging	
Explore disk after connecting	
Check for opened files before disconnecting	
Do not show exit program confirmation dialog	
Display icon on System taskbar	
Associate with <.dpd> file extension	
Choose the drive letter before connecting	
Disconnect all disks after inactivity period of:	minutes
Disconnect all disks before hibernating	
Try to create a backup copy of the disk's encryption key automatically	
Restore Defaults	
About Help	Close



Click Copy



**Ethical Hacking and Countermeasures v6** Copyright © **EC-Council** All Rights Reserved. Reproduction Strictly Prohibited.

### **EC-Council**

Browse the disk from the location click **Open** 

🛤 Private Disk	File image						? 🗙
Look in:	🍛 Local Disk (E:	)	~	G	1 🖻	•	
My Recent Documents Desktop	Funs     Softwares     songs     Traning session     H Disk	documents					
My Documents My Computer							
My Network Places	File name: Files of type:	Disk Private Disk files (*.dpd) Open as read-only			*		Cancel

Enter Password Click **Ok**

🕅 Decryption pas	sword 🛛 🔀
E: <sup>v</sup>	\Disk.dpd
Password:	
ок 💦	Cancel

## **EC-Council**

• To Save, Enter the file name and click **Save** 

🕅 Save encryp	tion key							? 🗙
Save in:	🝛 Local Disk (E:)		*	G	Ø	ø	<del></del> -	
My Recent Documents Desktop My Documents My Computer	Funs Softwares songs Training session H Disk file 1	documents						
My Network Places	File name:	Disk1				~		Save
	Save as type:	All files (*.*)				*		Cancel

• Enter encryption password, click **Ok** 

🕅 Encryption pas	isword 🛛 🔀
E	E:\Disk1
Password:	
Confirmation:	
Pass	word quality:
	19%
ок 🗟	Cancel

• To restore the disk encryption key from a password protected backup copy, click on **Restore** 

📕 Dekart P	Private Disk Multifactor	
Disk Op	tions Recovery Customize Key Reader	
	Creates a password protected backup copy of the disk's encryption key.	Сору
<b>2</b>	Restores the disk's encryption key from a password protected backup copy.	Restore
*	Tries to find out the forgotten password of virtual encrypted disk by using Brute-Force attack.	Password
	Creates a compressed, encrypted, password protected backup copy of the virtual encrypted disk.	Backup
	Restores data from the previously created backup copy of the virtual encrypted disk.	Restore
About		Close

Browse the disk, Click **Open** 

🕅 Open encry	ption key							? 🛛
Look in:	🥪 Local Disk (E:		~	G	ø	Þ	•••	
My Recent Documents Desktop My Documents	Euns Softwares songs Traning session	documents						
My Computer								
My Network Places	File name:	Disk				*	Ľ	Open
	Files of type:	All files (*.*)				*	L	<sup>°</sup> Cancel

Enter Password, Click Ok



•

• Enter file name, Click **Save** 

🕅 Private Disk	File image				·		? 🗙
Save in:	🥪 Local Disk (E:)		*	G	1 🖻	<b></b>	
My Recent Documents Desktop My Documents My Computer	Funs Softwares songs Traning session	documents					
My Network Places	File name:	Disk1			~		Slye
	Save as type:	Private Disk files (*.dpd	)		*		Cancel

• Enter password, Click **Ok** 

• To customize icons and set hot keys click on **customize** 

🛤 Dekart Private Disk Multifactor	
Disk Options Recovery Custon Key Reader	
Hot Keys	
Dismount all disks:	
Dismount all disks and exit the program:	
Connected disks status icon:	Change
No connected disks status icon:	Change
Private Disk File image:	Change
Restore Defaults	
About Help	Close

• To automatically connect disk after key insertion, click on Key Reader

📕 Dekart Private Disk Multif	actor 📃 🗖 🔀
H:\ Disk Options Recov	ery Customize Key Reader
Connect encrypted disk autor	natically on Key insertion
Change PIN	Key Reader     O Detect automatically     O Set manually
Change BIO ID	Virtual Reader, F:\
	Virtual Reader F:\
Unblock	
Duplicate	
Delete	
Format	
	Restore Defaults
About Help	Close
Please insert a Key into any Key read	ler.

### Ethical Hacking and Countermeasures v6 Lab Manual

#### **EC-Council**

• To unmount the encrypted disk from operating system, click on H :\--> Disconnect



Disk after unmounting



Ethical Hacking and Countermeasures v6 Copyright © **EC-Council** All Rights Reserved. Reproduction Strictly Prohibited.
- In the **CEHv6 Labs CD-ROM** navigate to **Module 46**
- Open the **Securing the Laptop.pdf** and read the content



- In the **CEHv6 Labs CD-ROM** navigate to **Module 46**
- Open the **Cyber Security Tips.pdf** and read the content

🔁 C y	/ber	r Security Tips.pdf - Adobe Reader 📃 🗖 🙋	×
File	Edit	View Document Tools Window Help	×
9	۲	90% - 🛃 🛃 Find -	
?		Texas Department of Information Resources CYBER SECURITY TIPS Monthly Newsletter	<ul> <li>•</li> </ul>
		Office of the Chief Information Security Officer January 2008   Volume 2, Issue 1	
		Laptop computers are increasing in popularity for both business and personal use. Their portability makes them extremely convenient. However, laptop owners must also be aware of the security risks from the loss or theft of laptops and take proprecautions. The potential loss is twofold – the loss of the laptop itself and any personal, private, or sensitive information the may contain.	
	l	strong passwords, and encrypting your information, it is also very important to physically protect your laptop. Laptops can easily be stolen from the locked trunk of a car, at an airport security checkpoint, at an Internet café, or even from a hotel ro Keep these tips in mind when you travel with your laptop:	
Ø		<ul> <li>Secure your laptop when unattended – Attach the laptop with a security cable to something immovable or to a heavy piece of furniture when it is unattended. Devices are available that sound an alarm when they detect unexpected motiv or when the computer is moved outside a specified range around you.</li> </ul>	
se		<ul> <li>Don't store your password with your laptop – Secure your laptop with a strong password, but don't keep the password the laptop case or on a piece of paper stuck to the laptop. For more information on choosing and protecting your</li> <li>8.50 × 11.00 in </li> </ul>	~

- In the CEHv6 Labs CD-ROM navigate to Module 46
- Open the Laptop Computer Security.pdf and read the content

🔁 Laptop Computer	Security.pdf (SECURED) - Adobe Reader	
File Edit View Docum	ent Tools Window Help	×
🕤 🖲 90% ▼	Find -	
<b>@</b>	1.0 Introduction	
•	Despite the slump in the overall PC market, growth in laptop computers continues. According to Gartner, worldwide laptop sales grew 21% in 2000, compared with only 2% overall growth in PCs (1). Early indications are that worldwide growth during the next few years will remain at least in the high single digits for laptops, despite the declining overall PC market.	
	The laptop is increasingly the computer of choice for both business and consumer buyers. As laptops proliferate, laptop theft has become an ever more critical security issue. Safeware Inc., the largest U.S. insurer of laptops, projected that 387,000 laptop computers were stolen in the U.S. in 2000, up 21% from 1999 (2).	
	Laptop buyers in search of a security solution are faced with a wide array of products, systems, and services, each of which addresses a part of the problem. There remains considerable confusion about the extent of protection provided by each product, and the overall level of security that is achieved when a combination of approaches is used. As theft rates increase, it is increasingly evident that an ad hoc approach to laptop security is not adequate. An integrated solution is needed.	
	2.0 The Laptop Security Problem	
0	Squad in San Francisco, conducts an annual survey on computer crime and security in U.S. corporations and government agencies. For five consecutive years, CSI has reported the types of security attack and misuses experienced by its respondents. Laptop theft has been consistently reported by about 60%, as shown below.	~
8.50 × 11.00 ir		>

- In the CEHv6 Labs CD-ROM navigate to Module 46
- Open the **Secure your laptop with the LaptopLock.pdf** and read the content

🔁 Secu	re your laptop with the LaptopLock.pdf - Adobe Reader	
File Edit	: View Document Tools Window Help	×
	) 100% 🕶 拱 🖓 Find 🕶	
Û	Get started with LaptopLock	
	LaptopLock is Windows-only software. (Mactop users can get a saucy security	
?	feature by <u>using their iSight as an FTP backed up security camera</u> ). To get	
	started, head to the LaptopLock homepage and sign up for an account. It's	
	completely free, requiring an email address and a password.	
	Add Computer to monitor.	
	Enter a name for the computer: My laptop Add Computer	
	Once you've signed up, you'll want to add the computers you're going to use	
	LaptopLock with to your account, so just pick a name and go with it. After you add	
	a computer, download the LaptopLock agent to that computer (the download link	
	is available on the site's Control Panel page), run the installer, and launch	
	LaptopLock. Now it's time to match your computer with your LaptopLock account.	
	To do this, you need to onter	
	the email address you Computer Computer Status	
	registered with and the	
R,	Computer ID generated by	
0	the LaptopLock web site. You 1785 My laptop Report Computer Missing	
-	should also set a password	
77	11.00 x 8.50 in	>

- In the CEHv6 Labs CD-ROM navigate to Module 46
- Open the laptop security.pdf and read the content



#### Laptop Use

some alarming security challenges.



over the last five years has been the a report". increased usage of laptop computers.

completely replaced desktop computers with laptop com- data and employee down time. 8.50 x 11.00 in 1

While many regard the 1990's as the decade of the Internet, According to NSW Bureau of Crime Statistics estimates, there is no doubt that we are currently in the age of mobile 3.4 per cent of laptop computers are stolen each year, with everything. From laptop computers to mobile phones, similar figures reported in Victoria. Australia-wide, this wireless and mobile communication is increasingly preva- represents a loss in excess of \$30 million. The 2005 CSI/ lent. The surge of mobile-computing innovation has FBI Computer Crime and Security Survey found that the brought enormous benefits to business and consumers theft of laptop computers ranked as the second most comalike, but it has also left many security professionals facing mon security incident experienced by organisations this year. Gilles Novel, managing director of Business Security Systems Australia, says the reported figures are not neces-One of the most significant trends in sarily a true indicator of the actual incidence of theft corporate information technology "because people without insurance wouldn't bother making

Once only the domain of executive The AusCERT Australian Computer Crime Survey found management and for special mobile that the average reported cost of replacing a stolen laptop applications, laptop computers are was in excess of \$17,000.00, when taking into account the now routinely issued to middle man- cost of replacement hardware, IT resources to re-install and agement and IT personnel, and some organisations have update operating systems and applications, recovering lost

Ŵ

- In the CEHv6 Labs CD-ROM navigate to Module 46
- Open the laptop\_computer\_security.pdf and read the content



**EC-Council** 

- In the CEHv6 Labs CD-ROM navigate to Module 46
- Open the **securing\_your\_laptop.pdf** and read the content

🔂 securing_your_laptop.pdf - Adobe Reader		
File Edit View Doc	ument Tools Window Help	×
💿 💿 75.9% 🗸	Find	
È	Securing Your Windows Laptop	
?	Arindam Mandal (arindam.mandal@paladion.net)	
	Paladion Networks (http://www.paladion.net) May 2004	
	Now-a-days laptops are part of our life. We carry laptops almost everywhere for our	
	work, connect it to different networks and store our sensitive information on it. But we	
	hardly care about the security of our laptop and that opens the door for an intruder to	
	attack or steal sensitive data from it. An insecure laptop is susceptible to the following	
	security risks:	
	<ul> <li>An attack to the laptop due to known vulnerabilities of Windows</li> </ul>	
	<ul> <li>A Virus/Worm hit can paralyze your laptop</li> </ul>	
	<ul> <li>Spywares installed on the laptop can steal your sensitive information</li> </ul>	
	<ul> <li>An attacker can try network based attack to hack into your laptop</li> </ul>	
	<ul> <li>Anybody can view/delete/modify your important files</li> </ul>	
	<ul> <li>Malicious scripts embedded in the web pages can damage the laptop</li> </ul>	
	<ul> <li>Easy to compromise the laptop due to insecure OS settings</li> </ul>	
	<ul> <li>Attacker can use brute force/dictionary attack to break your weak password</li> </ul>	
n	<ul> <li>Insecure share in your laptop can be used to implant virus/worm/trojans</li> </ul>	
<i>©</i>	<ul> <li>An attacker can sniff your sensitive information from an insecure WLAN</li> </ul>	
	Laptop can be stolen	
<b>1</b>		
	This paper describes how you can protect your Windows lanten eacily	~



## Module 47

# Spying Technologies

#### Lab 47-01

Objective:

Use SpyBoss to monitor everything which is doing on a Computer.

- In the CEHv6 Labs CD-ROM navigate to Module 47
- Install and launch "SpyBoss Pro" program
- Explore various options of the tools and click on Start Capture button to start capturing



Give a Capture Name and click on **OK** 

Capture Name	
What would you like to name this capture?	OK Cancel
5-12-2008 5-39-59 PM	



Click on Keystrokes button to check the keystroke captured





Click on Screenshots button to check the captured screenshots



#### Lab 47-02

- In the CEHv6 Labs CD-ROM navigate to Module 47
- Open the Who's Spying on Your Computer.pdf and read the content

🔁 Wh	o's Spying on Your Computer.pdf - Adobe Reader	×
<u>File E</u> o	lit <u>Y</u> iew <u>D</u> ocument <u>T</u> ools <u>W</u> indow <u>H</u> elp	×
0	🔊 85% 🔻 📑 🛃 Find 👻	
() (7	WHAT IS SPYWARE? Spyware, is a computer software program or hardware device that enables an unauthorized person (such as an abuser) to secretly monitor and gather information about your computer use. There are many types of computer software programs and hardware devices that can be installed to monitor your computer activities. They can be installed on your computer without your knowledge, and the person installing them doesn't even need to have physical access to your computer. Whether computer molitoring is legal or illegal depends on the state you live in a dot the context in which it in installed used. Departed on the logality Spearse in	( III )
	Spyware programs are sometimes marketed as ways to monitor your children or your employees. As an employer, it is always best to have your employees read and sign a "Technology Use Policy." This policy should explain allowable uses of company property, expectations of online behavior, and TELL employees if their computer will be monitored. Additionally, choose a software package that displays an icon to remind your employees that they're being monitored. (* Also - see note to parents at the end of this piece).	
	<ul> <li>There are some similarities and differences between Spyware and its close relatives For example:</li> <li>Adware: These are hidden marketing programs that deliver advertising to consumers, and might also profile users' Internet surfing &amp; shopping habits. Adware is often bundled or hidden in something else a user downloads. Most average computer users are infected with adware fairly regularly, and common symptoms include a sluggish system and lots of advertising pop-ups.</li> <li>Malware: This is any program that tries to install itself or damage a computer system without the owner's consent. Malware includes viruses, worms, spyware and adware.</li> </ul>	
Ø	For more information on adware and malware, see "Protecting Your Computer" at www.antispywarecoalition.org/documents/documents/ProtectingYourComputerflyerletter.pdf	
	660 Pennakurain Ava SE Suita 202 Washington DC 20002 yang angku an /Safatublat 202 542 5566	

#### Lab 47-03

- In the **CEHv6 Labs CD-ROM** navigate to **Module 4**7
- Open the **The Science of Spying.pdf** and read the content



#### **EC-Council**

#### Lab 47-04

- In the CEHv6 Labs CD-ROM navigate to Module 47
- Open the Stop the Corporate Spying.pdf and read the content



Ethical Hacking and Countermeasures v6 Lab Manual



# Module 48

## Corporate Espionage- Hacking Using Insiders

Page | 956

#### **EC-Council**

- In the CEHv6 Labs CD-ROM navigate to Module 48
- Open the **Comparing Insider IT Sabotage and Espionage.pdf** and read the content

🔁 Comparing Insider IT Sabotage and Espionage.pdf - Adobe Reader	
File Edit View Document Tools Window Help	×
💿 🖲 100% 🕶 拱 🚰 Find 👻	
Executive Summary	~
<ul> <li>The purpose of this study is to examine psychological, technical, organizational, and context factors we believe contribute to at least two forms of insider trust betrayal: insider sabotage<sup>1</sup> against critical information technology (IT) systems, and espionage. Security professionals a policy leaders currently view espionage and insider threat as serious problems but often as separate issues that should be addressed by a different configuration of security countermeas. In this study, our team of researchers investigated similarities and differences between inside sabotage and espionage cases to assess whether a single analytical framework based on syste dynamics modeling could be developed to isolate the major factors or conditions leading to b categories of trust betrayal.</li> </ul>	ual nd ures. er IT em poth
<ul> <li>Based on the results, it is our position that insider IT sabotage and espionage share many contributing and facilitating system dynamics features. It follows that they might be detected deterred by the same or similar administrative and technical safeguards. Research into countermeasures that address multiple threats should be of high priority so that organizations adopt safeguards that counter both espionage and IT sabotage crimes. One outcome of this prior is a description of research areas that are likely to identify such countermeasures.</li> <li>Our modeling effort found definite parallels between the two categories of trust betrayal. The team created three models: one for IT sabotage, one for espionage, and one model, which we 8.50 × 11.00 in</li> </ul>	and s can roject e call

- In the CEHv6 Labs CD-ROM navigate to Module 48
- Open the **The Insider Threat.pdf** and read the content



- In the CEHv6 Labs CD-ROM navigate to Module 48
- Open the **Insider Threat-Protecting The Enterprise From Sabotage.pdf** and read the content



- In the **CEHv6 Labs CD-ROM** navigate to **Module 48**
- Open the **Corporate Espionage.pdf** and read the content

🔁 C	orporate	Espionage.pdf - Ac	obe Reader	
File	Edit View	Document Tools V	/indow Help	×
0	3.8	ا 🔂 🧮 🔹	Find	
<u> </u>		Spy-Ops	Training Brief	
			March 2005	
Ø		Corp CONTENTS: Abstract Objectives Brief Key Words Glossary Summary References Exam On-line Exercise	orate Espionage         *	
100		Objectives:	Brief	~