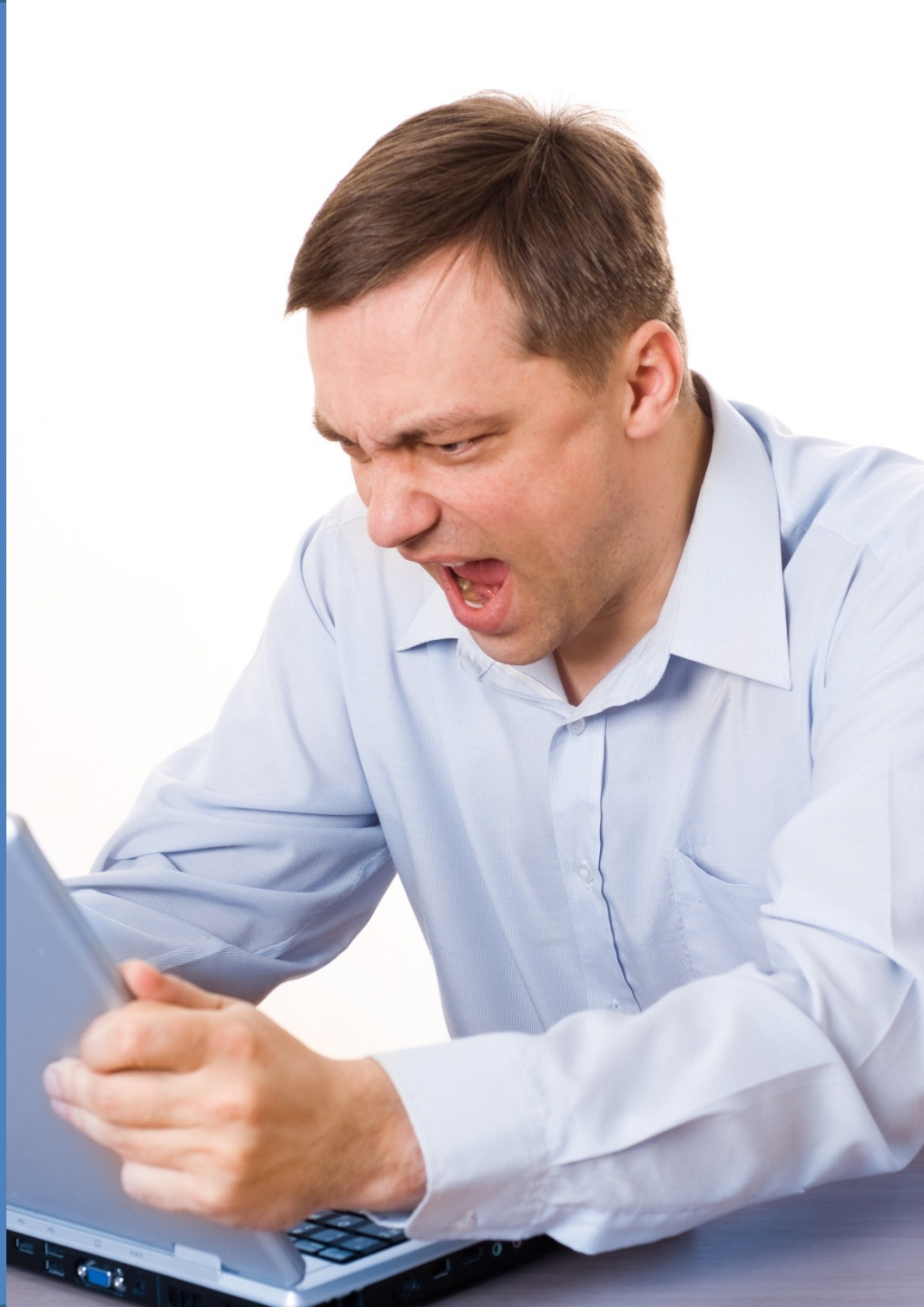
Ethical Hacking and Countermeasures

Steven Graham
Senior Director

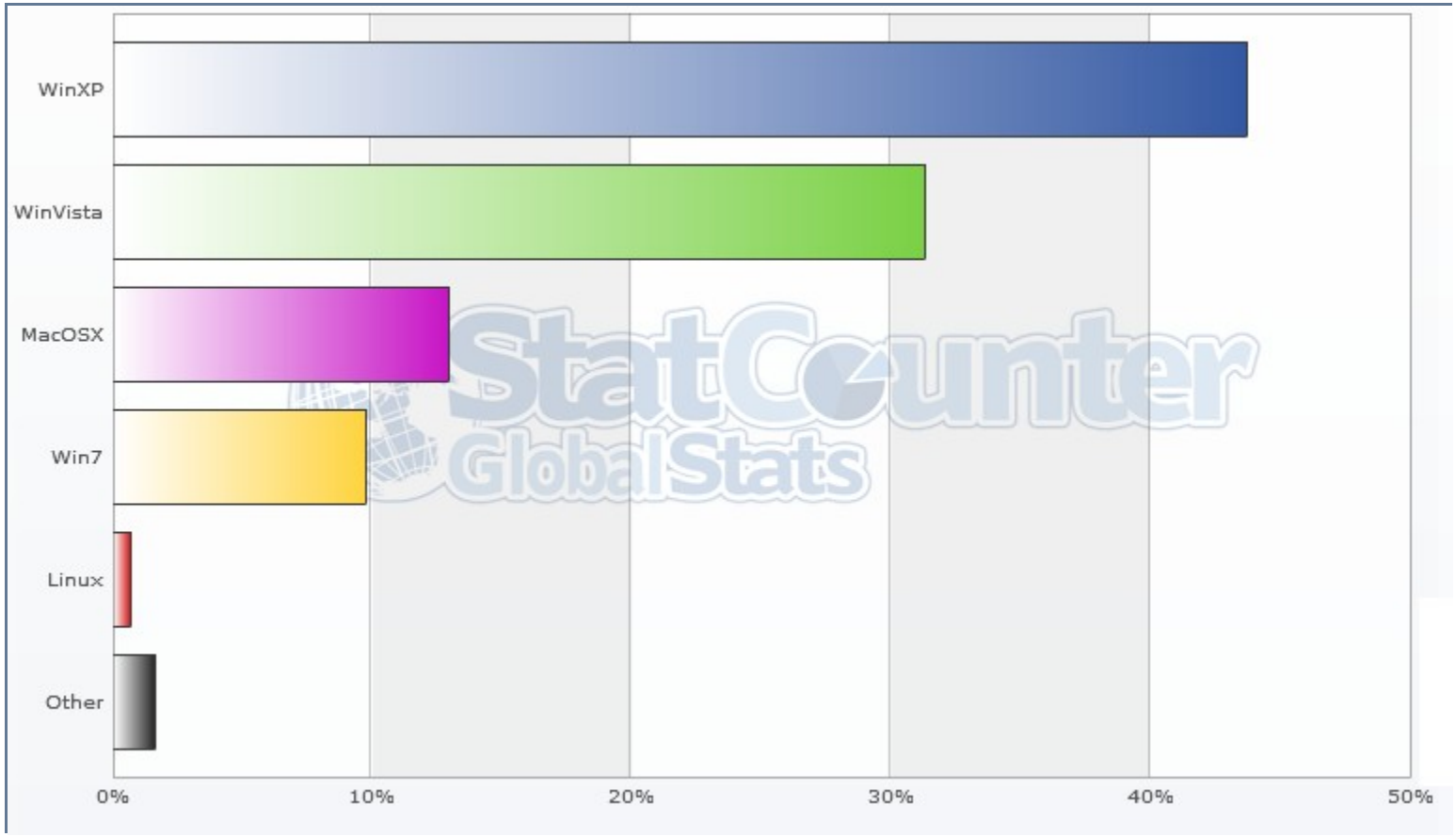
Operating System Vulnerabilities



Windows Vista

Windows Vista (codenamed Longhorn) was released on November 30, 2006 to business customers, with consumer versions following on January 30, 2007

Windows Vista intended to have enhanced security by User Account Control



Source: *http://gs.statcounter.com/, Jan 2010*

Top 5 Operating Systems in US

Metric	Windows Vista (year 1)
Vulnerabilities fixed	36
Security Updates	17
Patch Events	9
Weeks with at least 1 Patch Event	9

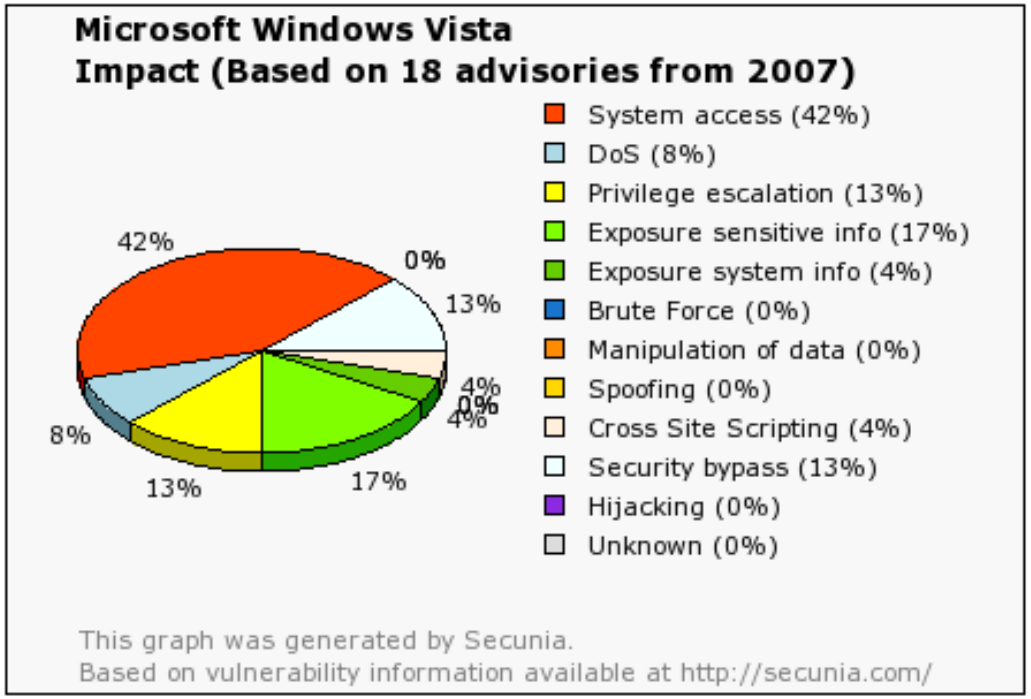
According to testers initial releases of Windows 2000 and XP were more stable than Vista

Windows Vista One Year Vulnerability Report

Windows Vista Vulnerabilities

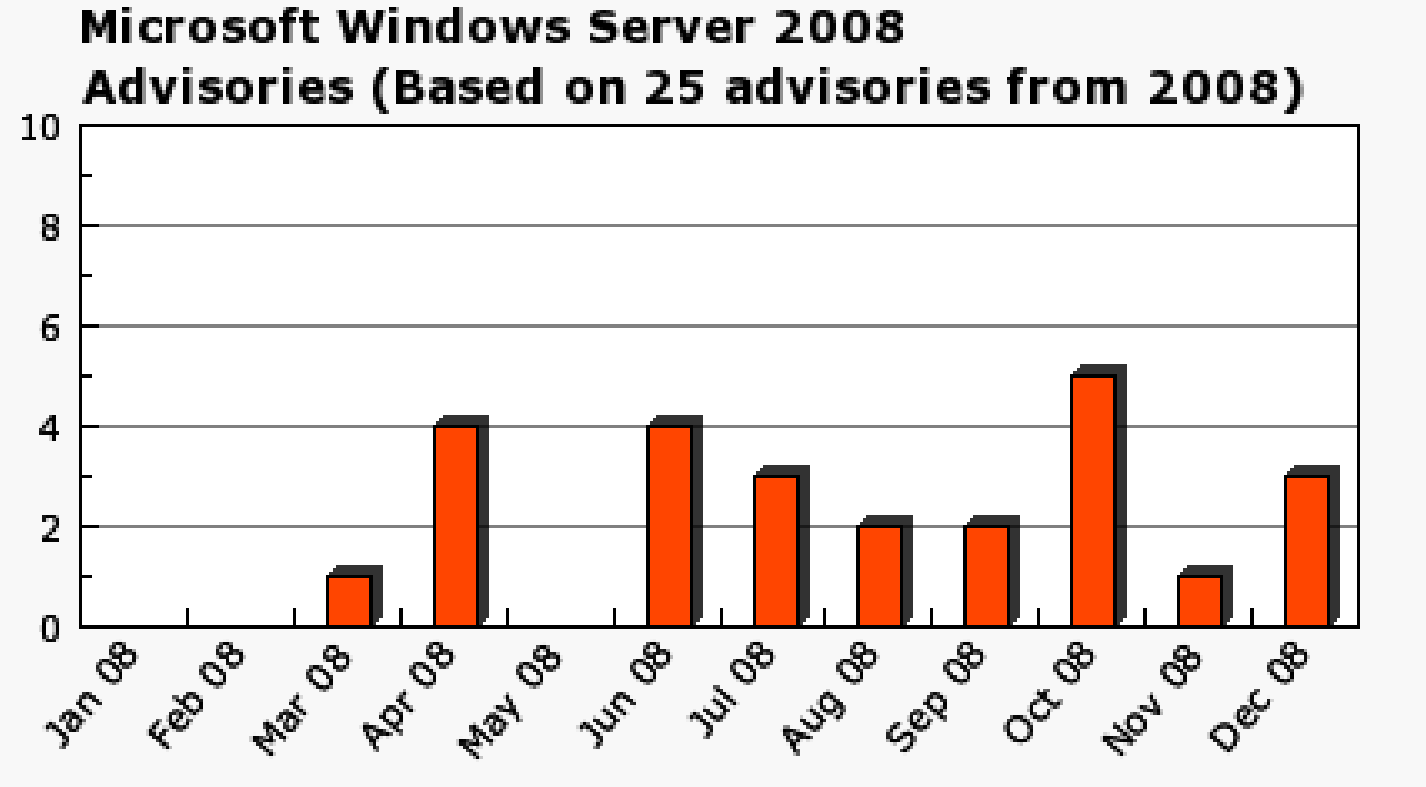
A technique that bypasses many of the new memory-protection safeguards in Windows Vista, such as address space layout randomization (ASLR) was developed resulting in buffer overflow bugs ,example was the 2007 animated cursor bug, CVE-2007-0038

According to PC Tools 97% of Worlds biggest security conference opined that Vista will have problems



Windows Server 2008 Microsoft Windows server line of operating systems officially released on February 27, 2008

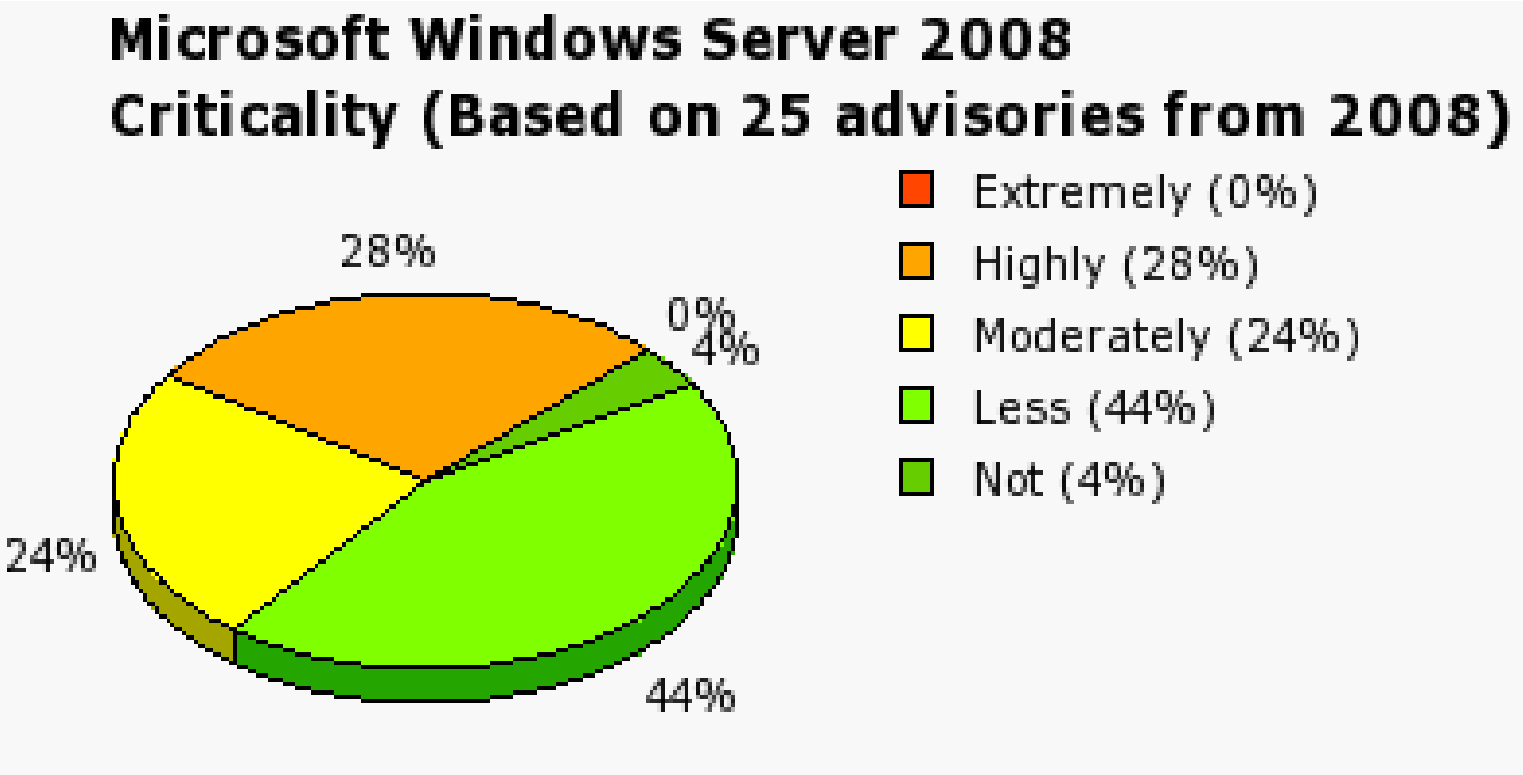
40% of the Windows 2000 Server users will move to Windows Server 2008 by the year 2010



The "Month by Month" graph above shows the number of issued Secunia advisories affecting Microsoft Windows Server 2008 on a month-by-month basis.

Windows Server 2008 Advisories

Windows Server 2008 Criticality



Windows 7

Windows 7 was released to manufacturing on July 22, 2009

Windows 7 was intended to be a more focused fully compatible with applications and hardware OS

Windows 7 software unit sales in the U.S. increased 234% over Windows Vista's first few

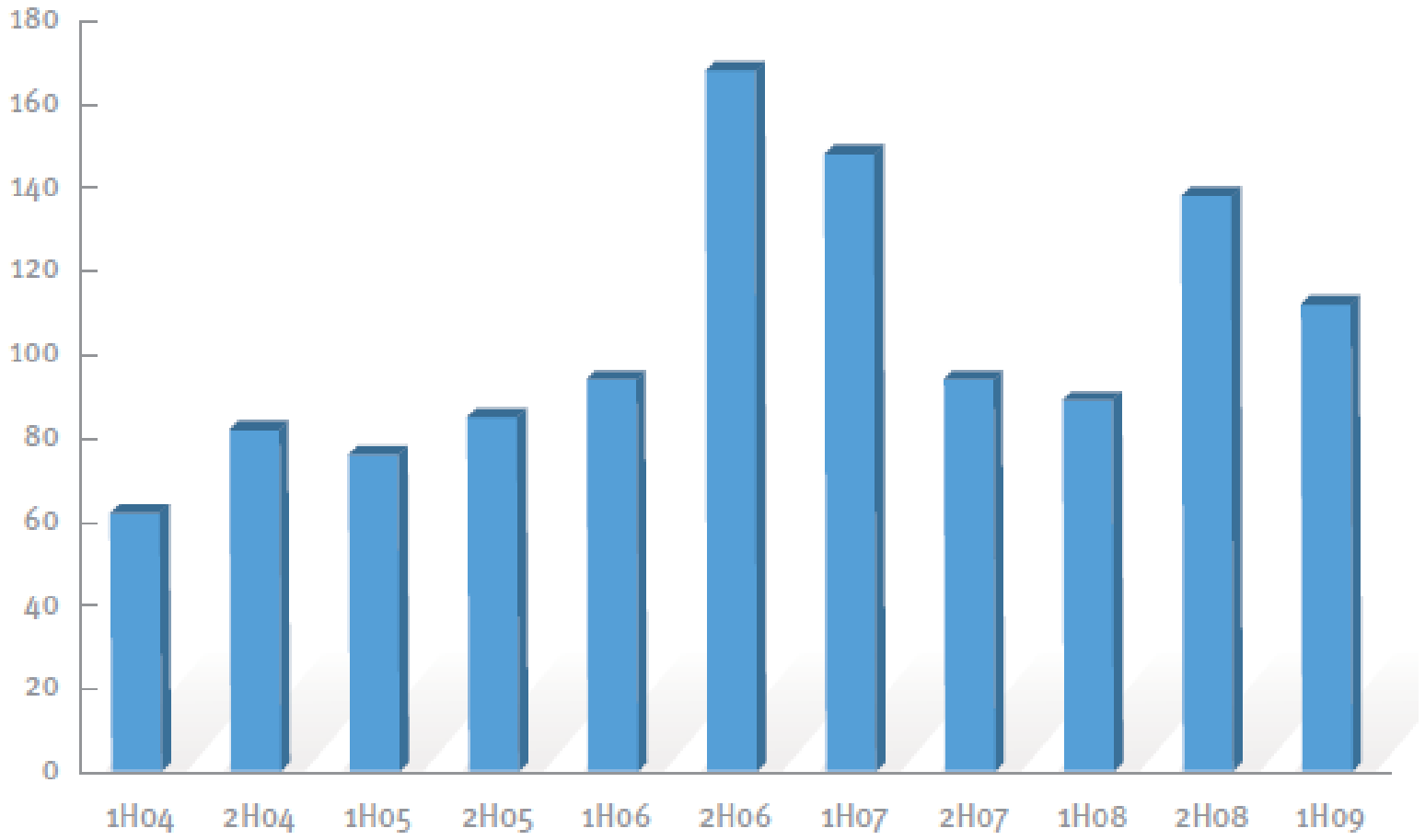
Windows 7

Windows 7 Vulnerabilities

An attacker can remotely crash without no user interaction

Windows7 machine with SMB driver Windows 7's default configuration of UAC is not effective at protecting a PC from modern malware opening Pandora's box of security vulnerabilities

Malware	Windows 7 (UAC)	Windows 7 (No UAC)	Notes
Troj/FakeAV-AFY	Ran	Ran	
Troj/Bredo-M	did not run	did not run	"Not Win32"
W32/Autorun-ATK	did not run *	Ran	"Failed to set data for MisVh55"
Mal/EncPk-KY	Ran	Ran	
Mal/EncPk-KP	Ran	Ran	
Troj/Agent-LIW	Ran	Ran	
Troj/Banker-EUT	did not run	did not run	"Failed to set data for **/Failed to create key list"
Troj/FakeAV-AFX	Ran	Ran	
Troj/Zbot-JN	Ran	Ran	
W32/Autorun-ATC	Ran	Ran	



Vulnerability Disclosure for Microsoft Products 1H04 – 1H09

Rouge
Anti-viruses

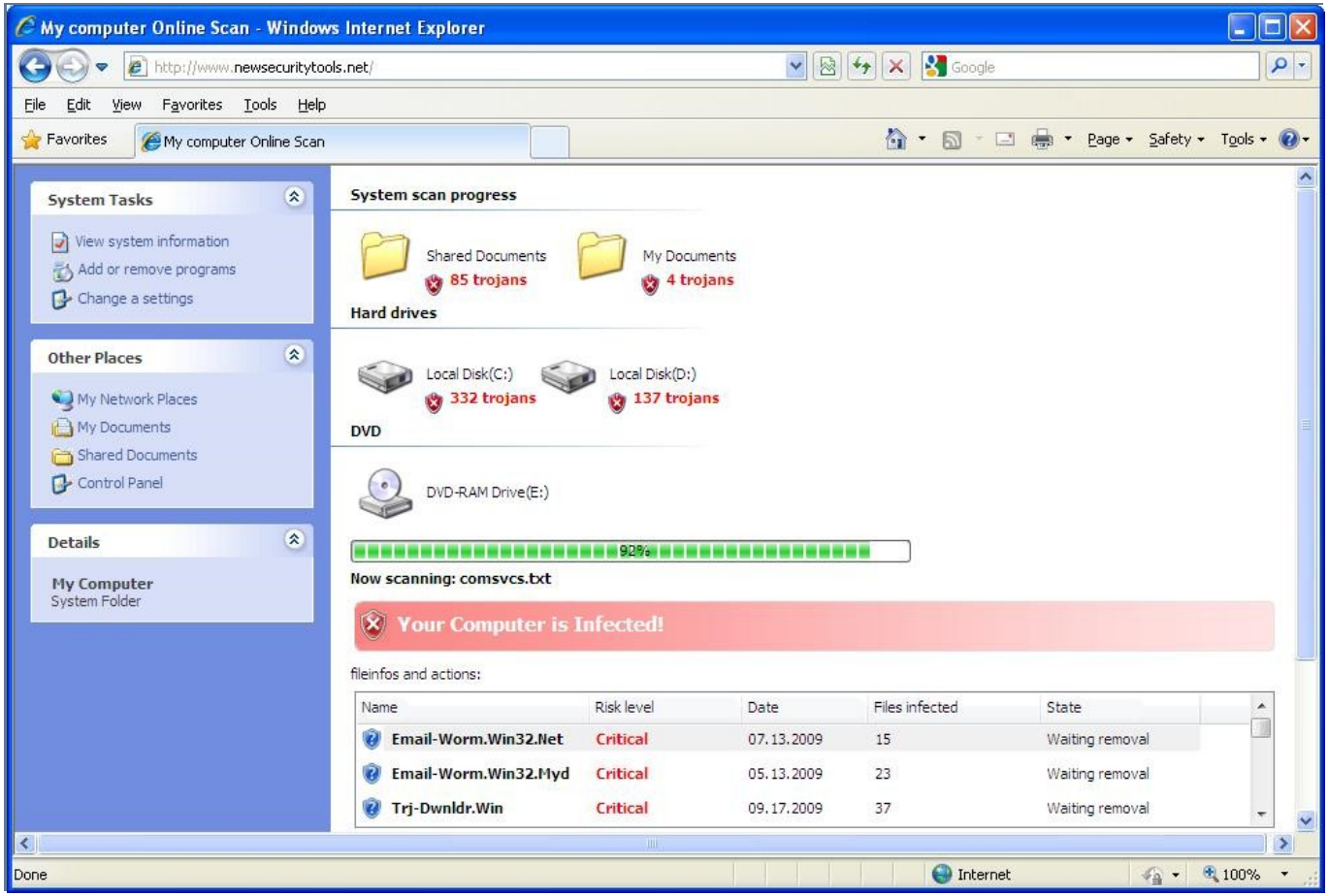
Fake Anti-Virus Websites

False Virus Websites falsely alert a web surfer as the users computer is infected with a dangerous code

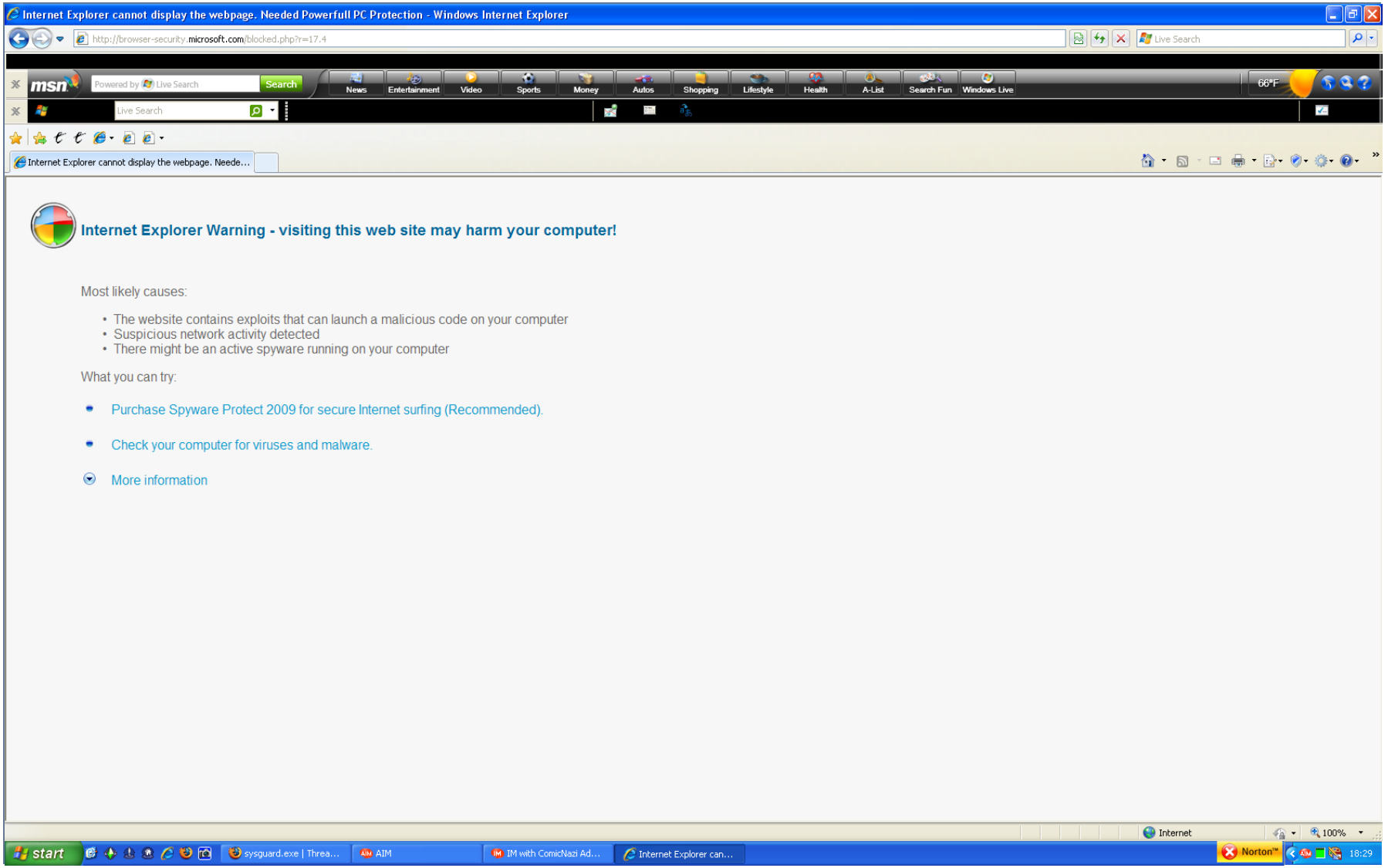
The user is then misguided to download false anti virus software which is infested with Trojans and Malware

Fake Anti-Virus Websites(cont'd)

People follow links in email of unknown sources



Fake Virus Websites(cont'd)



Fake Anti-viruses

Phishing Websites

Statistical Highlights for 1st Half, 2009

	Jan.	Feb.	March	April	May	June
Number of unique phishing email reports received by APWG from consumers	34,588	31,298	30,125	35,287	37,165	35,918
Number of unique phishing web sites detected	27,300	21,974	30,760	36,194	45,959	49,084
Number of brands hijacked by phishing campaigns	294	272	310	273	268	259
Country hosting the most phishing websites	USA	USA	USA	USA	USA	Sweden
Contain some form of target name in URL	69.01 %	64.44%	64.43%	63.25%	47.26%	33.12%
No hostname; just IP address	4.66%	8.69%	4.07%	2.33%	3.04%	1.86%
Percentage of sites not using port 80	0.05%	0.13%	0.09%	0.02%	0.10%	0.21%

Anti Hacking Forum - Tiger Woods/ Michael Jackson, etc.

Mobile Application Security

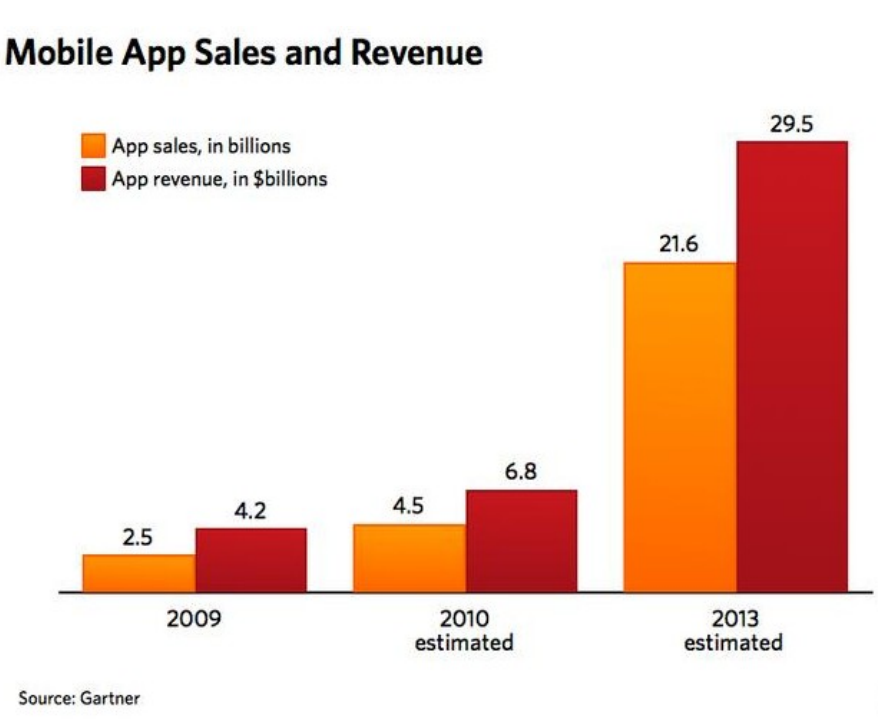
Apple Mobile Application Security

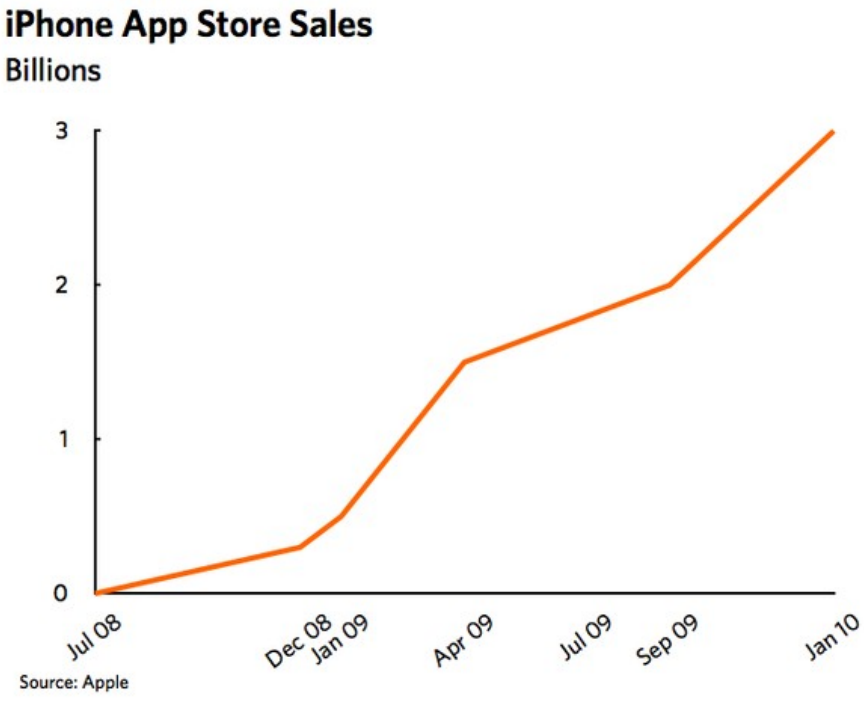
Apple's market share would be 99.4% of the three billion total app sales.

Two and a half billion app sold in 2009

By 2013, Gartner predicts 21.6 billion app sales for a total revenue of 29.5 billion dollars

jail Broken (rogue break apps) Leaving Communication channels open



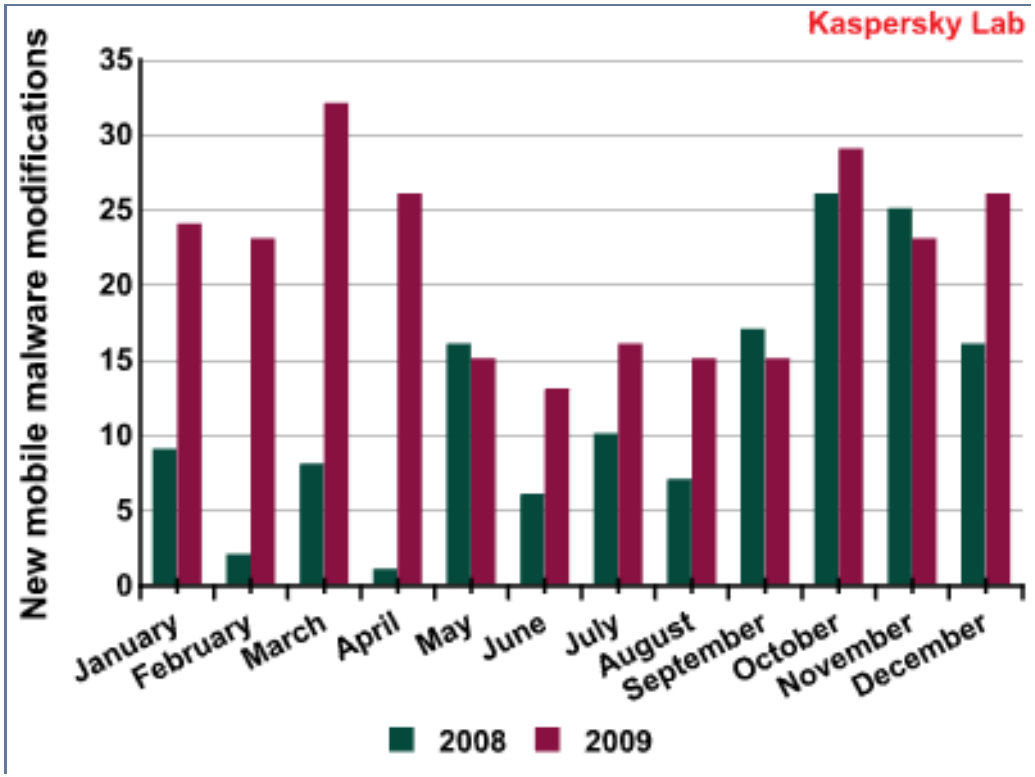


Apple Mobile Application Sales

Number of Infected Apps

One in 63 Smartphones Infected by Mobile Spyware and Malware

http://www.smobilesystems.com/



New mobile malware modifications by month (2008-2009 гг.)

iPhone Viruses

A new virus is infecting iPhones - the Ikee - forcing users to look at a picture of Rick Astley as their wallpaper.

It's 80-90% likely that we will see malware targetting the iPhone - Runald, Security Response Manager for F-Secure Security Labs

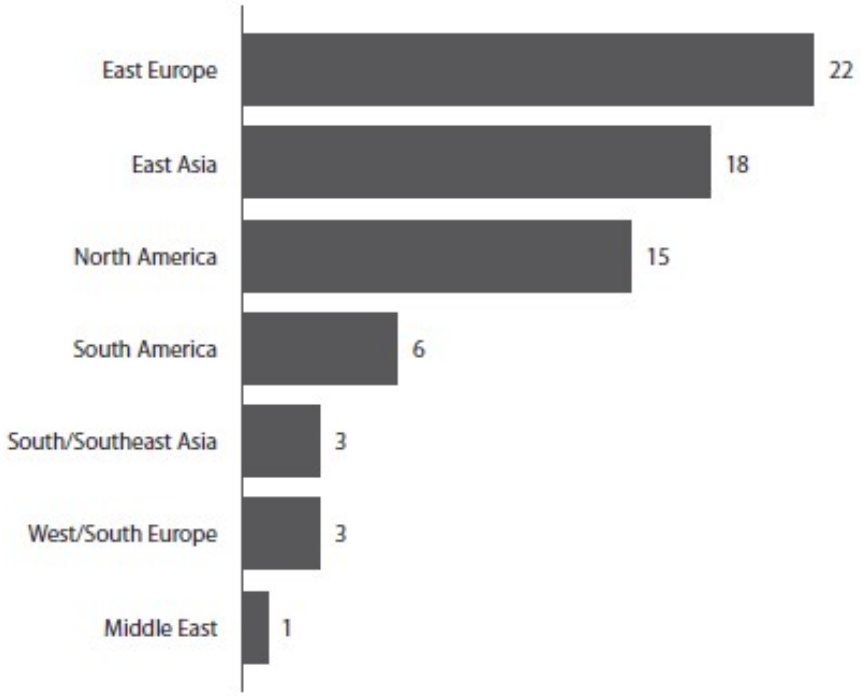
Major Security Breaches in 2009

- Phishing attacks on banking sites makes banks loose between 2.4 and 9.4 million dollars in January 2009 when attackers were able to steal more than 130,000,000 credit card records

- Terrorists intercept US Drone unencrypted Video Feeds using a $26 off the shelf software called SkyGrabber

- Hackers stole 8.3 million records, erased the originals and created an encrypted backup of Virginia State Prescription Monitoring

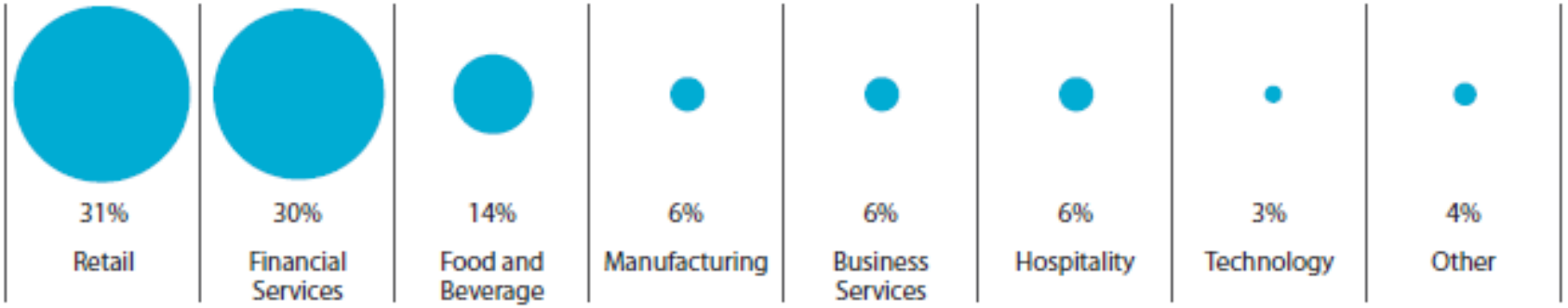
Figure 9. Location of attacking IP(s) by number of breaches



DOD IA Workforce Assessment Identifies GAP in US Workforce Preparedness

State of Cyber Security in 2009

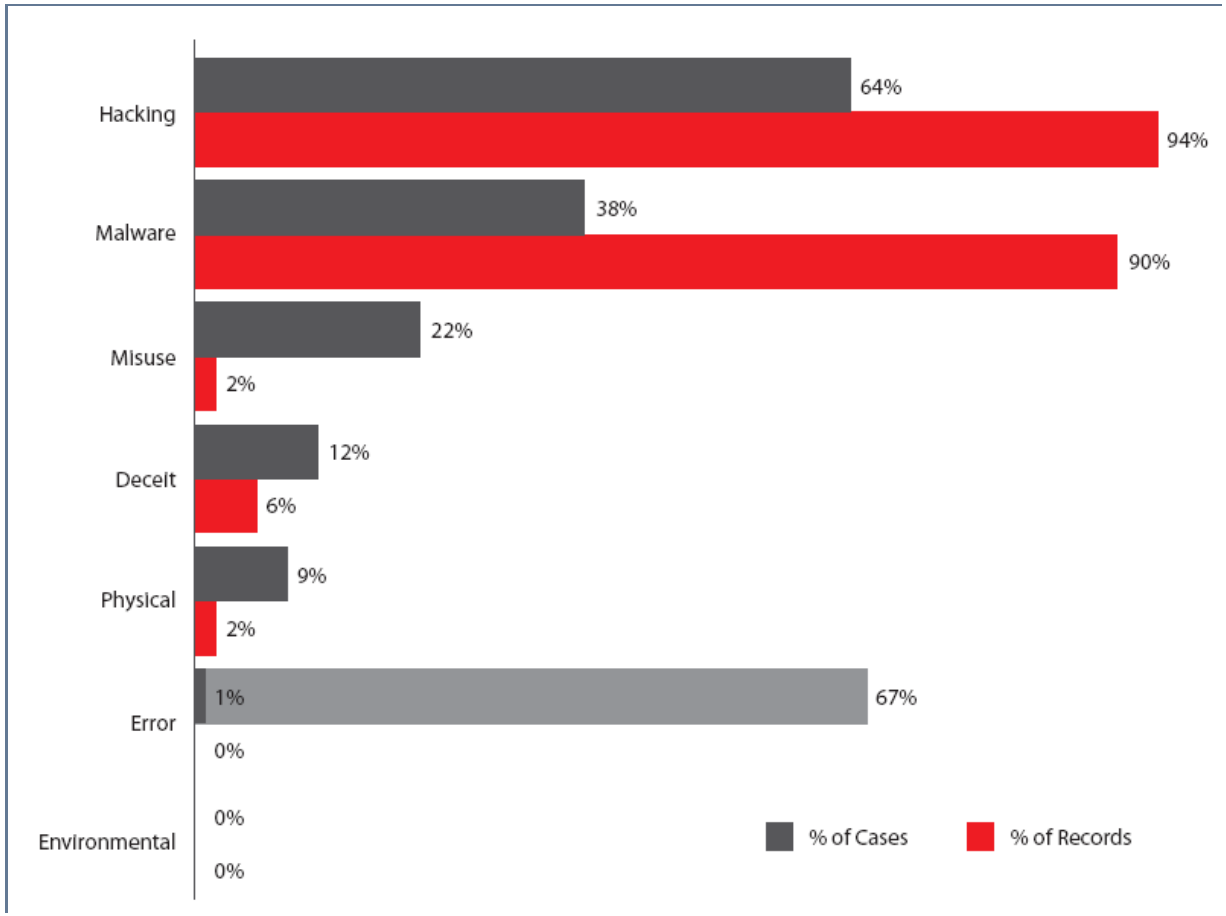
Figure 1. Industries represented by percent of breaches



Source: *http://www.verizonbusiness.com/*

Up to 30,000 email addresses and passwords from Gmail, Hotmail, Yahoo Mail, AOL, Comcast and EarthLink accounts were posted online at a number of sites including Pastebin.com

State of Cyber Security in 2009 (cont'd)



Source: *http://www.verizonbusiness.com/*

Threat categories by percent of breaches (black) and records (red)

Symantec Government Internet Security Threat Report

Top Web-based attacks

Rank	Web-based Attack	Percentage
1	Microsoft Internet Explorer ADODB.Stream Object File Installation Weakness	30%
2	Acrobat PDF Suspicious File Download	11%
3	ANI File Header Size Buffer Overflow	7%
4	Adobe SWF Remote Code Executable	7%
5	Microsoft Internet Explorer DHTML CreateControlRange Code Executable	6%
6	SnapShot Viewer ActiveX File Download	5%
7	Microsoft Internet Explorer XML Core Services XMLHTTP Buffer Overload	4%
8	Quicktime RTSP URI Buffer Overload	3%
9	AOL SuperBuddy ActiveX Code Executable	3%
10	Microsoft Internet Explorer WebViewFolderIcon ActiveX Control Buffer Overflow	2%

Source: Symantec Corporation April 09, http://eval.symantec.com

Symantec Government Internet Security Threat Report, Published April 2009

Top countries of origin for Web-based attacks

Rank	Country	Percentage
1	United States	38%
2	China	13%
3	Ukraine	12%
4	Netherlands	8%
5	Russia	5%
6	United Kingdom	5%
7	Canada	3%
8	Japan	2%
9	Latvia	1%
10	France	1%

Source: Symantec Corporation April 09, http://eval.symantec.com

Symantec Government Internet Security Threat Report, Published April 2009

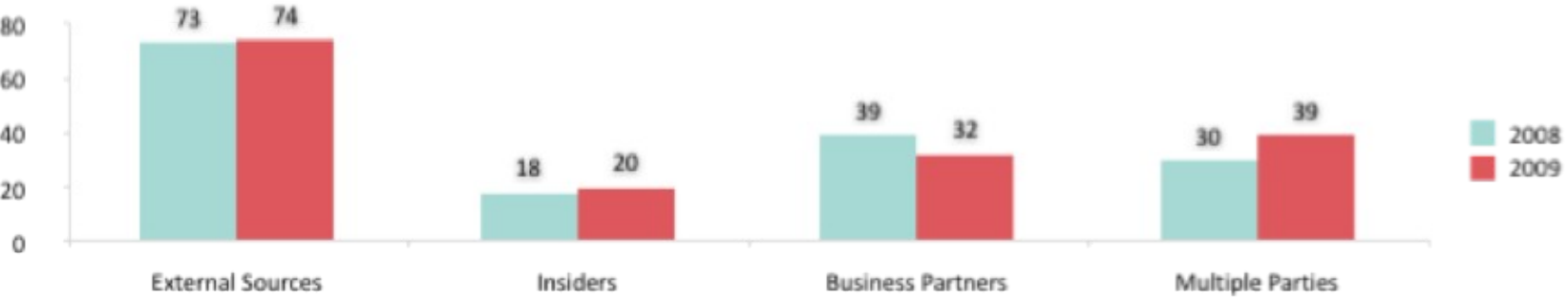
Malicious activity by country

2008 Rank	2008 Rank	Country	2008 Overall Percentage	2007 Overall Percentage	Malicious Code Rank	Spam Zombies Rank	Phishing Websites Host Rank	Bot Rank	Attack Origin Rank
1	1	United States	23%	26%	1	3	1	2	1
2	2	China	9%	11%	2	4	6	1	2
3	3	Germany	6%	7%	12	2	2	4	4
4	4	United Kingdom	5%	4%	4	10	5	9	3
5	8	Brazil	4%	3%	16	1	16	5	9
6	6	Spain	4%	3%	10	8	13	3	6
7	7	Italy	3%	3%	11	6	14	6	8
8	5	France	3%	4%	8	14	9	10	5
9	15	Turkey	3%	2%	15	5	24	8	12
10	12	Poland	3%	2%	23	9	8	7	17

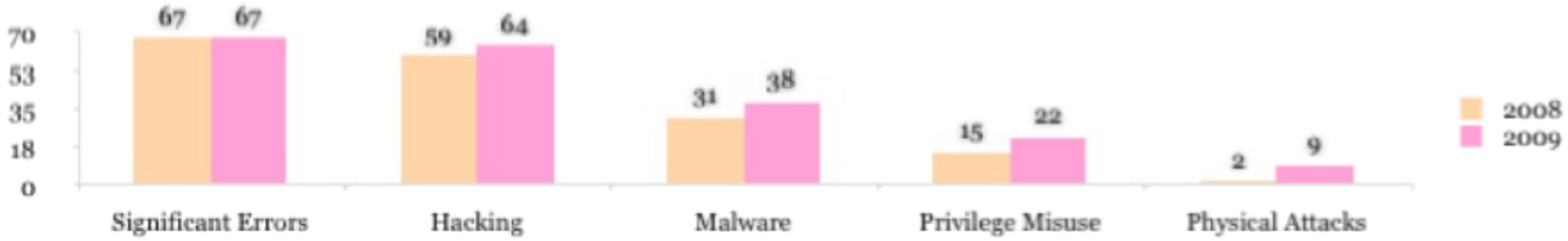
Source: Symantec Corporation April 09, http://eval.symantec.com

2009 Data Breach Investigations Report

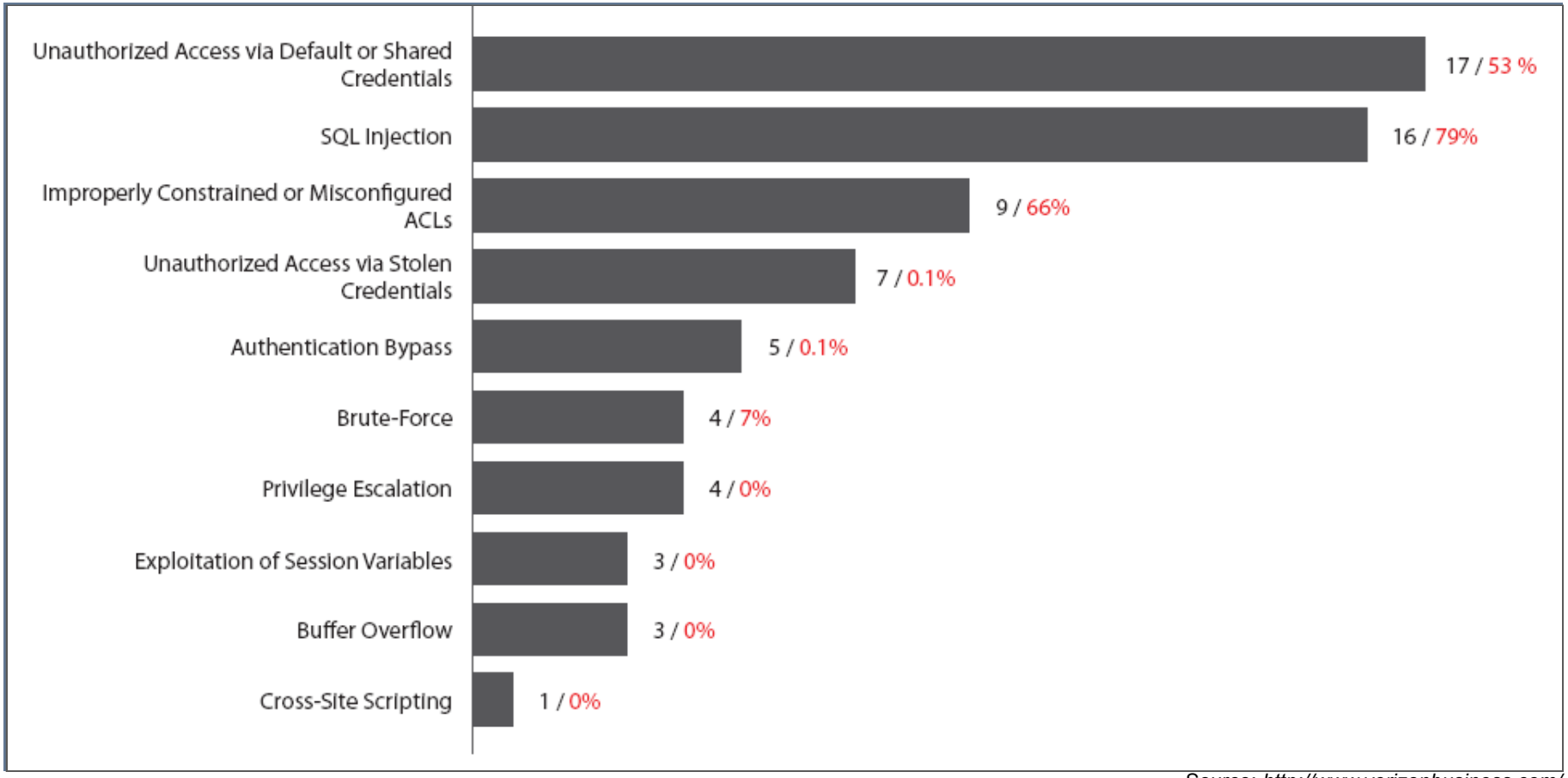
Who is behind the data breaches?



How do breaches occur?



Source: Verizon's 2009 Data Breach Investigations Report, www.verizon.com



Source: *http://www.verizonbusiness.com/*

Types of Hacking by Number of Breaches (Black) and Percent of Records (Red)

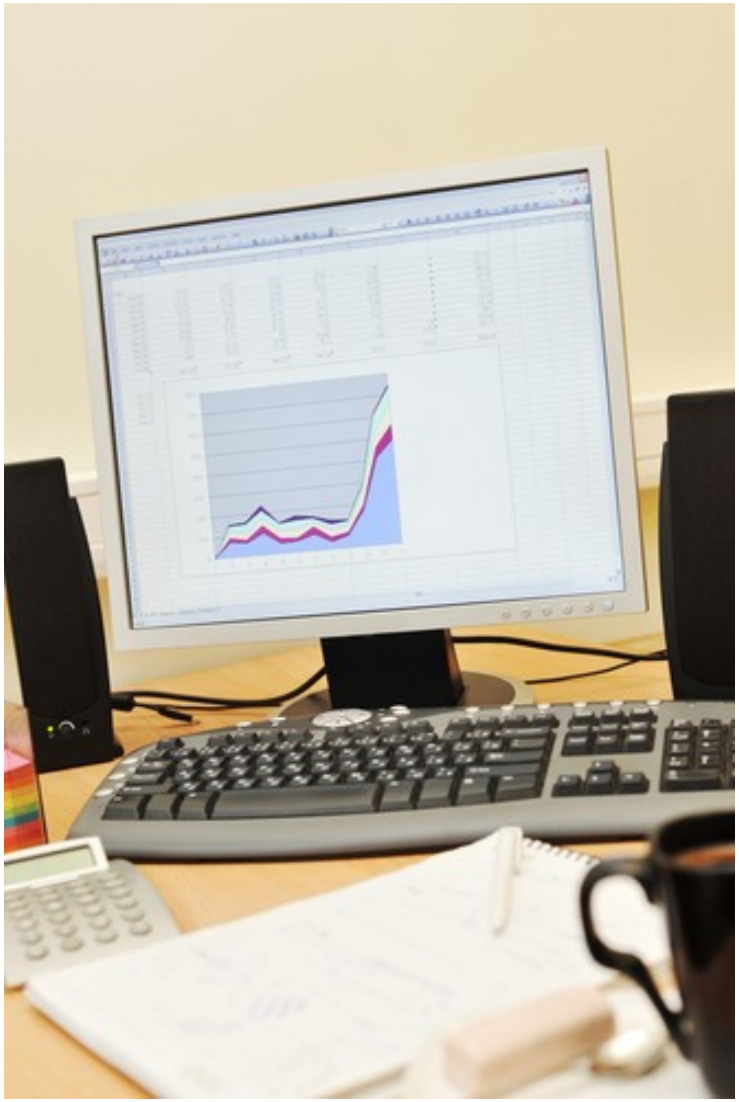
Certified Ethical Hacker Program Achieves DoD 8570.

Department of Defense Formally Approves EC-Council's CEH Certification to help defend US Interests.

Scams Target The Average Joe!

Online Frauds

- Employment Scams
  - Employment Scams (Job Scams) are just one more way in which scammers separate hard-working people from their money
- The "Money Mule“
  - A"money mule" or "money transfer agent" is used to launder funds obtained as a result of phishing and Trojan scams
  - A"money mule" or "money transfer agent" is used to launder funds obtained as a result of phishing and Trojan scams



Check Fraud

- Most job scams involve counterfeit checks or bankers drafts - some may be paid directly into the employee's bank account, with instructions to 'send on the rest as soon as possible‘

- By the time the check has been


THIS DOCUMENT HAS A COLORED BACKGROUND AND MICROPRINTING. THE REVERSE SIDE INCLUDES AN ARTIFICIAL WATERMARK.

CENTEX HOMES
CENTRAL VALLEY
1840 CENTRAL VALLEY
VISALIA, CA 93277

Bank of America N.A.
Atlanta, Dekalb City

CHECK NO. 829510

PAY EIGHT-THOUSAND THREE-HUNDRED AND 00/100********** DOLLARS

DATE	AMOUNT
09/29/2005	**8,300.00

TO THE ORDER OF
BEAU BALUNSAT
2082 QUESADA AVE
SAN FRANCISCO, CA 94124

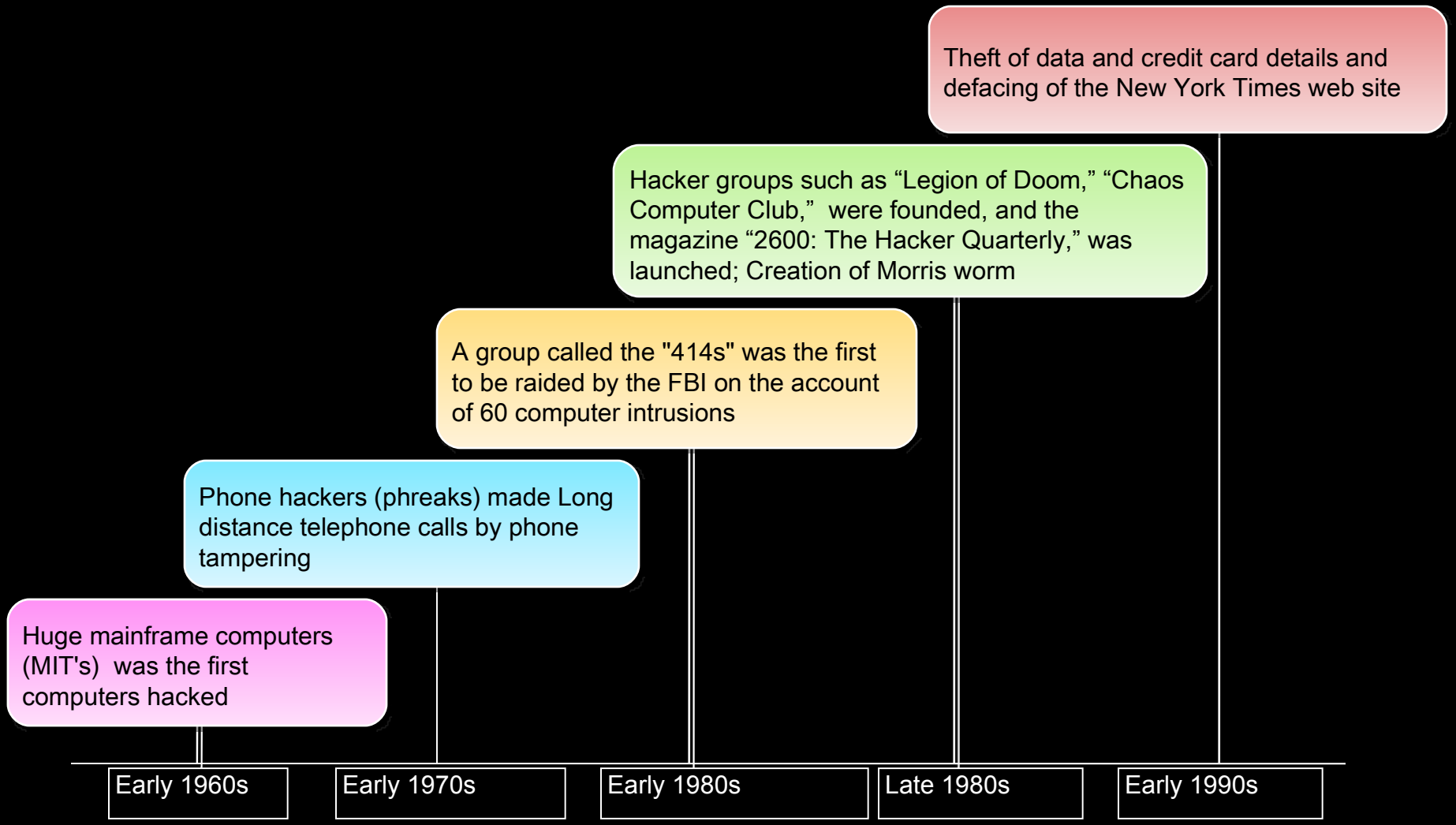
Remember This Rule!

If an attacker wants to get inside your system, he will and there is nothing you can do about it

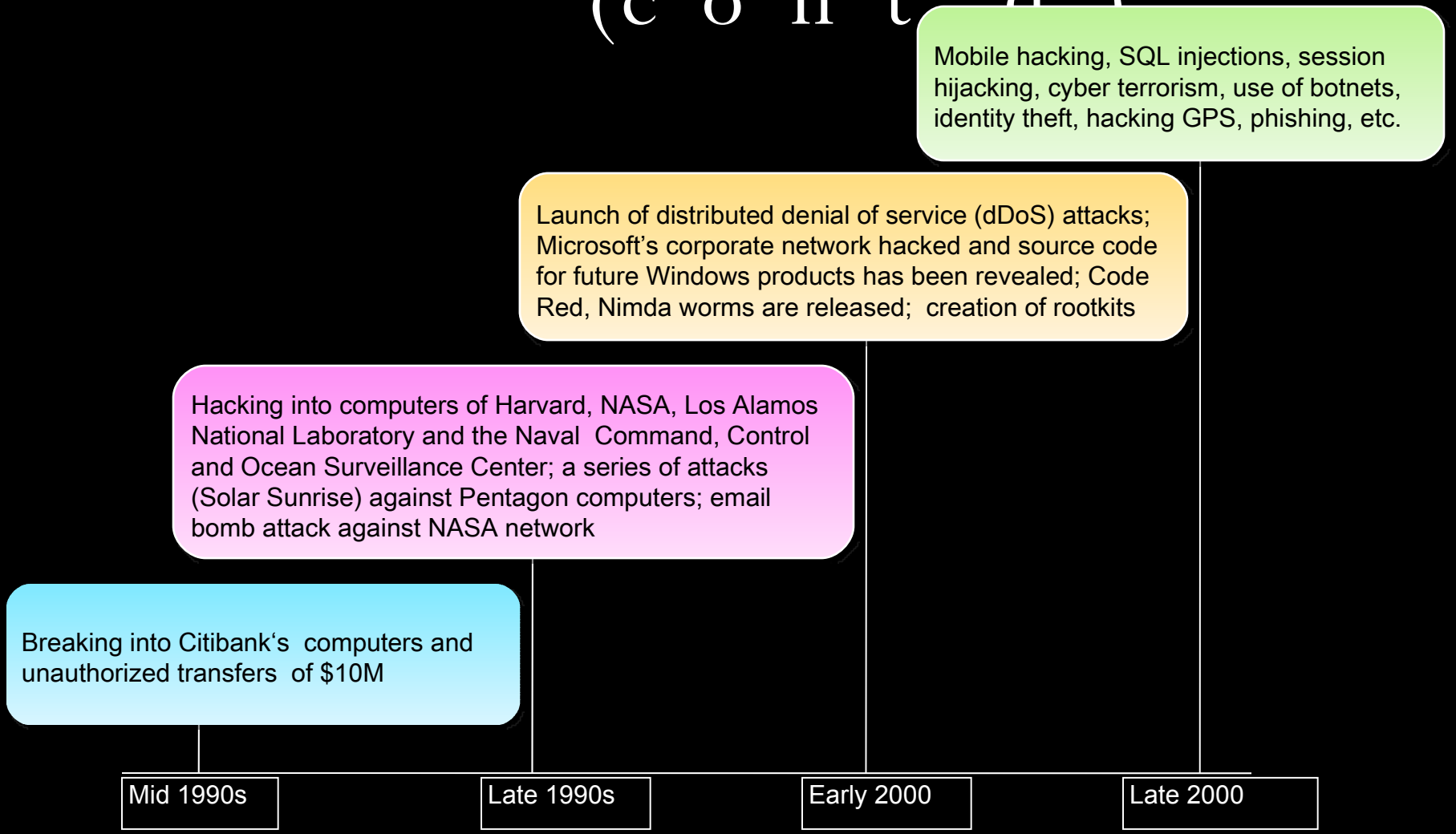
The only thing you can do is

make it harder for him to get in

Hacking History



Hacking History (cont'd)



Phase 1 - Reconnaissance

Reconnaissance refers to the preparatory phase where an attacker seeks to gather as much information as possible about a target of evaluation prior to launching an attack

Could be the future point of return, noted for ease of entry for an attack when more about the target is known on a broad scale

Business Risk: **Notable** - Generally noted as "rattling the door knobs" to see if someone is watching and responding

The Invisible hack

- KeyGhost keylogger
  - Can be installed even when the target computer is logged out, has a password, is locked or switched off.
  - The device can be unplugged and the keystrokes retrieved on another computer.
  - No software installation is needed
  - Impossible to detect or disable using software

- KeyKatcher keylogger

–Records everything, even BIOS passwords, where software loggers have not even started running yet.

–Similar to KeyGhost the device does not use system resources

–Even if the device is unplugged, or a computer is turned off, the KeyKatcher will continue to store the information.

- User unawareness
  - Since there is no clear destruction activity and a clandestine mode of exploit's operation the assaulted parties are not aware of what is going on.

- Deceptive appearance of hardware keyloggers.
  - For unsophisticated user a keylogger looks like a part of an extension cord or a computer part
    - Difficult to detect

Password information is recorded in the way presented below (user keystrokes are in bold):

User activity	Screen information
User types <ctr-alt-del>	<ON><PWR>
User types login password	<PWR><ctrl-alt-del>
A site URL	Wnt24~L4r
User types a user ID	www.americanexpress.com
User types a password	JohnDoe
	9ltrscr_T

Password information

Human-based Social Engineering: Dumpster Diving

Search for sensitive information at the target company's:

- Trash-bins
- Printer trash bins
- User desk for sticky notes etc.

Collect:

- Phone bills
- Contact information
- Financial information
- Operations related information etc.

Dumpster Diving Example

A man behind the building is loading the company's paper recycling bins into the back of a truck. Inside the bins are lists of employee titles and phone numbers, marketing plans, and the latest company financials

This information is sufficient to launch a social engineering attack on the company

Phase 2 - Scanning

Scanning refers to the pre-attack phase when the attacker scans the network for specific information on the basis of information gathered during reconnaissance

Scanning can include use of dialers, port scanners, network mapping, sweeping, vulnerability scanners, etc.

Business Risk: High

Attackers have to get a single point of entry to launch an attack

Phase 3 - Gaining Access

Gaining access refers to the point where the attacker obtains access to the operating system/applications on the computer/network

- He can proceed to escalate his privileges to obtain the complete control of the system
- In this process, he also compromises other intermediate systems that are connected to it

Examples include password cracking, buffer overflows, denial of service, session hijacking, etc.

Business Risk: **Highest**

The attacker can gain access at the operating system level, application level, or network level

Phase 4 - Maintaining Access

Maintaining access refers to the phase when the attacker tries to retain his/her ownership of the system

Attackers may prevent the system from being owned by other attackers by securing their exclusive access with Backdoors, RootKits, or Trojans

Attackers can upload, download, or manipulate data, applications, and configurations on the owned system

Business Risk: Highest

Attackers use the compromised system to launch further attacks

What is a [illegible]jan

s divided into two parts:

- *Client is* the controlling component at the attacker's side
- *Server is* the part installed on the victim's systems

ystem

Basic Working of Trojans

An attacker gets access to the Trojaned system as the system goes online

By the access provided by the Trojan, the attacker can stage different types of attacks

Phase 5 - Covering Tracks

Covering tracks refers to the activities carried out by an attacker to hide his malicious acts

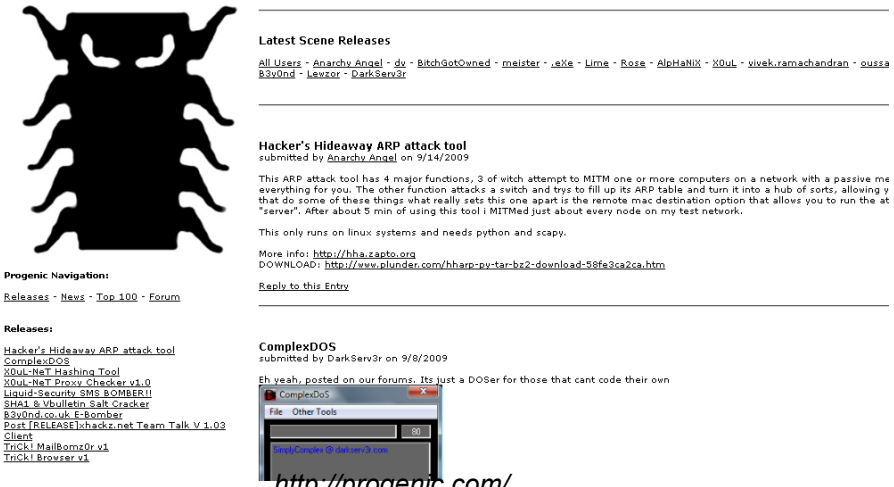
The attacker's intensions include: to continue access to the victim's system, to remain unnoticed/uncaught, to delete any evidence that might lead to his prosecution

The attacker overwrites the server, system, application logs to avoid suspicion

Eraser

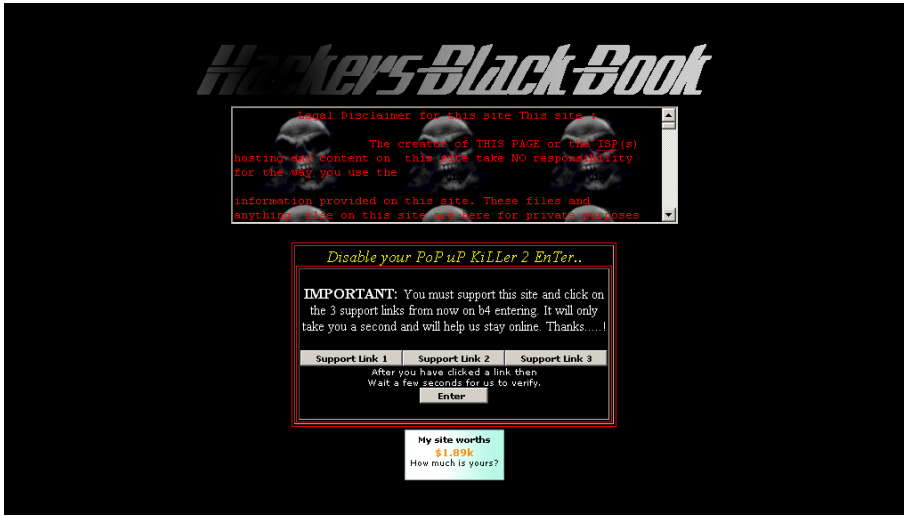
Underground Sites

www.astalavista.com/



http://progenic.com/

http://www.cultdeadcow.com/



www.hackers-black-book.com

Electronic Jihad

Electronic Jihad Program is a part of long-term vision jihadi Web site Al-jinan.org to use the Internet as a weapon

Electronic Jihad allows users to target specific IP addresses for attack in order to take any servers running at those IP addresses offline

Application includes a Windows-like interface that lets users choose from a list of target Web sites provided via the Al-jinan site, select an attack speed (weak, medium, or strong), and the click on the "attack" button

The attacks from jihadists are interested in taking Web sites down and disrupting economies that they do not like

'Electronic Jihad' App Offers Cyber-terrorism For The Masses

Although cyberterrorism has been around since the Internet reached the mainstream more than a decade ago, a relatively new Web-based application offers Islamic jihadis a way for even the relatively nontechnical to target and attack Web sites perceived to be anti-Islamic.

The "Electronic Jihad Program" is part of the long-term vision jihadi Web site Al-jinan.org has to use the Internet as a weapon, something that affects any organization that relies on the Web.

Electronic Jihad allows users to target specific IP addresses for attack in order to take any servers running at those IP addresses offline. The application even includes a Windows-like interface that lets users choose from a list of target Web sites provided via the Al-jinan site, select an attack speed (weak, medium, or strong), and the click on the "attack" button.

http://www.informationweek.com

Latest Threat on the Web! : *MOJAHEDEEN*

SECRETS Encrypt on Program

Mojahedeen Secrets 2 is a new version of an encryption tool, ostensibly written to help Al Qaeda members encrypt secrets as they communicate on the Internet

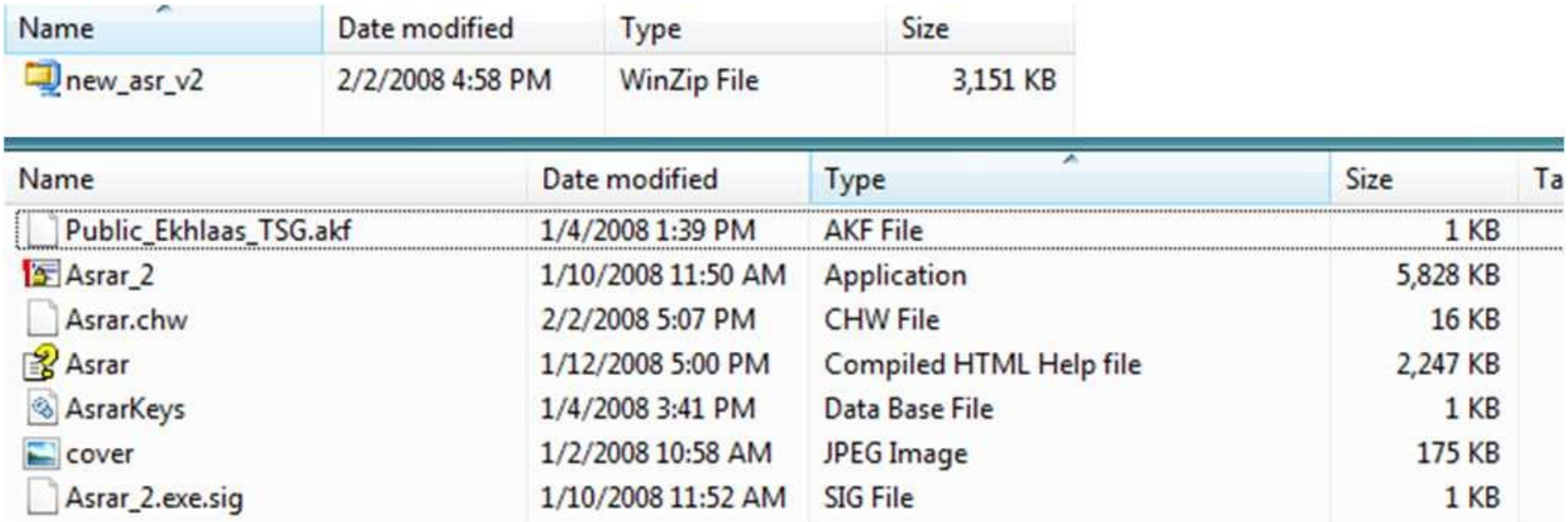
The first edition file contained several encryption algorithms (including AES 256), 2048-bit encryption keys, ROM compression encryption and encryption auto-detection, and file shredding capabilities

The second edition contains automatic message/messaging encryption/authentication and file encryption as well as code signing and checking, and file shredding

This toolset provides groups like Al-Qaida to securely transmit and wipe their files

Second edition toolset demonstrates a software development lifecycle with some level of sophistication and planning

MOJAHEDEEN SECRETS Encryption Program: Screenshot 1



Name	Date modified	Type	Size
new_asr_v2	2/2/2008 4:58 PM	WinZip File	3,151 KB

Name	Date modified	Type	Size	Ta
Public_Ekhlaas_TSG.akf	1/4/2008 1:39 PM	AKF File	1 KB	
Asrar_2	1/10/2008 11:50 AM	Application	5,828 KB	
Asrar.chw	2/2/2008 5:07 PM	CHW File	16 KB	
Asrar	1/12/2008 5:00 PM	Compiled HTML Help file	2,247 KB	
AsrarKeys	1/4/2008 3:41 PM	Data Base File	1 KB	
cover	1/2/2008 10:58 AM	JPEG Image	175 KB	
Asrar_2.exe.sig	1/10/2008 11:52 AM	SIG File	1 KB	

MOJAHEDEEN SECRETS Encryption Program: Screenshot 2

MOJAHEDEEN SECRETS Encryption Program: Screenshot 3

Websites Support Objectives of terrorist/Extremist

Terror Web 2.0

The Net-Centric Operations of Terrorist Groups Today

By Guest Contributor Jeffrey Carr

The latest phase of the Internet revolution, which has been widely referred to as Web 2.0, has not been overlooked by web-based terror networks. A recent study by the Artificial Intelligence Lab of the University of Arizona details precisely how these net-savvy terrorists are using the Web for fund-raising, recruitment, propaganda, logistical support, communications, training, and even cyber warfare.

Table 1: How Websites Support Objectives of Terrorist/Extremist Groups[1]

Terrorist objectives	Tasks supported by web sites	Web features
Enhance communication	• Composing, sending, and receiving messages • Searching for messages, information, and people • One-to-one and one-to-many communications • Maintaining anonymity	• Synchronous (chat, video conferencing, MUDs, MOOs) and Asynchronous (e-mail, bulletin board, forum, Usenet newsgroup) • GUI • Help function • Feedback form • Login • E-mail address for webmaster, organization contact
Increase fund raising	• Publicizing need for funds • Providing options for collecting funds	• Payment instruction and facility • E-commerce application • Hyperlinks to other resources

Terrorist objectives	Tasks supported by web sites	Web features
Diffuse propaganda	• Posting resources in multiple languages • Providing links to forums, videos, and other groups' web sites • Using web sites as online clearinghouses for statements from leaders	• Content management • Hyperlinks • Directory for documents • Navigation support • Search, browsable index • Free web site hosting • Accessible
Increase publicity	• Advertising groups' events, martyrs, history, ideologies • Providing groups' interpretation of the news	• Downloadable files • Animated and flashy banner, logo, slogan • Clickable maps • Information resources
Overcome obstacles from law enforcement and the military	• Send encrypted messages via e-mail, forums, or post on web sites • Move web sites to different servers so they are protected	• Anonymous e-mail accounts • Password-protected or encrypted services • Downloadable encryption software • E-mail security • Stenography

Affecting Future Infosec Workforce

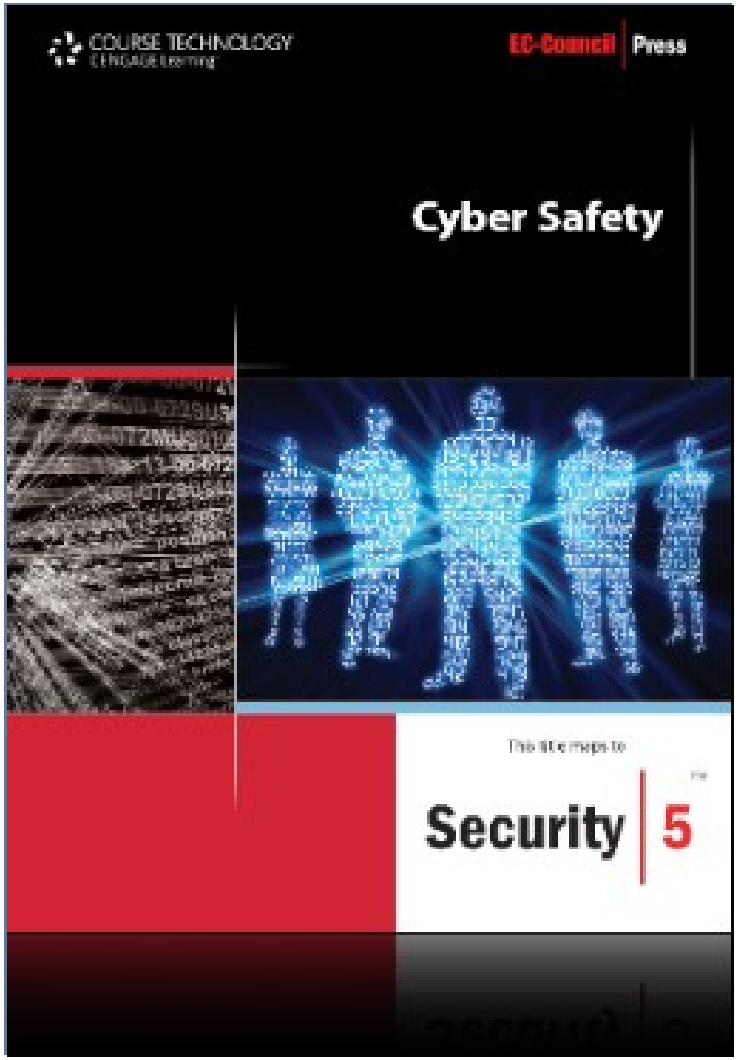
Building a complete infosec program with EC-Council Press

EC-Council Press

Fundamentals

Cyber Safety

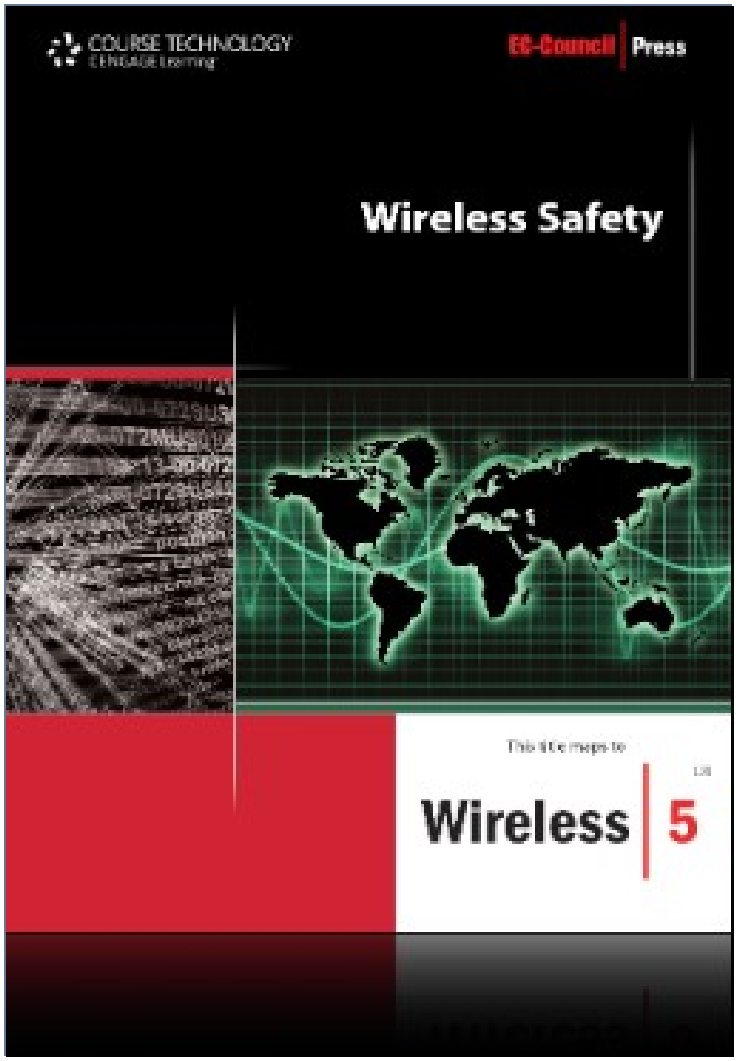
- Cyber Safety, part of the EC-Council is designed for anyone interested in learning computer security and networking basics, and prepares students for entry into high-end IT programs
- Beginning with an overview of cyber crime and security, Cyber Safety explains basic security procedures and challenges that arise in the workplace
- The reader will also learn how to address incident response and how to restrict site access
- Identify secure websites and establish security for a wireless network access point
- It provides readers with a solid base of knowledge to work towards Security|5 Certification or simply to better protect themselves and their information



Fundamentals (cont'd)

Wireless Safety

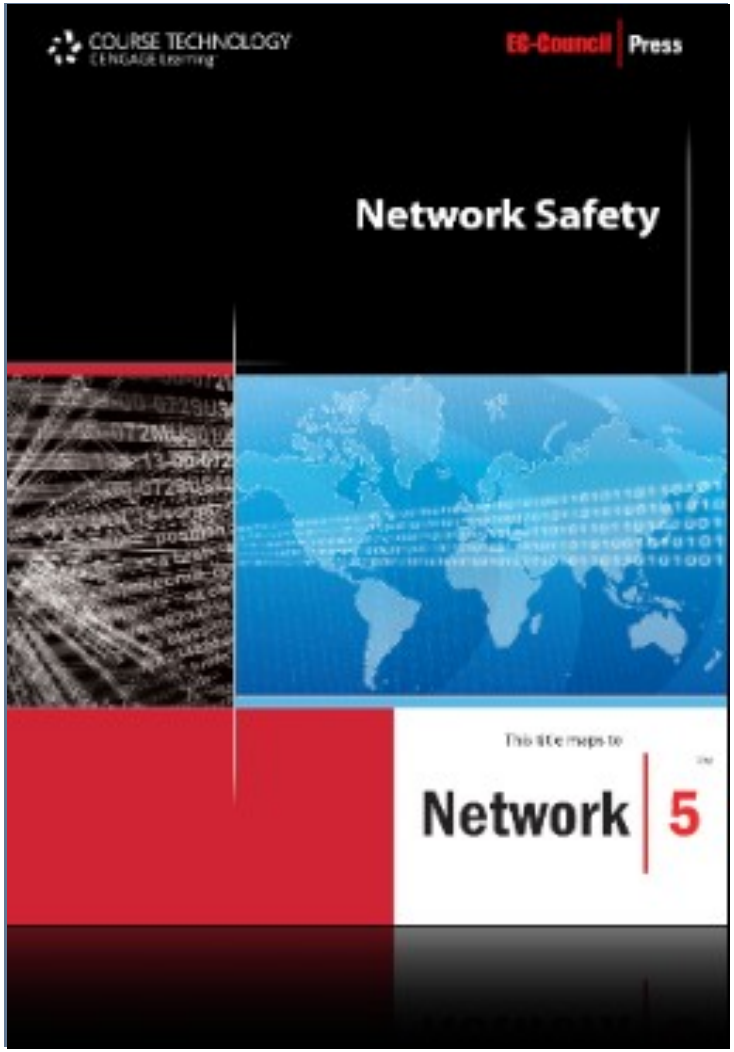
- Wireless Safety serves to expose the reader to diverse wireless communication technologies while mapping them to real world applications
- It provides an overview of WAP (wireless application protocol) and how developers view these enabling technologies, and gives a peek into future trends
- It includes IEEE and ETSI Wireless Standards, WLANs and Operation, Wireless Protocols and Communication Languages, Wireless Devices, and Wireless Security
- Wireless Safety requires no pre-requisite knowledge and aims to educate in simple applications of these technologies
- Preparing readers for success on the Wireless|5 certification from EC-Council



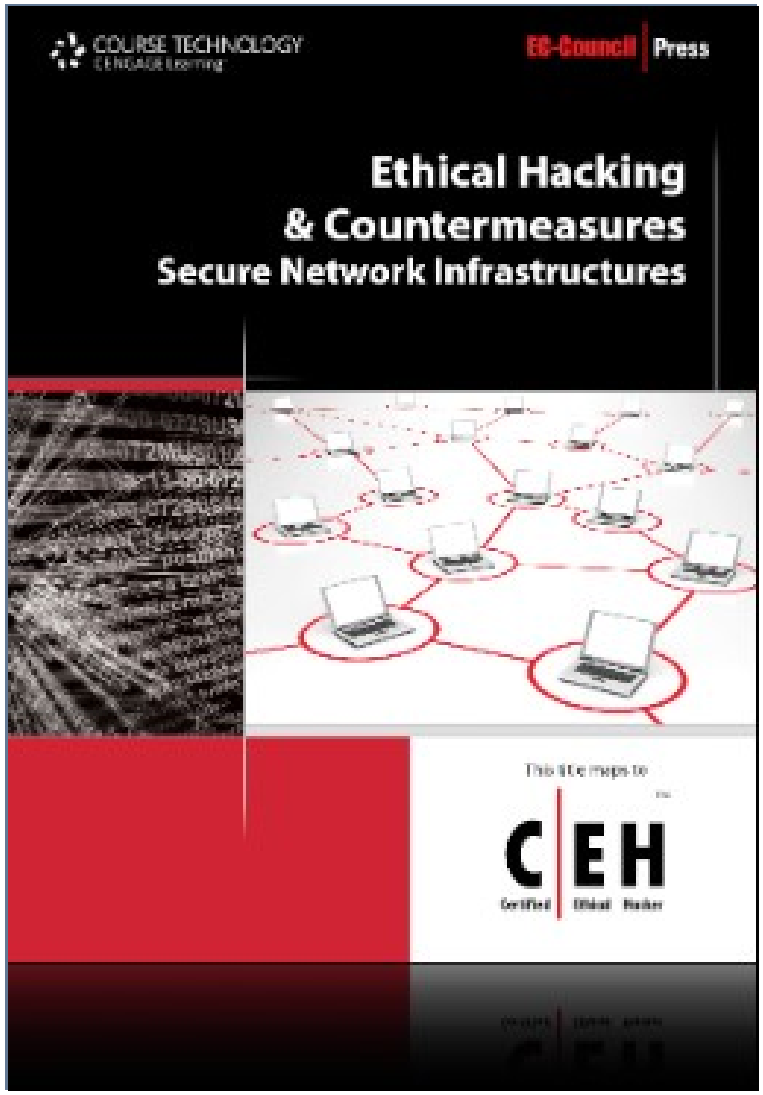
Fundamentals (cont'd)

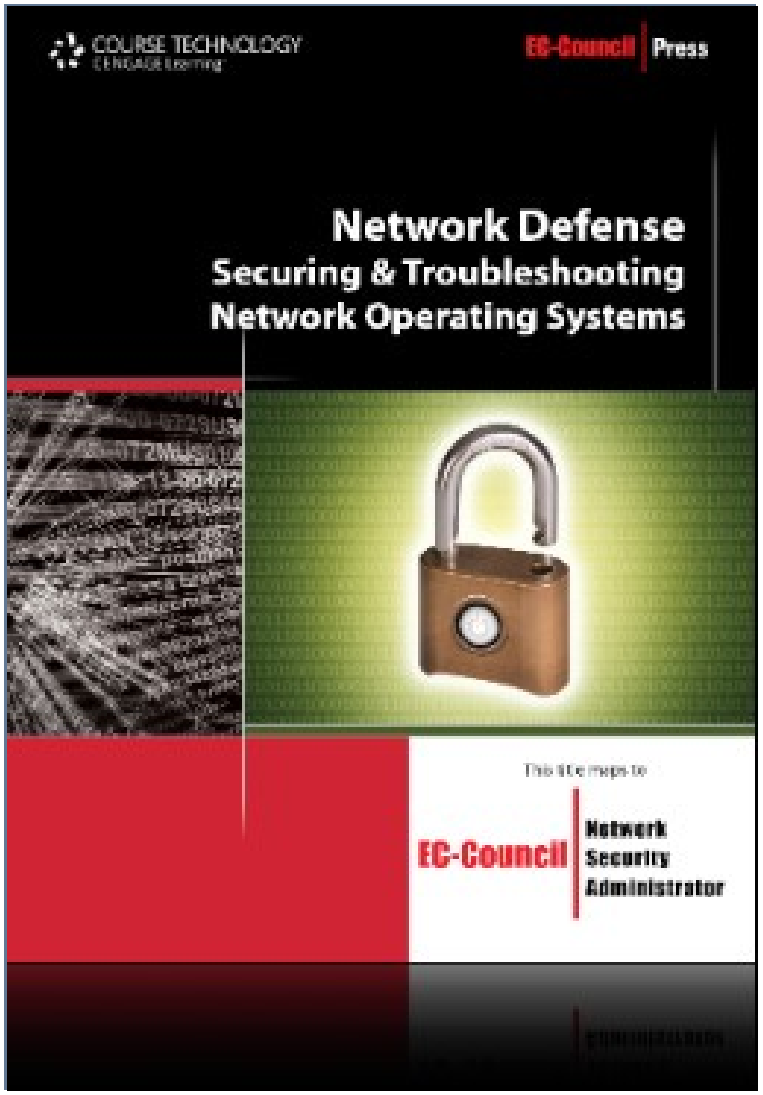
Network Safety

- The Network Safety Series from EC-Council | Press is comprised of 5 books designed to educate learners from a vendor-neutral standpoint how to defend the networks they manage
- This series covers the fundamental skills in evaluating internal and external threats to network security and design
- How to enforce network level security policies, and how to ultimately protect an organization's information
- It covers secure network fundamentals, protocols & analysis, standards and policy, hardening infrastructure, to configuring IPS, IDS, firewalls, bastion host and honeypots
- Along with the proper experience these books will prepare readers for the EC-Council

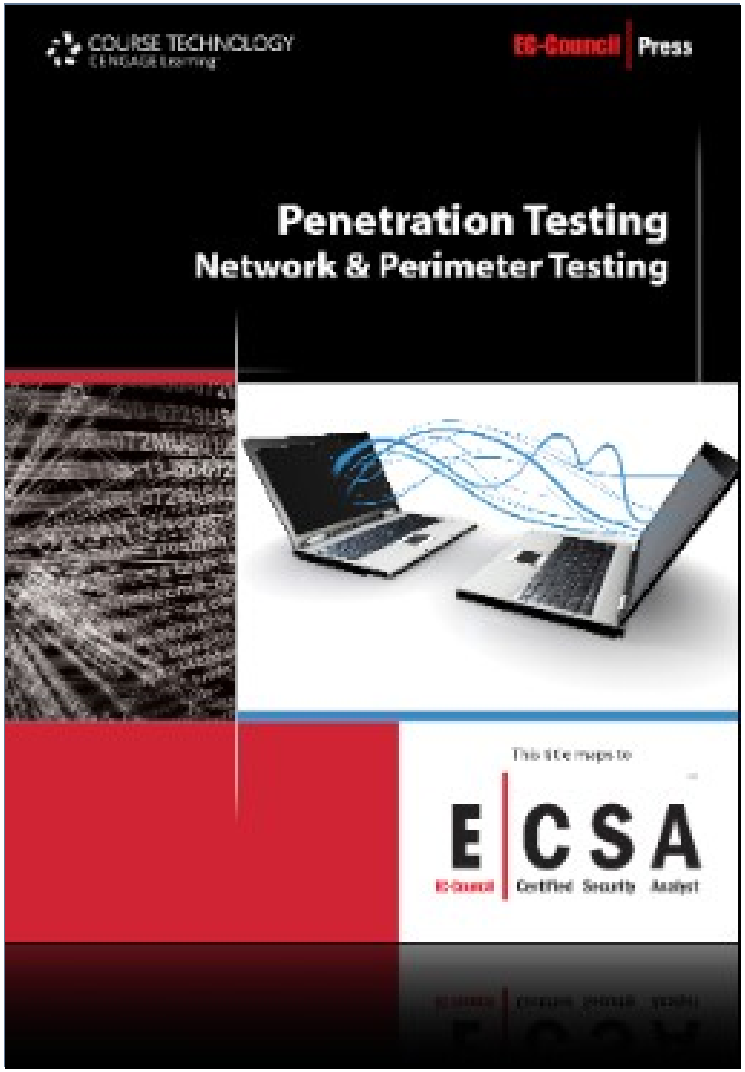


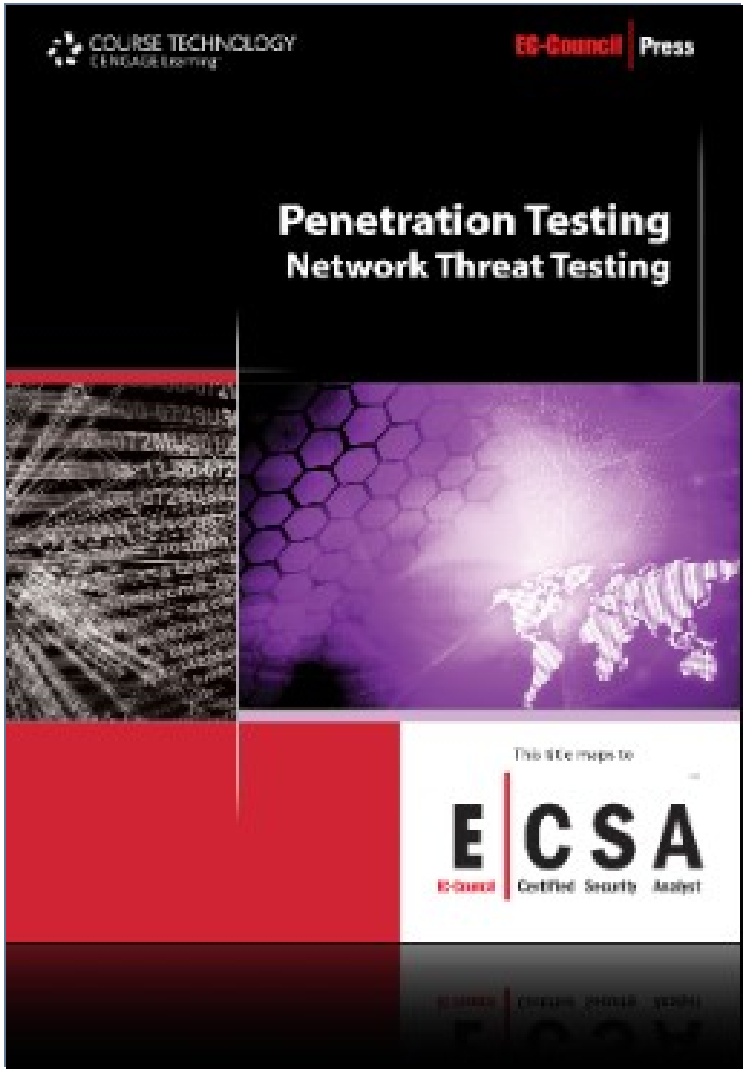
Secure Network Administration





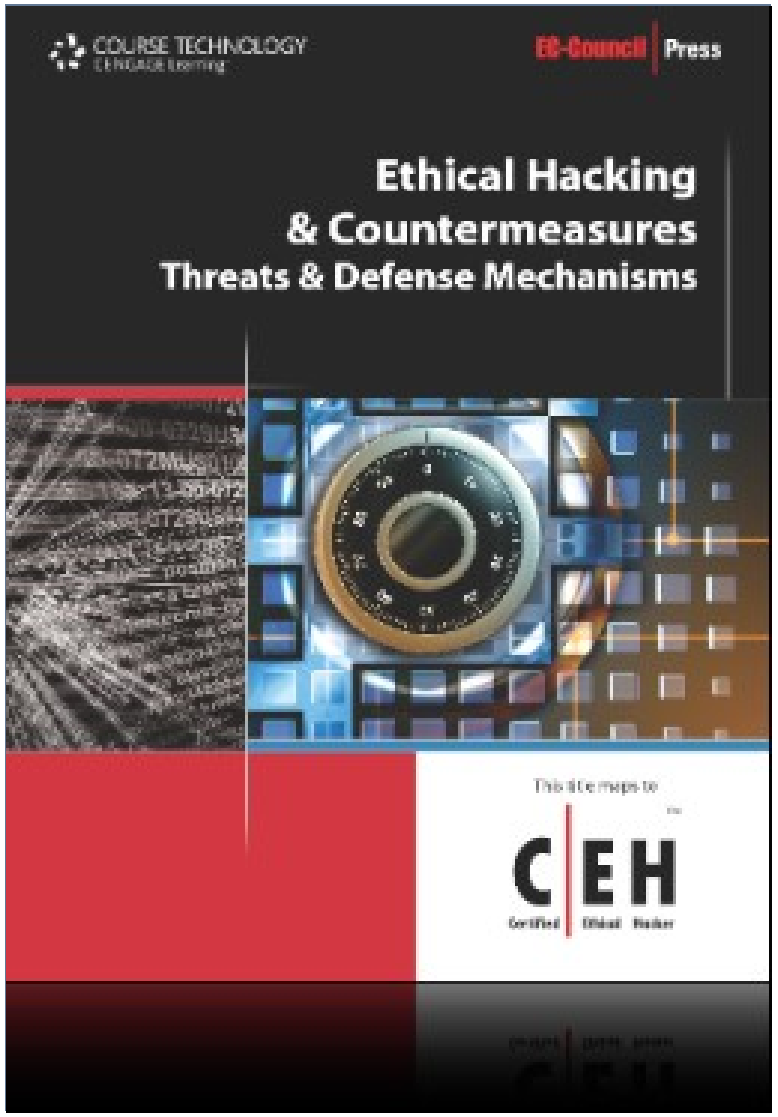
Secure Network Administration (cont'd)



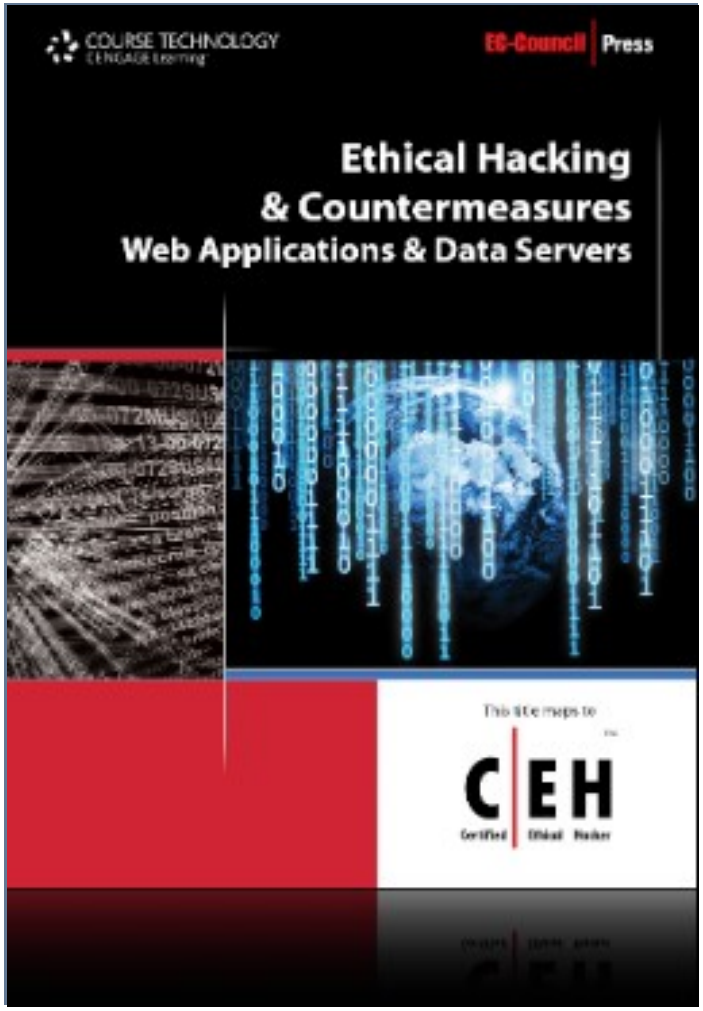


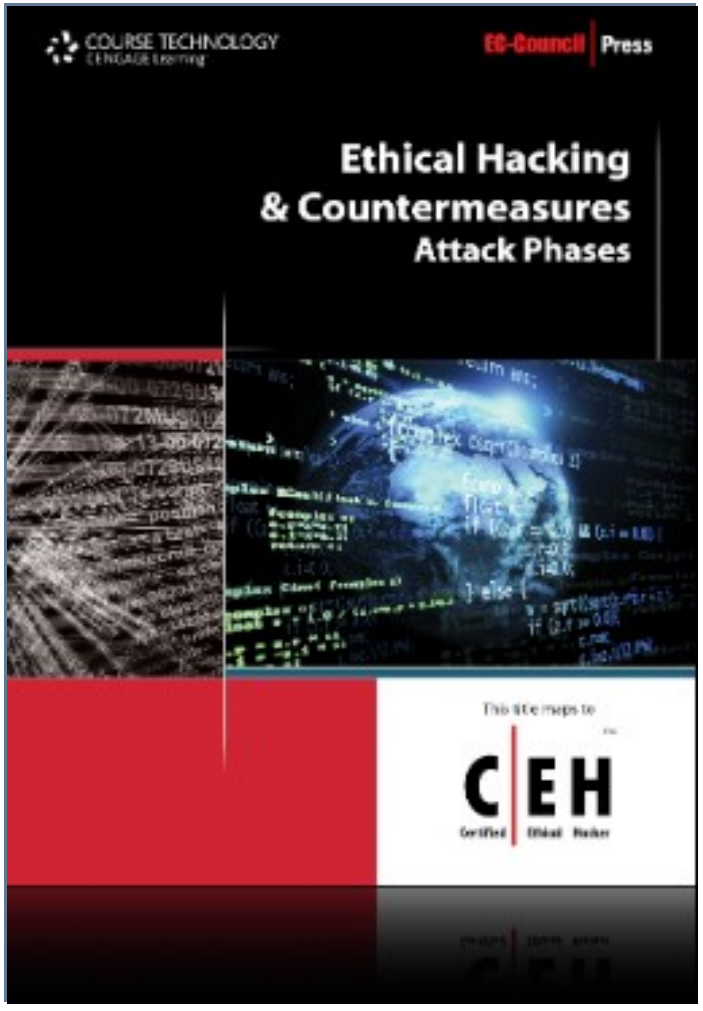
Ethical Hacking and Countermeasures

- An ethical hacker uses the same techniques as a malicious hacker but has permission from an organization
- The tools employed by malicious hackers for the purpose of testing, reporting and fixing security weaknesses
- Countermeasure techniques and strategies will be examined for their suitability against these attacks
- This program will be equipped with the skills to analyze and

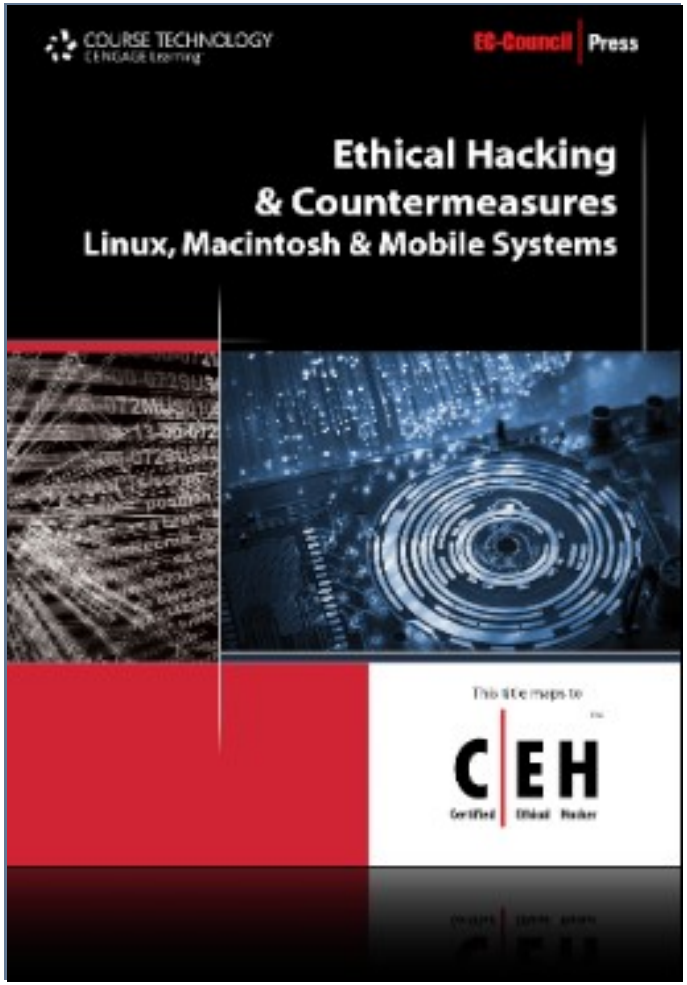


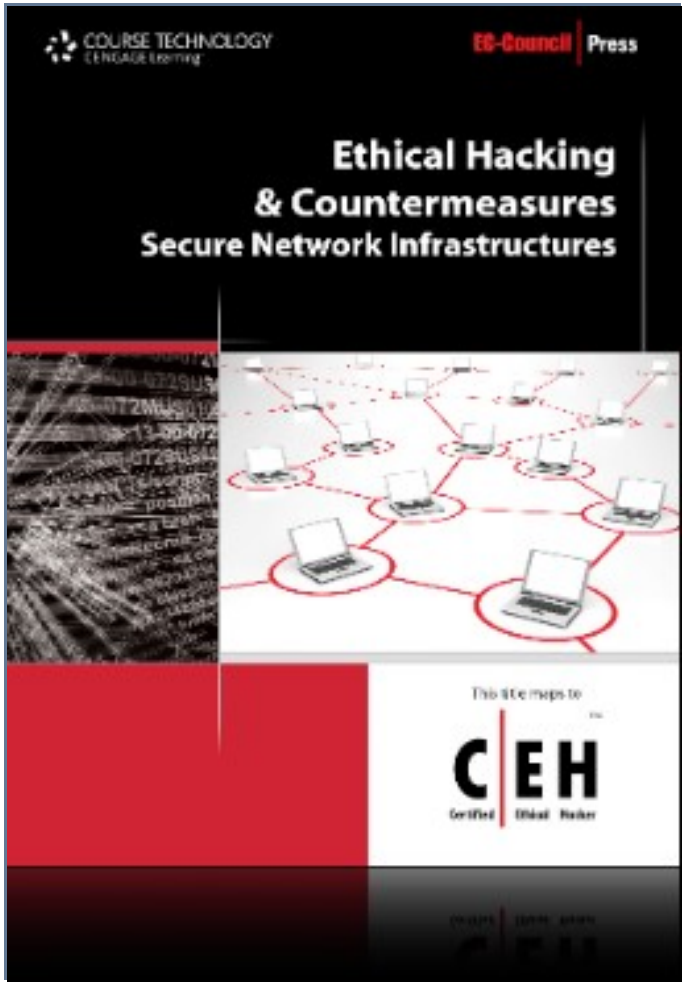
Ethical Hacking and Countermeasures (cont'd)





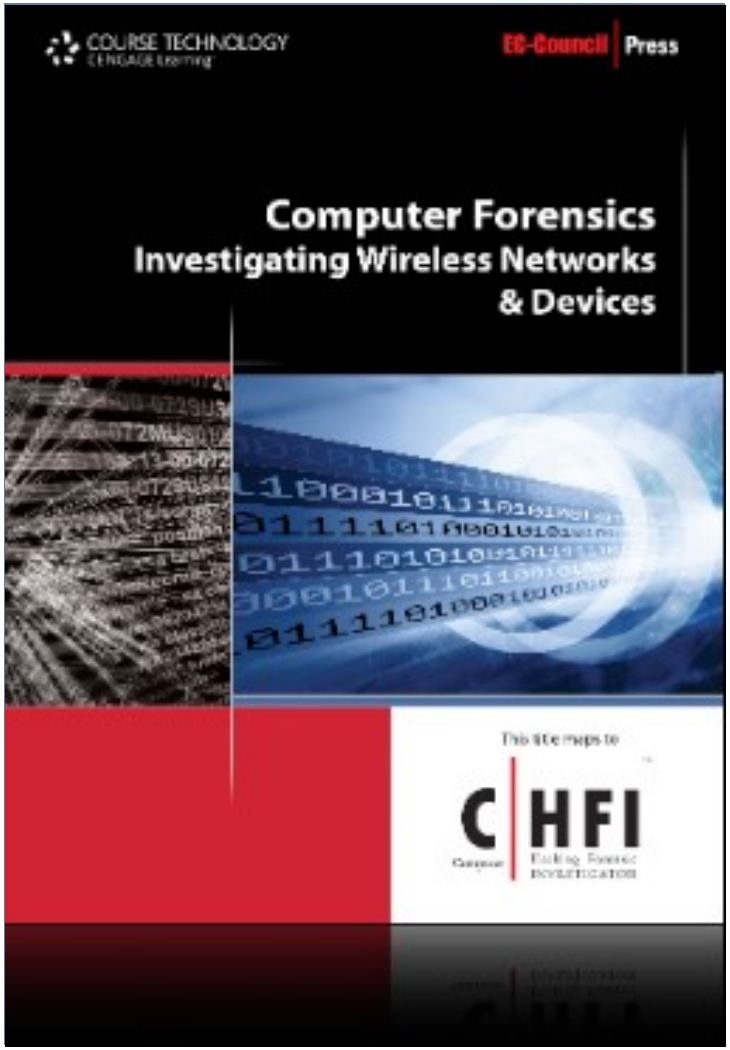
Ethical Hacking and Countermeasures (cont'd)



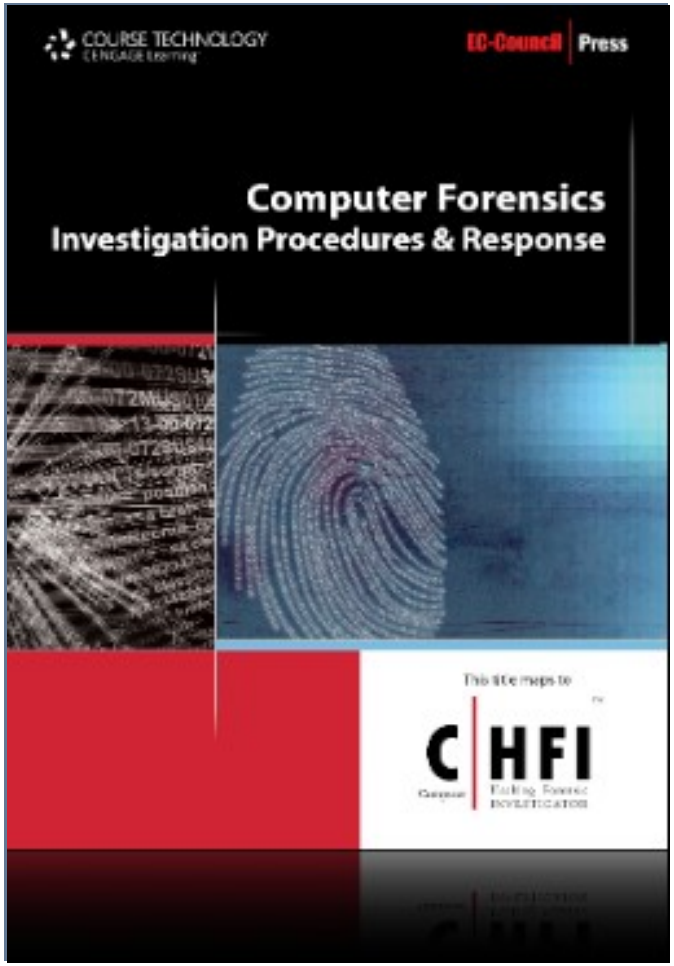


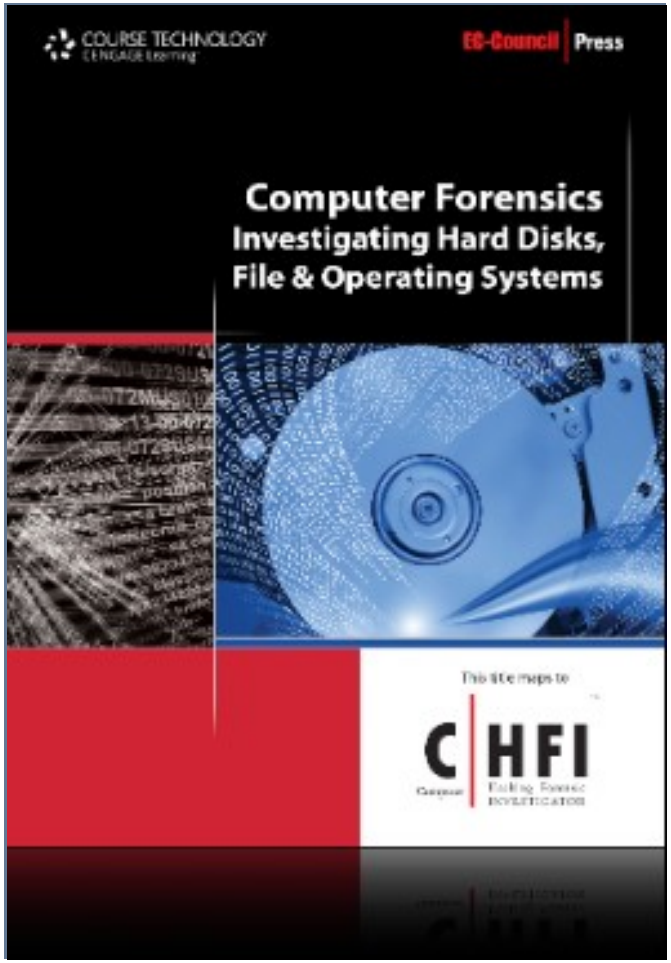
Computer Forensics

- Computer forensics enables the systematic and careful identification of evidence in computer related crime and abuse cases
- This may range from tracing the tracks of a hacker through a client's systems
- To tracing the originator of defamatory emails, to recovering signs of fraud.
- The CHFI course will provide participants the necessary skills to identify an intruder's footprints

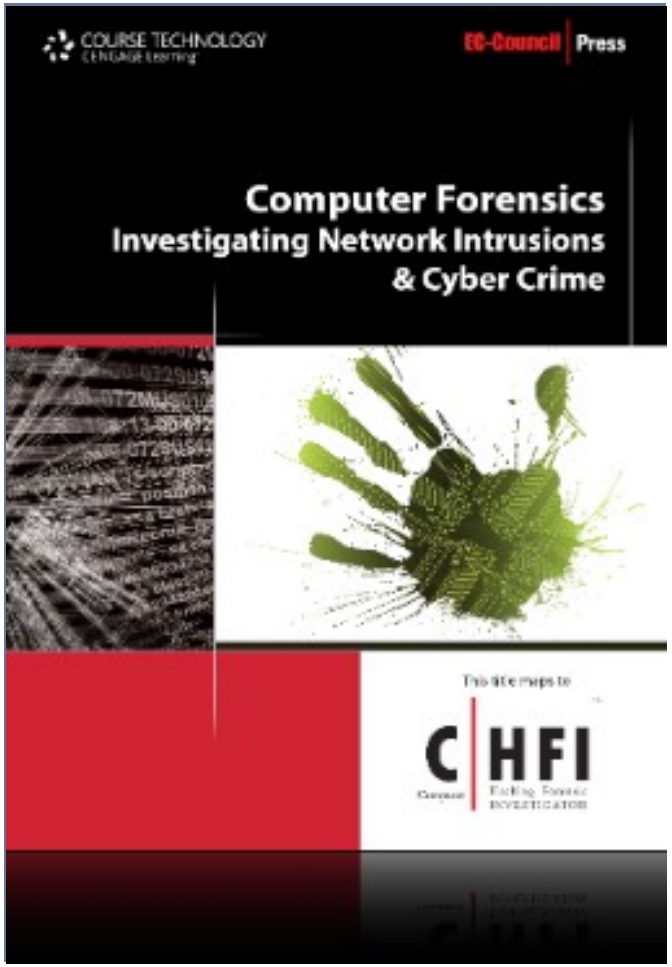


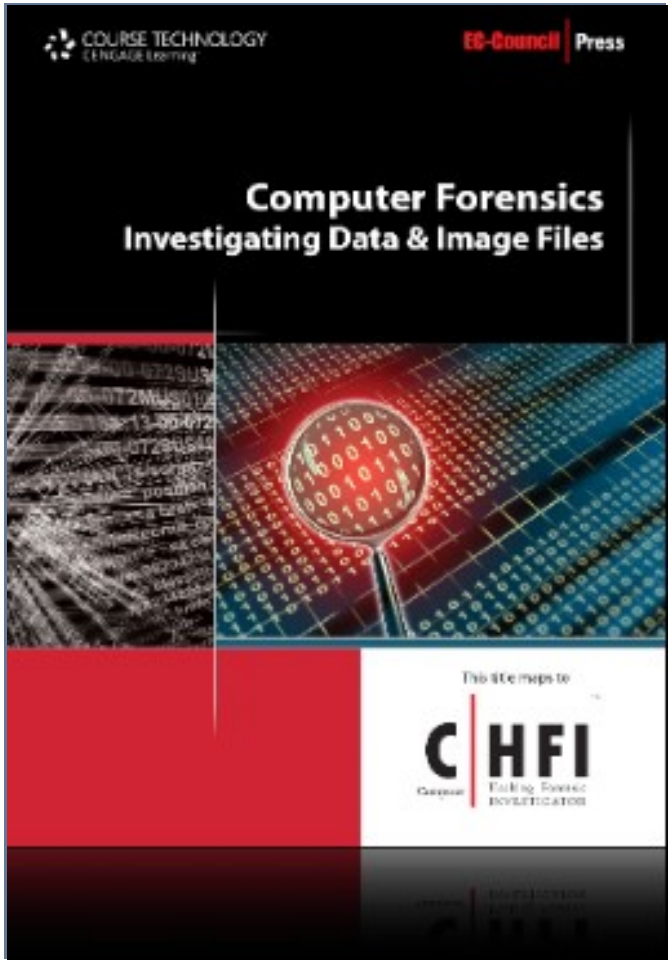
Computer Forensics (cont'd)





Computer Forensics (cont'd)





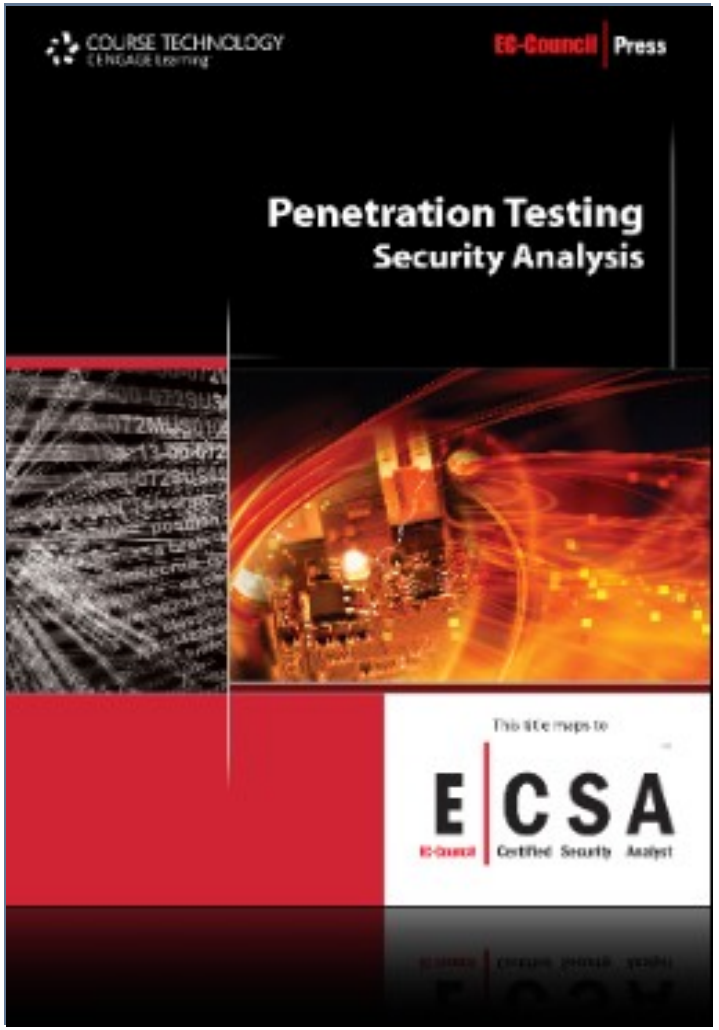
Penetration Testing

EC-Council Certified Security Analyst (ECSA) complements the Certified Ethical Hacker (CEH) certification by exploring the analytical phase of ethical hacking

ECSA takes it a step further by exploring how to analyze the outcome from these tools and technologies

Through groundbreaking penetration testing methods and techniques, ECSA class helps students perform the intensive assessments

This makes ECSA a relevant milestone towards achieving EC-Council's Licensed penetration Tester

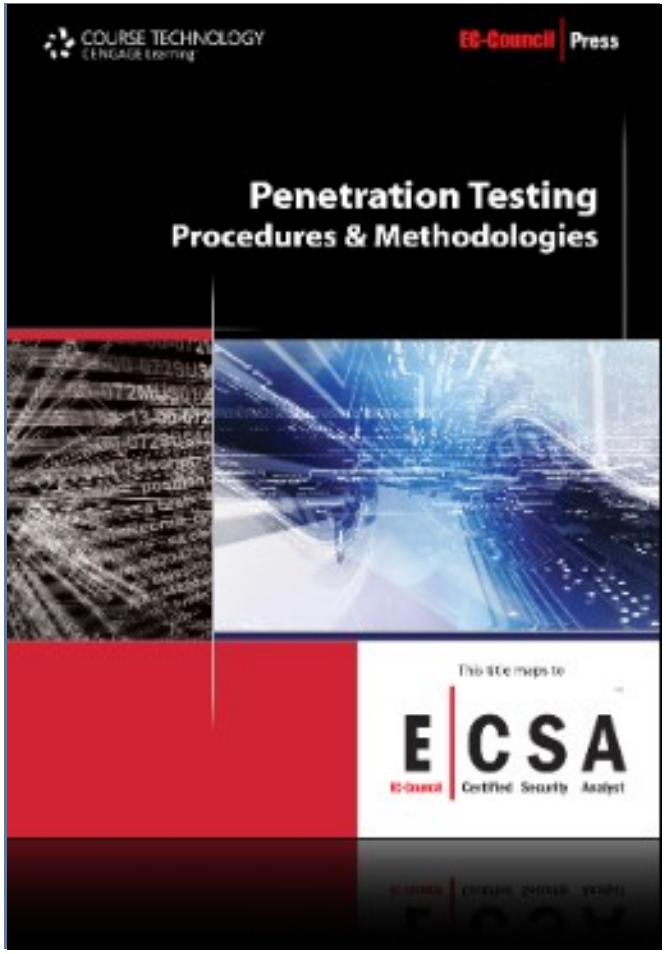


Penetration Testing (cont'd)

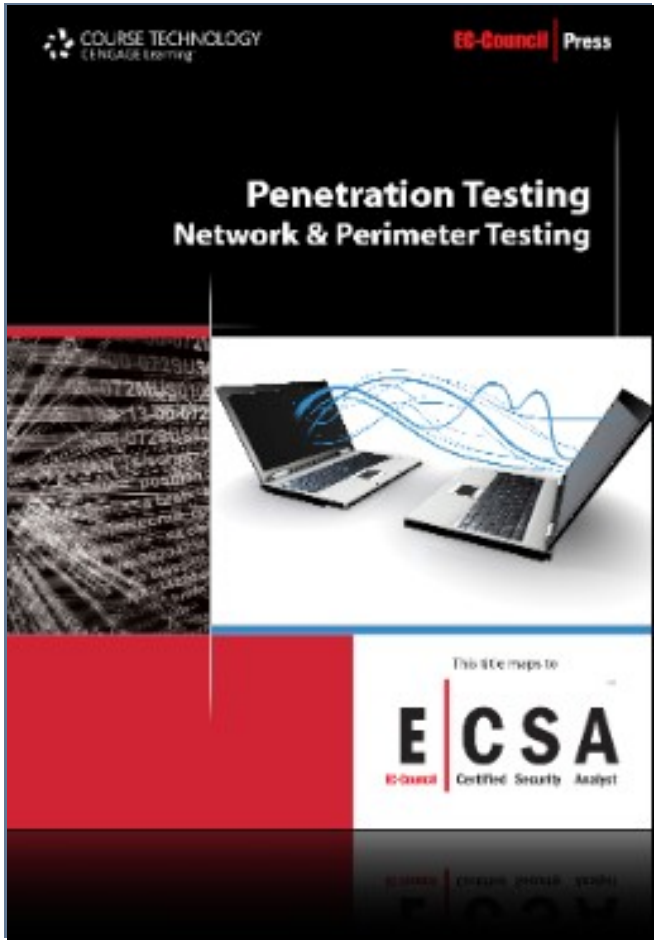
The Licensed Penetration Tester standardizes the knowledge base for penetration testing professionals by incorporating the best practices followed by experienced experts in the field

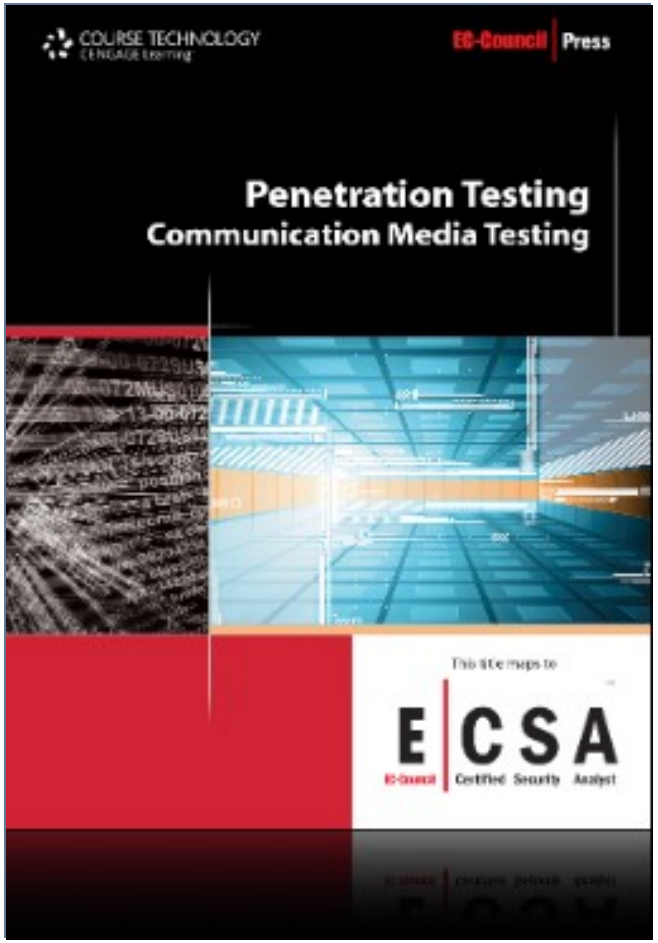
The objective of EC-Council Certified Security Analyst is to add value to experienced security professionals by helping them analyze the outcomes of their tests

ECSA leads the learner into the advanced stages of ethical hacking

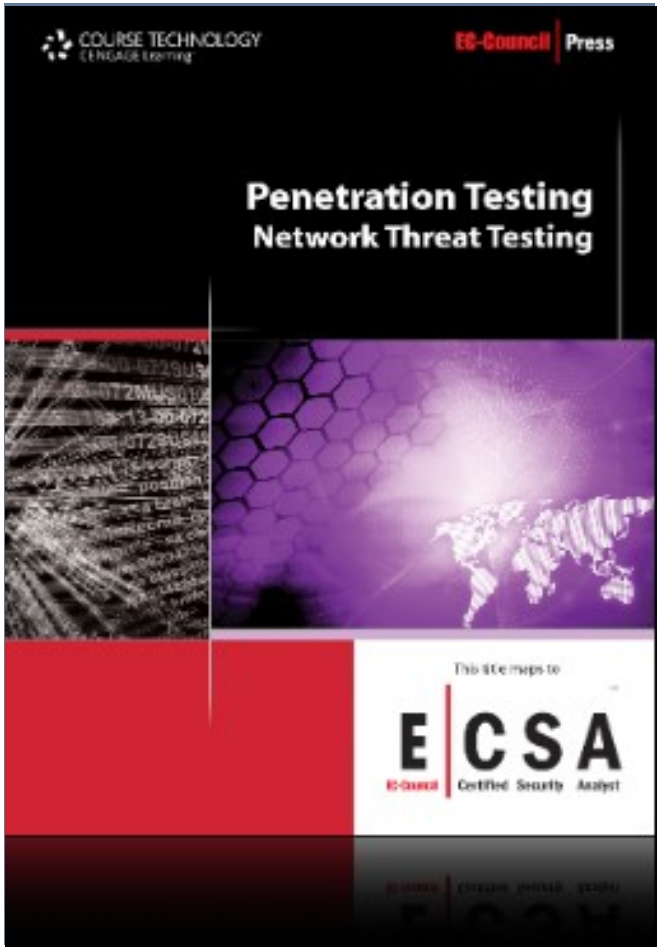


Penetration Testing (cont'd)





Penetration Testing (cont'd)



Disaster Recovery

The EDRP course teaches you the methods in identifying vulnerabilities and takes appropriate countermeasures to prevent and mitigate failure risks for an organization

It also provides the networking professional with a foundation in disaster recovery principles, including preparation of a disaster recovery plan, assessment of risks in the enterprise, development of policies, and procedures

Understanding of the roles and relationships of various members of an organization, implementation of the plan, and recovering from a disaster

This EDRP course takes an enterprise-wide approach to developing a disaster recovery plan

Students will learn how to create a secure network by putting policies and procedures in place, and how to restore a network in the event of a disaster

Disaster Recovery (cont'd)

The EC-Council Disaster Recovery and Virtualization Technology certification will fortify the virtualization technology knowledge of system administrators, systems engineers, enterprise system architects, hardware engineers, software engineers, technical support individuals, networking professionals, and any IT professional who is concerned about the integrity of the network infrastructure

This is an advanced course for experienced system administrators and system integrators scaling their organization's deployment of the virtualization technologies. The ECDR-ECVT Program certifies individuals and explores installation, configuration, and management of different virtualization products

Thank You!

You can reach me at steve.graham@eccouncil.org