Business and Technical Logistics for Pen Testing

Overview

What is a Penetration Test

Statistics and Costs

Recent Examples

What is the Evolving Threat

Vulnerability time line

Exploit Code Life Cycle

What are Zombies and Botnets

Various Penetration Tests

The Penetration Test Methodology

Tools or Techniques

Tools and Website Resources

Seven Management Errors

What to Expect in 2009

Review and Case Study

What is a Penetration Test

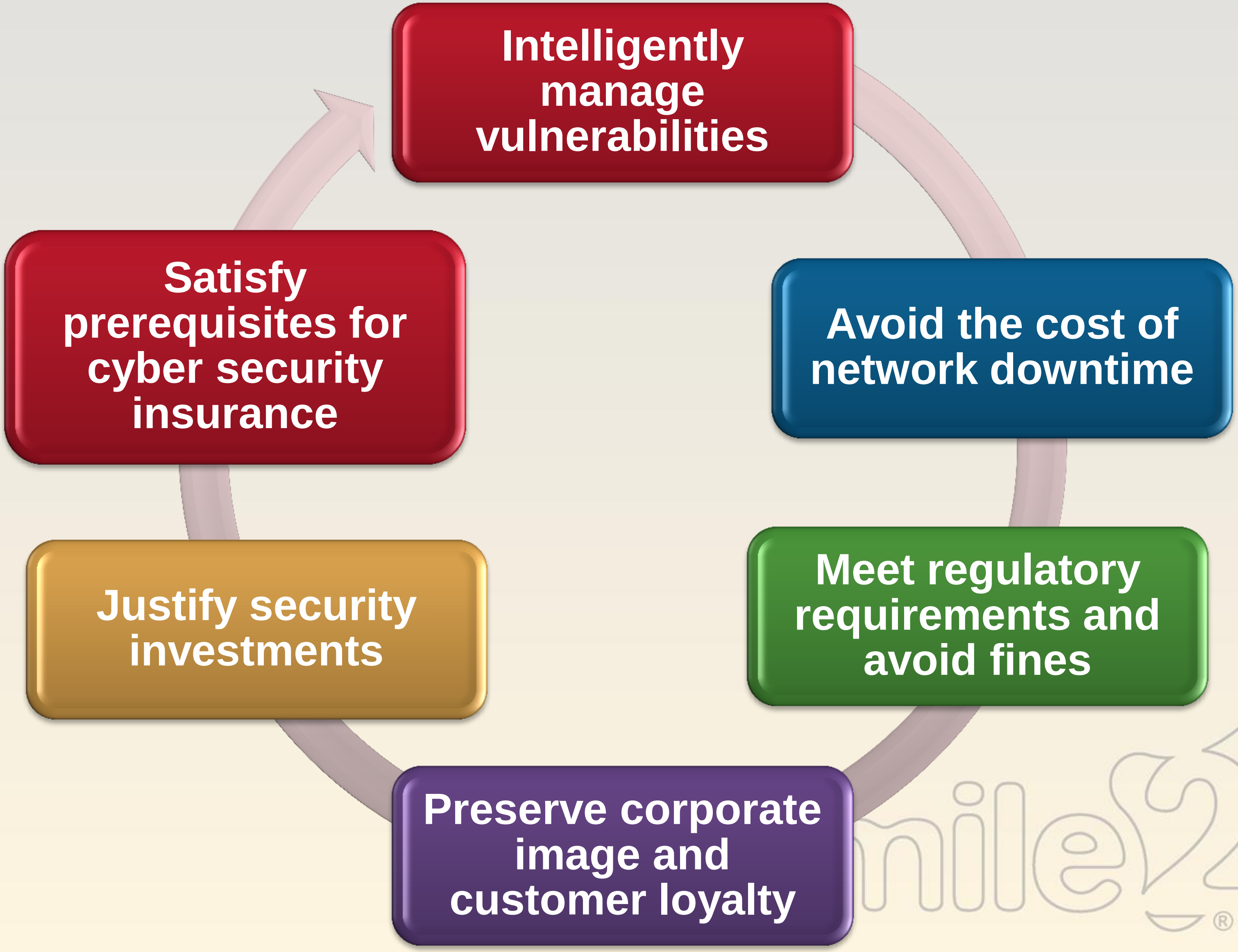
A penetration test is a method of evaluating the vulnerabilities of a computer system or network by simulating a malicious attack using current exploits, through Social Engineering, or physical attacks.

The basic process involves a diligent analysis of the target system for any weaknesses, technical flaws or vulnerabilities.

The analysis is carried out as if you are the potential attacker and can involve active exploitation of security vulnerabilities through electronic or physical means.

For a full definition Ref: http://en.wikipedia.org/wiki/Penetration_testing

Benefits of a Penetration Test



Intelligently manage vulnerabilities

Avoid the cost of network downtime

Meet regulatory requirements and avoid fines

Preserve corporate image and customer loyalty

Justify security investments

Satisfy prerequisites for cyber security insurance

Data Breach Insurance

There are growing numbers of compliance requirements and state laws mandating security breach disclosure, the costs of a security failure are becoming more evident.

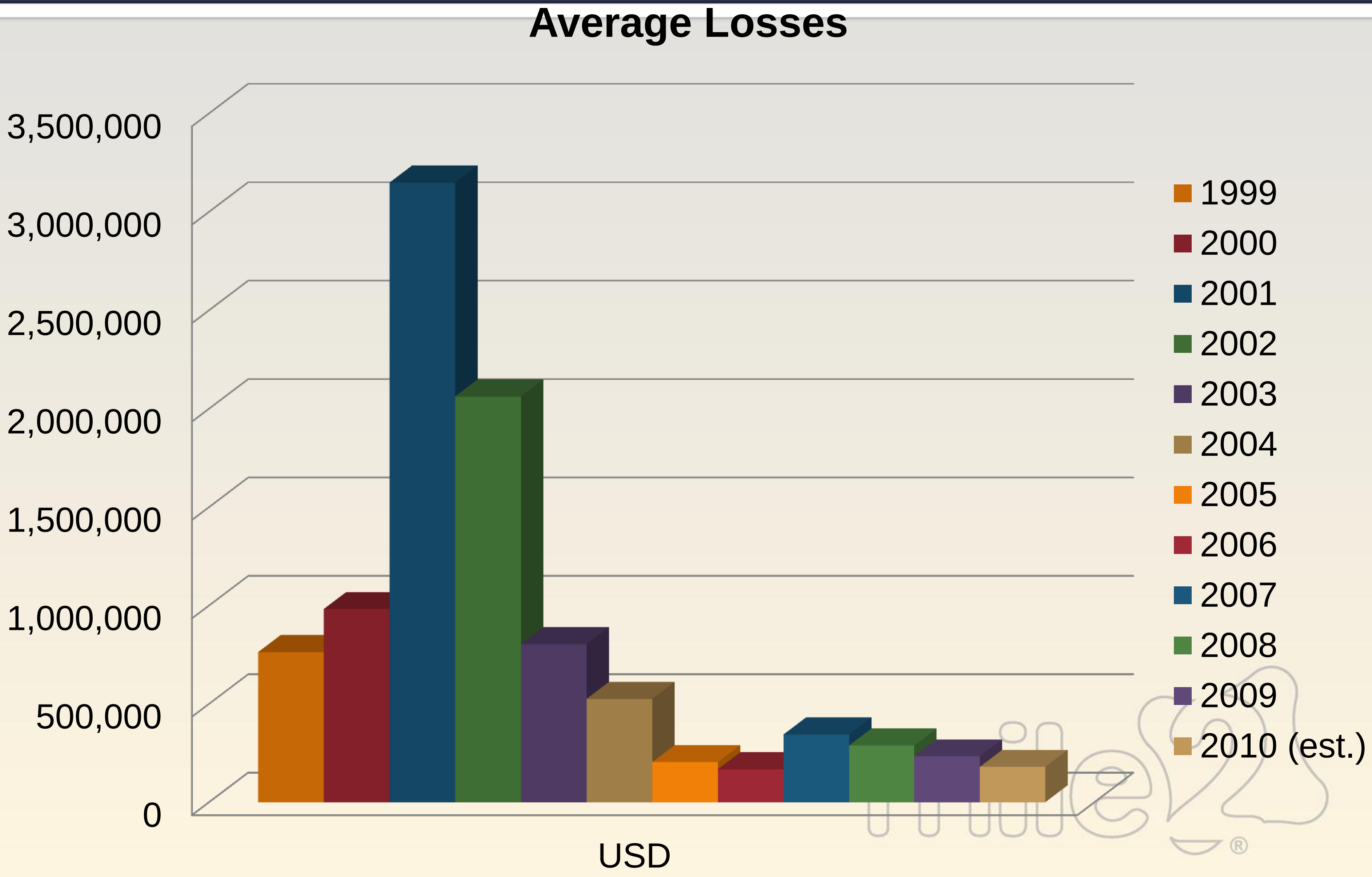
Currently, there are 11 carriers offering cyber-related insurance plans and many brokers that handle their business. (Feb. 2007)

In a study, Gartner found that many IT people believed security issues were covered by riders in their business insurance policies, only to find out later that they weren't.

For an annual premium ($1,500-$100,000+) enterprises can buy policies that will reimburse them in the event of unauthorized system access, stored data losses, customer privacy violations, cyber extortion, and cyber terrorism

There are a wide variety of cyber-related insurance coverage options, and most of them don't compare on an apples-to-apples basis.

CSI Computer Crime Survey



Recent Attacks & Security Breaches

darkreading.com

- click on: Attacks/Breaches

computerworld.com/securitytopics/security

asert.arbornetworks.com

securitynewsportal.com

scmagazineus.com

What does a Hack cost you?

After an industry-wide hunt, let us tell you:
There is no single, definitive figure on the cost of security incidents.

In cases where stolen IDs and passwords were used, the average loss per incident was $1.5 million. Some caused as much as $10 million.

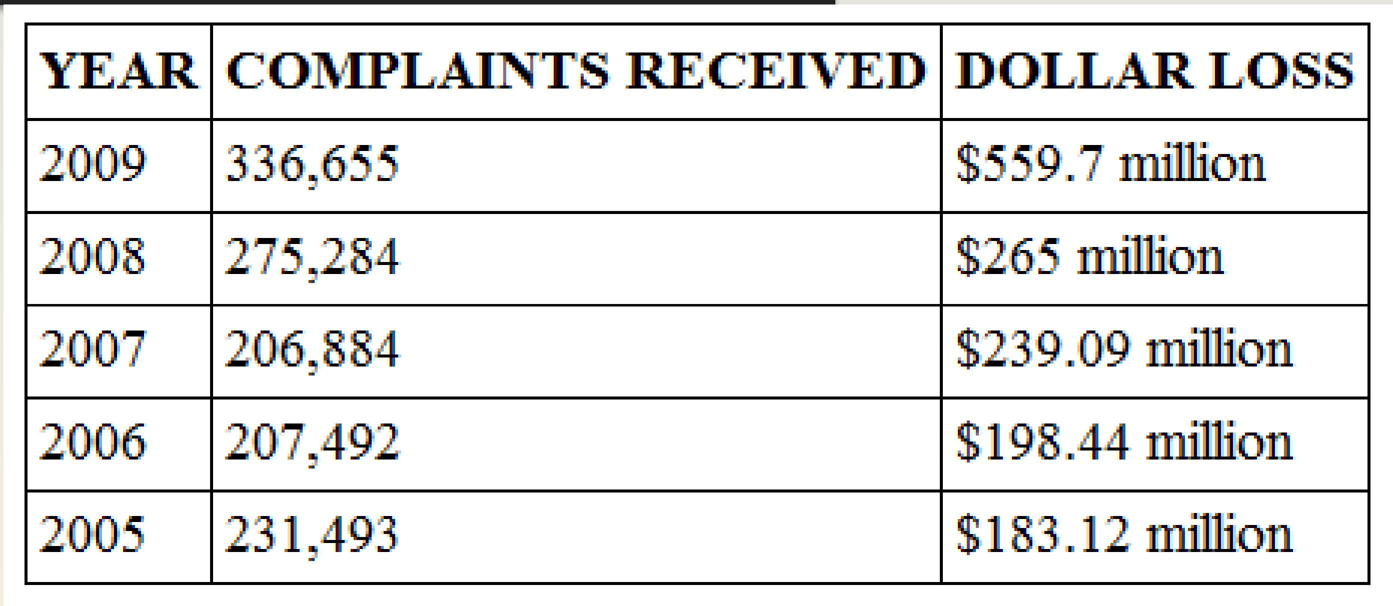
Companies lost an average of $14 million per breach/incident when customer data losses were incurred. The cost was as much as $50 million.

A recent survey by the Yankee Group indicates that more than half of companies rate their Internet downtime costs at more than $1,000 per hour.

Some rules of thumb say that $100,000 is a good starting point when measuring average loss per incident.

Internet Crime Complaint Center

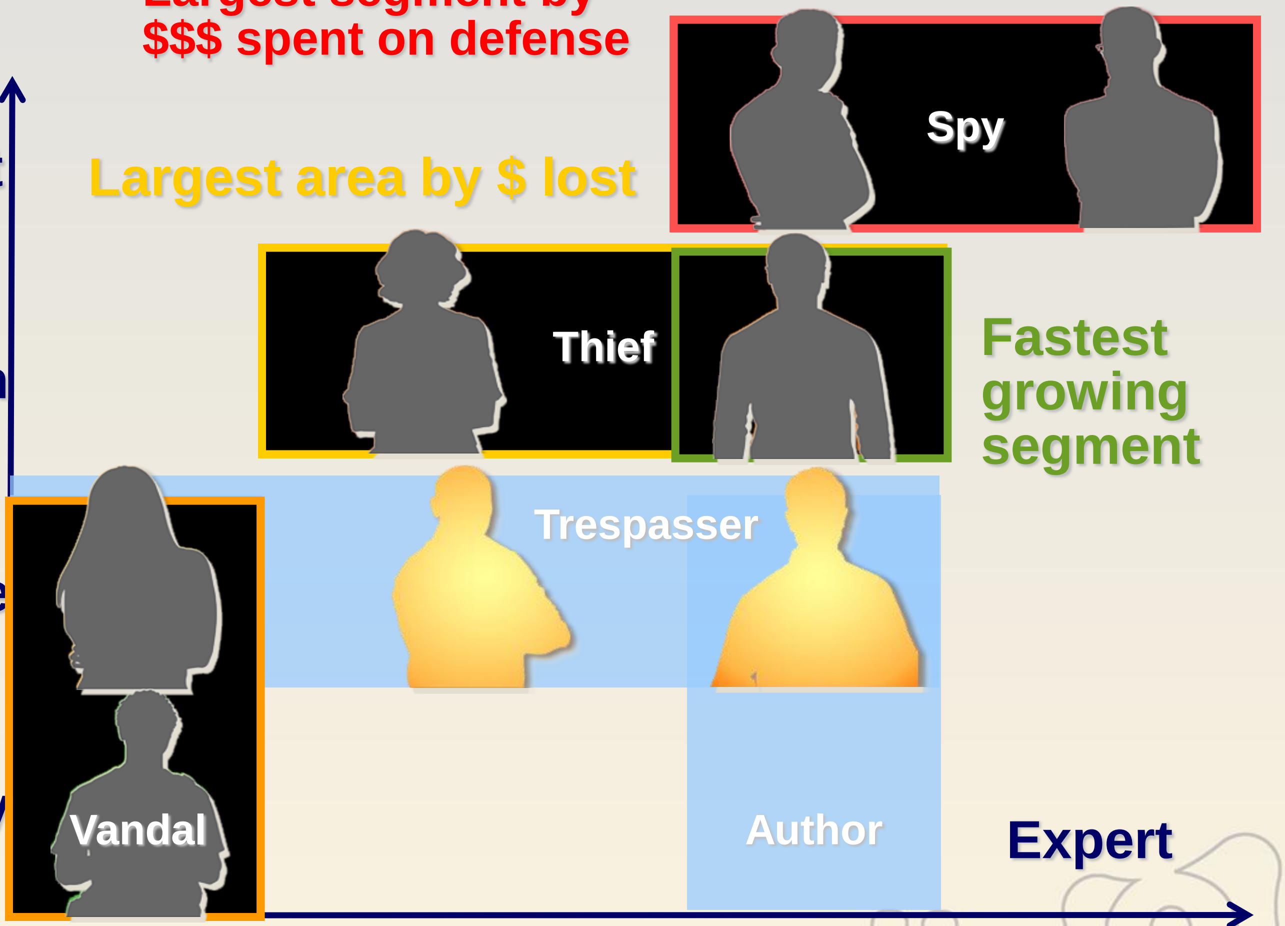
2009 annual report.



YEAR	COMPLAINTS RECEIVED	DOLLAR LOSS
2009	336,655	$559.7 million
2008	275,284	$265 million
2007	206,884	$239.09 million
2006	207,492	$198.44 million
2005	231,493	$183.12 million

The vast majority of cases were fraudulent in nature and involved a financial loss on the part of the complainant.

The Evolving Threat



Largest segment by $$$ spent on defense

National Interest

Spy

Largest area by $ lost

Personal Gain

Thief

Fastest growing segment

Personal Fame

Trespasser

Largest area by volume

Curiosity

Vandal

Author

Expert

Script-Kiddie

Hobbyist Hacker

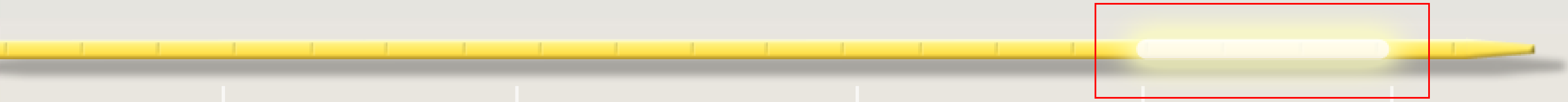
Specialist

***Slide Source: IT Forum 04**: Jesper Johansson*
Security Solutions Engineer
jesperjo@microsoft.com

Steve Riley
Senior Program Manager
steriley@microsoft.com

Security Vulnerability Life Cycle

Most attacks occur here



Product ship

Vulnerability discovered

Component modified

Patch released

Patch deployed at customer site

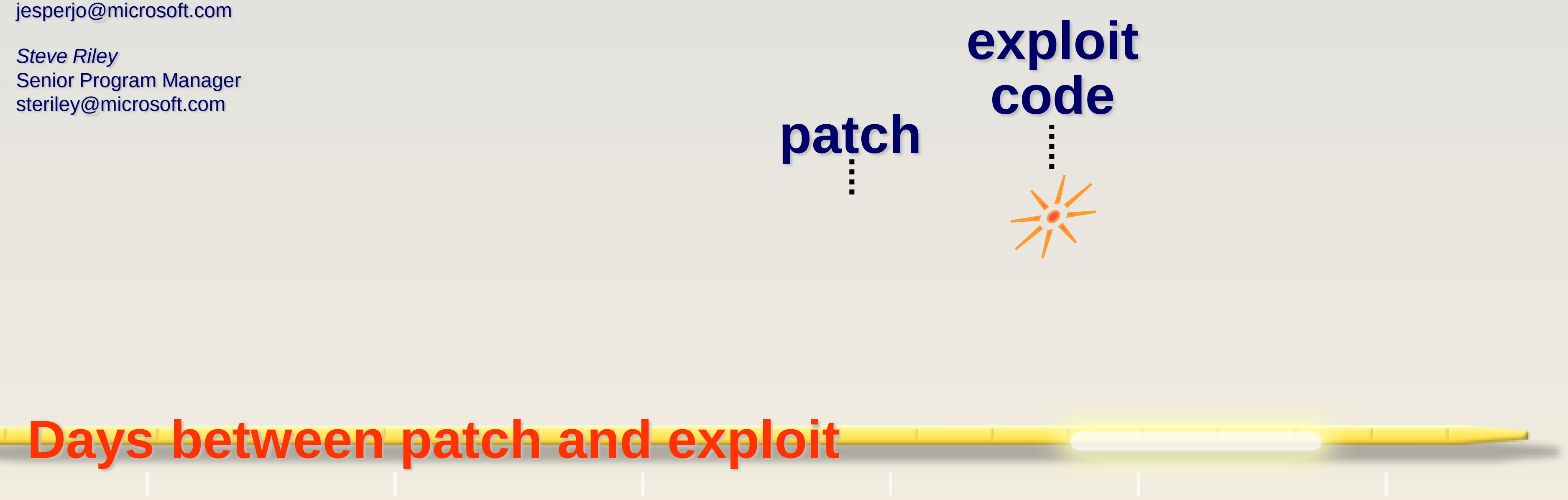
Slide Source: IT Forum 04: *Jesper Johansson*
Security Solutions Engineer
jesperjo@microsoft.com

Steve Riley
Senior Program Manager
steriley@microsoft.com

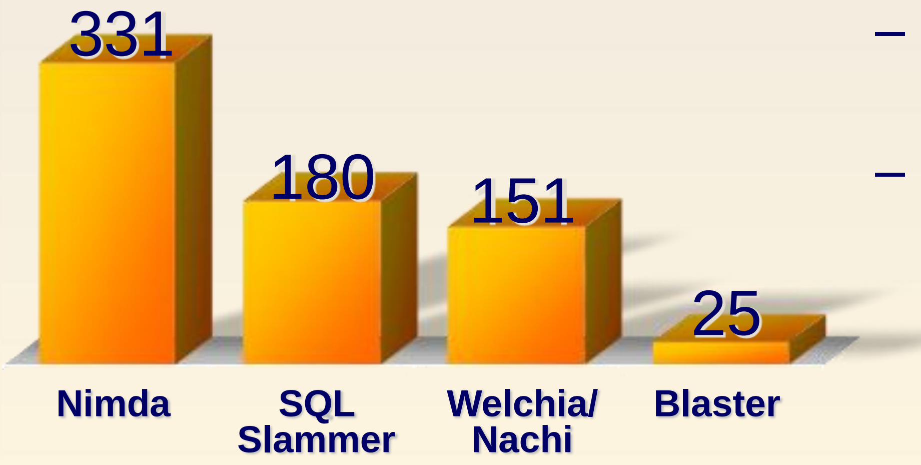
Exploit Timeline

Slide Source: IT Forum 04*: Jesper Johansson*
Security Solutions Engineer
jesperjo@microsoft.com

Steve Riley
Senior Program Manager
steriley@microsoft.com



Days between patch and exploit



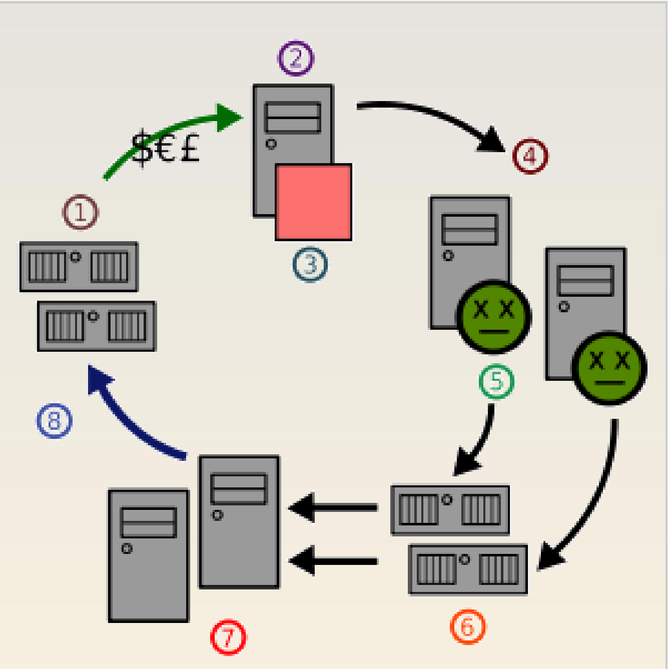
- The average is now 2 hours for a patch to be reverse-engineered
- As this cycle keeps getting shorter, patching is a less effective defense in large organizations

Zombie Definition

A zombie is a computer attached to the Internet that has been compromised by a hacker, a computer virus, or a Trojan horse.

Generally, a compromised machine is only one of many in a botnet, and will be used to perform malicious tasks of one sort or another under remote direction.

Most owners of zombie computers are unaware that their system is being used in this way. Because the owner tends to be unaware, these computers are metaphorically compared to zombies.



(1) Spammer's web site (2) Spammer (3) Spamware (4) Infected computers (5) Virus or trojan (6) Mail servers (7) Users (8) Web traffic

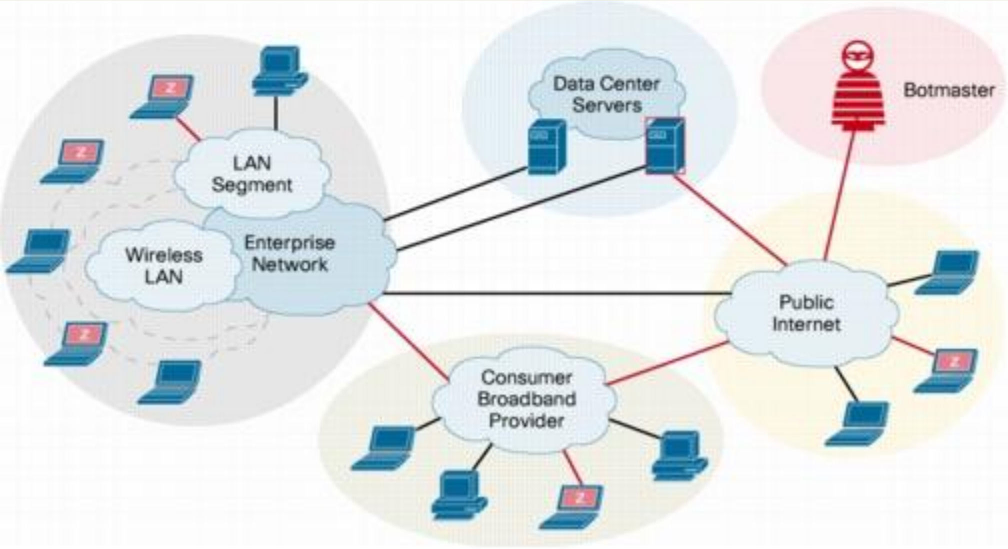
What is a Botnet?

A botnet is a collection of computers, connected to the internet, that interact to accomplish some distributed task.

Although such a collection of computers can be used for useful and constructive applications, the term botnet typically refers to such a system designed and used for illegal purposes.

Such systems are composed of compromised machines that are assimilated without their owner's knowledge.

The compromised machines are referred to as drones or zombies, while the malicious software running on them as 'bot'. The collection is known as a botnet or a zombie army.

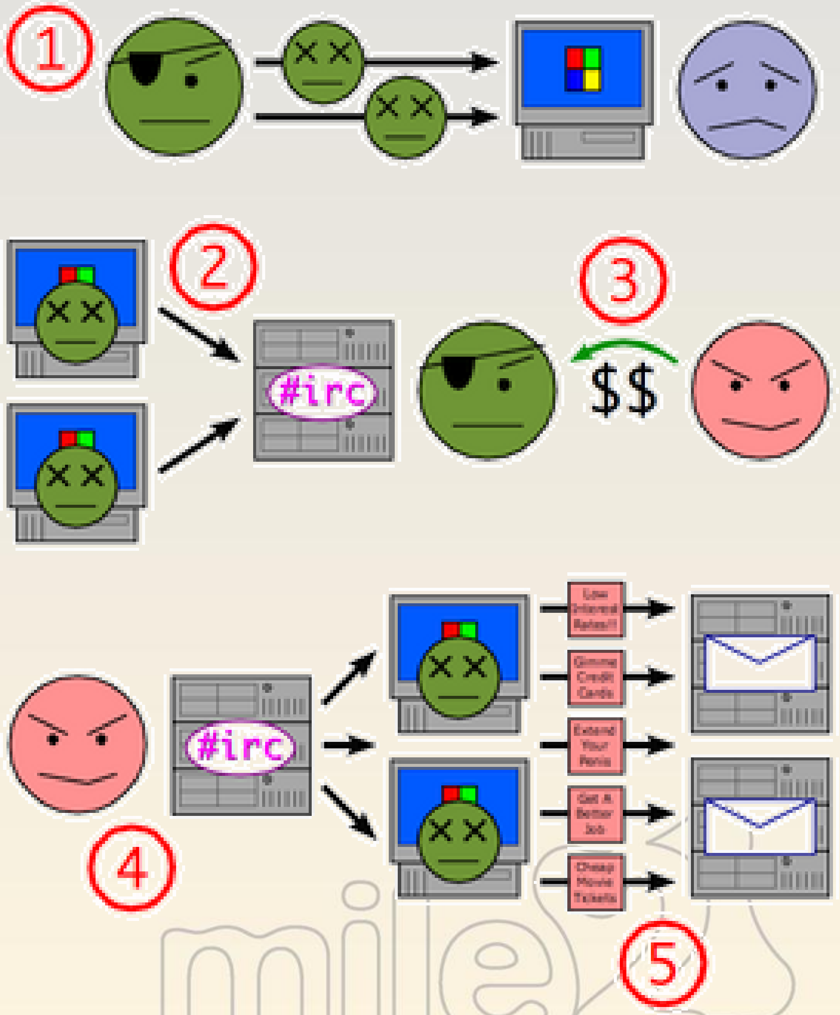


How is a Botnet Formed?

For a botnet to form and grow, it must accumulate drones, and each drone must be individually exploited, infected, and assimilated into the botnet.

For this reason, most bot software contains spreaders that automate the task of scanning ip addresses for vulnerable software holes.

Once found, the vulnerable machines are attacked and infected with the bot software, and the pattern continues.



Botnet Statistics

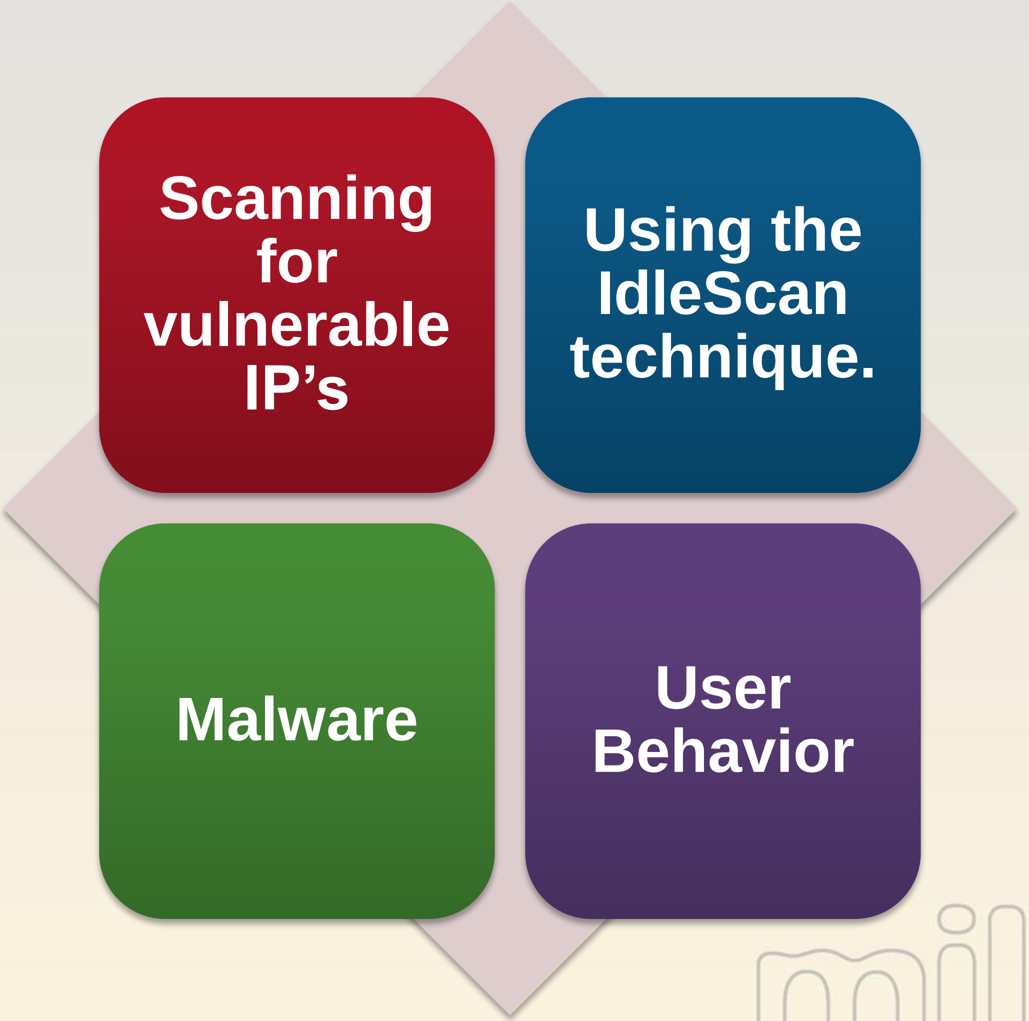
shadowserver

An all volunteer watchdog group of security professionals that gather, track, and report on malware, botnet activity, and electronic fraud. It is the mission of the Shadowserver Foundation to improve the security of the Internet by raising awareness of the presence of compromised servers, malicious attackers, and the spread of malware.

- Capturing and receiving malicious software, or information related to compromised devices
- Disassembling, sandboxing, and analyzing viruses and trojans
- Monitoring and reporting on malicious attackers
- Tracking and reporting on botnet activities
- Disseminating cyber threat information
- Coordinating incident response

The Shadowserver Foundation works alongside other security agencies to develop strategies against the threats and to form action plans to help mitigate the threats as they develop.

How are Botnet’s Growing?



Scanning for vulnerable IP’s

Using the IdleScan technique.

Malware

User Behavior

Types of Penetration Testing

Black box testing assumes no prior knowledge of the infrastructure to be tested. The testers must first determine the location and extent of the systems before commencing their analysis.

Black box testing is useful in the cases where the tester assumes the role of an outside hacker and tries to intrude into the system without adequate knowledge of the system.

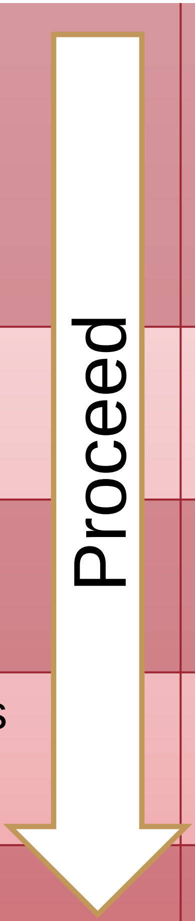
At the other end of the spectrum is white box testing. White box testing provides the tester with complete knowledge of the infrastructure to be tested, often including network diagrams, source code and IP addressing information. This assumes the role of a inside threat.

There are also several variations in between, often known as "Gray Box Testing".

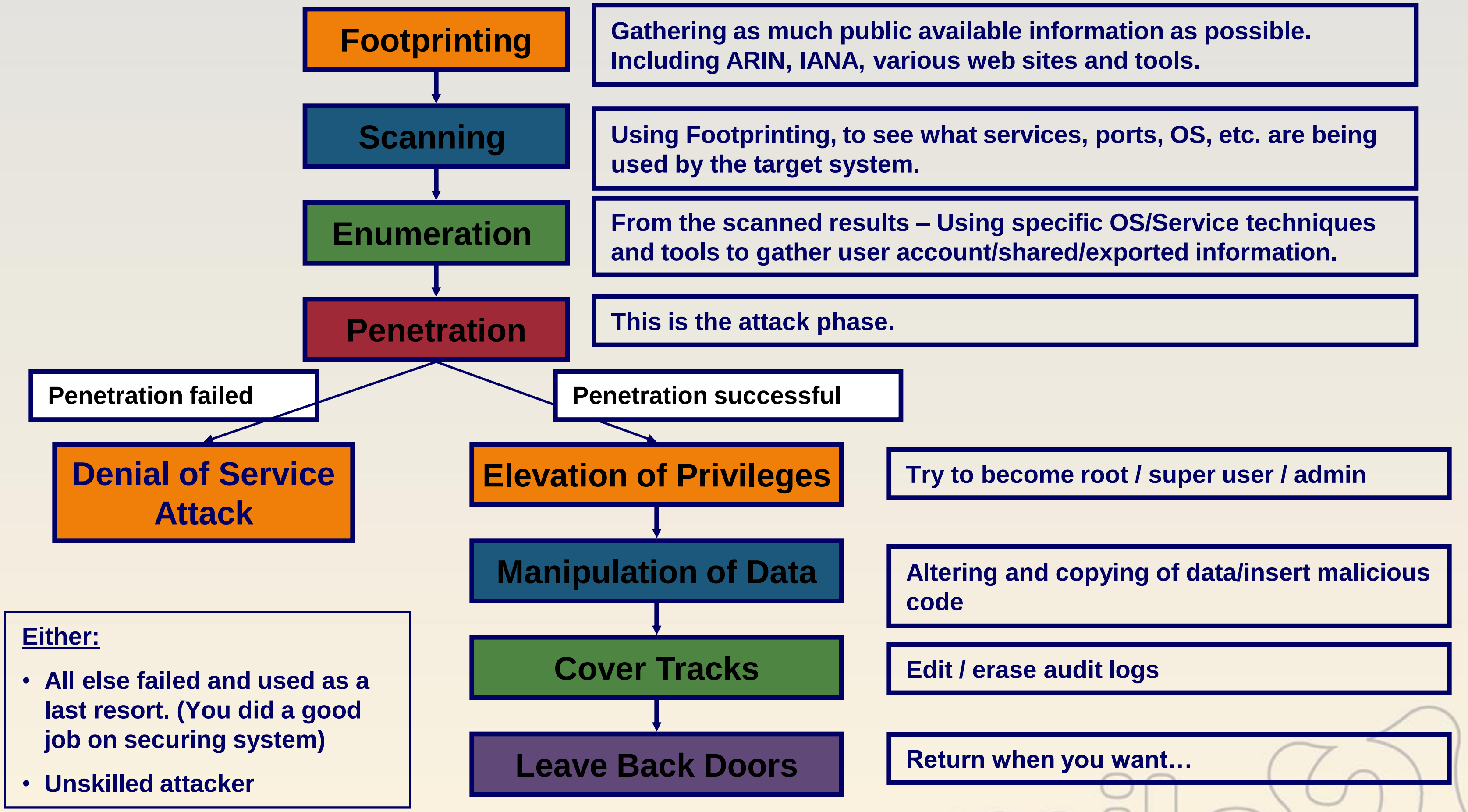
Ref: http://en.wikipedia.org/wiki/Penetration_testing

Hacking Methodology

Step in Attack	Explanation	Example
Reconnaissance	Intelligence work of obtaining information, either passively or actively.	Passively – Sniffing traffic, eavesdropping. Actively – ARIN and Whois databases, examining website HTML code, Social Engineering.
Scanning	Identifying systems that are running and the services active on them.	Ping sweeps and port scans.
Gaining Access	Exploiting identifiable vulnerabilities to gain unauthorized access.	Exploiting a buffer overflow or brute forcing a password and logging onto a system.
Maintaining Access	Uploading malicious software to ensure reentry is possible.	Installing a Trojan Horse that implements a backdoor on a system.
Covering Tracks	Carrying our activities to hide one's malicious activities.	Deleting or modifying data in system and application logs.



Methodology for Penetration Testing



Footprinting

Gathering as much public available information as possible. Including ARIN, IANA, various web sites and tools.

Scanning

Using Footprinting, to see what services, ports, OS, etc. are being used by the target system.

Enumeration

From the scanned results – Using specific OS/Service techniques and tools to gather user account/shared/exported information.

Penetration

This is the attack phase.

Penetration failed

Denial of Service Attack

Either:

- All else failed and used as a last resort. (You did a good job on securing system)
- Unskilled attacker

Penetration successful

Elevation of Privileges

Try to become root / super user / admin

Manipulation of Data

Altering and copying of data/insert malicious code

Cover Tracks

Edit / erase audit logs

Leave Back Doors

Return when you want…

Penetration Testing Methodologies

Open Source Security Testing Methodology Manual (OSSTMM)

- http://www.isecom.org/

NIST National Institute of Standards and Technology (SP 800-42) Guideline on Network Security Testing

- http://csrc.ncsl.nist.gov/publications/nistpubs/index.html

Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination

- http://www.ffiec.gov/ffiecinfobase/index.html
  - Information Security Booklet

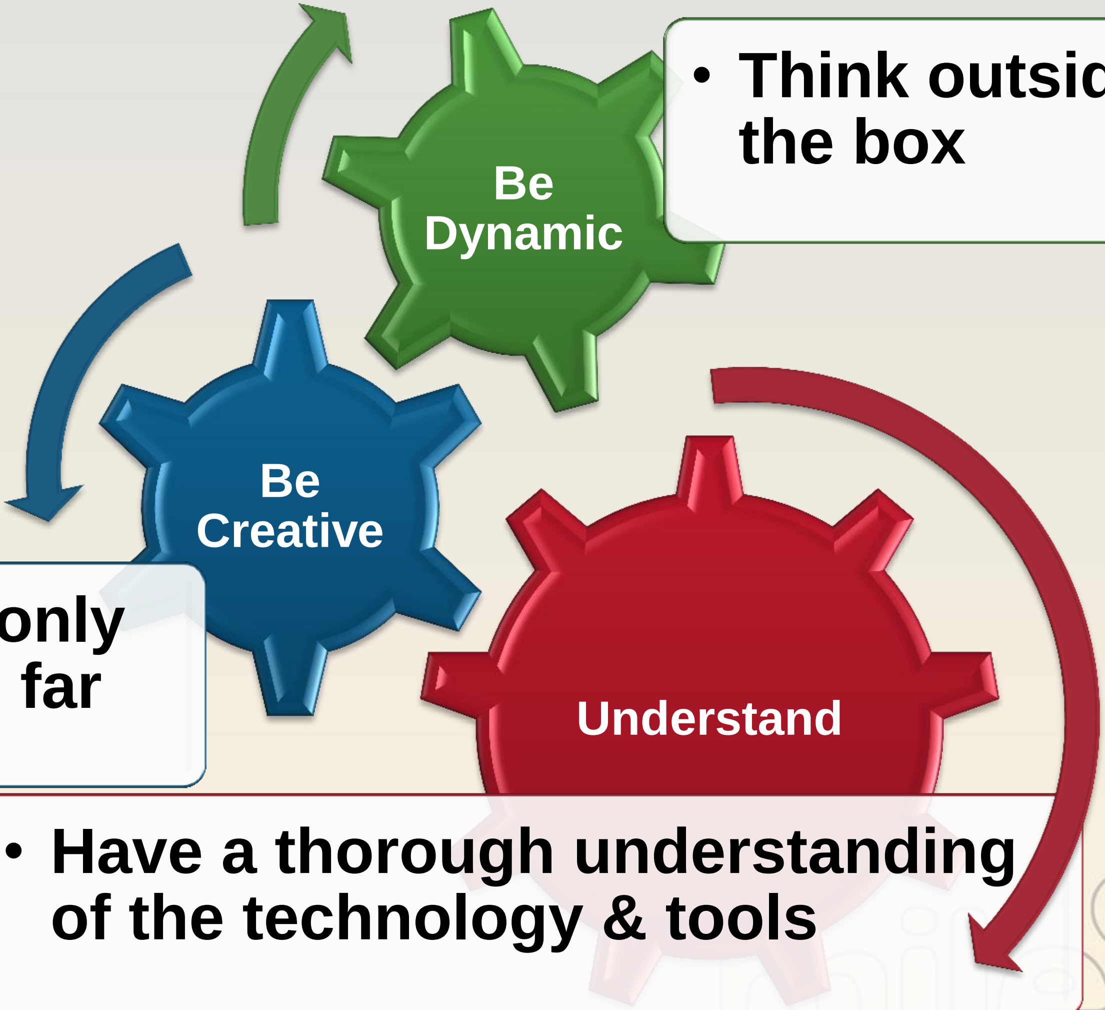
Information Systems Security Assessment Framework (ISSAF)

- http://www.oissg.org/

Hacker vs. Penetration Tester

Hacker	Penetration Tester
No Code of Ethics/Motivated by Greed, Cause, or Fame	Follows a Strict Code of Ethics
Gains Illegal Entry/Unauthorized	Legal Entry/Must have authorization
Will try any technique without regard to loss	Defined set of boundaries
Tries to bypass logging	Log/Records all activity
No report/shares exploits	Present a detailed report of test
Exploits vulnerabilities	Tries to correct vulnerabilities
Bad Guy/Black Hats	Good Guy/White Hats

Not Just Tools

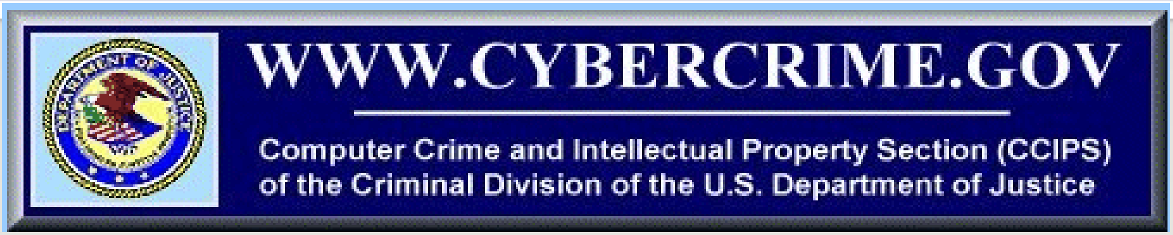


- Think outside the box

- Tools can only get you so far

- Have a thorough understanding of the technology & tools

Website Review



WWW.CYBERCRIME.GOV

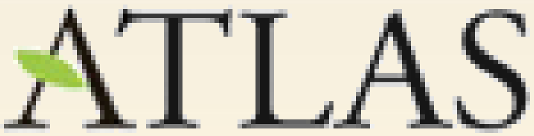
Computer Crime and Intellectual Property Section (CCIPS)
of the Criminal Division of the U.S. Department of Justice

COMPUTERWORLD An IDG company

Home | News | Topics | Print Edition | Services | Subscribe | Events | In Depth | XML Feeds

Management Careers Security Hardware Software Data Mgmt Networking Government Mobile Development Industry

SecurityWizardry.com



Website Review Con’t

http://www.darkreading.com/

SECURITY dark READING
Protect The Business Enable Access

http://www.scmagazine.com/

SC MAGAZINE

http://www.cesg.gov.uk/

http://www.astalavista.com/

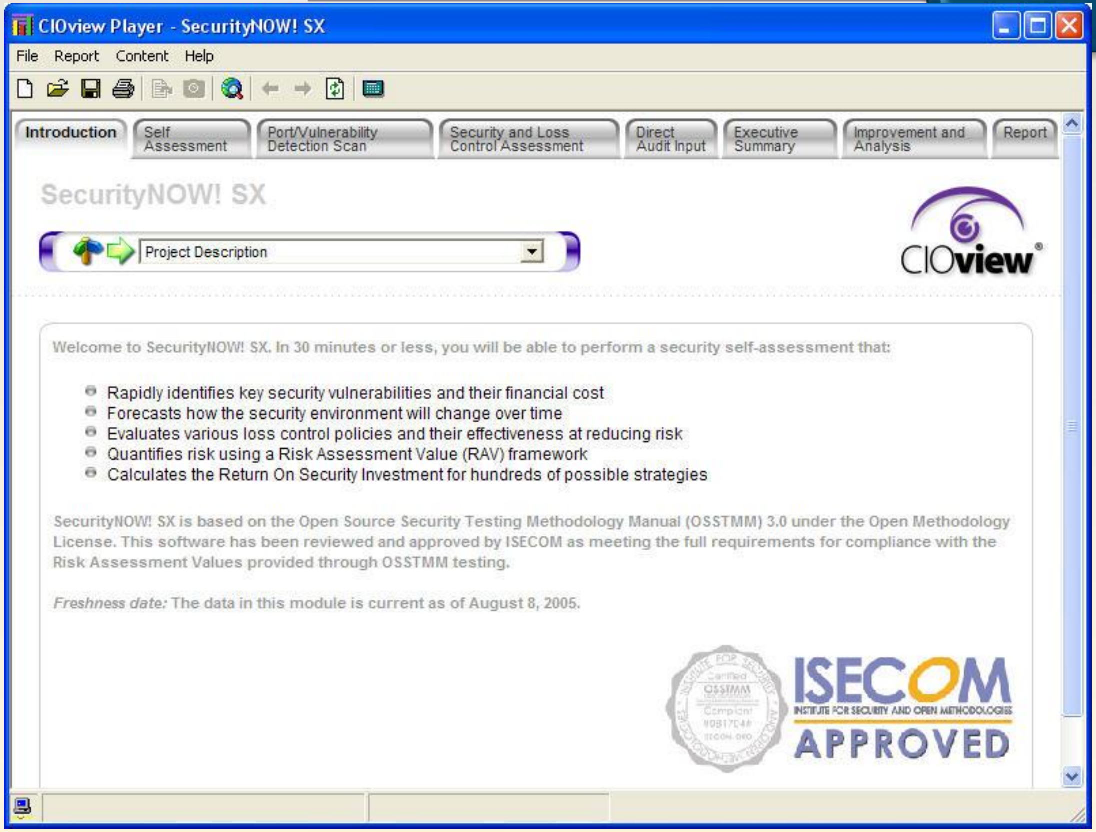
http://www.cve.mitre.org/

CVE
Common Vulnerabilities and Exposures
The Standard for Information Security Vulnerability Names

Tool: SecurityNOW! SX

www.cioview.com

CIOview Corp is the industry leader in validating the financial value proposition of specific IT solutions and creating financial assessment tools.



Welcome to SecurityNOW! SX. In 30 minutes or less, you will be able to perform a security self-assessment that:

- Rapidly identifies key security vulnerabilities and their financial cost
- Forecasts how the security environment will change over time
- Evaluates various loss control policies and their effectiveness at reducing risk
- Quantifies risk using a Risk Assessment Value (RAV) framework
- Calculates the Return On Security Investment for hundreds of possible strategies

SecurityNOW! SX is based on the Open Source Security Testing Methodology Manual (OSSTMM) 3.0 under the Open Methodology License. This software has been reviewed and approved by ISECOM as meeting the full requirements for compliance with the Risk Assessment Values provided through OSSTMM testing.

Freshness date: The data in this module is current as of August 8, 2005.

Seven Management Errors

From the SANS Institute:

There are seven management errors that lead to computer security vulnerabilities:

- Pretending the problem will go away.
- Authorizing reactive, short-term fixes so problems re-emerge rapidly.
- Failing to realize how much money their information and organizational reputations are worth.
- Relying primarily on a firewall and IDS.
- Failing to deal with the operational aspects of security: make a few fixes and then not allow the follow through necessary to ensure the problems stay fixed.
- Failing to understand the relationship of information security to the business problem; they understand physical security but do not see the consequences of poor information security.
- Assigning untrained people to maintain security and not providing the training or the time to make it possible to do the job.

Review

What is a Penetration Test

Statistics and Costs

Recent Examples

What is the Evolving Threat

Vulnerability time line

Exploit Code Life Cycle

What are Zombies and Botnets

Various Penetration Tests

The Penetration Test Methodology

Tools or Technique

Tools and Website Resources

Seven Management Errors

What to Expect in 2009

Review and Case Study

Lab Module 1
Getting Set Up