Ethical Hacking and Countermeasures

Version 6

Module XXVI

Penetration Testing

The Seattle Times
seattletimes.com

Sunday, November 4, 2007 - Page updated at 02:03 AM

"Ethical hackers" hired to act like the bad guys

By Shaheen Samavati
Newhouse News Service

With Social Security numbers, credit-card information and bank records making the move online, malicious hackers hold more power than ever.

Rapid changes in technology have made it tough for banks, retailers and other companies that store databases of consumer information to keep up with the latest Internet crime tactics.

For Cleveland-based Third Federal Savings & Loan, the solution was simple: It hired hackers to try to crack its Web site before any bad guys got the chance.

This business of "ethical hacking" or "penetration testing" has become commonplace among financial institutions and major corporations over the past six years. But increasingly, companies of all types and sizes are hiring security experts to act like the enemy.

"There's always been people breaking into Web sites," said Chris Wysopal, an expert in information security. "But now there's much more of a criminal element. It's gone almost commercial."

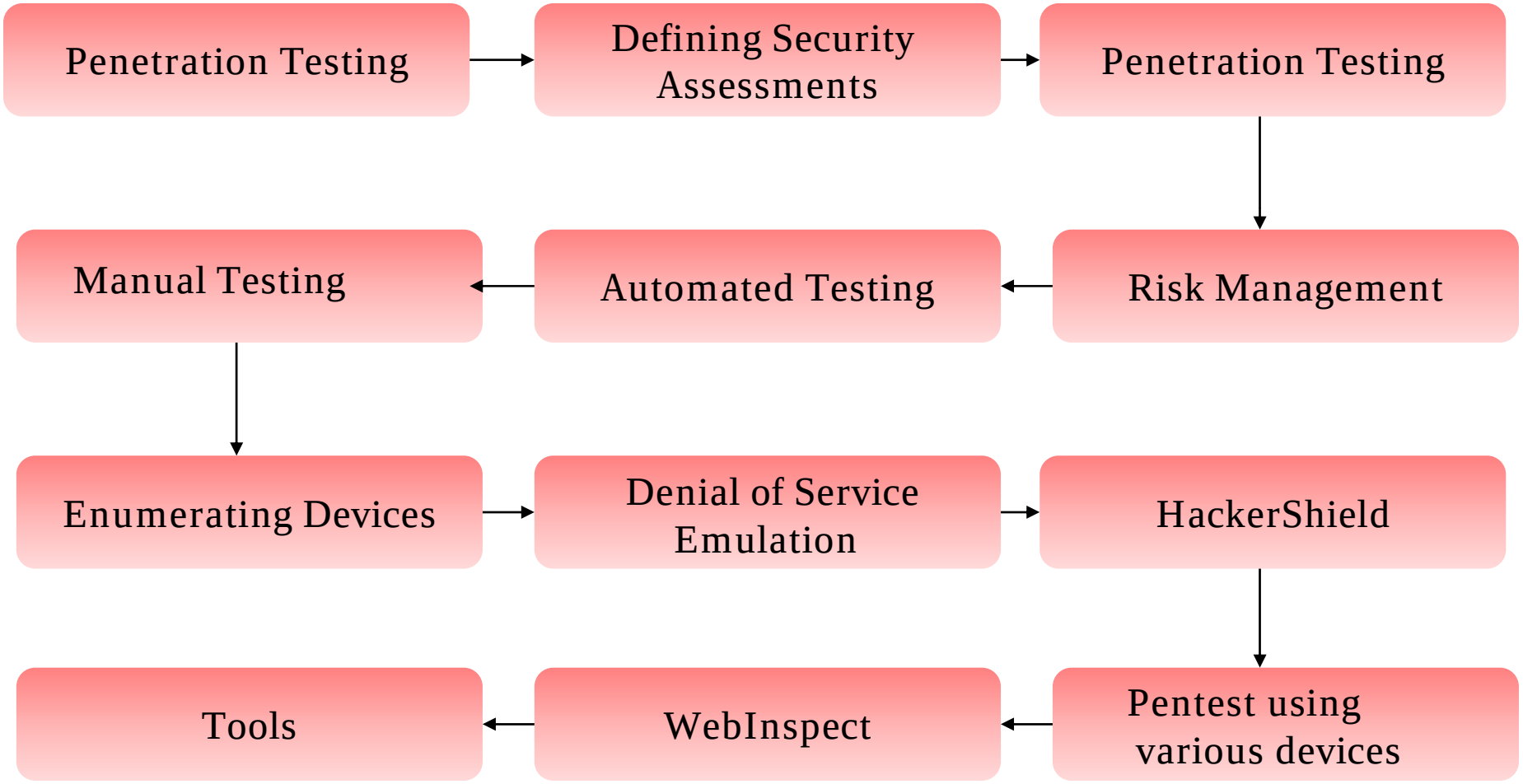
Source: *http://seattletimes.nwsource.com/*

Module Objective

This module will familiarize you with :

- Penetration Testing (PT)
- Security Assessments
- Risk Management
- Automated Testing
- Manual Testing
- Enumerating Devices
- Denial of Service Emulation
- HackerShield
- Pentest using various devices
- VigilENT
- WebInspect
- Tools

Module Flow



To Know more about Penetration Testing, Attend EC-Council's LPT Program

Introduction to PT

Most hackers follow a common approach when it comes to penetrating a system

In the context of penetration testing, the tester is limited by resources—namely time, skilled resources, and access to equipment—as outlined in the penetration testing agreement

A pentest simulates methods that intruders use to gain unauthorized access to an organization's networked systems and then compromise them

Categories of Security Assessments

Every organization uses different types of security assessments to validate the level of security on its network resources

Security assessment categories are security audits, vulnerability assessments, and penetration testing

Each type of security assessment requires that the people conducting the assessment have different skills

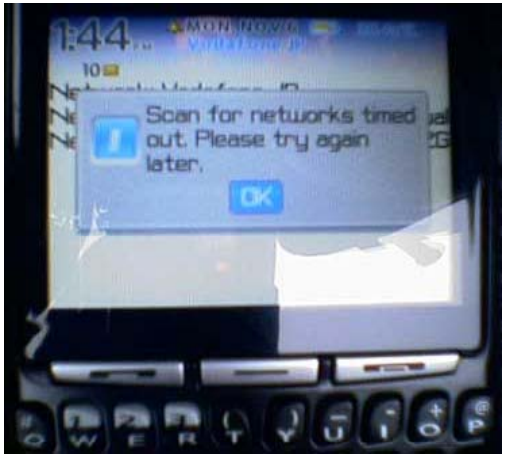
Vulnerability Assessment

Vulnerability assessment scans a network for known security weaknesses

Vulnerability scanning tools search network segments for IP-enabled devices and enumerate systems, operating systems, and applications

Vulnerability scanners can test systems and network devices for exposure to common attacks

Additionally, vulnerability scanners can identify common security configuration mistakes



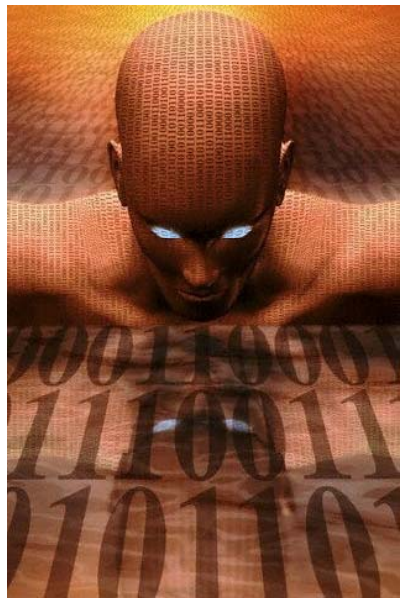
Limitations of Vulnerability Assessment

Vulnerability scanning software is limited in its ability to detect vulnerabilities at a given point in time

Vulnerability scanning software must be updated when new vulnerabilities are discovered or improvements are made to the software being used

The methodology used as well as the diverse vulnerability scanning software packages assess security differently

This can influence the result of the assessment



Testing

Penetration Testing

- Penetration testing assesses the security model of the organization as a whole
- It reveals potential consequences of a real attacker breaking into the network
- A penetration tester is differentiated from an attacker only by his intent and lack of malice
- Penetration testing that is not completed professionally can result in the loss of services and disruption of the business continuity

Types of Penetration Testing

External testing

- External testing involves analysis of publicly available information, a network enumeration phase, and the behavior of security devices analyzed

Internal testing

- Internal testing will be performed from a number of network access points, representing each logical and physical segment
  - Black-hat testing/zero-knowledge testing
  - Gray-hat testing/partial-knowledge testing
  - White-hat testing/complete-knowledge testing

Risk Management

An unannounced test is usually associated with higher risk and a greater potential of encountering unexpected problems

Risk = Threat x Vulnerability

A planned risk is any event that has the potential to adversely affect the penetration test

The pentest team is advised to plan for significant risks to enable contingency plans in order to effectively utilize time and resources

Do-it-Yourself Testing

The degree to which the testing can be automated is one of the major variables that affect the skill level and time needed to run a pentest

The degree of test automation, the extra cost of acquiring a tool, and the time needed to gain proficiency are factors that influence the test period

Outsourcing Penetration Testing Services

Drivers for outsourcing pentest services

- To get the network audited by an external agency to acquire an intruder's point of view
- The organization may require a specific security assessment and suggestive corrective measures

Underwriting penetration testing

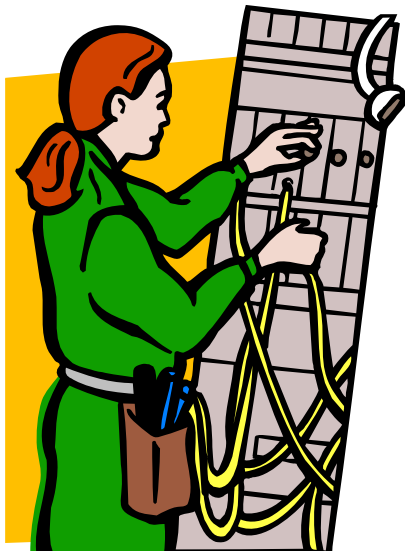
- Professional liability insurance pays for settlements or judgments for which pen testers become liable as a result of their actions, or failure to perform professional services
- It is also known as E&O insurance or professional indemnity insurance

Terms of Engagement

An organization will sanction a penetration test against any of its production systems after it agrees upon explicitly stated rules of engagement

It must state the terms of reference under which the agency can interact with the organization

It can specify the desired code of conduct, the procedures to be followed, and the nature of the interaction between the testers and the organization



Project Scope

Determining the scope of the pentest is essential to decide if the test is a targeted test or a comprehensive test

Comprehensive assessments are coordinated efforts by the pentest agency to uncover as much vulnerability as possible throughout the organization

A targeted test will seek to identify vulnerabilities in specific systems and practices

Pentest Service Level Agreements

A service level agreement is a contract that details the terms of service that an outsourcer will provide

Professionally done SLAs can include both remedies and penalties

The bottom line is that SLAs define the minimum levels of availability from the testers and determine what actions will be taken in the event of serious disruption

Testing Points

Organizations have to reach a consensus on the extent of information that can be divulged to the testing team to determine the starting point of the test

Providing a penetration testing team with additional information may give them an unrealistic advantage

Similarly, the extent to which the vulnerabilities need to be exploited without disrupting critical services needs to be determined

Testing Locations

The pentest team may have a choice of doing the test either remotely or on-site

A remote assessment may simulate an external hacker attack. However, it may miss assessing internal guards

An on-site assessment may be expensive and may not simulate an external threat exactly

Automated Testing

Automated testing can result in time and cost savings over a long term; however, it cannot replace an experienced security professional

Tools can have a high learning curve and may need frequent updating to be effective

With automated testing, there exists no scope for any of the architectural elements to be tested

As with vulnerability scanners, there can be false negatives or worse, false positives

Manual Testing

Manual testing is the best option an organization can choose to benefit from the experience of a security professional

The objective of the professional is to assess the security posture of the organization from a hacker's perspective

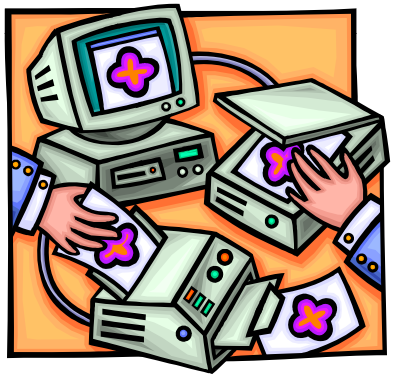
A manual approach requires planning, test designing, scheduling, and diligent documentation to capture the results of the testing process in its entirety

Using DNS Domain Name and IP Address Information

Data from the DNS servers related to the target network can be used to map a target organization's network

The DNS record also provides some valuable information regarding the OS or applications that are being run on the server

The IP block of an organization can be discerned by looking up the domain name and contact information for personnel



Enumerating Information about Hosts on Publicly-Available Networks

Enumeration can be done using port scanning tools, IP protocols, and listening to TCP/UDP ports

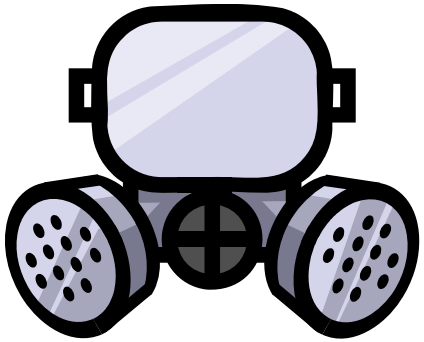
The testing team can then visualize a detailed network diagram that can be publicly accessed

Additionally, the effort can provide screened subnets and a comprehensive list of the types of traffic that are allowed in and out of the network

Website crawlers can mirror entire sites

Testing Network-Filtering Devices

The objective of the pentest team would be to ascertain that all legitimate traffic flows through the filtering device



Proxy servers may be subjected to stress tests to determine their ability to filter out unwanted packets

Testing for default installations of the firewall can be done to ensure that default user IDs and passwords have been disabled or changed

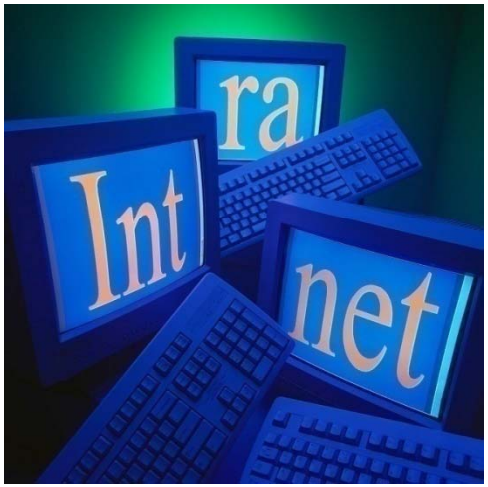
Testers can also check for any remote login capability that might have been enabled

Enumerating Devices

A device inventory is a collection of network devices together with some relevant information about each device that is recorded in a document

After the network has been mapped and the business assets identified, the next logical step is to make an inventory of the devices

A physical check may be conducted additionally to ensure that the enumerated devices have been located correctly

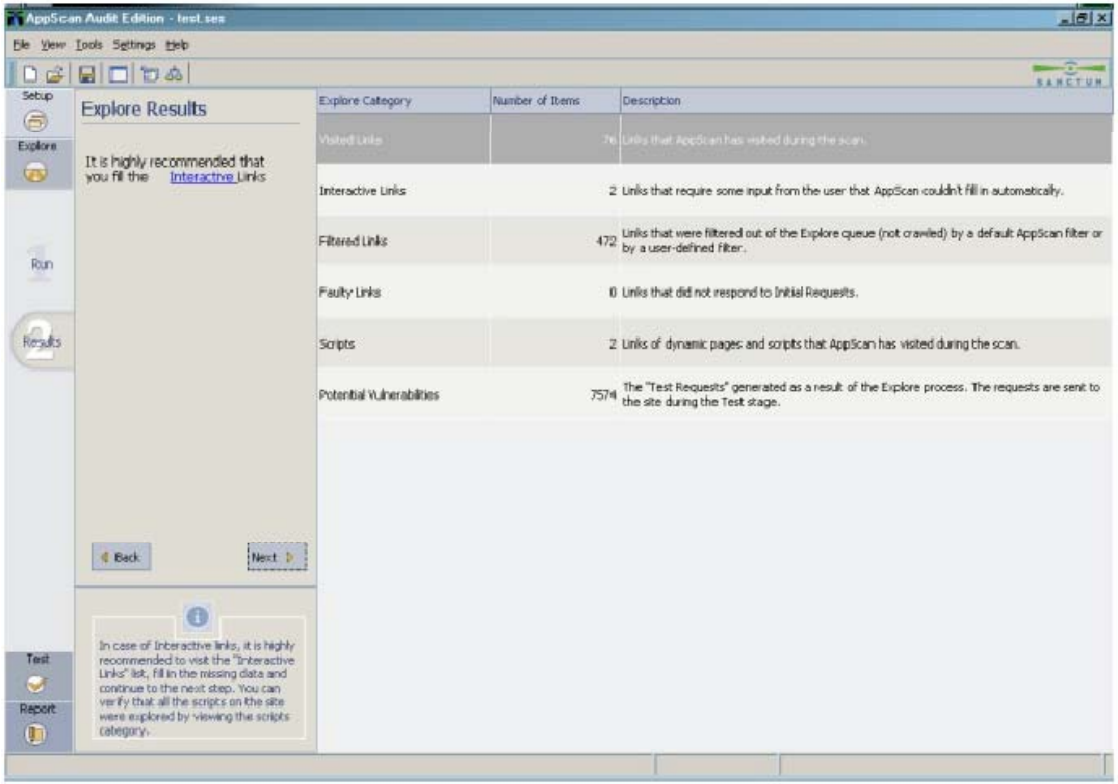


Denial of Service Emulation

- Emulating DoS attacks can be resource intensive
- DoS attacks can be emulated using hardware
- Some online sites simulate DoS attacks for a nominal charge
- These tests are meant to check the effectiveness of anti-DoS devices

Penetration Testing Tools

Pentest Using Appscan



AppScan is a tool developed for automated web application security testing and weakness assessment software

HackerShield

HackerShield is an anti-hacking program that identifies and fixes the vulnerabilities that hackers use to get into servers, workstations, and other IP devices

HackerShield Scan Summary: 10.30.102.39

Report Name:	10.30.102.39	**Report Date:**	08-07-2000 13:38:24
No. of Hosts Scanned:	1	**Scan Started:**	08-07-2000 13:38:24
No. of Groups Scanned:	1	**Scan Completed:**	08-07-2000 13:40:53
Total Unreachable Devices:	--	**Elapsed Time:**	00:02:29
AutoFix Enabled:	No		

Security Holes Found:

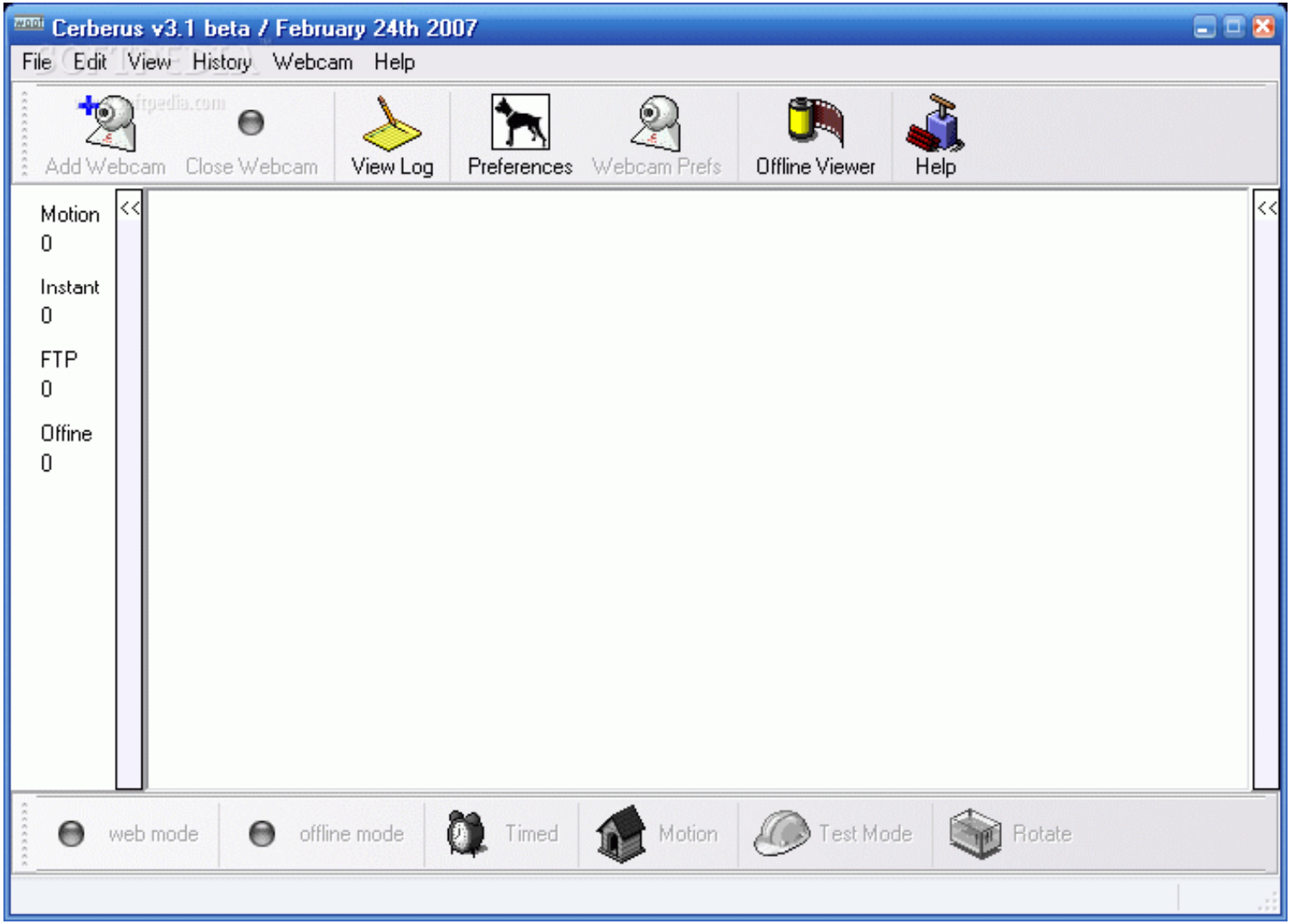
	Found	*Fixed*
High Risk	4	--
Medium Risk	12	--
Low Risk	20	--
Total	36	--
Unique	36	--

Pentest Using Cerberus Internet Scanner

Cerberus Information Security used to maintain the Cerberus Internet Scanner (CIS) is now available at @stake

It is programmed to assist administrators in finding and fixing vulnerabilities in their systems

Cerberus: Screenshot



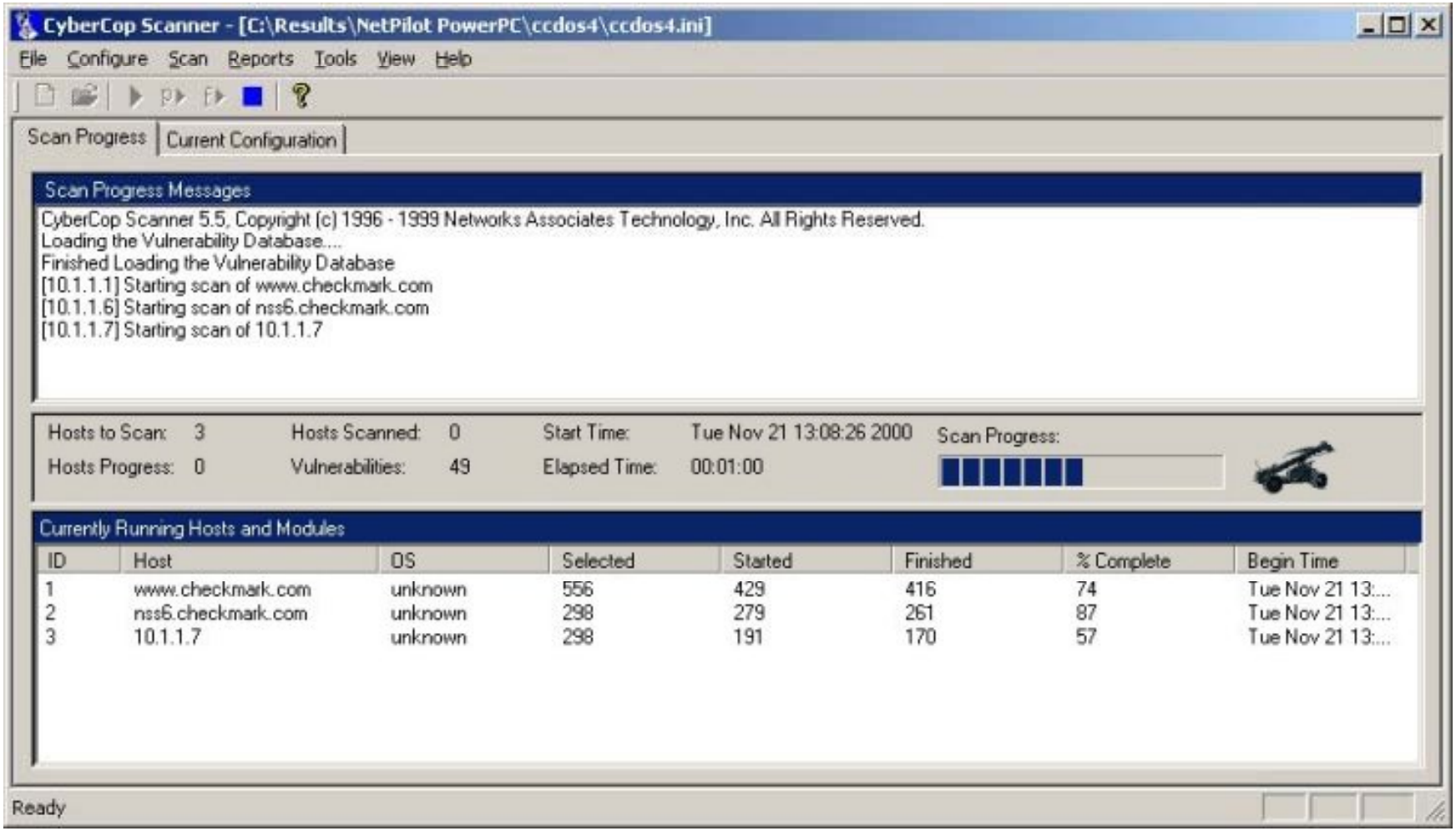
Pentest Using Cybercop Scanner

Cybercop Scanner enables the user to identify vulnerabilities by conducting more than 830 vulnerability checks

It is more effective as it runs a scan on over 100 hosts at the same time and also does applicable tests on network devices

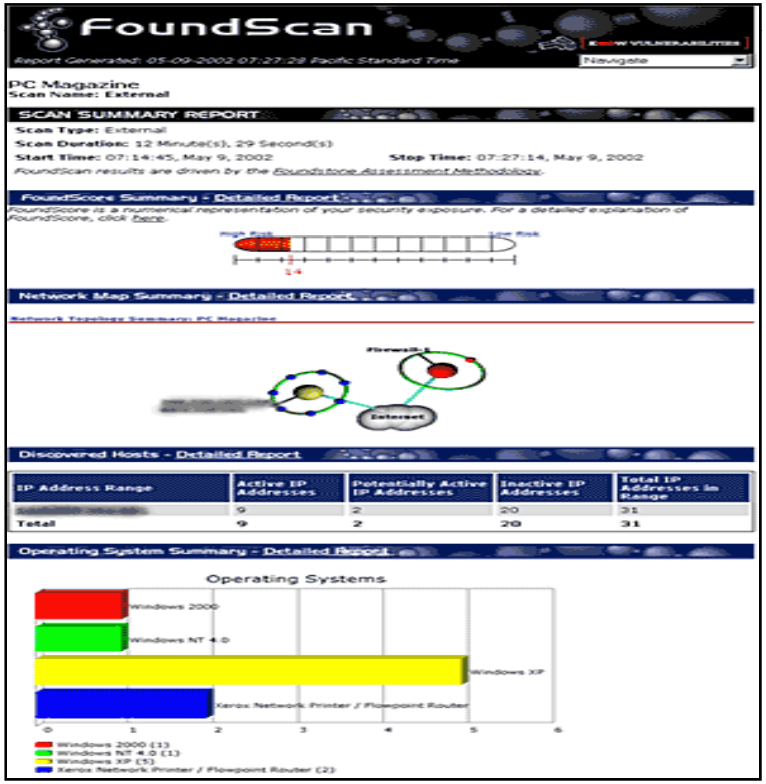
It is also useful to administrators for fixing problems and security holes

Cybercop: Screenshot



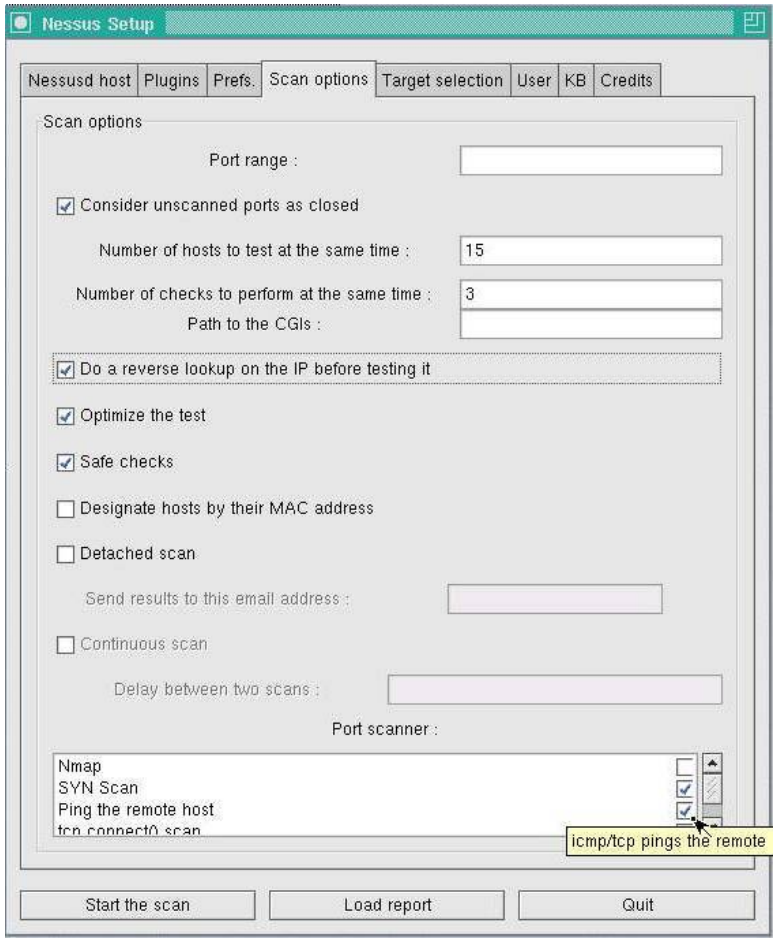
Pentest Using FoundScan Hardware Appliances

FoundScan tries to identify and locate the operating systems running on each live host by analyzing returned data with an algorithm



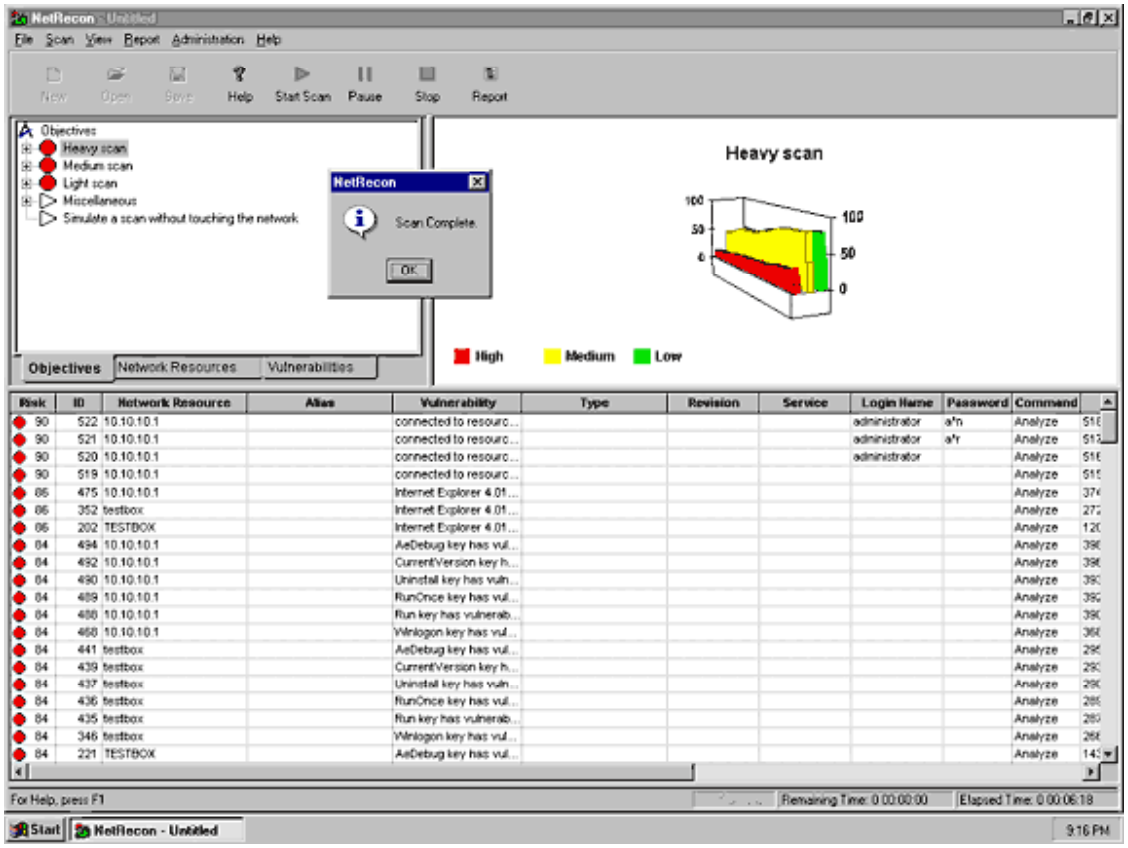
Pentest Using Nessus

Nessus is a suitable utility for service detection as it has an enhanced service-detecting feature



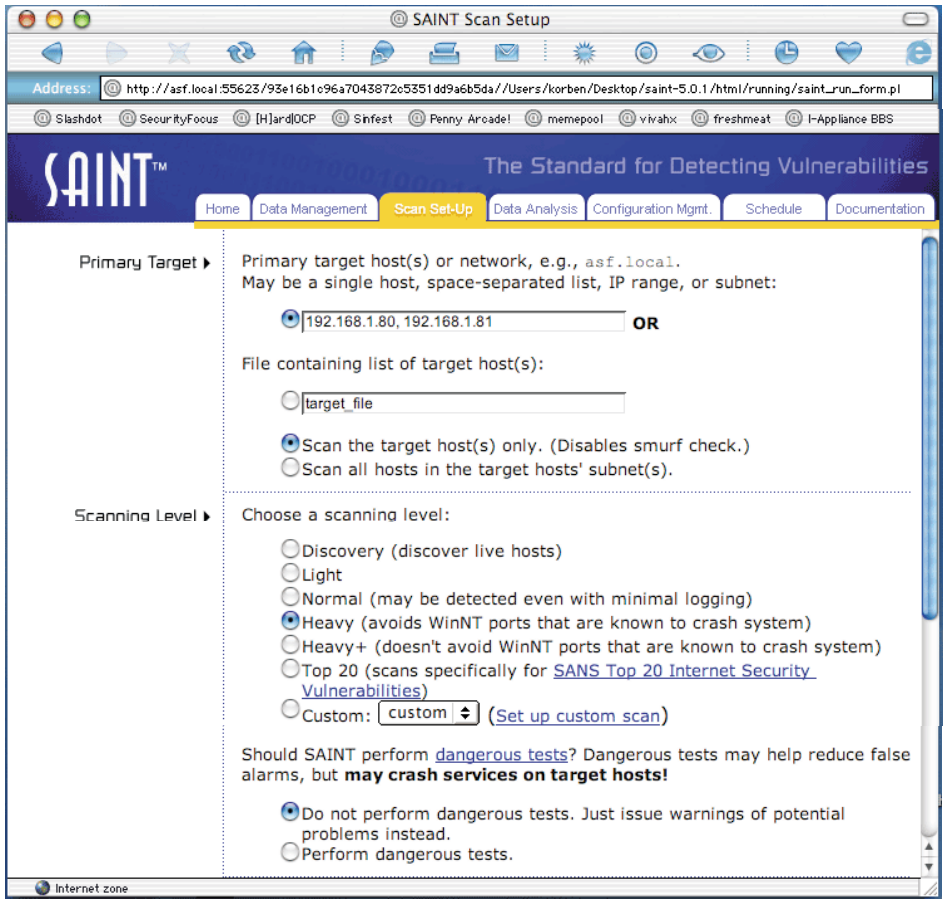
Pentest Using NetRecon

NetRecon is useful in defining common intrusion and attack scenarios to locate and report network holes



Pentest Using SAINT

SAINT monitors every live system on a network for TCP and UDP devices

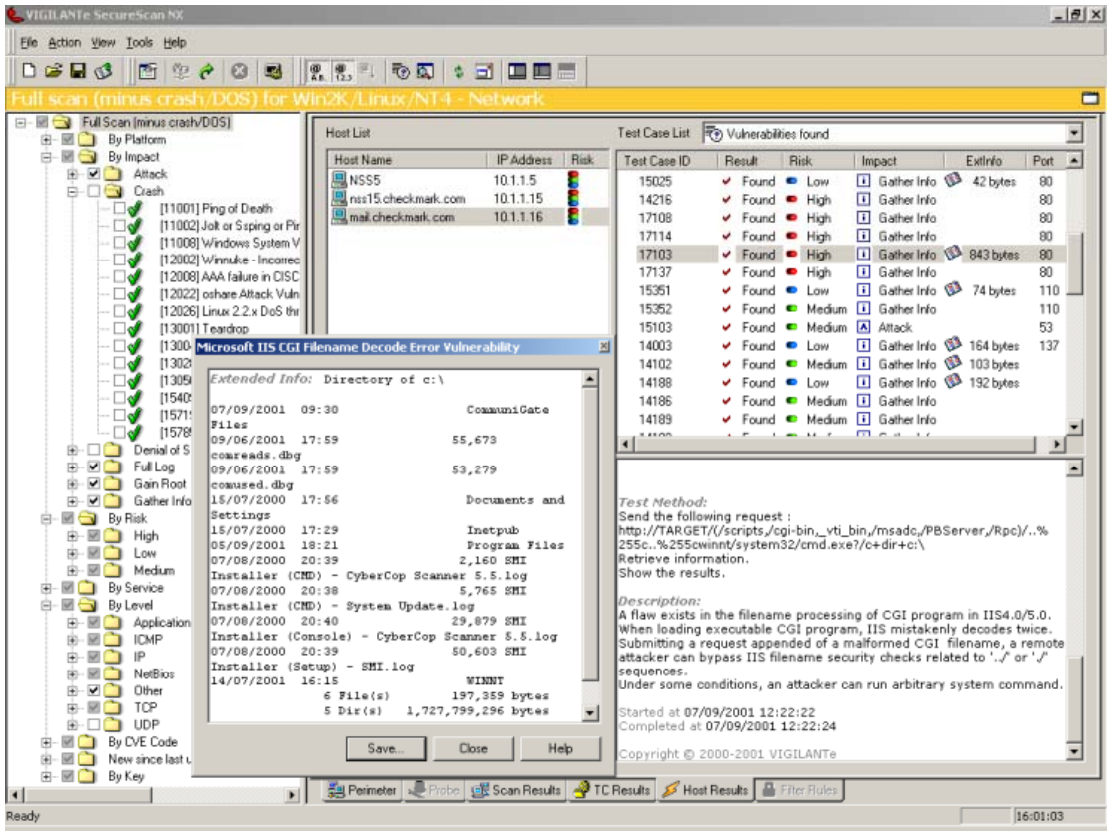


Pentest Using SecureNET Pro

SecureNET Pro is a fusion of many technologies, namely session monitoring, firewall, hijacking, and keyword-based intrusion detection

Pentest Using SecureScan

SecureScan is a network vulnerability assessment tool that determines whether internal networks and firewalls are vulnerable to attacks, and recommends corrective action for identified vulnerabilities



Pentest Using SATAN, SARA, and Security Analyzer

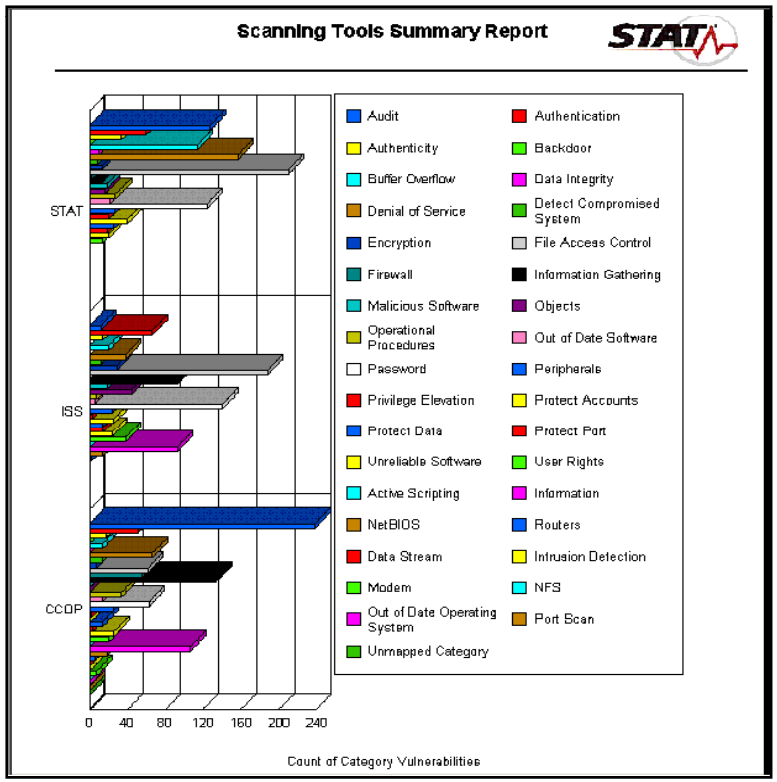
Security Auditor's Research Assistant (SARA) is a third generation Unix-based security analysis tool

SATAN is considered one of the pioneering tools that led to the development of vulnerability assessment tools

Security Analyzer helps in preventing attacks, protecting the critical systems, and safeguarding information

Pentest Using STAT Analyzer

STAT Analyzer is a vulnerability assessment utility that integrates state-of-the-art commercial network modeling and scanning tools

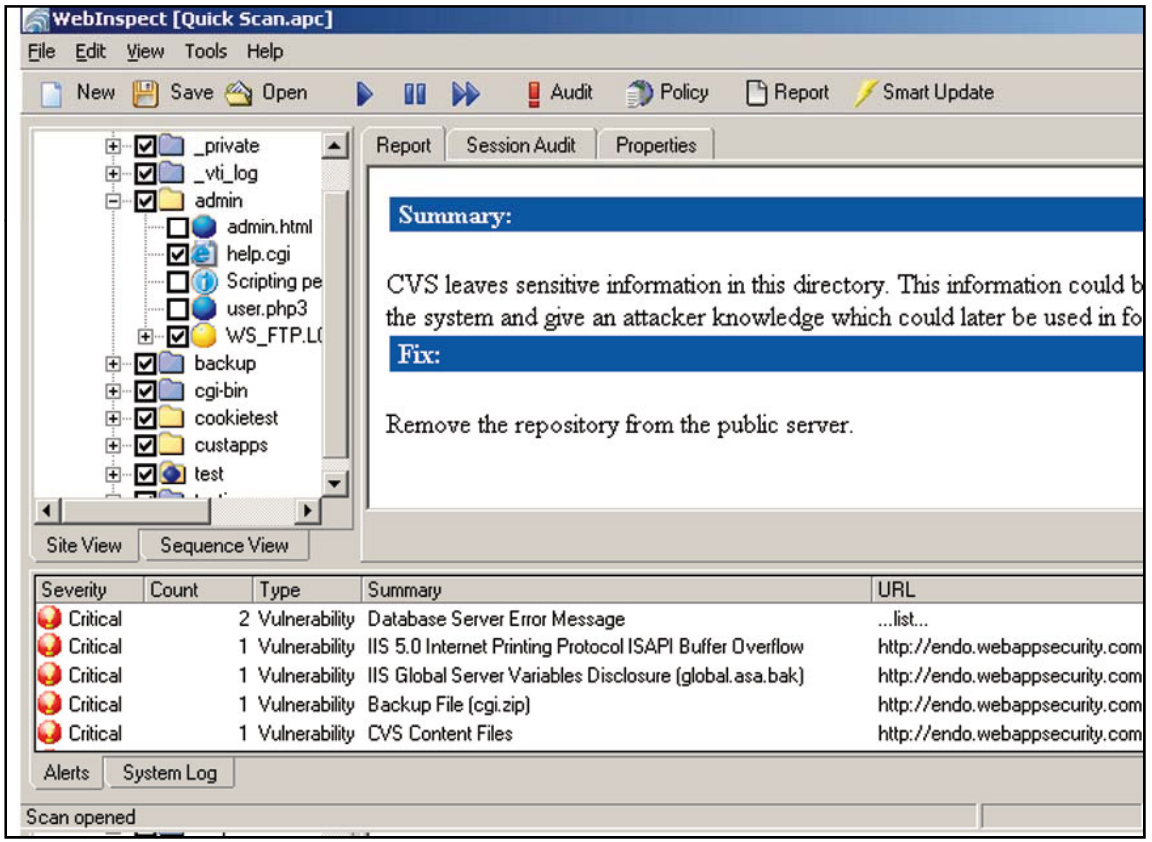


Pentest Using VigilENT

VigilENT helps to protect systems by assessing policy compliance, identifying security vulnerabilities, and helping correct exposures before they result in failed audits, security breaches, or costly downtime

Pentest Using WebInspect

WebInspect complements firewalls and intrusion detection systems by identifying web application security holes, defects, or bugs with a security suggestion



Pentest Using CredDigger

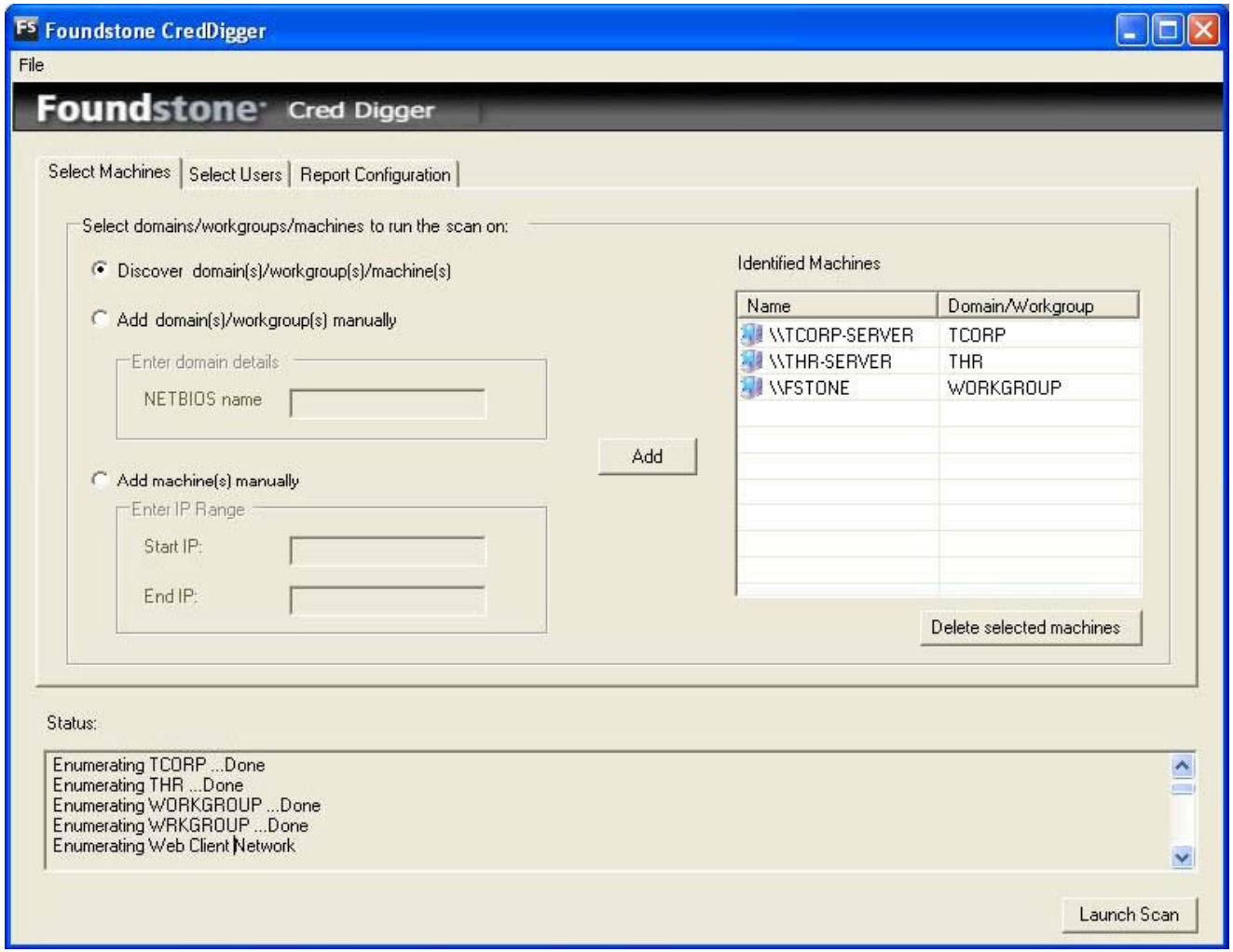
www.foundstone.com

CredDigger™ is a tool that attempts to gather data to assist penetration testing on a corporate network by:

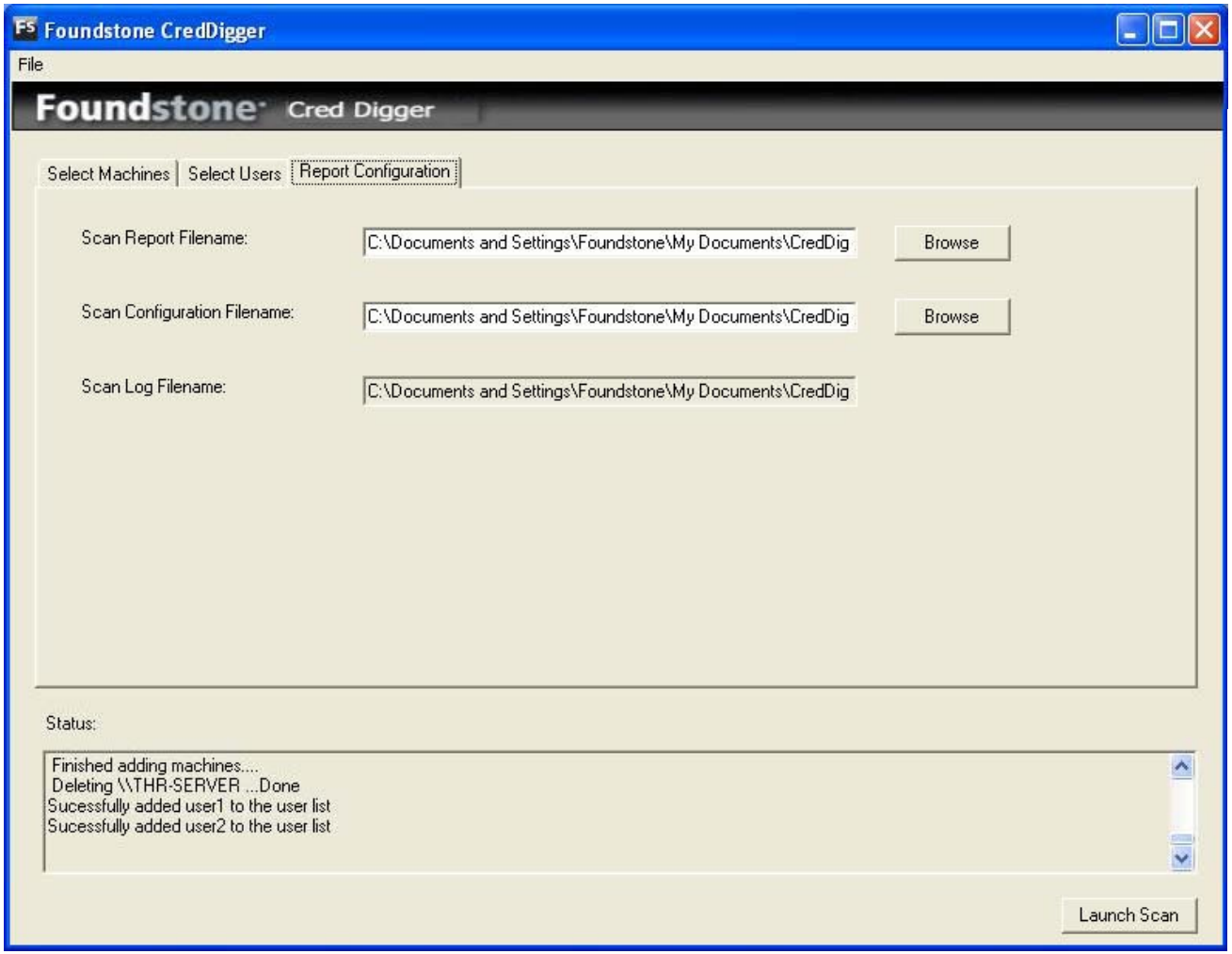
- Determining every host on which a given set of user credentials is valid
- Building a database of all user ID's through various means and protocols

It allows the penetration testers to identify and exploit all vectors into a given set of domains via acquired user credentials, leveraging any potential trust relationships implied by poor group structure

CredDigger: Screenshot 1



CredDigger: Screenshot 2



Pentest Using Nsauditor

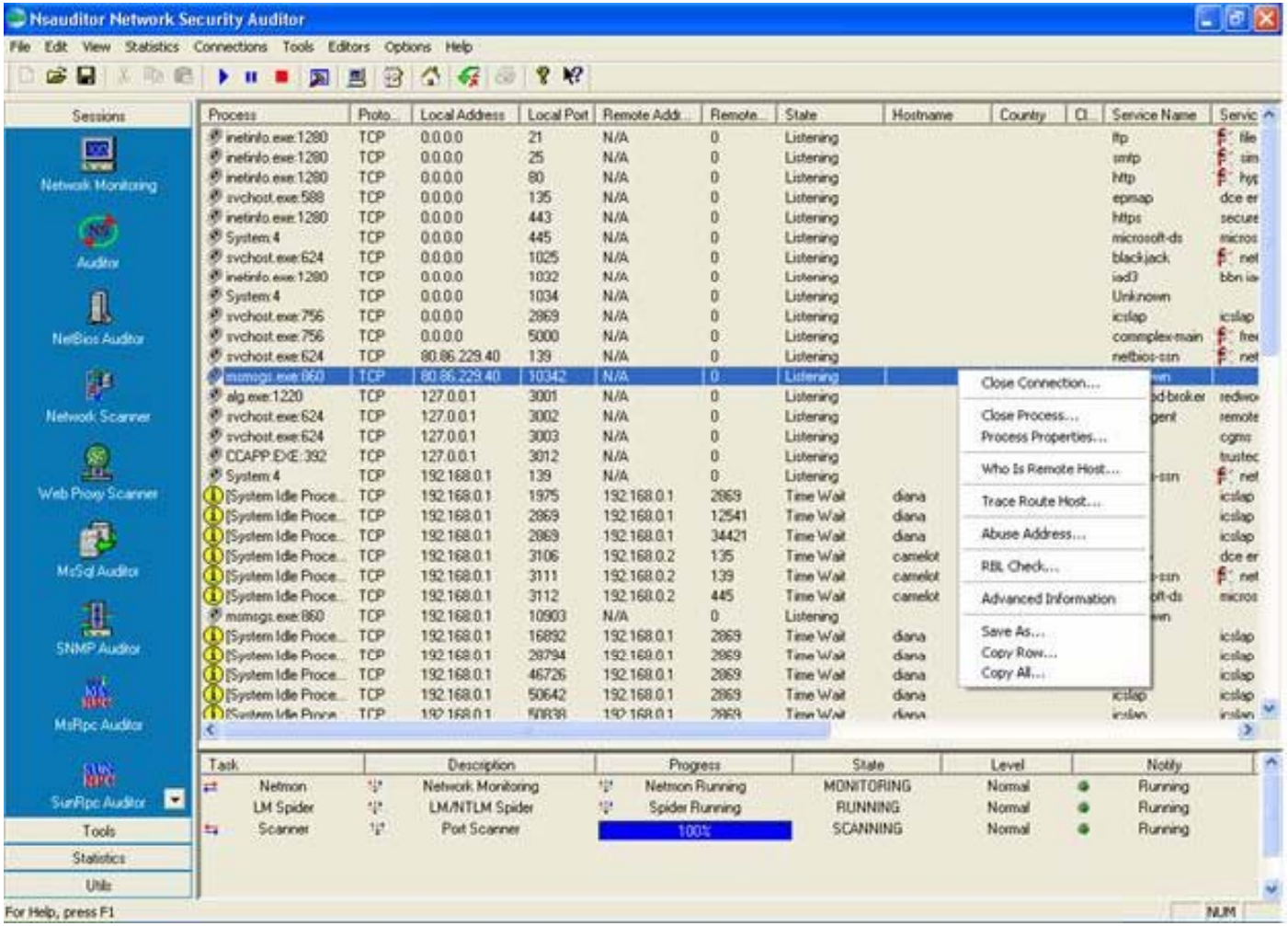
www.nsauditor.com

Nsauditor is a network security scanner that allows to audit and monitor remote network computers for possible vulnerabilities, checks your network for all potential methods that a hacker might use to attack

The program includes more than 45 network tools for scanning, sniffing, enumerating, and gaining access to machines and contains a built-in database of known network security vulnerabilities, which allows you to select the items for scanning and adds custom entries

It can reveal and catalog a variety of information, including installed software, shares, users, drives, hotfixes, NetBios, RPC, SQL and SNMP information, and open ports

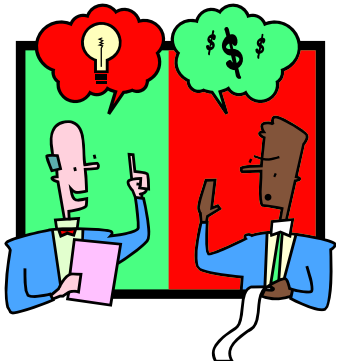
Nsauditor: Screenshot



Evaluating Different Types of Pentest Tools

The different factors affecting the type of tool selected include:

- Cost
- Platform
- Ease of use
- Compatibility
- Reporting capabilities

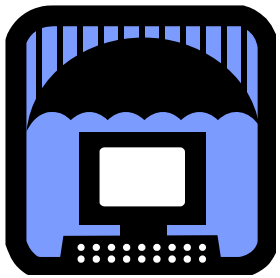


Asset Audit

Typically, an asset audit focuses on what needs to be protected in an organization

The audit enables organizations to specify what they have and how well these assets have been protected

The audit can help in assessing the risk posed by the threat to the business assets



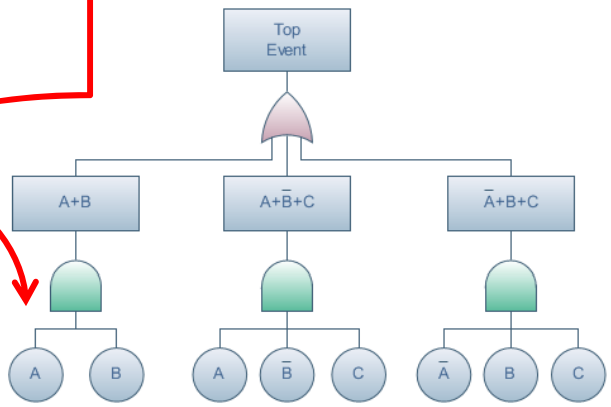
Fault Trees and Attack Trees

Commonly used as a deductive, top-down method for evaluating a system's events

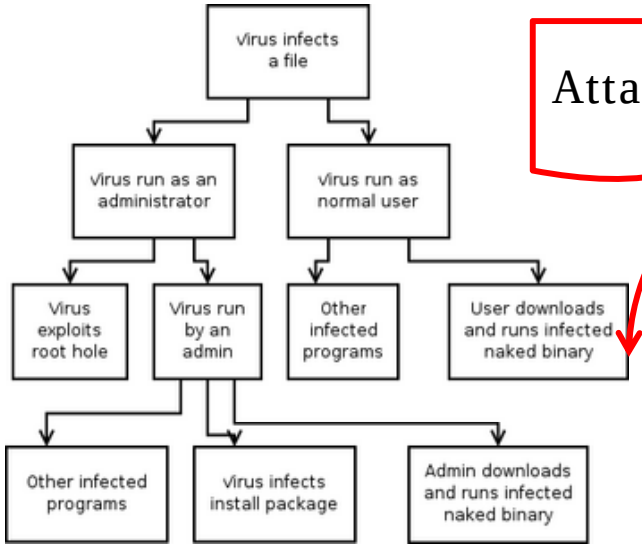
Involves specifying a root event to analyze, followed by identifying all the related events (or second-tier events) that could have caused the root event to occur

An attack tree provides a formal, methodical way of describing who, when, why, how, and with what probability an intruder might attack a system

Fault- Tree



Attack-Tree

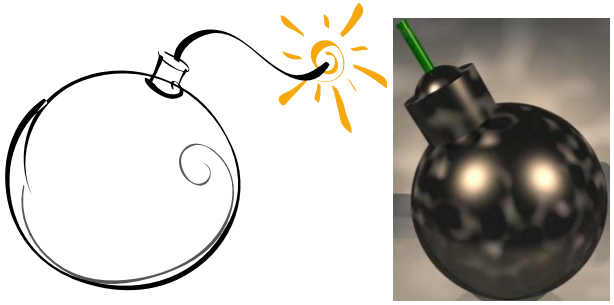


GAP Analysis

A GAP analysis is used to determine how complete are a system's security measures

The purpose of a GAP analysis is to evaluate the gaps between an organization's vision (where it wants to be) and current position (where it is)

In the area of security testing, the analysis is typically accomplished by establishing the extent to which the system meets the requirements of a specific internal or external standard (or checklist)



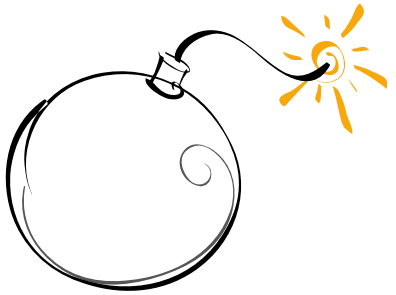
Threats

Threat

Once a device inventory has been compiled, the next step in this process is to list the different security threats

The pentest team can list the different security threats that each hardware device and software component might face

The possible threats could be determined by identifying the specific exploits that could cause such threats to occur



Business Impact of Threat

After a device inventory has been compiled, the next step is to list the various security threats that each hardware device and software component face

The pentesters need to rate each exploit and threat arising out of the exploit to assess the business impact

A relative severity can then be assigned to each threat

Internal Metrics Threat

Internal metrics is the information available within the organization that can be used for assessing the risk

The metrics may arrive differently by pentest teams depending on the method followed and their experience with the organization

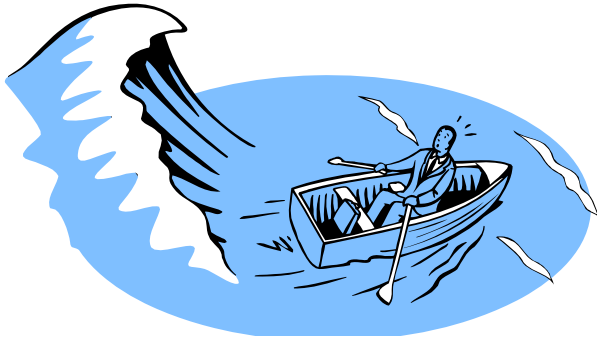
Sometimes this may be a time consuming effort or the data may be insufficient enough to be statistically valid

External Metrics Threat

External metrics can be derived from data collected outside the organization

This can be survey reports such as the FBI/CSI yearly security threat report, reports from agencies like CERT, or hacker activity reports from reputed security firms like Symantec

This must be done prior to the test



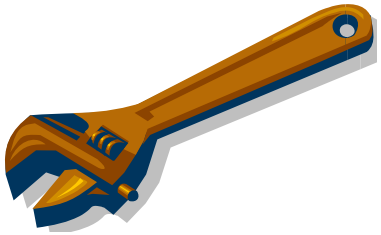
Calculating Relative Criticality

Once high, medium, and low values have been assigned to the probability of an exploit being successful, and the impact to the business should the event occur, it then becomes possible to combine these values into a single assessment of the criticality of this potential vulnerability

Test Dependencies

From the management perspective, test dependencies would be approvals, agreement on rules of engagement, signing a contract for non-disclosure, as well as ascertaining the compensation terms

Post-testing dependencies would include proper documentation, preserving logs, and recording screen captures



Other Tools Useful in Pen-Test

Defect Tracking Tools: Bug Tracker Server

Web-based Bug/Defect Tracking Software

- By Avensoft.com
- Bug Tracker Server is a web-based bug/defect tracking software that is used by product developers and manufacturers to manage product defects

SWB Tracker

- By softwarewithbrains.com
- SWBTracker supports multi-user platforms with concurrent licensing

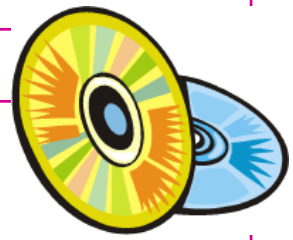
Advanced Defect Tracking Web Edition

- By http://www.borderwave.com
- The software allows you to track bugs, defects, feature requests, and suggestions by version or customer

Disk Replication Tools

Snapback DUP

- By http://www.hallogram.com
- This utility is programmed to create an exact image backup of a server or workstation hard drive



Daffodil Replicator

- By http://www.daffodildb.com
- Daffodil Replicator is a tool that enables the user to synchronize multiple data sources using a Java application

Image MASSter 4002i

- By http://www.ics-iq.com
- This tool allows the user to figure out a solution in setting up a workstation and operating system roll-out methods

DNS Zone Transfer Testing Tools

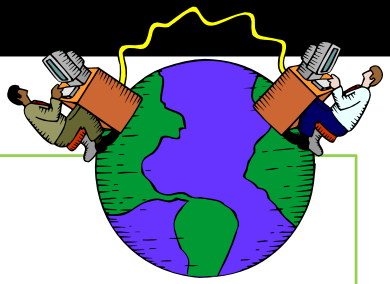
DNS analyzer

- http://www.solarwinds.net/Tools/IP_Address_Management/DNS%20Analyzer/index.html
- The DNS Analyzer application is used to display the order of the DNS resource records

Spam blacklist

- http://www.solarwinds.net/Tools/EmailMgmt
- DNS blacklists are a popular tool used by email administrators to help block reception of SPAM into their mail systems

Network Auditing Tools



eTrust Audit (AUDIT LOG REPOSITORY)

- By http://ca.com
- The system's performance is not reduced and undertakes loads of network traffic made by other auditing products

iInventory

- By http://www.iinventory.com
- The iInventory program enables the user to audit a Windows, Mac, or Linux operating system for detailed hardware and software configuration

Centennial Discovery

- Centennial Discovery program has unique pending LAN Probe software, which is able to locate every IP hardware that is connected to the network

Trace Route Tools and Services

Trellian Trace Route

- By www.tucows.com
- Trace route application allows the website administrator to see how many servers his website is passing through before it gets into the computer, informing the website administrator if there are any problem-causing servers, and even gives a ping time for each server in the path

Ip Tracer by www.soft32.com

- Ip Tracer is an application made for tracking down spammers

Network Sniffing Tools

Sniff'em

- By -//www.sniff-em.com/
- Sniff'em™ is a competitively priced, performance minded Windows-based packet sniffer, network analyzer, and network sniffer. It is a revolutionary new network management tool designed from the ground up with ease and functionality in mind

PromiScan

- By www.shareup.com
- PromiScan has better monitoring capabilities by providing nonstop watch to detect immoral programs starting and ending without increasing the network load

Denial-of-Service Emulation Tools

FlameThrower - By www.antara.net

- FlameThrower generates real-world Internet traffic from a single network appliance, so users can decide the overall site capacity and performance, and pinpoint weaknesses and potentially fatal bottlenecks

Mercury LoadRunner™- By http://www.mercury.com

- The Mercury LoadRunner application is the industry-standard performance-testing product for the system's behavior and performance

ClearSight Analyzer - By www.spirentcom.com

- ClearSight Analyzer has many features including an Application Troubleshooting Core that is used to troubleshoot applications with visual representations of the information

Traditional Load Testing Tools

PORTENT Supreme

- By www.loadtesting.com
- Portent Supreme is a featured tool for generating large amounts of HTTP, which can be uploaded into the webserver

WebMux

- By www.redhillnetworks.com/
- WebMux load balancer can share the load among a large number of servers making them appear as one large virtual server

SilkPerformer

- By www.segue.com/
- SilkPerformer enables the user to exactly predict the weaknesses in the application and its infrastructure before it is deployed, regardless of its size or complexity

System Software Assessment Tools

System Scanner

- By www.iss.net
- The System Scanner network security application operates as an integrated component of Internet Security Systems' security management platform, assessing host security, monitoring, detecting, and reporting system security weaknesses

Internet Scanner

- By www.shavlik.com
- This utility has a simple, spontaneous interface that allows the user to accurately control which groups are going to be scanned and by what principle, when, and how they are installed

Database Scanner

- By www.iss.net
- The database scanner assesses online business risks by identifying security exposures in leading database applications

Operating System Protection Tools

Bastille Linux

- Bastille Linux is programmed to inform the installing administrator about the issues regarding security concerned in each of the script's tasks

Source: *www.bastille-linux.org*

Engarde Secure Linux

- It provides greater levels of support
- It supports the advanced hardware and sophisticated upgrade path

Source: *www.engardelinux.org*

Fingerprinting Tools

@Stake LC 5:

- @Stake LC5 decreases the security risk by assisting the administrators in identifying and fixing security holes that are due to the use of weak or easily deduced passwords

Source: *www.atstake.com*

Foundstone:

- Foundstone's fully automated approach to vulnerability remediation enables organizations to easily track and manage the vulnerability fix process

Source: *www.foundstone.com*

Port Scanning Tools

Superscan

- By www.foundstone.com.
- This utility can scan through the port at a good speed and it also has this enhanced feature to support unlimited IP ranges

Advanced Port Scanner

- By www.pcflank.com
- Advanced Port Scanner is a user-friendly port scanner that executes multi-threaded for best possible performance

AW Security Port Scanner

- By www.atelierweb.com
- Atelier Web Security Port Scanner (AWSPS) is a resourceful network diagnostic toolset that adds a new aspect of capabilities to the store of network administrators and information security professionals

Directory and File Access Control Tools

Abyss Web Server for Windows

- By www.aprelium.com
- The Abyss Web server application is a small personal web server that can support HTTP/1.1 CGI scripts, partial downloads, caching negotiation, and indexing files

GFI LANguard Portable Storage Control

- By www.gfi.com
- The GFI LANguard Portable Storage Control tool allows network administrators to have absolute control over which user can access removable drives, floppy disks, and CD drives on the local machine

Windows Security Officer

- By www.bigfoot.com
- The Windows Security Officer application enables the network administrator to protect and totally controls access to all the systems present in the LAN

File Share Scanning Tools

Infiltrator Network Security Scanner

- By www.network-security-scan.com/
- This application is a network security scanner that can be used to audit network computers for possible vulnerabilities, exploits, and other information enumerations

Encrypted FTP 3

- By www.eftp.org
- GFILAN guard = www.meste.cl/soluciones/gfilan.htm

Password Directories

Passphrase Keeper

- By www.passphrasekeeper.com
- Passphrase Keeper enables the user to safely save and manage all account information such as user names, passwords, PINs, and credit card numbers

IISProtect

- By www.iisprotect.com
- IISProtect performs the function of authenticating the user and safeguarding passwords

Password Guessing Tools

Webmaster Password Generator

- By www.spychecker.com
- The Webmaster Password Generator application is a powerful and easy-to-use tool used to create a large list of random passwords

Internet Explorer Password Recovery Master

- By www.rixler.com
- Internet Explorer Password Revealer is a password recovery tool programmed for watching and cleaning the password and form data stored by Internet Explorer

Password Recovery Toolbox

- By www.rixler.com
- Internet Password Recovery Toolbox can recover passwords that fall into any one of these categories: Internet Explorer Passwords, network and dial-up passwords, and Outlook Express Passwords

Link Checking Tools

Alert Link Runner

- By www.alertbookmarks.com
- Alert Link Runner is an application that checks the validity of hyperlinks on a web page or site and across an entire enterprise network

Link Utility

- By www. net-promoter.com
- Link Utility is an application which has many functions. This includes checking links in the site and keeping the site fit

LinxExplorer

- By www.linxexplorer.com
- LinxExplorer is a link verification tool that enables the user to find and validate websites and HTML pages that have broken links

Web Testing-based Scripting Tools

Svoi.NET PHP Edit

- By http://phpedit.svoi.net/eng/main.phedit
- Svoi.NET PHP Edit is a utility that enables the user to edit, test, and debug PHP scripts and HTML/XML pages

OptiPerl

- By www.xarka.com
- OptiPerl enables the user to create CGI and console scripts in Perl or offline in Windows

Blueprint Software Web Scripting Editor

- By www.blueprint-software.net

Buffer Overflow Protection Tools

StackGuard

- By www.immunix.org
- It is a compiler that protects the program against stack smashing attacks

FormatGuard

- By www.immunix.org
- It is designed to provide solutions to the potentially large number of unknown format bugs

RaceGuard

- By www.immunix.org
- Race Guard protects against file system race conditions. In race conditions, the attacker seeks to exploit the time gap between a privileged program checking for the existence of a file and the program actually writing to that file

File Encryption Tools

Maxcrypt	• By www.tvcows.com • Maxcrypt is an automated computer encryption program that allows the user to not to worry about security regarding the message that is being sent
Secure IT	• By www.cypherix.co.uk/secureit2000/ • Secure IT is a compression and encryption application that offers 448-bit encryption and has a very high compression rate
Steganos	• By http://.steganos.com/?product=SSS7&language=en • The Steganos Internet Trace Destructor application deletes 150 work traces and caches cookies

Database Assessment Tools

EMS MySQL Manager

- By http://ems-hitech.com/mymanager/
- EMS MySQL Manager provides strong tools for MySQL Database Server administration and also for object management. The EMS MySQL Manager has a Visual Database manager that can design a database within seconds

SQL Server Compare

- By http://sql-server-tool.com
- The SQL Server Comparison Tool is a Windows application used for analyzing, comparing, and effectively documenting SQL Server databases

SQL Stripes

- By http://www.sql-server-tool.com/
- SQL Stripes is a program that helps network administrators to have complete control over the various SQL servers

Keyboard Logging and Screen Reordering Tools

Spector Professional

- By www.spectorsoft.com
- The Spector Keylogger has a feature named Smart Rename that helps to rename keylogger's executable files and registry entries

Handy Keylogger

- By http://www.handy-keylogger.com/
- A stealth keylogger for home and commercial use. The keylogger captures international keyboards, major 2-byte encodings, and character sets

Snapshot Spy

- By www.snapshotspy.com
- It has a deterrent feature that activates a pop-up showing a warning that the system is under surveillance. It is stealth in nature

System Event Logging and Reviewing Tools

LT Auditor+ Version

- By http://www.bluelance.com
- It monitors the network and user activities around the clock

ZVisual RACF

- By www.consul.com
- ZVisual RACF makes the job of the help desk staff and network administrators easy, as they can perform their day-to-day tasks from a Windows workstation

Network Intelligence Engine LS Series

- http://www.network-intelligence.com/
- An event log data warehouse system designed to address the information overload in distributed enterprise and service provider infrastructures
- It is deployed as a cluster and can manage large networks

Tripwire and Checksum Tools

Tripwire for Servers

- By www.tripwire.com
- Tripwire detects and points out any changes made to the system and configuration files

SecurityExpressions

- By www.pedestalsoftware.com
- A centralized vulnerability management system

MD5

- By http://en.wikipedia.org/wiki/Md5
- MD5 is a cryptographic checksum program that takes a message of arbitrary length as input and generates the output as 128-bit fingerprint or message digest of the input

Mobile-Code Scanning Tools

Vital Security

- By www.finjan.com
- This tool protects users from damaging mobile code, which is received by way of email and the Internet

E Trust Secure Content Manager

- By www3.ca.com
- E Trust Secure Content Manager gives users a built-in policy-based content security tool that allows the program to fend off attacks from business coercion to network integrity compromises

Internet Explorer Zone

- Internet Explorer Zones are split into four default zones, which are listed as the Local intranet zone, the Trusted sites zone, the Restricted Sites zone, and the Internet zone
- The administrators are given the power to configure and manage the risk from mobile code

Centralized Security Monitoring Tools

ASAP eSMART™ Software Usage	• This tool helps identify all the software installed across the organization, and also helps to detect unused applications and eliminate them Source: *www.asapsoftware.com*
WatchGuard VPN Manager	• System administrators of large organizations can monitor and manage tools centrally using WatchGuard VPN Manager Source: *www.watchguard.com*
Harvester	• Security checks and event logs Source: *http://farm9.org/*

Web Log Analysis Tools

Azure Web Log	• The tool generates reports for hourly hits, monthly hits, monthly site traffic, operating system used by the users, and browsers used by them to view the website and error requests Source: *www.azuredesktop.com*
AWStats	• AWStats is a powerful tool with lots of features that give a graphical representation of web, ftp, or mail server statistics Source: *http://awstats.sourceforge.net/*
Summary	• It has more than 200 types of reports that help the user to get the exact information he wants about the website Source: *http://www.summary.net*

Forensic Data and Collection Tools

Encase tool

- It can monitor networks in real time without disrupting operations

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

SafeBack

- It is mostly used to back up files and critical data
- It creates a mirror image of the entire hard drive just like how a photonegative is made

Source: *http://www.forensic-intl.com*

ILook Investigator

- It supports Linux platforms. It has password and passphrase dictionary generators

Source: *http://www.ilook-forensics.org*

Security Assessment Tools

Nessus Windows Technology

- Nessus Windows Technology (NeWT) is a standalone vulnerability scanner

Source: *www.nessus.org*

NetIQ Security Manager

- NetIQ Security Manager is an incident management tool that monitors the network in real time, automatically responds to threats, and provides safekeeping of important event information from a central console

Source: *ww.netiq.com*

STAT Scanner

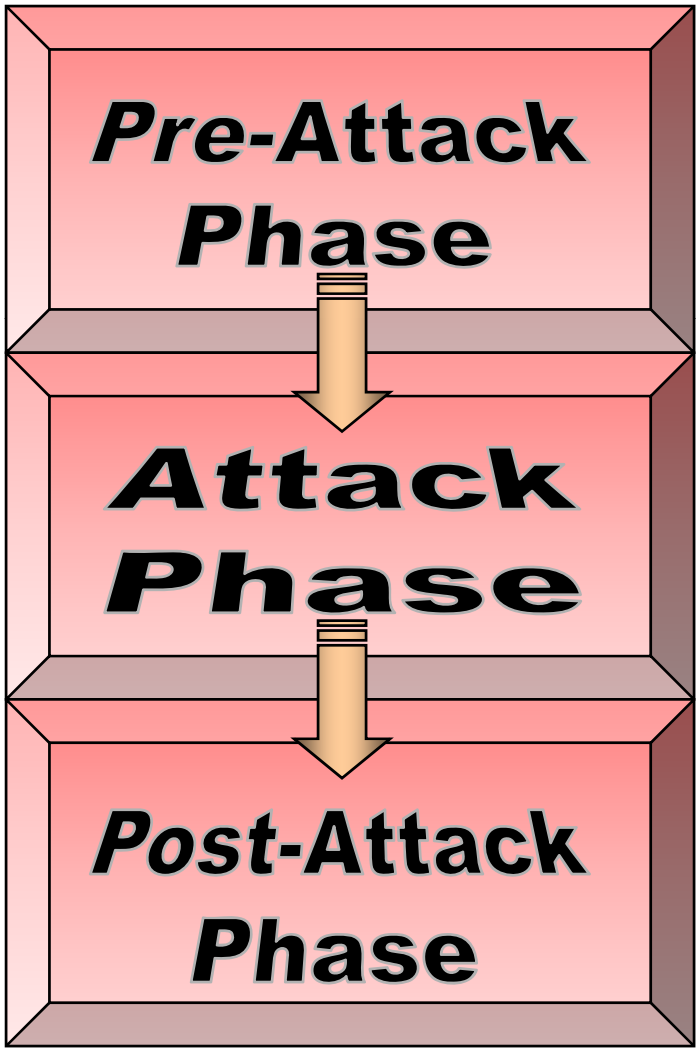
- STAT Scanner scans the network for vulnerabilities, and updates the system administrator with information regarding updates and patches

Source: *www.stat.harris.com*

Multiple OS Management Tools

Multiple Boot Manager	• Multiple Boot Manager (MBM) is a low-level system tool that helps to select any OS to boot with a menu Source: *www.elmchan.org*
Acronis OS Selector	• Acronis OS Selector v5 is a boot and partition manager, which allows the user to install more than 100 operating systems Source: *www.acronis.com*
Eon	• Eon 4000 is based on Linux and runs Windows, Unix, X Window, Internet, Java, and mainframe applications Source: *http://www.neoware.com*

Phases of Penetration Testing



Pre-Attack Phase

- Pre-Attack Phase
  - Passive Reconnaissance
  - Active Reconnaissance

Best Practices

1. It is vital to maintain a log of all the activities carried out, the results obtained, or a note of the absence of results
2. Ensure that all work is time stamped and communicated to the concerned person within the organization if it is so agreed upon in the rules of engagement
3. While planning an attack strategy, make sure that you are able to reason out your strategic choices to the input or output obtained from the pre-attack phase
4. Look at your log and start either developing the tools you need or acquiring them based on need. This will reduce the attack area that might be inadvertently passed over

Results that can be Expected

This phase can include information retrieval such as:

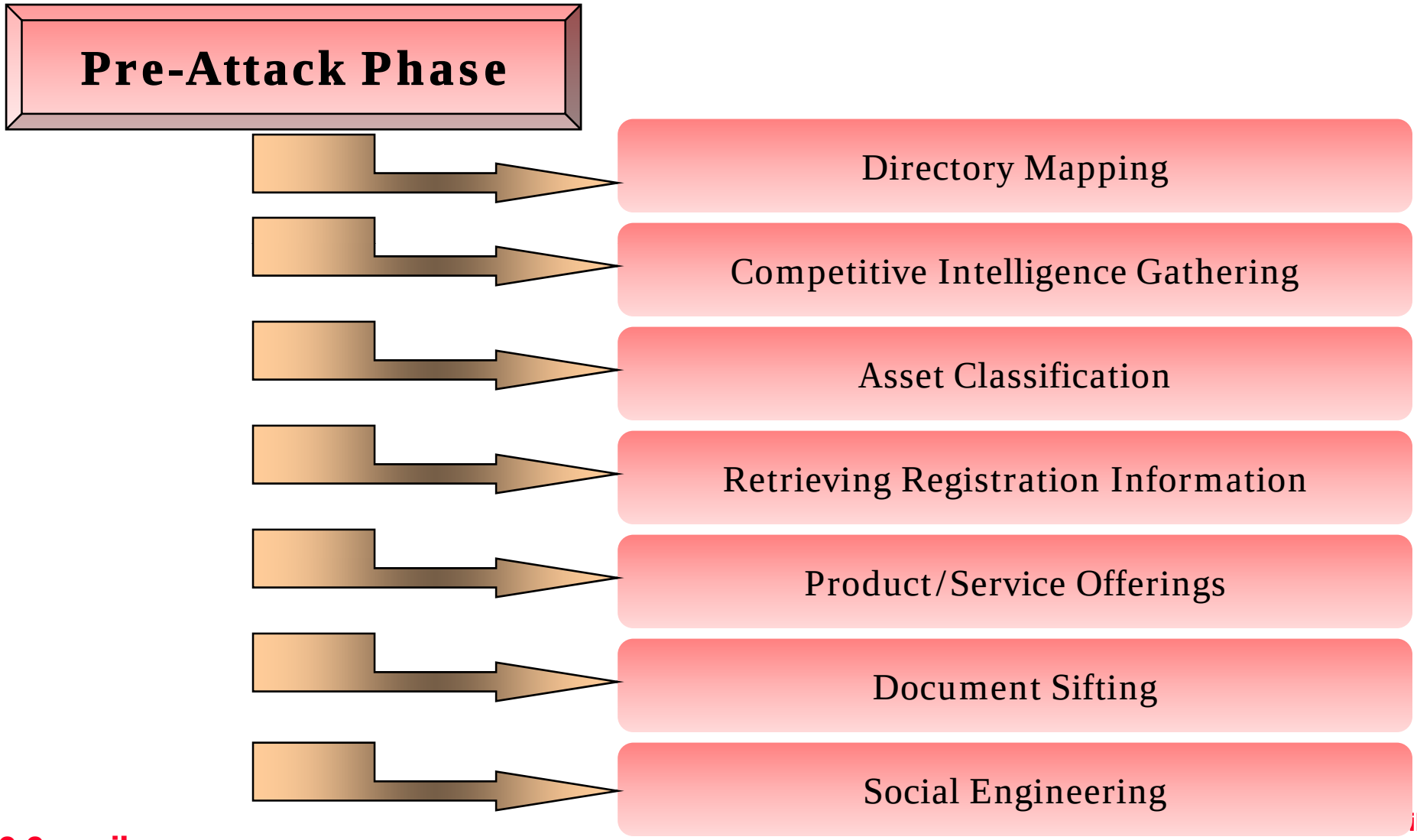
- Physical and logical location of the organization
- Analog connections
- Any contact information
- Information about other organizations
- Any other information that has potential to result in a possible exploitation

Passive Reconnaissance

Activities involve:

- Mapping the directory structure of the web servers and FTP servers
- Gathering competitive intelligence
- Determining worth of infrastructure that is interfacing with the web
- Retrieving network registration information
- Determining the product range and service offerings of the target company that are available online or can be requested online
- Document sifting refers to gathering information solely from the published material
- Social engineering

Passive Reconnaissance

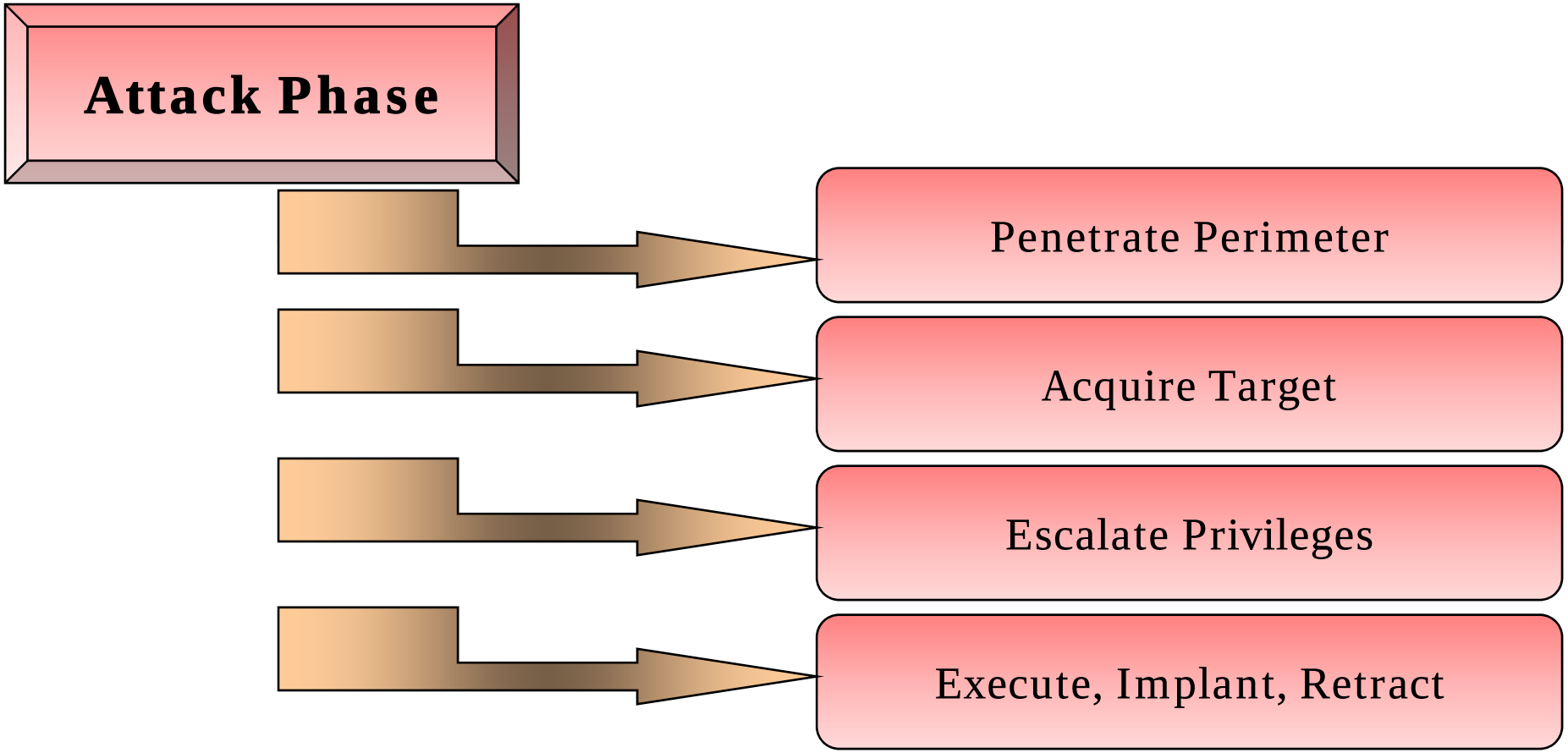


Active Reconnaissance

Some of the activities involved are:

- Network mapping
- Perimeter mapping
- System and service identification: through port scans
- Web profiling: This phase will attempt to profile and map the Internet profile of the organization

Attack Phase



Activity: Perimeter Testing

Testing methods for perimeter security include but are not limited to:

- Evaluating error reporting and error management with ICMP probes
- Checking access control lists by forging responses with crafted packets
- Measuring the threshold for denial of service by attempting persistent TCP connections, evaluating transitory TCP connections, and attempting streaming UDP connection
- Evaluating protocol filtering rules by attempting connections using various protocols such as SSH, FTP, and Telnet
- Evaluating the IDS capability by passing malicious content (such as malformed URL) and scanning the target variously for response to abnormal traffic
- Examining the perimeter security system's response to web server scans using multiple methods such as POST, DELETE, and COPY

Activity: Web Application Testing - I

Testing methods for web application testing include but are not limited to:

Input Validation:

- Tests include OS command injection, script injection, SQL injection, LDAP injection, and cross site scripting

Output Sanitization:

- Tests include parsing special characters and verifying error checking in the application

Access Control:

- It checks for access to administrative interfaces, sends data to manipulate form fields, attempts URL query strings, changes values on the client-side script, and attacks cookies

Activity: Web Application Testing - II

Checking for Buffer Overflows:

- Tests include attacks against stack overflows, heap overflows, and format string overflows

Denial of Service:

- It tests for DoS induced by malformed user input, user lockout, and application lockout due to traffic overload, transaction requests, or excessive requests on the application

Component Checking:

- It checks for security controls on web server/application components that might expose the web application to vulnerabilities

Data and Error Checking:

- It checks for data-related security lapses such as storage of sensitive data in the cache or throughput of sensitive data using HTML

Activity: Web Application Testing - III

Confidentiality Check:

- For applications using secure protocols and encryption, check for lapses in key exchange mechanism, adequate key length, and weak algorithms

Session Management:

- It checks time validity of session tokens, length of tokens, expiration of session tokens while transiting from SSL to non-SSL resources, presence of any session tokens in the browser history or cache, and randomness of session ID (check for use of user data in generating ID)

Configuration Verification:

- It attempts manipulation of resources using HTTP methods such as DELETE and PUT, check for version content availability and any visible restricted source code in public domains, attempt directory and file listing, and test for known vulnerabilities and accessibility of administrative interfaces in server and server components

Activity: Wireless Testing

Testing methods for wireless testing include but are not limited to:

- Check if the access point's default Service Set Identifier (SSID) is easily available. Test for "broadcast SSID" and accessibility to the LAN through this. Tests can include brute forcing the SSID character string using tools like Kismet
- Check for vulnerabilities in accessing the WLAN through the wireless router, access point, or gateway. This can include verifying if the default Wired Equivalent Privacy (WEP) encryption key can be captured and decrypted
- Audit for broadcast beacon of any access point and check all protocols available on the access points. Check if Layer 2 switched networks are being used instead of hubs for access point connectivity
- Subject authentication to playback of previous authentications in order to check for privilege escalation and unauthorized access
- Verify that access is granted only to client machines with registered MAC addresses

Activity: Acquiring Target

Acquiring a target is referred to the set of activities undertaken where the tester subjects the suspect machine to more intrusive challenges such as vulnerability scans and security assessment

Testing methods for acquiring target include but are not limited to:

- Active probing assaults: Use results of network scans to gather further information that can lead to a compromise
- Running vulnerability scans: Vulnerability scans are completed in this phase
- Trusted systems and trusted process assessment: Attempting to access the machine's resources using legitimate information obtained through social engineering or other means

Activity: Escalating Privileges

Once the target has been acquired, the tester attempts to exploit the system and gain greater access to the protected resources

Activities include (but are not limited to):

- The tester may take advantage of poor security policies and take advantage of email or unsafe web code to gather information that can lead to escalation of privileges
- Use of techniques such as brute force to achieve privileged status. Examples of tools include getadmin and password crackers
- Use of trojans and protocol analyzers
- Use of information gleaned through techniques such as social engineering to gain unauthorized access to privileged resources

Activity: Execute, Implant, and Retract

In this phase, the tester effectively compromises the acquired system by executing arbitrary code

The objective here is to explore the extent to which the security fails

Executing exploits already available or specially crafted to take advantage of the vulnerabilities identified in the target system

Post-Attack Phase and Activities

This phase is critical to any penetration test as it is the responsibility of the tester to restore the systems to their pre-test states

Post-attack phase activities include some of the following:

- Removing all files uploaded on the system
- Cleaning all registry entries and removing vulnerabilities created
- Removing all tools and exploits from the tested systems
- Restoring the network to the pre-test state by removing shares and connections
- Analyzing all results and presenting the same to the organization

Penetration Testing Deliverables Templates

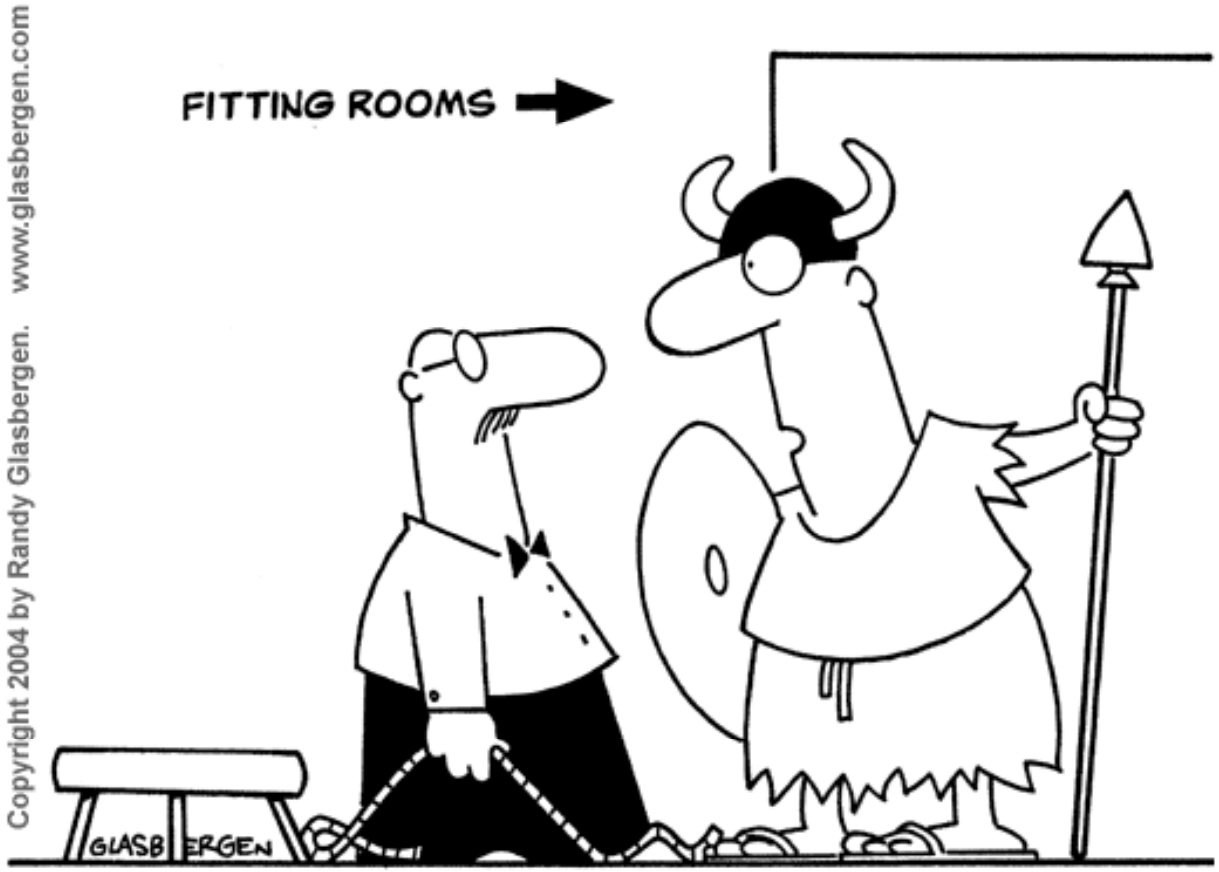
A pentest report will carry details of the incidents that have occurred during the testing process and the range of activities carried out by the testing team

Broad areas covered include objectives, observations, activities undertaken, and incidents reported

The team may also recommend corrective actions based on the rules of engagement

Summary

- A pentest simulates methods that intruders use to gain unauthorized access to an organization's networked systems and then compromise them
- Security assessment categories are security audits, vulnerability assessments, and penetration testing
- Vulnerability scanners can test systems and network devices for exposure to common attacks
- Penetration testing reveals potential consequences of a real attacker breaking into the network
- Risk = Threat x Vulnerability
- The Abyss Web server application is a small personal web server that can support HTTP/1.1 CGI scripts, partial downloads, caching negotiation, and indexing files



**"I don't want to conquer the world,
I just want to intimidate my computer!"**

"Network is down."