

IT Security Auditing

Mr. Watcharaphon Wongaphai

Senior Information Security Instructor

GIAC GCFA ,SSCP ,E | CSA ,C | EH ,CNE6 ,Security+ ,CCNA ,Network+



ACIS Professional Center

Class Introduction



❖ Introduce Instructor

❑ Watcharaphon Wongaphai

GIAC GCFA ,SSCP ,E | CSA ,C | EH ,CNE6 ,Security+ ,CCNA ,Network+

❖ Contact Point

- ❑ watcharaphon.wo@acisonline.net
- ❑ BtCs1@hotmail.com (MSN)
- ❑ facebook.com/watcharaphon.wo



❖ Session & Break

- | | | | |
|-------------|---------------|----------------------|---------------|
| ❑ Session 1 | 09:00 – 10:30 | ❑ Coffee Break | 10:30 – 10:45 |
| ❑ Session 2 | 10:45 – 12:00 | ❑ Lunch | 12:00 – 13:00 |
| ❑ Session 3 | 13:00 – 14:30 | ❑ Coffee Break | 14:30 – 14:45 |
| ❑ Session 4 | 14:45 – 16:00 | ❑ Summary of the Day | 16:00 |



Watcharaphon Wongaphai





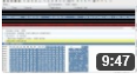
IKurpaik0

- GCFA ,SSCP ,E|CSA ,C|EH ,CNE6 ,Security+ ,CCNA ,Network+
- Instructor / Speaker ,Researcher
- My Folio
- ACIS Article
 - SSLStrip
 - How to steal cookie
 - How to recover Social Network and Vulnerability
- Public VDO
 - Vimeo.com (Kurapiko)
 - Youtube.com (IKurapiko)

Public VDO on Youtube.com ,Vimeo.com

วิดีโอที่ฉันอัปโหลด (7)

เพิ่มรายการ ▼ | การทำงาน ▼ | ดู: ทั้งหมด ▼ | จัดเรียงตาม: เพิ่มล่าสุด ▼

	Advance Cookie Stealing <small>HD</small> How to Steal Cookie Manually for Example Facebook 12 ตุลาคม 2011, 03:01 (PDT) สาธารณะ 4:33	จำนวนการดู: 4 ความคิดเห็น: 0 วิดีโอตอบกลับ: 0 👍 0 🗣️ 0
	How to Hack Facebook's Account and Hotmail , Twitter <small>HD</small> Steal Session from Social Network Website 9 กรกฎาคม 2011, 01:35 (PDT) สาธารณะ 2:46	จำนวนการดู: 57 ความคิดเห็น: 0 วิดีโอตอบกลับ: 0 👍 0 🗣️ 0
	SQL Injection upload PHP Shell via Mysql <small>HD</small> Use Sqlmap to get database's account then upload php shell 15 พฤษภาคม 2011, 10:01 (PDT) สาธารณะ 8:58	จำนวนการดู: 1,754 ความคิดเห็น: 2 วิดีโอตอบกลับ: 0 👍 3 🗣️ 0
	Bruteforce WPA without Dictionary with GPU <small>HD</small> How to Bruteforce WPA with very excellent performance from GPU 19 เมษายน 2011, 02:24 (PDT) สาธารณะ 7:55	จำนวนการดู: 12,669 ความคิดเห็น: 21 วิดีโอตอบกลับ: 0 👍 9 🗣️ 6
	Nmap Evasion Technique <small>HD</small> Evasion Using Nmap bypass Firewall ,IDS 16 เมษายน 2011, 11:48 (PDT) สาธารณะ 9:47	จำนวนการดู: 282 ความคิดเห็น: 2 วิดีโอตอบกลับ: 0 👍 0 🗣️ 0



Firesheep Hack Social Network Account

3 months ago ▶ 109 ❤️ 0 💬 0
 ARP Poisoning and Steal Session from Facebook , Hotmail , etc



Kurapiko



Firesheep+SSLStrip

3 months ago ▶ 1,477 ❤️ 1 💬 0
 Steal Facebook Account via Facebook's HTTPS



Kurapiko



SQLMap SQL Injection upload PHP Shell via Mysql

5 months ago ▶ 2,974 ❤️ 1 💬 0
 Use Sqlmap to get database's account then upload php shell



Kurapiko



Bruteforce WPA without Dictionary with GPU

6 months ago ▶ 3,633 ❤️ 0 💬 0
 How to Bruteforce WPA with very excellent performance from GPU



Kurapiko

Introduction Penetration Testing



ACIS Professional Center

Objective

- Importance of information security in today's world
- Elements of security
- Penetration Testing Framework
- Hacking methodology
- Hacktivism
- Vulnerability research and tools

Essential Terminologies

- Threat
 - An action or event that might compromise security. A threat is a potential violation of security
- Vulnerability
 - Existence of a weakness, design ,or implementation error that can lead an unexpected and undesirable event compromising the security system
- Target or Victim
 - An IT system .Product or component that is subjected to require security evaluation

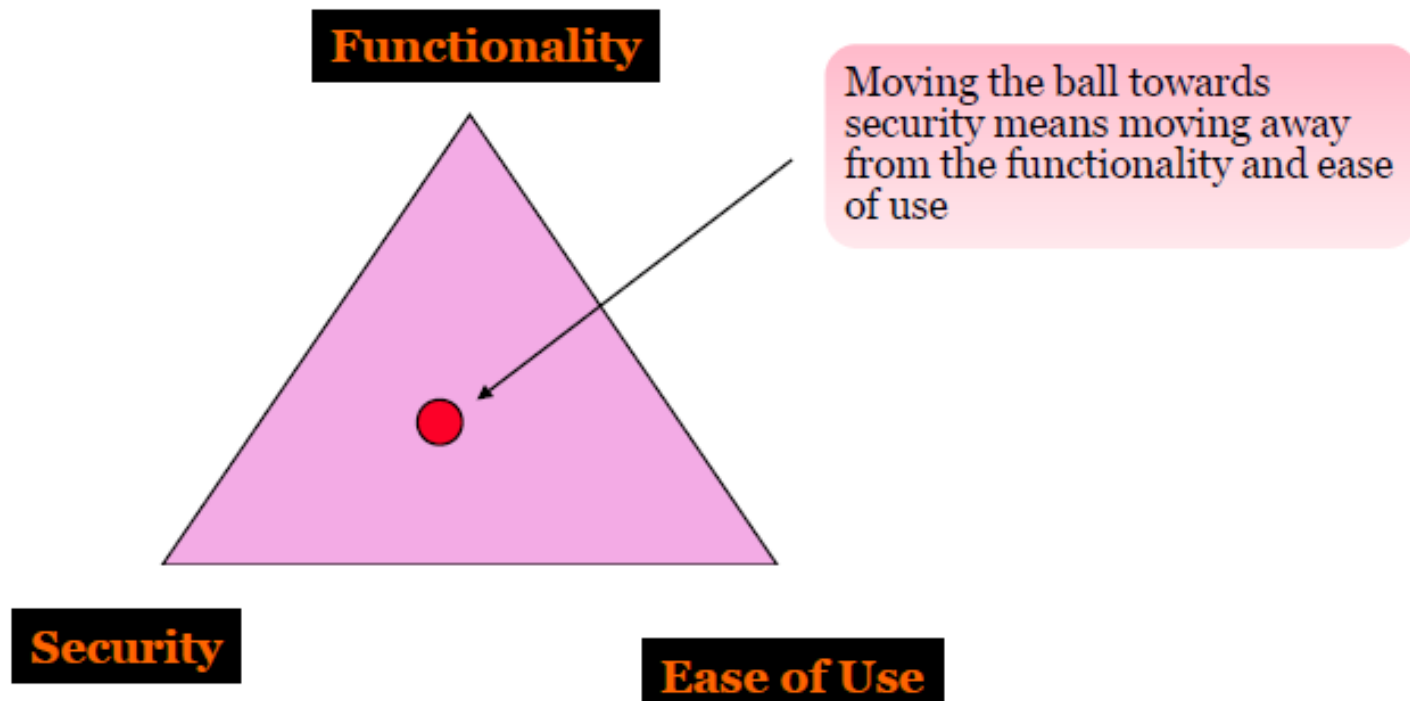
Essential Terminologies (Cont'd)

- Attack
 - An assault on the system security that is derived from intelligent threat
- Exploit
 - A defined way to breach the security of and IT system through vulnerability

Elements of Security

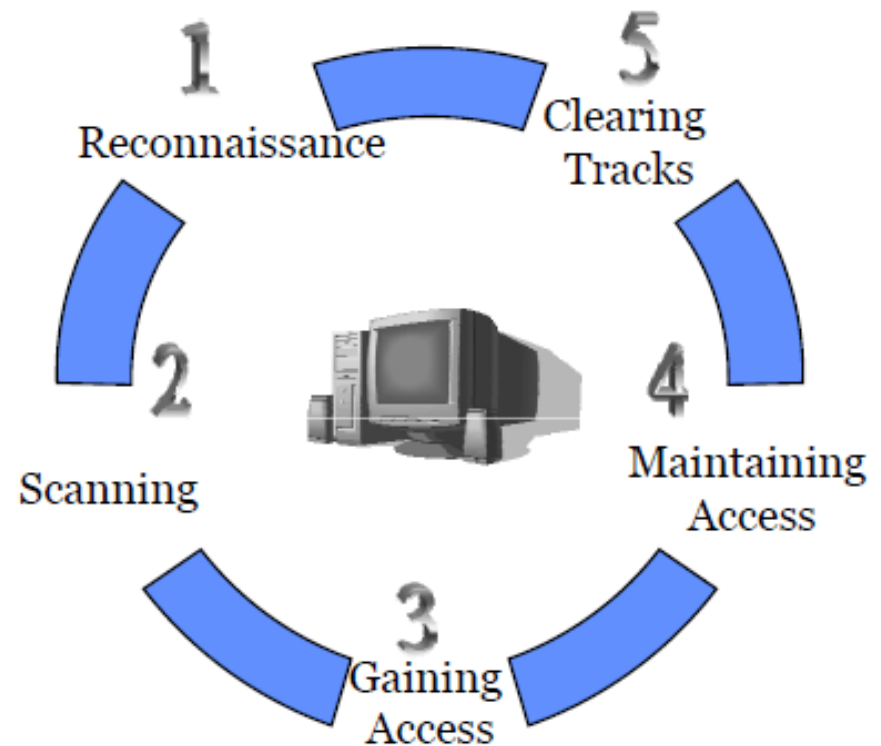
- Confidentiality
- Authenticity
- Integrity
- Availability

Balance the Security



EC-Council Hacking Methodology

- Foot printing
- Scanning
- Enumeration
- Gaining Access
- Maintaining Access
- Covering Tracks



Types of Hacker Attacks

- There are several ways an attacker can gain access to a system
- The attacker must be able to exploit a weakness or vulnerability in a system
 - Attack Types
 - Operating System attacks
 - Application-Level attacks
 - Shrink Wrap code attacks
 - Misconfiguration attacks

1. Operating System Attacks

Microsoft probes secret code leak

Microsoft is investigating how part of its Windows operating system source code found its way onto the net.

Microsoft spokesman Tom Pilla said it was not known how the chunks of Windows 2000 and NT code had leaked out.

"We are currently investigating these postings and are working with the appropriate law enforcement authorities," he said.

More than 90% of PCs use Microsoft software, so this leak of intellectual property is a concern for the company.

"It's illegal for third parties to post Microsoft source code, and we take such activity very seriously," added Mr Pilla.



It is the second security worry for Bill Gates' company this week

1. Operating System Attacks (Cont'd)

- Today's operating systems are complex in nature
- Operating systems run many services, Ports and modes of access and require extensive tweaking to lock them down
- The default installation of most operating systems has large numbers of services running and ports open
- Applying patches and hotfixes are not easy in today's complex network
- Attackers look for OS Vulnerabilities and exploit them to gain access to a network system

2. Application Level Attacks

- Software developers are under tight schedules to deliver products on time
- Extreme Programming is on the rise in software engineering methodology
- Software applications come with tons of functionalities and features
- Sufficient time is not there to perform complete testing before releasing products
- Poor or non-existent error checking in applications which leads to “Buffer Overflow Attacks”

3. Shrink Wrap Code Attacks

- Why reinvent the wheel when you can buy off-the-shelf “libraries” and code?
- When you install an OS/Application, it comes with tons of sample scripts to make the life of an administrator easy
- The problem is “not fine tuning” or customizing these scripts

3. Shrink Wrap Code Attacks (Cont'd)

```

01522 Private Function CleanUpLine(ByVal sLine As String) As String
01523     Dim lQuoteCount As Long
01524     Dim lcount As Long
01525     Dim sChar As String
01526     Dim sPrevChar As String
01527
01528     ' Starts with Rem it is a comment
01529     sLine = Trim(sLine)
01530     If Left(sLine, 3) = "Rem" Then
01531         CleanUpLine = ""
01532         Exit Function
01533     End If
01534
01535     ' Starts with ' it is a comment
01536     If Left(sLine, 1) = "'" Then
01537         CleanUpLine = ""
01538         Exit Function
01539     End If
01540
01541     ' Contains ' may end in a comment, so test if it is a comment or in the
01542     ' body of a string
01543     If InStr(sLine, "'") > 0 Then
01544         sPrevChar = ""
01545         lQuoteCount = 0
01546
01547         For lcount = 1 To Len(sLine)
01548             sChar = Mid(sLine, lcount, 1)
01549
01550             ' If we found ' then an even number of " characters in front
01551             ' means it is the start of a comment, and odd number means it is
01552             ' part of a string
01553             If sChar = "'" And sPrevChar = "'" Then
01554                 If lQuoteCount Mod 2 = 0 Then
01555                     sLine = Trim(Left(sLine, lcount - 1))
01556                     Exit For
01557                 End If
01558             ElseIf sChar = "" Then
01559                 lQuoteCount = lQuoteCount + 1
01560             End If
01561             sPrevChar = sChar
01562         Next lcount
01563     End If
01564
01565     CleanUpLine = sLine
01566 End Function

```

4. Misconfiguration Attacks

- Systems that should be fairly secure are hacked because they were not configured correctly
- Systems are complex and the administrator does not have the necessary skills or resources to fix the problem
- Administrator will create a simple configuration that works
- In order to maximize your chances of configuring a machine correctly, remove any unneeded service and software

Remember This Rule!

- If a hacker really want 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

Hacker Classes

- Black Hats
- White Hats
- Gray Hats
- Suicide Hackers

Can Hacking be Ethical

- **Hacker:** Refers to a person who enjoys learning the detail of computer systems and to stretch his capabilities
- **Cracker:** Refer to a person who uses his hacking skills for offensive purpose
- **Hacking:** Describes the repid development of new programs or the reverse engineeing of the already existing software to make the code better and more efficient
- **Ethical hacker:** Refers to security professionals who apply their hacking hacking skills for defensive purposes

What is Vulnerability Research

- Discovering vulnerabilities and designing weaknesses that will open an operating system and its applications to attack or misuse
- Includes both dynamic study of products and technologies and ongoing assessment of the hacking underground
- Relevant innovations are released in the form of alerts and are delivered within product improvement for security systems
- Can be classified based on
 - Severity level (Low, Medium ,Or high)
 - Exploit range (Local or remote)

Why Hackers Need Vulnerability Research

- To identify and correct network vulnerabilities
- To protect the network from being attacked by intruders
- To get information that helps to prevent security problems
- To Gather information about viruses
- To find weaknesses in the network and to alert the network administrator before a network attack
- To know how to recover from a network attack

Vulnerability Research Websites

- www.nist.gov
- www.cisecurity.org
- www.microsoft.com/security
- www.packetstormsecurity.com
- www.hackstorm.com
- www.hackerwatch.org
- www.securityfocus.com
- www.securitymagazine.com

National Vulnerability Database



Sponsored by
DHS National Cyber Security Division/US-CERT



NIST
National Institute of
Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities	Checklists	Product Dictionary	Impact Metrics	Data Feeds	Statistics
Home	ISAP/SCAP	SCAP Validated Tools	SCAP Events	About	Contact
					Vendor Comments

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

There are **126** matching records. Displaying matches 1 through 20.

[Next 20 Matches](#)

CVE-2007-1748 **TA07-128A** **TA07-103A** **YU#555920**
oval:org.mitre.oval:def:1228

Summary: Stack-based buffer overflow in the RPC interface in the Domain Name System (DNS) Server Service in Microsoft Windows 2000 Server SP 4, Server 2003 SP 1, and Server 2003 SP 2 allows remote attackers to execute arbitrary code via a long zone name containing character constants represented by escape sequences.

Published: 4/13/2007
CVSS Severity: 10.0 (High)

Resource Status

NVD contains:
29705 [CVE Vulnerabilities](#)
150 [Checklists](#)
132 [US-CERT Alerts](#)
2152 [US-CERT Vuln Notes](#)
3171 [OVAL Queries](#)
13723 [Vulnerable Products](#)
Last updated: 02/25/08

CVE-2006-7052

Summary: Multiple PHP remote file inclusion vulnerabilities in DotWidget For Articles (dotwidgeta) 0.2 allow remote attackers to execute arbitrary code via a URL in the (1) file_path parameter to (a) index.php, (b) showcatpicks.php, and (c) showarticle.php; and the (2) admin_header_file and (3) admin_footer_file parameters to (d) admin/authors.php, (e) admin/index.php, (f) admin/categories.php, (g) admin/editconfig.php, and (h) admin/articles.php.

Published: 2/23/2007
CVSS Severity: 10.0 (High)

CVE-2006-6199

Exploit-db.com

EXPLOIT DATABASE

Currently Archiving **15412** Exploits
Updated (CVE And Archive): **Sun Jan 1 2012**

HOME BLOG GHDB ABOUT REMOTE LOCAL WEB DOS SHELLCODE PAPERS SEARCH SUBMIT

DOWNLOAD acunetix Web Vulnerability Scanner

The Exploit Database

The Exploit Database (EDB) - an ultimate archive of exploits and vulnerable software. A great resource for penetration testers, vulnerability researchers, and security addicts alike. Our aim is to collect exploits from submittals and mailing lists and concentrate them in one, easy to navigate database.

GOOGLE HACKING-DATABASE

WordPress TimThumb Exploitation
vbSEO - From XSS to Reverse PHP Shell
Owned and Exposed

Remote Exploits

Date	D	A	V	Description	Plat.	Author
2011-12-30	↓	-	✓	Reaver WiFi Protected Setup Exploit	3102 hardware	cheffner

How to Conduct Ethical Hacking

- Step 1: Talk to your client on the needs of testing
- Step 2: Prepare NDA document and ask the client to sign them
- Step 3: Prepare an ethical hacking team and draw up schedule for testing
- Step 4: Conduct the test
- Step 5: Analyze the results and prepare a report
- Step 6: Deliver the report to the client

Ethical hacking Testing

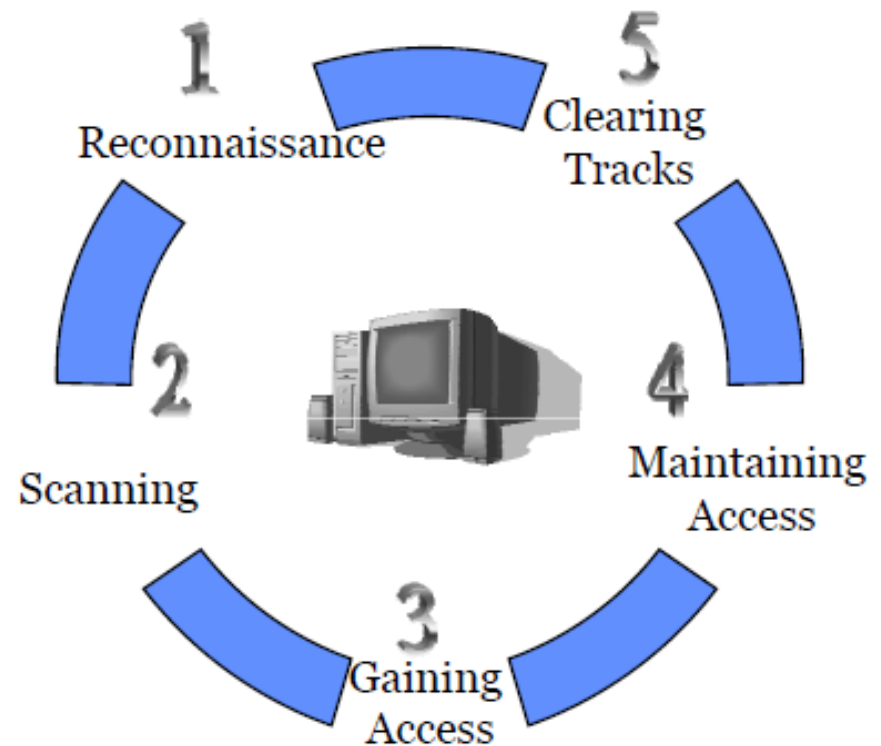
- Approaches to testing are shown below:
 - Black box: with no prior knowledge of the infrastructure to be tested
 - White box: With a complete knowledge of the network infrastructure
 - Gray box: Also known as internal Testing. It examines the extent of the access by insiders

Hacking methodology

- EC – Council Hacking Methodology
- Foundstone Hacking Methodology
- Hacking Exposed Methodology

EC-Council Hacking Methodology

- Foot printing
- Scanning
- Enumeration
- Gaining Access
- Maintaining Access
- Covering Tracks



Security Testing Framework

- Open source security testing methodology manual (OSSTMM)
- SP 800-115 NIST Publication
- The Information System Security Assessment Framework (ISSAF)

NIST SP800-115: Technical Guide to Information Security Testing (Draft)

Release date: Nov 14, 2007

Replace: SP800-42

The publication provides practical recommendations for designing, implementing, and maintaining technical information security testing processes and procedures.

SP 800-115 provides an overview of key elements of security testing, with an emphasis on technical testing techniques, the benefits and limitations of each technique, and recommendations for their use.

Information Security Testing Overview

Information security testing is the process of validating the effective implementation of security controls for information systems and networks, based on the organization's security requirements.

Technical information security testing can identify, validate, and assess technical vulnerabilities, which helps organizations to understand and improve the security posture of their systems and networks.

Security testing is required by FISMA and other regulations.

Information Security Testing Methodology

The testing methodology should contain at least the following phases:

Planning

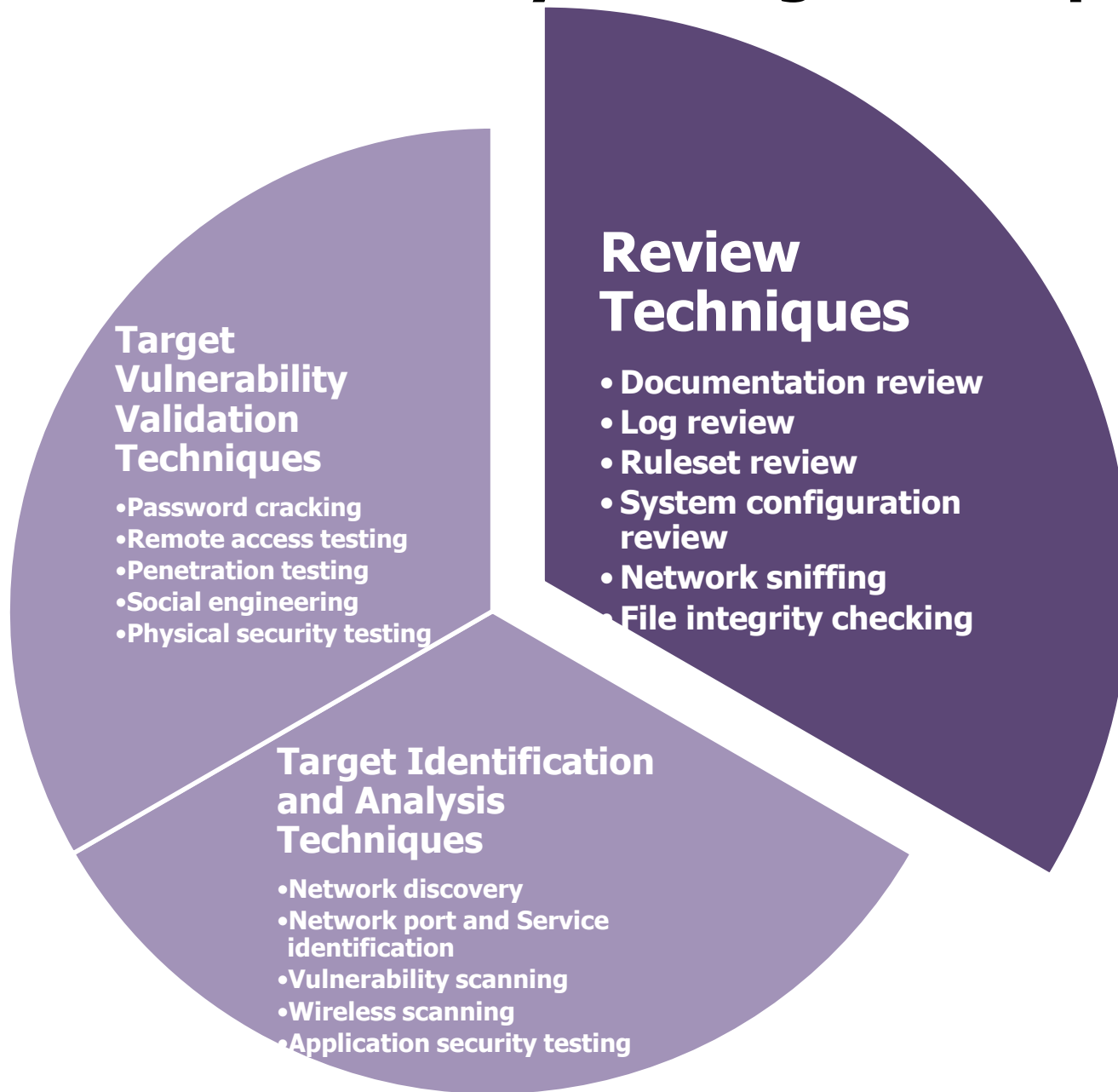
Execution

Post-Execution

NIST does not endorse one methodology over another; the intent is to provide options to organizations so they can make an informed decision to adopt an existing methodology or take several others to develop a unique methodology that best suits the organization.

One of these methodologies was created by NIST and is documented in Special Publication (SP) 800-53A, Guide for Assessing the Security Controls in Federal Information Systems (Draft), which offers suggestions for assessing the effectiveness of security controls recommended in NIST SP 800-53

Information Security Testing Techniques



Review Techniques: Documentation Review

**Documents to
review for
technical accuracy
and completeness
include**

Security policies

Architectures

Requirements

**Standard
operating
procedure
s**

**System
security
plans and
authorizatio
n
agreements**

**Memoranda
of
understandin
g and
agreement
for system
inter-
connections**

**Incident
response
plans**

Review Techniques:

Log Review

The following are examples of log information that may be useful when conducting security testing:

- Authentication server or system logs may include successful and failed authentication attempts.
- System logs may include system and service startup and shutdown information, installation of unauthorized software, file accesses, security policy changes, account changes (e.g., account creation and deletion, account privilege assignment), and use of privileges.
- Intrusion detection and prevention system logs may include malicious activity and inappropriate use.

Review Techniques:

Log Review (2)

- Firewall and router logs may include outbound connections that indicate compromised internal devices (e.g., rootkits, bots, Trojan horses, spyware).
- Firewall logs may include unauthorized connection attempts and inappropriate use.
- Application logs may include unauthorized connection attempts, account changes, use of privileges, and application or database usage information.
- Antivirus logs may include update failures and other indications of outdated signatures and software.
- Security logs, in particular patch management and some IDS and intrusion Prevention system (IPS) products, may record information on known vulnerable services and applications.

Review Techniques: Log Review (2)

NIST SP 800-92, Guide to Security Log Management

provides more information on security log management methods and techniques, including log review.

It is available at <http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf>

CDIC2007 LAB: How to centralize and audit log / How to write IT Audit Report and present Audit Result

Review Techniques:

Ruleset Review

Router access control lists

- Each rule is still required (for example, rules that were added for temporary purposes are removed as soon as they are no longer needed).
- Only traffic that is authorized per policy is permitted and all other traffic is denied by default.

Firewall rulesets

- Each rule is still required.
- The rules enforce least privilege access, such as specifying only required IP addresses and ports.
- More specific rules are triggered before general rules.
- There are no unnecessary open ports that could be closed to tighten the perimeter security.
- The ruleset does not allow traffic to bypass other security defenses.
- For host-based firewall rulesets, the rules do not indicate the presence of backdoors, spyware activity, or prohibited applications such as peer-to-peer file sharing programs.

IDS/IPS rulesets

- Unnecessary signatures have been disabled or removed to eliminate false positives and improve performance.
- Necessary signatures are enabled and have been fine-tuned and properly maintained.

Review Techniques:

System Configuration Review

System configuration review is the process of identifying weaknesses in security configuration controls, such as

- Systems not being hardened properly
- Not being configured according to security policies.

For example, system configuration review will

- ❖ Reveal unnecessary services and applications
- ❖ Improper user account and password settings
- ❖ Improper logging and backup settings

Review Techniques:

System Configuration Review (2)

Testers using manual review techniques use security **configuration guides or checklists** to verify that system settings are configured to minimize security risks

NIST maintains a repository of security configuration checklists for IT products at <http://checklists.nist.gov>

NIST SP800-70: Security Configuration Checklists Program for IT Products



Defense Information Systems Agency
Department of Defense



The name of the organization and authors that produce the checklist

- Center for Internet Security (CIS)
- Citadel Security Software
- Defense Information Systems Agency (DISA)
- National Security Agency (NSA)
- NIST, Computer Security Division
- ThreatGuard
- HP, Kyocera Mita America INC, LJK Software, Microsoft Corporation

Example:

CISCO Router and Switch

- National Security Agency (NSA)
 - Router Security Configuration Guide
 - http://www.nsa.gov/snac/downloads_cisco.cfm
- Center for Internet Security (CIS)
 - Gold Standard Benchmark for Cisco IOS, Level 1 and 2 Benchmarks
 - **Documents**
 - **Tool - RAT (Router Auditing Tool) Version 2.2 Update Nov 20, 2007**
- Defense Information Security Agency (DISA)
 - Network Checklist Version 7, Release 1.1 Update Nov, 2007
 - Defense Switched Network Checklist Version 2, Release 3.2 Update Nov 24, 2006

Hacking Methodology



ACIS Professional Center

Footprinting

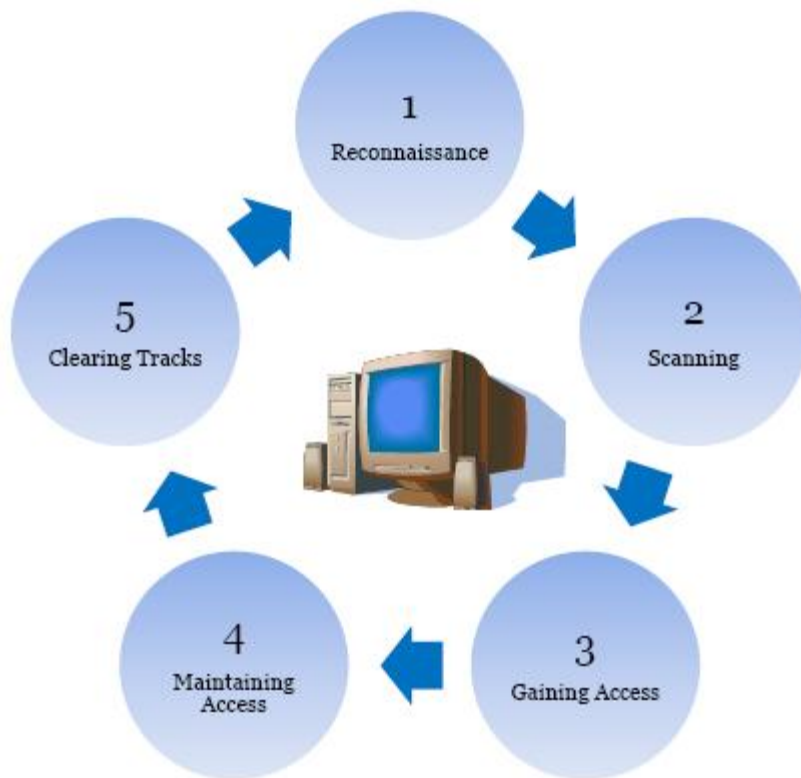


ACIS Professional Center

Module Objective

- This module will familiarize you with:
 - Overview of the Reconnaissance Phase
 - Footprinting: An Introduction
 - Information Gathering Methodology of Hackers
 - Competitive Intelligence gathering
 - Tools that aid in Footprinting

Revisiting 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
- It involves network scanning, either external or internal, without authorization

Defining Footprinting

- Footprinting is the blueprint of the security profile of an organization, undertaken in a methodological manner
- Footprinting is one of the three pre-attack phases
- An attacker spends 90% of the time in profiling an organization and another 10% in launching the attack
- Footprinting results in a unique organization profile with respect to networks
(Internet/intranet/extranet/wireless) and systems involved

Areas and Information which Attackers Seek

Internet

- Domain Name
- Network blocks
- IP addresses of reachable systems
- TCP and UDP services running
- System architecture
- ACLs
- IDSes running
- System enumeration (user and group names, system banners, routing tables, and SNMP info)

Remote access

- Analog/digital telephone numbers
- Remote system type
- Authentication mechanisms

Intranet

- Networking protocols used
- Internal domain names
- Network blocks
- IP addresses of reachable systems
- TCP and UDP services running
- System architecture
- ACLs
- IDSes running
- System enumeration

Extranet

- Connection origination and destination
- Type of connection
- Access control mechanism

Information Gathering



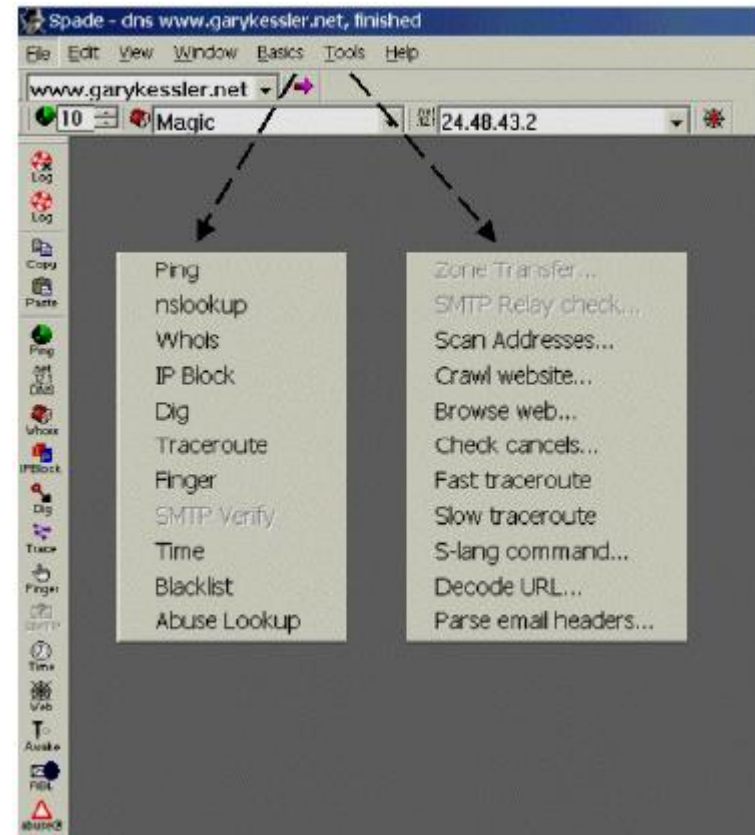
ACIS Professional Center

Information Gathering Methodology

- Unearth initial information
- Locate the network range
- Ascertain active machines
- Discover open ports/access points
- Detect operating systems
- Uncover services on ports
- Map the network

Unearthing Initial Information

- Hacking tool
- Sam Spade
- Commonly includes:
 - Domain name lookup
 - Locations
 - Contacts (telephone / mail)
- Information Sources:
 - Open source
 - Whois
 - Nslookup



Extracting Archive of of a Website

- You can get all information of a company's website since the time it was launched at www.archive.org
For example : www.eccouncil.org
- You can see updates made to the website
- You can look for employee's database, past products, press releases, contact information, and more

www.archive.org



[Web](#) | [Moving Images](#) | [Texts](#) | [Audio](#) | [Software](#) | [Education](#) | [Patron Info](#) | [About IA](#)
[Forums](#) | [FAQs](#) | [Contributions](#) | [Jobs](#) | [Donate](#)
 Search: All Media Types

Universal access
to human knowledge


[Upload](#) Anonymous User ([login](#) or [join us](#))


Announcements [\(more\)](#)
[Zotero and Internet Archive join forces](#)
[80 Libraries Going Open](#)
[More bandwidth](#)

Web 85 billion pages


[Take Me Back](#) [Advanced Search](#)

Welcome to the Archive [RSS](#)
 The Internet Archive is building a digital library of Internet sites and other cultural artifacts in digital form. Like a paper library, we provide free access to researchers, historians, scholars, and the general public.

Moving Images 
 115,146 movies
[Browse](#) [\(by keyword\)](#)
Curator's Choice [\(more\)](#)

Star Wars: The Han Solo Affair
 Official Star Wars parody from Site

Live Music Archive 
 47,053 concerts
[Browse](#) [\(by band\)](#)
Curator's Choice [\(more\)](#)

Live music archive
[Hot Buttered Rum Live at Great American Music...](#)
 Set / Flask Alas! Virginia's Gnn Evolution> Angeline>Cindy Firefly Idaho Pines Sugaree Well Oiled...

Audio 
 231,411 recordings
[Browse](#) [\(by keyword\)](#)
Curator's Choice [\(more\)](#)

open source audio
[Bathroom Sink](#)
 Being yourself is where it's at.

Texts 
 348,856 texts
[Browse](#) [\(by keyword\)](#)
Curator's Choice [\(more\)](#)


www.archive.org (con'd)

Enter Web Address: All [Adv. Search](#) [Compare Archive Pages](#)

<http://microsoft.com> 1866 Results

ates are not shown. [See all.](#)

ite was updated.

becomes available here 6 months after collection. [See FAQ.](#)

Search Results for Jan 01, 1996 - Aug 26, 2007

1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007
0 pages	2 pages	19 pages	103 pages	263 pages	139 pages	28 pages	146 pages	304 pages	152 pages	94 pages
Dec 05, 1998 *	Jan 17, 1999 *	Feb 29, 2000 *	Jan 03, 2001 *	Jan 21, 2002 *	Jan 30, 2003 *	Feb 08, 2004 *	Jan 04, 2005 *	Jan 01, 2006 *	Jan 02, 2007	
Dec 12, 1998 *	Jan 25, 1999 *	Mar 01, 2000	Jan 03, 2001 *	Jan 25, 2002 *	Feb 08, 2003 *	Feb 09, 2004	Jan 10, 2005 *	Jan 01, 2006 *	Jan 03, 2007	
	Feb 03, 1999 *	Mar 02, 2000	Jan 04, 2001	Jan 27, 2002 *	Feb 20, 2003 *	Mar 25, 2004 *	Jan 15, 2005 *	Jan 01, 2006 *	Jan 07, 2007 *	
	Feb 08, 1999 *	Mar 02, 2000 *	Jan 05, 2001	Jun 03, 2002 *	Mar 21, 2003 *	Apr 01, 2004 *	Jan 16, 2005 *	Jan 01, 2006 *	Jan 07, 2007 *	
	Feb 18, 1999 *	Mar 02, 2000 *	Jan 06, 2001 *	Jun 04, 2002 *	Mar 24, 2003 *	Apr 10, 2004 *	Jan 18, 2005 *	Jan 01, 2006 *	Jan 08, 2007	
	Feb 22, 1999 *	Mar 03, 2000	Jan 06, 2001 *	Jun 05, 2002	Mar 28, 2003 *	Apr 15, 2004 *	Jan 20, 2005 *	Jan 01, 2006 *	Jan 12, 2007	
	Feb 29, 1999 *	Mar 03, 2000 *	Jan 07, 2001	Jul 01, 2002 *	Apr 11, 2003 *	Apr 18, 2004 *	Jan 21, 2005 *	Jan 02, 2006 *	Jan 14, 2007	
	Apr 22, 1999 *	Mar 04, 2000	Jan 08, 2001	Jul 02, 2002	May 05, 2003 *	May 18, 2004 *	Jan 22, 2005 *	Jan 02, 2006 *	Jan 17, 2007	
	Apr 23, 1999	Apr 07, 2000 *	Jan 08, 2001 *	Jul 03, 2002	May 13, 2003 *	May 22, 2004	Jan 24, 2005 *	Jan 02, 2006 *	Jan 25, 2007	
	Apr 28, 1999 *	Apr 09, 2000 *	Jan 09, 2001 *	Jul 03, 2002 *	May 29, 2003 *	May 26, 2004 *	Jan 25, 2005 *	Jan 02, 2006 *	Jan 26, 2007	
	Apr 29, 1999 *	May 10, 2000 *	Jan 09, 2001	Jul 04, 2002	Jun 18, 2003 *	Jun 08, 2004 *	Jan 27, 2005 *	Jan 02, 2006 *	Jan 28, 2007	
	May 01, 1999 *	May 10, 2000	Jan 18, 2001 *	Jul 07, 2002 *	Jun 18, 2003 *	Jun 09, 2004 *	Jan 29, 2005 *	Jan 03, 2006 *	Jan 29, 2007	
	May 06, 1999 *	May 10, 2000 *	Jan 18, 2001	Jul 08, 2002	Jun 23, 2003 *	Jun 10, 2004	Jan 29, 2005 *	Jan 03, 2006 *	Jan 30, 2007 *	
	Oct 04, 1999 *	May 11, 2000	Jan 30, 2001	Jul 09, 2002 *	Jun 24, 2003 *	Jun 10, 2004 *	Jan 30, 2005 *	Jan 03, 2006 *	Feb 02, 2007 *	
	Oct 07, 1999	May 11, 2000 *	Feb 02, 2001	Jul 11, 2002 *	Jul 17, 2003 *	Jun 12, 2004	Jan 31, 2005 *	Jan 04, 2006	Feb 02, 2007 *	

Your Privacy Exposed (Cont.)

<http://tracker.clima.me/>

Tweet List

at LH1-334 (Kasetsart University, ลาดยาว)
<http://t.co/C7nMEqGO>


BESTstm Tue, 06 Mar 2012 01:08:13

Alone mak T T (@ LH1-334) <http://t.co/gpER4YAE>


sonebouy Tue, 06 Mar 2012 01:06:13

The map shows a route in Bangkok, Thailand, with red arrows indicating movement. The route starts near the Satharanasuk 2 area and moves towards the Kasetsart University area. The map includes labels for various roads and landmarks, such as the Medical Correctional Institution, Vibhavadi Hospital, and Kasetsart University.

Your Privacy Exposed (Cont.)




[Sign up](#)
[Log in](#)



foursquare helps you keep up with friends, discover what's nearby, save money & unlock rewards

[Get Started Now](#)




Sutthima C. checked in to **LH1-334**

“ Alone mak T T


40 minutes ago via foursquare for iPhone

Only Sutthima's friends can see comments and add their own.



LH1-334
ลาดยาว, กรุงเทพมหานคร

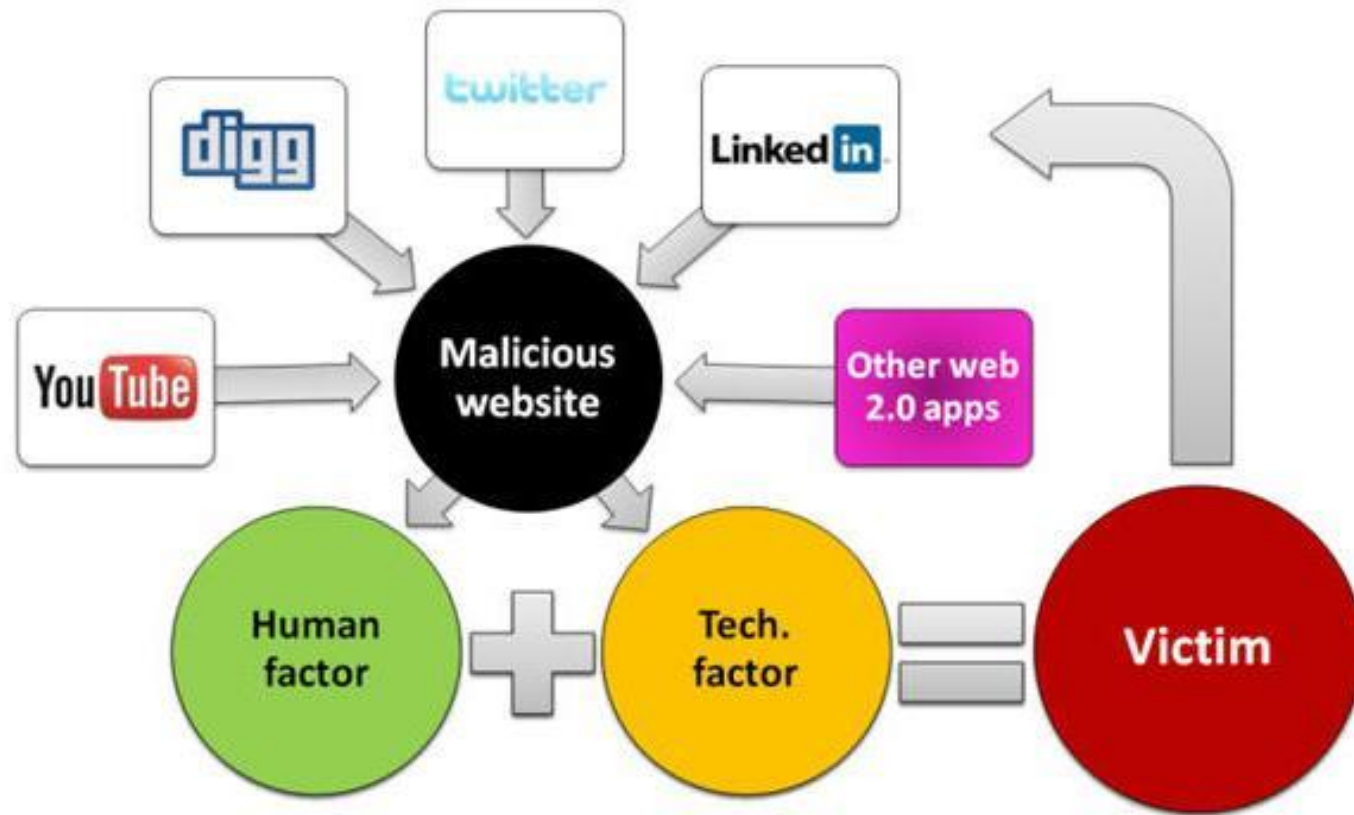
[+ Save](#) [✓ Done](#)



[Terms & Conditions](#)

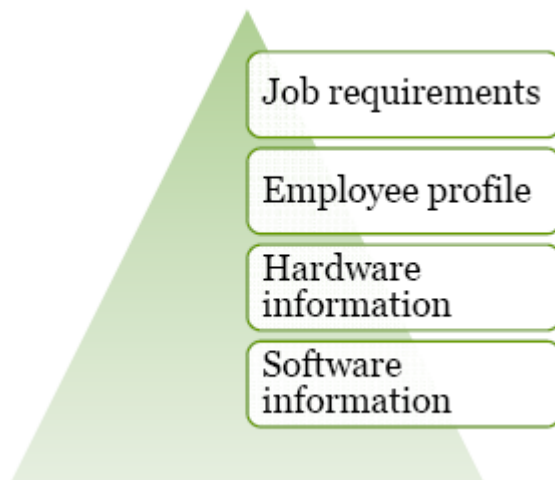
TOTAL PEOPLE	TOTAL CHECKINS	HERE NOW
46	178	5

Increasing use of Web 2.0 malware




Footprinting Through Job Sites

- You can gather company's infrastructure details from job postings
- Look for company's infrastructure postings such as "looking for system administrator to manage Solaris 10 network"
- This means that the company has Solaris networks on site
 - E.g., www.jobsdb.com



Whois


Whois

Registrant:
 targetcompany (targetcompany-DOM)
 XXX Everest Bldg, A, Inclosure
 Hyderabad
 Andrapradesh, 500018
 IN
 Domain Name: targetcompany.COM

Administrative Contact:
 #####, ##### (B/XXXX-ORG) targetcompany@domain.com
 targetcompany
 XXX, Everest Block, A, Inclosure,
 Hyderabad, Andrapradesh 500018
 IN 61 40 XXXX XXXX Fax- 61 40 XXXX XXXX

Technical Contact:
 #####, ##### (B/XXXX-ORG) techcontact@WEBHOSTA.COM
 techcontact@WEBHOSTA.COM
 408/XXX-XXXX 408/XXX-XXXX
 US 408/XXX-XXXX 408/XXX-XXXX
 Record expires on 14-Oct-200X.
 Record created on 18-Oct-1999.
 Database last updated on 17-Mar-2009 07:49:04 EST.

Domain servers in listed order:
 NS1.WEBHOSTA.COM 204.XXX.140.XXX
 NS2.WEBHOSTA.COM 204.XXX.141.XXX

Registrant:
 targetcompany (targetcompany-DOM)
 # Street Address
 City, Province
 State, Pin, Country
Domain Name: targetcompany.COM

Administrative Contact:
 Surname, Name (SNIDNo-ORG) targetcompany@domain.com
 targetcompany (targetcompany-DOM) # Street Address
 City, Province, State, Pin, Country
 Telephone: XXXXXX Fax XXXXXX

Technical Contact:
 Surname, Name (SNIDNo-ORG) targetcompany@domain.com
 targetcompany (targetcompany-DOM) # Street Address
 City, Province, State, Pin, Country
 Telephone: XXXXXX Fax XXXXXX

Domain servers in listed order:
 NS1.WEBHOST.COM XXX.XXX.XXX.XXX
 NS2.WEBHOST.COM XXX.XXX.XXX.XXX

DNS Information Extraction

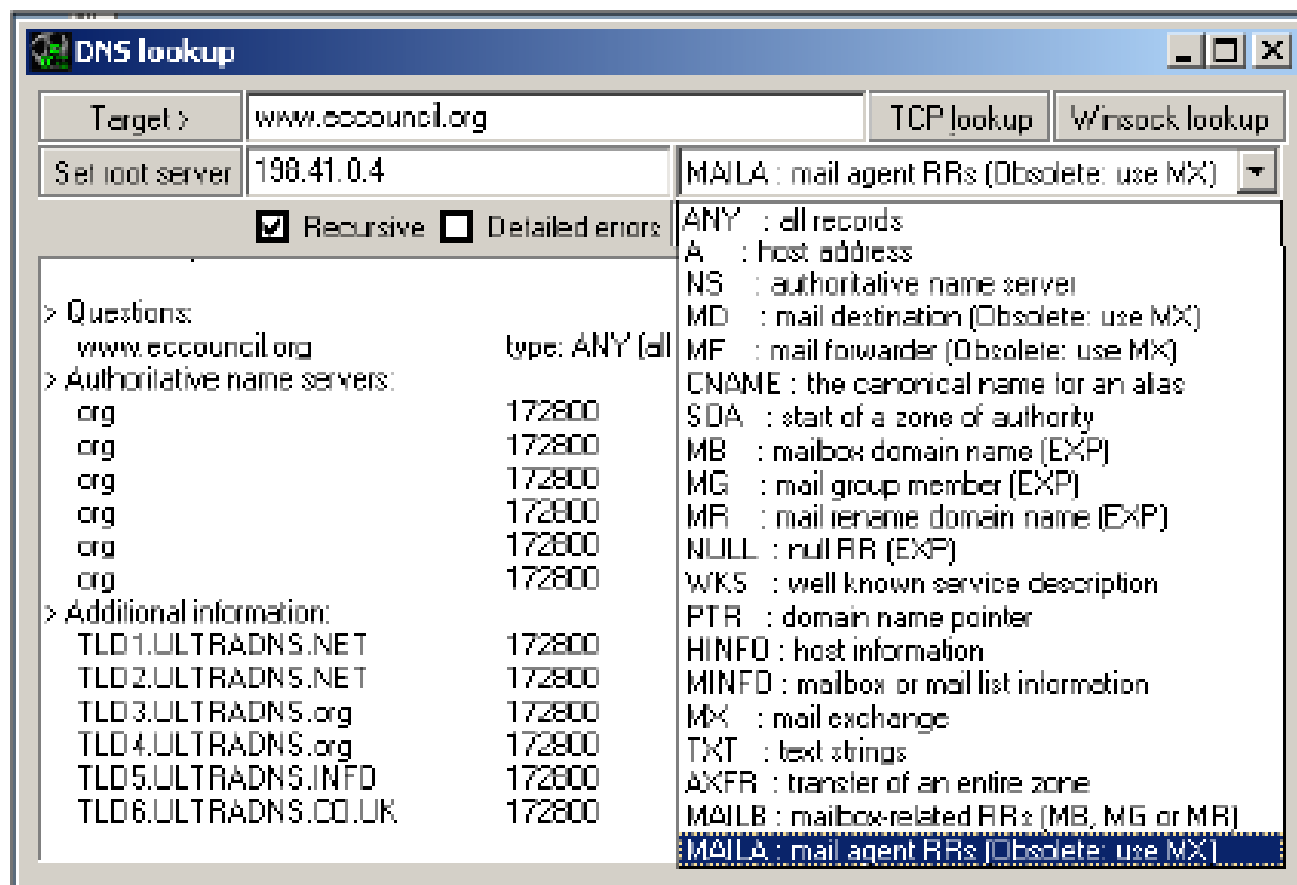


ACIS Professional Center

Types of DNS Records

A	A host's IP address. An address record allowing a computer name to be translated into an IP address. Each computer must have this record for its IP address to be located.
MX	Host's or domain's mail exchanger(s).
NS	Host's or domain's name server(s).
CNAME	Host's canonical name allows additional names or aliases to be used to locate a computer.
SOA	Indicates authority for the domain.
SRV	Service location record.
RP	Responsible person.
PTR	Host's domain name, host identified by its IP address.
TXT	Generic text record.
HINFO	Host information record with CPU type and operating system

Tool: Necrosoft Advanced DIG



Scanning



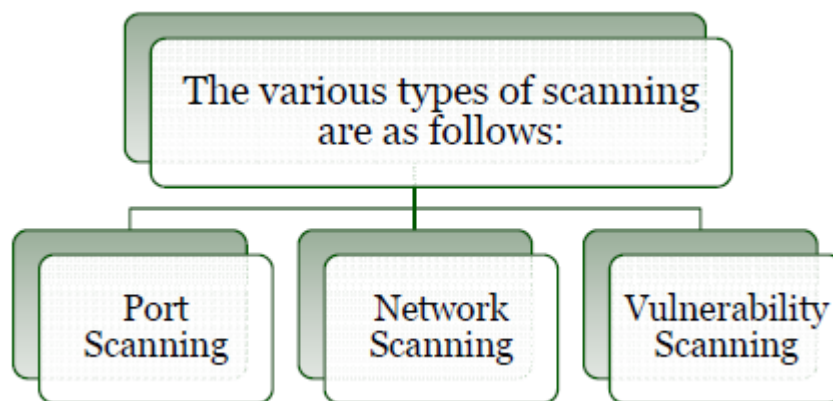
ACIS Professional Center

Objective

- Definition of scanning
- Types and objectives of scanning
- Understanding scanning methodology
- Checking live systems and open ports
- Understanding scanning techniques
- Different tools present to perform scanning
- Understanding banner grabbing and OS fingerprinting
- Drawing network diagrams of vulnerable hosts
- Preparing proxies
- Understanding anonymizers
- Scanning countermeasures

Scanning – Definition

- Scanning is one of the three components of intelligence gathering for an attacker
 - The attacker finds information about
 - Specific IP Address
 - Operating System
 - System architecture
 - Services running on each computer



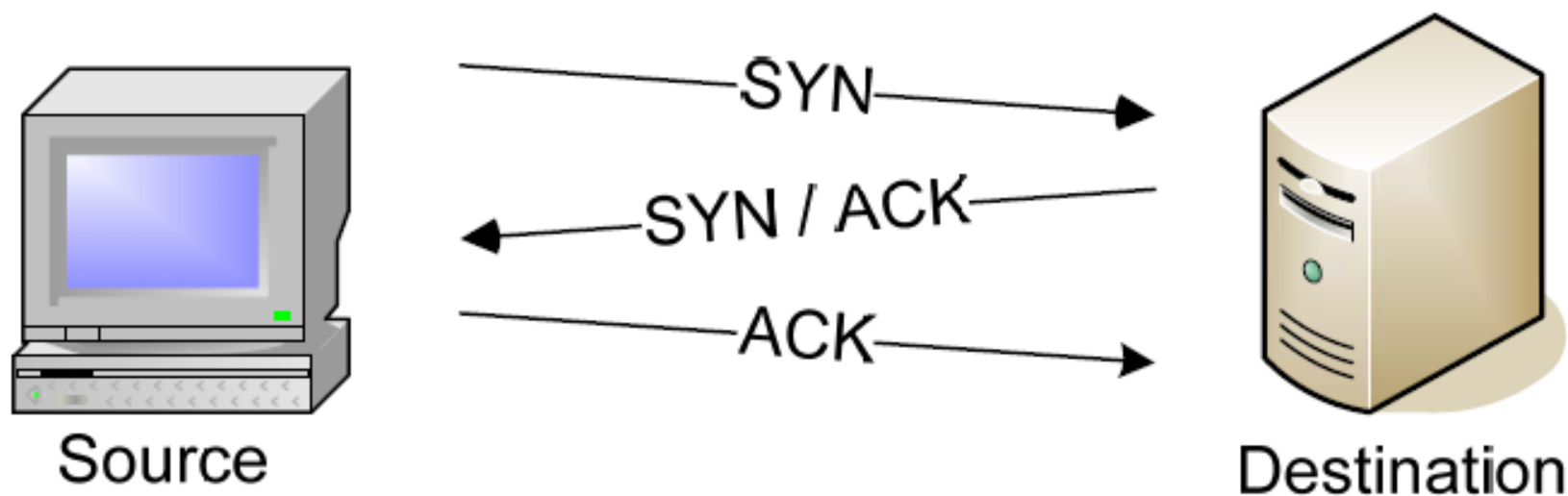
Types of Scanning

- Port Scanning
 - A series of messages sent by someone attempting to break into a computer to learn about the computer's network service
 - Each associated with a "well-know" port number
- Network Scanning
 - A procedure for identifying active on a network
 - Either for the purpose of attacking them or for network security assessment
- Vulnerability Scanning
 - The automated process of proactively identifying vulnerabilities of computing systems present in a network

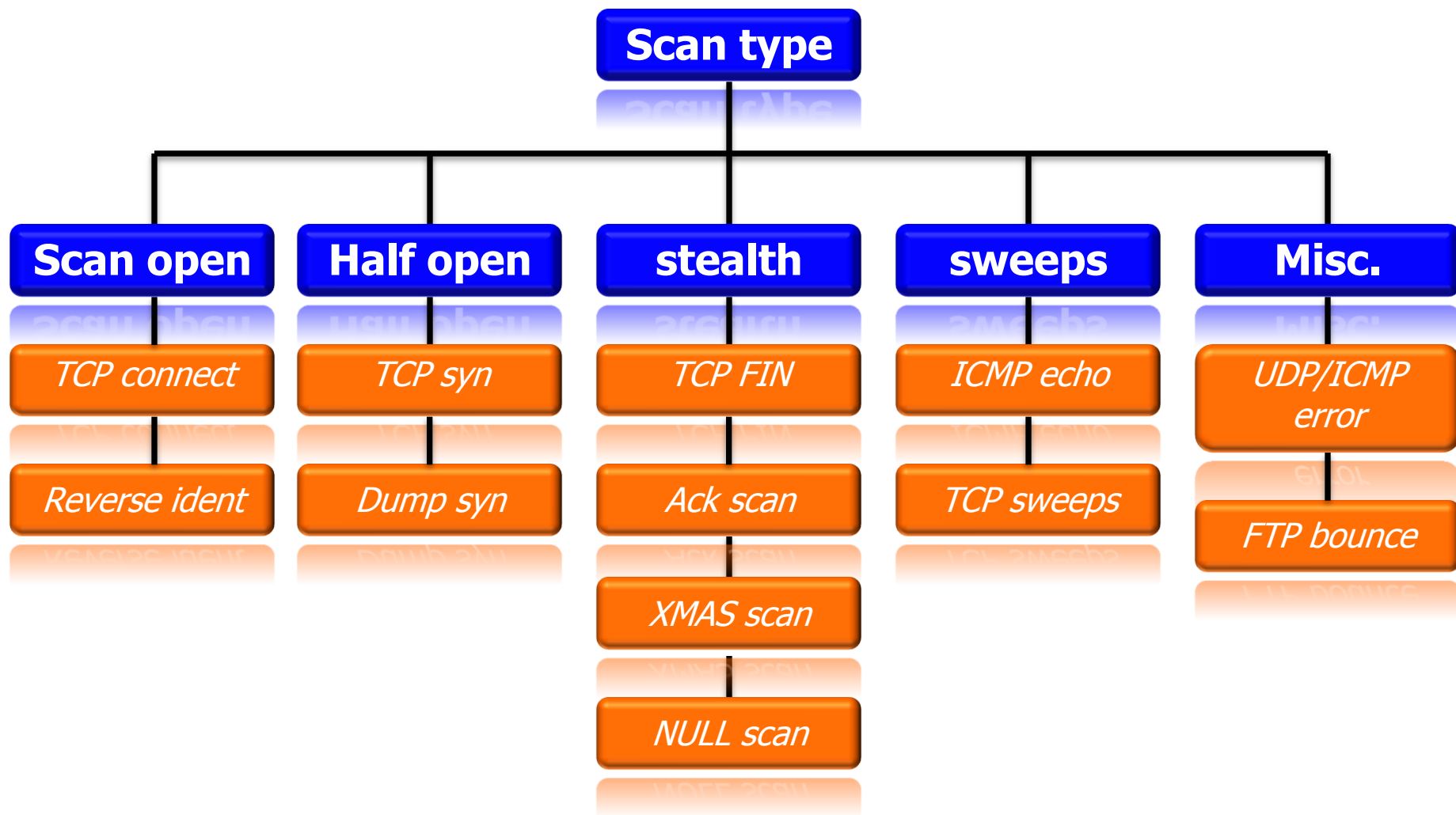
Objectives of Scanning

- To detect live systems running on the network
- To discover which ports are active/running
- To discover the operating system running on the target system(fingerprint)
- To discover the service running/listening on the target system
- To discover the IP address of the target system

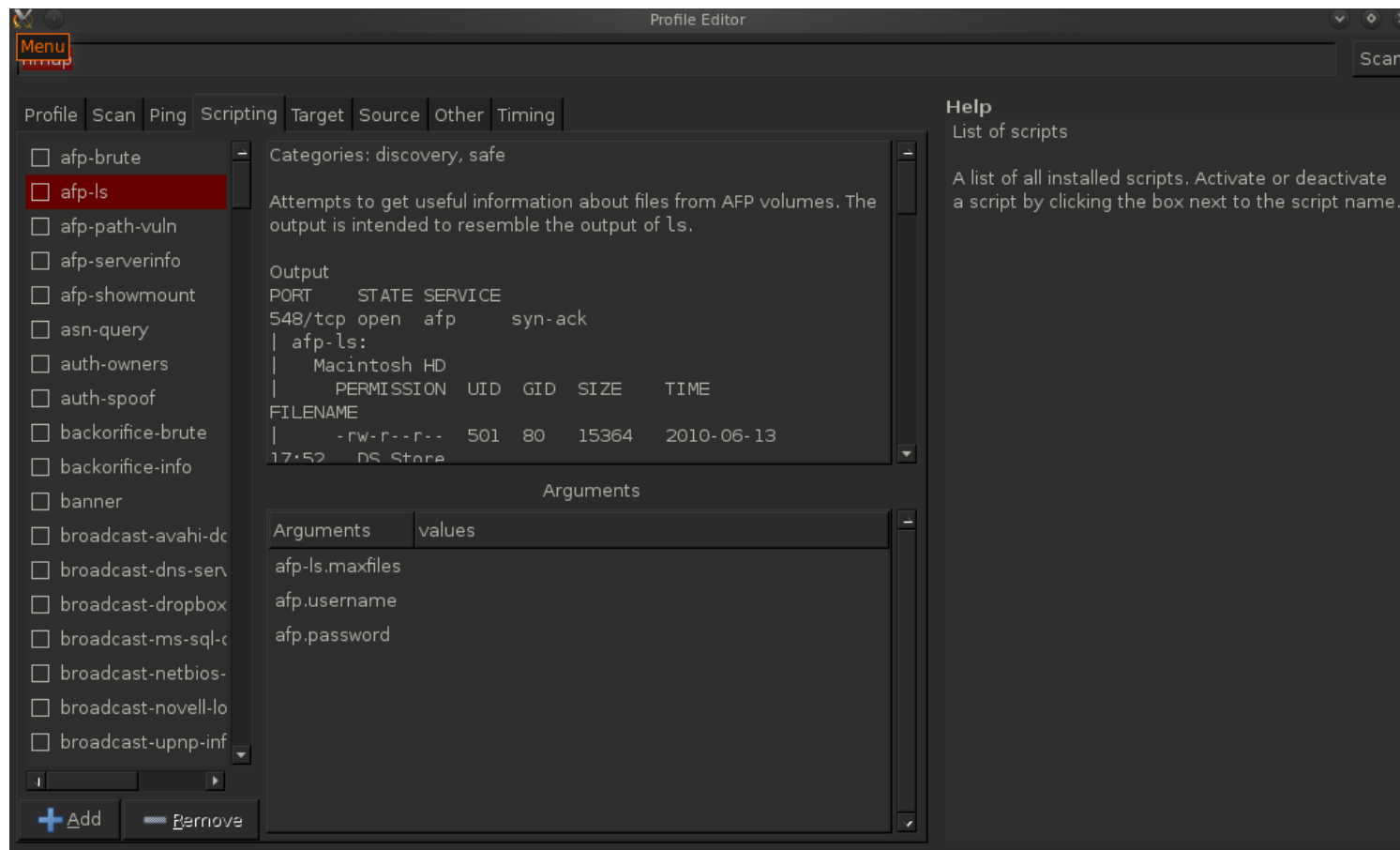
The TCP Handshake



Port Scan



Nmap



BANNER GRABBING

OS Fingerprinting

- OS fingerprinting is the method to determine the operating system that is running on the target system
 - Active stack fingerprinting
 - Passive fingerprinting

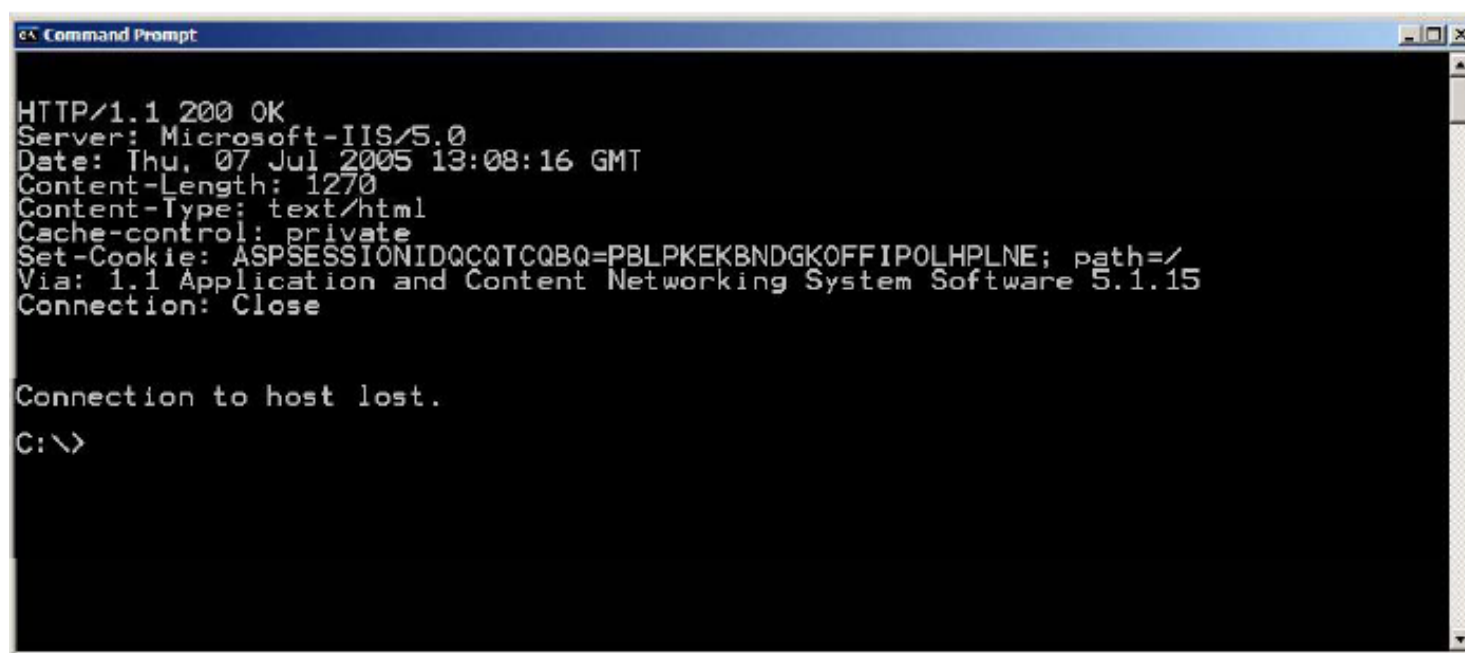
Active Stack Fingerprinting

- Based on the fact that OS Vendors implement the TCP stack differently
- Specially crafted packets are sent to remote OS and the response is noted
- The responses are then compared with a database to determine the OS
- The firewall logs your active banner grabbing scan since you are probing directly

Passive Fingerprinting

- Passive banner grabbing refers to indirectly scanning a system to reveal
- It is also based on the differential implantation of the stack and the various ways an OS responds to it
- It uses sniffing techniques instead of the scanning techniques
- It is less accurate than active fingerprinting

Active Banner Grabbing Using Telnet



```
Command Prompt

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Thu, 07 Jul 2005 13:08:16 GMT
Content-Length: 1270
Content-Type: text/html
Cache-control: private
Set-Cookie: ASPSESSIONIDQCQTCQBQ=PBLPKEKBNDGKOFFIPOLHPLNE; path=/
Via: 1.1 Application and Content Networking System Software 5.1.15
Connection: Close

Connection to host lost.
C:\>
```

P0f

```

C:\WINDOWS\System32\cmd.exe
J:\Ethical Hacking and Countermeasures v5\Module 03 - Scanning\p0f>p0f -i 2
p0f - passive os fingerprinting utility, version 2.0.4
<C> M. Zalewski <lcantuf@diuone.cc>, W. Stearns <wstearns@pobox.com>
WIN32 port <C> M. Davis <mike@datanerds.net>, K. Kuehl <kkuehl@cisco.com>
p0f: listening (SYN) on '\Device\NPF_{CCA17F4E-51D5-4A9F-918B-F59F0643E936}', 22
3 sigs (12 generic), rule: 'all'
10.0.0.11:14638 - Windows 2000 SP4, XP SP1
-> 64.90.188.178:80 (distance 0, link: ethernet/modem)
10.0.0.11:14639 - Windows 2000 SP4, XP SP1
-> 64.90.188.178:80 (distance 0, link: ethernet/modem)
10.0.0.11:14640 - Windows 2000 SP4, XP SP1
-> 64.90.188.178:80 (distance 0, link: ethernet/modem)
10.0.0.11:14641 - Windows 2000 SP4, XP SP1
-> 64.90.188.178:80 (distance 0, link: ethernet/modem)
10.0.0.11:14642 - Windows 2000 SP4, XP SP1
-> 64.90.188.178:80 (distance 0, link: ethernet/modem)
10.0.0.11:14643 - Windows 2000 SP4, XP SP1
-> 64.90.188.178:80 (distance 0, link: ethernet/modem)
10.0.0.11:14644 - Windows 2000 SP4, XP SP1
-> 64.90.188.178:80 (distance 0, link: ethernet/modem)
10.0.0.11:14645 - Windows 2000 SP4, XP SP1
-> 64.90.188.178:80 (distance 0, link: ethernet/modem)
10.0.0.11:14646 - Windows 2000 SP4, XP SP1
-> 64.90.188.178:80 (distance 0, link: ethernet/modem)

```

Disable or change banner

Apache Server

- Apache 2.x users who have the `mod_headers` module loaded can use a simple directive in their `httpd.conf` file to change banner information **Header set Server "New Server Name"**
- Apache 1.3.x users have to edit defines in `httpd.h` and recompile Apache to get the same result

IIS Server

IIS users can use following tools to disable or change banner information

IIS Lockdown Tool

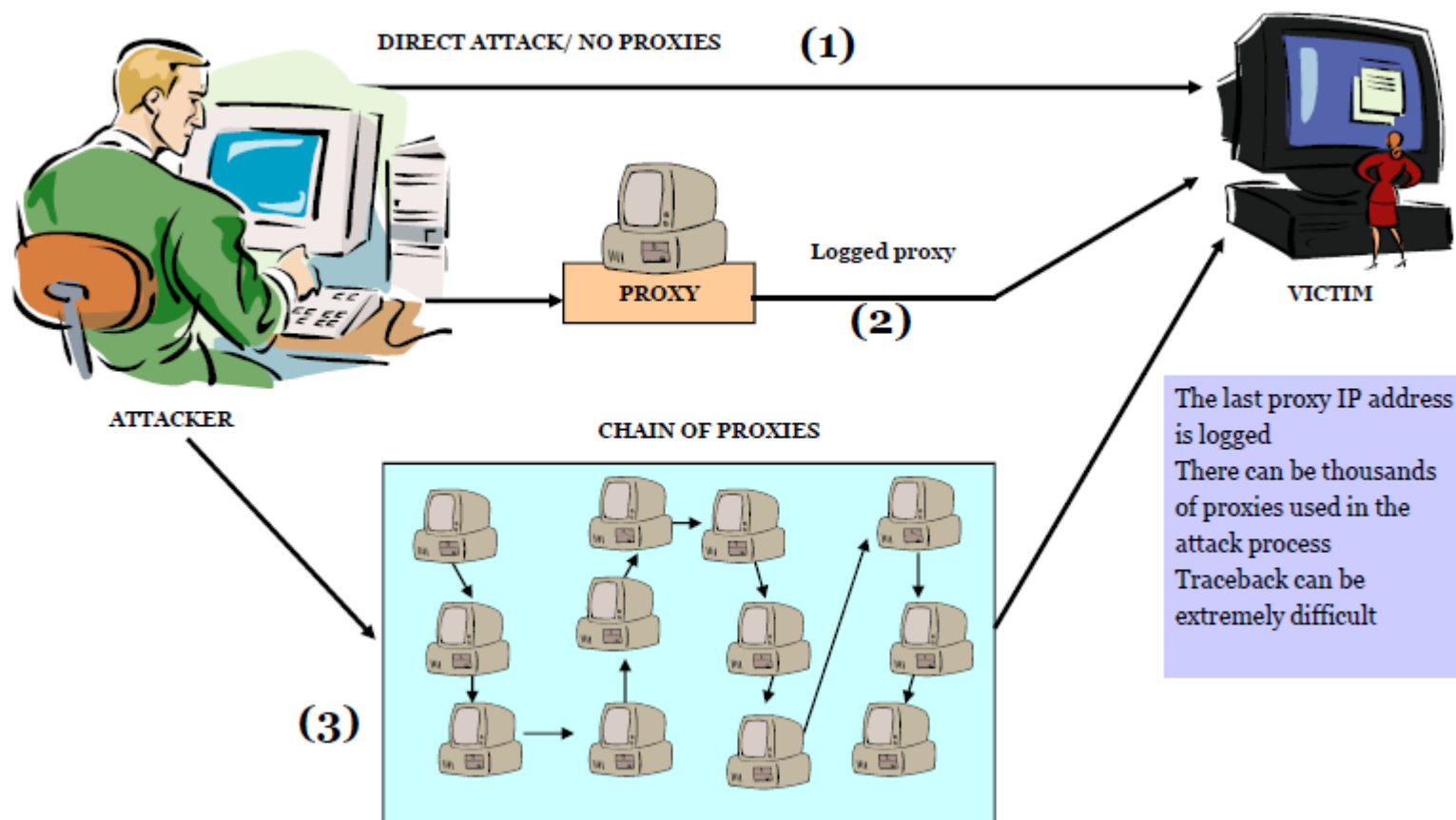
ServerMask

PREPARING PROXY

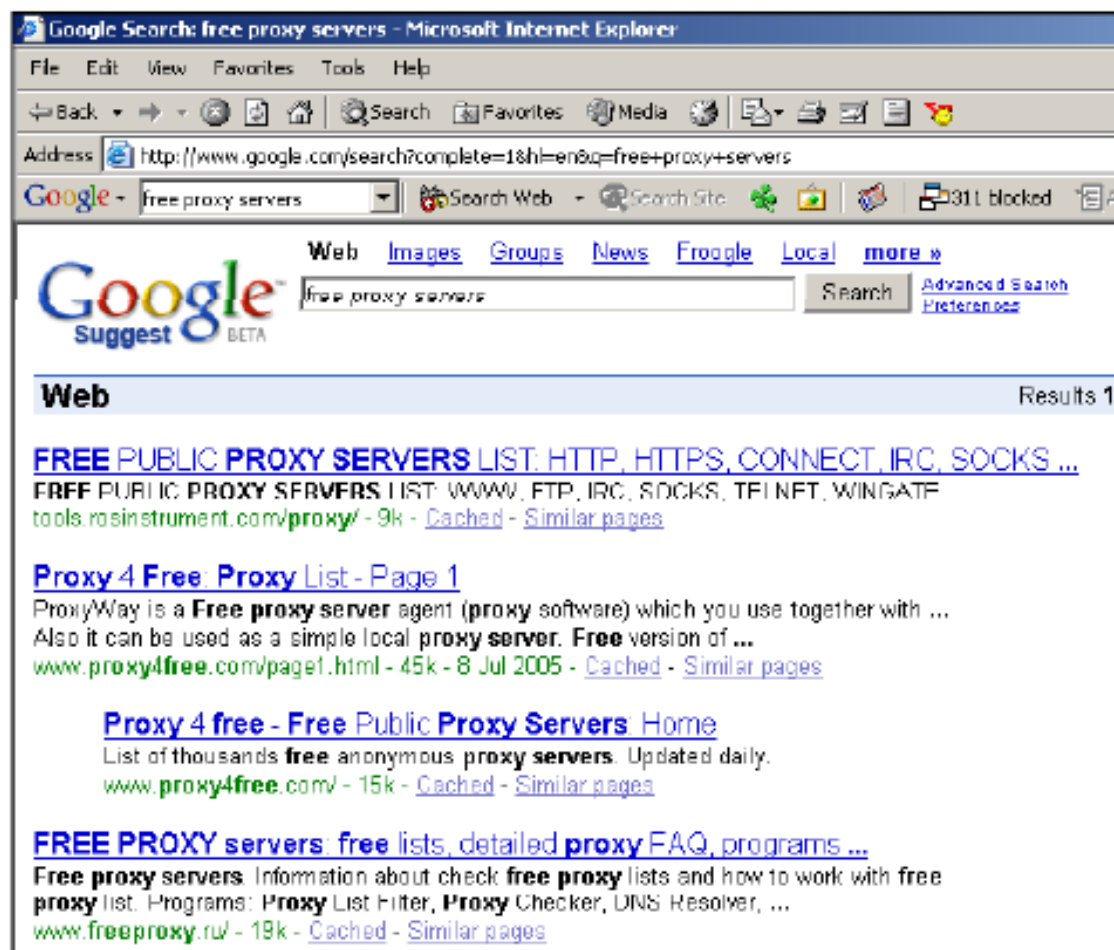
Proxy Servers

- Proxy is a network computer that can serve as an intermediate for connection with other computer
They are usually used for the following purposes:
 - As a Firewall , a proxy protect the local network from outside access
 - As an IP address multiplexer a proxy allows the connection of a number of computer to the internet when having only one IP

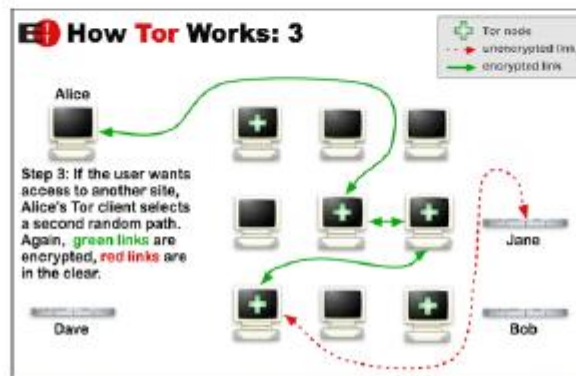
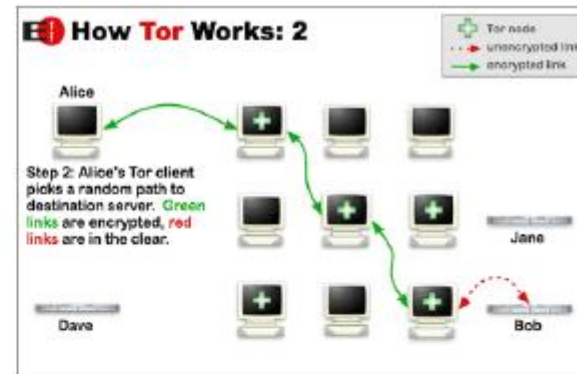
Use of Proxies for attack



Free Proxy server



TOR Proxy



Anonymous Proxy Browser

