

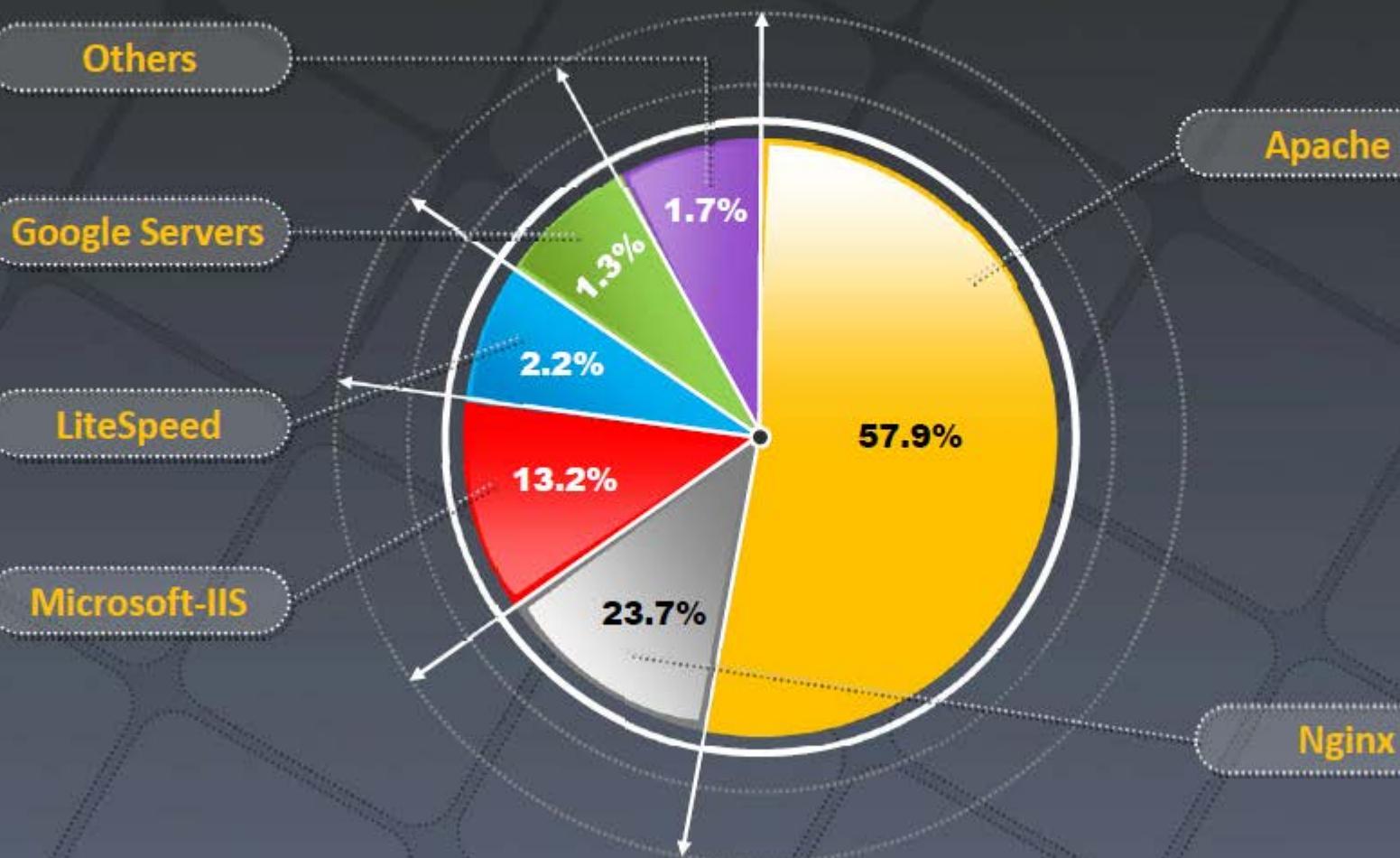
Hacking Webservers

Module 11

Unmask the Invisible Hacker.



Webserver Market Shares



<http://w3techs.com>

Module Objectives

- Understanding Webserver Concepts
- Understanding Webserver attacks
- Understanding Webserver Attack Methodology
- Webserver Attack Tools



- Countermeasures against Webserver Attacks
- Overview of Patch Management
- Webserver Security Tools
- Overview of Webserver Penetration Testing



Module Flow

CEH
Certified Ethical Hacker



**Webserver
Concepts**

1



**Webserver
Attacks**

2



**Attack
Methodology**

3



**Webserver
Attack Tools**

4



**Counter-
measures**

5



**Patch
Management**

6



**Webserver
Security Tools**

7

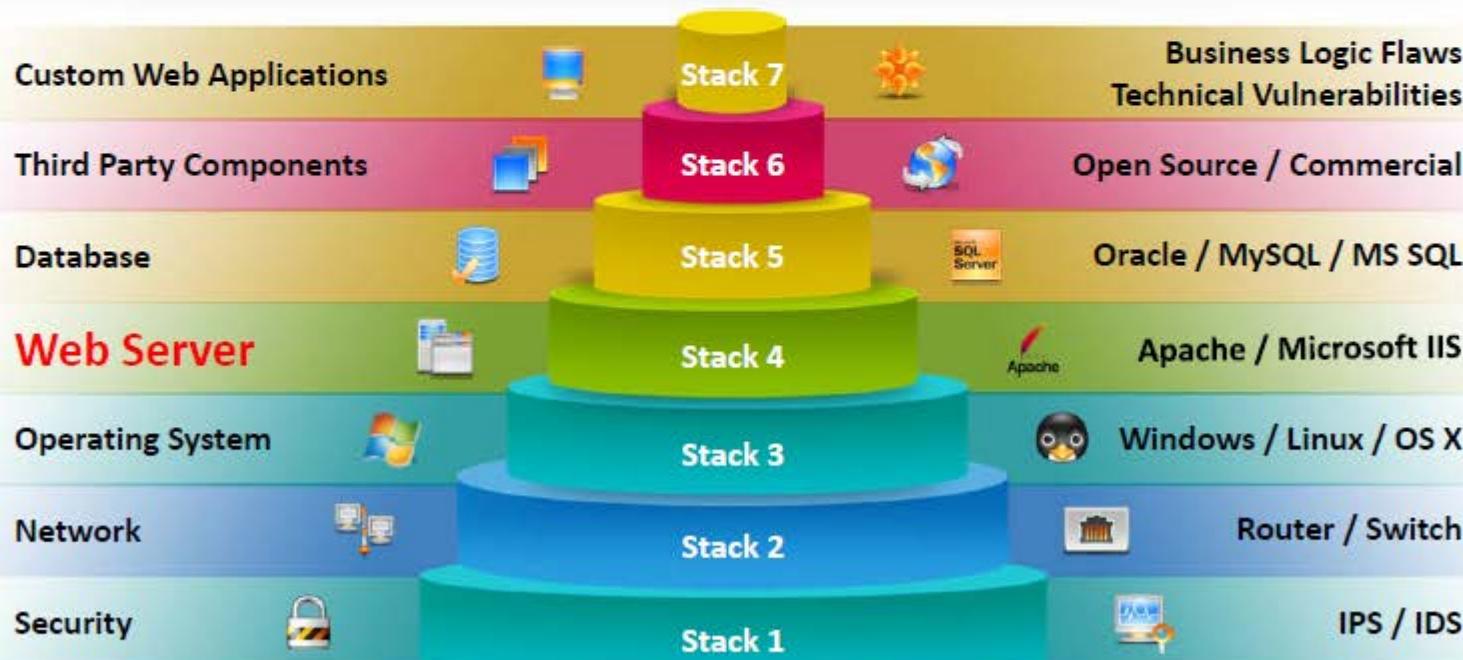


**Webserver
Pen Testing**

8

Web Server Security Issue

- Web server is a program (both hardware and software) that hosts websites; attackers usually target **software vulnerabilities** and configuration errors to compromise web servers
- Nowadays, **network** and **OS level attacks** can be well defended using proper network security measures such as firewalls, IDS, etc., however, web servers are accessible from anywhere on the web, which makes them **less secured** and **more vulnerable** to attacks



Why Web Servers Are Compromised



- Improper file and directory permissions
- Installing the server with default settings
- Unnecessary services enabled, including content management and remote administration
- Security conflicts with business ease-of-use case
- Lack of proper security policy, procedures, and maintenance
- Improper authentication with external systems
- Default accounts with their default or no passwords
- Unnecessary default, backup, or sample files
- Misconfigurations in web server, operating systems, and networks
- Bugs in server software, OS, and web applications
- Misconfigured SSL certificates and encryption settings
- Administrative or debugging functions that are enabled or accessible on web servers
- Use of self-signed certificates and default certificates

Impact of Webserver Attacks

CEH
Certified Ethical Hacker

01

Compromise of user accounts



02

Website defacement

03

Secondary attacks from the Website

04

Root access to other applications or servers

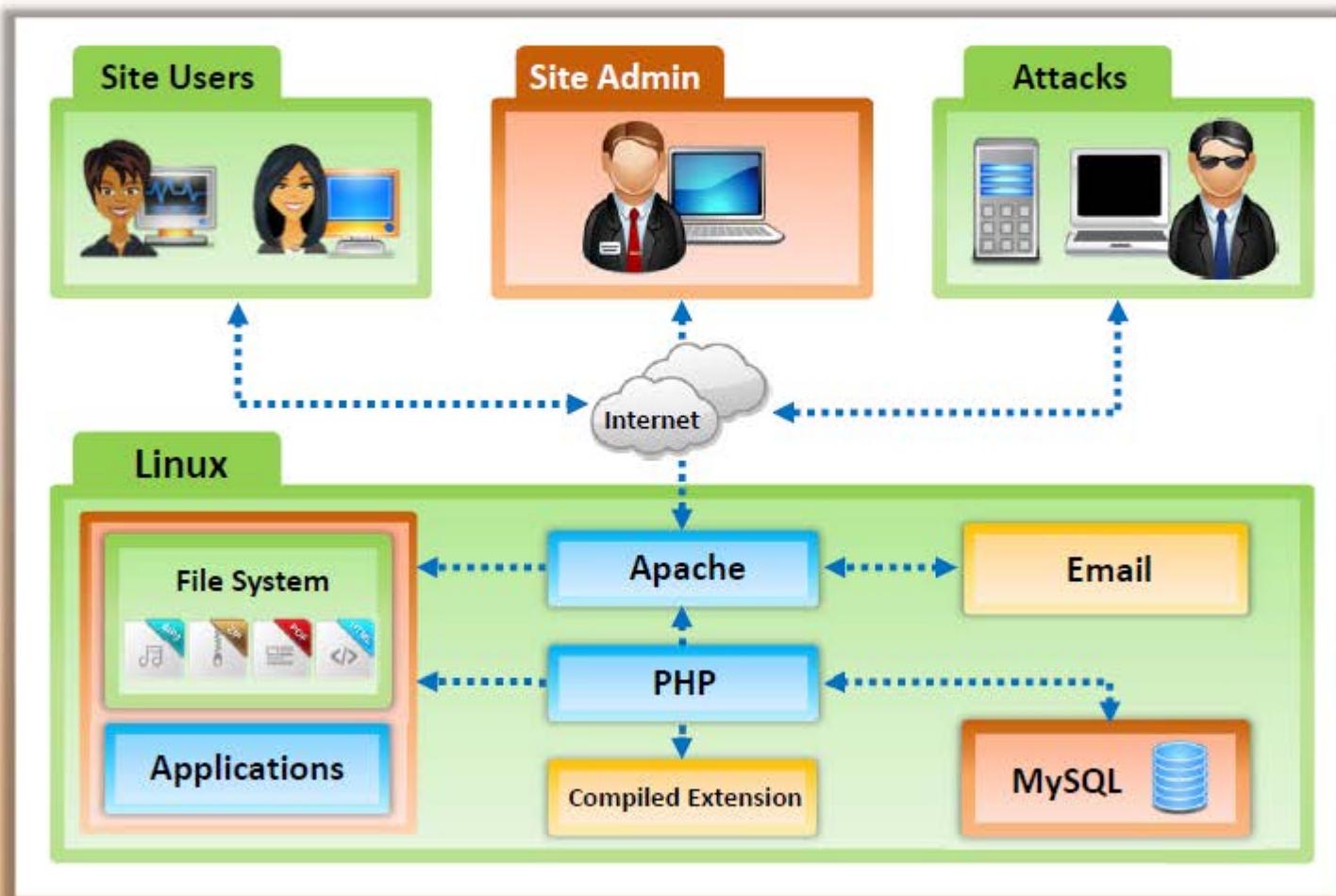
05

Data tampering and data theft



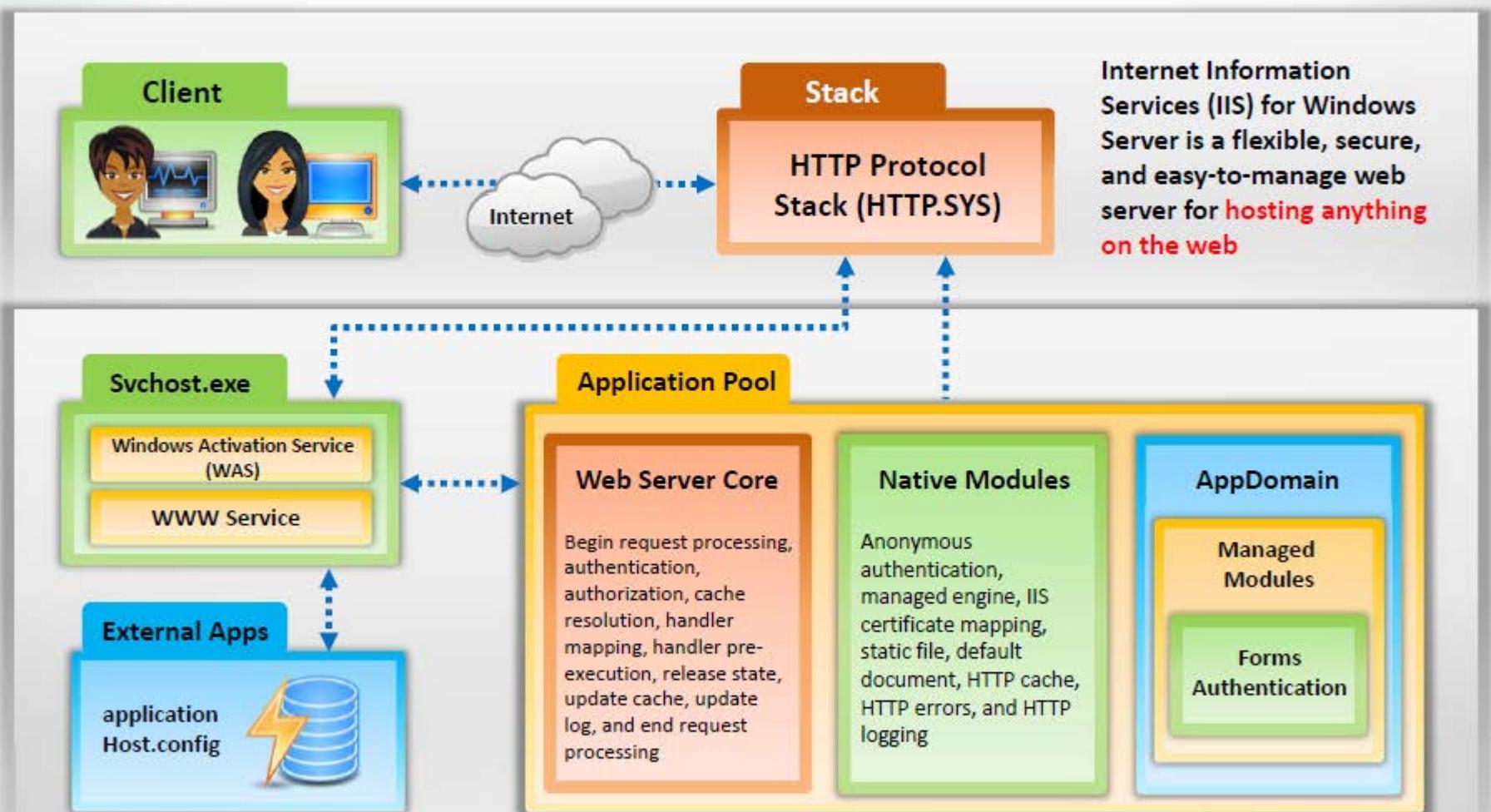
Open Source Webserver Architecture

CEH
Certified Ethical Hacker



IIS Web Server Architecture

C|EH
Certified Ethical Hacker



Module Flow

CEH
Certified Ethical Hacker



Webserver Concepts

1



Webserver Attacks

2



Attack Methodology

3



Webserver Attack Tools

4



Counter-measures

5



Patch Management

6



Webserver Security Tools

7



Webserver Pen Testing

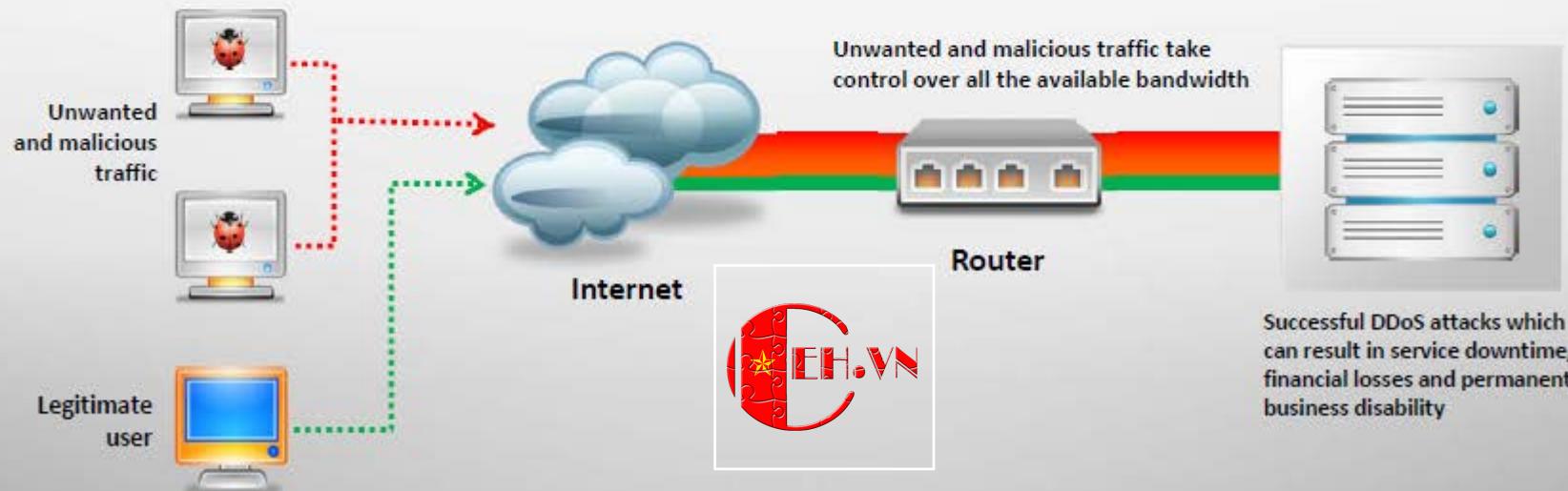
8

DoS/DDoS Attacks

CEH
Certified Ethical Hacker

Attackers may send numerous **fake requests** to the web server which results in the **web server crash** or become unavailable to the legitimate users

Attackers may target **high profile web servers** such as banks, credit card payment gateways, government owned services, etc. to **steal user credentials**

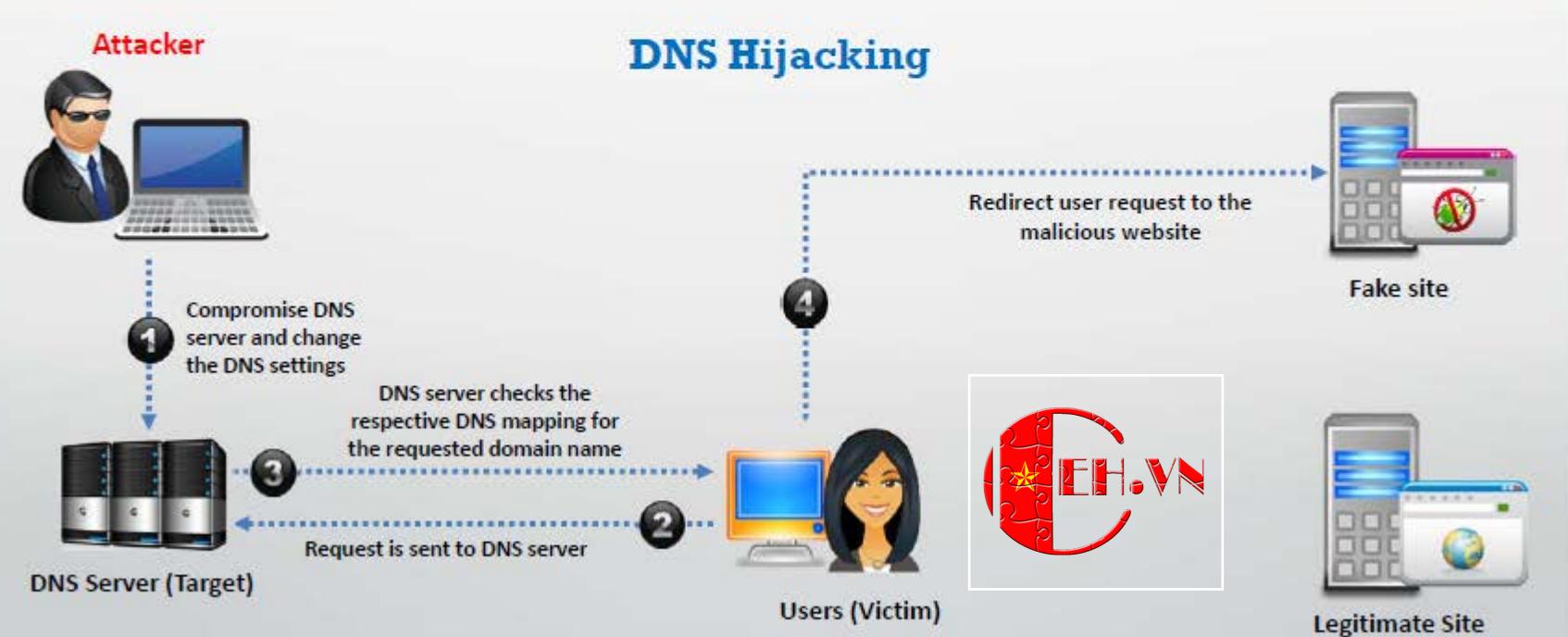


DNS Server Hijacking

CEH
Certified Ethical Hacker



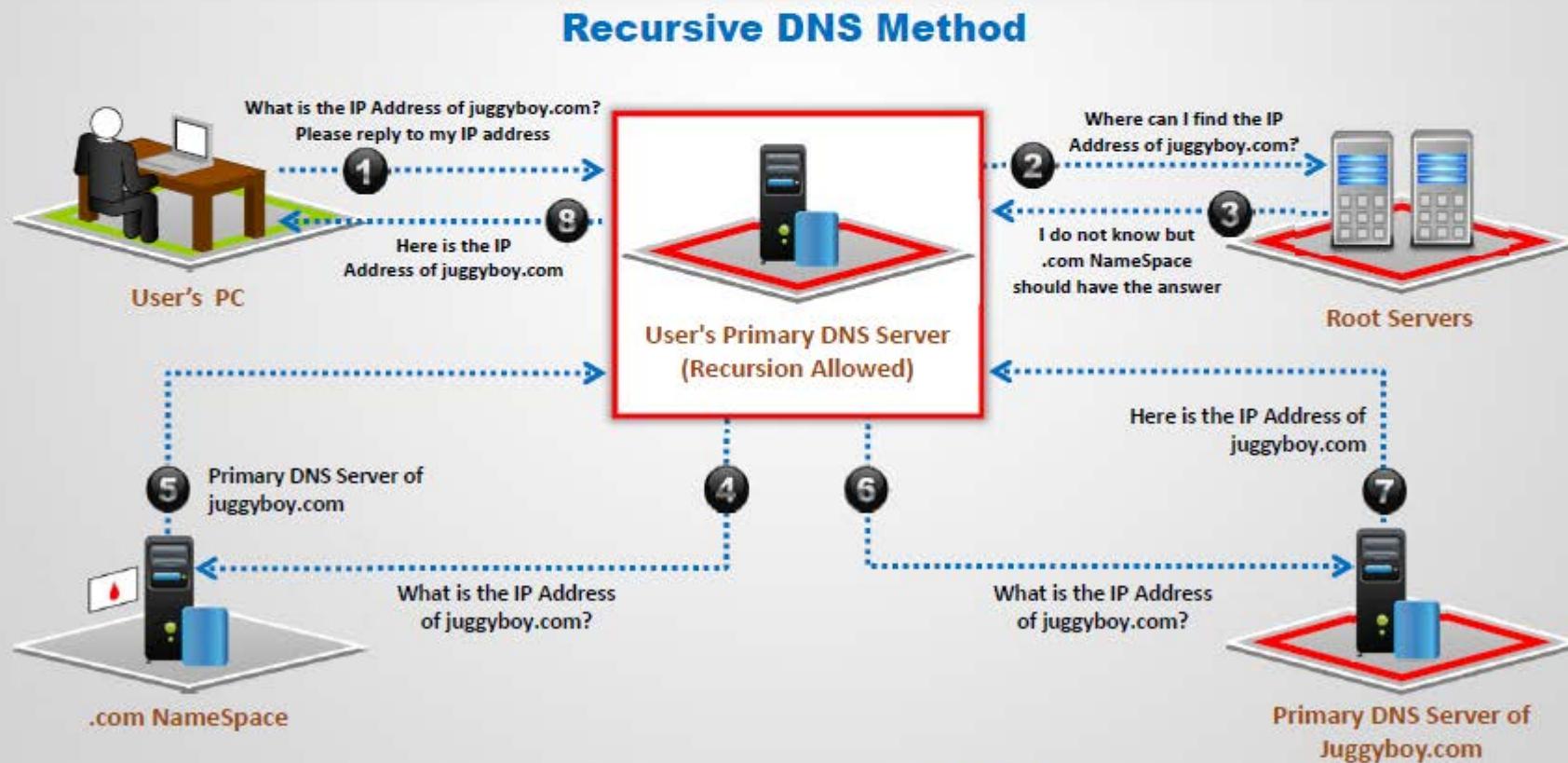
Attacker compromises DNS server and **changes the DNS settings** so that all the request coming toward the target web server should be redirected to his/her own malicious server



DNS Amplification Attack



Attacker takes the advantage of **DNS recursive method** of DNS redirection to perform DNS amplification attack



Directory Traversal Attacks

In directory traversal attacks, attackers use .. (dot-dot-slash) sequence to access restricted directories outside of the web server root directory

Attackers can use trial and error method to navigate the outside of root directory and access sensitive information in the system



`http://server.com/scripts/..%5c../Windows/System32/cmd.exe?/c+dir+c:\`

Volume in drive C has no label.
Volume Serial Number is D45E-9FEE

Directory of C:\

```
06/02/2013 11:31 AM    1,024 .rnd
09/28/2013 06:43 PM      0 123.text
05/21/2013 03:10 PM      0 AUTOEXEC.BAT
09/27/2013 08:54 PM  <DIR>    CATALINA_HOME
05/21/2013 03:10 PM      0 CONFIG.SYS
08/11/2013 09:16 AM  <DIR>    Documents and Settings
09/25/2013 05:25 PM  <DIR>    Downloads
08/07/2013 03:38 PM  <DIR>    Intel
09/27/2013 09:36 PM  <DIR>    Program Files
05/26/2013 02:36 AM  <DIR>    Snort
09/28/2013 09:50 AM  <DIR>    WINDOWS
09/25/2013 02:03 PM   569,344 WinDump.exe
7 File(s)     570,368 bytes
13 Dir(s)  13,432,115,200 bytes free
```



Man-in-the-Middle/Sniffing Attack

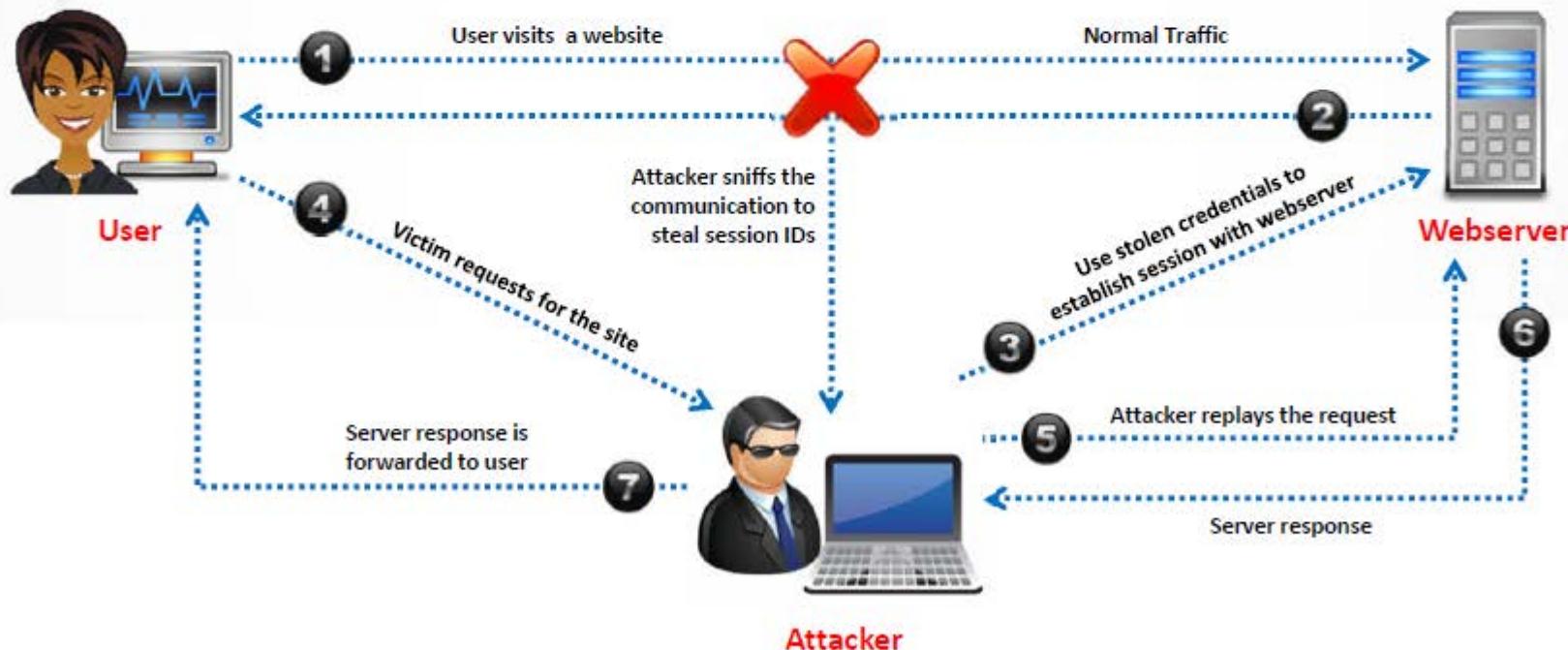


01

Man-in-the-Middle (MITM) attacks allow an attacker to access sensitive information by **intercepting and altering communications** between an end-user and webservers

02

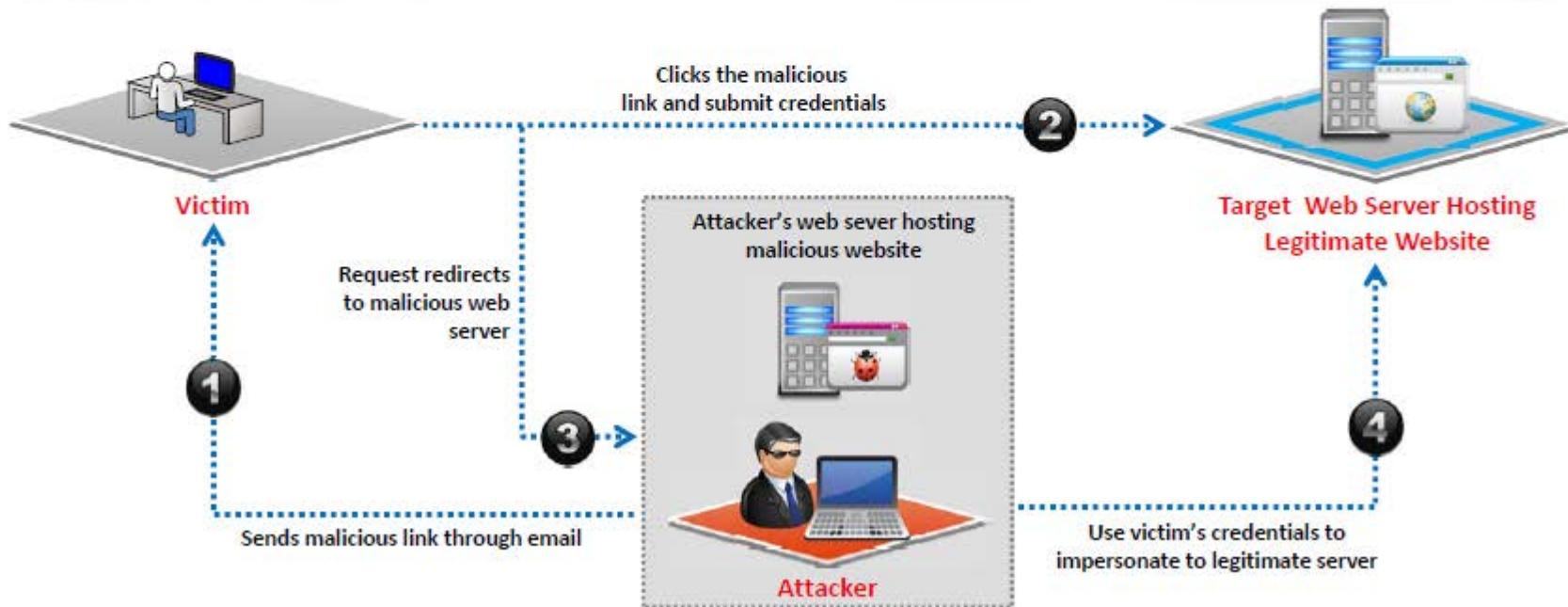
Attacker **acts as a proxy** such that all the communication between the user and webserver passes through him



Phishing Attacks



- Attacker tricks user to submit **login details** for website that looks legitimate, but it redirect to the malicious website hosted on attacker web server
- Attacker **steals the credentials** entered and use it to impersonate with the website hosted on the legitimate target server
- Attacker then can perform **unauthorized** or **malicious operation** with the website target server



Website Defacement

CEH
Certified Ethical Hacker

- Web defacement occurs when an intruder **maliciously alters visual appearance of a web page** by inserting or substituting provocative and frequently offending data
- Defaced pages exposes visitors to some propaganda** or misleading information until the unauthorized change is discovered and corrected
- Attackers uses variety of methods such as **MYSQL injection** to access a site in order to deface it



Web Server Misconfiguration



Server misconfiguration refers to **configuration weaknesses** in web infrastructure that can be exploited to launch various attacks on web servers such as directory traversal, server intrusion, and data theft



Verbose Debug/Error
Messages

Anonymous or Default
Users/Passwords

Sample Configuration,
and Script Files

Remote Administration
Functions

Unnecessary
Services Enabled

Misconfigured/Default
SSL Certificates

Web Server Misconfiguration Example



This configuration allows anyone to view the **server status** page, which contains detailed information about the current use of the web server, including information about the **current hosts** and requests being processed

httpd.conf file on an **Apache** server

```
<Location /server-status>
  SetHandler server-status
</Location>
```

This configuration gives **verbose error messages**



php.ini file

```
display_error = On
log_errors = On
error_log = syslog
ignore_repeated_errors = Off
```

HTTP Response Splitting Attack

CEH
Certified Ethical Hacker



HTTP response splitting attack involves **adding header response data into the input field** so that the server split the response into two responses



The attacker can **control the second response to redirect user to a malicious website** whereas the other responses will be discarded by web browser

Server Code

```
String author =  
request.getParameter(AUTHOR_PARAM);  
...  
Cookie cookie = new  
Cookie("author", author);  
cookie.setMaxAge(cookieExpiration);  
response.addCookie(cookie);
```

Input = Jason

HTTP/1.1 200 OK

Set-Cookie: author=Jason

...

Input = JasonTheHacker\r\nHTTP/1.1 200 OK\r\n

First Response (Controlled by Attacker)

Set-Cookie: author=JasonTheHacker
HTTP/1.1 200 OK

...

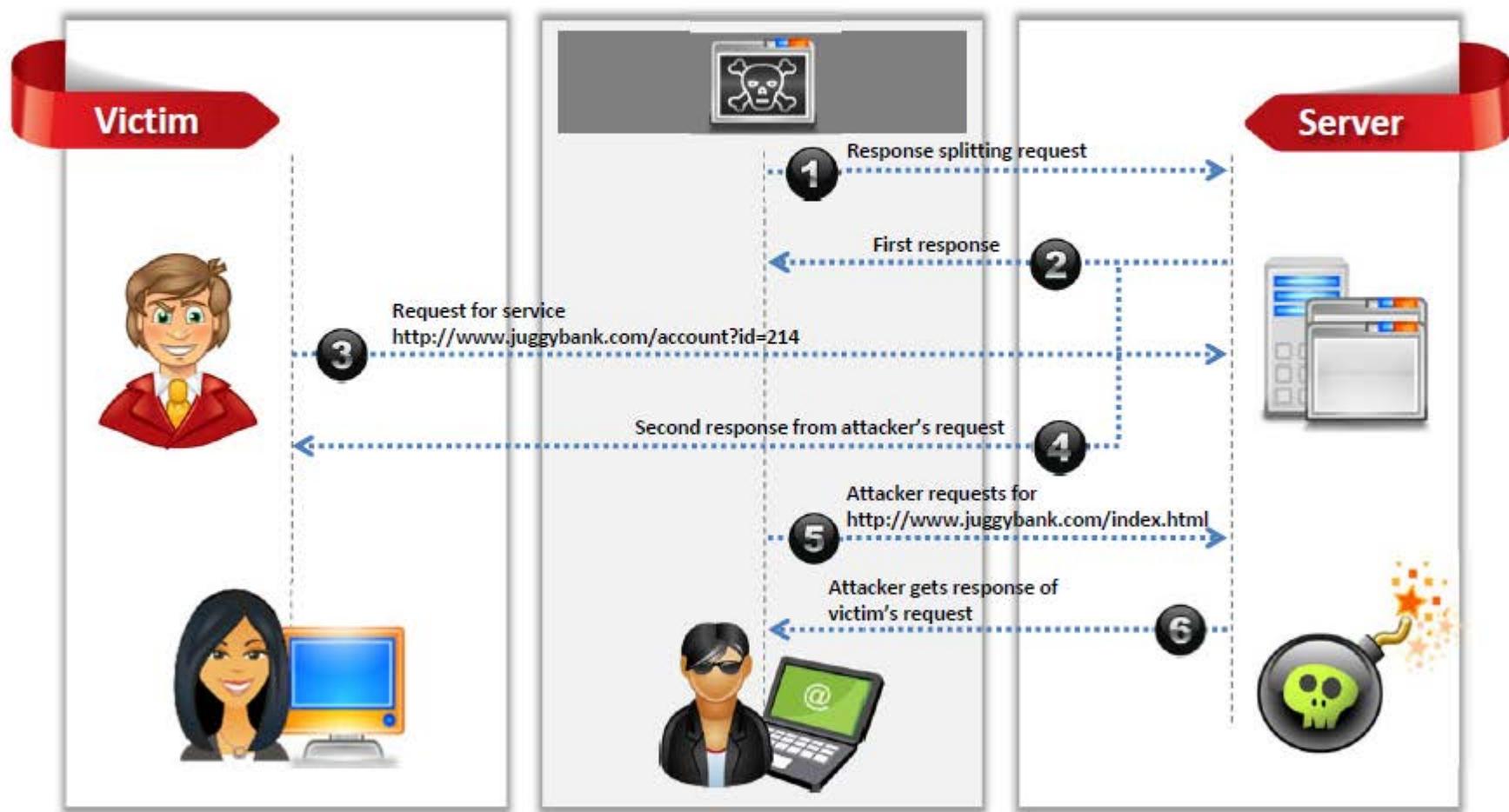
Second Response

HTTP/1.1 200 OK

...

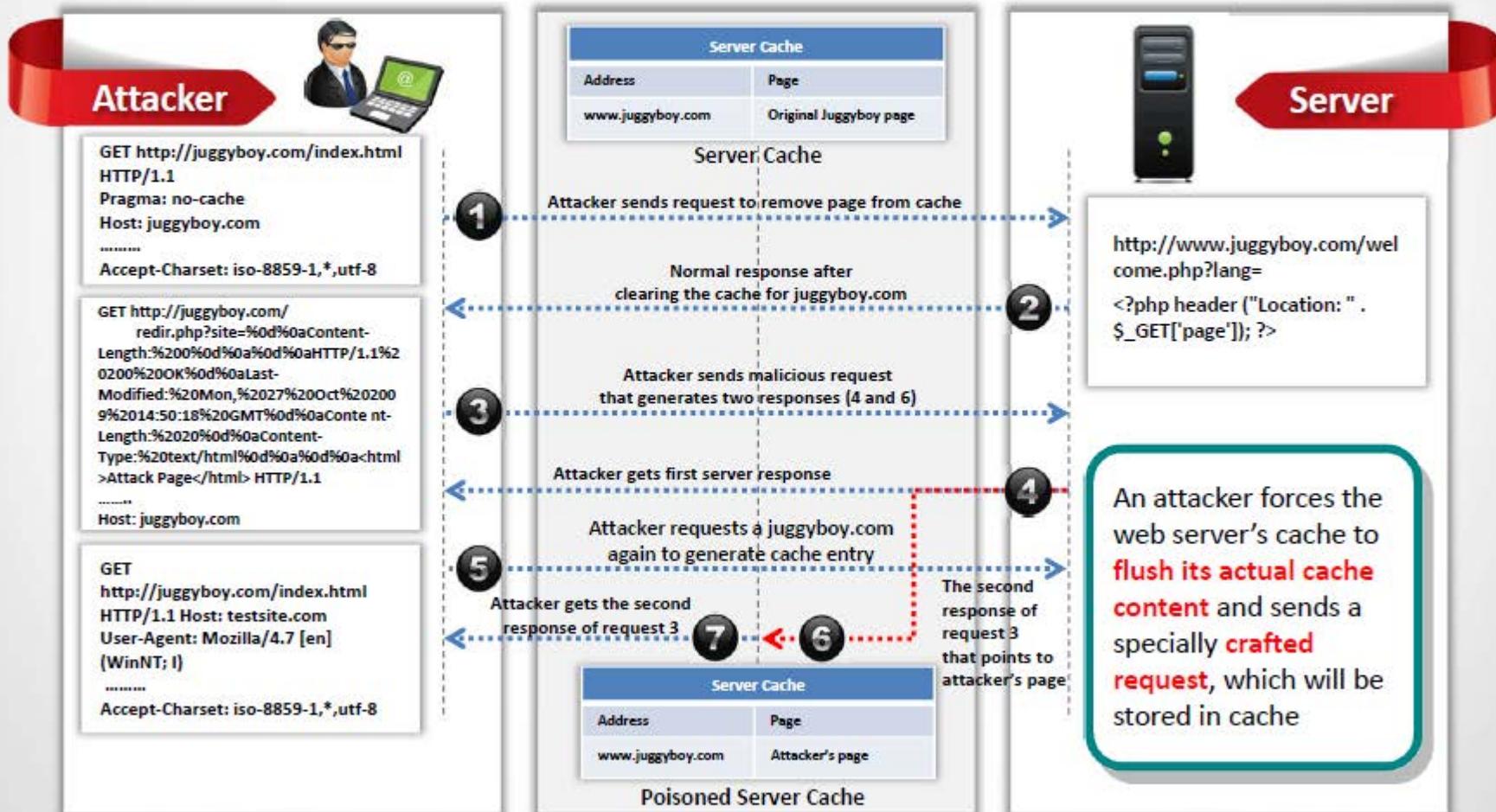
HTTP Response Splitting Attack

(Cont'd)



Web Cache Poisoning Attack

CEH
Certified Ethical Hacker



SSH Bruteforce Attack

1

SSH protocols are used to create an **encrypted SSH tunnel** between two hosts in order to transfer unencrypted data over an **insecure network**

2

Attackers can brute force SSH login credentials to gain **unauthorized access** to a **SSH tunnel**

3

SSH tunnels can be used to **transmit malwares** and other exploits to victims without being detected



Webserver Password Cracking



An attacker tries to exploit weaknesses to hack **well-chosen passwords**



The most **common passwords** found are password, root, administrator, admin, demo, test, guest, qwerty, pet names, etc.



Attacker target mainly for:

- ➊ SMTP servers
- ➋ Web shares
- ➌ SSH Tunnels
- ➍ Web form authentication cracking
- ➎ FTP servers



Attackers use different methods such as **social engineering, spoofing, phishing**, using a Trojan Horse or virus, wiretapping, keystroke logging, etc.



Many hacking attempts start with **cracking passwords** and proves to the webserver that they are a **valid user**

Webserver Password Cracking Techniques



- Passwords may be cracked **manually** or with **automated tools** such as Cain & Abel, Brutus, THC Hydra, etc.
- Passwords can be cracked by using following techniques:



Guessing

A common cracking method used by attackers to guess passwords either by **humans** or by **automated tools** provided with dictionaries

Dictionary Attacks

A **file of words is run against user accounts**, and if the password is a simple word, it can be found pretty quickly

Brute Force Attack

The most time-consuming, but comprehensive way to crack a password. Every **combination of character is tried** until the password is broken.

Hybrid Attack

A hybrid attack works similar to dictionary attack, but it adds **numbers** or **symbols** to the password attempt

Web Application Attacks



Vulnerabilities in **web applications** running on a webserver provide a broad attack path for webserver compromise



Note: For complete coverage of web application attacks refer to Module 12: Hacking Web Applications

Module Flow



Webserver Attack Methodology



**Information
Gathering**

01

**Webserver
Footprinting**



**Mirroring
Website**

03

**Vulnerability
Scanning**



**Session
Hijacking**

05

**Hacking
Webserver
Passwords**



Webserver Attack Methodology: Information Gathering



1

Information gathering involves collecting information about the **targeted company**

2

Attackers search the **Internet, newsgroups, bulletin boards**, etc. for information about the company

3

Attackers use **Whois, Traceroute, Active Whois**, etc. tools and query the Whois databases to get the details such as a domain name, an IP address, or an autonomous system number

The screenshot shows the WHOIs.net website interface. A search bar at the top contains the text "ebay.com". Below the search bar, the text "Your Domain Starting Place..." is visible. The main content area displays the WHOIS information for the domain ebay.com.

WHOIS information for ebay.com:**

```
[Querying whois.verisign-grs.com]
[whois.verisign-grs.com]
Whois Server Version 2.0
Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

Domain Name: EBAY.COM
Registrar: MARKMONITOR INC
Whois Server: whois.markmonitor.com
Referral URL: http://www.markmonitor.com
Name Server: NS1.P47.DYNECT.NET
Name Server: SJC-DNS1.EBAYDNS.COM
Name Server: SJC-DNS2.EBAYDNS.COM
Name Server: SMF-DNS1.EBAYDNS.COM
Name Server: SMF-DNS2.EBAYDNS.COM
Status: clientDeleteProhibited
Status: clientTransferProhibited
Status: clientUpdateProhibited
Status: serverDeleteProhibited
Status: serverTransferProhibited
Status: serverUpdateProhibited
Updated Date: 29-oct-2013
Creation Date: 04-aug-1995
Expiration Date: 03-aug-2018
```

<http://www.whois.net>

Note: For complete coverage of information gathering techniques refer to Module 02: Footprinting and Reconnaissance

Webserver Attack Methodology: Information Gathering from Robots.txt File



- The robots.txt file contains the **list of the web server directories and files** that the web site owner wants to hide from web crawlers
- Attacker can simply request Robots.txt file from the URL and retrieve the sensitive information such as **root directory structure, content management system information**, etc., about the target website



```
File Edit Format View Help
User-agent: *
Disallow: /wp-admin/
Disallow: /wp-includes/
Disallow: /*/download/confirmation.aspx?
Disallow: /ctl/
Disallow: /admin/
Disallow: /App_Browsers/
Disallow: /genuine/ajax/
Disallow: /App_Code/
Disallow: /App_Data/
Disallow: /App_GlobalResources/
Disallow: /bin/
Disallow: /Components/
Disallow: /Config/
Disallow: /contest/
Disallow: /genuine/survey/
Disallow: /controls/
Disallow: /DesktopModules/
Disallow: /HttpModules/
Disallow: /Install/
Disallow: /js/
Disallow: /software
Disallow: /software.aspx
Disallow: /windows/404.aspx?*
Disallow: /Userlogin
Disallow: /testgallery
Sitemap: http://www.juggyboy.com/sitemap.xml
```

Webserver Attack Methodology: Webserver Footprinting



01

Gather **valuable system-level data** such as account details, operating system, software versions, server names, and database schema details

02

Telnet a webserver to footprint a webserver and gather information such as server name, server type, operating systems, applications running, etc.

03

Use tool such as **ID Serve**, **httprecon**, and **Netcraft** to perform footprinting



NETCRAFT

Search Web by Domain

Explore 1,472,431 web sites visited by users of the Netcraft Toolbar 1st November 2013

Search: site contains search tips lookup example: site contains .netcraft.com

Results for microsoft

First 500 sites returned

Site	Site Report	First seen	Netblock	OS
1. www.microsoft.com		august 1995	ms hotmail	citrix netScaler
2. go.microsoft.com		november 2001	ms hotmail	windows server 2008
3. support.microsoft.com		october 1997	microsoft corporation	unknown
4. technet.microsoft.com		august 1999	microsoft corporation	windows server 2012
5. windows.microsoft.com		june 1998	microsoft corporation	unknown
6. msdn.microsoft.com		september 1998	microsoft corporation	windows server 2013
7. social-technet.microsoft.com		august 2008	microsoft corporation	citrix netScaler
8. office.microsoft.com		november 1998	microsoft corporation	windows server 2008
9. answers.microsoft.com		august 2009	microsoft limited	windows server 2008
10. social.msn.microsoft.com		august 2008	microsoft corporation	citrix netScaler
11. download.microsoft.com		august 1999	akamai international, bv	linux
12. login.microsoftonline.com		december 2010	microsoft corporation	windows server 2008
13. www.microsoftstore.com		november 2008	digital river ireland ltd.	f5 big-ip
14. seach.microsoft.com		january 1997	akamai technologies	linux
15. 015.officeredir.microsoft.com		may 2012	microsoft corporation	windows server 2008
16. www.update.microsoft.com		may 2007	microsoft corporation	windows server 2008
17. r.office.microsoft.com		november 2003	microsoft corporation	windows server 2008

<http://toolbar.netcraft.com>

Webserver Footprinting Tools



httprecon

httprecon 7.3 - http://www.juggyboy.com:80/

File Configuration Fingerprinting Reporting Help

Target (Microsoft IIS 6.0)

http:// www.juggyboy.com : 80 Analyze

GET existing | GET long request | GET non-existing | GET wrong protocol | HEAD existing

```
HTTP/1.1 200 OK
Date: Tue, 05 Nov 2013 06:27:44 GMT
Content-Length: 6517
Content-Type: text/html
Content-Location: http://www.juggyboy.com/index.html
Last-Modified: Thu, 24 Oct 2013 12:17:26 GMT
Accept-Ranges: bytes
ETag: "978630b0d0ce1:7e49"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
```

Matchlist (352 Implementations) | Fingerprint Details | Report Preview

Name	Hits	Match %
Microsoft IIS 6.0	90	100
Microsoft IIS 5.0	73	81.11...
Microsoft IIS 5.1	67	74.44...
Microsoft IIS 7.0	65	72.22...
Sun Sun ONE Web Server 6.1	65	72.22...
Apache 1.3.26	64	71.11...

Generate TXT Report... Done.

<http://www.computech>

ID Serve

Internet Server Identification Utility v1.02
Personal Security Freeware by Steve Gibson
Copyright (c) 2003 by Gibson Research Corp.

Background Server Query Q&A / Help

Enter or copy / paste an Internet server URL or IP address here (example: www.microsoft.com):
① www.certifiedhacker.com

② Query The Server When an Internet URL or IP has been provided above, press this button to initiate a query of the specified server.

③ Server query processing:
The server returned the following response headers:
HTTP/1.1 200 OK
Content-Length: 9660
Content-Type: text/html
Content-Location: http://www.certifiedhacker.com/index.html

④ The server identified itself as:
④ Microsoft-IIS/6.0

Copy Goto ID Serve web page Exit

<http://www.grc.com>

Enumerating Webserver Information Using Nmap



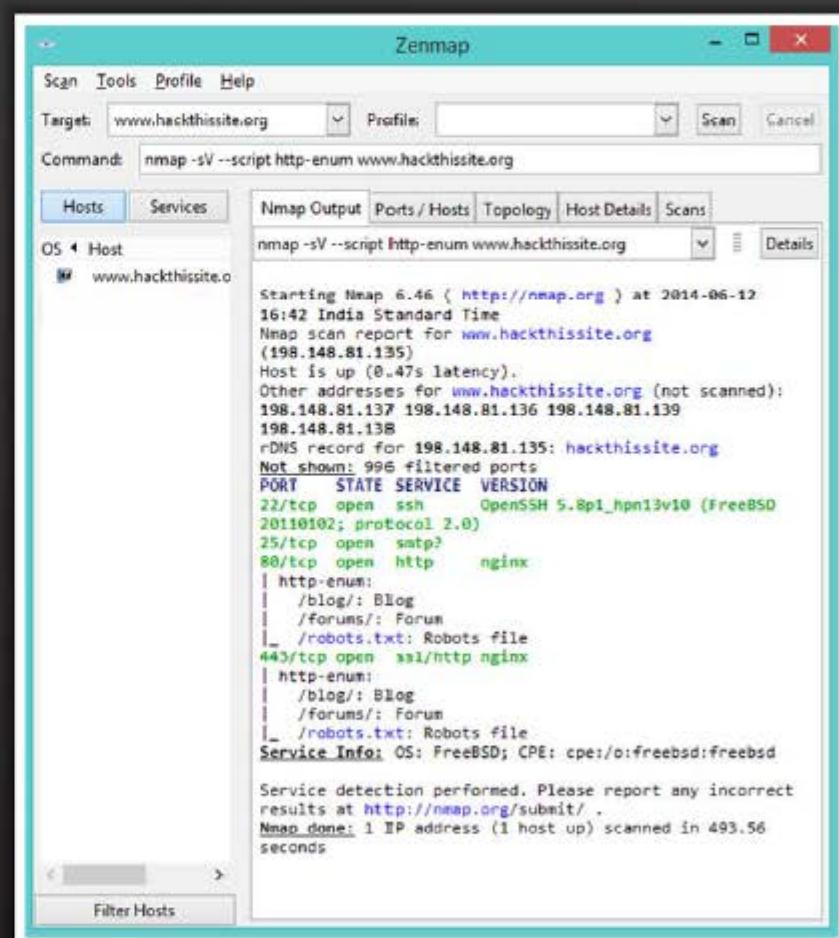
1 Attackers can use advanced **Nmap commands** and **Nmap Scripting Engine (NSE) scripts** to enumerate information about the target website

2 `nmap sv -O -p target IP address`

3 `nmap -sV --script=http-enum target IP address`

4 `nmap target IP address -p 80 --script = http-frontpage-login`

5 `nmap --script http-passwd --script-args http-passwd.root =/ target IP address`

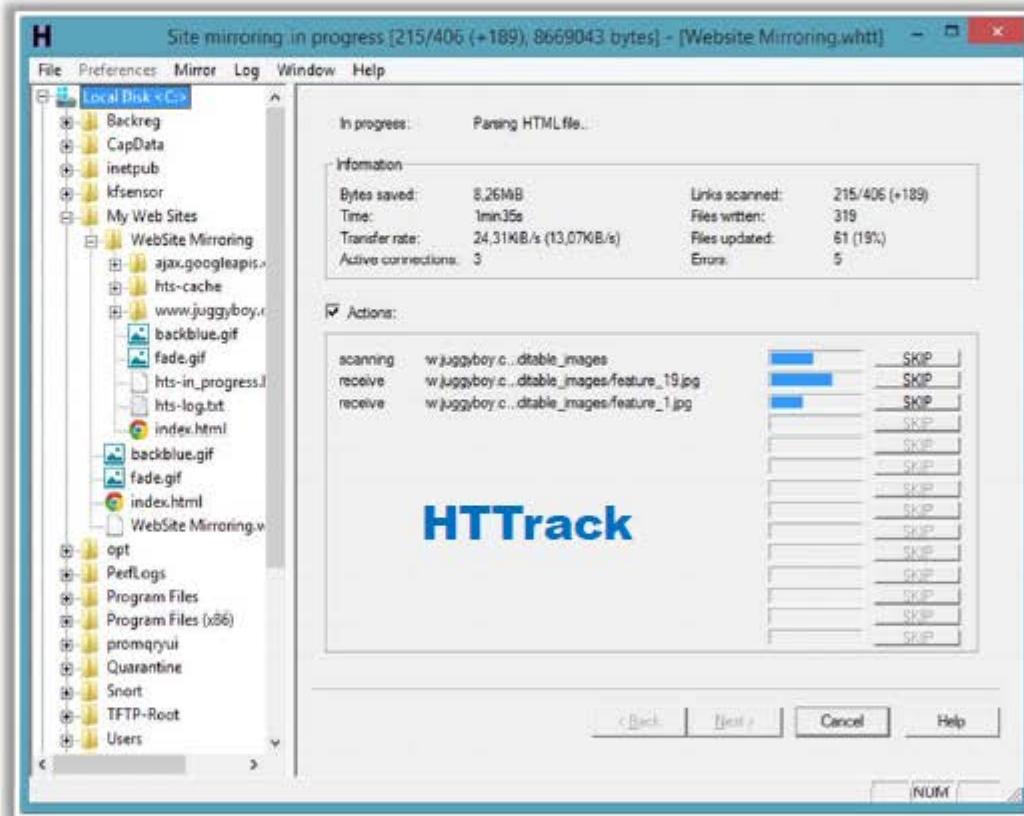


<http://nmap.org>

Webserver Attack Methodology: Mirroring a Website



- Mirror a website to create a complete profile of the site's **directory structure, files structure, external links**, etc.
- Search for comments and other items in the **HTML source code** to make footprinting activities more efficient
- Use tools **HTTrack**, **WebCopier Pro**, **BlackWidow**, etc. to mirror a website



<http://www.httrack.com>

Webserver Attack Methodology: Vulnerability Scanning



01

Implement vulnerability scan to **identify weaknesses** in a network and determine if the system can be exploited

02

Use vulnerability scanners such as HP WebInspect, Acunetix Web Vulnerability Scanner, etc. to find **hosts, services**, and **vulnerabilities**

03

Sniff the network traffic to find out **active systems, network services, applications**, and vulnerabilities present

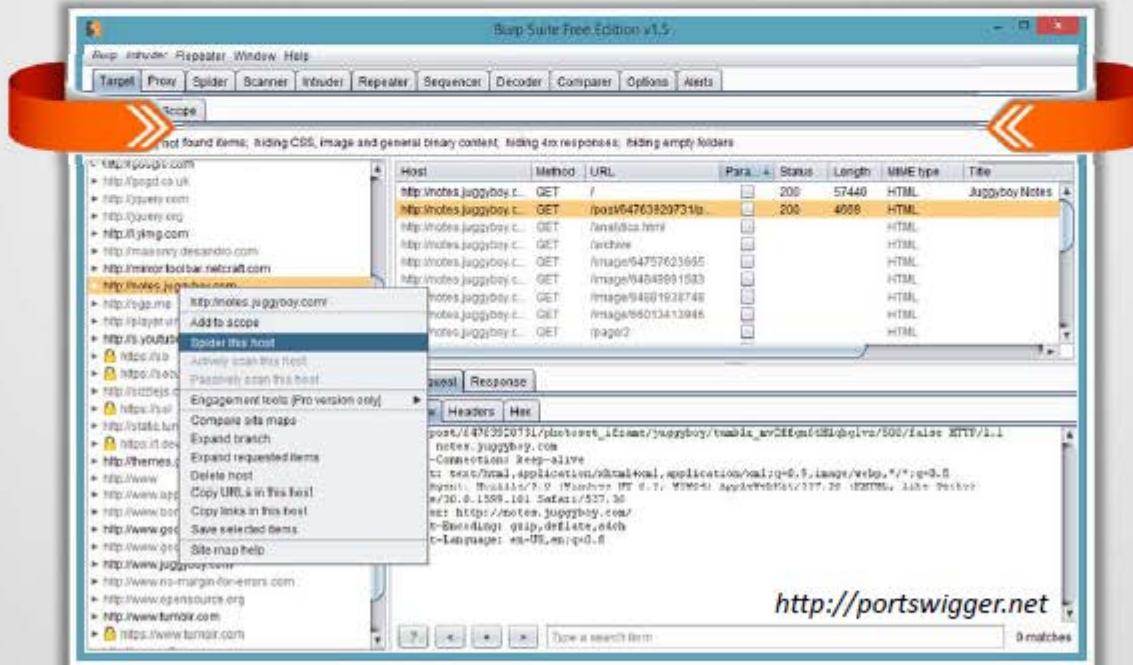
04

Test the **web server infrastructure** for any misconfigurations, outdated content, and vulnerabilities

Webserver Attack Methodology: Session Hijacking



- 1 Sniff valid session IDs to **gain unauthorized access** to the Web Server and snoop the data
- 2 Use session hijacking techniques such as session fixation, session sidejacking, Cross-site scripting, etc. to **capture valid session cookies and IDs**
- 3 Use tools such as **Burp Suite**, **Firesheep**, **JHijack**, etc. to automate session hijacking



Note: For complete coverage of Session Hijacking concepts and techniques refer to Module 10: Session Hijacking

Webserver Attack Methodology: Hacking Web Passwords



Use password cracking techniques such as **brute force attack, dictionary attack, password guessing** to crack webserver passwords

Use tools such as **THC-Hydra, Brutus**, etc.

The screenshot shows the HydraGTK graphical user interface. The window title is "HydraGTK". The menu bar includes "Quit", "Target", "Passwords", "Tuning", "Specific", and "Start". The "Passwords" tab is selected. The main area displays the output of the Hydra v4.1 tool. The log shows the following:

```
Hydra v4.1 (c) 2004 by van Hauser / THC - use allowed only for legal purposes.  
Hydra (http://www.thc.org) starting at 2004-05-17 21:58:52  
[DATA] 32 tasks, 1 servers, 45380 login tries (l:1/p:45380), ~1418 tries per task  
[DATA] attacking service ftp on port 21  
[STATUS] 14056.00 tries/min, 14056 tries in 00:01h, 31324 todo in 00:03h  
[STATUS] 14513.00 tries/min, 29026 tries in 00:02h, 16354 todo in 00:02h  
[21][ftp] host: 127.0.0.1 login: marc password: success  
Hydra (http://www.thc.org) finished at 2004-05-17 22:01:38  
<finished>
```

At the bottom of the window, there are buttons for "Start", "Stop", "Save Output", and "Clear Output". Below the window, a command line shows the executed command: `hydra 127.0.0.1 ftp -l marc -P /tmp/passlist.txt -e ns -t 32`.

<https://www.thc.org>

Module Flow



Webserver Attack Tool: Metasploit



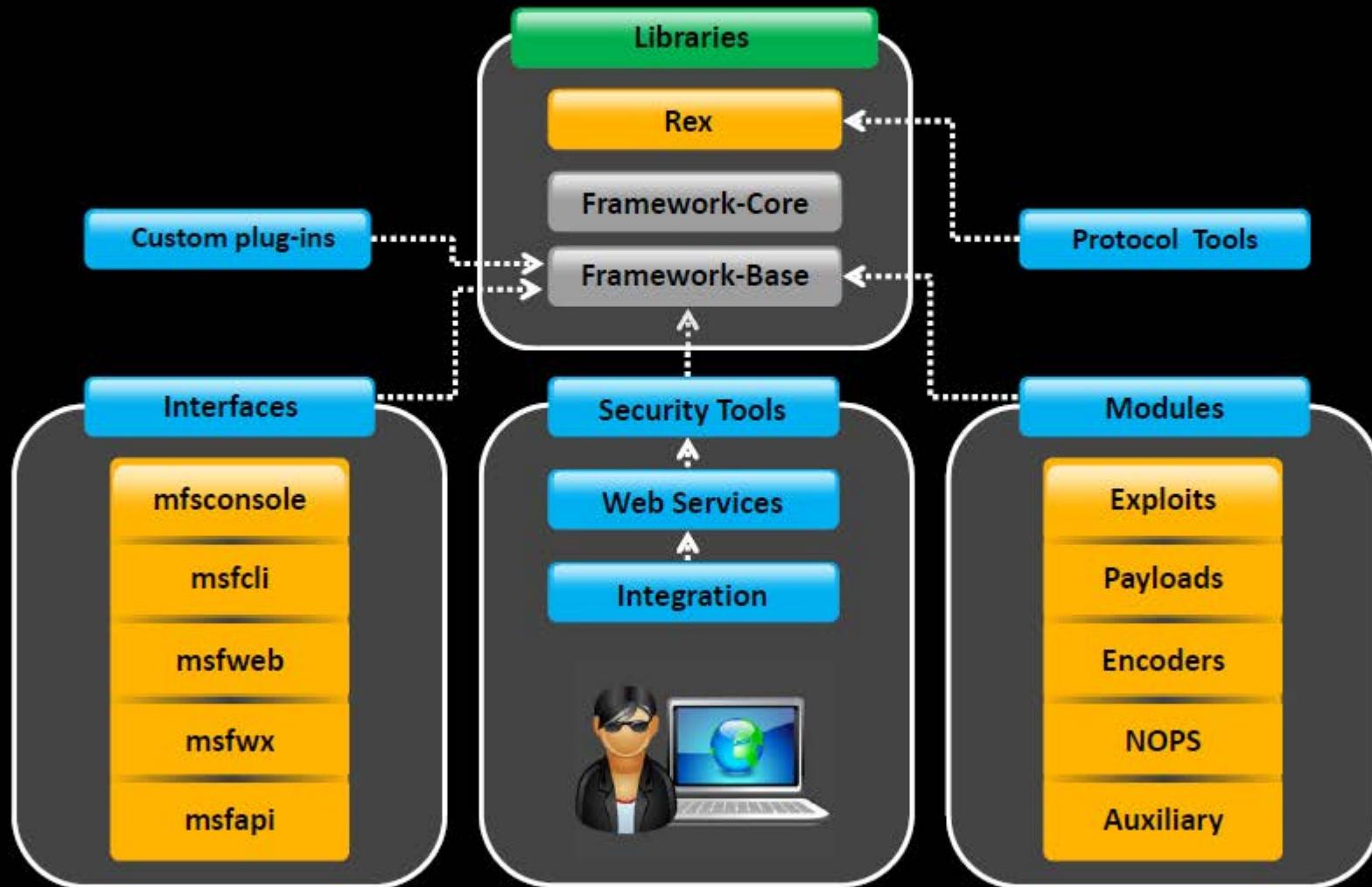
- The Metasploit Framework is a **penetration testing toolkit**, exploit development platform, and **research tool** that includes hundreds of working remote exploits for a variety of platforms
- It supports fully automated **exploitation of web servers**, by abusing known vulnerabilities and leveraging weak passwords via Telnet, SSH, HTTP, and SNM

The screenshot shows the Metasploit Framework's interface. At the top, there's a navigation bar with tabs for Overview, Analysis, Sessions, Campaigns, Web Apps, Modules, Tags, Reports, and Tasks. Below that is a toolbar with buttons for Go to Host, Delete, Scan, Import, Response, Modules, Bruteforce, Exploit, and New Host. The main area is a table titled "Hosts" with 100 entries. The columns include IP Address, Hostname, Operating System, VM, Purpose, Sys, Vins, Act, Notes, Updated, and Status. Most hosts are listed as "Scanned". The operating systems listed include Microsoft Windows 7 Professional, Microsoft Windows 2008, Microsoft Windows 7 Professional 7601 Service Pack 1, and Microsoft Windows XP SP2+.

IP Address	Hostname	Operating System	VM	Purpose	Sys	Vins	Act	Notes	Updated	Status
192.168.168.100	ecc100	Windows 7 Professional 7601 Service Pack 1		device	1				8 minutes ago	Scanned
192.168.168.102	ecc102	Windows 7 Professional 7601 Service Pack 1		device	1				8 minutes ago	Scanned
192.168.168.111	ecc111	Microsoft Windows 7 Professional 7601 Service Pack 1		client	16		4		9 minutes ago	Scanned
192.168.168.110	ecc110	Windows 7 Professional 7601 Service Pack 1		device	1				8 minutes ago	Scanned
192.168.168.113	ADMIN-PC	Microsoft Windows 7 Professional 7601 Service Pack 1		client	9		4		9 minutes ago	Scanned
192.168.168.115	WWW-WW-WWW-100	Microsoft Windows (2008)		device	6		3		9 minutes ago	Scanned
192.168.168.120	ecc120	Microsoft Windows 7 Professional 7601 Service Pack 1		client	9		4		9 minutes ago	Scanned
192.168.168.13	ecc13	Microsoft Windows 7 Professional 7601 Service Pack 1		client	11		4		9 minutes ago	Scanned
192.168.168.133	ADMIN-PC	Microsoft Windows 7 Professional 7601 Service Pack 1		client	9		4		9 minutes ago	Scanned
192.168.168.14	ecc14	Microsoft Windows (XP) SP2+		client	8		2		7 minutes ago	Scanned

<http://www.metasploit.com>

Metasploit Architecture



Metasploit Exploit Module

CEH
Certified Ethical Hacker

- It is the basic module in Metasploit used to **encapsulate an exploit** using which users target many platforms with a single exploit
- This module comes with **simplified meta-information fields**
- Using a Mixins feature, users can also **modify exploit behavior dynamically**, brute force attacks, and attempt passive exploits



Steps to exploit a system follow the Metasploit Framework

- 1 Configuring Active Exploit
- 2 Verifying the Exploit Options
- 3 Selecting a Target
- 4 Selecting the Payload
- 5 Launching the Exploit

Metasploit Payload Module



- Payload module establishes a **communication channel** between the Metasploit framework and the victim host
- It combines the **arbitrary code** that is executed as the result of an exploit succeeding
- To generate **payloads**, first select a payload using the command:



```
C:\ Command Prompt

msf > use windows/shell_reverse_tcp
msf payload(shell_reverse_tcp) > generate -h
Usage: generate [options]

Generates a payload.

OPTIONS:

-b <opt> The list of characters to avoid:
  '\x00\xff'

-e <opt> The name of the encoder module to use.

-h Help banner.

-o <opt> A comma separated list of options in
        VAR=VAL format.

-s <opt> NOP sled length.

-t <opt> The output type: ruby, perl, c, or raw.

msf payload(shell_reverse_tcp) >
```

Metasploit Auxiliary Module



- Metasploit's auxiliary modules can be **used to perform arbitrary**, one-off actions such as port scanning, denial of service, and even fuzzing
- To run auxiliary module, either use the **run** command, or use the **exploit** command

```
c:\ Command Prompt  
  
msf > use dos/windows/smb/ms06_035_mailslot  
msf auxiliary(ms06_035_mailslot) > set RHOST 1.2.3.4  
RHOST => 1.2.3.4  
msf auxiliary(ms06_035_mailslot) > run  
[*] Mangling the kernel, two bytes at a time...
```



Metasploit NOPS Module



- NOP modules generate a no-operation instructions used for blocking out buffers
- Use **generate** command to generate a NOP sled of an arbitrary size and display it in a given format

OPTIONS:

- b <opt>: The list of characters to avoid: '\x00\xff'
- h: Help banner
- s <opt>: The comma separated list of registers to save
- t <opt>: The output type: ruby, perl, c, or raw

```
msf nop(opty2)>
```



Generates a NOP sled of a given length

```
msf > use x86/opty2  
msf nop(opty2) > generate -h  
Usage: generate [options] length
```



Command to generate a 50 byte NOP sled

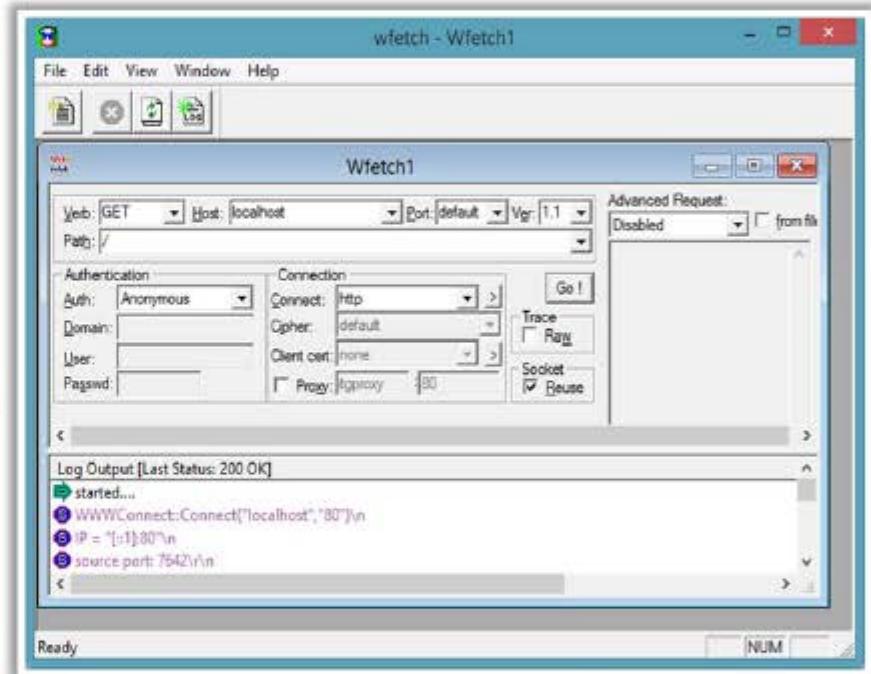
```
msf nop(opty2) > generate -t c 50  
unsigned char buf[] =  
"\xf5\x3d\x05\x15\xf8\x67\xba\x7d\x08\xd6\x  
66\x9f\xb8\x2d\xb6"  
"\x24\xbe\xb1\x3f\x43\x1d\x93\xb2\x37\x35\x  
84\xd5\x14\x40\xb4"  
"\xb3\x41\xb9\x48\x04\x99\x46\xa9\xb0\xb7\x  
2f\xfd\x96\x4a\x98"  
"\x92\xb5\xd4\x4f\x91";  
msf nop(opty2) >
```

Webserver Attack Tool: Wfetch



WFetch allows attacker to fully customize an **HTTP request** and send it to a Web server to see the raw HTTP request and response data

It allows attacker to test the performance of Web sites that contain new elements such as **Active Server Pages** (ASP) or wireless protocols



<http://www.microsoft.com>



fully customize HTTP request



Web Password Cracking Tools: THC-Hydra and Brutus



THC-Hydra

- Hydra is a parallelized **login cracker** which supports numerous protocols to attack

```
xHydra
Target  Passwords  Tuning  Specific  Start
Output
Hydra v7.1 (c)2011 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2012-10-21 17:01:09
[DEBUG] cmdline: /usr/bin/hydra -S -v -V -d -l Administrator -P /home/ /Desktop/pass -t 16 192.168.168.1:3389
[DATA] 4 tasks, 1 server, 4 login tries (l:1/p:4), ~1 try per task
[DATA] attacking service rdp on port 3389
[VERBOSE] Resolving addresses ...
[DEBUG] resolving 192.168.168.1
done
[DEBUG] Code: attack Time: 1350819069
[DEBUG] Options: mode 1 scl 1 restore 0 showAttempt 1 tasks 4 max_use 1
[DEBUG] Brains: active 0 targets 1 finished 0 todo_all 4 todo 4 sent 0 found 0
[DEBUG] Target 0 - target 192.168.168.1 ip 192.168.168.1 login_no wpass_nc
[DEBUG] Task 0 - pid 0 active 0 redo 0 current_login_ptr (null) current_pass_
[DEBUG] Task 1 - pid 0 active 0 redo 0 current_login_ptr (null) current_pass_
[DEBUG] Task 2 - pid 0 active 0 redo 0 current_login_ptr (null) current_pass_
[DEBUG] Task 3 - pid 0 active 0 redo 0 current_login_ptr (null) current_pass_
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce load
[VERBOSE] More tasks defined than login/pass pairs exist. Tasks reduced to 4
[DEBUG] head_no[0] active 0
[DEBUG] child 0 got target 0 selected
[DEBUG] head_no[1] active 0
[INFO] child 1 not selected
Start  Stop  Save Output  Clear Output
hydra -S -v -V -d -l Administrator -P /home/ /Desktop/pass -t 16 192.168.168.1:3389
```

http://www.thc.org

Brutus

- It includes a multi-stage authentication engine and can **make 60 simultaneous target connections**
- It supports no user name, single user name, **multiple user name**, password list, combo (user/password) list and configurable brute force modes

Brutus - AET2 - www.hoobie.net/brutus - (January 2000)

File	Tools	Help	
Target: 127.0.0.1	Type: HTTP (Basic Auth)	Start Stop Clear	
Connection Options:			
Port: 80	Connections: 10	Timeout: 10	
<input type="checkbox"/> Use Proxy Define			
HTTP (Basic) Options:			
Method: HEAD	<input checked="" type="checkbox"/> KeepAlive		
Authentication Options:			
<input checked="" type="checkbox"/> Use Username	<input type="checkbox"/> Single User	Pass Mode: Word List	
User File: users.txt	Binaries	Pass File: words.txt	
Positive Authentication Results:			
Target	Type	Username	Password
127.0.0.1/	HTTP (Basic Auth)	admin	ads
127.0.0.1/	HTTP (Basic Auth)	backup	

Located and installed 1 authentication plugins
Installing:
Target 127.0.0.1 verified
Opened user file containing 6 users.
Opened password file containing 8192 Passwords.
Maximum number of authentication attempts will be 4908
Engaging target 127.0.0.1 with HTTP (Basic Auth)
Testing username: admin

http://www.hoobie.net

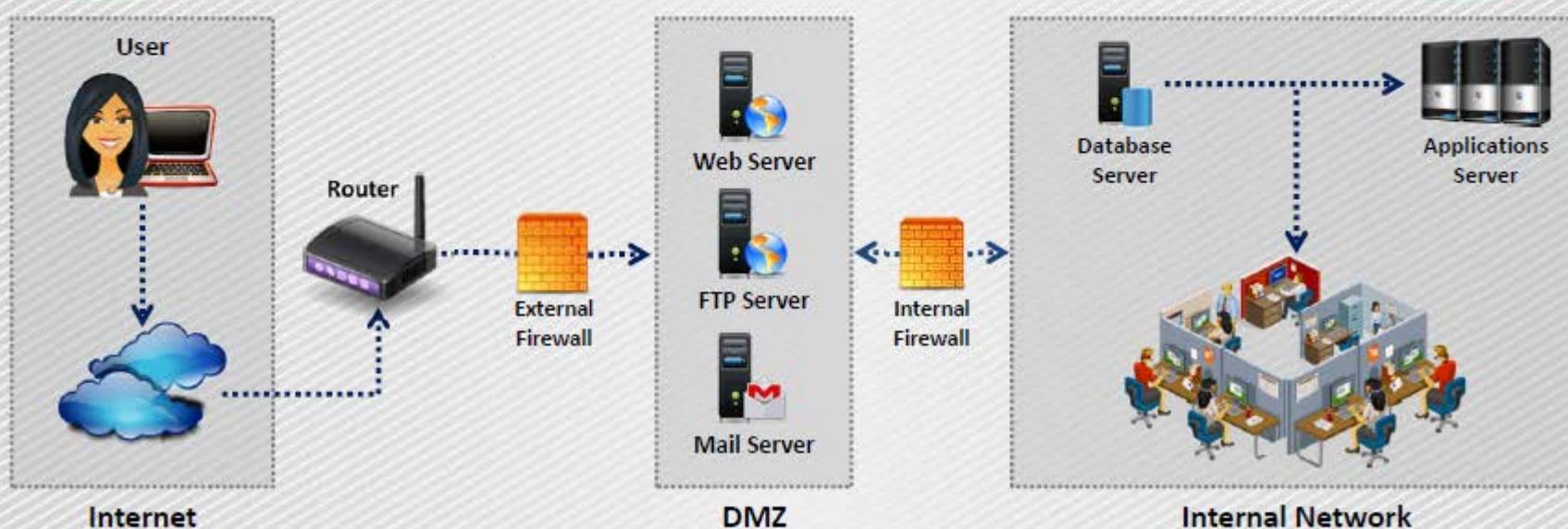
Module Flow



Place Web Servers in Separate Secure Server Security Segment on Network

CEH
Certified Ethical Hacker

- An ideal **web hosting network** should be designed with at least **three segments** namely Internet segment, secure server security segment often called demilitarized zone (DMZ), internal network
- Place the web server in **Server Security Segment** (DMZ) of the network isolated from public network as well as internal network
- The firewalls should be place for **internal network** as well as **Internet traffic** going towards DMZ



Countermeasures: Patches and Updates



01

Scan for existing vulnerabilities, patch, and update the **server software regularly**

05

Ensure that service packs, hotfixes, and security patch levels are consistent on **all Domain Controllers (DCs)**

02

Before applying any service pack, hotfix, or security patch, **read and peer review** all relevant documentation

06

Ensure that **server outages** are scheduled and a complete set of **backup tapes** and emergency repair disks are available

03

Apply all updates, regardless of their type on an "**as-needed**" basis

07

Have a **back-out plan** that allows the system and enterprise to return to their original state, prior to the failed implementation

04

Test the service packs and hotfixes on a representative **non-production environment** prior to being deployed to production

08

Schedule periodic service pack upgrades as part of operations maintenance and never try to have **more than two service packs behind**

Countermeasures: Protocols



01

Block all unnecessary ports, Internet Control Message Protocol (ICMP) traffic, and unnecessary protocols such as NetBIOS and SMB



02

Harden the TCP/IP stack and consistently apply the latest software patches and updates to system software



03

If using insecure protocols such as Telnet, POP3, SMTP, FTP, take appropriate measures to provide secure authentication and communication, for example, by using IPSec policies



04

If remote access is needed, make sure that the remote connection is secured properly, by using tunneling and encryption protocols



05

Disable WebDAV if not used by the application or keep secure if it is required



Countermeasures: Accounts



	Remove all unused modules and application extensions	
	Disable unused default user accounts created during installation of an operating system	
	When creating a new web root directory, grant the appropriate (least possible) NTFS permissions to the anonymous user being used from the IIS web server to access the web content	
	Eliminate unnecessary database users and stored procedures and follow the principle of least privilege for the database application to defend against SQL query poisoning	
	Use secure web permissions, NTFS permissions, and .NET Framework access control mechanisms including URL authorization	
	Slow down brute force and dictionary attacks with strong password policies, and then audit and alert for logon failures	
	Run processes using least privileged accounts as well as least privileged service and user accounts	

Countermeasures: Files and Directories



Eliminate unnecessary files within the **.jar files**



Disable serving of **directory listings**

Eliminate **sensitive configuration** information within the **byte code**



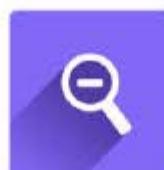
Eliminate the **presence of non web files** such as archive files, backup files, text files, and header/include files

Avoid mapping **virtual directories** between two different servers, or over a network



Disable serving certain **file types** by creating a resource mapping

Monitor and check all **network services logs**, **website access logs**, **database server logs** (e.g., Microsoft SQL Server, MySQL, Oracle) and OS logs frequently



Ensure the presence of **web application** or **website files** and **scripts** on a separate partition or drive other than that of the operating system, logs, and any other system files

Detecting Web Server Hacking Attempts



Use **Website Change Detection System** to detect hacking attempts on the web server

Website Change Detection System involves:



Running specific script on the server that detects any changes made in the existing executable file or new file included on the server



Periodically comparing the **hash values** of the files on the server with their respective master hash value to detect the changes made in codebase



Alerting the user upon any change detection on the server



For example: **WebsiteCDS** is a script that goes through your entire web folder and detects any changes made to the your code base and alert you using email

How to Defend Against Web Server Attacks



01

Ports

- Audit the ports on server regularly to ensure that an **insecure** or unnecessary service is not active on your web server
- Limit inbound traffic to **port 80 for HTTP** and **port 443 for HTTPS (SSL)**
- Encrypt or restrict **intranet traffic**

02

Server Certificates

- Ensure that **certificate data ranges** are valid and that certificates are used for their intended purpose
- Ensure that the certificate has not been revoked and **certificate's public key** is valid all the way to a trusted root authority

03

Machine.config

- Ensure that protected resources are mapped to **HttpForbiddenHandler** and unused **HttpModules** are removed
- Ensure that **tracing is disabled** <trace enable="false"/> and **debug compiles** are turned off

04

Code Access Security

- Implement **secure coding** practices
- Restrict **code access security policy** settings
- Configure IIS** to reject URLs with "../" and install new patches and updates

How to Defend Against Web Server Attacks (Cont'd)



UrlScan

- UrlScan is a security tool that **restricts** the types of HTTP requests that IIS will process
- By blocking specific HTTP requests, the UrlScan security tool helps to **prevent potentially harmful requests** from reaching applications on the server
- UrlScan screens all incoming requests to the server by filtering the requests based on **rules** that are set by the administrator

Services

- UrlScan can be configured to filter HTTP query string values and other HTTP headers to **mitigate SQL injection** attacks while the root cause is being fixed in the application.
- It provides **W3C formatted logs** for easier log file analysis through log parsing solutions like Microsoft Log Parser 2.2

How to Defend Against Web Server Attacks (Cont'd)



- 01

 - Apply **restricted ACLs** and block remote registry administration
 - Secure the **SAM** (Stand-alone Servers Only)
- 02

Ensure that security related settings are **configured appropriately** and access to the metabase file is restricted with hardened **NTFS permissions**
- 03

Remove unnecessary ISAPI filters from the webserver
- 04

 - Remove all unnecessary file shares including the **default administration shares** if not required
 - Secure the shares with restricted **NTFS permissions**
- 05

Relocate sites and virtual directories to **non-system partitions** and use IIS Web permissions to restrict access
- 06

Remove all unnecessary **IIS script mappings** for optional file extensions to avoid exploiting any bugs in the ISAPI extensions that handle these types of files
- 07

Enable a **minimum level of auditing** on your web server and use NTFS permissions to protect the log files

How to Defend Against Web Server Attacks (Cont'd)



Do use a **dedicated machine** as a web server

Do physically protect the **webserver machine** in a secure machine room

Create **URL mappings** to internal servers cautiously

Do not connect an IIS Server to the **Internet** until it is fully hardened

Do not install the **IIS server** on a domain controller

Do not allow anyone to **locally log on** to the machine except for the administrator

Use server side **session ID tracking** and match connections with time stamps, IP addresses, etc.

Do configure a **separate anonymous user account** for each application, if you host multiple web applications

If a database server, such as **Microsoft SQL Server**, is to be used as a backend database, install it on a **separate server**

Limit the **server functionality** in order to support the web technologies that are going to be used

Use **security tools** provided with web server software and **scanners** that automate and make the process of securing a web server easy

Screen and filter the **incoming traffic request**

How to Defend against HTTP Response Splitting and Web Cache Poisoning



Server Admin



- Use latest **web server software**
- Regularly **update/patch OS** and webserver
- Run **web Vulnerability Scanner**

Application Developers



- Restrict web application access to **unique IPs**
- Disallow **carriage return** (%0d or \r) and line feed (%0a or \n) characters
- Comply to **RFC 2616** specifications for HTTP/1.1

Proxy Servers



- Avoid sharing **incoming TCP connections** among different clients
- Use different TCP connections with the proxy for different **virtual hosts**
- Implement “**maintain request host header**” correctly

How to Defend against DNS Hijacking



Choose an ICANN accredited **registrar** and encourage them to set **Registrar Lock** on the domain name



Safeguard the **registrant account information**



Include DNS hijacking into **incident response and business continuity planning**



Use DNS monitoring tools/services to **monitor DNS server IP address and alert**



Avoid downloading **audio and video codecs** and other downloaders from untrusted websites



Install **antivirus** program and update it regularly



Change the **default router password** that comes with the factory settings

Module Flow



Patches and Hotfixes



Hotfixes are an **update to fix a specific customer issue** and not always distributed outside the customer organization

A patch is a **small piece of software designed to fix problems**, security vulnerabilities, and bugs and improve the performance of a computer program or its supporting data

Users may be notified through **emails** or through the **vendor's website**

A patch can be considered as a **repair job to a programming problem**

Hotfixes are sometimes packaged as a set of fixes called a **combined hotfix** or **service pack**

What is Patch Management?



"Patch management is a process used to ensure that the **appropriate patches** are installed on a system and help fix known vulnerabilities"



An automated patch management process

Detect

Use tools to detect missing security patches

Assess

Asses the issue(s) and its associated severity by mitigating the factors that may influence the decision

Acquire

Download the patch for testing

Test

Install the patch first on a testing machine to verify the consequences of the update

Deploy

Deploy the patch to the computers and make sure the applications are not affected

Maintain

Subscribe to get notifications about vulnerabilities as they are reported

Identifying Appropriate Sources for Updates and Patches



1 First make a **patch management plan** that fits the operational environment and business objectives



2 Find appropriate **updates** and **patches** on the home sites of the applications or operating systems' vendors



3 The recommended way of tracking issues relevant to **proactive patching** is to register to the home sites to **receive alerts**

Installation of a Patch



01

Users can access and install security patches via the **World Wide Web**

Patches can be installed in two ways

Manual Installation

In this method, the user has to **download the patch** from the vendor and fix it



Automatic Installation

In this method, the applications use the **Auto Update** feature to update themselves



Implementation and Verification of a Security Patch or Upgrade



1



Before installing any patch **verify the source**

2



Use proper **patch management program** to validate files versions and checksums before deploying security patches

3



The patch management tool must be **able to monitor the patched systems**

4



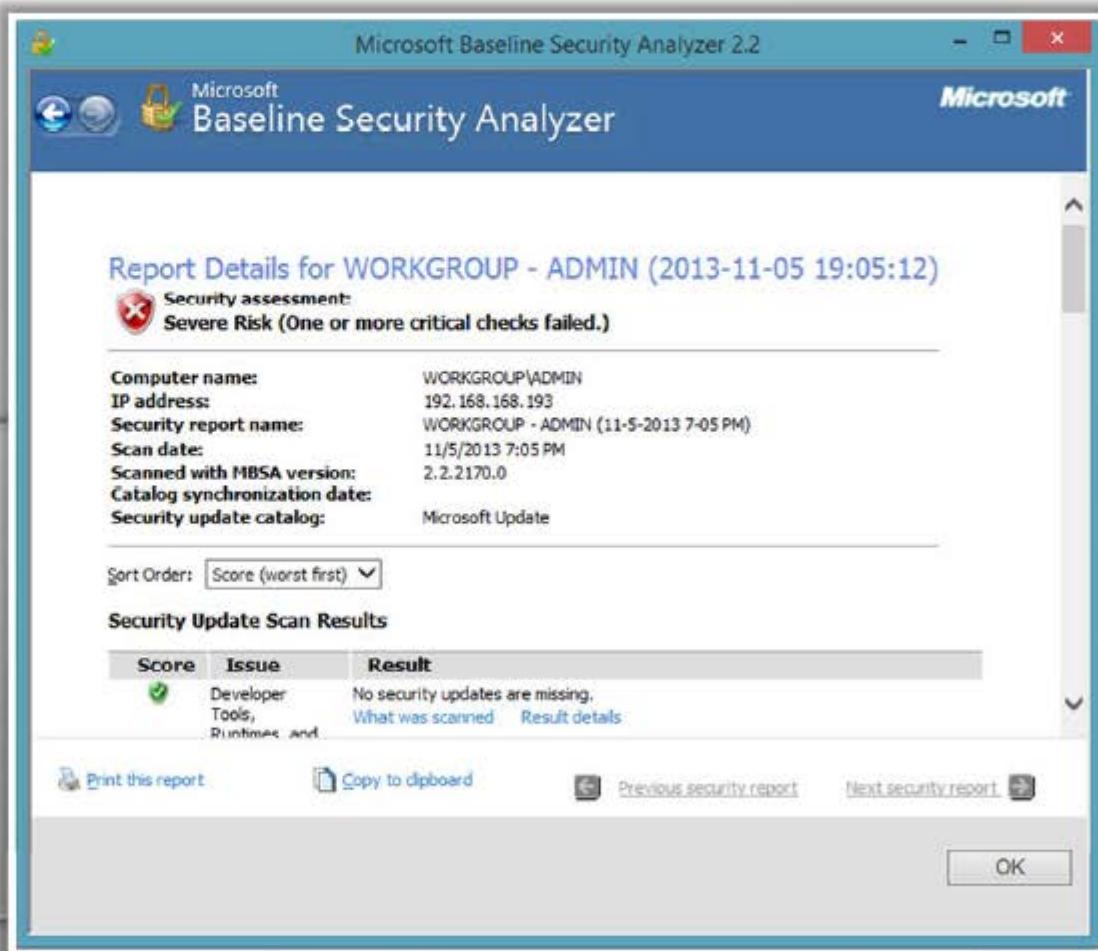
The **patch management team** should check for updates and patches regularly

Patch Management Tool: Microsoft Baseline Security Analyzer (MBSA)

C|EH
Certified Ethical Hacker



- MBSA checks for **available updates** to the operating system, Microsoft Data Access Components (MDAC), MSXML (Microsoft XML Parser), .NET Framework, and SQL Server
- It also scans a computer for insecure **configuration settings**



<http://www.microsoft.com>

Patch Management Tools



Altiris Client Management Suite
<http://www.symantec.com>



GFI LanGuard
<http://www.gfi.com>



Kaseya Security Patch Management
<http://www.kaseya.com>



ZENworks® Patch Management
<http://www.novell.com>



Security Manager Plus
<http://www.manageengine.com>



Prism Suite
<http://www.newboundary.com>



MaaS360® Patch Analyzer Tool
<http://www.maas360.com>



Secunia CSI
<http://secunia.com>



Lumension® Patch and Remediation
<http://www.lumension.com>



VMware vCenter Protect
<http://www.vmware.com>

Module Flow



 Webserver
Concepts

1

 Webserver
Attacks

2

 Attack
Methodology

3

 Webserver
Attack Tools

4

 Counter-
measures

5

 Patch
Management

6

 Webserver
Security Tools

7

 Webserver
Pen Testing

8

Web Application Security Scanners: Syhunt Dynamic and N-Stalker Web Application Security Scanner



Syhunt Dynamic

Syhunt Dynamic helps to automate **web application security** testing and guard organization's **web infrastructure** against various web application security threats

Session 1304713798 [demo.syhunt.com] - Sandcat Pro Hybrid

File Edit View Recent Help Advanced Tools Help

Search Results

demo.syhunt.com

Application Checks

Server Checks

Code Analysis

Time Taken: 27 seconds ago

Time Left: 00:00:01

Vulnerabilities: 10

Requests: 400

Errors: 0

Warnings: 0

Critical: 0

Optimized: 0

Optimized (%): 0

Apache

Last Message: Check Complete [try-use-XSS-27]

Event List

Main Vulnerabilities Crawling Discovery JavaScript Protocol Debug

SandcatCS.exe executed.

Launching SandcatCS.exe... [demo.syhunt.com:80-inSession-1304713798-node-Index...]

Module loaded with pid:244

Analyzing index...

Analyzing index Done.

Checking robots...

Checking robots file: robots...

Spidering/Crawling Stage initiated.

Spidering/Crawling Stage completed.

Starting application vulnerability checks...

Testing web application for vulnerabilities...

Starting Class/Site Scripting Test...

Found < basic.php/XSS

Found < basic.php/XSS

Found < login.php/XSS

Found index_hidden.php/XSS

Check [Data Site Spider /HS-29.. 1 of 200]

demo.syhunt.com

N-Stalker Web Application Security Scanner

N-Stalker is a **WebApp Security Scanner** to search for vulnerabilities such as SQL injection, XSS, and known attacks



N-Stalker Web Application Security Scanner X - Free Edition

Start Scan Thread 4 Engine & Scanner Settings URL Redirection Settings Scan Details Scan Spiders Control Scan Engine Thread 15 Coding HTTP+HTTP Control False-Positive Control

Website Tree Scanner Events Scanner Dashboard

Scanner

- Dashboard
- Site Sequence
- Allowed Hosts
- Rejected Hosts

Objects

- Cookies
- Scripts (2)
- Comments
- Web Forms (4)
- E-mails
- Broken pages (1)
- Hidden Fields
- Information Leakage

Vulnerabilities

- http://www.certifiedhacker.com

Scan Status

- Completed: Spider
- Completed: Run Modules
- Completed: Big Scanner

Scan Details

Scan Session:

- Start Time: Nov 8, 2013 11:30:22
- Duration: 9 Hours + 4 Minutes

Spider Engine:

- Crawled URLs: 10
- Crawled Hosts: 1
- Default Page Size: 8,648 bytes

Network

- Total Requests: 632
- Failed Requests: 0
- Attack: 400
- 404 Errors: 561
- 302 Redirection: 0
- Bytes Sent: 179,028
- Bytes Received: 1,495,297
- Avg Response Time: 0.16 s
- Avg Transfer Rate: 70.59 KB/s
- Requests/Minute: 155.00 requests

Component Name URL Location Comments

- Web Server Information Found: Microsoft-IIS/6.0 http://www.certifiedhacker.com:80/ (Port: 80)
- Web Server Technology Detected: Unknown Server http://www.certifiedhacker.com:80/ (Port: 80)

Scan Modes Components Scan Events Module Events

Notice: N-Stalker Scanner session is being closed...[Desktop Thread]

<http://www.syhunt.com>

<http://www.nstalker.com>

Web Server Security Scanners: Wikto and Acunetix Web Vulnerability Scanner



Wikto



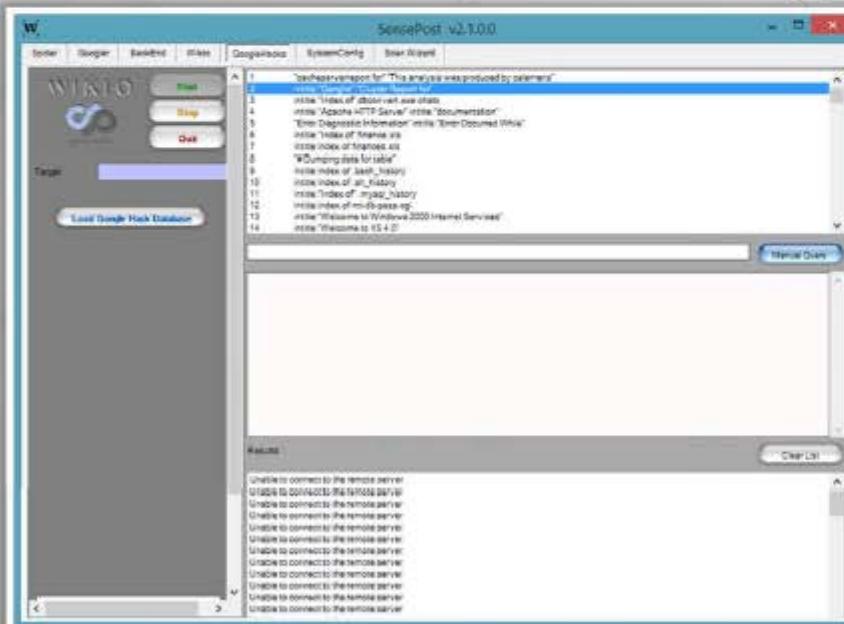
Wikto is a **web server security scanner** for windows

- Fuzzy logic error code checking
- Google assisted directory mining
- Back-end miner
- Real time HTTP request/response monitoring

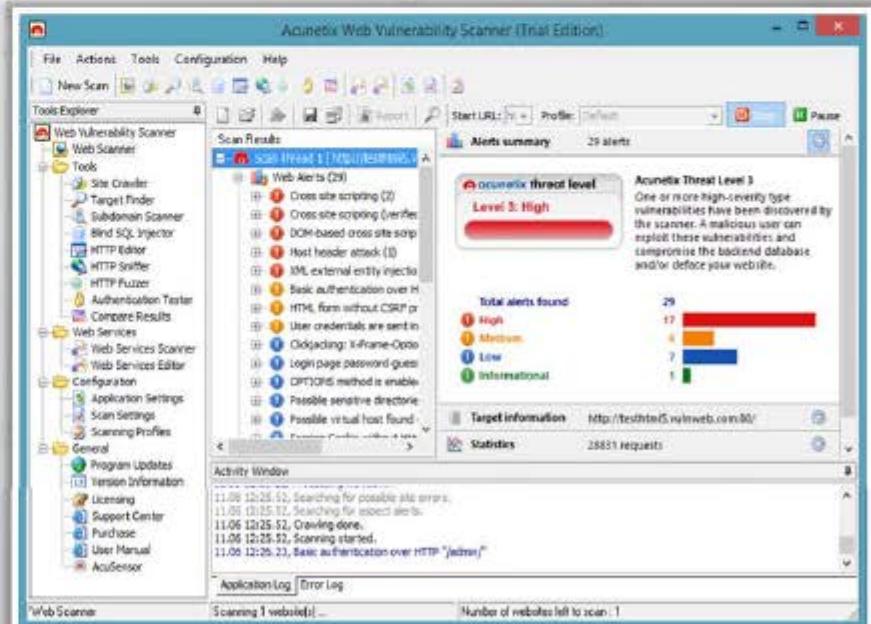


Acunetix Web Vulnerability Scanner

- Acunetix WVS **checks web applications** for SQL injections, cross-site scripting, etc.
- It includes advanced penetration testing tools to ease **manual security audit processes**, and also creates professional security audit and regulatory compliance reports



<http://www.sensepost.com>



<http://www.acunetix.com>

Web Server Malware Infection Monitoring Tool: HackAlert



HackAlert is a **cloud-based service** that identifies hidden zero-day malware and drive-by downloads in websites and online advertisements

Features

- Protects clients and customers from malware injected websites
- Identifies malware
- Displays injected code snippets
- Deploys as cloud-based SaaS
- Integrates with WAF or web server modules for instant mitigation

The screenshot shows the HackAlert dashboard with the following details:

7 Days Report

- Change Period Ending Date and Select Site: 2010-06-03, Submit
- All Sites
- Period: 2010-05-28 - 2010-06-03
- Number of Sites Monitored: 3
- Total Scans Performed: 152
- Active Exploits detected: 8
- Blacklisted URLs detected: 8
- AV Flagged: 2
- Suspicious URLs detected: 1

Details

Privileges: System Admin
Action: Logout Account Settings

Links: Clean URLs, Active Exploits, Blacklisted URLs, AV Flagged, Suspicious URLs, Connection Issues

Date	Action	Clean URLs
2010-05-28 00:23:59	Malicious	52
2010-05-28 01:23:59	Malicious	54
2010-05-28 02:23:59	Malicious	52
2010-05-28 03:23:59	Malicious	52
2010-05-28 04:22:02	Malicious	54
2010-05-28 05:00:08	Malicious	54
2010-05-28 05:34:02	Malicious	54
2010-05-28 06:21:57	Malicious	53
2010-05-28 07:31:57	Malicious	53
2010-05-28 08:22:57	Malicious	54
2010-05-28 09:23:57	Malicious	54
2010-05-28 10:22:30	Malicious	54
2010-05-28 11:22:37	Malicious	54
2010-05-28 12:23:31	Malicious	53
2010-05-28 13:23:31	Malicious	54
2010-05-28 14:22:31	Malicious	54
2010-05-28 15:23:30	Malicious	54
2010-05-28 16:22:00	Malicious	54
2010-05-28 17:23:29	Malicious	54
2010-05-28 18:23:29	Malicious	54
2010-05-28 19:26:00	Malicious	53
2010-05-28 20:24:59	Malicious	54

<http://www.armozize.com>

Web Server Malware Infection Monitoring Tool: QualysGuard Malware Detection



- QualysGuard® Malware Detection Service scans websites for **malware infections** and **threats**



The image shows two screenshots of the QualysGuard Portal. The left screenshot displays the 'Site Creation' process, Step 5 of 5, titled 'Review and confirm your settings'. It shows the following configuration:

- Site Details:** Title: Test Site; Site URL: <http://www.certifiedhacker.com>
- Tags:** Assigned tags: Malware Content Assets.
- Scan Options:** Maximum Pages: 30; Scan Intensity: High; Headers: No headers have been defined.
- Grant exclusion lists:** White list, White list (Regular Expression), Black list, Black list (Regular Expression).
- Scheduling Information:** Start Date: 19 Nov 2013 11:30AM; End Date: (not specified); Time Zone: (UTC -08:00) Pacific Standard Time (PST America/Los Angeles); Description: (not specified).

The right screenshot shows the 'Scan Management' interface with the 'Scan List' tab selected. It displays a table of scan results:

ID#	Scan Title	Scan Date	Scanned Pages	Status	Sent
1	Test Site	19 Nov 2013	30	Success	100%

<http://www.qualys.com>

Webserver Security Tools



Retina CS
<http://www.beyondtrust.com>



Nscan
<http://nscan.hypermart.net>



NetIQ Secure Configuration Manager
<http://www.netiq.com>



SAINTscanner
<http://www.saintcorporation.com>



HP WebInspect
<https://download.hpsmartupdate.com>



Arirang
<http://monkey.org>



N-Stalker Web Application Security Scanner
<http://www.nstalker.com>



Infiltrator
<http://www.infiltration-systems.com>



WebCruiser
<http://sec4app.com>



dotDefender
<http://www.aplicure.com>

Module Flow



Web Server Penetration Testing



- Web server pen testing is used to **identify, analyze, and report vulnerabilities** such as authentication weaknesses, configuration errors, protocol related vulnerabilities, etc. in a web server
- The best way to perform penetration testing is to **conduct a series of methodical and repeatable tests**, and to work through all of the different application vulnerabilities

Why Webserver Pen Testing?

Verification of Vulnerabilities

To exploit the vulnerability in order to test and fix the issue

Remediation of Vulnerabilities

To retest the solution against vulnerability to ensure that it is completely secure

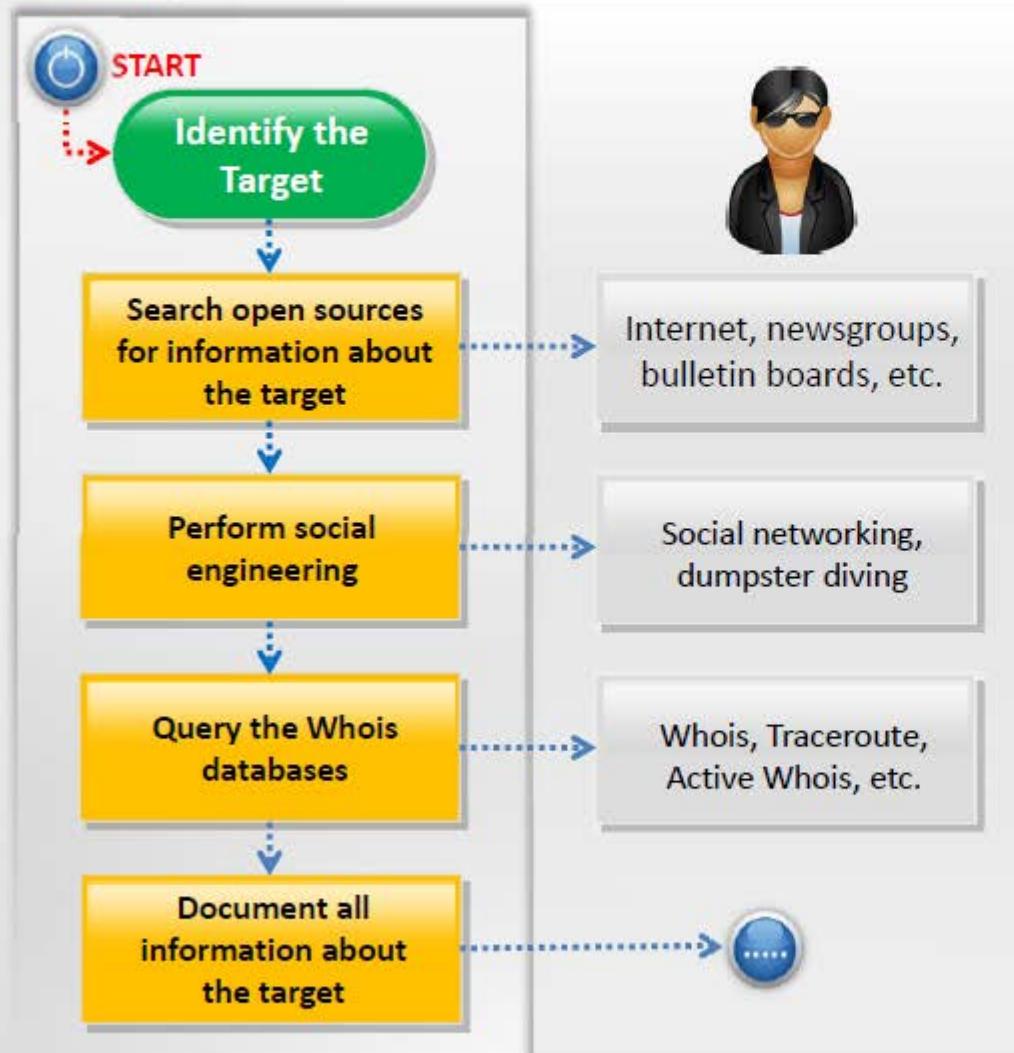


Identification of Web Infrastructure

To identify make, version, and update levels of web servers; this helps in selecting exploits to test for associated published vulnerabilities

Web Server Penetration Testing

(Cont'd)

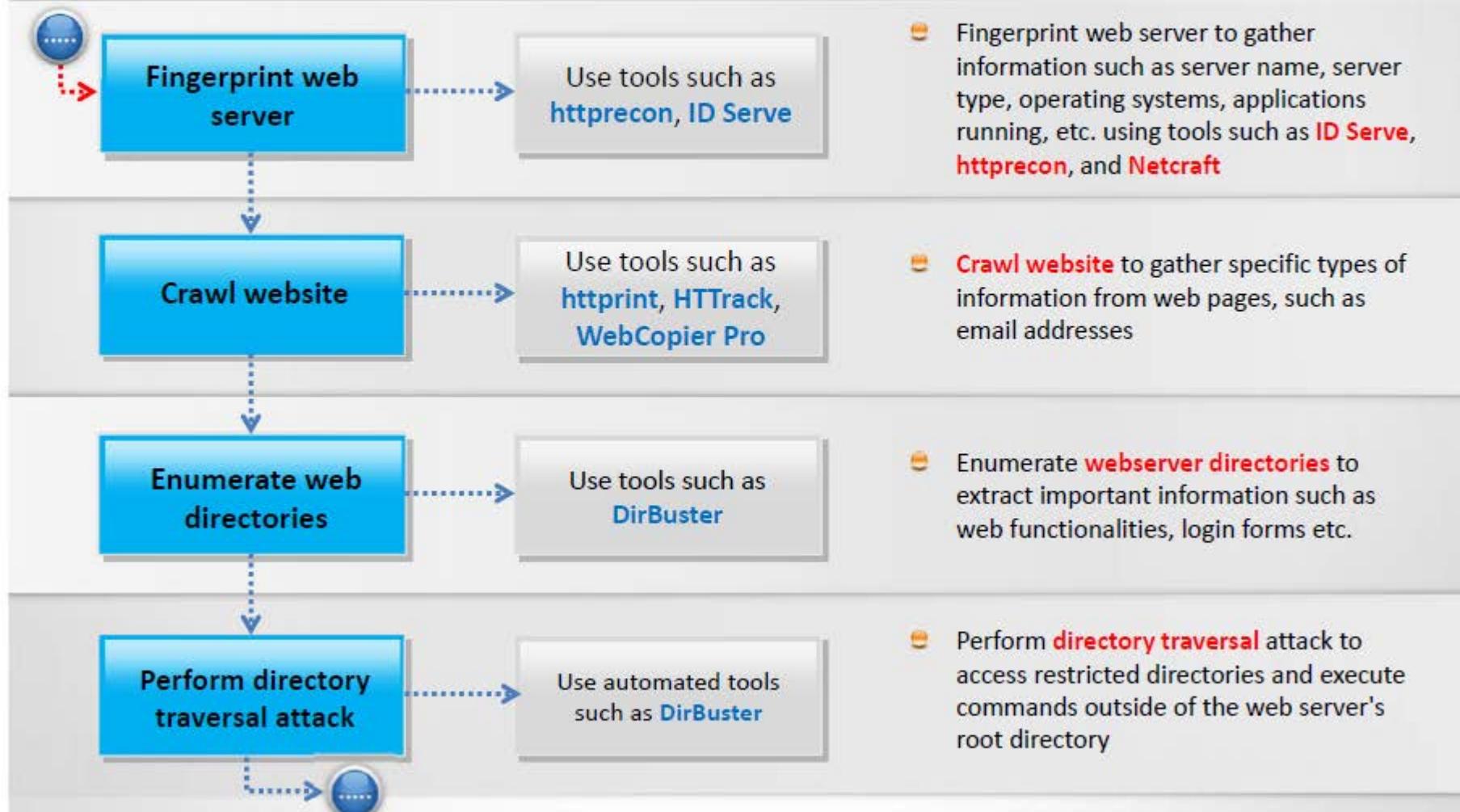


- Webserver penetration testing starts with **collecting as much information** as possible about an organization ranging from its physical location to operating environment
- Use **social engineering techniques** to collect information such as human resources, contact details, etc. that may help in **webserver authentication testing**
- Use **Whois database query tools** to get the details about the target such as domain name, IP address, administrative contacts, Autonomous System Number, DNS, etc.
- Note:** Refer Module 02: Footprinting and Reconnaissance for more information gathering techniques



Web Server Penetration Testing

(Cont'd)



● Fingerprint web server to gather information such as server name, server type, operating systems, applications running, etc. using tools such as **ID Serve**, **httprecon**, and **Netcraft**

● **Crawl website** to gather specific types of information from web pages, such as email addresses

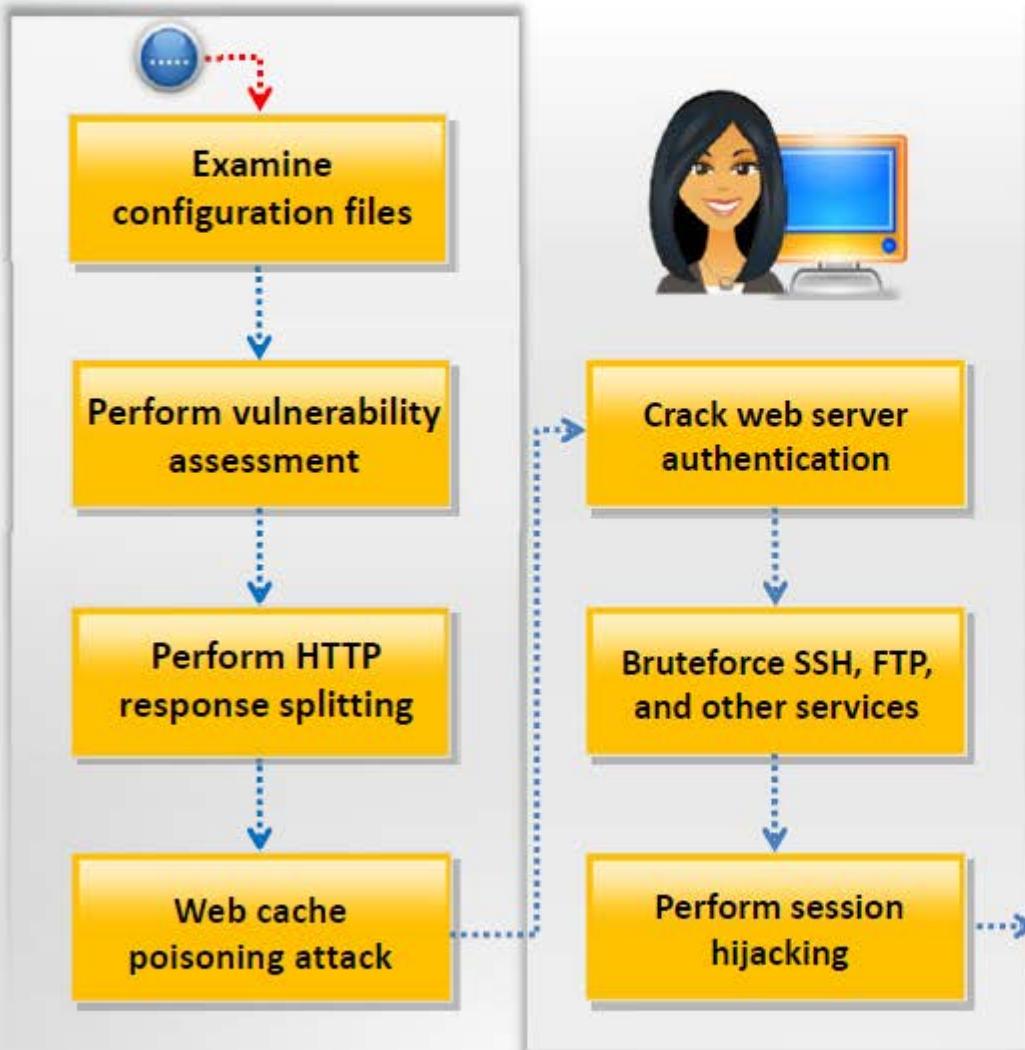
● Enumerate **webserver directories** to extract important information such as web functionalities, login forms etc.

● Perform **directory traversal** attack to access restricted directories and execute commands outside of the web server's root directory

Web Server Penetration Testing

(Cont'd)

CEH
Certified Ethical Hacker



- Perform vulnerability scanning to **identify weaknesses** in a network using tools such as **HP WebInspect**, **Nessus**, etc. and determine if the system can be exploited
- Perform HTTP response splitting attack to pass malicious data to a vulnerable application that includes the data in an HTTP response header
- Perform web cache poisoning attack to force the web server's cache to **flush its actual cache content** and send a specially **crafted request**, which will be stored in cache
- Bruteforce SSH, FTP, and other services login credentials to gain **unauthorized access**
- Perform session hijacking to **capture valid session cookies and IDs**. Use tools such as Burp Suite, Firesheep, Jhijack, etc. to automate session hijacking

Web Server Penetration Testing

(Cont'd)



Perform MITM attack

- Perform MITM attack to access sensitive information by **intercepting and altering communications** between an end-user and web servers

Perform web application pen testing

- **Note:** Refer Module 12: Hacking Web Applications for more information on how to conduct web application pen testing

Examine webserver logs

- Use tools such as Webalizer, AWStats, Ktmatu Relax, etc. to **examine web sever logs**

Exploit frameworks

Document all the findings

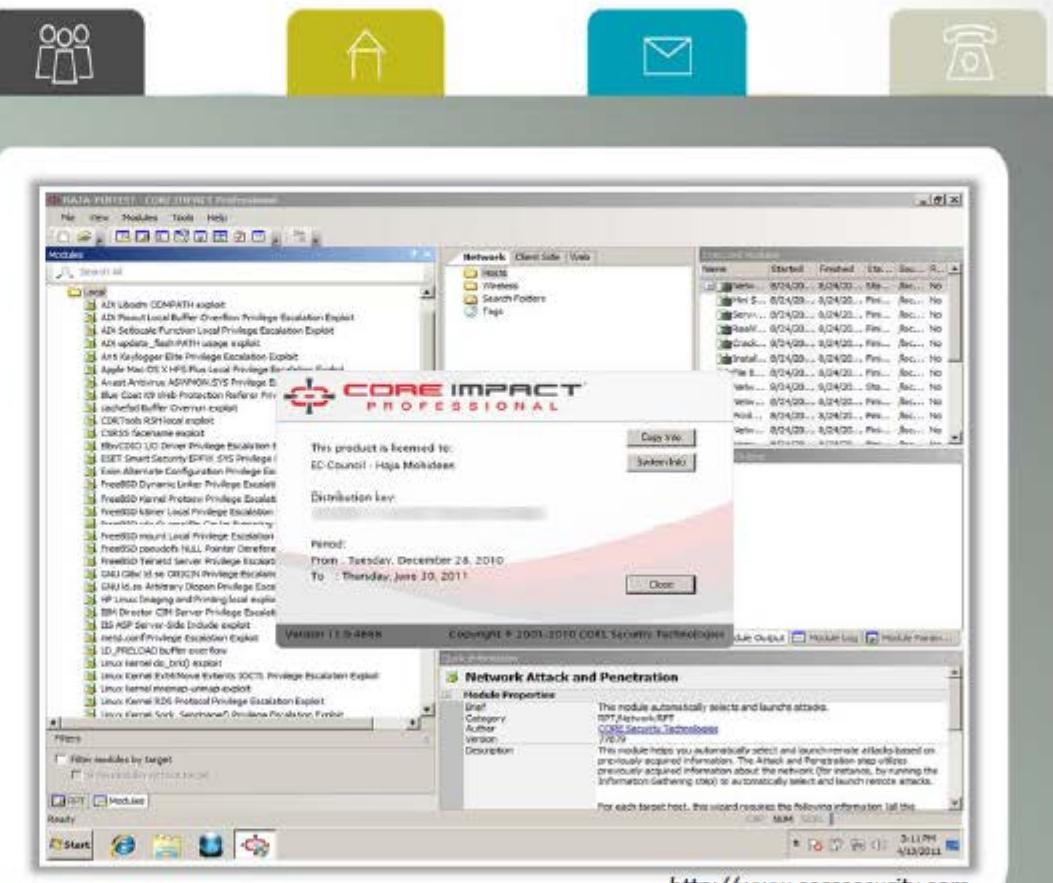
- Use tools such as **Metasploit, w3af**, etc. to exploit frameworks

Web Server Pen Testing Tool: CORE Impact® Pro



CORE Impact® Pro is the software solution for assessing and testing **security vulnerabilities** in the organization:

- Web Applications
- Network Systems
- Endpoint systems
- Wireless Networks
- Network Devices
- Mobile Devices
- IPS/IDS and other defenses



<http://www.coresecurity.com>

Web Server Pen Testing Tool: Immunity CANVAS



CANVAS is an automated exploitation system, and a comprehensive, reliable **exploit development framework** to security professionals and penetration testers



The screenshot shows the Immunity CANVAS software interface. At the top, there's a menu bar with File, Listeners, Session, and Help. Below the menu, there are fields for Target Host (10.10.31.1), Current Callback (127.0.0.1), and Current Target(s) (127.0.0.1). A 'Screen Shots' button is also present. The main window has a 'Modules' tab selected, showing a list of categories like Favorites, New, Exploits, Trojans, Commands, DoS, Tools, Recon, Servers, ImportExport, and Fuzzers. A search bar is located above the module list. A central panel displays a 'View' section with options like CANVAS World Map and CmdLine. A modal dialog box titled 'Add a Host' is open, containing a text input field with '172.16.173.132' and two buttons: 'Cancel' and 'OK'. At the bottom, there are tabs for Current Status, Canvas Log, Debug Log, and Data View, along with a 'Set Covertness' slider set to 1.0. A status bar at the bottom shows '202 ENGINES'.

This screenshot shows the Immunity CANVAS interface with a different configuration. The top bar includes Listener, Stop Exploit, OS Config, and a new 'Ins config' option. The main window shows a 'Node Tree' panel with a tree view of nodes, including a selected 'Localnode' entry. To the right is an 'Exploit Description' panel with tabs for Node Management, Classic Node View, CANVAS World Map, and CmdLine. The bottom panel shows a 'Current Status' section with log entries from a terminal window. The log entries include:

```
Tue 2 14:52:18 [!] Your CANVAS subscription is registered to bob@example.com  
Tue 2 14:52:18 [!] If you are getting close to expiring, contact 212-534-6857 or admin@immunityinc.com  
to renew.  
Tue 2 15:25:44 [!] Getting name for 172.16.173.132  
Tue 2 15:25:44 [!] Get host by name result: 172.16.173.132  
Tue 2 15:25:44 [!] Country code of 172.16.173.132: none  
Tue 2 15:25:44 [!] Host added: 172.16.173.132
```

At the bottom, there's a 'Set Covertness' slider at 1.0 and a status bar with '202 ENGINES'.

<http://www.immunitysec.com>

Web Server Pen Testing Tool: Arachni



Arachni is an open source, feature-full, modular, high-performance Ruby framework aimed towards helping penetration testers and administrators evaluate the **security of web applications**



The screenshot shows the Arachni v0.4.0 - WebUI v0.4.3 interface. At the top, it displays the URL <http://testfire.net>. Below the URL, there's a progress bar indicating the scan is 0% complete. The main area is titled "Issues" and lists several findings:

Type	Count	URL	Input	Element	
Path Traversal	1	The web application exhibits improper validation of a parameter to a restricted directory. (CWE)	GET /index.php?path=../../../../etc/passwd	Form	Link
Cross-site Scripting (XSS)	3	Client-side code (JavaScript) can be injected into the web application, which is then rendered by the user's browser. This can lead to a compromise of the client system or serve as a starting point for other attacks. (CWE)	GET /index.php?search=script%20injection	Search	Form
SQL Injectors	2	SQL code can be injected into the web application. (CWE)	GET /index.php?search=script%20injection	Search	Form

<http://www.arachni-scanner.com>

Module Summary



- ❑ Web servers assume critical importance in the realm of Internet security
- ❑ Vulnerabilities exist in different releases of popular web servers and respective vendors patch these often
- ❑ The inherent security risks owing to the compromised web servers have impact on the local area networks that host these websites, even on the normal users of web browsers
- ❑ Looking through the long list of vulnerabilities that had been discovered and patched over the past few years, it provides an attacker ample scope to plan attacks to unpatched servers
- ❑ Different tools/exploit codes aid an attacker in perpetrating web server's hacking
- ❑ Countermeasures include scanning for the existing vulnerabilities and patching them immediately, anonymous access restriction, incoming traffic request screening, and filtering