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?

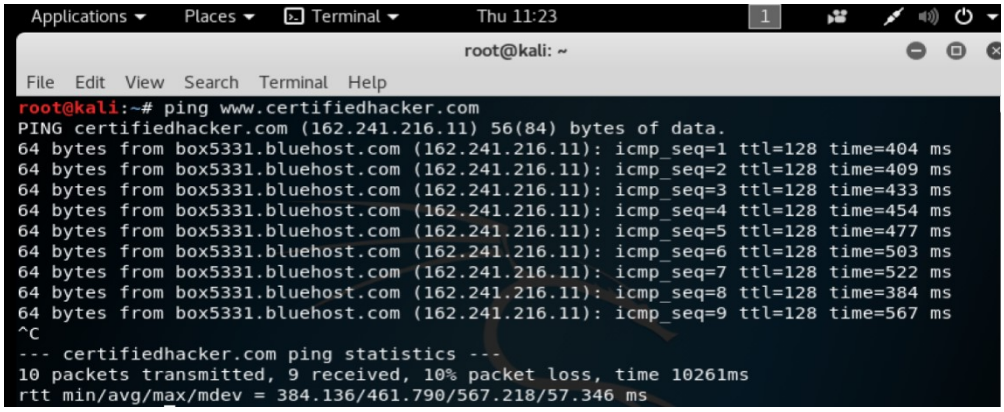
In a black-box testing, the penetration tester is placed in the role of the average hacker, with no internal knowledge of the target system. Testers are not provided with any architecture diagrams or source code that is not publicly available. A black-box penetration test determines the vulnerabilities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

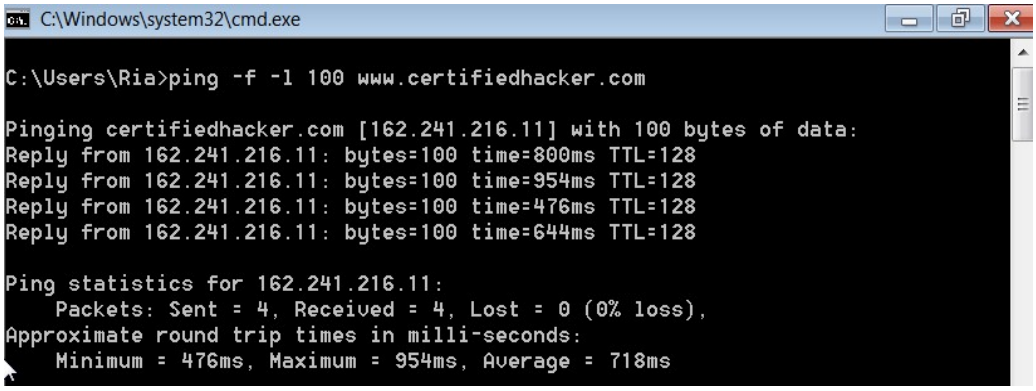
STAGE 1 - PLANNING AND RECONNAISSANCE

In this stage, we define the scope and goals of a test which includes the systems to be adressed 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.





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 - Unif 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
```

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	*Not Present*		
Keywords	*Not Present*		
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	*Not Present*	**Reverse DNS**	bo
Domain registrar	networksolutions.com	**Nameserver organisation**	wh
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		

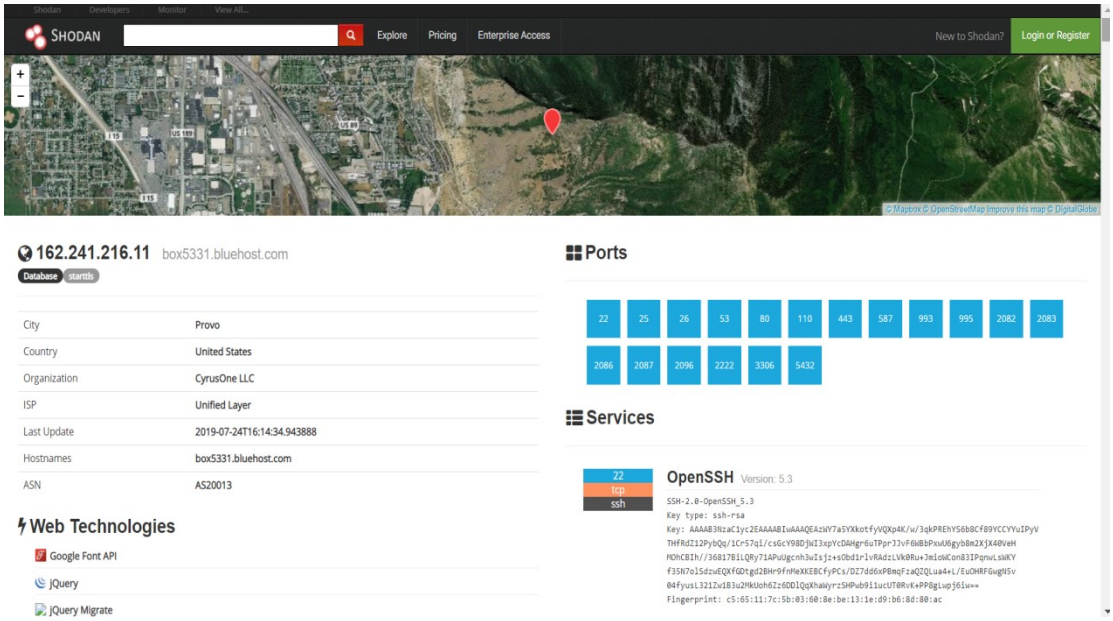
Last Reboot (125 days ago)

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

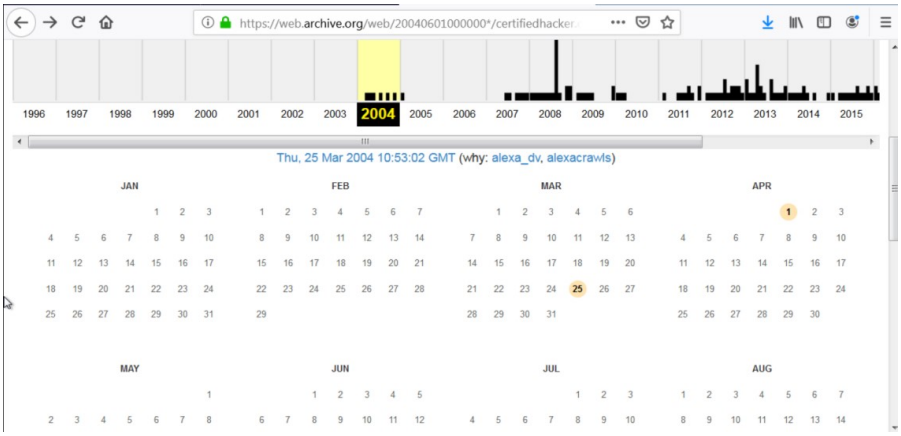
SHODAN -

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.

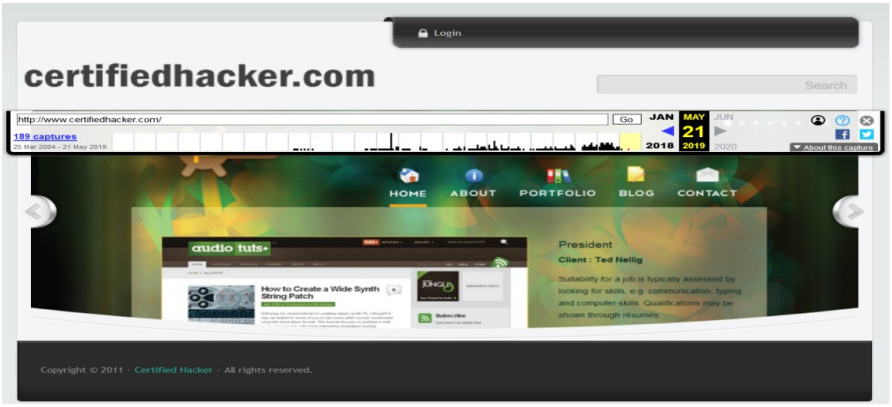


WEBSITE HISTORY -

For this, we use a website named a*rchives.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.



CEH Classroom Attack Lab Website



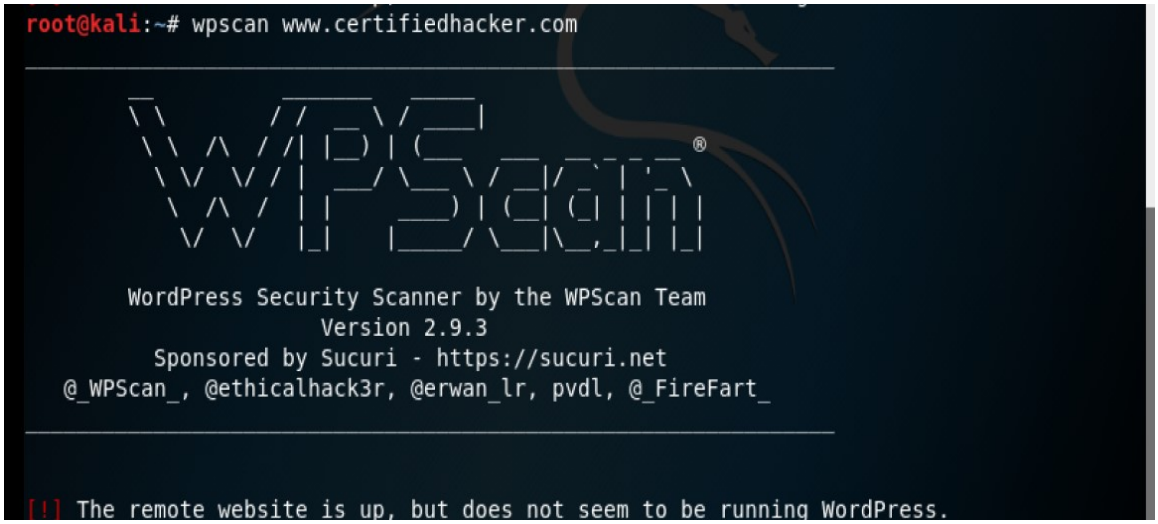
STAGE 2 - SCANNING

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 -

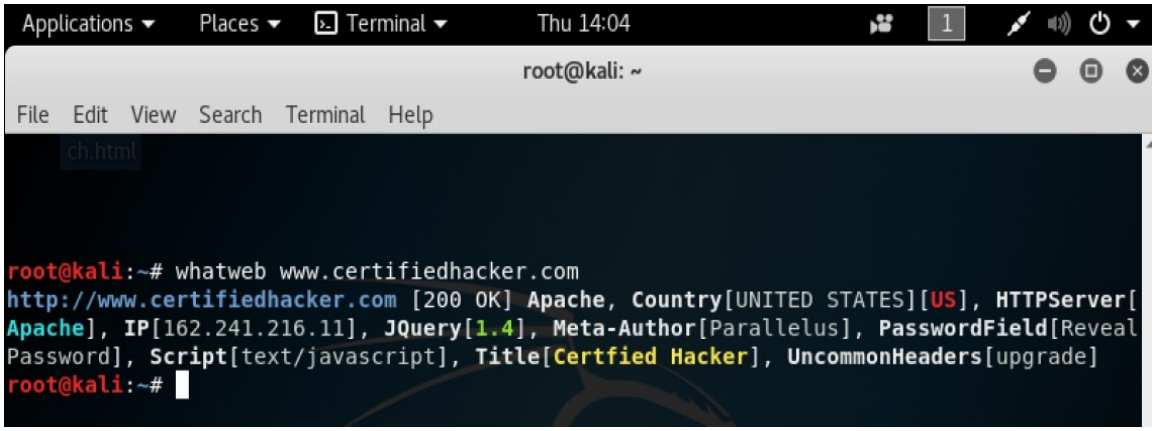
WPScan is a black box WordPress vulnerability scanner that can be used to scan remote WordPress installations to find security issues.

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



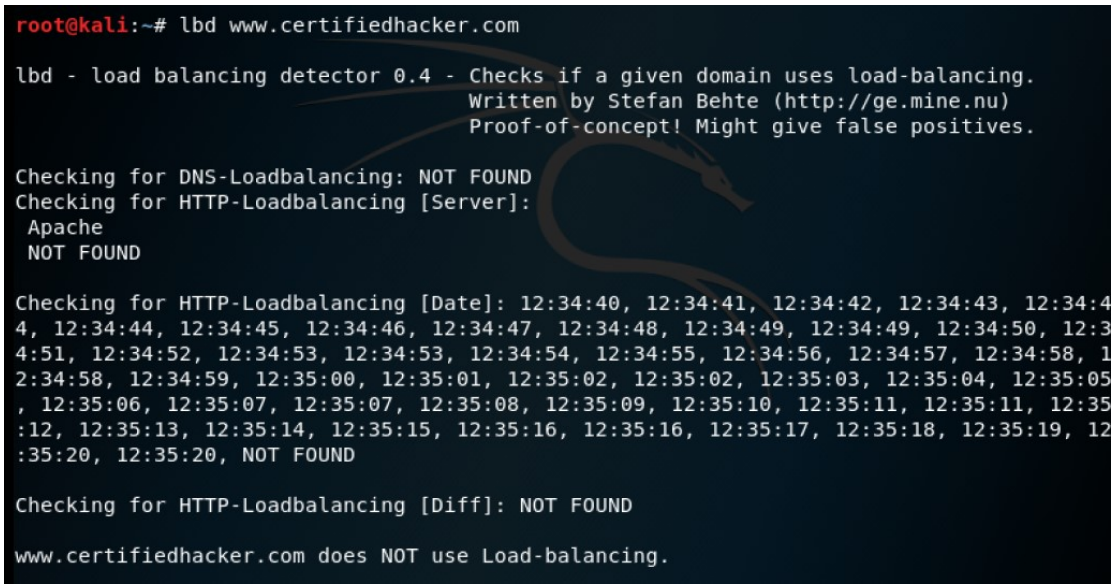
Whatweb-

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



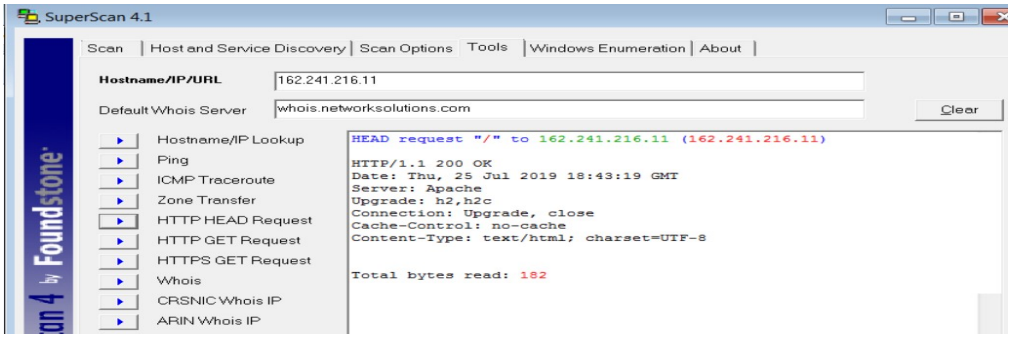
Load Balancer -

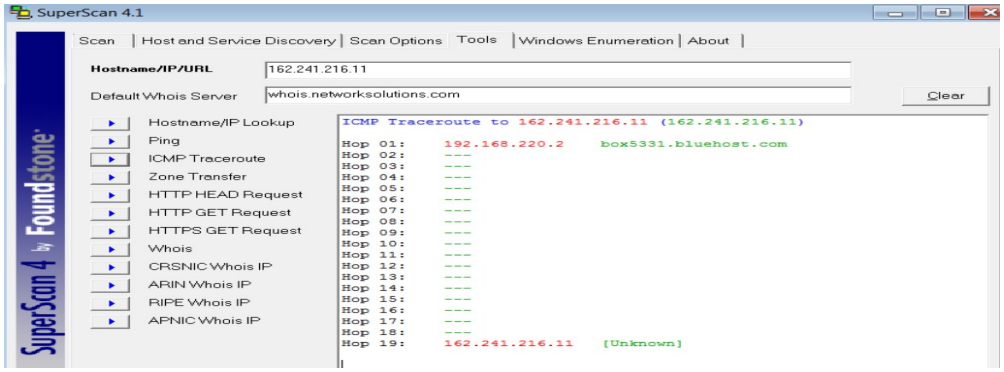
lbd (Load balancing detector) detects if a given domain uses DNS and/or HTTP Load-Balancing.

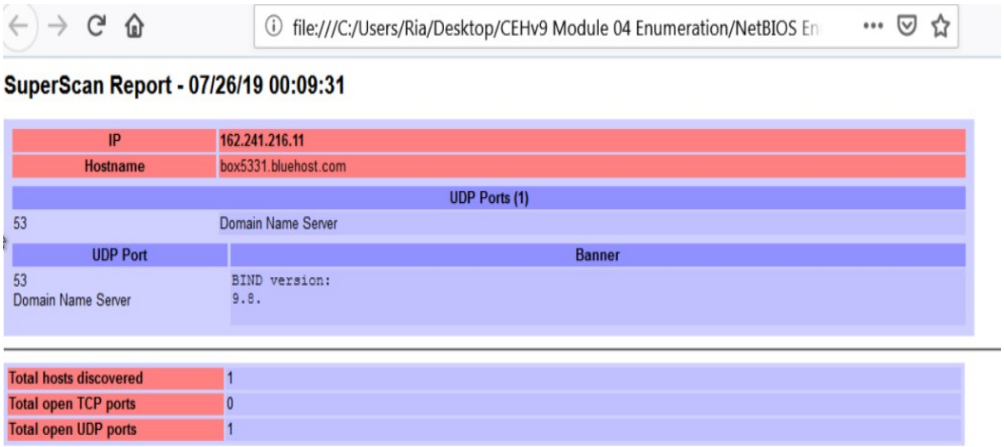


SuperScan –

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.

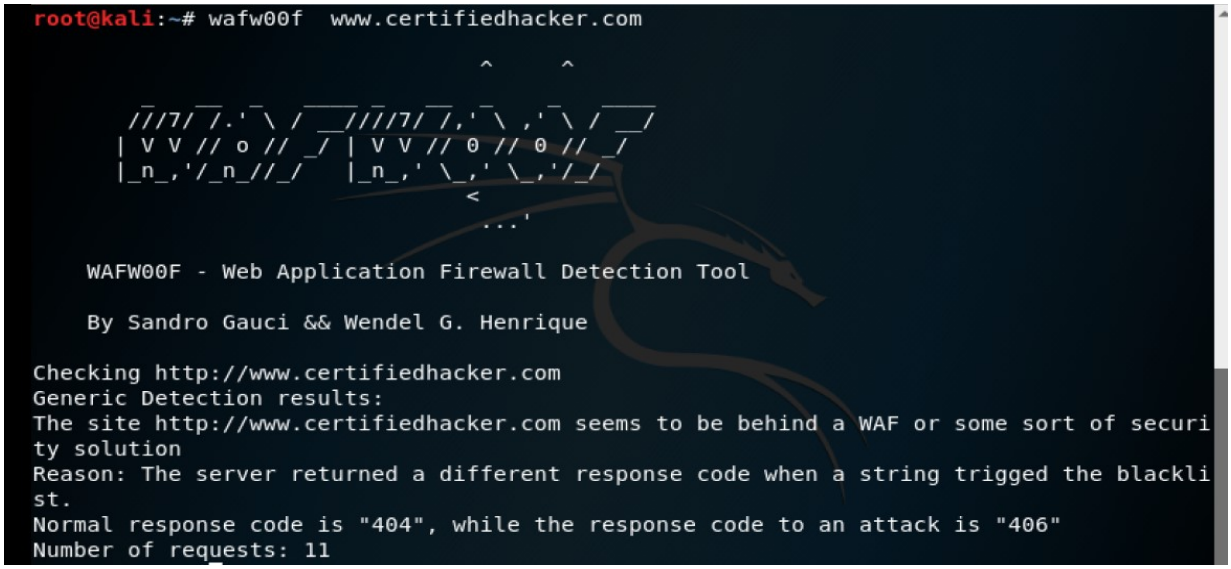






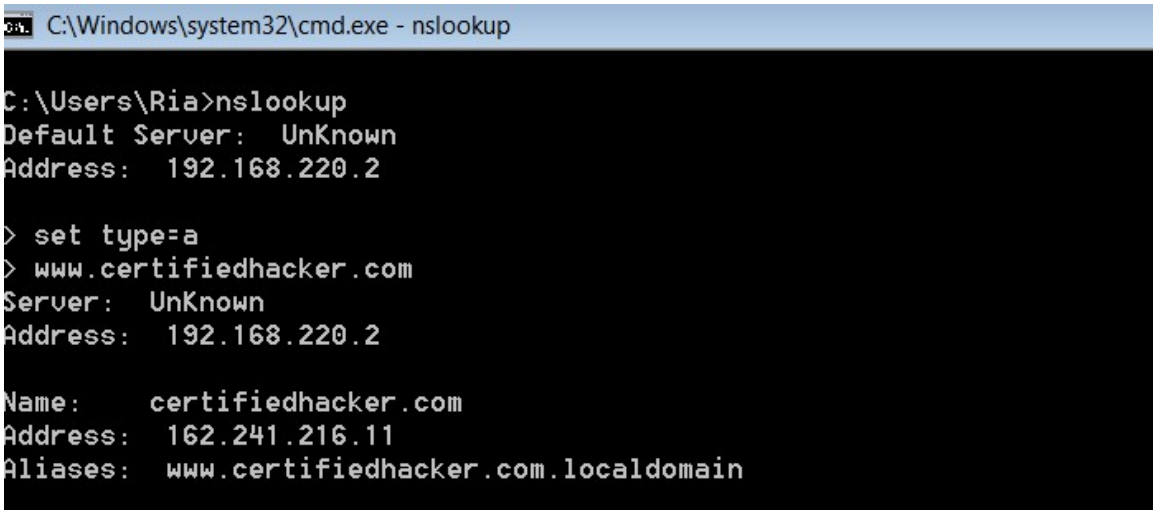
Firewall testing using *waf00f* -

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



NSLOOKUP -

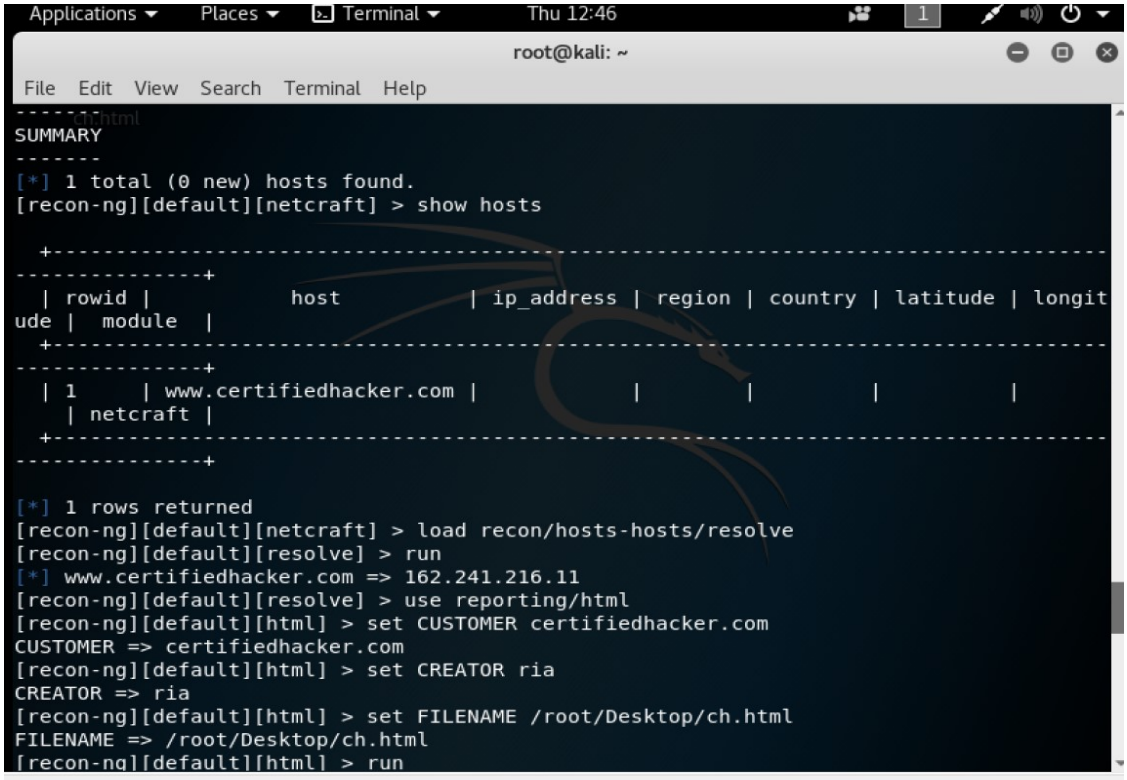
Nslookup (name server lookup) command is used in Kali to obtain DNS details such as IP Address of a particular computer system, the MX records for a domain or the NS servers of a domain.



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.

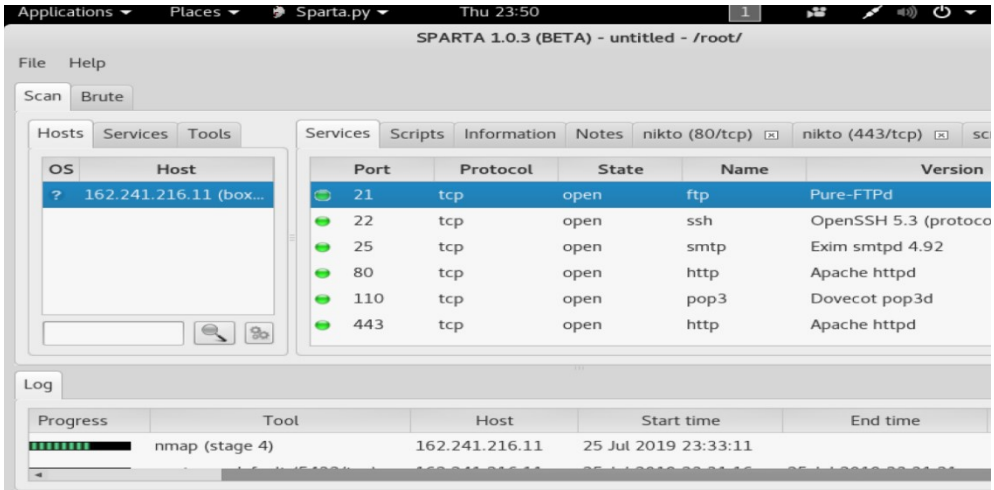
Recon-ng -

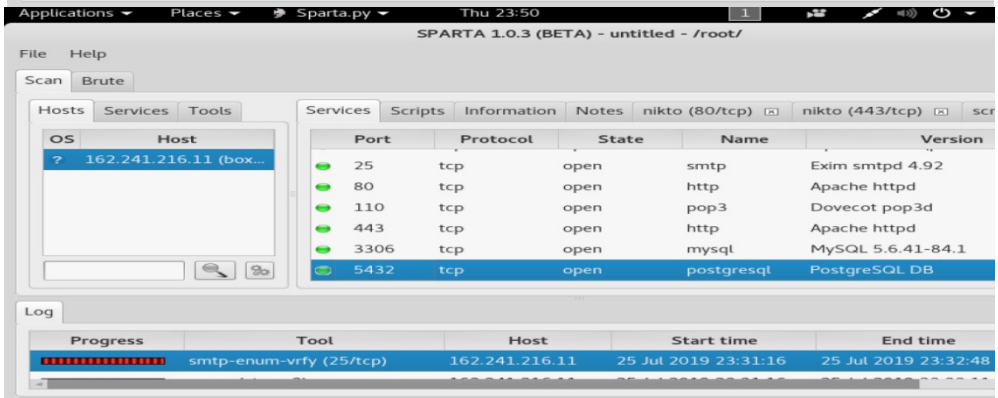
Recon-ng is a tool pre-installed in Linux Operating System. It can be opened manually by typing *recon-ng* in the terminal. It is a powerful tool which can be used to gather information like host, IP Address, Region, Country, Vulnerabilities etc.

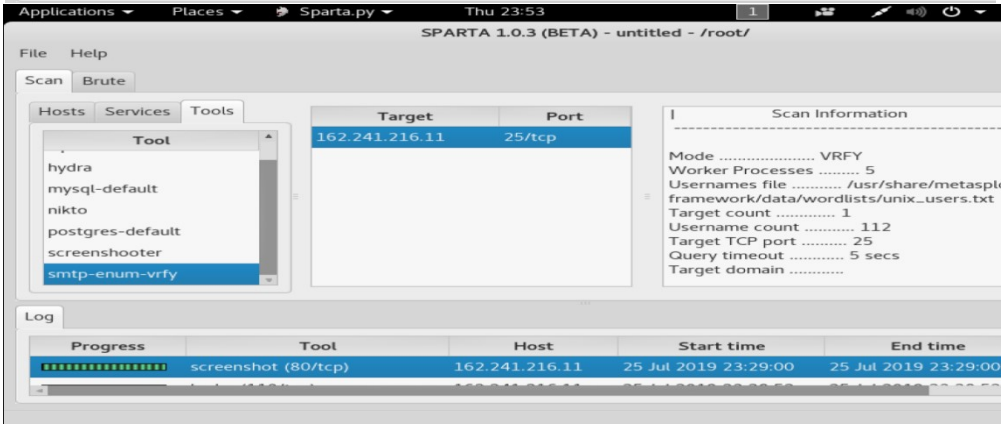


Sparta -

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.





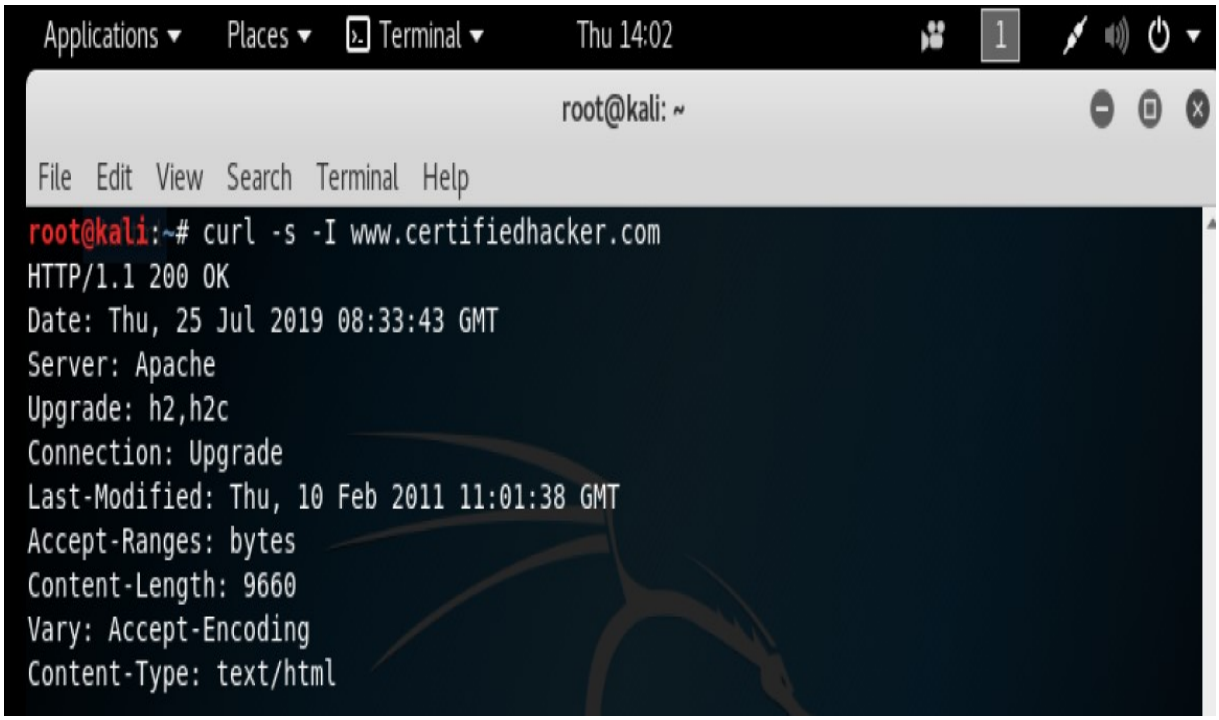


STAGE 3 - SERVER PENETRATION

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.

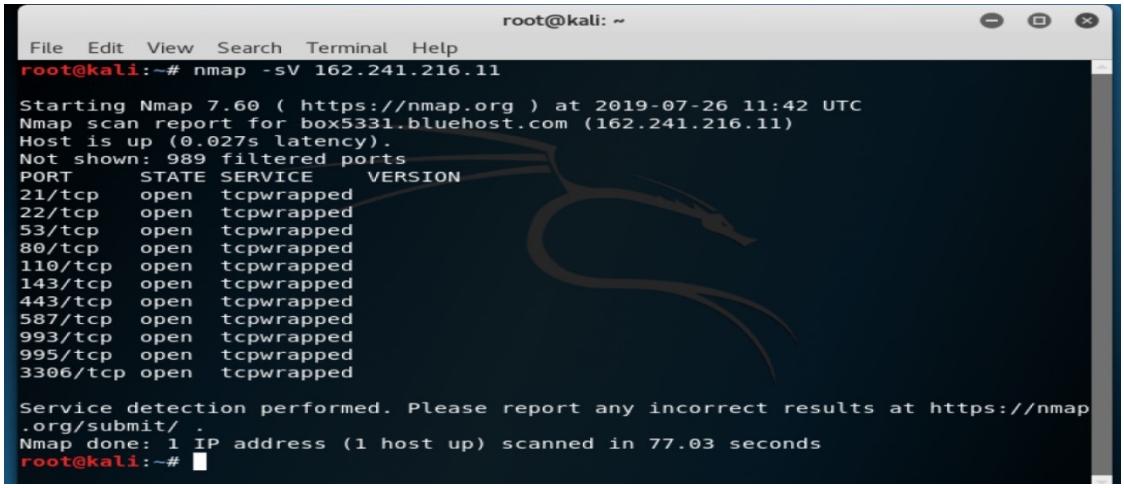
Curl -

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



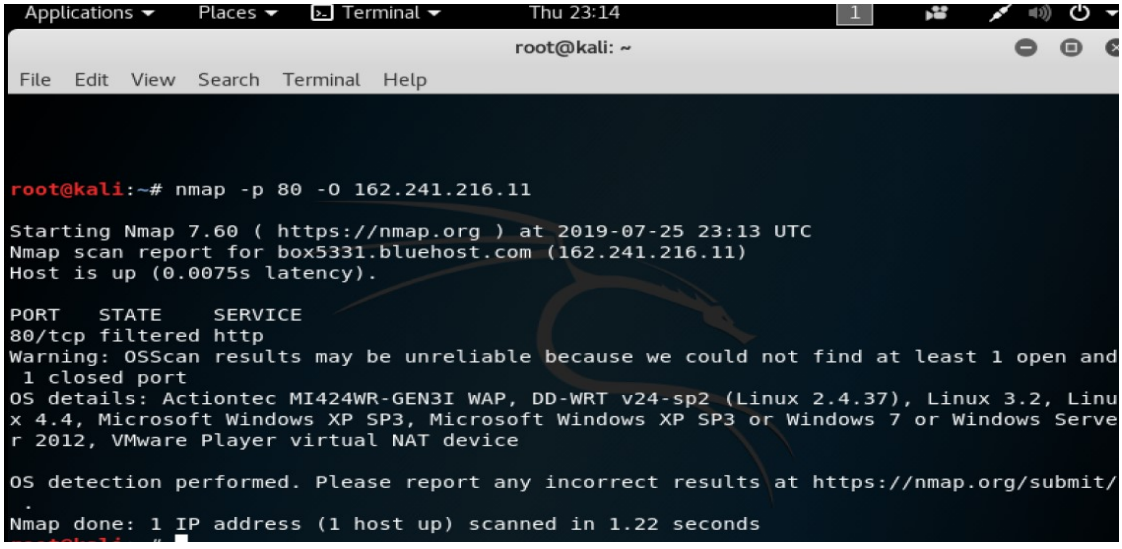
NMAP -

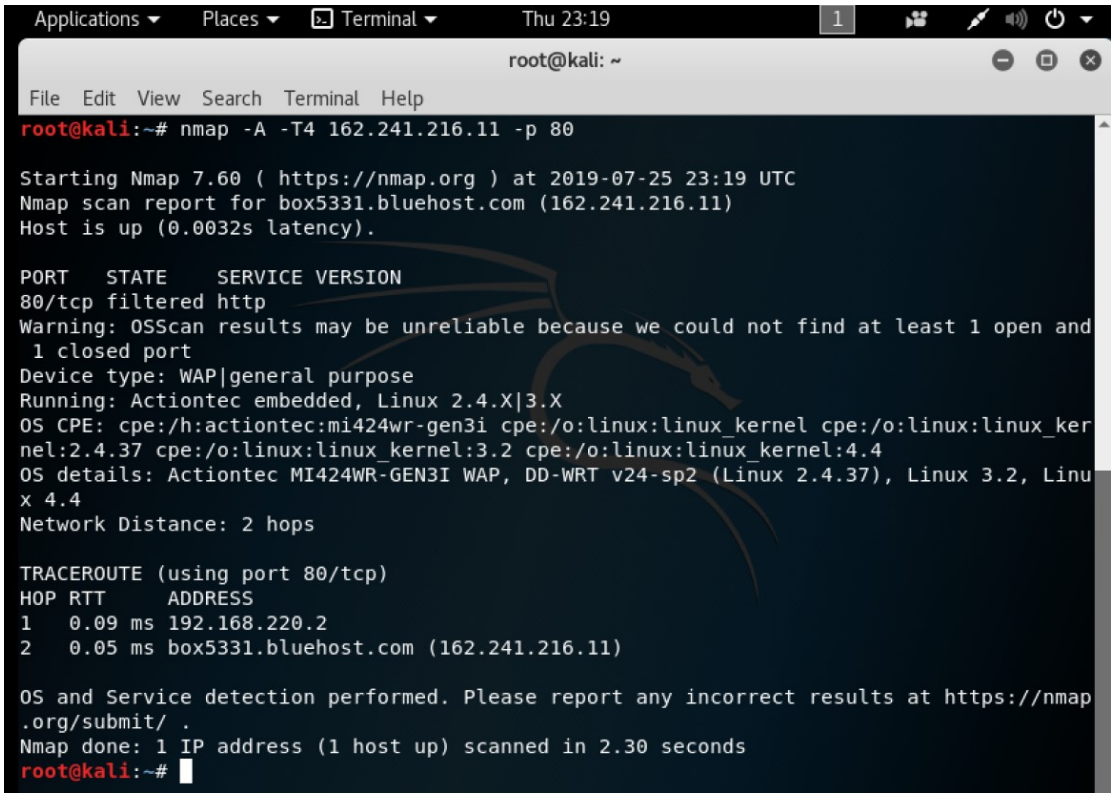
Nmap is a tool in kali which is used to get information about the open ports on the server, which is a very critical intel.



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.



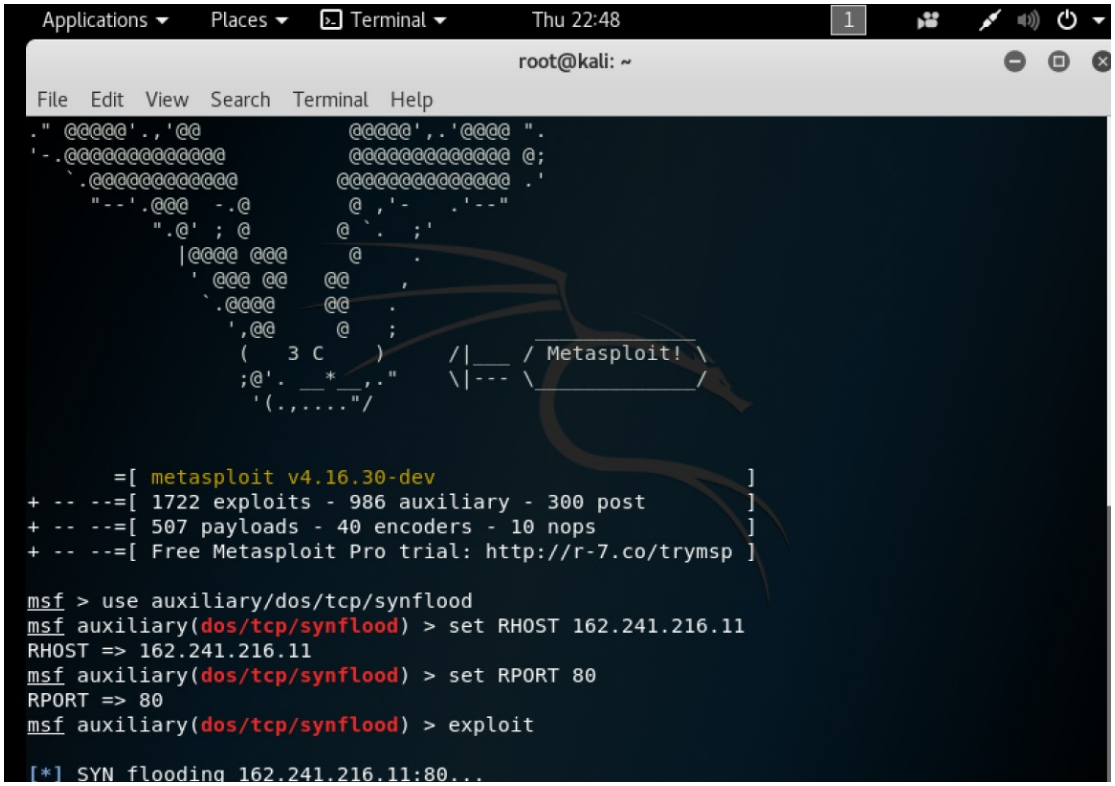


This command give us more idea about port 80.

DENIAL OF SERVICE USING METASPLOIT :

DOS :

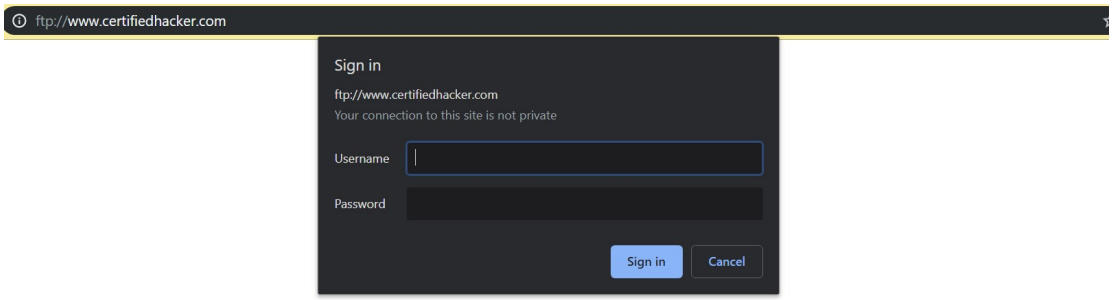
Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.



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

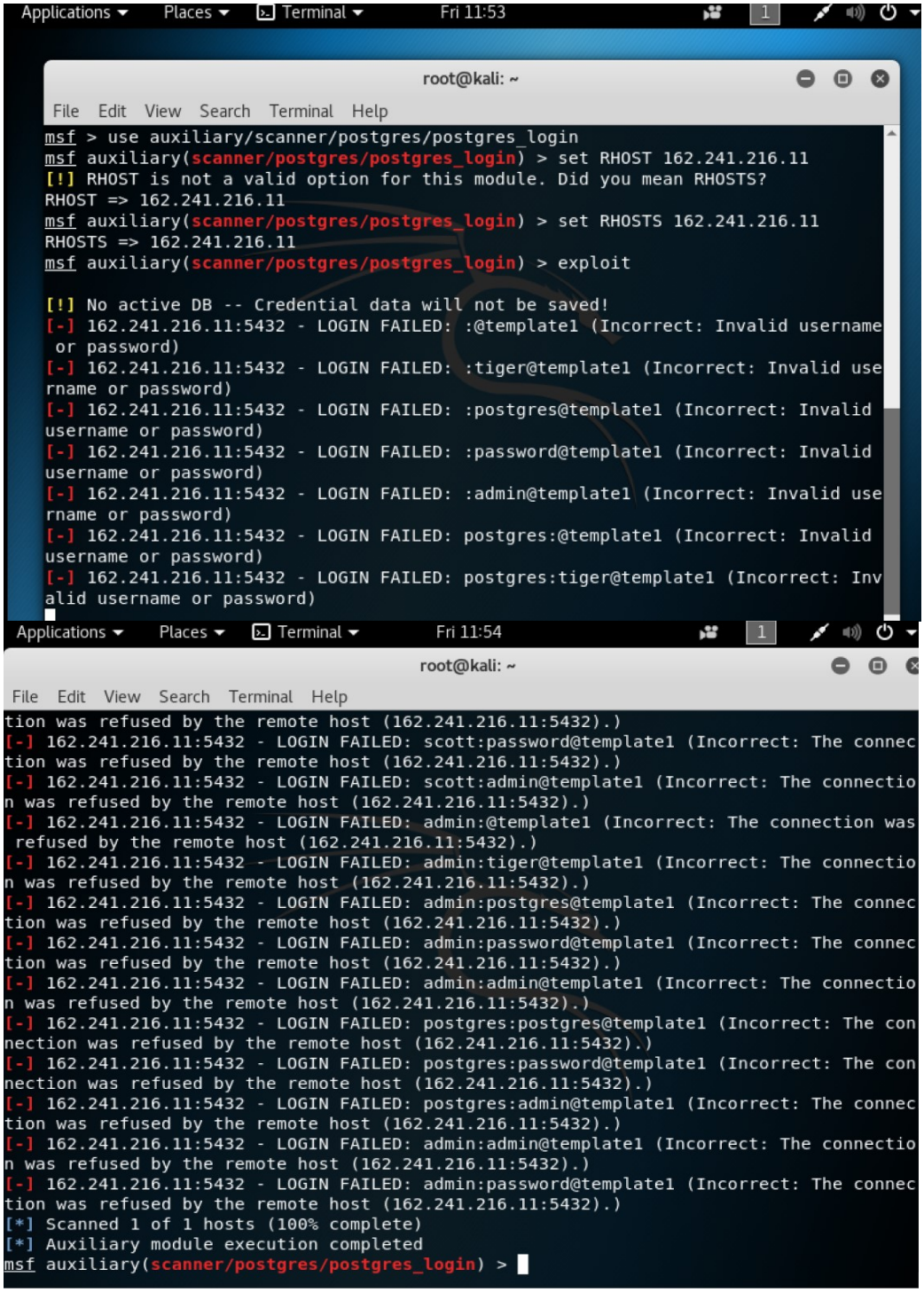
FTP-LOGIN -

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



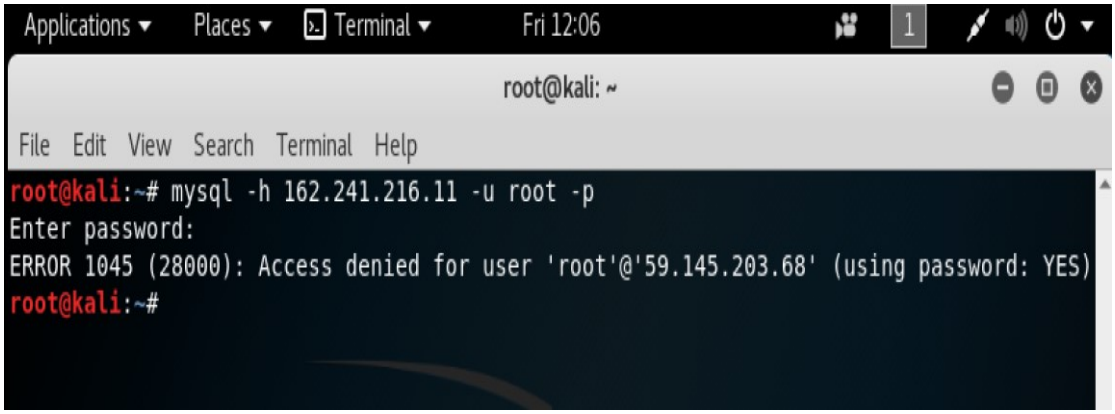
The ftp access to website is password protected hence it is very secure.

Attacking the DATABASE :



The attempts to crack the PostreSQL database from metasploit were failed hence the database is not prone to such attacks.

MSF-SQL Login -



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

SERVER INFO	
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.lststl.org

ISP INFO	
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 :

ATTACK / TEST	RESULT
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