Explore the vulnerable website specifically designed for testing ethical hacking tools. Experiment with different information gathering and scanning tools in kali linux on the websites identified.

We used the website ***scanme.nmap.org*** for commands.

Tools used

1. **Nmap**

A command-line utility for network research and security audits in Linux is called Nmap. Hackers, cybersecurity enthusiasts, and even network and system administrators utilize this application frequently. It serves the following functions:

- Information from a network in real time
- Comprehensive details on every IP that has been enabled on your network
- The quantity of open ports in a network
- Give the list of present hosts.
- OS, port, and host scanning

To scan a System with Hostname and IP address.

Syntax: nmap [Hostname/ IP address]

Eg: $nmap manipal.edu

```
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-09 10:39 IST
Nmap scan report for manipal.edu (18.66.53.117)
Host is up (0.12s latency).
Other addresses for manipal.edu (not scanned): 18.66.53.74 18.66.53.32 18.66.53.62
rDNS record for 18.66.53.117: server-18-66-53-117.bom78.r.cloudfront.net
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 17.12 seconds
```

$nmap 18.66.53.117

```
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-09 10:44 IST
Nmap scan report for server-18-66-53-117.bom78.r.cloudfront.net (18.66.53.117)
Host is up (0.11s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 14.32 seconds
```

$nmap -v scanme.nmap.org
//for detailed information about websites, ports which are open, closed.

$sudo nmap -sA scanme.nmap.org
//to detect firewall settings.

$sudo nmap -sL scanme.nmap.org
//to identify host names.

$sudo nmap -sS scanme.nmap.org
//to recognize the open and closed ports.

$sudo nmap -O 172.16.59.52
//to detect the operating system of the IP specified.

2. **The Harvester**
   $theharvester -d scanme.nmap.org
   //basic domain search

   $theharvester -d scanme.nmap.org -l 50
   //basic domain search can be limited to 50.

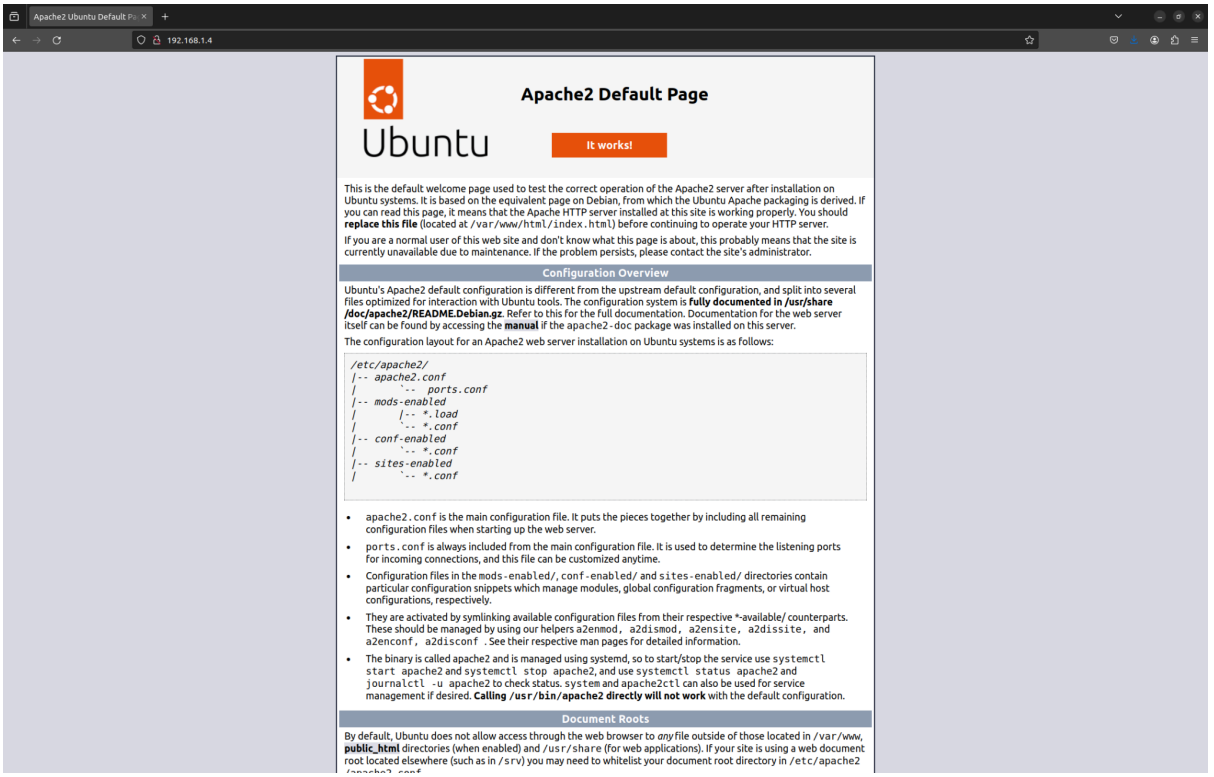
   $theharvester -d scanme.nmap.org -b pgp
   //to search for pgp keys.

   $theharvester -d scanme.nmap.org -b google bing
   //to search for emails and hosts using specific sources

3. **Installing apache server.**
   $sudo apt install apache2
   //to install apachev2.

   $sudo systemctl start apache2
   //to start apachev2 server.

$ifconfig
//to retrieve IP address, paste that IP address in browser to get below page



$sudo systemctl status apache2
//to check if apache server is disabled/ enabled

$sudo systemctl stop apache2
//to disable apache server

$cd /etc/apache2
//this directory contains configuration file(apache2.conf) of apache server which can be modified to enable or disable some functionalities but it requires admin privileges.

Other tools for gathering informations

1. **Whois**

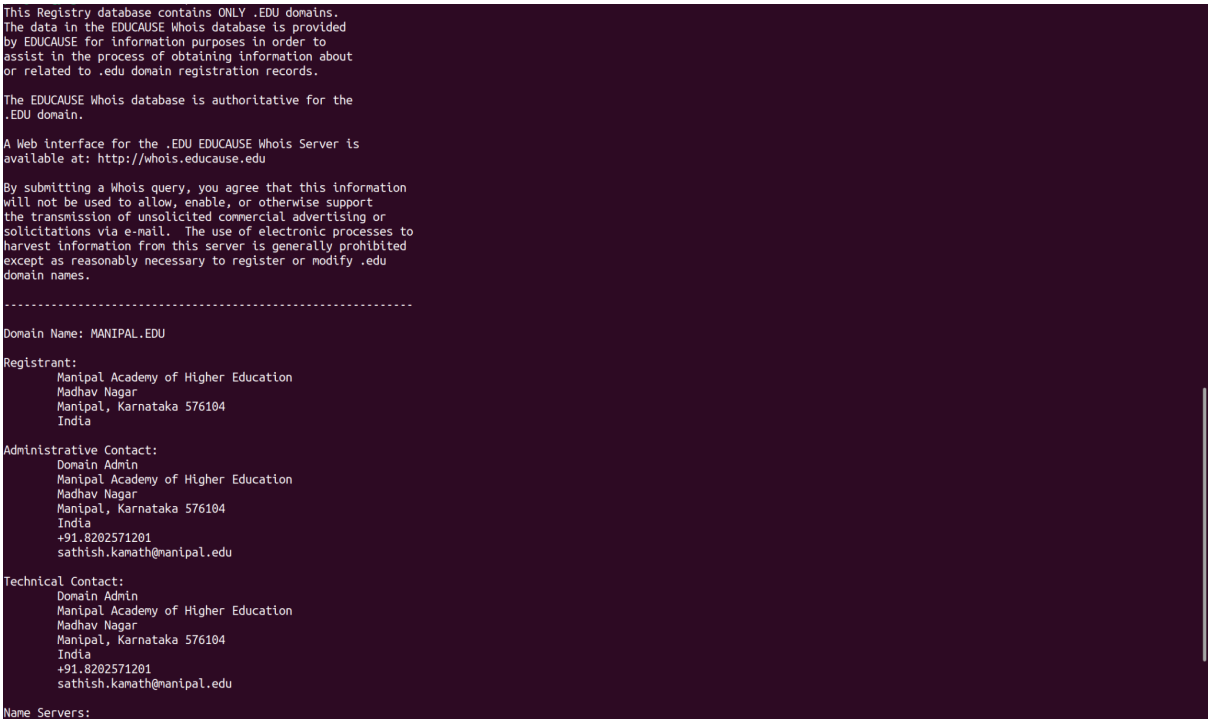
   WHOIS (pronounced as the phrase "who is") is a query and response protocol that is used for querying databases that store an Internet resource's registered users or assignees. A Whois domain lookup allows you to trace the ownership and tenure of a domain name. Similar to how all houses are registered with a governing authority, all domain name registries maintain a record of information about every domain name purchased through them, along with who owns it, and the date till which it has been purchased.

   Usage: whois [OPTION]... OBJECT...

-h HOST, --host HOST connect to server HOST
-p PORT, --port PORT connect to PORT
-I query whois.iana.org and follow its referral
-H hide legal disclaimers
--verbose explain what is being done
--no-recursion disable recursion from registry to registrar servers
--help display this help and exit
--version output version information and exit

a. Eg: $whois manipal.edu

It will extract the information about the domain (manipal.edu). In the below screenshot, you can see that we have information like Registry Domain ID, WHOIS Server, Updated Date, etc.



b. whois [ip address]

It will be extracting information by giving the IP Address as input to the whois command. In the below screenshot, we have got the information about the IP Address such as NetRange, CIDR, etc.

Eg: ***$whois 8.8.8.8***

```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2023, American Registry for Internet Numbers, Ltd.
#



# start

NetRange:       8.0.0.0 - 8.127.255.255
CIDR:           8.0.0.0/9
NetName:        LVLT-ORG-8-8
NetHandle:      NET-8-0-0-0-1
Parent:         NET8 (NET-8-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Level 3 Parent, LLC (LPL-141)
RegDate:        1992-12-01
Updated:        2018-04-23
Ref:            https://rdap.arin.net/registry/ip/8.0.0.0
```

2. DIG

Domain Information Groper is what the command dig stands for. It is employed to obtain DNS name server information. Basically, network administrators use it. It is used to do DNS lookups and to check and solve DNS issues. Older tools like the host and nslookup are replaced by the dig command.

Syntax: dig [server] [name] [type]

By Default DIG is ***"verbose"*** *(it gives extended/extra Information)*

$dig manipal.edu

```
; <<>> DiG 9.18.12-0ubuntu0.22.04.3-Ubuntu <<>> manipal.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18594
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;manipal.edu.                   IN      A

;; ANSWER SECTION:
manipal.edu.            3307    IN      A       18.66.53.74
manipal.edu.            3307    IN      A       18.66.53.32
manipal.edu.            3307    IN      A       18.66.53.62
manipal.edu.            3307    IN      A       18.66.53.117

;; Query time: 252 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Nov 09 10:08:17 IST 2023
;; MSG SIZE  rcvd: 104
```

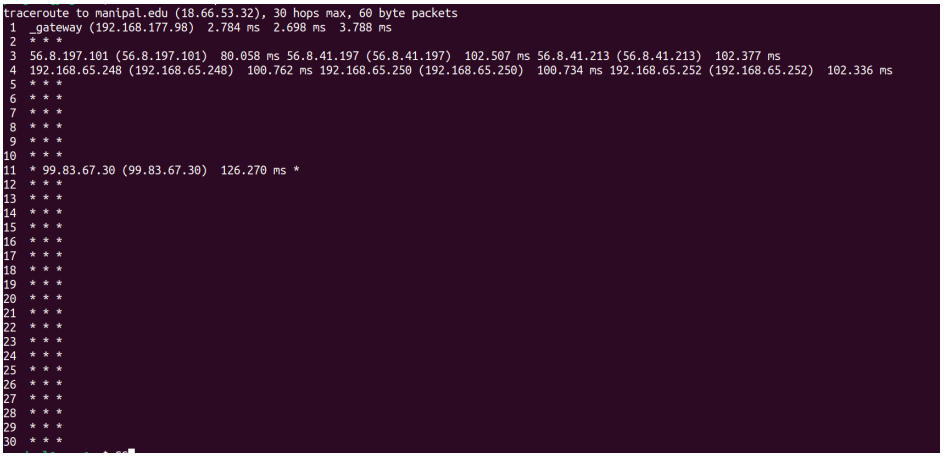
3.Traceroute

Traceroute is a command-line utility that returns information about the communication route between two nodes on an Internet Protocol (IP) network.

Traceroute is a useful tool for determining the response delays and routing loops present in a network pathway across packet switched nodes. It also helps to locate any points of failure encountered while en route to a certain destination.

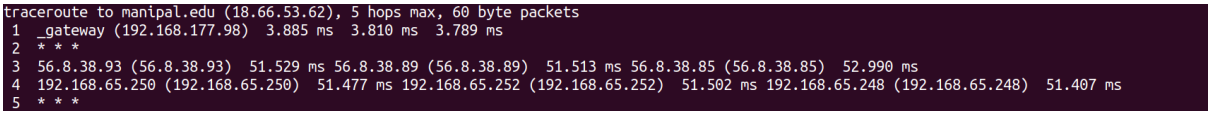
<u>Syntax:</u> $traceroute [IP Version] [IP Address]/[Domain Name]

$traceroute manipal.edu



$traceroute -m 5 manipal.edu

-m option gives provision to determine maximum number of hops.



4. Nslookup

Nslookup (stands for “Name Server Lookup”) is a useful command for getting information from the DNS server. It is a network administration tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or any other specific DNS record. It is also used to troubleshoot DNS-related problems.

Syntax: ***nslookup [option] [hosts]***

$nslookup manipal.edu

The "A Record" (IP Address) of the domain will be shown when the domain name is entered into nslookup. To locate a domain's address record, use this command. It obtains the information by contacting domain name servers.