Name:Prasheela

Date:2/3/2023

Task:2

1. Perform IP address spoofing

IP address spoofing is the act of falsifying the content in the Source IP header, usually with 6randomized numbers, either to mask the sender's identity or to launch a reflected DDoS attack, as described below.Name

Command:

$ ifconfig eth0 192.168.29.12

$ ifconfig

```
┌──(root㉿kali)-[~]
└─# ifconfig eth0 192.168.30.13

┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.30.13  netmask 255.255.255.0  broadcast 192.168.30.255
        inet6 fe80::ac8:1c5f:5b1c:5b5e  prefixlen 64  scopeid 0x20<link>
        ether 22:e1:b9:bf:64:84  txqueuelen 1000  (Ethernet)
        RX packets 108  bytes 7050 (6.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23  bytes 1812 (1.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[~]
└─# echo "prasheela"
prasheela
```

2.MAC address spoofing

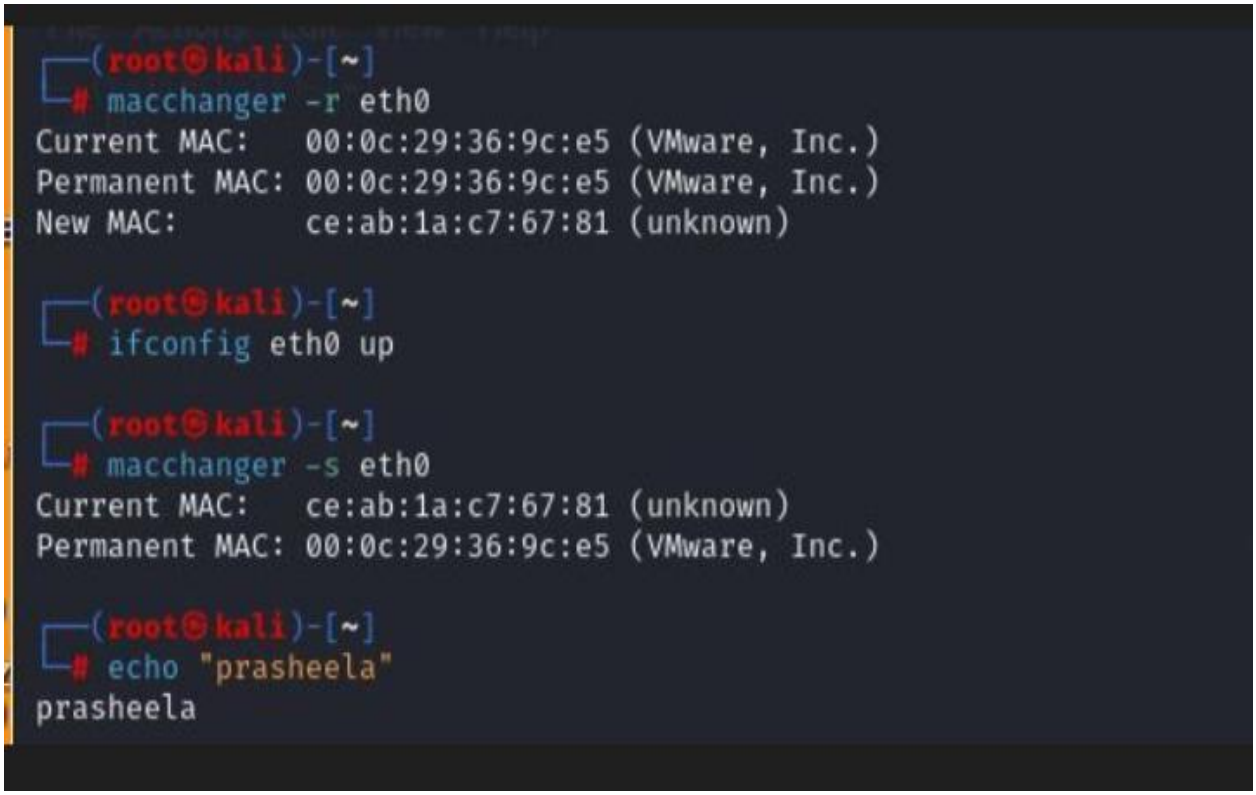
MAC Spoofing is a type of attack used to exploit flaws in the authentication mechanism implemented by wired and wireless networking hardware. In layman's terms, MAC spoofing is when someone or something intercepts, manipulate or otherwise tampers with the control messages exchanged between a networked device and its unique MAC address.

Command:

$ macchanger -r eth0

$ ifconfig eth0 up

$ macchanger -s eth0



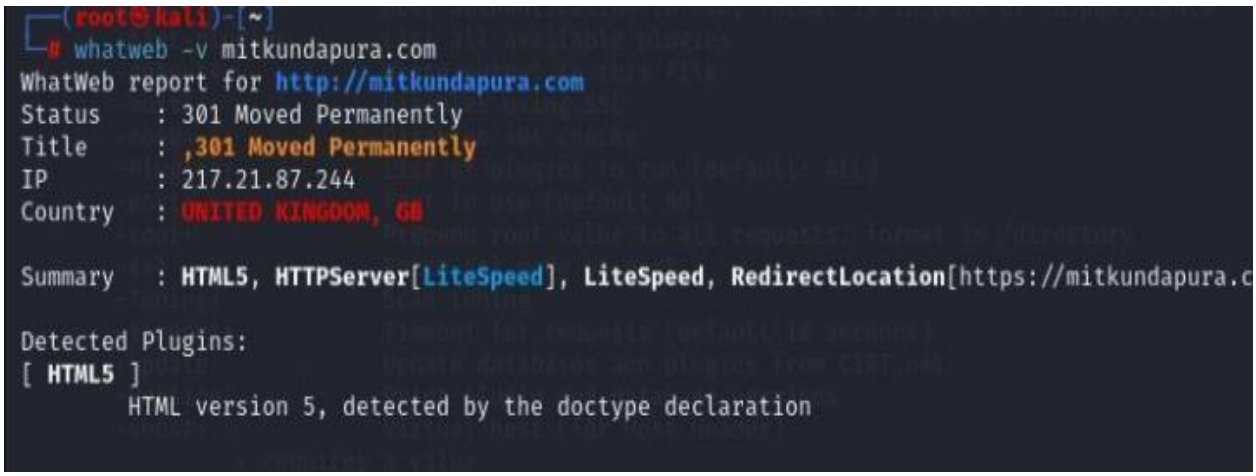
3.Whatweb

The WhatWeb tool is used to identify different web technologies used by the website. It is included in Kali Linux, and it can be accessed by going to Applications | 03 – Web Application Analysis | Web Vulnerability scanners.

Command:

$ whatweb mitkundapura.com

$ whatweb -v mitkundapura.com



$ whatweb -a 3 testfire.net

$ whatweb -v -a 3 testfire.net

$ whatweb –max-redirect 2 tesfire.net

4.Nslookup

Nslookup is the name of a program that lets an Internet server administrator or any computer user enter a host name and find out the corresponding IP address or domain name system (DNS) record. The user can also enter a command for it to do a reverse DNS lookup and find the host name for an IP address that is specified.

Command:

$ nslookup mitkundapura.com

```
┌──(root㉿kali)-[~]
└─# nslookup mitkundapura.com
Server:         192.168.29.2
Address:        192.168.29.2#53

Non-authoritative answer:
Name:   mitkundapura.com
Address: 217.21.87.244
Name:   mitkundapura.com
Address: 2a02:4780:11:771:0:2d4c:6d7f:1


┌──(root㉿kali)-[~]
└─# echo "prasheela"
prasheela
```

$nslookup -type=a mitkundapura.com

```
┌──(root㉿kali)-[~]
└─# nslookup -type=a mitkundapura.com
Server:         192.168.29.2
Address:        192.168.29.2#53

Non-authoritative answer:
Name:   mitkundapura.com
Address: 217.21.87.244


┌──(root㉿kali)-[~]
└─# echo "prasheela"
prasheela
```

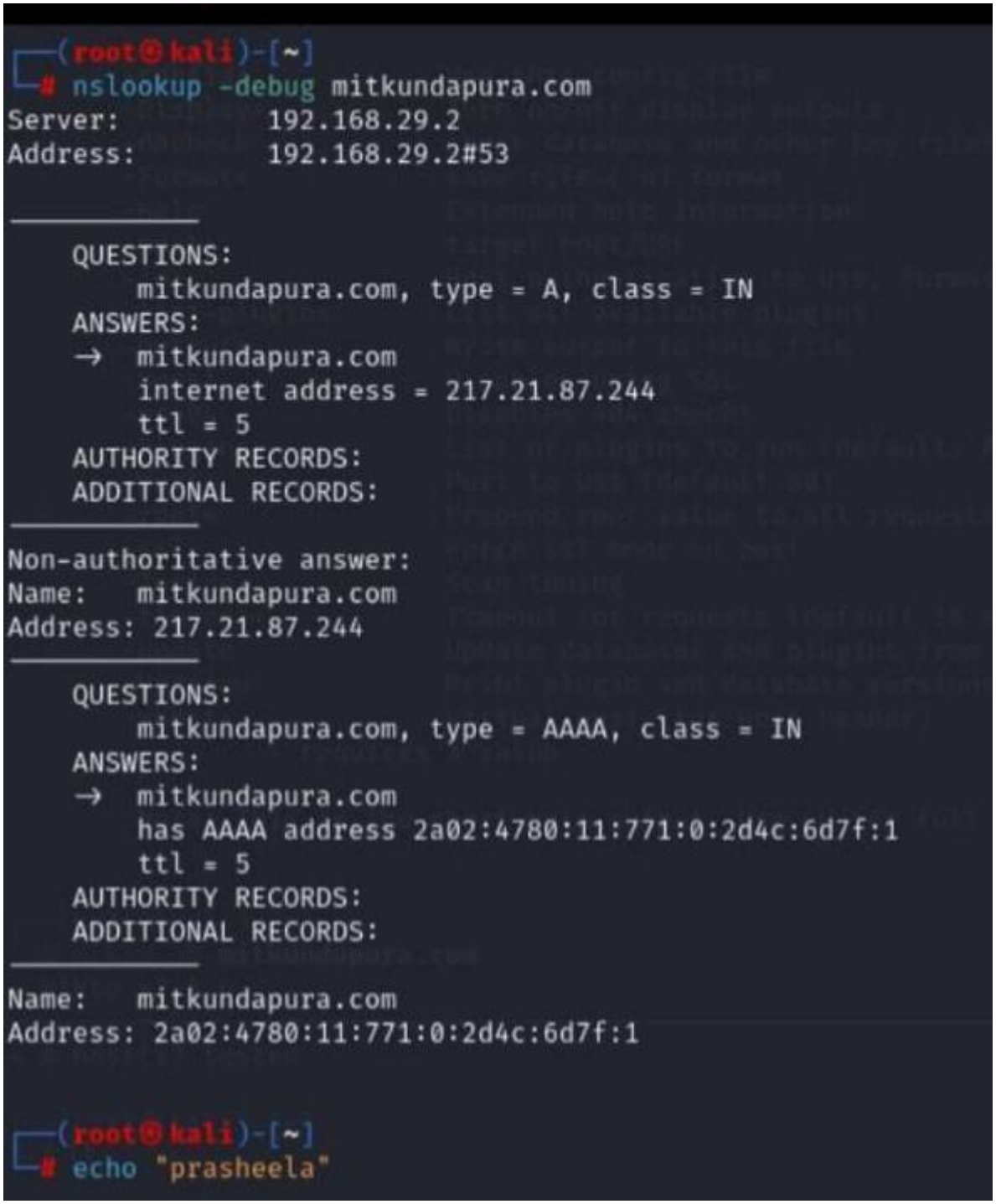
$ nslookup -type=ns mitkundapura.com

```
┌──(root㉿kali)-[~]
└─# nslookup -type=ns mitkundapura.com
Server:         192.168.29.2
Address:        192.168.29.2#53

Non-authoritative answer:
mitkundapura.com        nameserver = ns1.dns-parking.com.
mitkundapura.com        nameserver = ns2.dns-parking.com.

Authoritative answers can be found from:


┌──(root㉿kali)-[~]
└─# echo "prasheela"
prasheela
```

$nslookup -query=mx mitkundapura.com

```
┌──(root㉿kali)-[~]
└─# nslookup -query=mx mitkundapura.com
Server:         192.168.29.2
Address:        192.168.29.2#53

Non-authoritative answer:
mitkundapura.com        mail exchanger = 5 alt2.aspmx.l.google.com.
mitkundapura.com        mail exchanger = 1 aspmx.l.google.com.
mitkundapura.com        mail exchanger = 5 alt1.aspmx.l.google.com.
mitkundapura.com        mail exchanger = 10 alt4.aspmx.l.google.com.
mitkundapura.com        mail exchanger = 10 alt3.aspmx.l.google.com.

Authoritative answers can be found from:


┌──(root㉿kali)-[~]
└─# echo "prasheela"
prasheela
```

$nslookup -debug mitkundapura.com

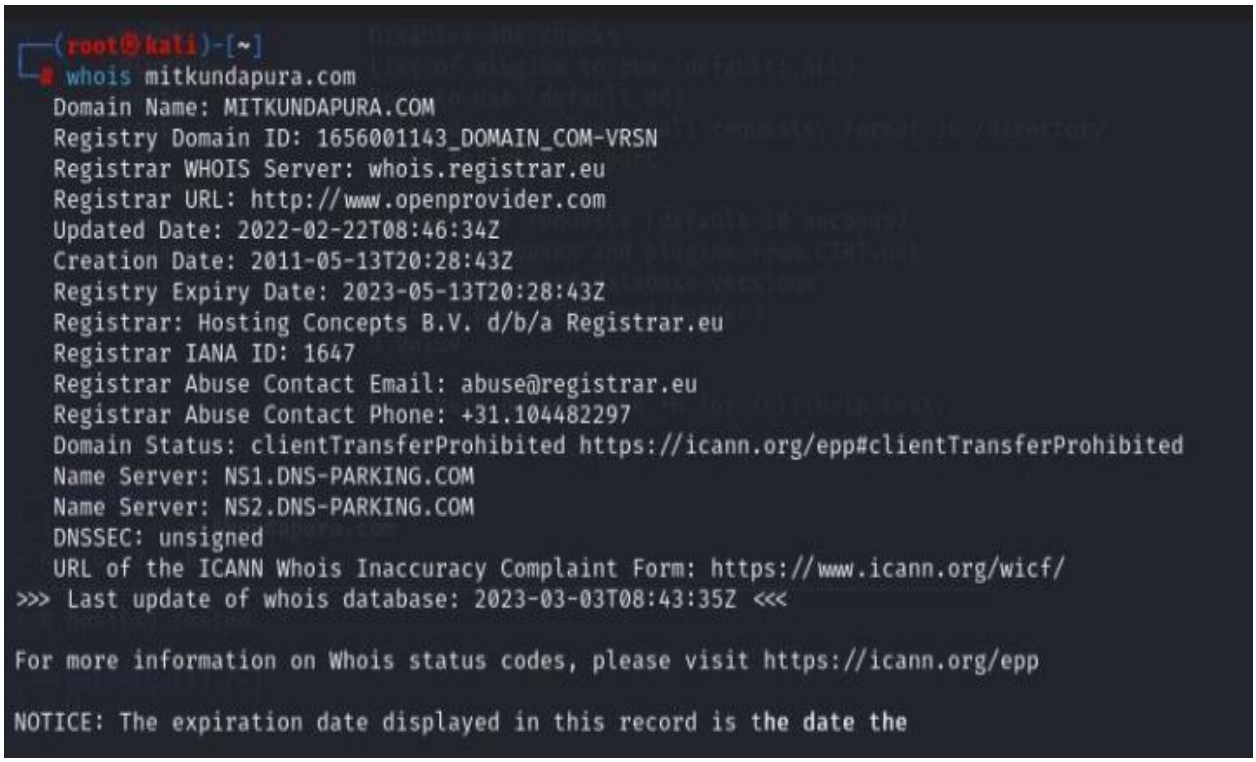


5. Whois

Whois is a widely used Internet record listing that identifies who owns a domain and how to get in contact with them. The Internet Corporation for Assigned Names and Numbers (ICANN) regulates domain name registration and ownership.

Commands:

$ whois mitkundapura.com



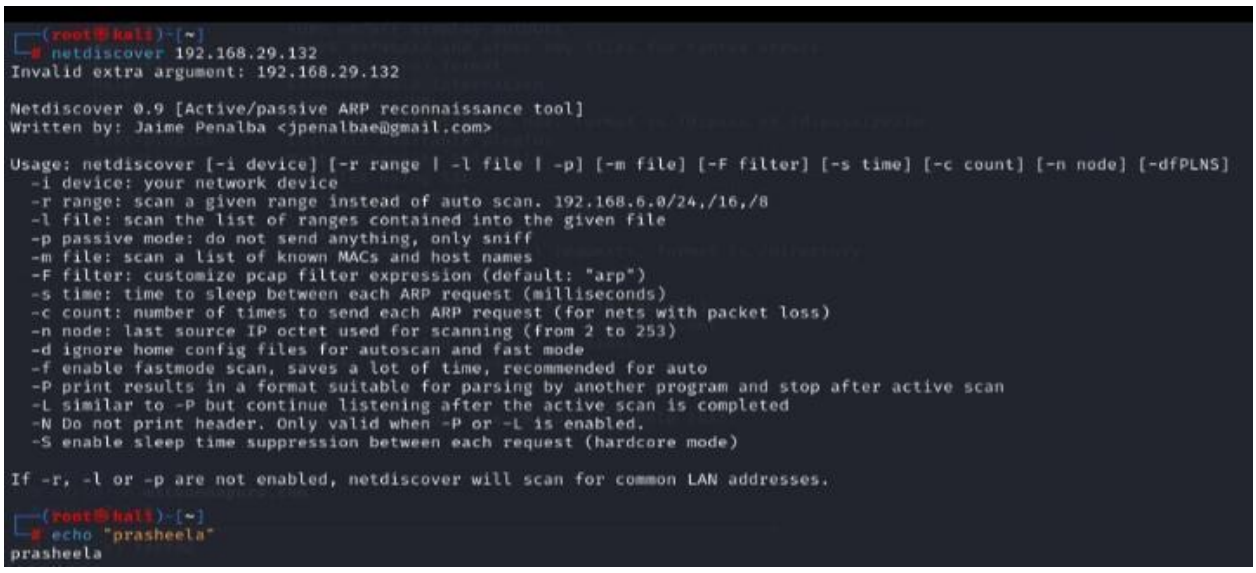
6. Netdiscover

Netdiscover is an active/passive address reconnaissance tool, mainly developed for those wireless networks without dhcp server, when you are wardriving. It can be also used on hub/switched networks.

Command:

$ netdiscover -h

$ netdiscover 192.168.29.132



$ netdiscover -r 192.168.29.0/24

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.29.1    00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.29.2    00:50:56:ff:d2:f8      1      60  VMware, Inc.
192.168.29.131  00:0c:29:2a:6d:ff      1      60  VMware, Inc.
192.168.29.254  00:50:56:f1:34:10      1      60  VMware, Inc.

zsh: suspended  netdiscover -r 192.168.29.0/24

┌──(root㉿kali)-[~]
└─# echo "prasheela"
prasheela
```

$ netdiscover –r 192.168.29.0/24 –P

```
┌──(root㉿kali)-[~]
└─# netdiscover -r 192.168.29.0/24 -P
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.29.1    00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.29.2    00:50:56:ff:d2:f8      1      60  VMware, Inc.
192.168.29.254  00:50:56:ef:db:68      1      60  VMware, Inc.

-- Active scan completed, 3 Hosts found.

┌──(root㉿kali)-[~]
└─# echo "prasheela"
prasheela
```

$ netdiscover –r 192.168.1.0/24 –PN

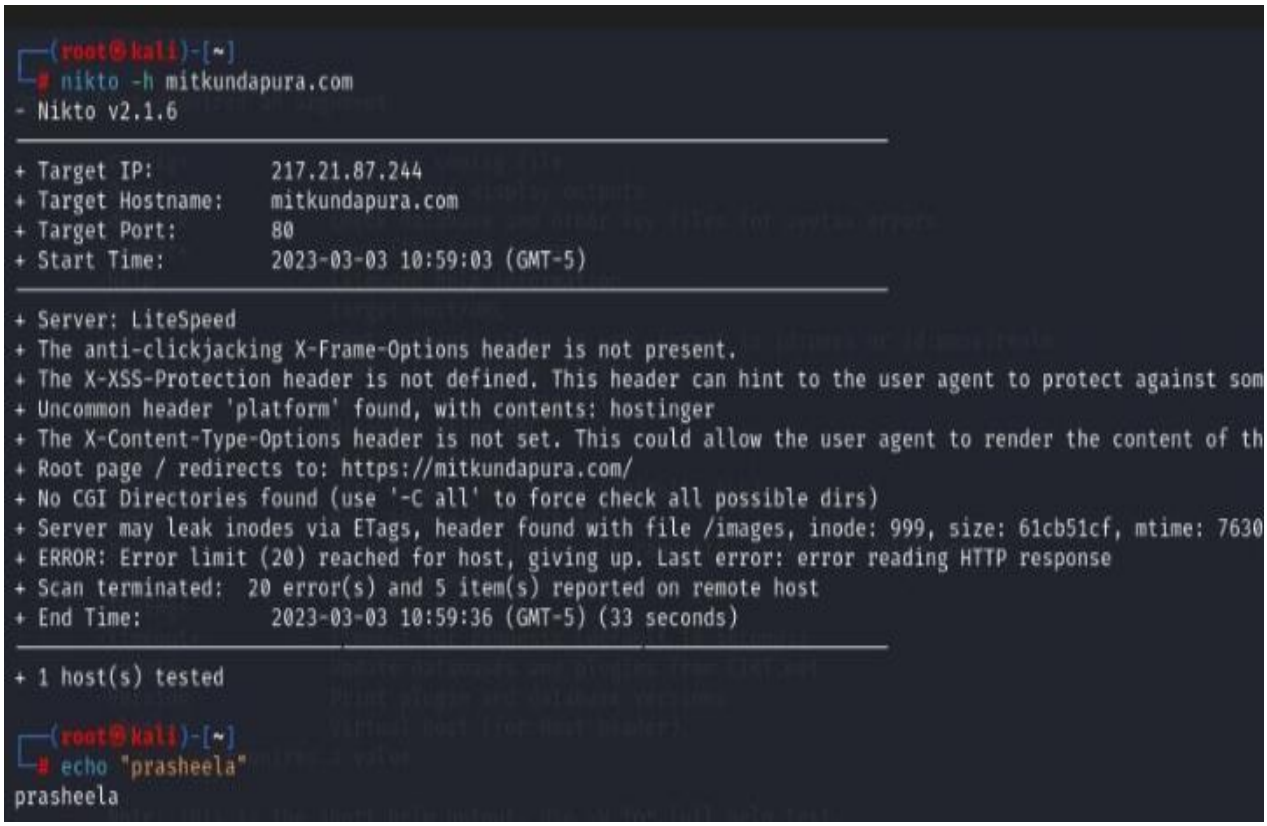
```
┌──(root㉿kali)-[~]
└─# netdiscover -r 192.168.29.0/24 -PN
192.168.29.1    00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.29.2    00:50:56:ff:d2:f8      1      60  VMware, Inc.
192.168.29.254  00:50:56:ef:db:68      1      60  VMware, Inc.

-- Active scan completed, 3 Hosts found.

┌──(root㉿kali)-[~]
└─# echo "prasheela"
prasheela
```

7.Nikto

Nikto is an Open Source software written in Perl language that is used to scan a web-server for the vulnerability that can be exploited and can compromise the server. It can also check for outdated version details of 1200 server and can detect problems with specific version details of over 200 servers.

Command:

$ nikto -h mitkundapura.com

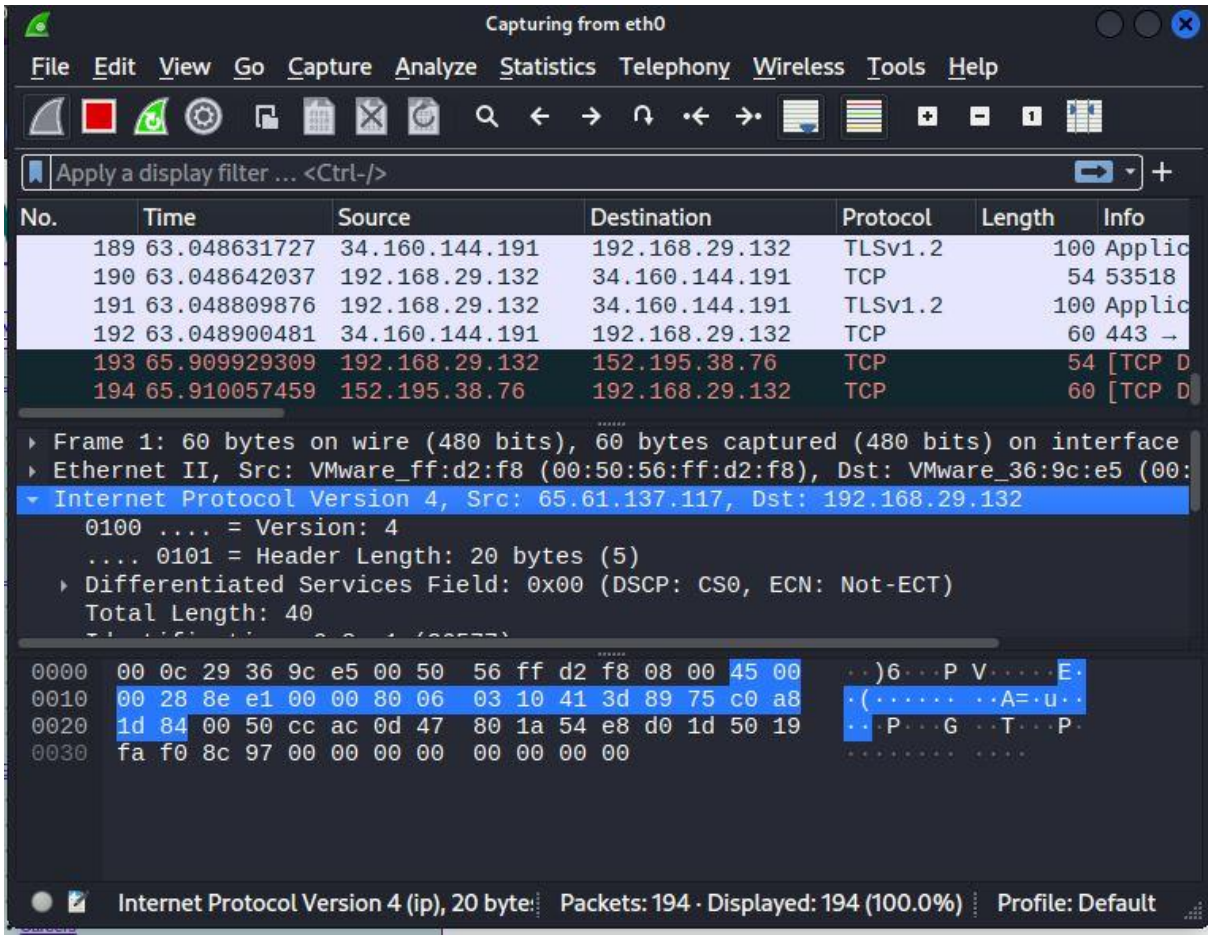


8.Cryto configuration flaw

Cryptographic failures are where attackers often target sensitive data, such as passwords, credit card numbers, and personal information, when you do not properly protect them. This is the root cause of sensitive data exposure.

9. Find data packet using Wireshark

Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical Ethernet network. Wireshark is the most often-used packet sniffer in the world.



10.Find Xml pages in website using dirbuster

DirBuster is a multi threaded java application designed to brute force directories and files names on web/application servers. Often is the case now of what looks like a web server in a state of default installation is actually not, and has pages and applications hidden within.