Task Report 2

02/03/2023

Name: Darshan Achar
Register No. : 145cs20004

GOVERNMENT POLYTECHNIC UDUPI

1.Perform IP Address Spoofing.

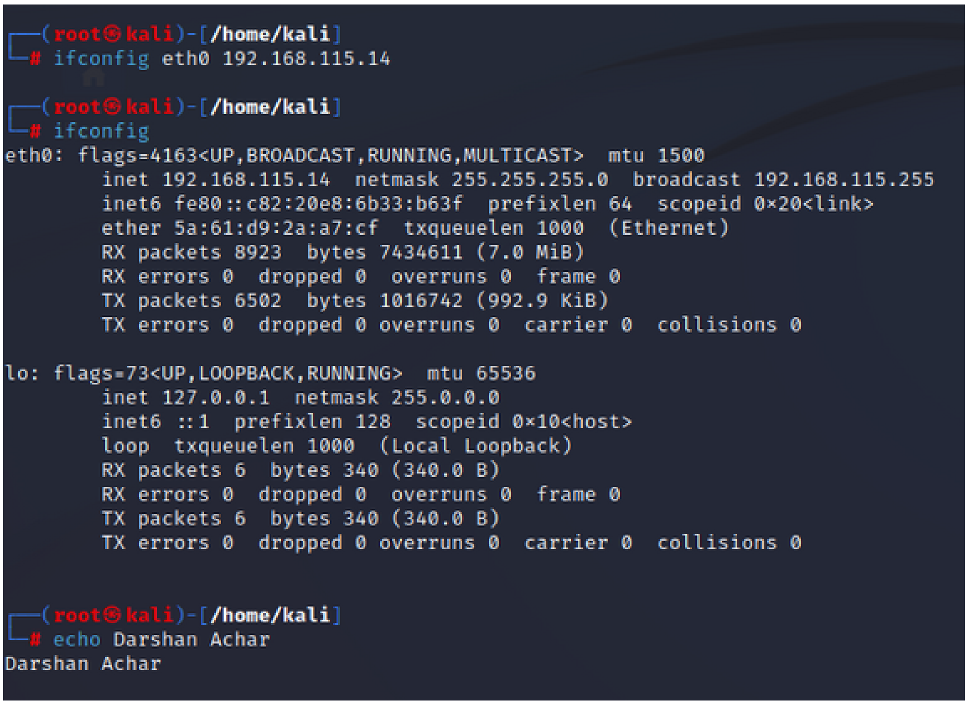
Internet Protocol (IP) spoofing is a type of malicious attack in which the threat actor conceals the true source of IP packets in order to make it difficult to determine where they originated. The attacker generates packets by changing the source IP address in order to impersonate another computer system, conceal the sender's identity, or both. The header field for the source IP address in the spoofed packet contains an address that differs from the actual source IP address.

Attackers frequently use IP spoofing to launch distributed denial of service (DDoS) and man-in-the-middle attacks against targeted devices or surrounding infrastructures. DDoS attacks seek to overwhelm a target with traffic while concealing the identity of the malicious source, thereby preventing mitigation efforts.

Attackers can use spoofed IP addresses to prevent authorities from discovering who they are and implicating them in the attack; prevent targeted devices from sending alerts about attacks in which they are unwitting participants; and circumvent security scripts, devices, and services that blocklist IP addresses known to be sources of malicious traffic.

Command: ifconfig eth0 <IP Address>

Output:



```
┌──(root㉿kali)-[/home/kali]
└─# ifconfig eth0 192.168.115.14

┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.115.14  netmask 255.255.255.0  broadcast 192.168.115.255
        inet6 fe80::c82:20e8:6b33:b63f  prefixlen 64  scopeid 0x20<link>
        ether 5a:61:d9:2a:a7:cf  txqueuelen 1000  (Ethernet)
        RX packets 8923  bytes 7434611 (7.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6502  bytes 1016742 (992.9 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 6  bytes 340 (340.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6  bytes 340 (340.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[/home/kali]
└─# echo Darshan Achar
Darshan Achar
```

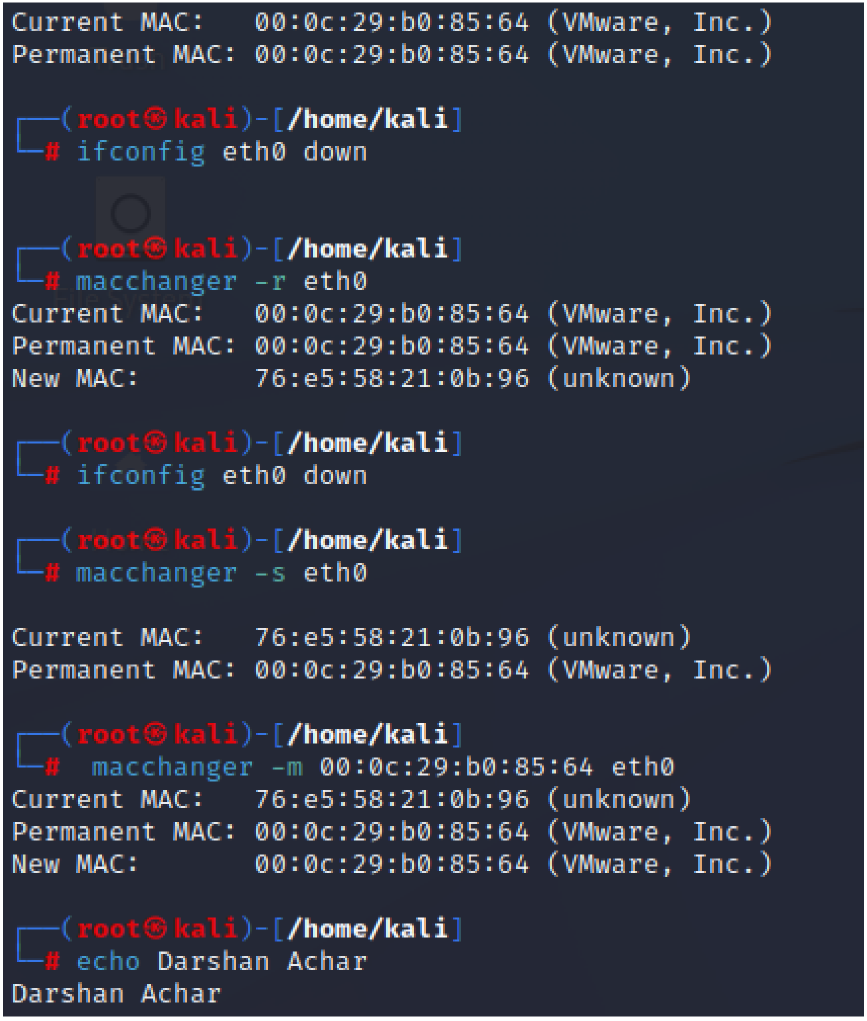
2.Perform Mac Address Spoofing.

MAC spoofing is most commonly associated with the attack method used in Wireless Network Hacking. MAC spoofing is a popular technique for breaking into wireless networks and stealing wireless network credentials. It can also be used to install an unauthorised access point or simulate an access point with a packet sniffer from the same operating system and network segment.

Commands:

- ifconfig eth0 down
- macchanger -r eth0
- macchanger -s eth0
- macchanger -m <Mac which you to set> eth0
- ifconfig eth0 up

Output:



```
Current MAC:   00:0c:29:b0:85:64 (VMware, Inc.)
Permanent MAC: 00:0c:29:b0:85:64 (VMware, Inc.)

┌──(root㉿kali)-[/home/kali]
└─# ifconfig eth0 down


┌──(root㉿kali)-[/home/kali]
└─# macchanger -r eth0
Current MAC:   00:0c:29:b0:85:64 (VMware, Inc.)
Permanent MAC: 00:0c:29:b0:85:64 (VMware, Inc.)
New MAC:       76:e5:58:21:0b:96 (unknown)

┌──(root㉿kali)-[/home/kali]
└─# ifconfig eth0 down

┌──(root㉿kali)-[/home/kali]
└─# macchanger -s eth0

Current MAC:   76:e5:58:21:0b:96 (unknown)
Permanent MAC: 00:0c:29:b0:85:64 (VMware, Inc.)

┌──(root㉿kali)-[/home/kali]
└─#  macchanger -m 00:0c:29:b0:85:64 eth0
Current MAC:   76:e5:58:21:0b:96 (unknown)
Permanent MAC: 00:0c:29:b0:85:64 (VMware, Inc.)
New MAC:       00:0c:29:b0:85:64 (VMware, Inc.)

┌──(root㉿kali)-[/home/kali]
└─# echo Darshan Achar
Darshan Achar
```

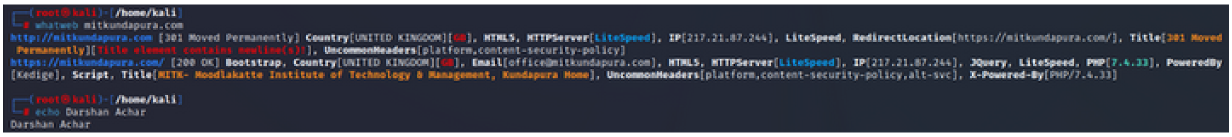
3.Whatweb Commands.

Whatweb is a website identification service. It recognises web technologies such as CMS, blogging platforms, JavaScript libraries, and embedded devices. Whatweb has over 900 plugins, each of which recognises a different thing. It also identifies version numbers, email address, account id and more.

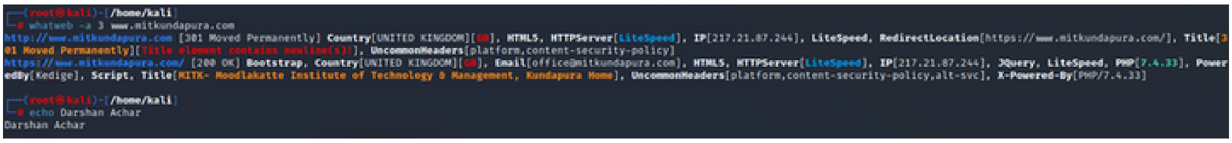
Command:

- whatweb mitkundapura.com
- whatweb -v mitkundapura.com
- whatweb -a 3 mitkundapura.com
- whatweb --max-redirect 2 mitkundapura.com
- whatweb -v -a 3 mitkundapura.com

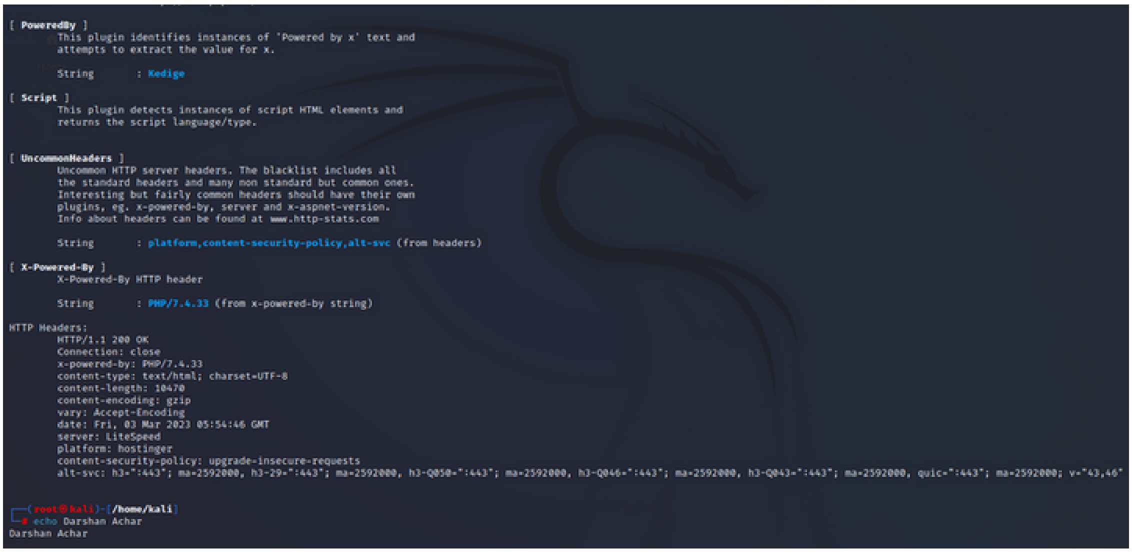
Output:



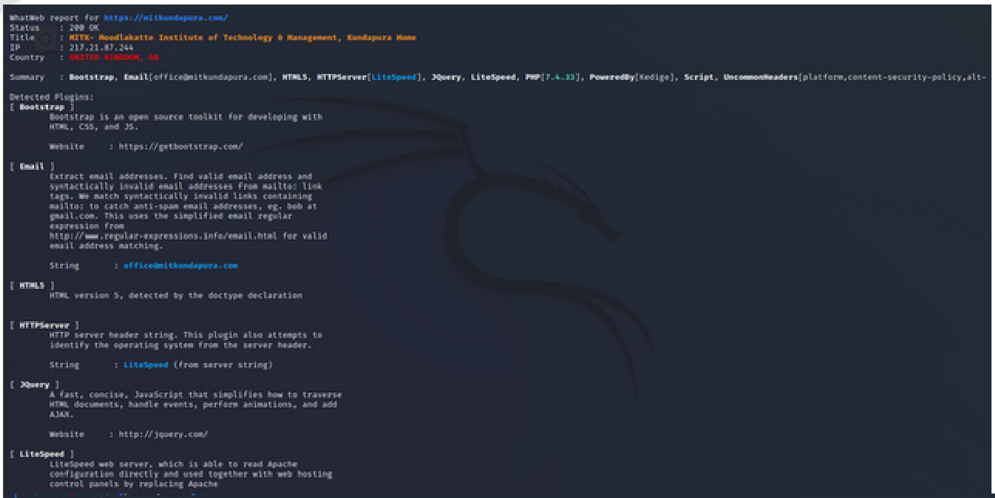
```
┌──(root㉿kali)-[/home/kali]
└─# whatweb mitkundapura.com
http://mitkundapura.com [301 Moved Permanently] Country[UNITED KINGDOM][GB], HTML5, HTTPServer[LiteSpeed], IP[217.21.87.244], LiteSpeed, RedirectLocation[https://mitkundapura.com/], Title[301 Moved
 Permanently][Title element contains newline(s)!], UncommonHeaders[platform,content-security-policy]
https://mitkundapura.com/ [200 OK] Bootstrap, Country[UNITED KINGDOM][GB], Email[office@mitkundapura.com], HTML5, HTTPServer[LiteSpeed], IP[217.21.87.244], JQuery, LiteSpeed, PHP[7.4.33], PoweredBy
[Kedige], Script, Title[MITK- Moodlakatte Institute of Technology & Management, Kundapura Home], UncommonHeaders[platform,content-security-policy,alt-svc], X-Powered-By[PHP/7.4.33]

┌──(root㉿kali)-[/home/kali]
└─# echo Darshan Achar
Darshan Achar
```



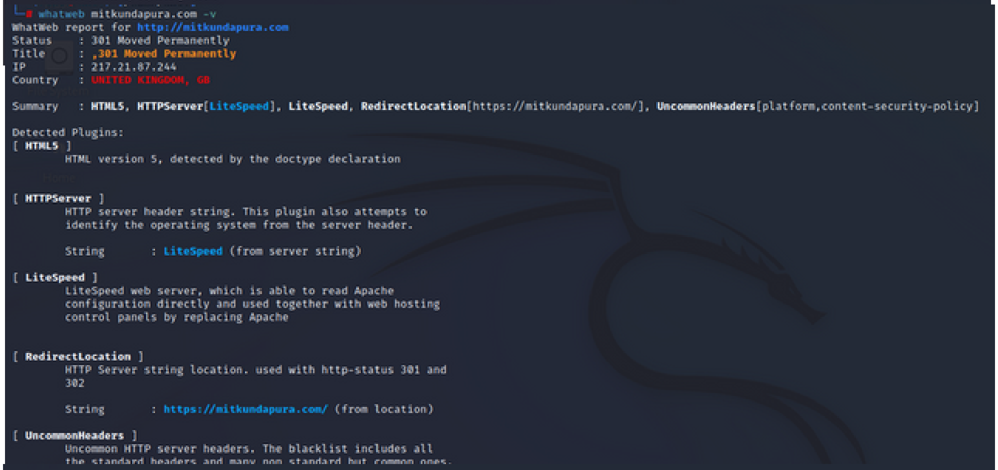
```
┌──(root㉿kali)-[/home/kali]
└─# whatweb -a 3 www.mitkundapura.com
http://www.mitkundapura.com [301 Moved Permanently] Country[UNITED KINGDOM][GB], HTML5, HTTPServer[LiteSpeed], IP[217.21.87.244], LiteSpeed, RedirectLocation[https://www.mitkundapura.com/], Title[3
01 Moved Permanently][Title element contains newline(s)!], UncommonHeaders[platform,content-security-policy]
https://www.mitkundapura.com/ [200 OK] Bootstrap, Country[UNITED KINGDOM][GB], Email[office@mitkundapura.com], HTML5, HTTPServer[LiteSpeed], IP[217.21.87.244], JQuery, LiteSpeed, PHP[7.4.33], Power
edBy[Kedige], Script, Title[MITK- Moodlakatte Institute of Technology & Management, Kundapura Home], UncommonHeaders[platform,content-security-policy,alt-svc], X-Powered-By[PHP/7.4.33]

┌──(root㉿kali)-[/home/kali]
└─# echo Darshan Achar
Darshan Achar
```



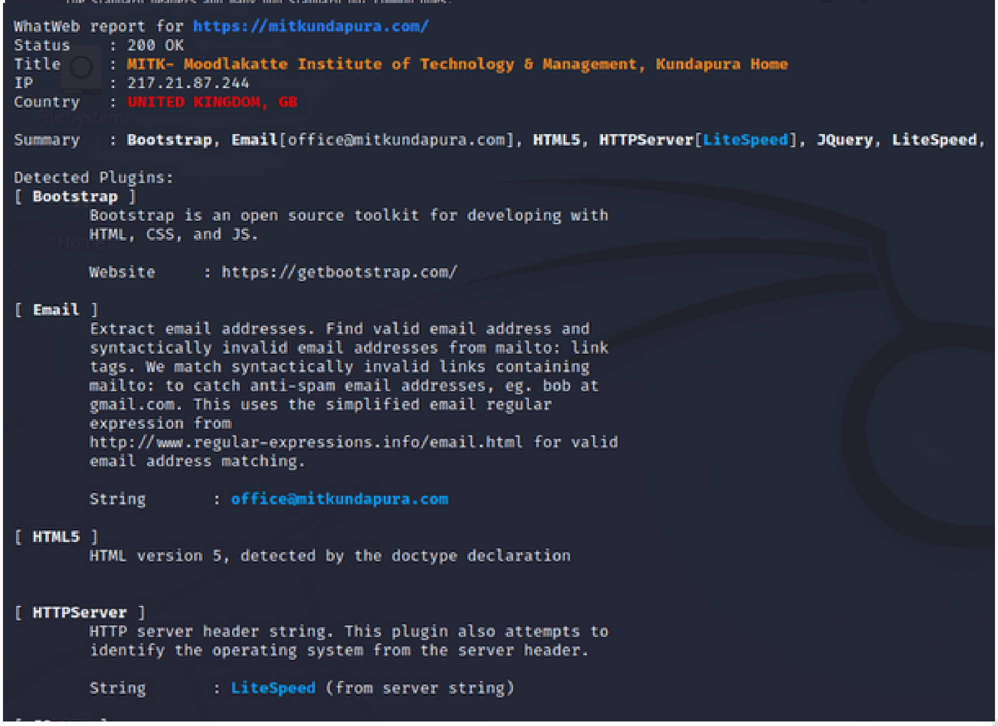
```
[ PoweredBy ]
        This plugin identifies instances of 'Powered by x' text and
        attempts to extract the value for x.

        String       : Kedige

[ Script ]
        This plugin detects instances of script HTML elements and
        returns the script language/type.


[ UncommonHeaders ]
        Uncommon HTTP server headers. The blacklist includes all
        the standard headers and many non standard but common ones.
        Interesting but fairly common headers should have their own
        plugins, eg. x-powered-by, server and x-aspnet-version.
        Info about headers can be found at www.http-stats.com

        String       : platform,content-security-policy,alt-svc (from headers)

[ X-Powered-By ]
        X-Powered-By HTTP header

        String       : PHP/7.4.33 (from x-powered-by string)

HTTP Headers:
        HTTP/1.1 200 OK
        Connection: close
        x-powered-by: PHP/7.4.33
        content-type: text/html; charset=UTF-8
        content-length: 10470
        content-encoding: gzip
        vary: Accept-Encoding
        date: Fri, 03 Mar 2023 05:54:46 GMT
        server: LiteSpeed
        platform: hostinger
        content-security-policy: upgrade-insecure-requests
        alt-svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"


┌──(root㉿kali)-[/home/kali]
└─# echo Darshan Achar
Darshan Achar
```



```
WhatWeb report for https://mitkundapura.com/
Status     : 200 OK
Title      : MITK- Moodlakatte Institute of Technology & Management, Kundapura Home
IP         : 217.21.87.244
Country    : UNITED KINGDOM, GB

Summary    : Bootstrap, Email[office@mitkundapura.com], HTML5, HTTPServer[LiteSpeed], JQuery, LiteSpeed, PHP[7.4.33], PoweredBy[Kedige], Script, UncommonHeaders[platform,content-security-policy,alt-

Detected Plugins:
[ Bootstrap ]
        Bootstrap is an open source toolkit for developing with
        HTML, CSS, and JS.

        Website     : https://getbootstrap.com/

[ Email ]
        Extract email addresses. Find valid email address and
        syntactically invalid email addresses from mailto: link
        tags. We match syntactically invalid links containing
        mailto: to catch anti-spam email addresses, eg. bob at
        gmail.com. This uses the simplified email regular
        expression from
        http://www.regular-expressions.info/email.html for valid
        email address matching.

        String       : office@mitkundapura.com

[ HTML5 ]
        HTML version 5, detected by the doctype declaration


[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : LiteSpeed (from server string)

[ JQuery ]
        A fast, concise, JavaScript that simplifies how to traverse
        HTML documents, handle events, perform animations, and add
        AJAX.

        Website     : http://jquery.com/

[ LiteSpeed ]
        LiteSpeed web server, which is able to read Apache
        configuration directly and used together with web hosting
        control panels by replacing Apache
```



```
└─# whatweb mitkundapura.com -v
WhatWeb report for http://mitkundapura.com
Status    : 301 Moved Permanently
Title     : ,301 Moved Permanently
IP        : 217.21.87.244
Country   : UNITED KINGDOM, GB

Summary   : HTML5, HTTPServer[LiteSpeed], LiteSpeed, RedirectLocation[https://mitkundapura.com/], UncommonHeaders[platform,content-security-policy]

Detected Plugins:
[ HTML5 ]
        HTML version 5, detected by the doctype declaration


[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : LiteSpeed (from server string)

[ LiteSpeed ]
        LiteSpeed web server, which is able to read Apache
        configuration directly and used together with web hosting
        control panels by replacing Apache


[ RedirectLocation ]
        HTTP Server string location. used with http-status 301 and
        302

        String       : https://mitkundapura.com/ (from location)

[ UncommonHeaders ]
        Uncommon HTTP server headers. The blacklist includes all
        the standard headers and many non standard but common ones.
```



```
WhatWeb report for https://mitkundapura.com/
Status     : 200 OK
Title      : MITK- Moodlakatte Institute of Technology & Management, Kundapura Home
IP         : 217.21.87.244
Country    : UNITED KINGDOM, GB

Summary    : Bootstrap, Email[office@mitkundapura.com], HTML5, HTTPServer[LiteSpeed], JQuery, LiteSpeed,

Detected Plugins:
[ Bootstrap ]
        Bootstrap is an open source toolkit for developing with
        HTML, CSS, and JS.

        Website     : https://getbootstrap.com/

[ Email ]
        Extract email addresses. Find valid email address and
        syntactically invalid email addresses from mailto: link
        tags. We match syntactically invalid links containing
        mailto: to catch anti-spam email addresses, eg. bob at
        gmail.com. This uses the simplified email regular
        expression from
        http://www.regular-expressions.info/email.html for valid
        email address matching.

        String       : office@mitkundapura.com

[ HTML5 ]
        HTML version 5, detected by the doctype declaration


[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : LiteSpeed (from server string)
```

4.NsLookUp Commands.

Nslookup (name server lookup) is a useful command for retrieving information from a DNS server. It is a network administration tool that queries the DNS to obtain domain name or IP address mapping information, as well as any other specific DNS record. It is also used to troubleshoot DNS issues.

Commands:

1.nslookup followed by the domain name will display the “A Record” (IP address) of the domain.

```
# nslookup google.com
```

2.SOA record provides the authoritative information about the domain, e-mail, the serial numbers etc...

```
# nslookup -type==soa google.com
```

3.NS (name server) it will output the name serves which are associated with given domains.

```
# nslookup -type=ns google.com
```

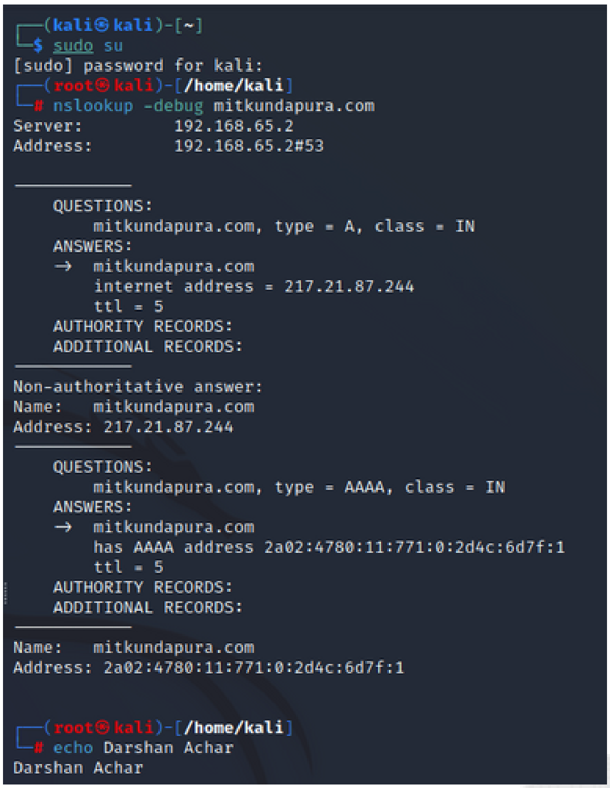
4.MX (mail exchange) record maps a domain name to list of mail exchange servers for that domain.

```
# nslookup -type=mx google.com
```

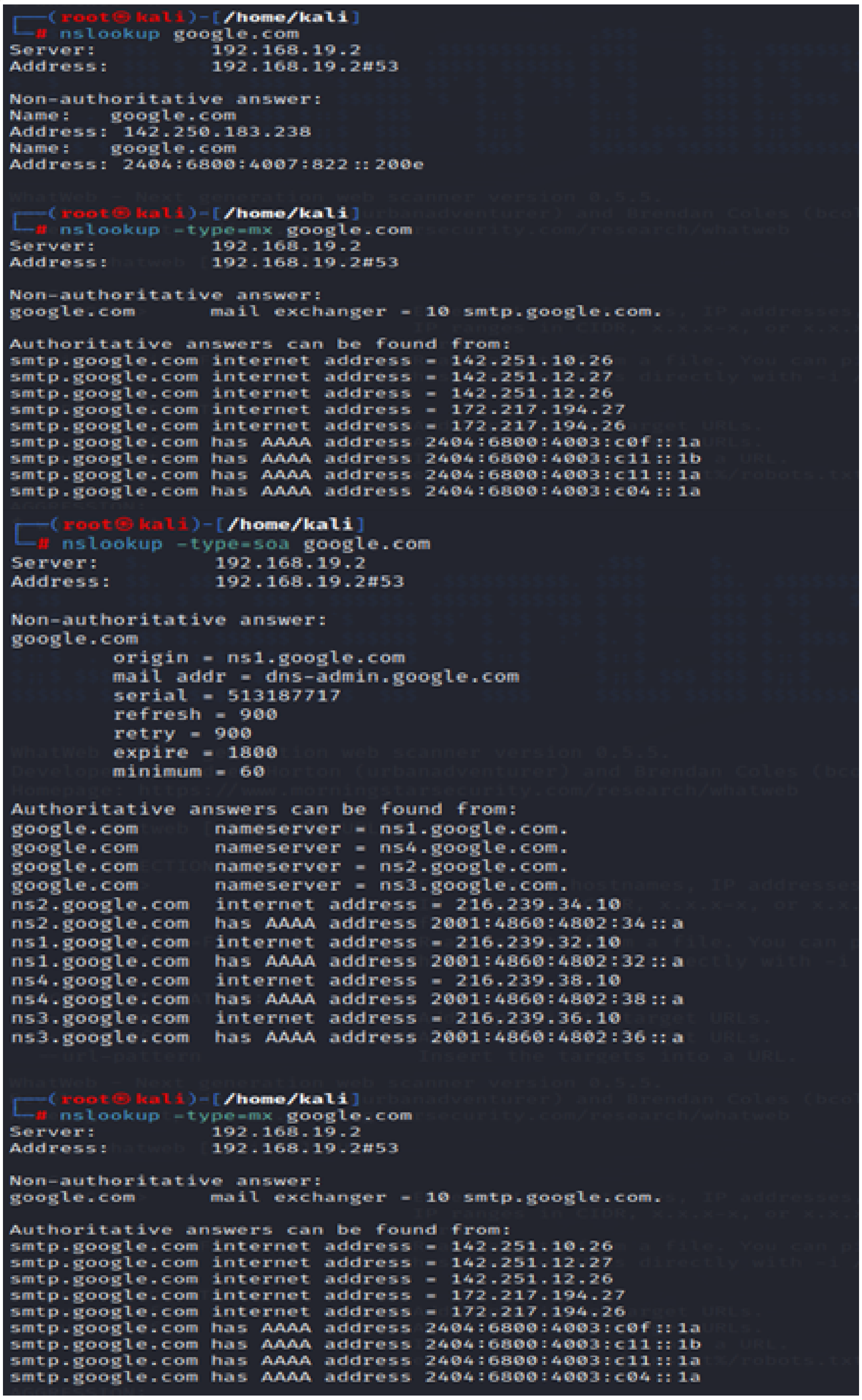
5.To view information useful for debugging, use the debug option

```
# nslookup -debug google.com
```

Output:



```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nslookup -debug mitkundapura.com
Server:         192.168.65.2
Address:        192.168.65.2#53

────────────
    QUESTIONS:
        mitkundapura.com, type = A, class = IN
    ANSWERS:
    ->  mitkundapura.com
        internet address = 217.21.87.244
        ttl = 5
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
────────────
Non-authoritative answer:
Name:   mitkundapura.com
Address: 217.21.87.244
────────────
    QUESTIONS:
        mitkundapura.com, type = AAAA, class = IN
    ANSWERS:
    ->  mitkundapura.com
        has AAAA address 2a02:4780:11:771:0:2d4c:6d7f:1
        ttl = 5
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
────────────
Name:   mitkundapura.com
Address: 2a02:4780:11:771:0:2d4c:6d7f:1


┌──(root㉿kali)-[/home/kali]
└─# echo Darshan Achar
Darshan Achar
```



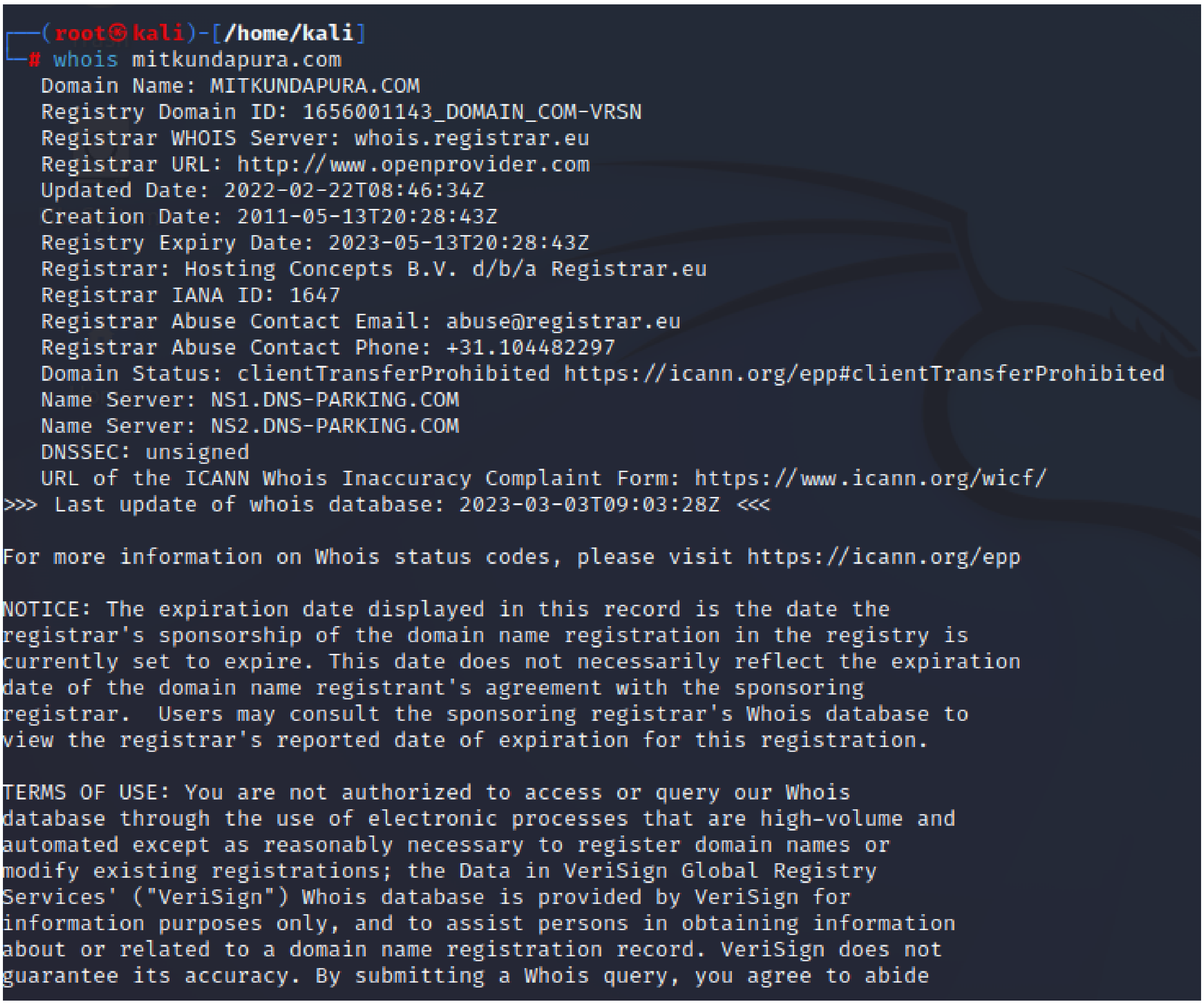
```
┌──(root㉿kali)-[/home/kali]
└─# nslookup google.com
Server:         192.168.19.2
Address:        192.168.19.2#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.183.238
Name:   google.com
Address: 2404:6800:4007:822::200e

┌──(root㉿kali)-[/home/kali]
└─# nslookup -type=mx google.com
Server:         192.168.19.2
Address:        192.168.19.2#53

Non-authoritative answer:
google.com      mail exchanger = 10 smtp.google.com.

Authoritative answers can be found from:
smtp.google.com internet address = 142.251.10.26
smtp.google.com internet address = 142.251.12.27
smtp.google.com internet address = 142.251.12.26
smtp.google.com internet address = 172.217.194.27
smtp.google.com internet address = 172.217.194.26
smtp.google.com has AAAA address 2404:6800:4003:c0f::1a
smtp.google.com has AAAA address 2404:6800:4003:c11::1b
smtp.google.com has AAAA address 2404:6800:4003:c11::1a
smtp.google.com has AAAA address 2404:6800:4003:c04::1a

┌──(root㉿kali)-[/home/kali]
└─# nslookup -type=soa google.com
Server:         192.168.19.2
Address:        192.168.19.2#53

Non-authoritative answer:
google.com
        origin = ns1.google.com
        mail addr = dns-admin.google.com
        serial = 513187717
        refresh = 900
        retry = 900
        expire = 1800
        minimum = 60

Authoritative answers can be found from:
google.com      nameserver = ns1.google.com.
google.com      nameserver = ns4.google.com.
google.com      nameserver = ns2.google.com.
google.com      nameserver = ns3.google.com.
ns2.google.com  internet address = 216.239.34.10
ns2.google.com  has AAAA address 2001:4860:4802:34::a
ns1.google.com  internet address = 216.239.32.10
ns1.google.com  has AAAA address 2001:4860:4802:32::a
ns4.google.com  internet address = 216.239.38.10
ns4.google.com  has AAAA address 2001:4860:4802:38::a
ns3.google.com  internet address = 216.239.36.10
ns3.google.com  has AAAA address 2001:4860:4802:36::a

┌──(root㉿kali)-[/home/kali]
└─# nslookup -type=mx google.com
Server:         192.168.19.2
Address:        192.168.19.2#53

Non-authoritative answer:
google.com      mail exchanger = 10 smtp.google.com.

Authoritative answers can be found from:
smtp.google.com internet address = 142.251.10.26
smtp.google.com internet address = 142.251.12.27
smtp.google.com internet address = 142.251.12.26
smtp.google.com internet address = 172.217.194.27
smtp.google.com internet address = 172.217.194.26
smtp.google.com has AAAA address 2404:6800:4003:c0f::1a
smtp.google.com has AAAA address 2404:6800:4003:c11::1b
smtp.google.com has AAAA address 2404:6800:4003:c11::1a
smtp.google.com has AAAA address 2404:6800:4003:c04::1a
```

6. WhoIs Command.

The whois command displays information about a website's record. You may get all the information about a website regarding its registration and owner's information.

Command : # whois mitkundapura.com

Output :



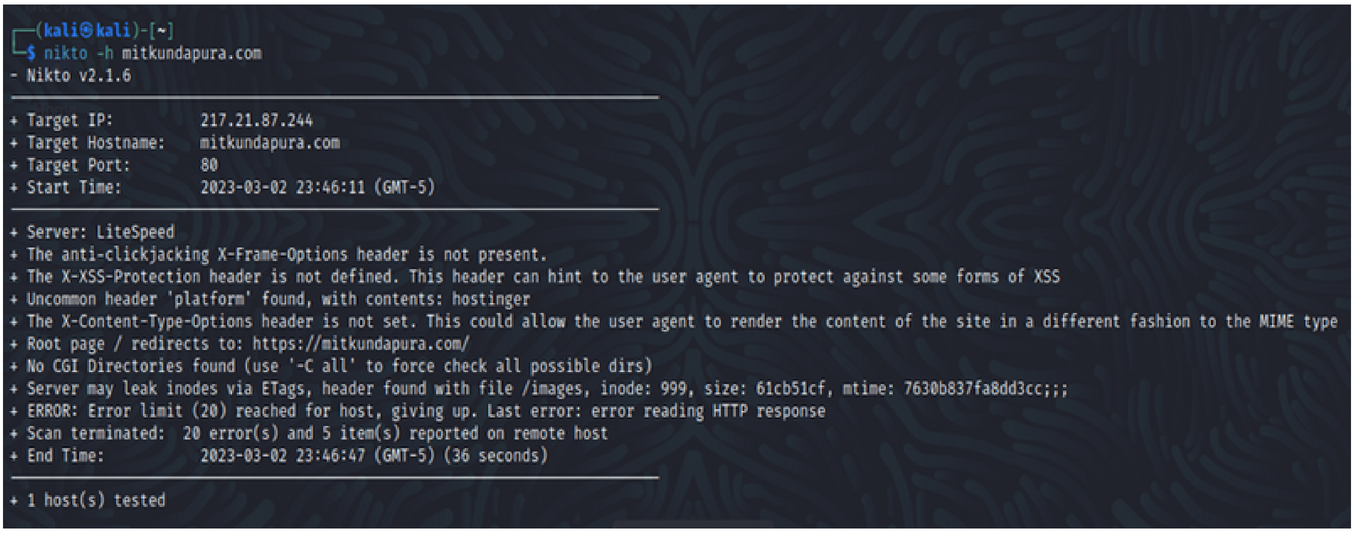
```
┌──(root㉿kali)-[/home/kali]
└─# whois mitkundapura.com
   Domain Name: MITKUNDAPURA.COM
   Registry Domain ID: 1656001143_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.registrar.eu
   Registrar URL: http://www.openprovider.com
   Updated Date: 2022-02-22T08:46:34Z
   Creation Date: 2011-05-13T20:28:43Z
   Registry Expiry Date: 2023-05-13T20:28:43Z
   Registrar: Hosting Concepts B.V. d/b/a Registrar.eu
   Registrar IANA ID: 1647
   Registrar Abuse Contact Email: abuse@registrar.eu
   Registrar Abuse Contact Phone: +31.104482297
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: NS1.DNS-PARKING.COM
   Name Server: NS2.DNS-PARKING.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-03-03T09:03:28Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
```

7.Nikto.

Nikto is an open-source command-line vulnerability scanner that looks for potentially dangerous files, outdated versions, server configuration files, and other issues on web servers. It is a well-known, simple-to-use, and extremely powerful pen testing tool.

command: nikto -h mitkundapura

Output :

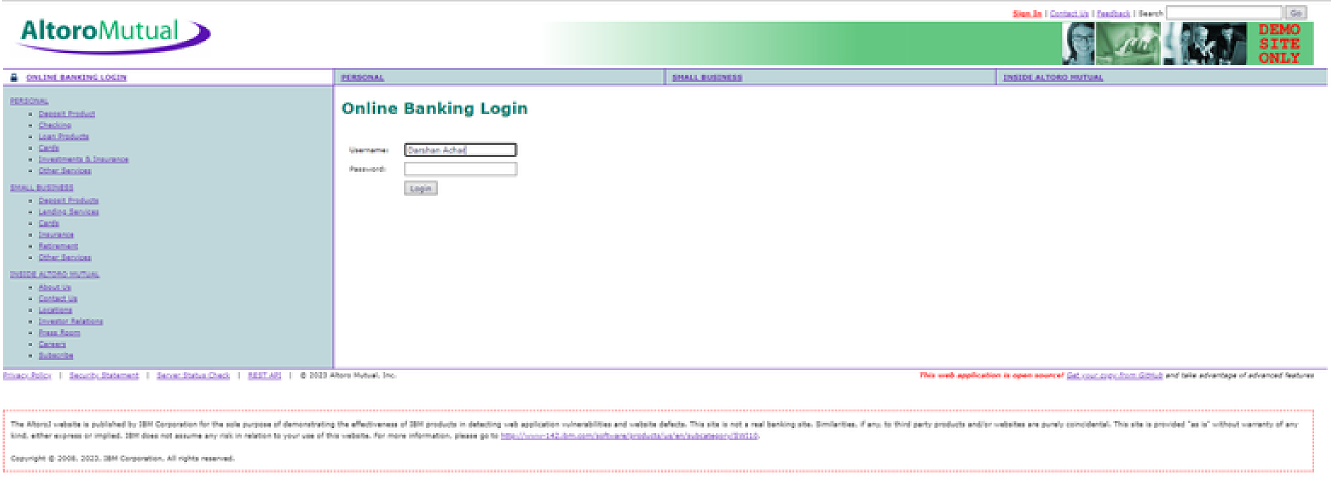


```
┌──(kali㉿kali)-[~]
└─$ nikto -h mitkundapura.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          217.21.87.244
+ Target Hostname:    mitkundapura.com
+ Target Port:        80
+ Start Time:         2023-03-02 23:46:11 (GMT-5)
---------------------------------------------------------------------------
+ Server: LiteSpeed
+ 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
+ Uncommon header 'platform' found, with contents: hostinger
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: https://mitkundapura.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /images, inode: 999, size: 61cb51cf, mtime: 7630b837fa8dd3cc;;;
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated:  20 error(s) and 5 item(s) reported on remote host
+ End Time:           2023-03-02 23:46:47 (GMT-5) (36 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

8.Crypto Configuration Flaw.

A cryptographic failure is a critical web application security flaw that exposes sensitive application data due to a faulty or non-existent cryptographic algorithm. Passwords, patient health records, business secrets, credit card information, email addresses, and other personal user information are examples.

Output :



Sign In | Contact Us | Feedback | Search [ ] Go

DEMO SITE ONLY

ONLINE BANKING LOGIN | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

PERSONAL
- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS
- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL
- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Online Banking Login

Username: Darshan Achal

Password:

Login

Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The Altoro) website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

Copyright © 2008, 2023, IBM Corporation, All rights reserved.

9.NetDiscover.

Netdiscover is a simple ARP scanner that can be used to search a network for live hosts. It can also search for multiple subnets. It simply displays the output in real time (ncurse). This can be used in the early stages of a pentest where you have network access. Netdiscover is a simple initial reconnaissance tool that can be very useful.

Command: To view the usage options.

```
# netdiscover -h
```

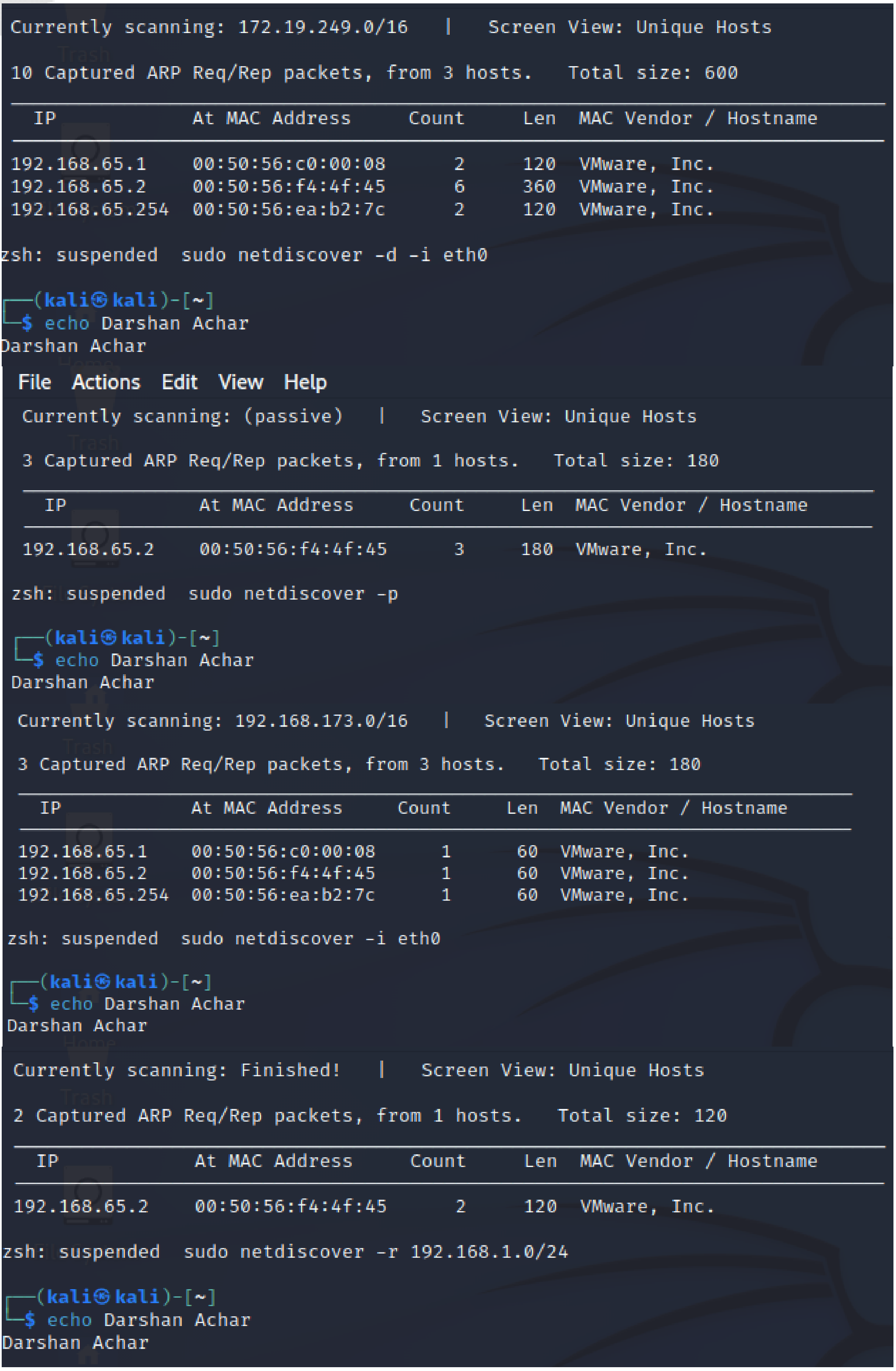
·use following command to check the IP Address:

```
# ifconfig
```

- We can scan a specific range with -r option

```
# netdiscover -r 192.168.19.0/24
```

Output :



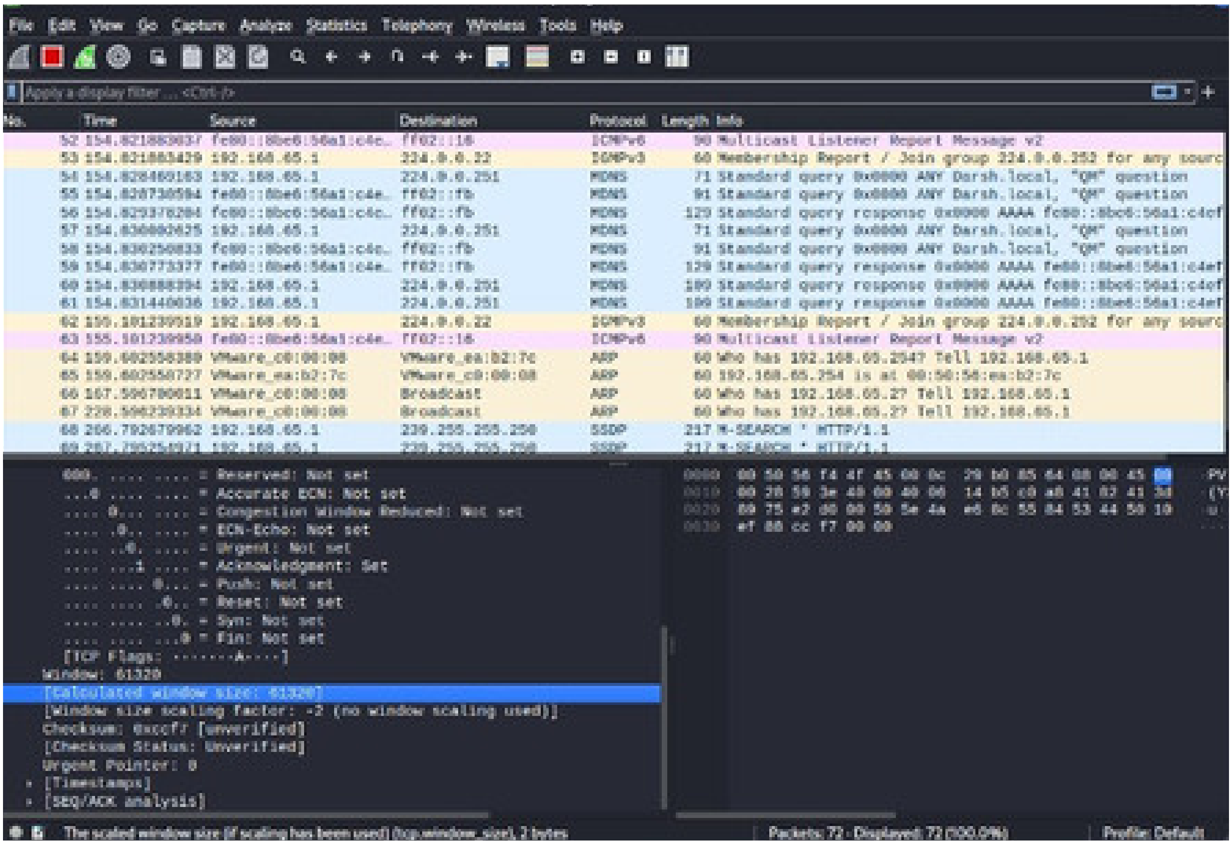
```
Currently scanning: 172.19.249.0/16   |   Screen View: Unique Hosts

10 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 600
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.65.1    00:50:56:c0:00:08      2     120  VMware, Inc.
192.168.65.2    00:50:56:f4:4f:45      6     360  VMware, Inc.
192.168.65.254  00:50:56:ea:b2:7c      2     120  VMware, Inc.

zsh: suspended  sudo netdiscover -d -i eth0

┌──(kali㉿kali)-[~]
└─$ echo Darshan Achar
Darshan Achar
```

```
Currently scanning: (passive)   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 180
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.65.2    00:50:56:f4:4f:45      3     180  VMware, Inc.

zsh: suspended  sudo netdiscover -p

┌──(kali㉿kali)-[~]
└─$ echo Darshan Achar
Darshan Achar

Currently scanning: 192.168.173.0/16   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.65.1    00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.65.2    00:50:56:f4:4f:45      1      60  VMware, Inc.
192.168.65.254  00:50:56:ea:b2:7c      1      60  VMware, Inc.

zsh: suspended  sudo netdiscover -i eth0

┌──(kali㉿kali)-[~]
└─$ echo Darshan Achar
Darshan Achar

Currently scanning: Finished!   |   Screen View: Unique Hosts

2 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 120
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.65.2    00:50:56:f4:4f:45      2     120  VMware, Inc.

zsh: suspended  sudo netdiscover -r 192.168.1.0/24

┌──(kali㉿kali)-[~]
└─$ echo Darshan Achar
Darshan Achar
```

9.Finding Data Packets 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.

Output:



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time           Source                     Destination        Protocol  Length Info
   52 154.821883037  fe80::8be6:56a1:c4e…        ff02::16           ICMPv6      90 Multicast Listener Report Message v2
   53 154.821883429  192.168.65.1               224.0.0.22         IGMPv3      60 Membership Report / Join group 224.0.0.252 for any sourc
   54 154.828460163  192.168.65.1               224.0.0.251        MDNS        71 Standard query 0x0000 ANY Darsh.local, "QM" question
   55 154.828730594  fe80::8be6:56a1:c4e…        ff02::fb           MDNS        91 Standard query 0x0000 ANY Darsh.local, "QM" question
   56 154.829376204  fe80::8be6:56a1:c4e…        ff02::fb           MDNS       129 Standard query response 0x0000 AAAA fe80::8be6:56a1:c4ef
   57 154.830802625  192.168.65.1               224.0.0.251        MDNS        71 Standard query 0x0000 ANY Darsh.local, "QM" question
   58 154.830250833  fe80::8be6:56a1:c4e…        ff02::fb           MDNS        91 Standard query 0x0000 ANY Darsh.local, "QM" question
   59 154.830773377  fe80::8be6:56a1:c4e…        ff02::fb           MDNS       129 Standard query response 0x0000 AAAA fe80::8be6:56a1:c4ef
   60 154.830888394  192.168.65.1               224.0.0.251        MDNS       109 Standard query response 0x0000 AAAA fe80::8be6:56a1:c4ef
   61 154.831440036  192.168.65.1               224.0.0.251        MDNS       109 Standard query response 0x0000 AAAA fe80::8be6:56a1:c4ef
   62 155.101239519  192.168.65.1               224.0.0.22         IGMPv3      60 Membership Report / Join group 224.0.0.252 for any sourc
   63 155.101239950  fe80::8be6:56a1:c4e…        ff02::16           ICMPv6      90 Multicast Listener Report Message v2
   64 159.602556389  VMware_c0:00:08            VMware_ea:b2:7c    ARP         60 Who has 192.168.65.254? Tell 192.168.65.1
   65 159.602556727  VMware_ea:b2:7c            VMware_c0:00:08    ARP         60 192.168.65.254 is at 00:50:56:ea:b2:7c
   66 167.596780611  VMware_c0:00:08            Broadcast          ARP         60 Who has 192.168.65.2? Tell 192.168.65.1
   67 228.596239334  VMware_c0:00:08            Broadcast          ARP         60 Who has 192.168.65.2? Tell 192.168.65.1
   68 266.792679962  192.168.65.1               239.255.255.250    SSDP       217 M-SEARCH * HTTP/1.1
   69 267.795754071  192.168.65.1               239.255.255.250    SSDP       217 M-SEARCH * HTTP/1.1
```

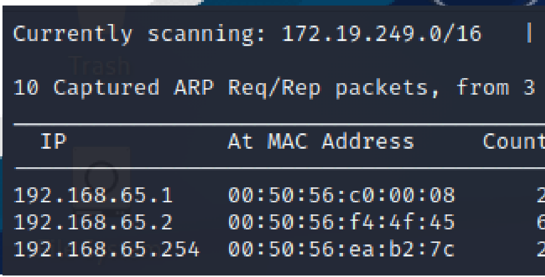
```
      000. .... .... = Reserved: Not set
      ...0 .... .... = Accurate ECN: Not set
      .... 0... .... = Congestion Window Reduced: Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······A····]
   Window: 61320
   [Calculated window size: 61320]
   [Window size scaling factor: -2 (no window scaling used)]
   Checksum: 0xccf7 [unverified]
   [Checksum Status: Unverified]
   Urgent Pointer: 0
 › [Timestamps]
 › [SEQ/ACK analysis]
```

```
0000  00 50 56 f4 4f 45 00 0c  29 b0 85 64 08 00 45 00   PV
0010  00 28 59 3e 40 00 40 06  14 b5 c0 a8 41 82 41 3d   (Y
0020  89 75 e2 d0 00 50 5e 4a  e6 8c 55 84 53 44 50 10   u
0030  ef 88 cc f7 00 00
```

The scaled window size (if scaling has been used) (tcp.window_size), 2 bytes

Packets: 72 · Displayed: 72 (100.0%)

Profile: Default

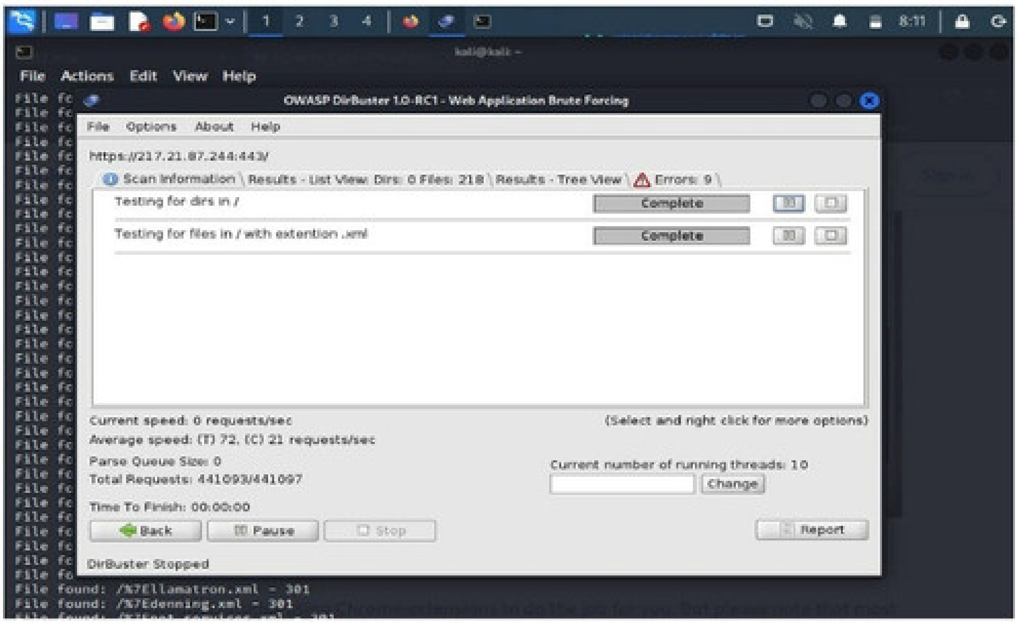


```
Currently scanning: 172.19.249.0/16   |

10 Captured ARP Req/Rep packets, from 3
_____________________________________________
  IP            At MAC Address       Count
---------------------------------------------
192.168.65.1    00:50:56:c0:00:08       2
192.168.65.2    00:50:56:f4:4f:45       6
192.168.65.254  00:50:56:ea:b2:7c       2
```

10.Finding XML pages in website using Dirbuster.

Dirbuster is used once you have scanned an IP address and found any vulnerabilities. DirBuster will help you map out the application. Building a directory of the target site is useful in finding as many potential points of entry to the target.

Output:



https://217.21.87.244:443/

Testing for dirs in / Complete

Testing for files in / with extention .xml Complete

Current speed: 0 requests/sec

(Select and right click for more options)

Average speed: (T) 72, (C) 21 requests/sec

Parse Queue Size: 0

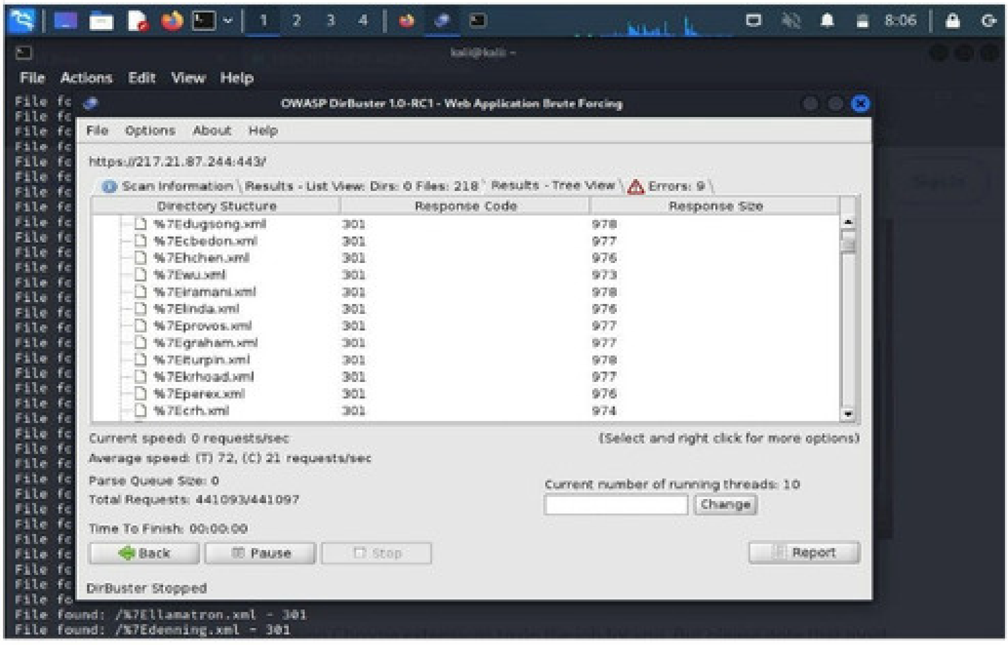
Current number of running threads: 10

Total Requests: 441093/441097

Time To Finish: 00:00:00

DirBuster Stopped

```
File found: /%7Ellamatron.xml - 301
File found: /%7Edenning.xml - 301
```



https://217.21.87.244:443/

Directory Stucture	Response Code	Response Size
%7Edugsong.xml	301	978
%7Ecbedon.xml	301	977
%7Ehchen.xml	301	976
%7Ewu.xml	301	973
%7Eiramani.xml	301	978
%7Elinda.xml	301	976
%7Eprovos.xml	301	977
%7Egraham.xml	301	977
%7Eturpin.xml	301	978
%7Ekrhoad.xml	301	977
%7Eperex.xml	301	976
%7Ecrh.xml	301	974

Current speed: 0 requests/sec

(Select and right click for more options)

Average speed: (T) 72, (C) 21 requests/sec

Parse Queue Size: 0

Current number of running threads: 10

Total Requests: 441093/441097

Time To Finish: 00:00:00

DirBuster Stopped

```
File found: /%7Ellamatron.xml - 301
File found: /%7Edenning.xml - 301
```