

Name: PRAMAL POOJARY

REG NO : 145CS20011

Date:02-03-2023

Task:2

1.Perform IP address spoofing:

In IP spoofing, a hacker uses tools to modify the source address in the packet header to make the receiving computer system think the packet is from a trusted source, such as another computer on a legitimate network, and accept it. This occurs at the network level, so there are no external signs of tampering.

```
$ ifconfig eth0 192.168.209.15
```

```
$ ifconfig
```

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.220.1 netmask 255.255.255.0 broadcast 192.168.220.255
    inet6 fe80::232b:b2eb:6cc:ea90 prefixlen 64 scopeid 0<20<link>
    ether 9e:01:23:fa:87:ea txqueuelen 1000 (Ethernet)
    RX packets 850 bytes 65030 (63.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 266 bytes 25888 (25.2 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 0<10<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

(kali㉿kali)-[~]
$ ifconfig eth0 192.168.220.2
SIOCSIFADDR: Operation not permitted
SIOCSIFFLAGS: Operation not permitted

(kali㉿kali)-[~]
$ sudo ifconfig eth0 192.168.220.2
[sudo] password for kali:

(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.220.2 netmask 255.255.255.0 broadcast 192.168.220.255
```

```
$ ifconfig eth0 192.168.220.2
SIOCSIFADDR: Operation not permitted
SIOCSIFFLAGS: Operation not permitted

(kali㉿kali)-[~]
$ sudo ifconfig eth0 192.168.220.2
[sudo] password for kali:

(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.220.2 netmask 255.255.255.0 broadcast 192.168.220.255
    inet6 fe80::232b:b2eb:6cc:ea90 prefixlen 64 scopeid 0<20<link>
    ether 9e:01:23:fa:87:ea txqueuelen 1000 (Ethernet)
    RX packets 866 bytes 65990 (64.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 266 bytes 25888 (25.2 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 0<10<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

(kali㉿kali)-[~]
$ echo PRAMAL
PRAMAL
```

2.Perform MAC address spoofing:

An attacker can mimic your MAC address and redirect data sent to your device to another and access your data. A MAC spoofing attack is when a hacker changes the MAC address of their device to match the MAC address of another on a network in order to gain unauthorized access or launch a Man- in-the-Middle attack.

```
$ macchanger -s eth0
```

```
$ ifconfig
```

```
$ macchanger -r eth0
```

```
(kali@kali)-[~]
└─$ macchanger -s eth0
Current MAC: 42:46:af:9b:9b:97 (unknown)
Permanent MAC: 00:0c:29:a7:fc:b0 (VMware, Inc.)

(kali@kali)-[~]
└─$ sudo macchanger -r eth0
Current MAC: 42:46:af:9b:9b:97 (unknown)
Permanent MAC: 00:0c:29:a7:fc:b0 (VMware, Inc.)
New MAC: 26:99:b3:6a:75:22 (unknown)

(kali@kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.220.132 netmask 255.255.255.0 broadcast 192.168.220.255
    inet6 fe80::232b:b2eb:6cc:ea90 prefixlen 64 scopeid 0<20<link>
    ether 26:99:b3:6a:75:22 txqueuelen 1000 (Ethernet)
    RX packets 3036 bytes 563209 (550.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 196237 bytes 11799596 (11.2 MiB)
    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 0<10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 5 bytes 330 (330.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 5 bytes 330 (330.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
Permanent MAC: 00:0c:29:a7:fc:b0 (VMware, Inc.)
New MAC: 26:99:b3:6a:75:22 (unknown)

(kali@kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.220.132 netmask 255.255.255.0 broadcast 192.168.2
    inet6 fe80::232b:b2eb:6cc:ea90 prefixlen 64 scopeid 0<20<link>
    ether 26:99:b3:6a:75:22 txqueuelen 1000 (Ethernet)
    RX packets 3036 bytes 563209 (550.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 196237 bytes 11799596 (11.2 MiB)
    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 0<10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 5 bytes 330 (330.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 5 bytes 330 (330.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
└─$ echo PRAMAL
PRAMAL
```

3.Any 5 whatweb commands:

Basic scanning:

The most basic command to scan a website with WhatWeb is:

\$ whatweb testfire.net

```
(kali@kali)-[~]
$ whatweb testfire.net
http://testfire.net [200 OK] Apache, Cookies[JSESSIONID], Country[UNITED STATES][US], HTTPServer[Apache-Coyote/1.1], HttpOnly[JSESSIONID], IP[65.61.137.117], Java, Title[Altoro Mutual]

(kali@kali)-[~]
$ echo PRAMAL
PRAMAL
```

This will perform a default scan of the website and display the identified technologies.

Verbose scanning:

If you want more detailed information about the website, you can use the verbose flag (-v):

\$ whatweb -v [website URL]

```
(kali@kali)-[~]
$ whatweb -v testfire.net
WhatWeb report for http://testfire.net
Status : 200 OK
Title : Altoro Mutual
IP : 65.61.137.117
Country : UNITED STATES, US

Summary : Apache, Cookies[JSESSIONID], HTTPServer[Apache-Coyote/1.1], HttpOnly[JSESSIONID], Java

Detected Plugins:
[ Apache ]
The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows NT. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards.

Google Dorks: (3)
Website : http://httpd.apache.org/

[ Cookies ]
Display the names of cookies in the HTTP headers. The values are not returned to save on space.

String : JSESSIONID

[ HTTPServer ]
HTTP server header string. This plugin also attempts to
```

This will perform a more thorough scan and provide additional details, such as HTTP headers and server information.

\$ whatweb -a 3 testfire.net

```
(kali@kali)-[~]
$ whatweb -v -a 3 testfire.net
WhatWeb report for http://testfire.net
Status : 200 OK
Title : Altoro Mutual
IP : 65.61.137.117
Country : UNITED STATES, US

Summary : Apache, Cookies[JSESSIONID], HTTPServer[Apache-Coyote/1.1], HttpOnly[JSESSIONID], Java

Detected Plugins:
[ Apache ]
The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows NT. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards.

Google Dorks: (3)
Website : http://httpd.apache.org/

[ Cookies ]
Display the names of cookies in the HTTP headers. The values are not returned to save on space.

String : JSESSIONID

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

```
kali@kali: ~
File Actions Edit View Help
String      : Apache-Coyote/1.1 (from server string)

[ HttpOnly ]
If the HttpOnly flag is included in the HTTP set-cookie
response header and the browser supports it then the cookie
cannot be accessed through client side script - More Info:
http://en.wikipedia.org/wiki/HTTP_cookie

String      : JSESSIONID

[ Java ]
Java allows you to play online games, chat with people
around the world, calculate your mortgage interest, and
view images in 3D, just to name a few. It's also integral
to the intranet applications and other e-business solutions
that are the foundation of corporate computing.

Website     : http://www.java.com/

HTTP Headers:
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=E1760CDEE1BA65C7D170D9912ADE9925; Path=/; HttpOnly
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Fri, 03 Mar 2023 08:49:41 GMT
Connection: close

(kali@kali)-[~]
$ echo PRAMAL
PRAMAL
```

\$ whatweb --max-redirect 2 testfire.net

```
(kali@kali)-[~]
$ whatweb --max-redirect 2 testfire.net
http://testfire.net [200 OK] Apache, Cookies[JSESSIONID], Country[UNITED STATES][US], HTTPServer[Apache-Coyote/1.1], HttpOnly[JSESSIONID], IP[65.61.137.117]
, Java, Title[Altoro Mutual]

(kali@kali)-[~]
$ echo PRAMAL
PRAMAL
```

\$ whatweb -v -a 3 testfire.net

```
(kali@kali)-[~]
$ whatweb -v -a 3 testfire.net
WhatWeb report for http://testfire.net
Status      : 200 OK
Title       : Altoro Mutual
IP          : 65.61.137.117
Country     : UNITED STATES, US

Summary     : Apache, Cookies[JSESSIONID], HTTPServer[Apache-Coyote/1.1], HttpOnly[JSESSIONID], Java

Detected Plugins:
[ Apache ]
The Apache HTTP Server Project is an effort to develop and
maintain an open-source HTTP server for modern operating
systems including UNIX and Windows NT. The goal of this
project is to provide a secure, efficient and extensible
server that provides HTTP services in sync with the current
HTTP standards.

Google Dorks: (3)
Website      : http://httpd.apache.org/

[ Cookies ]
Display the names of cookies in the HTTP headers. The
values are not returned to save on space.

String       : JSESSIONID

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

```
kali@kali: ~
File Actions Edit View Help
String      : Apache-Coyote/1.1 (from server string)

[ HttpOnly ]
If the HttpOnly flag is included in the HTTP set-cookie
response header and the browser supports it then the cookie
cannot be accessed through client side script - More Info:
http://en.wikipedia.org/wiki/HTTP_cookie

String      : JSESSIONID

[ Java ]
Java allows you to play online games, chat with people
around the world, calculate your mortgage interest, and
view images in 3D, just to name a few. It's also integral
to the intranet applications and other e-business solutions
that are the foundation of corporate computing.

Website     : http://www.java.com/

HTTP Headers:
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=E1760CDEE1BA65C7D170D9912ADE9925; Path=/; HttpOnly
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Fri, 03 Mar 2023 08:49:41 GMT
Connection: close

(kali@kali)-[~]
$ echo PRAMAL
PRAMAL
```

4.Any 5 nslookup commands:

\$ nslookup testfire.net

```
(kali㉿kali)-[~]
└─$ nslookup testfire.net
Server:      192.168.220.2
Address:     192.168.220.2#53

Non-authoritative answer:
Name:   testfire.net
Address: 65.61.137.117

(kali㉿kali)-[~]
└─$ echo PRAMAL
PRAMAL
```

\$ nslookup -type=mx testfire.net

This command will perform a DNS lookup for the mail exchange (MX) records associated with the domain name “testfire.net”.

```
(kali㉿kali)-[~]
└─$ nslookup -type=mx testfire.net
Server:      192.168.220.2
Address:     192.168.220.2#53

Non-authoritative answer:
** Can't find testfire.net: No answer

Authoritative answers can be found from:
testfire.net
  origin = asia3.akam.net
  mail addr = hostmaster.akamai.com
  serial = 1366025607
  refresh = 43200
  retry = 7200
  expire = 604800
  minimum = 86400

(kali㉿kali)-[~]
└─$ echo PRAMAL
PRAMAL
```

\$ nslookup -type=ns testfire.net

This command will perform a DNS lookup for the name server (NS) records associated with the domain name “testfire.net”.

```
(kali㉿kali)-[~]
└─$ nslookup -type=ns testfire.net
Server:      192.168.220.2
Address:     192.168.220.2#53

Non-authoritative answer:
testfire.net    nameserver = eur2.akam.net.
testfire.net    nameserver = ns1-99.akam.net.
testfire.net    nameserver = usc3.akam.net.
testfire.net    nameserver = ns1-206.akam.net.
testfire.net    nameserver = usc2.akam.net.
testfire.net    nameserver = usw2.akam.net.
testfire.net    nameserver = asia3.akam.net.
testfire.net    nameserver = eur5.akam.net.

Authoritative answers can be found from:

(kali㉿kali)-[~]
└─$ echo PRAMAL
PRAMAL
```

\$ nslookup -type=a www.testfire.net

This command will perform a DNS lookup for the IPv6 address associated with the subdomain www. testfire.net

```
(kali㉿kali)-[~]
└─$ nslookup -type=a testfire.net
Server:      192.168.220.2
Address:     192.168.220.2#53

Non-authoritative answer:
Name:   testfire.net
Address: 65.61.137.117

(kali㉿kali)-[~]
└─$ echo PRAMAL
PRAMAL
```


\$ Nslookup -type=aaaa mitkundapura

```
(kali㉿kali)-[~]
$ nslookup -type=aaaa mitkundapura.com
Server:      192.168.220.2
Address:     192.168.220.2#53

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

(kali㉿kali)-[~]
$ echo PRAMAL
PRAMAL
```

5.whois Commands:

The whois command is a protocol used to look up information about domain names, IP addresses, and other network-related information. Here are some common WHOIS commands:

\$ whois mitkundapura.com

This command will display information about the domain name, such as the name of the registrant, the name servers, and the date of registration

```
File Actions Edit View Help
(kali㉿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: 2023-03-06T04:35:11Z <<<

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
```

```
File Actions Edit View Help
Name Server: ns2.dns-parking.com
Name Server: ns1.dns-parking.com
DNSSEC: unsigned

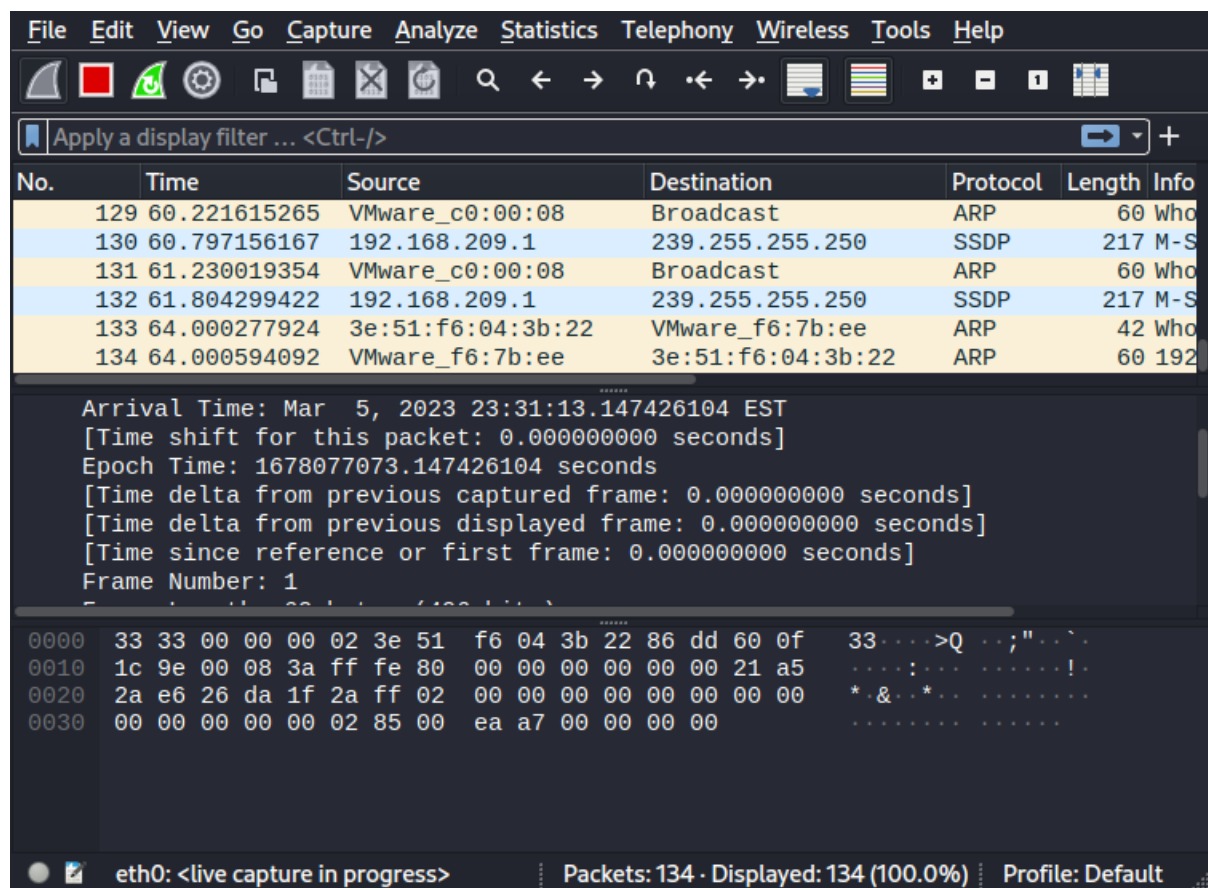
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2023-03-06T04:35:27Z <<<

; The data in this registrar whois database is provided to you for
; information purposes only, and may be used to assist you in obtaining
; information about or related to domain name registration records.
; We do not guarantee its accuracy.
; By submitting a WHOIS query, you agree that you will use this data
; only for lawful purposes and that, under no circumstances, you will
; use this data to
; a) allow, enable, or otherwise support the transmission by e-mail,
; telephone, or facsimile of mass, unsolicited, commercial advertising
; or solicitations to entities other than the data recipient's own
; existing customers; or
; b) enable high volume, automated, electronic processes that send queries
; or data to the systems of any Registry Operator or ICANN-Accredited
; registrar, except as reasonably necessary to register domain names
; or modify existing registrations.
; The compilation, repackaging, dissemination or other use of this data
; is expressly prohibited without prior written consent.
; These terms may be changed without prior notice. By submitting this
; query, you agree to abide by this policy.

(kali@kali)-[~]
$ echo PRAMAL
PRAMAL
```

6.Find data packets using wireshark:

You can easily find packets once you have captured some packets or have read in a previously saved capture file. Simply select Edit Find Packet... in the main menu. Wireshark will open a toolbar between the main toolbar and the packet list, "The "Find Packet" toolbar".



7.Any 5 netdiscover command:

Netdiscover is a network scanning tool used for discovering hosts and gathering information about them on a local network. Here are some of the basic commands:

\$ netdiscover -i eth0

```
File Actions Edit View Help
Currently scanning: 172.26.191.0/16 | Screen View: Unique Hosts
52 Captured ARP Req/Rep packets, from 3 hosts. Total size: 3120
+-----+-----+-----+-----+-----+
| IP           | At MAC Address | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+
| 192.168.220.1 | 00:50:56:c0:00:08 | 49    | 2940 | VMware, Inc.          |
| 192.168.220.254 | 00:50:56:fd:20:60 | 2     | 120  | VMware, Inc.          |
| 192.168.220.2  | 00:50:56:f4:a6:be | 1     | 60   | VMware, Inc.          |
+-----+-----+-----+-----+-----+
zsh: suspended netdiscover -i eth0
(root@kali)~# echo PRAMAL
PRAMAL
```

\$ netdiscover -p

```
File Actions Edit View Help
Currently scanning: (passive) | Screen View: Unique Hosts
43 Captured ARP Req/Rep packets, from 3 hosts. Total size: 2580
+-----+-----+-----+-----+-----+
| IP           | At MAC Address | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+
| 192.168.220.1 | 00:50:56:c0:00:08 | 41    | 2460 | VMware, Inc.          |
| 192.168.220.2 | 00:50:56:f4:a6:be | 1     | 60   | VMware, Inc.          |
| 192.168.220.254 | 00:50:56:fd:20:60 | 1     | 60   | VMware, Inc.          |
+-----+-----+-----+-----+-----+
zsh: suspended netdiscover -p
(root@kali)~# echo PRAMAL
PRAMAL
```

\$ netdiscover -r 192.168.0.15

```
File Actions Edit View Help
Currently scanning: Finished! | 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 |
+-----+-----+-----+-----+-----+
| 192.168.220.1 | 00:50:56:c0:00:08 | 1     | 60   | VMware, Inc.          |
| 192.168.220.2 | 00:50:56:f4:a6:be | 1     | 60   | VMware, Inc.          |
| 192.168.220.254 | 00:50:56:fd:20:60 | 1     | 60   | VMware, Inc.          |
+-----+-----+-----+-----+-----+
zsh: suspended netdiscover -r 192.168.220.138
(root@kali)~# echo pramal
pramal
```



```
$ netdiscover -i eth0 -f
```

```
File Actions Edit View Help
Currently scanning: 172.28.160.0/16 | 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 |
+-----+-----+-----+-----+-----+-----+
| 192.168.220.1 | 00:50:56:c0:00:08 | 1     | 60  | VMware, Inc.          |
| 192.168.220.2 | 00:50:56:f4:a6:be | 1     | 60  | VMware, Inc.          |
| 192.168.220.254 | 00:50:56:fd:20:60 | 1     | 60  | VMware, Inc.          |
+-----+-----+-----+-----+-----+-----+

zsh: suspended netdiscover -i eth0 -f

(root@kali)-[~]
# echo PRAMAL
PRAMAL
```

```
$ netdiscover -s 0.5
```

```
Root Terminal Emulator
Opens a terminal as the root user, using sudo to ask for the password
Currently scanning: 172.16.30.0/16 | Screen View: Unique Hosts
6 Captured ARP Req/Rep packets, from 3 hosts. Total size: 360

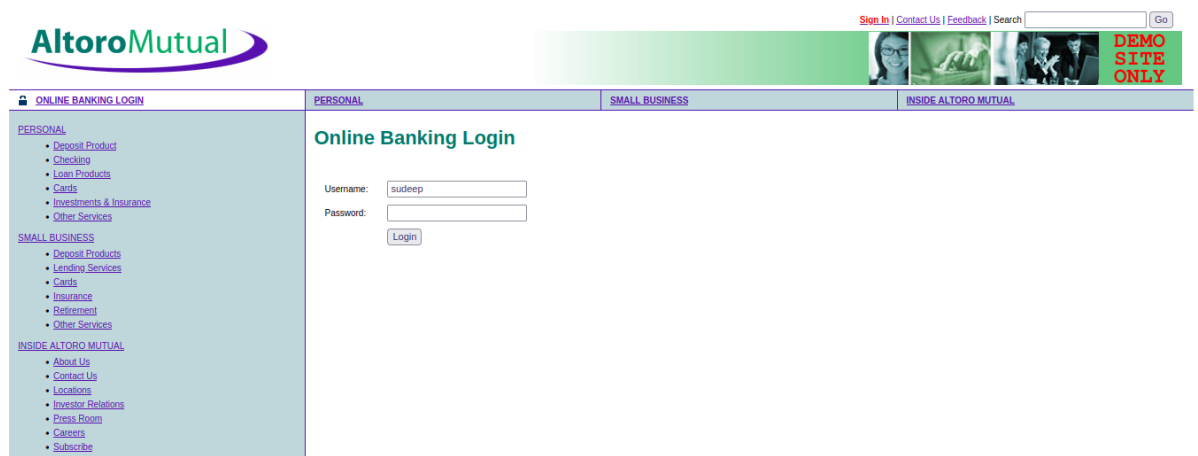
+-----+-----+-----+-----+-----+-----+
| IP           | At MAC Address | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+-----+
| 192.168.220.1 | 00:50:56:c0:00:08 | 2     | 120 | VMware, Inc.          |
| 192.168.220.2 | 00:50:56:f4:a6:be | 2     | 120 | VMware, Inc.          |
| 192.168.220.254 | 00:50:56:fd:20:60 | 2     | 120 | VMware, Inc.          |
+-----+-----+-----+-----+-----+-----+

zsh: suspended netdiscover -s 0.5

(root@kali)-[~]
# echo PRAMAL
PRAMAL
```

8.CryptoConfiguration Flaw:


CryptoConfiguration typically refers to the configuration of cryptographic protocols and algorithms used to protect sensitive data and communications.A flaw is context could refers to a weakness or vulnarability in the configuration that could that could potentially be exploited by the attackers.



9. Nikto commands:

Nikto is a popular web server scanner that can help you identify potential vulnerabilities on a web server. Here are some common Nikto commands:

```
$ nikto -host vulnweb.com
```



```
File Actions Edit View Help
(kali@kali)~]
$ nikto -host vulnweb.com
- Nikto v2.1.6

+ Target IP: 44.228.249.3
+ Target Hostname: vulnweb.com
+ Target Port: 80
+ Start Time: 2023-03-06 01:14:25 (GMT-5)

+ Server: nginx/1.19.0
+ 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
+ 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
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 3 item(s) reported on remote host
+ End Time: 2023-03-06 01:16:03 (GMT-5) (98 seconds)

+ 1 host(s) tested

(kali@kali)~]
$ echo PRAMAL
PRAMAL
```

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. DirBuster attempts to find these. DirBuster searches for hidden pages and directories on a web server. Sometimes developers will leave a page accessible, but unlinked. DirBuster is meant to find these potential vulnerabilities. This is a Java application developed by OWASP.

