

Name:SHREYAS HEGDE

Reg No:145CS20018

Date:02-03-2023

Task:2

1.Perform IP address spoofing:

IP address spoofing is the act of falsifying the source IP address of a network packet to hide the identity of the sender or to impersonate another system.

```
$ ifconfig eth0 192.168.209.15
```

```
$ ifconfig
```

```
(kali㉿kali)-[~]
└─$ sudo ifconfig eth0 192.168.209.15
[sudo] password for kali:

(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.209.15 netmask 255.255.255.0 broadcast 192.168.209.255
    inet6 fe80::7b85:501d:ae77:6c46 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:7c:60:ab txqueuelen 1000 (Ethernet)
    RX packets 31 bytes 2428 (2.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 26 bytes 3548 (3.4 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

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

(kali㉿kali)-[~]
└─$
```

2.Perform MAC address spoofing:

MAC address spoofing is the act of modifying the Media Access Control (MAC) address of a network interface to impersonate another device or to hide the identity of the sender.

```
$ macchanger -s eth0
```

```
$ ifconfig
```

```
$ macchanger -r eth0
```

```
$ ifconfig eth0 down
```

```
(kali@kali)~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.11.138 netmask 255.255.255.0 broadcast 192.168.11.255
    inet6 fe80::7b85:581d:ae77:6c46 prefixlen 64 scopeid 0<20<link>
    ether 00:0c:29:7c:60:ab txqueuelen 1000 (Ethernet)
    RX packets 79 bytes 5308 (5.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 31 bytes 3852 (3.7 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 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)~$ sudo macchanger -s eth0
Current MAC: 00:0c:29:7c:60:ab (VMware, Inc.)
Permanent MAC: 00:0c:29:7c:60:ab (VMware, Inc.)

(kali@kali)~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.11.138 netmask 255.255.255.0 broadcast 192.168.11.255
    inet6 fe80::7b85:581d:ae77:6c46 prefixlen 64 scopeid 0<20<link>
    ether 00:0c:29:7c:60:ab txqueuelen 1000 (Ethernet)
    RX packets 79 bytes 5308 (5.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 31 bytes 3852 (3.7 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 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
```

```
File Actions Edit View Help
RX packets 79 bytes 5308 (5.1 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 31 bytes 3852 (3.7 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 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)~$ sudo macchanger -r eth0
Current MAC: 00:0c:29:7c:60:ab (VMware, Inc.)
Permanent MAC: 00:0c:29:7c:60:ab (VMware, Inc.)
New MAC: 0e:94:1f:56:98:fb (unknown)

(kali@kali)~$ sudo ifconfig eth0 down

(kali@kali)~$ ifconfig
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 shreyas
shreyas

(kali@kali)~$
```

3. Any 5 whatweb commands:

Basic scanning:

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

```
$ whatweb websiteURL
```

```
(kali@kali)-[~]
└─$ uname -a
Linux kali 4.15.0-46-generic #49-Ubuntu SMP Tue Aug 14 22:03:10 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
└─$ curl -s http://www.mitkundapura.com
http://www.mitkundapura.com [301 Moved Permanently] Country[UNITED KINGDOM][GB], HTML5, HTTPServer[LiteSpeed], IP[217.21.87.244], LiteSpeed, RedirectLocation
status 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]
lakatte Institute of Technology & Management, Kundapura Home], UncommonHeaders[platform,content-security-policy,alt-svc], X-Powered-By[PHP/7.4.33]

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

(kali@kali)-[~]
└─$
```

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]
```

```

[~]$ curl@kali:~$-[-]
[~]$ whatweb -v http://www.mitkundapura.com
WhatWeb report for http://www.mitkundapura.com
Status : 301 Moved Permanently
Title : 301 Moved Permanently
IP : 217.21.87.244
Country : United Kingdom, GB

Summary : HTML5, HTTPServer[LiteSpeed], LiteSpeed, RedirectedLocation[https://www.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

[ RedirectedLocation ]
    HTTP Server string location, used with http-status 301 and
    302
    String      : https://www.mitkundapura.com/ (from location)

[ 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
    plugin, eg. x-powered-by, server and x-aspect-version.
    Info about headers can be found at www.http-stats.com

    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
    plugin, eg. x-powered-by, server and x-aspect-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
transfer-encoding: chunked
content-encoding: gzip
vary: Accept-Encoding
date: Fri, 03 Mar 2023 06:51:51 GMT
server: LiteSpeed
platform: hostingtor
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, h3-Q041="443"; ma=2592000, h3-Q038="443"; ma=2592000, h3-Q035="443"; ma=2592000, h3-Q032="443"; ma=2592000, h3-Q030="443"; ma=2592000, h3-Q027="443"; ma=2592000, h3-Q025="443"; ma=2592000, h3-Q023="443"; ma=2592000, h3-Q022="443"; ma=2592000, h3-Q021="443"; ma=2592000, h3-Q019="443"; ma=2592000, h3-Q018="443"; ma=2592000, h3-Q016="443"; ma=2592000, h3-Q015="443"; ma=2592000, h3-Q014="443"; ma=2592000, h3-Q013="443"; ma=2592000, h3-Q012="443"; ma=2592000, h3-Q011="443"; ma=2592000, h3-Q010="443"; ma=2592000, h3-Q009="443"; ma=2592000, h3-Q008="443"; ma=2592000, h3-Q007="443"; ma=2592000, h3-Q006="443"; ma=2592000, h3-Q005="443"; ma=2592000, h3-Q004="443"; ma=2592000, h3-Q003="443"; ma=2592000, h3-Q002="443"; ma=2592000, h3-Q001="443"; ma=2592000, h3="443"; ma=2592000

[~]$ curl@kali:~$-[-]
[~]$ echo shreyas
shreyas

```

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

\$ whatweb -a 3 http://www.mitkundapura.com

```
(kali@kali)-[~]
└─$ whatweb -a 3 http://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/], 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], lakatte Institute of Technology & Management, Kundapura Home, UncommonHeaders[platform,content-security-policy,alt-svc], X-Powered-By[PHP/7.4.33]

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

(kali@kali)-[~]
└─$
```

\$ whatweb --max-redirect 2 http://www.mitkundapura.com

```
(kali@kali)-[~]
└─$ whatweb --max-redirect 2 http://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/], 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], lakatte Institute of Technology & Management, Kundapura Home, UncommonHeaders[platform,content-security-policy,alt-svc], X-Powered-By[PHP/7.4.33]

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

(kali@kali)-[~]
└─$
```

\$ whatweb -v -a 3 http://www.mitkundapura.com

```
(kali@kali)-[~]
└─$ whatweb -v -a 3 http://www.mitkundapura.com
WhatWeb report for http://www.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://www.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://www.mitkundapura.com/ (from location)
[ 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-aspmet-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
transfer-encoding: chunked
content-encoding: gzip
vary: Accept-Encoding
date: Fri, 03 Mar 2023 07:38:59 GMT
server: LiteSpeed
platform: hostingner
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="

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

4. Any 5 nslookup commands:

\$ nslookup google.com

```
(kali@kali)-[~]
└─$ nslookup google.com
Server:      192.168.11.2
Address:     192.168.11.2#53
Non-authoritative answer:
Name:   google.com
Address: 172.217.166.46
Name:   google.com
Address: 2404:6800:4007:81f::200e

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

(kali@kali)-[~]
└─$
```

\$ nslookup -type=mx mitkundapura.com

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

```
(kali@kali)-[~]
└─$ nslookup -type=mx mitkundapura.com
Server:      192.168.11.2
Address:     192.168.11.2#53
Non-authoritative answer:
mitkundapura.com mail exchanger = 5 alt1.aspmx.l.google.com.
mitkundapura.com mail exchanger = 10 alt4.aspmx.l.google.com.
mitkundapura.com mail exchanger = 5 alt2.aspmx.l.google.com.
mitkundapura.com mail exchanger = 1 aspmx.l.google.com.
mitkundapura.com mail exchanger = 10 alt3.aspmx.l.google.com.

Authoritative answers can be found from:

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

(kali@kali)-[~]
└─$
```

\$ nslookup -type=ns mitkundapura.com

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

```
(kali@kali)-[~]
└─$ nslookup -type=ns mitkundapura.com
Server:      192.168.11.2
Address:     192.168.11.2#53
Non-authoritative answer:
mitkundapura.com nameserver = ns2.dns-parking.com.
mitkundapura.com nameserver = ns1.dns-parking.com.

Authoritative answers can be found from:

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

(kali@kali)-[~]
└─$
```

```
$ nslookup -type=a www.mitkundapura.com
```

This command will perform a DNS lookup for the IPv4 address associated with the subdomain www.example.com.

```
(kali@kali)-[~]
$ nslookup -type=a www.mitkundapura.com
Server:      192.168.11.2
Address:     192.168.11.2#53
Non-authoritative answer:
www.mitkundapura.com canonical name = mitkundapura.com.
Name:   mitkundapura.com
Address: 217.21.87.244

(kali@kali)-[~]
$ echo shreyas
shreyas

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

```
$ nslookup -type=aaaa www.mitkundapura.com
```

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

```
(kali@kali)-[~]
$ nslookup -type=aaaa www.mitkundapura.com
Server:      192.168.11.2
Address:     192.168.11.2#53
Non-authoritative answer:
www.mitkundapura.com canonical name = mitkundapura.com.
Name:   mitkundapura.com
Address: 2a02:4780:11:771:0:2d4c:6d7f:1

(kali@kali)-[~]
$ echo shreyas
shreyas

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


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

```
(kali@kali)-[~]
└─$ whois mitkundapura.com
Domain Name: MITKUNDAPURA.COM
Registry Domain ID: 165600133_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrar.eu
Registrar URL: http://www.openprovider.com
Updated Date: 2022-02-22T08:46:54Z
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: +31.184482297
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: 2023-03-03T05:15:07Z <<<

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
```

```
If you have a legitimate interest in viewing the non-public WHOIS details, send
your request and the reasons for your request to whoisrequest@markmonitor.com
and specify the domain name in the subject line. We will review that request and
may ask for supporting documentation and explanation.

The data in MarkMonitor's WHOIS database is provided for information purposes,
and to assist persons in obtaining information about or related to a domain
name's registration record. While MarkMonitor believes the data to be accurate,
the data is provided "as is" with no guarantee or warranties regarding its
accuracy.

By submitting a WHOIS query, you agree that you will use this data only for
lawful purposes and that, under no circumstances will you use this data to:
(1) allow, enable, or otherwise support the transmission by email, telephone,
or facsimile of mass, unsolicited, commercial advertising, or spam; or
(2) enable high volume, automated, or electronic processes that send queries,
data, or email to MarkMonitor (or its systems) or the domain name contacts (or
its systems).

MarkMonitor reserves the right to modify these terms at any time.

By submitting this query, you agree to abide by this policy.

MarkMonitor Domain Management(TM)
Protecting companies and consumers in a digital world.

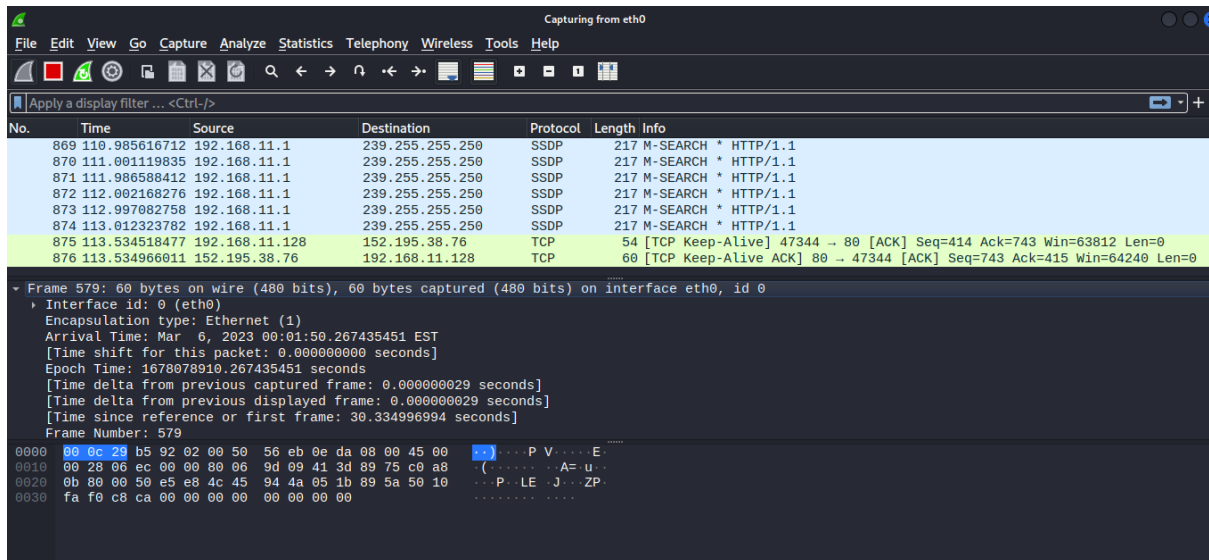
Visit MarkMonitor at https://www.markmonitor.com
Contact us at +1.8007459229
In Europe, at +44.02032062220
-

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

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".

\$Wireshark



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

```
Currently scanning: 192.168.243.0/16 | Screen View: Unique Hosts
19 Captured ARP Req/Rep packets, from 3 hosts. Total size: 1140


| IP             | At MAC Address    | Count | Len | MAC Vendor / Hostname |
|----------------|-------------------|-------|-----|-----------------------|
| 192.168.11.1   | 00:50:56:c0:00:08 | 15    | 900 | VMware, Inc.          |
| 192.168.11.2   | 00:50:56:eb:0e:da | 2     | 120 | VMware, Inc.          |
| 192.168.11.254 | 00:50:56:f5:65:0a | 2     | 120 | VMware, Inc.          |


zsh: suspended sudo netdiscover -i eth0
(kali@kali)-[~]
$ echo shreyas
shreyas
(kali@kali)-[~]
$
```

\$ netdiscover -p

```
Currently scanning: (passive) | Screen View: Unique Hosts
26 Captured ARP Req/Rep packets, from 1 hosts. Total size: 1560


| IP           | At MAC Address    | Count | Len  | MAC Vendor / Hostname |
|--------------|-------------------|-------|------|-----------------------|
| 192.168.11.1 | 00:50:56:c0:00:08 | 26    | 1560 | VMware, Inc.          |


zsh: suspended sudo netdiscover -p
(kali@kali)-[~]
$ echo shreyas
shreyas
(kali@kali)-[~]
$
```

\$ netdiscover -r 192.168.0.15

```
Currently scanning: Finished! | Screen View: Unique Hosts
19 Captured ARP Req/Rep packets, from 3 hosts. Total size: 1140


| IP             | At MAC Address    | Count | Len | MAC Vendor / Hostname |
|----------------|-------------------|-------|-----|-----------------------|
| 192.168.11.1   | 00:50:56:c0:00:08 | 15    | 900 | VMware, Inc.          |
| 192.168.11.2   | 00:50:56:eb:0e:da | 2     | 120 | VMware, Inc.          |
| 192.168.11.254 | 00:50:56:f5:65:0a | 2     | 120 | VMware, Inc.          |


zsh: suspended sudo netdiscover -r 192.168.11.128
(kali@kali)-[~]
$ echo shreyas
shreyas
(kali@kali)-[~]
$
```

```
$ netdiscover -d -i eth0
```

```
File Actions Edit View Help
Currently scanning: 192.168.19.0/16 | 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 |
+-----+-----+-----+-----+-----+-----+
| 192.168.11.1 | 00:50:56:c0:00:08 | 1     | 60  | VMware, Inc.          |
| 192.168.11.2 | 00:50:56:eb:0e:da | 1     | 60  | VMware, Inc.          |
| 192.168.11.254 | 00:50:56:f5:65:0a | 1     | 60  | VMware, Inc.          |
+-----+-----+-----+-----+-----+-----+

zsh: suspended sudo netdiscover -d -i eth0

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

(kali@kali)-[~]
└─$
```

```
$ sudo netdiscover -c 192.168.11.128
```

```
Currently scanning: 192.168.0.0/16 | Screen View: Unique Hosts
12 Captured ARP Req/Rep packets, from 1 hosts. Total size: 720

+-----+-----+-----+-----+-----+-----+
| IP           | At MAC Address | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+-----+
| 192.168.11.1 | 00:50:56:c0:00:08 | 12    | 720 | VMware, Inc.          |
+-----+-----+-----+-----+-----+-----+

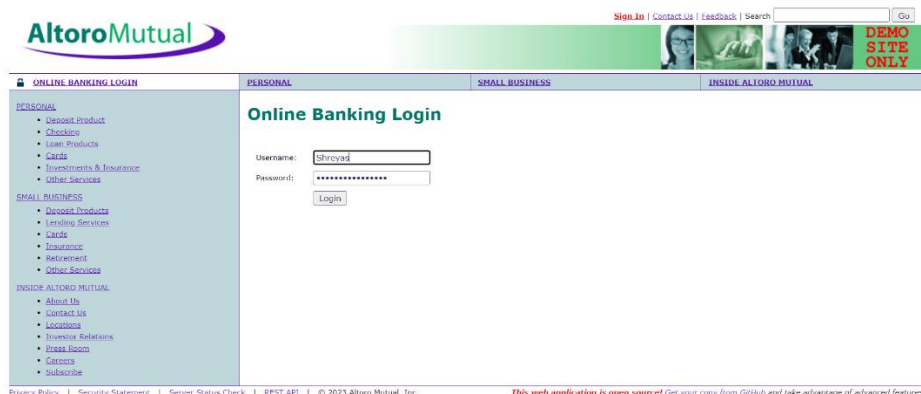
zsh: suspended sudo netdiscover -c 192.168.11.128

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

(kali@kali)-[~]
└─$
```

8.CryptoConfiguration Flaw:

CryptoConfiguration typically refers to the configuration of cryptographic protocols and algorithms used to protect sensitive data and communications. A flaw in context could refer to a weakness or vulnerability in the configuration 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 http://www.vulnweb.com/
```

```
(kali@kali)~$ nikto -host http://www.vulnweb.com/
+ Nikto v2.1.6
+ Target IP: 44.228.249.3
+ Target Hostname: www.vulnweb.com
+ Target Port: 80
+ Start Time: 2023-03-06 01:08:15 (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 fashion to the MIME type
+ 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 01:10:32 (GMT-5) (137 seconds)
+ 1 host(s) tested
(kali@kali)~$ echo shreyas
shreyas
(kali@kali)~$
```

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.

