

Name:Ganesh Gowda

Reg No:145CS21702

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)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.11.130 netmask 255.255.255.0 broadcast 192.168.11.255
    inet6 fe80::7b85:501d:ae77:6c46 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:7c:60:ab txqueuelen 1000 (Ethernet)
    RX packets 204 bytes 12804 (12.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 42 bytes 4672 (4.5 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)-[~]
$ sudo ifconfig eth0 192.168.11.15
[sudo] password for kali:

(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.11.15 netmask 255.255.255.0 broadcast 192.168.11.255
    inet6 fe80::7b85:501d:ae77:6c46 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:7c:60:ab txqueuelen 1000 (Ethernet)
    RX packets 204 bytes 12804 (12.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 42 bytes 4672 (4.5 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 ganesh
ganesh
```

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)-[~]
$ 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 192.168.11.130 netmask 255.255.255.0 broadcast 192.168.11.255
    inet6 fe80::7b85:501d:ae77:6c46 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:7c:60:ab txqueuelen 1000 (Ethernet)
    RX packets 236 bytes 14724 (14.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 46 bytes 4914 (4.7 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

(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: d2:6d:e2:e4:3f:0d (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 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 ganesh
ganesh
```

3.Any 5 whatweb commands:

Basic scanning:

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

\$ whatweb websiteURL

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

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

(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]

```
(kali@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, 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-aspnet-version.
    Info about headers can be found at www.http-stats.com

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

HTTP Headers:
    HTTP/1.1 301 Moved Permanently
    Connection: close
    content-type: text/html
    content-length: 707
    date: Mon, 06 Mar 2023 14:39:16 GMT
    server: LiteSpeed
    location: https://www.mitkundapura.com/
```

```
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: Mon, 06 Mar 2023 14:39:17 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"

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

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][en], HTML5, HTTPServer[LiteSpeed], IP[217.21.87.244], LiteSpeed, RedirectLocation[https://www.mitkundapura.com/], Title[301 Moved Permanently][title element contains newline(s)], UncommonHeaders[platform,content-security-policy]
https://www.mitkundapura.com/ [200 OK] Bootstrap, Country[UNITED KINGDOM][en], Email[office@mitkundapura.com], HTML5, HTTPServer[LiteSpeed], IP[217.21.87.244], JQuery, LiteSpeed, PHP[7.4.33], PowerBy[Kedige], Script, Title[MITK- Moodlakarta Institute of Technology & Management, Kundapura Home], UncommonHeaders[platform,content-security-policy,alt-svc], X-Powered-By[PHP/7.4.33]

(kali@kali)~$ echo ganesh
ganesh
```

\$ 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][en], HTML5, HTTPServer[LiteSpeed], IP[217.21.87.244], LiteSpeed, RedirectLocation[https://www.mitkundapura.com/], Title[301 Moved Permanently][title element contains newline(s)], UncommonHeaders[platform,content-security-policy]
https://www.mitkundapura.com/ [200 OK] Bootstrap, Country[UNITED KINGDOM][en], Email[office@mitkundapura.com], HTML5, HTTPServer[LiteSpeed], IP[217.21.87.244], JQuery, LiteSpeed, PHP[7.4.33], PowerBy[Kedige], Script, Title[MITK- Moodlakarta Institute of Technology & Management, Kundapura Home], UncommonHeaders[platform,content-security-policy,alt-svc], X-Powered-By[PHP/7.4.33]

(kali@kali)~$ echo ganesh
ganesh
```

\$ 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-aspnet-version. Info about headers can be found at www.http-stats.com

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

HTTP Headers:
    HTTP/1.1 301 Moved Permanently
    Connection: close
    content-type: text/html
    content-length: 707
    date: Mon, 06 Mar 2023 14:42:06 GMT
    server: LiteSpeed
    location: https://www.mitkundapura.com/
```

```
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: Mon, 06 Mar 2023 14:42:08 GMT
    server: LiteSpeed
    platform: hosting
    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-Q040="443"; ma=2592000, h3-Q037="443"; ma=2592000, h3-Q034="443"; ma=2592000, h3-Q031="443"; ma=2592000, h3-Q028="443"; ma=2592000, h3-Q025="443"; ma=2592000, h3-Q022="443"; ma=2592000, h3-Q019="443"; ma=2592000, h3-Q016="443"; ma=2592000, h3-Q013="443"; ma=2592000, h3-Q010="443"; ma=2592000, h3-Q007="443"; ma=2592000, h3-Q004="443"; ma=2592000, h3-Q001="443"; ma=2592000, h3="443"; ma=2592000

(kali@kali)~$ echo ganesh
ganesh
```

4.Any 5 nslookup commands:

\$ nslookup google.com

```
File Actions Edit View Help
(kali@kali)-[~]
$ nslookup google.com
Server:      192.168.78.2
Address:     192.168.78.2#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.205.238
Name:   google.com
Address: 2404:6800:4007:803::200e

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

\$ 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 example.com
Server:      192.168.78.2
Address:     192.168.78.2#53

Non-authoritative answer:
example.com  mail exchanger = 0 .

Authoritative answers can be found from:

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

(kali@kali)-[~]
$ nslookup -type=ns example.com
Server:      192.168.78.2
Address:     192.168.78.2#53
```

\$ 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”.

```
ganesh
(kali@kali)-[~]
$ nslookup -type=ns example.com
Server:      192.168.78.2
Address:     192.168.78.2#53

Non-authoritative answer:
example.com  nameserver = a.iana-servers.net.
example.com  nameserver = b.iana-servers.net.

Authoritative answers can be found from:

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

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

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


```
Home

(kali㉿kali)-[~]
└─$ nslookup -type=a www.example.com
Server:          192.168.78.2
Address:         192.168.78.2#53

Non-authoritative answer:
Name:   www.example.com
Address: 93.184.216.34

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

\$ 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.example.com
Server:          192.168.78.2
Address:         192.168.78.2#53

Non-authoritative answer:
Name:   www.example.com
Address: 2606:2800:220:1:248:1893:25c8:1946

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

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 google.com
Domain Name: GOOGLE.COM
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-09-09T15:29:04Z
Creation Date: 1997-09-15T04:00:00Z
Registry Expiry Date: 2020-09-14T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2088517500
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-03-06T14:43:13Z otc

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
by the following terms of use: you agree that you may 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 of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
```

```
If you wish to contact this domain's Registrant, Administrative, or Technical
contact, and such email address is not visible above, you may do so via our web
form, pursuant to ICANN's Temporary Specification. To verify that you are not a
robot, please enter your email address to receive a link to a page that
facilitates email communication with the relevant contact(s).

Web-based WHOIS:
https://domains.markmonitor.com/whois

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.

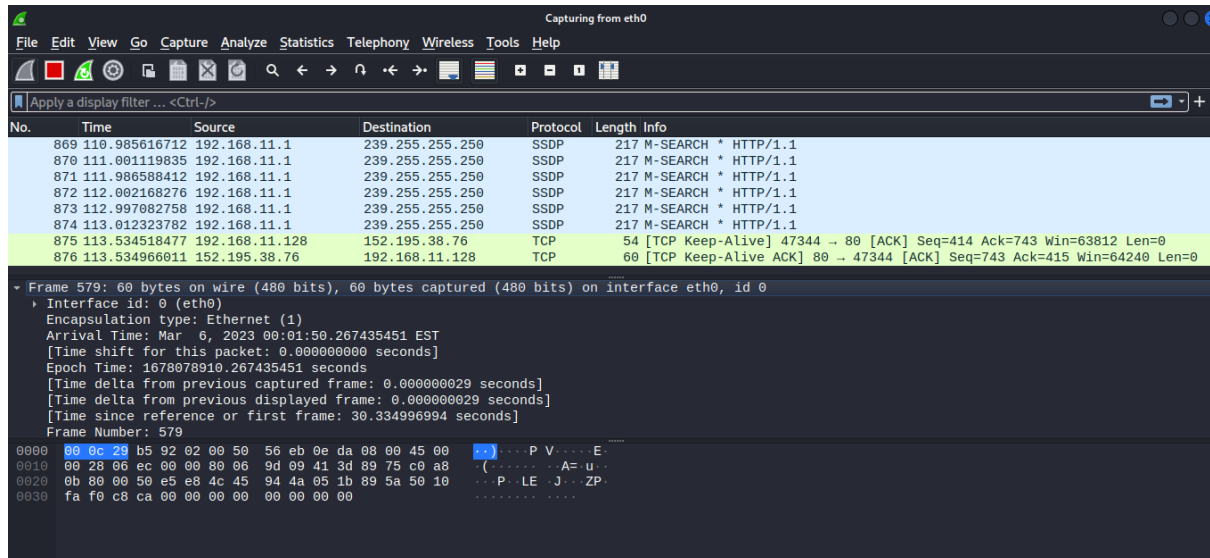
Visit MarkMonitor at https://www.markmonitor.com
Contact us at +1.800.745.9229
In Europe, at +44.02032062220
--

(kali@kali) ~$ echo ganesh
ganesh
```

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

```
File Actions Edit View Help
Currently scanning: 172.26.137.0/16 | Screen View: Unique Hosts
59 Captured ARP Req/Rep packets, from 3 hosts. Total size: 3540

IP          At MAC Address    Count  Len  MAC Vendor / Hostname
-----
192.168.78.2 00:50:56:f9:7c:e4  7      420  VMware, Inc.
192.168.78.1 00:50:56:c0:00:08  50     3000  VMware, Inc.
192.168.78.254 00:50:56:e6:e5:28  2      120  VMware, Inc.

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

\$ netdiscover -p

```
Currently scanning: Finished! | Screen View: Unique Hosts
18 Captured ARP Req/Rep packets, from 3 hosts. Total size: 1080

IP          At MAC Address    Count  Len  MAC Vendor / Hostname
-----
192.168.78.2 00:50:56:f9:7c:e4  3      180  VMware, Inc.
192.168.78.1 00:50:56:c0:00:08  14     840  VMware, Inc.
192.168.78.254 00:50:56:e6:e5:28  1      60   VMware, Inc.

zsh: suspended sudo netdiscover -r 192.168.78.128
(kali@kali)-[~]
$ echo ganesh
ganesh
(kali@kali)-[~]
$
```

\$ netdiscover -r 192.168.0.15

```
File Actions Edit View Help
Currently scanning: 192.168.2.0/16 | Screen View: Unique Hosts
14 Captured ARP Req/Rep packets, from 2 hosts. Total size: 840

IP          At MAC Address    Count  Len  MAC Vendor / Hostname
-----
192.168.78.1 00:50:56:c0:00:08  12     720  VMware, Inc.
192.168.78.2 00:50:56:f9:7c:e4  2      120  VMware, Inc.

zsh: suspended sudo netdiscover -s 192.168.78.128
(kali@kali)-[~]
$ echo ganesh
ganesh
(kali@kali)-[~]
$
```

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

```
File Actions Edit View Help
Currently scanning: 192.168.0.0/16 | Screen View: Unique Hosts
16 Captured ARP Req/Rep packets, from 1 hosts. Total size: 960

  IP            At MAC Address    Count    Len  MAC Vendor / Hostname
  ---            -
192.168.78.1    00:50:56:c0:00:08    16      960  VMware, Inc.

zsh: suspended sudo netdiscover -c 192.168.78.128

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

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

```
File Actions Edit View Help
Currently scanning: 192.168.0.0/16 | Screen View: Unique Hosts
16 Captured ARP Req/Rep packets, from 1 hosts. Total size: 960

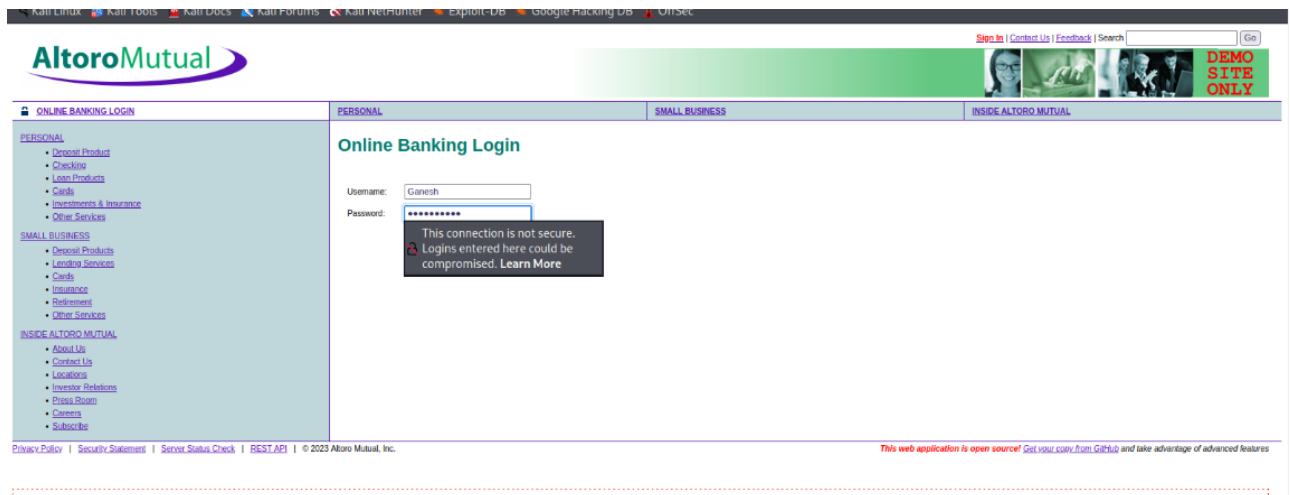
  IP            At MAC Address    Count    Len  MAC Vendor / Hostname
  ---            -
192.168.78.1    00:50:56:c0:00:08    16      960  VMware, Inc.

zsh: suspended sudo netdiscover -c 192.168.78.128

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

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:     2023-03-07 02:07:13 (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:       2023-03-07 02:09:07 (GMT-5) (114 seconds)

+ 1 host(s) tested

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

(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.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

https://www.kali.org:443/

Scan Information Results - List View: Dirs: 0 Files: 32 Results - Tree View Errors: 0

Type	Found	Response	Size
Dir	/	200	45595
Dir	/index/	200	392
Dir	/feed/	302	301
Dir	/downloads/	302	303
Dir	/category/	302	299
Dir	/download/	302	303
Dir	/contact/	200	392
Dir	/docs/	200	392
Dir	/newsletter/	200	392
Dir	/features/	200	392
Dir	/blog/	200	392
Dir	/community/	200	392
Dir	/tools/	200	392
Dir	/releases/	200	392
Dir	/author/	302	303
Dir	/get/	302	303
File	/sitemap.xml	200	464
Dir	/about-us/	200	392
File	/rss.xml	200	464
Dir	/get-kali/	200	392
Dir	/docs/community/	200	392
Dir	/404/	200	392
Dir	/docs/community/contribute/	200	392
Dir	/partnerships/	200	392
Dir	/docs/general-use/	200	392
Dir	/docs/general-use/metapackages/	200	392
Dir	/docs/development/	200	392
Dir	/docs/development/live-build-a-custom-kali-iso/	200	392
File	/tools	302	314
Dir	/tools/burpsuite/	200	392

Current speed: 587 requests/sec
Average speed: (T) 540, (C) 568 requests/sec
Parse Queue Size: 0
Total Requests: 20539/415346
Current number of running threads: 200
Time To Finish: 00:11:35
Back Pause Stop Xbox Report