

Name:Darshan S Kundar

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.

```
$ sudo ifconfig eth0 192.168.209.15
```

```
$ ifconfig
```

```
(kali㉿kali)-[~]
$ sudo ifconfig eth0 192.168.220.132
[sudo] password for kali:

(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 0x20<link>
    ether 00:0c:29:a7:fc:b0 txqueuelen 1000 (Ethernet)
    RX packets 79674 bytes 85764944 (81.7 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 531912 bytes 35385497 (33.7 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 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 24 bytes 1240 (1.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 24 bytes 1240 (1.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali㉿kali)-[~]
$ echo darshan kundar
darshan kundar
```

Size: 167 x 35

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.

```
$ sudo macchanger -s eth0
```

```
$ ifconfig
```

```
$ macchanger -r eth0
```

```
$ ifconfig eth0 down
```

```
(kali@kali)-[~]
$ sudo macchanger -s eth0
Current MAC: 00:0c:29:a7:fc:b0 (VMware, Inc.)
Permanent MAC: 00:0c:29:a7:fc:b0 (VMware, Inc.)

(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 0x20<link>
    ether 00:0c:29:a7:fc:b0 txqueuelen 1000 (Ethernet)
    RX packets 79965 bytes 85799374 (81.8 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 531917 bytes 35386067 (33.7 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 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 24 bytes 1240 (1.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 24 bytes 1240 (1.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$ sudo macchanger -r eth0
Current MAC: 00:0c:29:a7:fc:b0 (VMware, Inc.)
Permanent MAC: 00:0c:29:a7:fc:b0 (VMware, Inc.)
New MAC: ee:0e:42:37:74:2d (unknown)

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

```
(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 0x20<link>
    ether ee:0e:42:37:74:2d txqueuelen 1000 (Ethernet)
    RX packets 79965 bytes 85799374 (81.8 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 531920 bytes 35386247 (33.7 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 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 24 bytes 1240 (1.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 24 bytes 1240 (1.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$ echo darshan kumar
darshan kumar
```

3.Any 5 whatweb commands:

Basic scanning:

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

\$ whatweb [website URL]

```
(kali㉿kali)-[~]
└─$ whatweb 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/], Title[301 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], 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]

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

(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
```

```
[ 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 06:54:24 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 darshan kumar
darshan kumar

(kali@kali)-[~]
└─$
```

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

\$ whatweb -a 3 [website URL]

```
(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/], Title[301 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], 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]

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

(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/], Title[301 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], 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]

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

\$ whatweb --max-redirect 2 [website URL]

```
(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/], Title[301 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], 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]

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

(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/], Title[301 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], 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]

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

\$ whatweb -v -a 3 [website URL]

```
(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
```

```
[ 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 07:40:52 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 darshan kumar
darshan kumar
```


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 darshan kundan
darshan kundan
```

\$ nslookup -type=mx [website URL]

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 alt2.aspmx.l.google.com.
mitkundapura.com      mail exchanger = 5 alt1.aspmx.l.google.com.
mitkundapura.com      mail exchanger = 10 alt3.aspmx.l.google.com.
mitkundapura.com      mail exchanger = 1 aspmx.l.google.com.
mitkundapura.com      mail exchanger = 10 alt4.aspmx.l.google.com.

Authoritative answers can be found from:

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

\$ nslookup -type=ns [website URL]

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 = ns1.dns-parking.com.
mitkundapura.com      nameserver = ns2.dns-parking.com.

Authoritative answers can be found from:

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

\$ nslookup -type=a [website URL]

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

```
(kali㉿kali)-[~] | ip: //www.mitkundapura.com
└─$ 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)-[~] | ip: //www.mitkundapura.com
└─$ echo darshan kumar
darshan kumar
```

\$ nslookup -type=aaaa [website URL]

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

```
(kali㉿kali)-[~] | ip: //www.mitkundapura.com
└─$ 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)-[~] | ip: //www.mitkundapura.com
└─$ echo darshan kumar
darshan kumar
```

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 [website URL]

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
Country: UNITED STATES
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2010-09-09T15:30:04Z
Creation Date: 1997-09-15T04:00:00Z
Registry Expiry Date: 2028-09-14T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
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: 2023-03-03T09:00:27Z <<<
```

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

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.

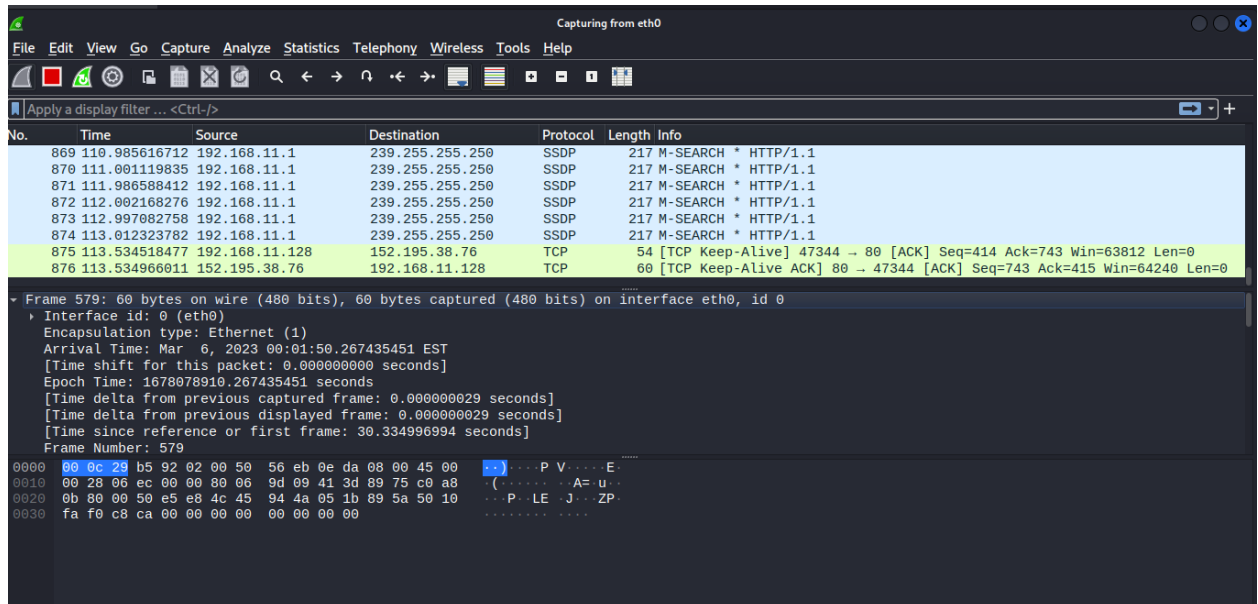
MarkMonitor Domain Management(TM)
Protecting companies and consumers in a digital world.

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

```
(kali@kali)-[~]
$ echo darshan kundar
darshan kundar
```


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: 192.168.24.0/16 | Screen View: Unique Hosts

8 Captured ARP Req/Rep packets, from 3 hosts. Total size: 480



| IP             | At MAC Address    | Count | Len | MAC Vendor / Hostname |
|----------------|-------------------|-------|-----|-----------------------|
| 192.168.11.1   | 00:50:56:c0:00:08 | 6     | 360 | 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 -i eth0

(kali㉿kali)-[~]
$ echo darshan kumar
darshan kumar
```

\$ netdiscover -r 192.168.11.128

```
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 |
|----------------|-------------------|-------|-----|-----------------------|
| 192.168.11.1   | 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 -r 192.168.11.128

(kali㉿kali)-[~]
$ echo darshan kumar
darshan kumar
```

\$ netdiscover -p

```
File Actions Edit View Help
Currently scanning: (passive) | Screen View: Unique Hosts

13 Captured ARP Req/Rep packets, from 1 hosts. Total size: 780



| IP           | At MAC Address    | Count | Len | MAC Vendor / Hostname |
|--------------|-------------------|-------|-----|-----------------------|
| 192.168.11.1 | 00:50:56:c0:00:08 | 13    | 780 | VMware, Inc.          |



zsh: suspended sudo netdiscover -p

(kali㉿kali)-[~]
$ echo darshan kumar
darshan kumar
```

```
$ netdiscover -c 192.168.11.128
```

```
File Actions Edit View Help
Currently scanning: 192.168.0.0/16 | Screen View: Unique Hosts

13 Captured ARP Req/Rep packets, from 1 hosts. Total size: 780

  IP            At MAC Address    Count    Len  MAC Vendor / Hostname
  ---            -
192.168.11.1    00:50:56:c0:00:08    13      780  VMware, Inc.

zsh: suspended sudo netdiscover -c 192.168.11.128

(kali㉿kali)-[~]
$ echo darshan kumar
darshan kumar
```

```
$ netdiscover -c 192.168.11.128
```

```
File Actions Edit View Help
Currently scanning: 192.168.0.0/16 | Screen View: Unique Hosts

13 Captured ARP Req/Rep packets, from 1 hosts. Total size: 780

  IP            At MAC Address    Count    Len  MAC Vendor / Hostname
  ---            -
192.168.11.1    00:50:56:c0:00:08    13      780  VMware, Inc.

zsh: suspended sudo netdiscover -c 192.168.11.128

(kali㉿kali)-[~]
$ echo darshan kumar
darshan kumar
```

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.

AltoroMutual

[Sign In](#) | [Contact Us](#) | [Feedback](#) | [Search](#)

DEMO SITE ONLY

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

Online Banking Login

Username:

Password:

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](#)

[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*

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 kali.org
```

```
(kali㉿kali)-[~]
└─$ nikto -host kali.org
- Nikto v2.1.6

+ Target IP: 50.116.58.136
+ Target Hostname: kali.org
+ Target Port: 80
+ Start Time: 2023-03-06 01:03:16 (GMT-5)

+ Server: Apache
+ 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
+ Root page / redirects to: https://www.kali.org/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect (timeout): Transport endpoint is not connected
+ Scan terminated: 20 error(s) and 3 item(s) reported on remote host
+ End Time: 2023-03-06 01:07:58 (GMT-5) (282 seconds)

+ 1 host(s) tested

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


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.

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
Time To Finish: 00:11:35
Current number of running threads: 200
(Select and right click for more options)

Back Pause Stop Xbox Report