

**Name:SUDEEP**

**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
```

```
(root@kali)-[~]
# ifconfig eth0 192.168.209.15

(root@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::21a5:2ae6:26da:1f2a prefixlen 64 scopeid 0<20<link>
    ether 00:0c:29:21:18:cd txqueuelen 1000 (Ethernet)
    RX packets 205439 bytes 154533565 (147.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 266734 bytes 21569396 (20.5 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 985 bytes 92097 (89.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 985 bytes 92097 (89.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@kali)-[~]
# echo sudeep
sudeep

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

## 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
```

```
$ ifconfig eth0 down
```

```
(root@kali)-[~]
# macchanger -s eth0
Current MAC: 00:0c:29:21:18:cd (VMware, Inc.)
Permanent MAC: 00:0c:29:21:18:cd (VMware, Inc.)

(root@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::21a5:2ae6:26da:1f2a prefixlen 64 scopeid 0<20<link>
    ether 00:0c:29:21:18:cd txqueuelen 1000 (Ethernet)
    RX packets 205694 bytes 154558761 (147.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 266734 bytes 21569396 (20.5 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 985 bytes 92097 (89.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 985 bytes 92097 (89.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@kali)-[~]
# macchanger -r eth0
Current MAC: 00:0c:29:21:18:cd (VMware, Inc.)
Permanent MAC: 00:0c:29:21:18:cd (VMware, Inc.)
New MAC: a2:0e:04:ce:a1:60 (unknown)

(root@kali)-[~]
# ifconfig eth0 down
```

```
(root@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 1033 bytes 95745 (93.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1033 bytes 95745 (93.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@kali)-[~]
# echo sudeep
sudeep

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

### 3. Any 5 whatweb commands:

#### Basic scanning:

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

\$ whatweb mitkundapura.com

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

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

(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 mitkundapura.com
WhatWeb report for http://mitkundapura.com
Status : 301 Moved Permanently
Title : 301 Moved Permanently
IP : 217.21.87.244
Country : UNITED KINGDOM, GB
Summary : HTML5, HTTPServer[LiteSpeed], LiteSpeed, RedirectLocation[https://mitkundapura.com/], UncommonHeaders[platform,content-security-policy]

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

[ HTTPServer ]
HTTP server header string. This plugin also attempts to identify the operating system from the server header.
String : LiteSpeed (from server string)

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

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

[ UncommonHeaders ]
```

```
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 06:36:16 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=":443"; ma=2592000; v="43,46"

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

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

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 -a 3 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 sudeep
sudeep

(kali@kali)-[~]
└─$
```

\$ 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 sudeep
sudeep
```

\$ 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.

String       : Apache-Coyote/1.1 (from server string)

[ HttpOnly ]

HTTP Headers:
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=73C16A250DC2A938AEDBB23B778875CD; Path=/; HttpOnly
Content-Type: text/html; charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Fri, 03 Mar 2023 09:05:06 GMT
Connection: close

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

#### 4. Any 5 nslookup commands:

\$ nslookup google.com

```
(kali@kali)-[~]
$ nslookup google.com
Server:      192.168.209.2
Address:     192.168.209.2#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.183.238
Name:   google.com
Address: 2404:6800:4007:823::200e

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

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

\$ nslookup -type=mx example.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:      192.168.209.2
Address:     192.168.209.2#53

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

Authoritative answers can be found from:
example.com nameserver = a.iana-servers.net.
example.com nameserver = b.iana-servers.net.

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

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

\$ nslookup -type=ns example.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 example.com
Server:      192.168.209.2
Address:     192.168.209.2#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 sudeep
sudeep

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

\$ nslookup -type=a www.example.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.example.com
Server:
  192.168.209.2
Address:
  192.168.209.2#53

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

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

(kali@kali)-[~]
└─$
```

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

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

```
(kali@kali)-[~]
└─$ nslookup -type=a www.example.com
Server:
  192.168.209.2
Address:
  192.168.209.2#53

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

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

(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: 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: 2023-03-03T05:15:07Z <<<

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
```

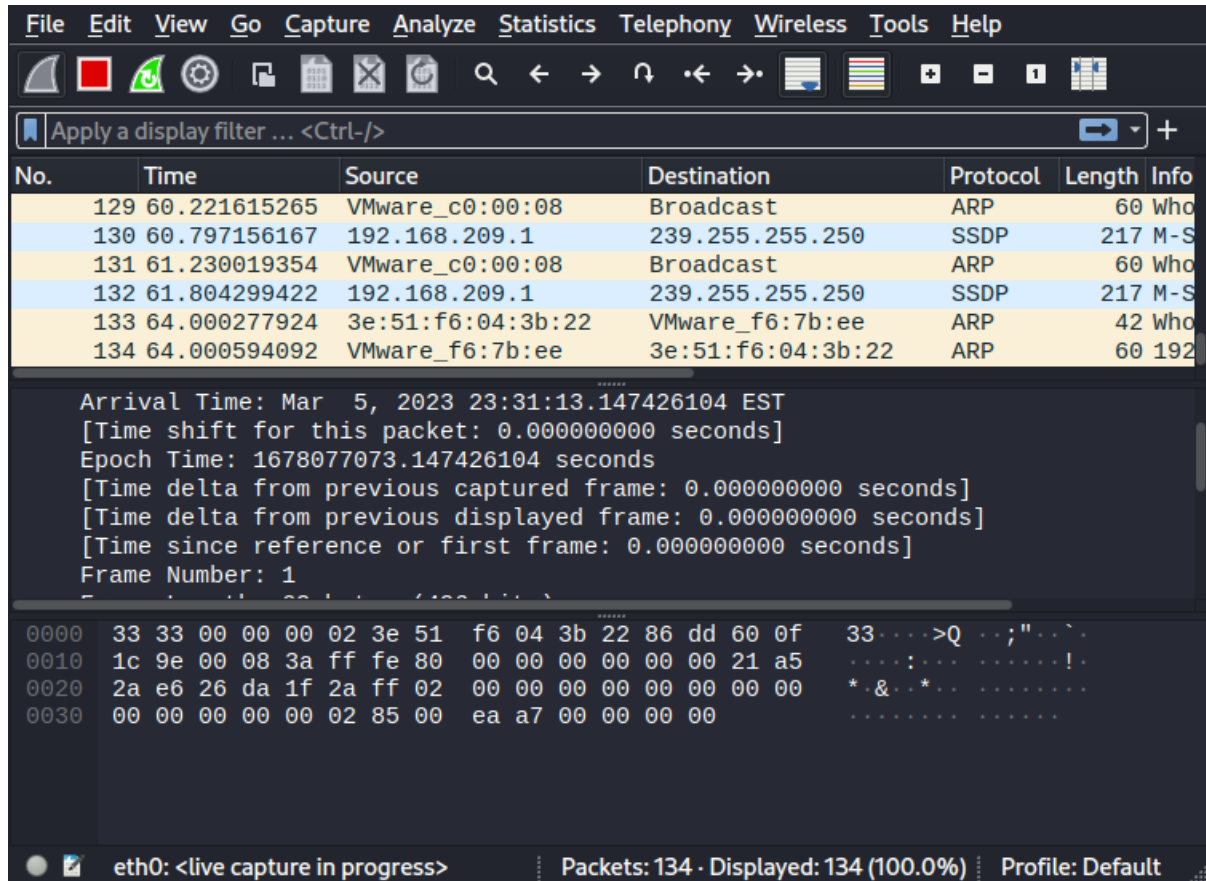
```
; a) allow, enable, or otherwise support the transmission by e-mail,
; telephone, or facsimile of mass, unsolicited, commercial advertising
; or solicitations to entities other than the data recipient's own
; existing customers; or
; b) enable high volume, automated, electronic processes that send 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 sudeep
sudeep

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

## 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

```
Currently scanning: 192.168.207.0/16 | Screen View: Unique Hosts
17 Captured ARP Req/Rep packets, from 4 hosts. Total size: 1020


| IP              | At                | MAC Address | Count | Len          | MAC Vendor / Hostname |
|-----------------|-------------------|-------------|-------|--------------|-----------------------|
| 192.168.209.1   | 00:50:56:c0:00:08 | 14          | 840   | VMware, Inc. |                       |
| 192.168.209.2   | 00:50:56:f6:7b:ee | 1           | 60    | VMware, Inc. |                       |
| 192.168.209.130 | 00:0c:29:22:29:cf | 1           | 60    | VMware, Inc. |                       |
| 192.168.209.254 | 00:50:56:f3:4d:9f | 1           | 60    | VMware, Inc. |                       |


zsh: suspended netdiscover -i eth0
(root@kali)~# echo sudeep
```

\$ netdiscover -p

```
Currently scanning: (passive) | Screen View: Unique Hosts
15 Captured ARP Req/Rep packets, from 3 hosts. Total size: 900


| IP              | At                | MAC Address | Count | Len          | MAC Vendor / Hostname |
|-----------------|-------------------|-------------|-------|--------------|-----------------------|
| 192.168.209.130 | 00:0c:29:22:29:cf | 1           | 60    | VMware, Inc. |                       |
| 192.168.209.254 | 00:50:56:f3:4d:9f | 1           | 60    | VMware, Inc. |                       |
| 192.168.209.1   | 00:50:56:c0:00:08 | 13          | 780   | VMware, Inc. |                       |


zsh: suspended netdiscover -p
(root@kali)~# echo sudeep
sudeep
(root@kali)~#
```

\$ netdiscover -r 192.168.0.15

```
Currently scanning: Finished! | Screen View: Unique Hosts
136 Captured ARP Req/Rep packets, from 4 hosts. Total size: 8160


| IP              | At                | MAC Address | Count | Len          | MAC Vendor / Hostname |
|-----------------|-------------------|-------------|-------|--------------|-----------------------|
| 192.168.209.1   | 00:50:56:c0:00:08 | 129         | 7740  | VMware, Inc. |                       |
| 192.168.209.2   | 00:50:56:f6:7b:ee | 1           | 60    | VMware, Inc. |                       |
| 192.168.209.130 | 00:0c:29:22:29:cf | 2           | 120   | VMware, Inc. |                       |
| 192.168.209.254 | 00:50:56:f3:4d:9f | 4           | 240   | VMware, Inc. |                       |


zsh: suspended netdiscover -r 192.168.0.15
(root@kali)~# echo sudeep
sudeep
(root@kali)~#
```

\$ netdiscover -i eth0 -f

```
Currently scanning: 172.31.42.0/16 | 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 |
|-----------------|-------------------|-------|-----|-----------------------|
| 192.168.209.1   | 00:50:56:c0:00:08 | 2     | 120 | VMware, Inc.          |
| 192.168.209.2   | 00:50:56:f6:7b:ee | 2     | 120 | VMware, Inc.          |
| 192.168.209.254 | 00:50:56:f3:4d:9f | 2     | 120 | VMware, Inc.          |


zsh: suspended netdiscover -i eth0 -f
(kali@kali)-[~]
└─$ echo sudeep
sudeep
(kali@kali)-[~]
└─$
```

\$ netdiscover -s 0.5

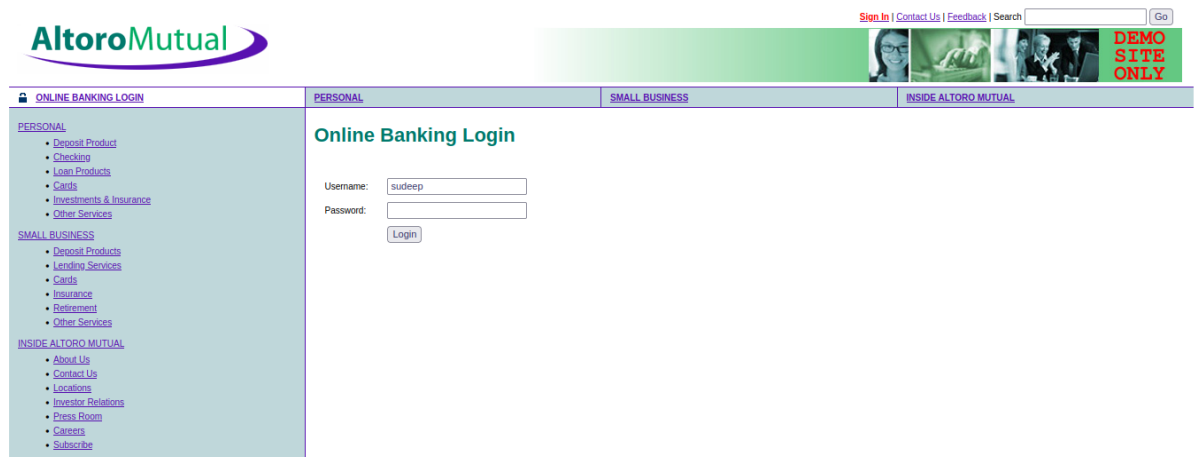
```
Currently scanning: 192.168.246.0/16 | Screen View: Unique Hosts
8 Captured ARP Req/Rep packets, from 4 hosts. Total size: 480


| IP              | At MAC Address    | Count | Len | MAC Vendor / Hostname |
|-----------------|-------------------|-------|-----|-----------------------|
| 192.168.209.1   | 00:50:56:c0:00:08 | 2     | 120 | VMware, Inc.          |
| 192.168.209.2   | 00:50:56:f6:7b:ee | 2     | 120 | VMware, Inc.          |
| 192.168.209.130 | 00:0c:29:22:29:cf | 2     | 120 | VMware, Inc.          |
| 192.168.209.254 | 00:50:56:f3:4d:9f | 2     | 120 | VMware, Inc.          |


zsh: suspended sudo netdiscover -s 0.5
(kali@kali)-[~]
└─$ echo sudeep
sudeep
(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.



**AltoroMutual**

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

**ONLINE BANKING LOGIN**

**PERSONAL** | **SMALL BUSINESS** | **INSIDE ALTORO MUTUAL**

**PERSONAL**

- [Deposit Products](#)
- [Checking](#)
- [Loan Products](#)
- [Cards](#)
- [Investments & Insurance](#)
- [Other Services](#)

**SMALL BUSINESS**

- [Deposit Products](#)
- [Lending Services](#)
- [Cards](#)
- [Insurance](#)
- [Retirement](#)
- [Other Services](#)

**INSIDE ALTORO MUTUAL**

- [About Us](#)
- [Contact Us](#)
- [Locations](#)
- [Investor Relations](#)
- [Press Room](#)
- [Careers](#)
- [Subscribe](#)

**Online Banking Login**

Username:

Password:

**DEMO SITE ONLY**

## 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: 2023-03-02 23:31:50 (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): Operation now in progress
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream
+ can't connect (timeout): Operation now in progress
+ Scan terminated: 21 error(s) and 3 item(s) reported on remote host
+ End Time: 2023-03-02 23:40:19 (GMT-5) (509 seconds)

+ 1 host(s) tested

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

(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.

