

Government Polytechnic

Udupi

Name: Rekha K

Register No.:145CS20014

Task Report: 2

1. Perform IP address spoofing:

IP address spoofing is a technique used to change the source IP address in an IP packet. IP spoofing can be used for malicious purpose, such as DDoS attacks or simply to make it more difficult to track down the source of problem.

Command: `ifconfig eth0 <ip address>`

```
(root@kali)-[/home/kali]
# ifconfig eth0 192.168.10.70

(root@kali)-[/home/kali]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.10.70 netmask 255.255.255.0 broadcast 192.168.10.255
    inet6 fe80::e53e:740c:5163:df26 prefixlen 64 scopeid 0x20<link>
    ether 42:5e:f9:3e:07:2f txqueuelen 1000 (Ethernet)
    RX packets 4516 bytes 1821842 (1.7 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2126 bytes 327830 (320.1 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

(root@kali)-[/home/kali]
# echo "rekha"
rekha
```

2.Perform MAC address spoofing:

MAC address spoofing is a technique for changing a factory assigned media Access Control address of a network interface on a networked device. MAC addresses are unique identifiers on networks, they only need to be, unique they can be changed on most network hardware.

Command: execute macchanger with an options -s and an argument eth0.

```
# macchanger -s eth0
```

- **Use ifconfig command to turn off your network interface**

```
# ifconfig eth0 down.
```

- **Change network cards hardware MAC address to some random hexadecimal numbers:**

```
# macchanger -r eth0
```

- **Network interface up and display your new MAC address:**

```
# ifconfig eth0 up
```

```
# macchanger -s eth0
```

```
(root@kali)-[/home/kali]
# macchanger -s eth0
Current MAC: e2:35:89:82:36:f3 (unknown)
Permanent MAC: 00:0c:29:d8:1c:23 (VMware, Inc.)

(root@kali)-[/home/kali]
# ifconfig eth0 down

(root@kali)-[/home/kali]
# macchanger -r eth0
Current MAC: e2:35:89:82:36:f3 (unknown)
Permanent MAC: 00:0c:29:d8:1c:23 (VMware, Inc.)
New MAC: 42:5e:f9:3e:07:2f (unknown)

(root@kali)-[/home/kali]
# ifconfig eth0 up

(root@kali)-[/home/kali]
# macchanger -s eth0
Current MAC: 42:5e:f9:3e:07:2f (unknown)
Permanent MAC: 00:0c:29:d8:1c:23 (VMware, Inc.)

(root@kali)-[/home/kali]
# echo "rekha"
rekha
```

3. Whatweb:

The Whatweb is used to identify different web technologies used by the website. It is included in Kali linux, and it can be accessed by going to applications, Web application analysis, Web vulnerability scanner. Whatweb also identifies version numbers, email address, account Id.

Command: whatweb <url>

```
# whatweb mitkundapura.com

# whatweb -v mitkundapura.com

# whatweb -a 3 mitkundapura.com

# whatweb --max-redirect 2 mitkundapura.com

# whatweb -v -a 3 mitkundapura.com
```

```
(root@kali)~/home/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]

(root@kali)~/home/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

(root@kali)~/home/kali
# whatweb -a 3 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]

(root@kali)~/home/kali
# whatweb --max-redirect 2 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]

(root@kali)~/home/kali
# whatweb -v -a 3 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.
```

```
[ 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 09:42:59 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"

(root@kali)-[/home/kali]
# echo "rekha"
rekha
```

4. nslookup:

Nslookup (Name Server Lookup) is a useful command for getting information from the DNS server. The nslookup command is a tool used to query Domain Name System (DNS) server and retrieve information about specific domain or IP address.

Command: nslookup followed by the domain name will display the IP Address of the domain.

```
# nslookup google.com
```

- **MX (Mail Exchange) record maps a domain name to a list of mail exchange servers for that domain.**
nslookup -type=mx google.com
- **NS (Name Server) record maps a domain name to a list of DNS servers authoritative for that domain.**
nslookup -type=ns google.com
- **SOA (Start of Authority) record provides the authoritative information about the domain, e-mail address of the domain admin, the domain serial number, etc...**
nslookup -type=soa google.com
- **To view information useful for debugging, use the debug option**
nslookup -debug google.com

```

(root@kali)-[/home/kali]
# nslookup google.com
Server:      192.168.19.2
Address:     192.168.19.2#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.183.238
Name:   google.com
Address: 2404:6800:4007:81e::200e

Authoritative answers can be found from:
smtp.google.com internet address = 74.125.24.27
smtp.google.com internet address = 74.125.24.26
smtp.google.com internet address = 142.250.4.27
smtp.google.com internet address = 142.250.4.26
smtp.google.com internet address = 142.251.10.27
smtp.google.com has AAAA address 2404:6800:4003:c03::1a
smtp.google.com has AAAA address 2404:6800:4003:c03::1b
smtp.google.com has AAAA address 2404:6800:4003:c06::1b
smtp.google.com has AAAA address 2404:6800:4003:c06::1a

(root@kali)-[/home/kali]
# nslookup -type=mx google.com
Server:      192.168.19.2
Address:     192.168.19.2#53

Non-authoritative answer:
google.com mail exchanger = 10 smtp.google.com.

Authoritative answers can be found from:
smtp.google.com internet address = 74.125.24.27
smtp.google.com internet address = 74.125.24.26
smtp.google.com internet address = 142.250.4.27
smtp.google.com internet address = 142.250.4.26
smtp.google.com internet address = 142.251.10.27
smtp.google.com has AAAA address 2404:6800:4003:c03::1a
smtp.google.com has AAAA address 2404:6800:4003:c03::1b
smtp.google.com has AAAA address 2404:6800:4003:c06::1b
smtp.google.com has AAAA address 2404:6800:4003:c06::1a

(root@kali)-[/home/kali]
# nslookup -type=ns google.com
Server:      192.168.19.2
Address:     192.168.19.2#53

Non-authoritative answer:
google.com nameserver = ns1.google.com.
google.com nameserver = ns4.google.com.
google.com nameserver = ns2.google.com.
google.com nameserver = ns3.google.com.

Authoritative answers can be found from:
ns1.google.com internet address = 216.239.32.10
ns1.google.com has AAAA address 2001:4860:4802:32::a
ns4.google.com internet address = 216.239.38.10
ns4.google.com has AAAA address 2001:4860:4802:38::a
ns2.google.com internet address = 216.239.34.10
ns2.google.com has AAAA address 2001:4860:4802:34::a
ns3.google.com internet address = 216.239.36.10
ns3.google.com has AAAA address 2001:4860:4802:36::a

(root@kali)-[/home/kali]
# nslookup -type=soa google.com
Server:      192.168.19.2
Address:     192.168.19.2#53

Non-authoritative answer:
google.com
origin = ns1.google.com
mail addr = dns-admin.google.com
serial = 513489231
refresh = 900

```



```
retry = 900
expire = 1800
minimum = 60
```

Authoritative answers can be found from:

```
google.com      nameserver = ns1.google.com.
google.com      nameserver = ns4.google.com.
google.com      nameserver = ns2.google.com.
google.com      nameserver = ns3.google.com.
ns4.google.com  internet address = 216.239.38.10
ns4.google.com  has AAAA address 2001:4860:4802:38::a
ns3.google.com  internet address = 216.239.36.10
ns3.google.com  has AAAA address 2001:4860:4802:36::a
ns1.google.com  internet address = 216.239.32.10
ns1.google.com  has AAAA address 2001:4860:4802:32::a
ns2.google.com  internet address = 216.239.34.10
ns2.google.com  has AAAA address 2001:4860:4802:34::a
```

```
(root@kali)-[/home/kali]
# nslookup -debug google.com
Server:      192.168.19.2
Address:     192.168.19.2#53
```

QUESTIONS:

```
google.com, type = A, class = IN
```

ANSWERS:

```
→ google.com
internet address = 142.250.183.238
```

```
ttl = 5
```

AUTHORITY RECORDS:

ADDITIONAL RECORDS:

Non-authoritative answer:

Name: google.com

Address: 142.250.183.238

QUESTIONS:

```
google.com, type = AAAA, class = IN
```

ANSWERS:

```
→ google.com
has AAAA address 2404:6800:4007:81e::200e
ttl = 5
```

AUTHORITY RECORDS:

ADDITIONAL RECORDS:

Name: google.com

Address: 2404:6800:4007:81e::200e

```
(root@kali)-[/home/kali]
# echo "rekha"
rekha
```

5.Whois:

Whois command searches a username directory and displays information about the user ID or nickname specified in the name parameter.

Syntax: whois <website name>

Command: # whois mitkundapura.com

```
(root@kali)-[/home/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: 2023-03-03T09:47:14Z <<<
```

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

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

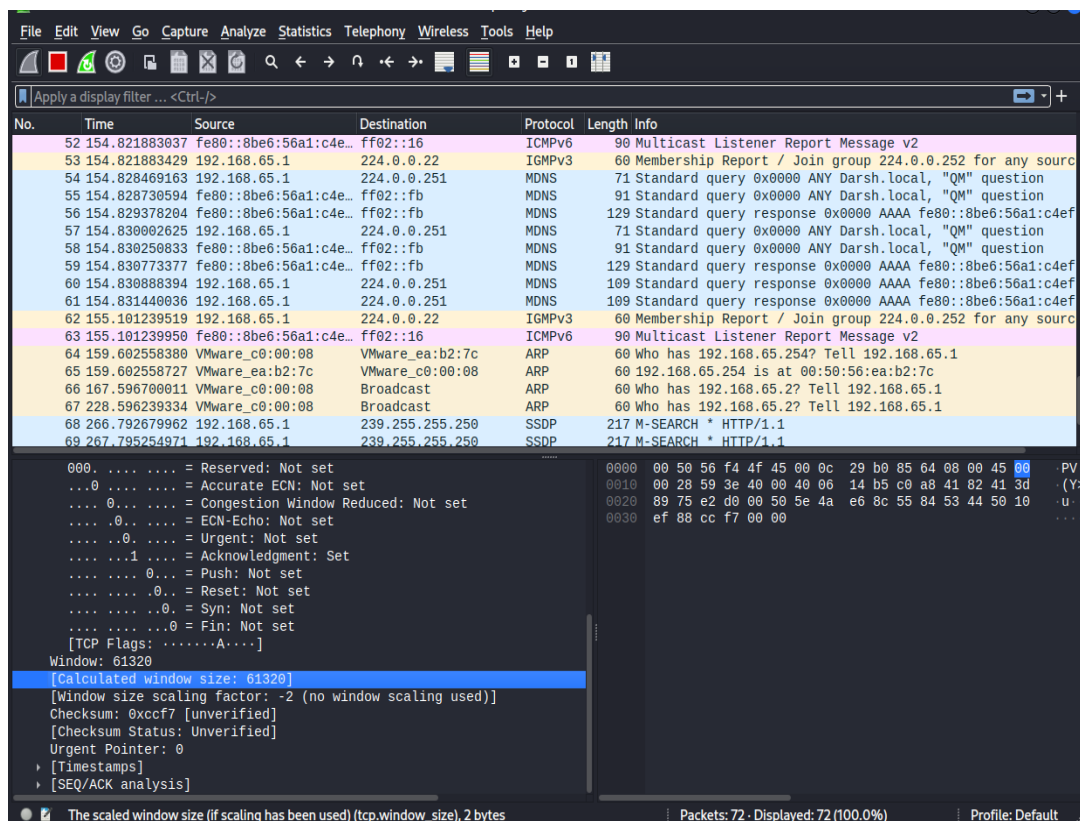
```

Add a prefix to target URLs.
--url-prefix          Add a prefix to target URLs.
--url-suffix          Add a suffix to target URLs.
--url-pattern          Insert the targets into a URL.
                        e.g. example.com/*insert*/robots.txt

(root@kali)-[/home/kali]
# echo "rekha"
rekha
```

6.Data packet using wireshark:

Wireshark is an open source packet analyser, which is used for education, analysis, software development, communication protocol development and network troubleshooting. Wireshark is a network protocol analyzer, or an application that captures packets from a network connection.



7.Netdiscover commands:

Netdiscover is a simple ARP scanner that can be used to scan for live hosts in a network. It can scan for multiple subnet also. It simply produces the output in a live display. This can be used in the first phases of a pentest where you have access to a network.

Command:

```
# netdiscover -h
```

- Use the following command to check the IP address:

```
# ifconfig
```

- We can scan a specific range with -r option:

```
# netdiscover -r 192.168.19.0/24
```



```
(root@kali)-[/home/kali]
# netdiscover -h
Netdiscover 0.9 [Active/passive ARP reconnaissance tool]
Written by: Jaime Penalba <jpenalba@gmail.com>

Usage: netdiscover [-i device] [-r range | -l file | -p] [-m file] [-F filter] [-s time] [-c count] [-n node] [-dfPLNS]
-i device: your network device
-r range: scan a given range instead of auto scan. 192.168.6.0/24,/16,/8
-l file: scan the list of ranges contained into the given file
-p passive mode: do not send anything, only sniff
-m file: scan a list of known MACs and host names
-F filter: customize pcap filter expression (default: "arp")
-s time: time to sleep between each ARP request (milliseconds)
-c count: number of times to send each ARP request (for nets with packet loss)
-n node: last source IP octet used for scanning (from 2 to 253)
-d ignore home config files for autoscan and fast mode
-f enable fastmode scan, saves a lot of time, recommended for auto
-P print results in a format suitable for parsing by another program and stop after active scan
-L similar to -P but continue listening after the active scan is completed
-N Do not print header. Only valid when -P or -L is enabled.
-S enable sleep time suppression between each request (hardcore mode)
```

If -r, -l or -p are not enabled, netdiscover will scan for common LAN addresses.

```
(root@kali)-[/home/kali]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.19.132 netmask 255.255.255.0 broadcast 192.168.19.255
    inet6 fe80::e53e:740c:5163:df26 prefixlen 64 scopeid 0x20<link>
    ether 42:5e:f9:3e:07:2f txqueuelen 1000 (Ethernet)
    RX packets 8493 bytes 3321127 (3.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4342 bytes 571067 (557.6 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
```

```
(root@kali)-[/home/kali]
# netdiscover 192.168.19.132
Invalid extra argument: 192.168.19.132

Netdiscover 0.9 [Active/passive ARP reconnaissance tool]
Written by: Jaime Penalba <jpenalba@gmail.com>

Usage: netdiscover [-i device] [-r range | -l file | -p] [-m file] [-F filter] [-s time] [-c count] [-n node] [-dfPLNS]
-i device: your network device
-r range: scan a given range instead of auto scan. 192.168.6.0/24,/16,/8
-l file: scan the list of ranges contained into the given file
-p passive mode: do not send anything, only sniff
-m file: scan a list of known MACs and host names
-F filter: customize pcap filter expression (default: "arp")
-s time: time to sleep between each ARP request (milliseconds)
-c count: number of times to send each ARP request (for nets with packet loss)
-n node: last source IP octet used for scanning (from 2 to 253)
-d ignore home config files for autoscan and fast mode
-f enable fastmode scan, saves a lot of time, recommended for auto
-P print results in a format suitable for parsing by another program and stop after active scan
-L similar to -P but continue listening after the active scan is completed
-N Do not print header. Only valid when -P or -L is enabled.
-S enable sleep time suppression between each request (hardcore mode)
```

Currently scanning: Finished! | Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180

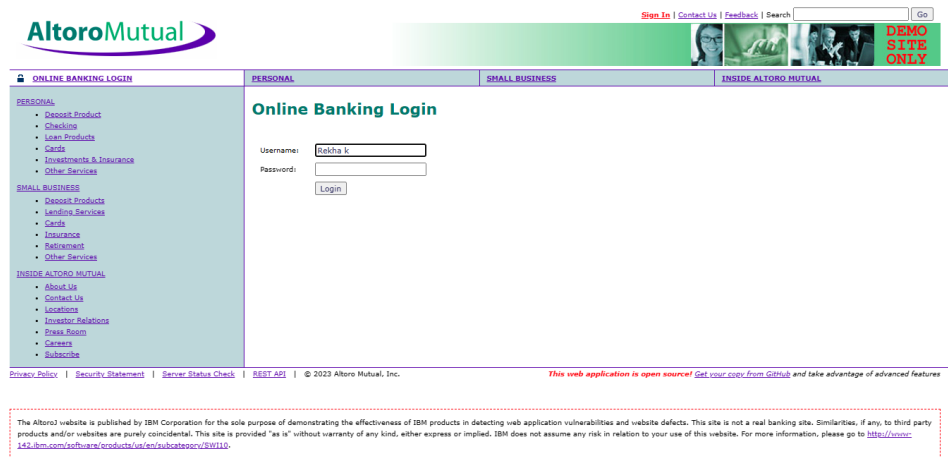
IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.19.1	00:50:56:c0:00:08	1	60	VMware, Inc.
192.168.19.2	00:50:56:e7:d9:92	1	60	VMware, Inc.
192.168.19.254	00:50:56:ec:93:e4	1	60	VMware, Inc.

zsh: suspended netdiscover -r 192.168.19.0/24

```
(root@kali)-[/home/kali]
# echo "rekha"
rekha
```

8. CryptoConfiguration flaw:

A Cryptographic failure is a critical web application security vulnerability that exposes sensitive application data on a weak or non-existence cryptographic algorithm.



9. Nikto:

Nikto is an open sources web server scanner which performs comprehensive tests against web servers for multiple items. Nikto can check for server configuration items such as the presence of multiple index files, HTTP server option, and will attempt to identify installed web server and software.

Syntax: nikto -h <website name>

Command: # nikto -h mitkundapura.com

```
(kali@kali)-[~]
$ nikto -h mitkundapura.com
- Nikto v2.1.6

+ Target IP: 217.21.87.244
+ Target Hostname: mitkundapura.com
+ Target Port: 80
+ Start Time: 2023-03-03 00:09:45 (GMT-5)

+ Server: LiteSpeed
+ 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
+ Uncommon header 'platform' found, with contents: hostingerr
+ 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://mitkundapura.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /images, inode: 999, size: 61cb51cf, mtime: 7630b837fa8dd3cc;;
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 5 item(s) reported on remote host
+ End Time: 2023-03-03 00:10:30 (GMT-5) (45 seconds)

+ 1 host(s) tested

(kali@kali)-[~]
$ echo "rekha"
rekha
```

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.

DirBuster is a tool created to discover, by brute force, the existing files and directories in a web server. We will use it in this recipe to search for a specific list of files and directories.

