

Name: KEERTHAN

REG NO :145CS20007

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
```

```
(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.78.220 netmask 255.255.255.0 broadcast 192.168.78.255
    inet6 fe80::fa0b:cbb5:d619:6126 prefixlen 64 scopeid 0<link>
    ether 00:0c:29:b2:ef:b0 txqueuelen 1000 (Ethernet)
    RX packets 5389 bytes 899808 (878.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 272625 bytes 16457897 (15.6 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<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 78 bytes 6087 (5.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 78 bytes 6087 (5.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali㉿kali)-[~]
└─$ sudo ifconfig eth0 192.168.78.120

(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
```

```
File Actions Edit View Help
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 78 bytes 6087 (5.9 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali㉿kali)-[~]
└─$ sudo ifconfig eth0 192.168.78.120

(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.78.120 netmask 255.255.255.0 broadcast 192.168.78.255
    inet6 fe80::fa0b:cbb5:d619:6126 prefixlen 64 scopeid 0<link>
    ether 00:0c:29:b2:ef:b0 txqueuelen 1000 (Ethernet)
    RX packets 5399 bytes 900408 (879.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 272625 bytes 16457897 (15.6 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<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 78 bytes 6087 (5.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 78 bytes 6087 (5.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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

(kali㉿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
```

```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.78.128 netmask 255.255.255.0 broadcast 192.168.78.255
    inet6 fe80::fa0b:cbb5:d619:6126 prefixlen 64 scopeid 0<20<link>
    ether 72:bf:44:fa:03:c5 txqueuelen 1000 (Ethernet)
    RX packets 5800 bytes 945540 (923.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 272819 bytes 16475868 (15.7 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 0<10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 78 bytes 6087 (5.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 78 bytes 6087 (5.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$ sudo macchanger -r eth0
Current MAC: 72:bf:44:fa:03:c5 (unknown)
Permanent MAC: 00:0c:29:b2:ef:b0 (VMware, Inc.)
New MAC: d2:cb:9d:77:bc:7e (unknown)

(kali@kali)-[~]
$ sudo macchanger -s eth0
Current MAC: d2:cb:9d:77:bc:7e (unknown)
Permanent MAC: 00:0c:29:b2:ef:b0 (VMware, Inc.)

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

3. Any 5 whatweb commands:

Basic scanning:

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

```
$ whatweb mitkundapura.com
```

```
(kali@kali)-[~]
$ sudo whatweb www.mitkundapura.com
http://www.mitkundapura.com [301 Moved Permanently] Country[UNITED KINGDOM][GB], HTML5, HTTPServer[LiteSpeed], IP[217.21.87.244], LiteSpeed, RedirectLocation[ww.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], 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 keerthan
keerthan
```

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)-[~]
└─$ sudo whatweb -v https://www.kali.org
WhatWeb report for https://www.kali.org
Status      : 200 OK
Title       : <None>
IP          : 104.18.4.159
Country     : UNITED STATES, US

Summary     : HTML5, HTTPServer[cloudflare], Open-Graph-Protocol, Script, UncommonHeaders[permissions-policy,cf-cache-status,cf-ray]

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      : cloudflare (from server string)

[ Open-Graph-Protocol ]
  The Open Graph protocol enables you to integrate your Web
  pages into the social graph. It is currently designed for
  Web pages representing profiles of real-world things .
  things like movies, sports teams, celebrities, and
  restaurants. Including Open Graph tags on your Web page,
  makes your page equivalent to a Facebook Page.

[ Script ]
  This plugin detects instances of script HTML elements and
  returns the script language/type.

[ UncommonHeaders ]
  Uncommon HTTP server headers. The blacklist includes all
```

```
[ Script ]
  This plugin detects instances of script HTML elements and
  returns the script language/type.

[ UncommonHeaders ]
  Uncommon HTTP server headers. The blacklist includes all
  the standard headers and many non standard but common ones.
  Interesting but fairly common headers should have their own
  plugins, eg. x-powered-by, server and x-aspnet-version.
  Info about headers can be found at www.http-stats.com

  String      : permissions-policy,cf-cache-status,cf-ray (from headers)

HTTP Headers:
  HTTP/1.1 200 OK
  Date: Mon, 06 Mar 2023 05:10:09 GMT
  Content-Type: text/html; charset=utf-8
  Transfer-Encoding: chunked
  Connection: close
  Cache-Control: max-age=600
  Expires: Mon, 06 Mar 2023 05:20:08 UTC
  Last-Modified: Mon, 06 Mar 2023 05:07:25 GMT
  Permissions-Policy: interest-cohort=()
  Vary: Origin
  CF-Cache-Status: DYNAMIC
  Server: cloudflare
  CF-RAY: 7a38172d19591bd8-BOM
  Content-Encoding: gzip

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

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

\$ whatweb -a 3 kali.org

```
(kali@kali)-[~]
$ whatweb -a 3 https://www.kali.org/
https://www.kali.org/ [200 OK] Country[UNITED STATES][US], HTML5, HTTPServer[cloudflare], IP[104.18.4.159], Open-Graph-Protocol, Script, UncommonHeaders[permissions-policy,cf-cache-status,cf-ray]

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

\$ whatweb --max-redirect 2 kali.org

```
(kali@kali)-[~]
$ whatweb --max-redirect 2 https://www.kali.org/
https://www.kali.org/ [200 OK] Country[UNITED STATES][US], HTML5, HTTPServer[cloudflare], IP[104.18.4.159], Open-Graph-Protocol, Script, UncommonHeaders[permissions-policy,cf-cache-status,cf-ray]

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

\$ whatweb -v -a 3 kali.org

```
(kali@kali)-[~]
$ whatweb -v -a 3 https://www.kali.org/
WhatWeb report for https://www.kali.org/
Status : 200 OK
Title : <None>
IP : 104.18.4.159
Country : UNITED STATES, US

Summary : HTML5, HTTPServer[cloudflare], Open-Graph-Protocol, Script, UncommonHeaders[permissions-policy,cf-cache-status,cf-ray]

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 : cloudflare (from server string)

[ Open-Graph-Protocol ]
    The Open Graph protocol enables you to integrate your Web pages into the social graph. It is currently designed for Web pages representing profiles of real-world things, things like movies, sports teams, celebrities, and restaurants. Including Open Graph tags on your Web page, makes your page equivalent to a Facebook Page.

[ Script ]
    This plugin detects instances of script HTML elements and returns the script language/type.
```

```
[ Script ]
This plugin detects instances of script HTML elements and
returns the script language/type.

[ UncommonHeaders ]
Uncommon HTTP server headers. The blacklist includes all
the standard headers and many non standard but common ones.
Interesting but fairly common headers should have their own
plugins, eg. x-powered-by, server and x-aspnet-version.
Info about headers can be found at www.http-stats.com

String      : permissions-policy,cf-cache-status,cf-ray (from headers)

HTTP Headers:
HTTP/1.1 200 OK
Date: Mon, 06 Mar 2023 05:32:56 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: close
Cache-Control: max-age=600
Expires: Mon, 06 Mar 2023 05:42:56 UTC
Last-Modified: Mon, 06 Mar 2023 05:07:25 GMT
Permissions-Policy: interest-cohort=()
Vary: Origin
CF-Cache-Status: DYNAMIC
Server: cloudflare
CF-RAY: 7a38388dcdf31a5-BOM
Content-Encoding: gzip

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

4. Any 5 nslookup commands:

\$ nslookup google.com

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

Non-authoritative answer:
Name:   google.com
Address: 142.250.193.110
Name:   google.com
Address: 2404:6800:4007:822::200e

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

\$ 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:      192.168.78.2
Address:     192.168.78.2#53

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

Authoritative answers can be found from:

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



```
$ 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:      192.168.78.2  
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:
```

```
$ 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:      192.168.78.2  
Address:     192.168.78.2#53  
  
Non-authoritative answer:  
Name:   www.example.com  
Address: 93.184.216.34  
  
(kali㉿kali)-[~]  
$ echo keerthan  
keerthan
```

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: 2023-03-06T05:44:16Z <<<

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
```

```
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: https://contact-form.registrar.eu/?domainName=mitkundapura.com&purpose=tech
Name Server: ns2.dns-parking.com
Name Server: ns1.dns-parking.com
DNSSEC: unsigned

URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2023-03-06T05:44:32Z <<<

: 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.

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

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: 172.26.66.0/16 | Screen View: Unique Hosts
49 Captured ARP Req/Rep packets, from 3 hosts. Total size: 2940
  IP            At MAC Address    Count  Len  MAC Vendor / Hostname
  ---            -
  192.168.78.1   00:50:56:c0:00:08   42     2520 VMware, Inc.
  192.168.78.2   00:50:56:f9:7c:e4    3      180 VMware, Inc.
  192.168.78.254 00:50:56:e6:e5:28    4      240 VMware, Inc.

zsh: suspended sudo netdiscover -i eth0

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

\$ netdiscover -p

```
Currently scanning: (passive) | 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
  ---            -
  192.168.78.1   00:50:56:c0:00:08   16     960 VMware, Inc.
  192.168.78.2   00:50:56:f9:7c:e4    1      60 VMware, Inc.
  192.168.78.254 00:50:56:e6:e5:28    1      60 VMware, Inc.

zsh: suspended sudo netdiscover -p

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

\$ netdiscover -r 192.168.0.15

```
Currently scanning: Finished! | Screen View: Unique Hosts
64 Captured ARP Req/Rep packets, from 3 hosts. Total size: 3840
  IP            At MAC Address    Count  Len  MAC Vendor / Hostname
  ---            -
  192.168.78.2   00:50:56:f9:7c:e4    6      360 VMware, Inc.
  192.168.78.1   00:50:56:c0:00:08   57     3420 VMware, Inc.
  192.168.78.254 00:50:56:e6:e5:28    1      60 VMware, Inc.

zsh: suspended sudo netdiscover -r 192.168.0.15

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

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

\$ netdiscover -i eth0 -f


```
Currently scanning: 172.17.211.0/16 | Screen View: Unique Hosts
9 Captured ARP Req/Rep packets, from 3 hosts. Total size: 540

  IP            At MAC Address    Count  Len  MAC Vendor / Hostname
  ---            -
  192.168.78.1   00:50:56:c0:00:08    7     420  VMware, Inc.
  192.168.78.2   00:50:56:f9:7c:e4    1      60  VMware, Inc.
  192.168.78.254 00:50:56:e6:e5:28    1      60  VMware, Inc.

zsh: suspended sudo netdiscover -i eth0 -f

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

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

\$ netdiscover -s 0.5

```
Currently scanning: 192.168.130.0/16 | Screen View: Unique Hosts
3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180

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

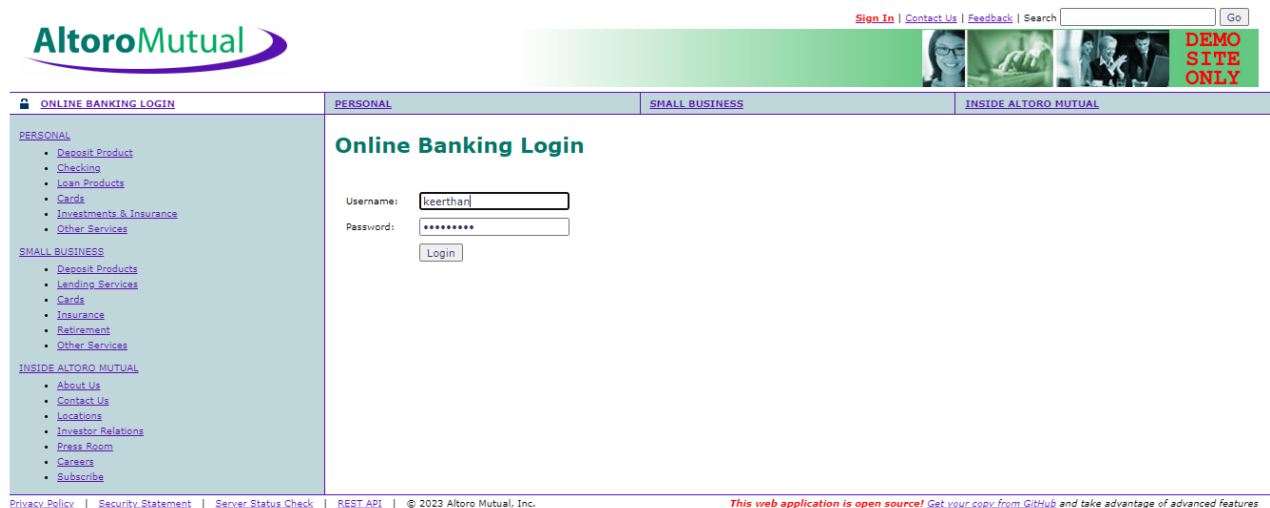
zsh: suspended sudo netdiscover -s 0,5

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

(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 is context could refers to a weakness or vulnarability in the configuration that could 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 kali.org

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

+ 0 host(s) tested

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

+ Target IP: 217.21.87.244
+ Target Hostname: www.mitkundapura.com
+ Target Port: 80
+ Start Time: 2023-03-06 01:19:40 (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: hostinger
+ 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.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: 7630b037fa8dd3ccc;;
+ 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: 2023-03-06 01:20:22 (GMT-5) (42 seconds)

+ 1 host(s) tested

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

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

