Name: Sanketh

REG NO : 145CS21704

Date:02-03-2023

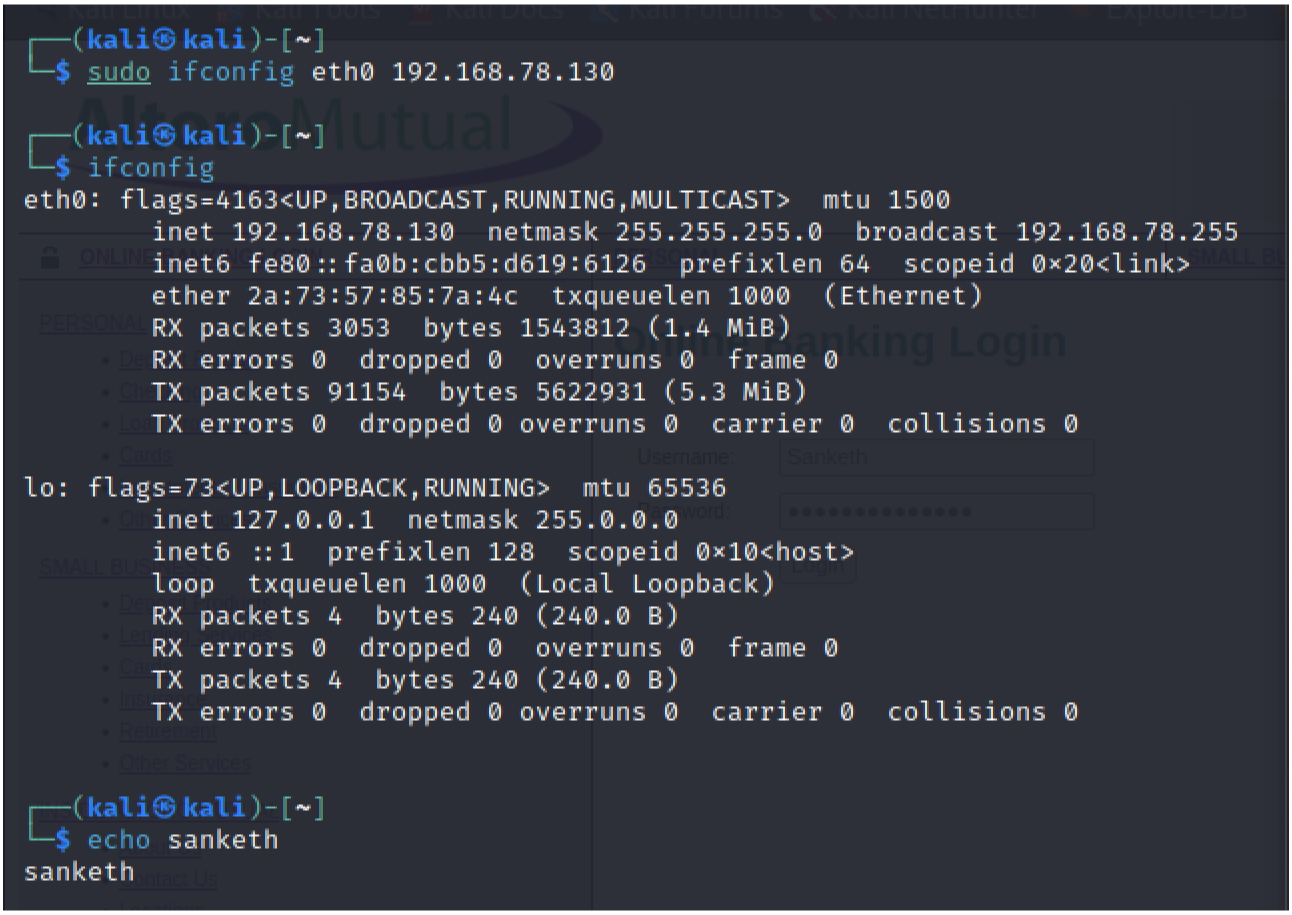
Task:2

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)-[~]
└─$ sudo ifconfig eth0 192.168.78.130

┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.78.130  netmask 255.255.255.0  broadcast 192.168.78.255
        inet6 fe80::fa0b:cbb5:d619:6126  prefixlen 64  scopeid 0×20<link>
        ether 2a:73:57:85:7a:4c  txqueuelen 1000  (Ethernet)
        RX packets 3053  bytes 1543812 (1.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 91154  bytes 5622931 (5.3 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 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 sanketh
sanketh
```

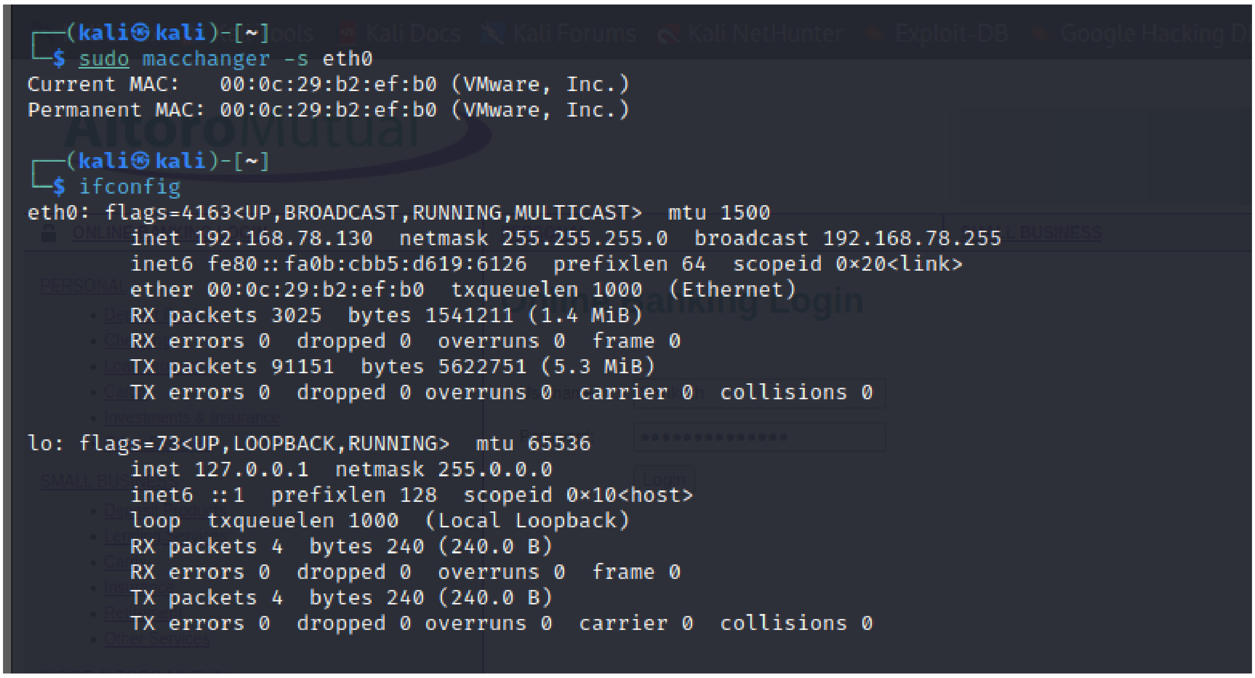
2.Perform MAC address spoofing:

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.

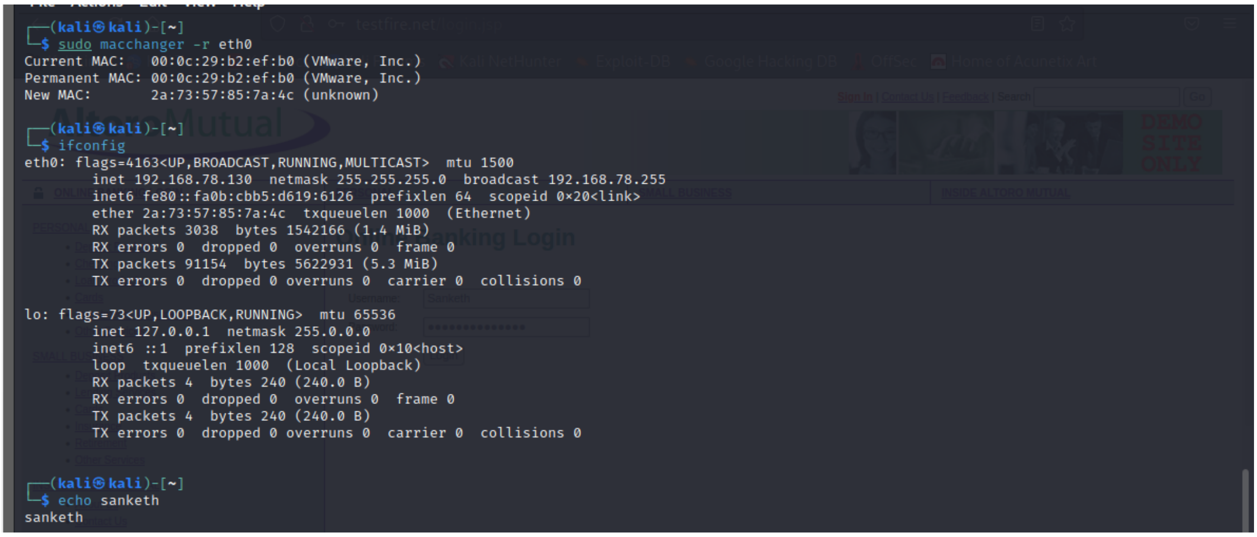
$ macchanger –s eth0

$ ifconfig

$ macchanger –r eth0



```
┌──(kali㉿kali)-[~]
└─$ sudo macchanger -s eth0
Current MAC:   00:0c:29:b2:ef:b0 (VMware, Inc.)
Permanent MAC: 00:0c:29:b2:ef:b0 (VMware, Inc.)

┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.78.130  netmask 255.255.255.0  broadcast 192.168.78.255
        inet6 fe80::fa0b:cbb5:d619:6126  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:b2:ef:b0  txqueuelen 1000  (Ethernet)
        RX packets 3025  bytes 1541211 (1.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 91151  bytes 5622751 (5.3 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 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
```



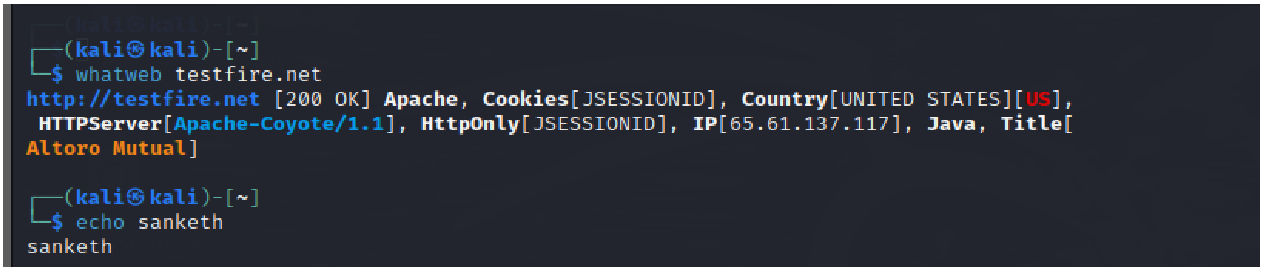
```
┌──(kali㉿kali)-[~]
└─$ sudo macchanger -r eth0
Current MAC:   00:0c:29:b2:ef:b0 (VMware, Inc.)
Permanent MAC: 00:0c:29:b2:ef:b0 (VMware, Inc.)
New MAC:       2a:73:57:85:7a:4c (unknown)

┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.78.130  netmask 255.255.255.0  broadcast 192.168.78.255
        inet6 fe80::fa0b:cbb5:d619:6126  prefixlen 64  scopeid 0×20<link>
        ether 2a:73:57:85:7a:4c  txqueuelen 1000  (Ethernet)
        RX packets 3038  bytes 1542166 (1.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 91154  bytes 5622931 (5.3 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 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 sanketh
sanketh
```

3.Any 5 whatweb commands:

Basic scanning:

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

$ whatweb testfire.net



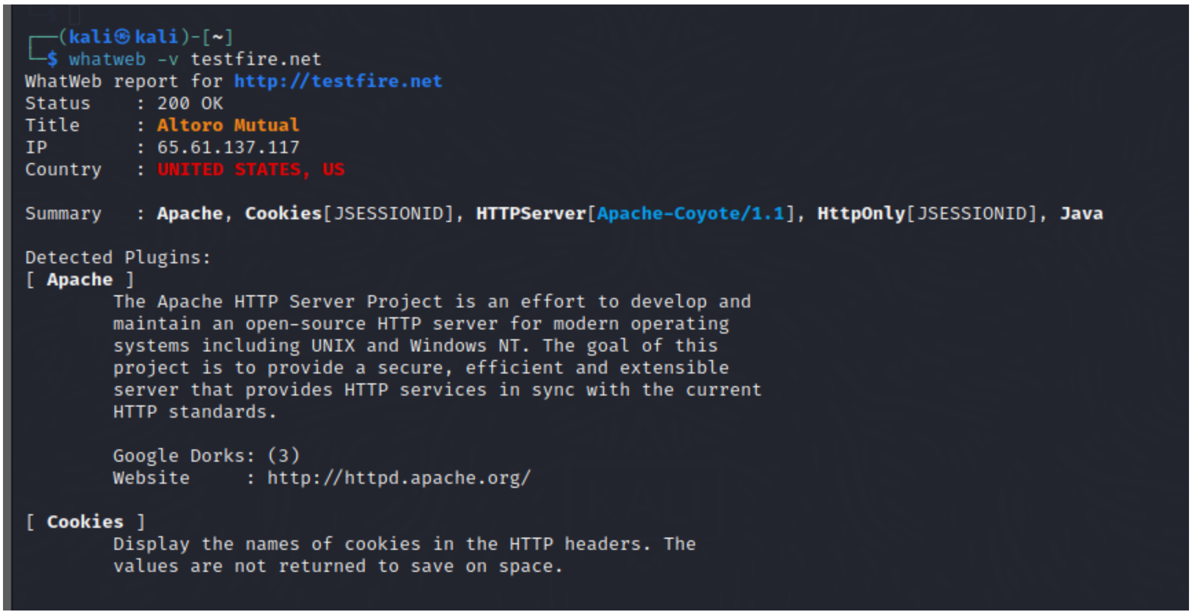
```
┌──(kali㉿kali)-[~]
└─$ whatweb testfire.net
http://testfire.net [200 OK] Apache, Cookies[JSESSIONID], Country[UNITED STATES][US],
 HTTPServer[Apache-Coyote/1.1], HttpOnly[JSESSIONID], IP[65.61.137.117], Java, Title[
Altoro Mutual]

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

This will perform a default scan of the website and display the identified technologies.

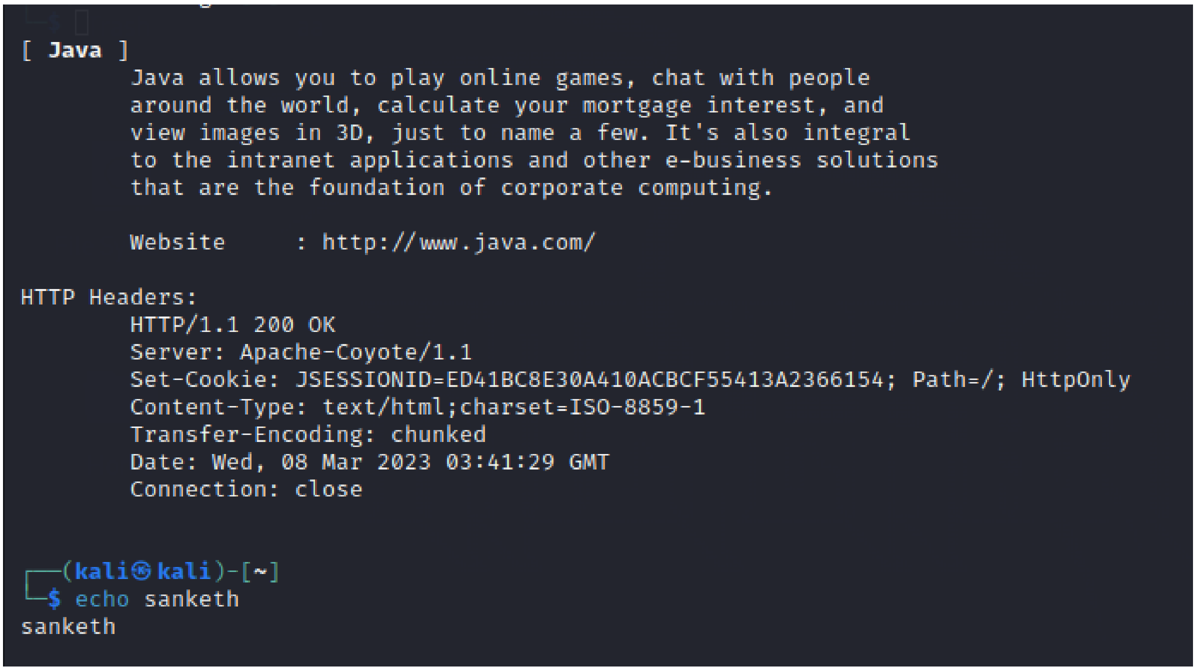
Verbose scanning:

If you want more detailed information about the website, you can use the verbose flag (-v):

$ whatweb -v [website URL]



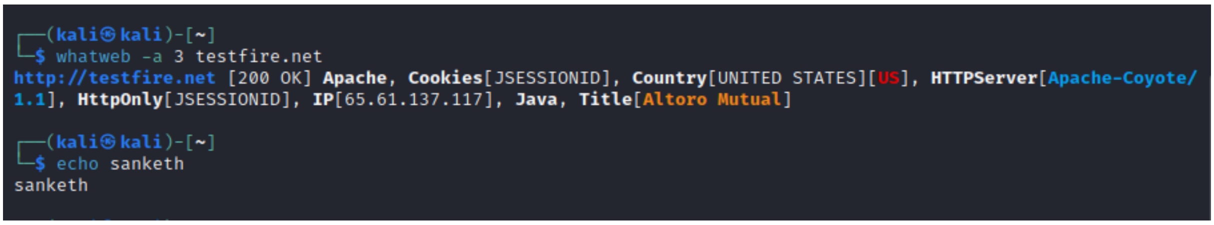
```
┌──(kali㉿kali)-[~]
└─$ whatweb -v testfire.net
WhatWeb report for http://testfire.net
Status    : 200 OK
Title     : Altoro Mutual
IP        : 65.61.137.117
Country   : UNITED STATES, US

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.
```



```
[ Java ]
        Java allows you to play online games, chat with people
        around the world, calculate your mortgage interest, and
        view images in 3D, just to name a few. It's also integral
        to the intranet applications and other e-business solutions
        that are the foundation of corporate computing.

        Website     : http://www.java.com/

HTTP Headers:
        HTTP/1.1 200 OK
        Server: Apache-Coyote/1.1
        Set-Cookie: JSESSIONID=ED41BC8E30A410ACBCF55413A2366154; Path=/; HttpOnly
        Content-Type: text/html;charset=ISO-8859-1
        Transfer-Encoding: chunked
        Date: Wed, 08 Mar 2023 03:41:29 GMT
        Connection: close


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

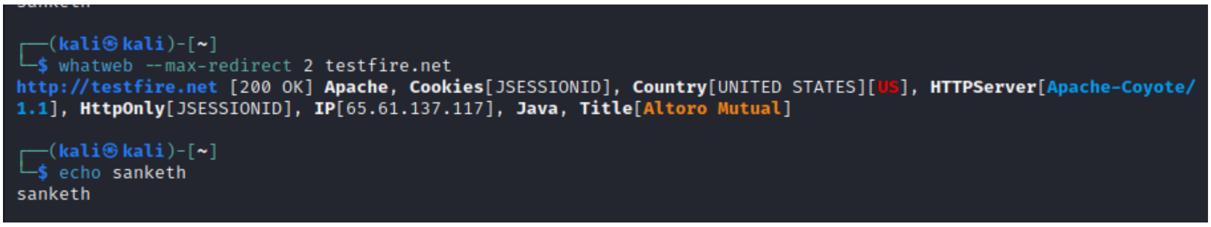
This will perform a more thorough scan and provide additional details, such as HTTP headers and server information.

$ whatweb –a 3 testfire.net



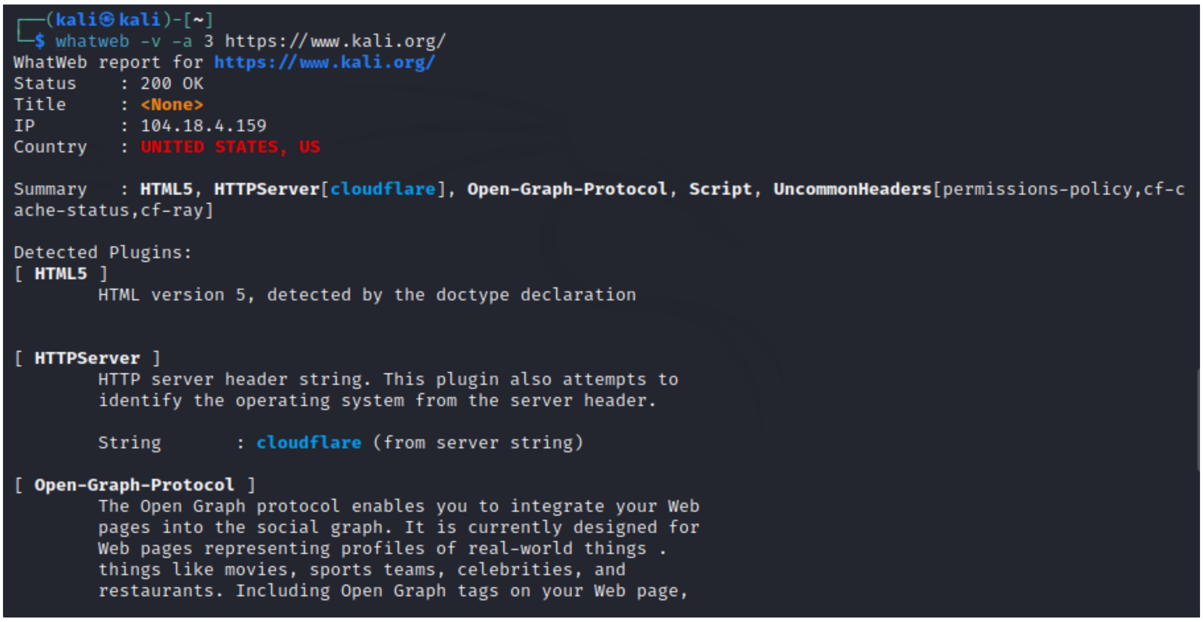
```
┌──(kali㉿kali)-[~]
└─$ whatweb -a 3 testfire.net
http://testfire.net [200 OK] Apache, Cookies[JSESSIONID], Country[UNITED STATES][US], HTTPServer[Apache-Coyote/
1.1], HttpOnly[JSESSIONID], IP[65.61.137.117], Java, Title[Altoro Mutual]

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

$ whatweb --max –redirect 2 testfire.net

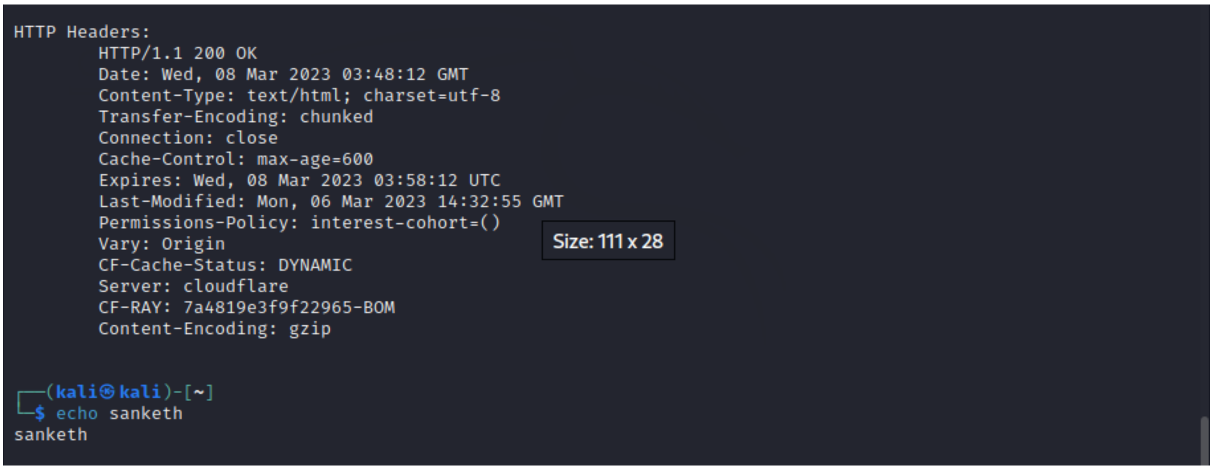


```
┌──(kali㉿kali)-[~]
└─$ whatweb --max-redirect 2 testfire.net
http://testfire.net [200 OK] Apache, Cookies[JSESSIONID], Country[UNITED STATES][US], HTTPServer[Apache-Coyote/
1.1], HttpOnly[JSESSIONID], IP[65.61.137.117], Java, Title[Altoro Mutual]

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

$ whatweb –v –a 3 testfire.net



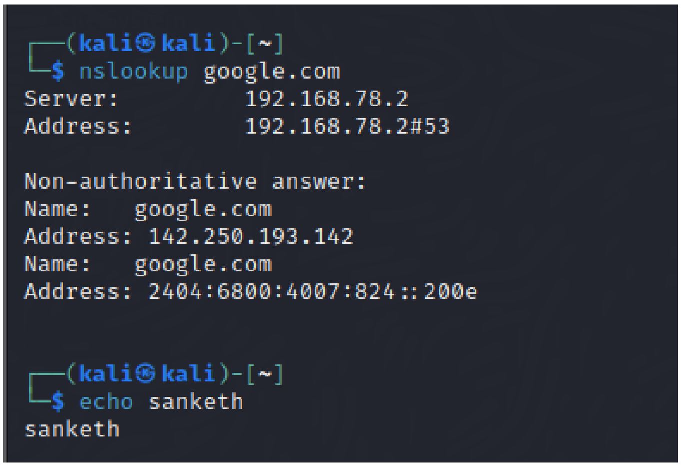
```
┌──(kali㉿kali)-[~]
└─$ whatweb -v -a 3 https://www.kali.org/
WhatWeb report for https://www.kali.org/
Status    : 200 OK
Title     : <None>
IP        : 104.18.4.159
Country   : UNITED STATES, US

Summary   : HTML5, HTTPServer[cloudflare], Open-Graph-Protocol, Script, UncommonHeaders[permissions-policy,cf-c
ache-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,
```



```
HTTP Headers:
        HTTP/1.1 200 OK
        Date: Wed, 08 Mar 2023 03:48:12 GMT
        Content-Type: text/html; charset=utf-8
        Transfer-Encoding: chunked
        Connection: close
        Cache-Control: max-age=600
        Expires: Wed, 08 Mar 2023 03:58:12 UTC
        Last-Modified: Mon, 06 Mar 2023 14:32:55 GMT
        Permissions-Policy: interest-cohort=()
        Vary: Origin
        CF-Cache-Status: DYNAMIC
        Server: cloudflare
        CF-RAY: 7a4819e3f9f22965-BOM
        Content-Encoding: gzip


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

4.Any 5 nslookup commands:

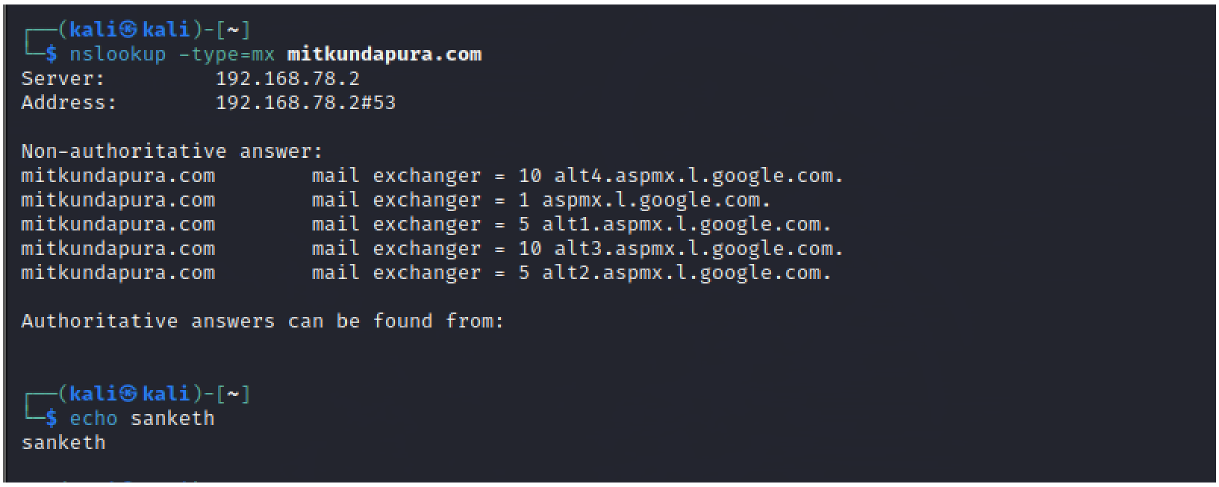
$ nslookup tesfire.net



```
┌──(kali㉿kali)-[~]
└─$ nslookup google.com
Server:         192.168.78.2
Address:        192.168.78.2#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.193.142
Name:   google.com
Address: 2404:6800:4007:824::200e


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

$ nslookup -type=mx testfire.net

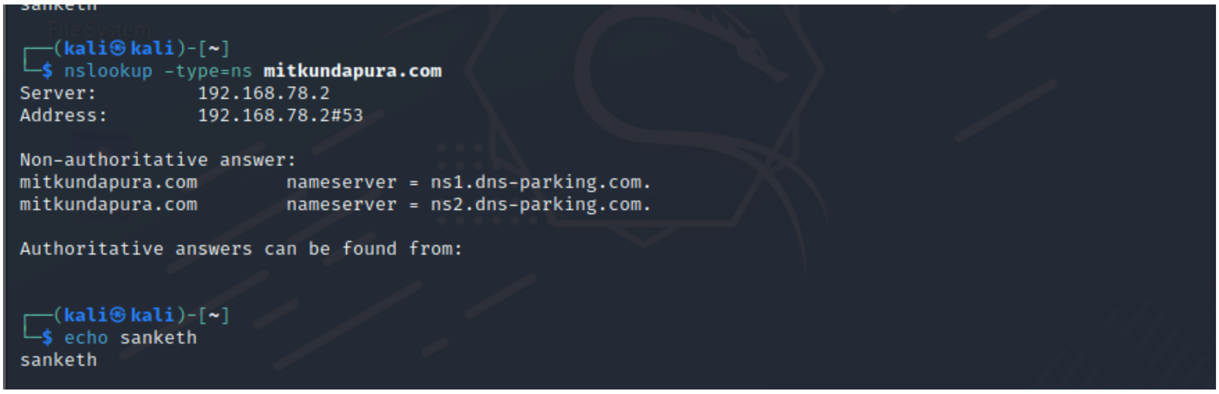
This command will perform a DNS lookup for the mail exchange (MX) records associated with the domain name “testfire.net”.



```
┌──(kali㉿kali)-[~]
└─$ nslookup -type=mx mitkundapura.com
Server:         192.168.78.2
Address:        192.168.78.2#53

Non-authoritative answer:
mitkundapura.com        mail exchanger = 10 alt4.aspmx.l.google.com.
mitkundapura.com        mail exchanger = 1 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 = 5 alt2.aspmx.l.google.com.

Authoritative answers can be found from:


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

$ nslookup -type=ns testfire.net

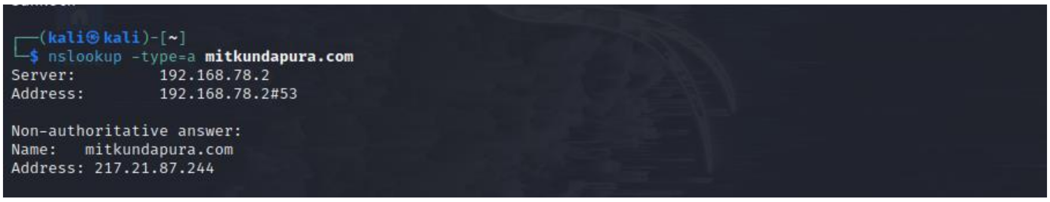
This command will perform a DNS lookup for the name server (NS) records associated with the domain name “testfire.net”.



```
┌──(kali㉿kali)-[~]
└─$ nslookup -type=ns mitkundapura.com
Server:         192.168.78.2
Address:        192.168.78.2#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 sanketh
sanketh
```

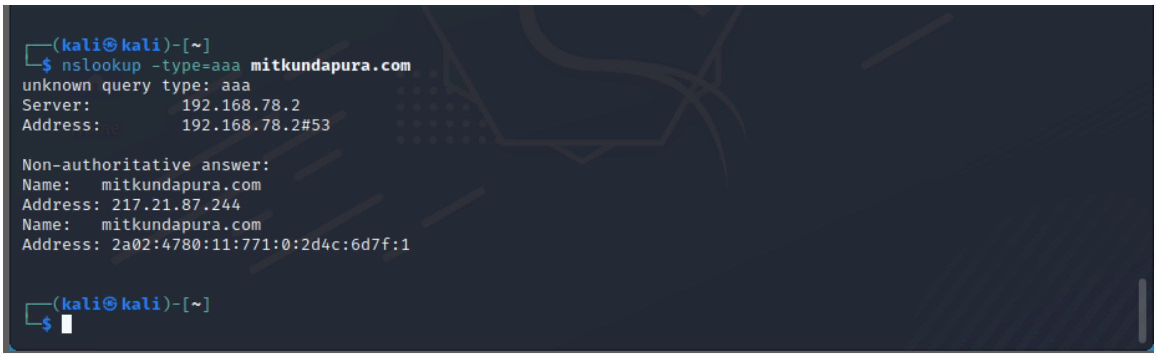
$ nslookup -type=a www.testfire.net

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



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

Non-authoritative answer:
Name:   mitkundapura.com
Address: 217.21.87.244
```

$ Nslookup –type=aaaa mitkundapura



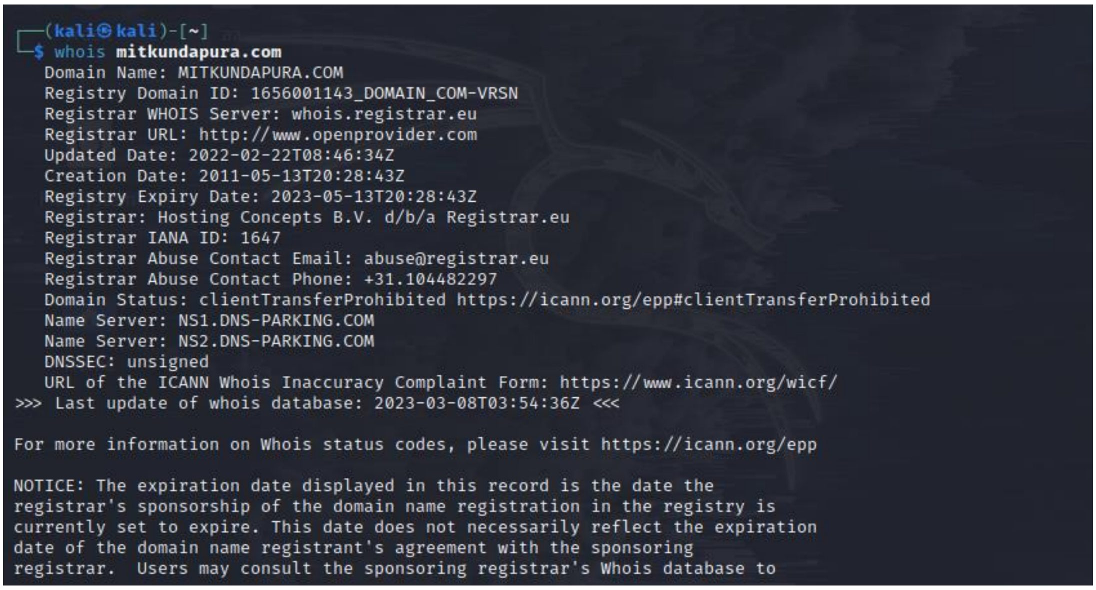
```
┌──(kali㉿kali)-[~]
└─$ nslookup -type=aaa mitkundapura.com
unknown query type: aaa
Server:         192.168.78.2
Address:        192.168.78.2#53

Non-authoritative answer:
Name:   mitkundapura.com
Address: 217.21.87.244
Name:   mitkundapura.com
Address: 2a02:4780:11:771:0:2d4c:6d7f:1


┌──(kali㉿kali)-[~]
└─$ █
```

5.whois Commands:

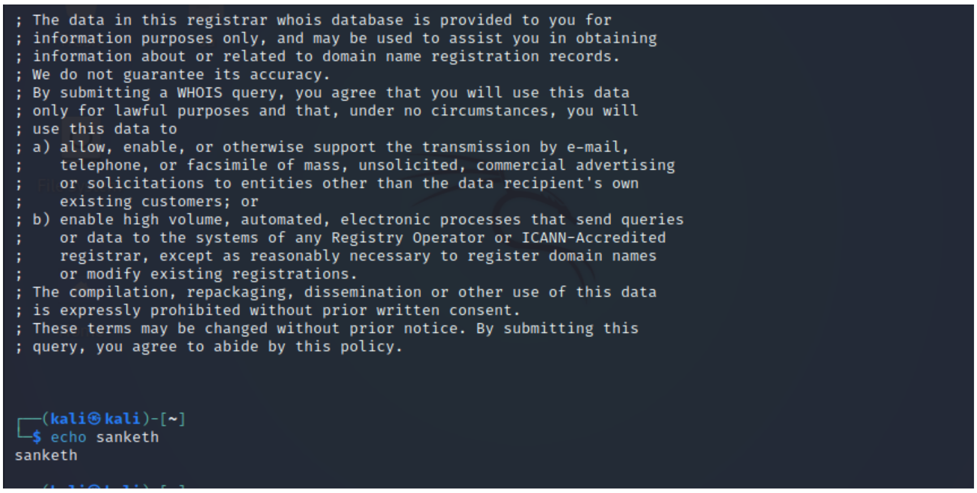
The whois command is a protocol used to look up information about domain names, IP addresses, and other network-related information. Here are some common WHOIS commands:

$ 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



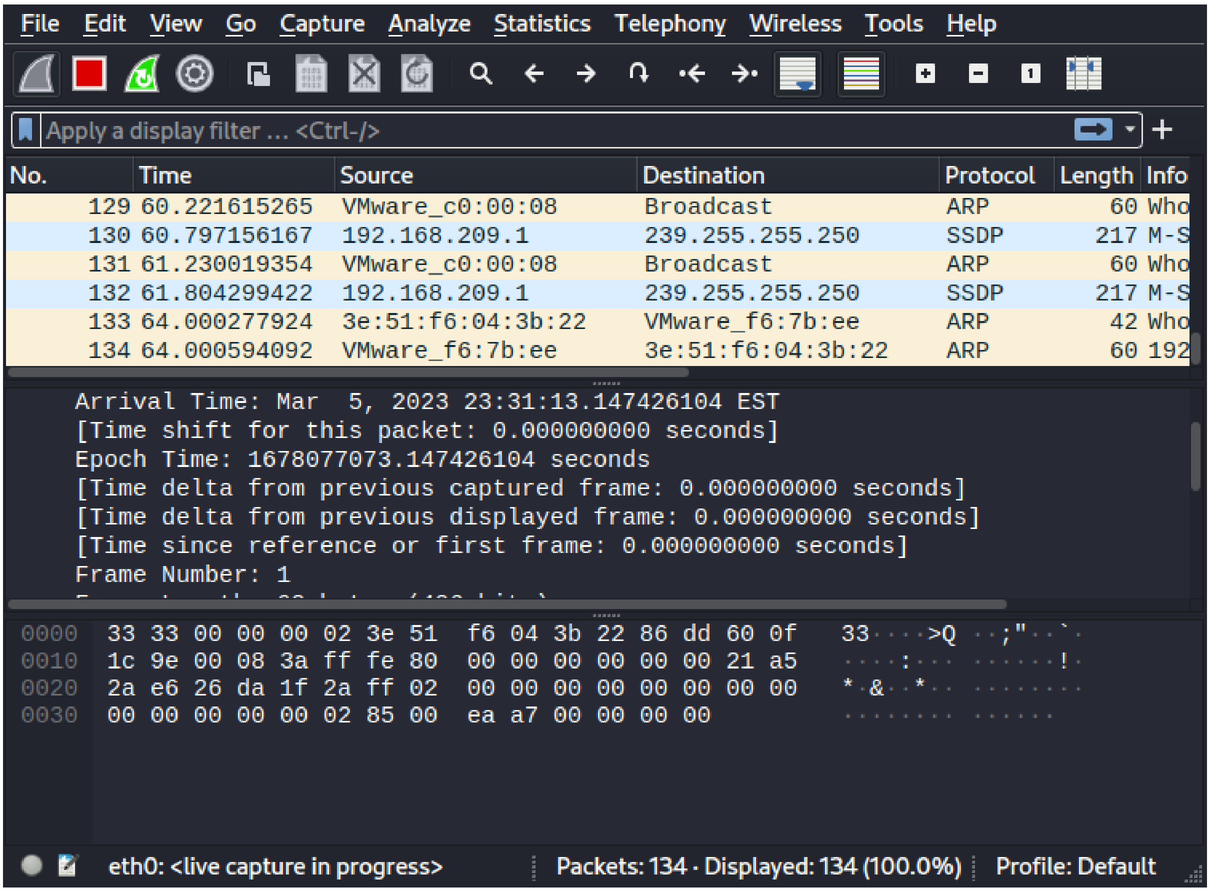
```
┌──(kali㉿kali)-[~]
└─$ whois mitkundapura.com
   Domain Name: MITKUNDAPURA.COM
   Registry Domain ID: 1656001143_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.registrar.eu
   Registrar URL: http://www.openprovider.com
   Updated Date: 2022-02-22T08:46:34Z
   Creation Date: 2011-05-13T20:28:43Z
   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: 2023-03-08T03:54:36Z <<<

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
```



```
; 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 sanketh
sanketh
```

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".


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.        Time           Source              Destination         Protocol  Length Info
       129 60.221615265   VMware_c0:00:08     Broadcast           ARP           60 Who
       130 60.797156167   192.168.209.1       239.255.255.250     SSDP         217 M-S
       131 61.230019354   VMware_c0:00:08     Broadcast           ARP           60 Who
       132 61.804299422   192.168.209.1       239.255.255.250     SSDP         217 M-S
       133 64.000277924   3e:51:f6:04:3b:22   VMware_f6:7b:ee     ARP           42 Who
       134 64.000594092   VMware_f6:7b:ee     3e:51:f6:04:3b:22   ARP           60 192
```

```
    Arrival Time: Mar  5, 2023 23:31:13.147426104 EST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1678077073.147426104 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
```

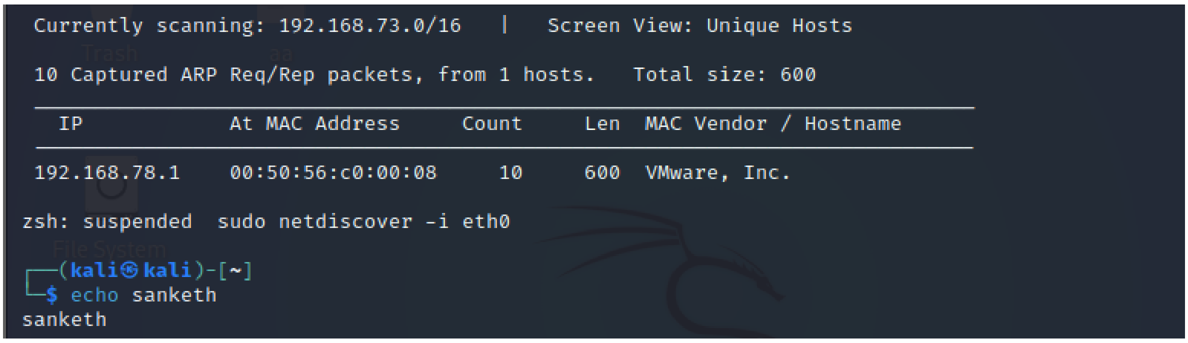
```
0000  33 33 00 00 00 02 3e 51  f6 04 3b 22 86 dd 60 0f   33····>Q ··;"··`·
0010  1c 9e 00 08 3a ff fe 80  00 00 00 00 00 00 21 a5   ····:··· ······!·
0020  2a e6 26 da 1f 2a ff 02  00 00 00 00 00 00 00 00   *·&··*·· ········
0030  00 00 00 00 00 02 85 00  ea a7 00 00 00 00         ········ ······
```

eth0: <live capture in progress> Packets: 134 · Displayed: 134 (100.0%) Profile: Default

7.Any 5 netdiscover command:

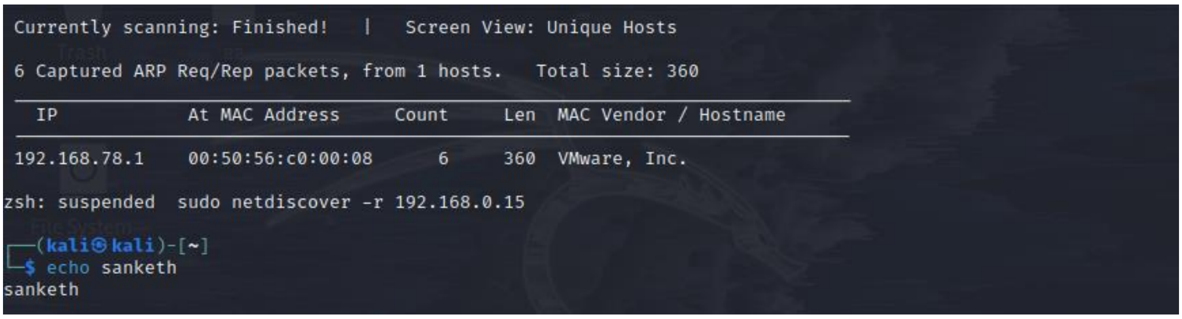
Netdiscover is a network scanning tool used for discovering hosts and gathering information about them on a local network. Here are some of the basic commands:

$ netdiscover -i eth0



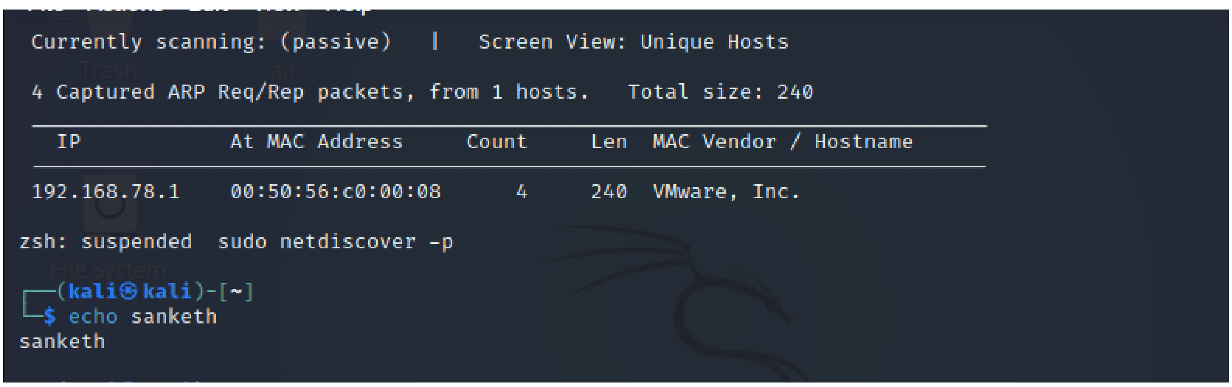
```
 Currently scanning: 192.168.73.0/16   |   Screen View: Unique Hosts

 10 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 600
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.78.1    00:50:56:c0:00:08     10      600  VMware, Inc.

zsh: suspended  sudo netdiscover -i eth0

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

$ netdiscover -r 192.168.0.15



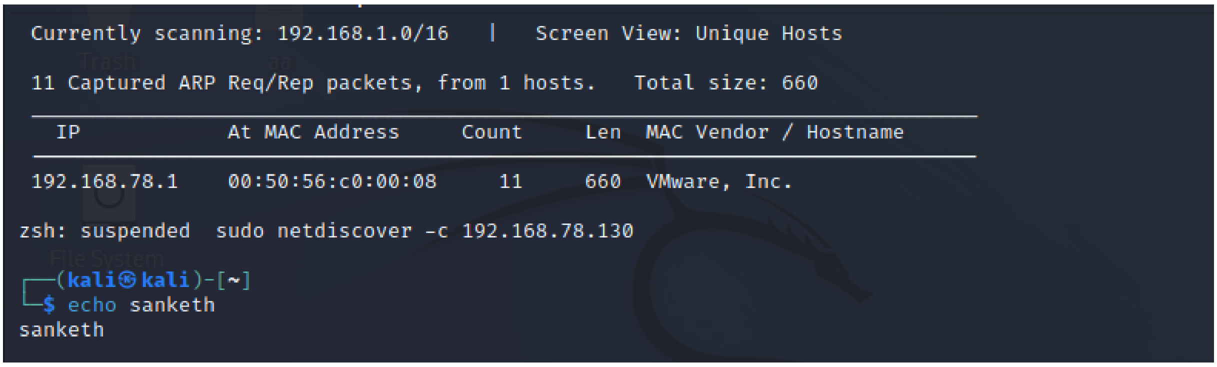
```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 6 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 360
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.78.1    00:50:56:c0:00:08      6      360  VMware, Inc.

zsh: suspended  sudo netdiscover -r 192.168.0.15

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

$ netdiscover -p



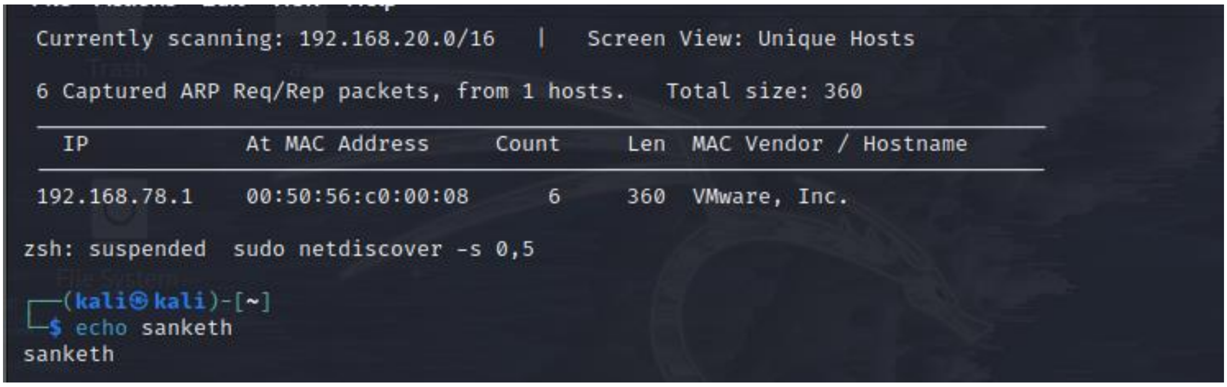
```
 Currently scanning: (passive)   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.78.1    00:50:56:c0:00:08      4      240  VMware, Inc.

zsh: suspended  sudo netdiscover -p

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

$ netdiscover -c 192.168.78.130



```
 Currently scanning: 192.168.1.0/16   |   Screen View: Unique Hosts

 11 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 660
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.78.1    00:50:56:c0:00:08     11      660  VMware, Inc.

zsh: suspended  sudo netdiscover -c 192.168.78.130

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

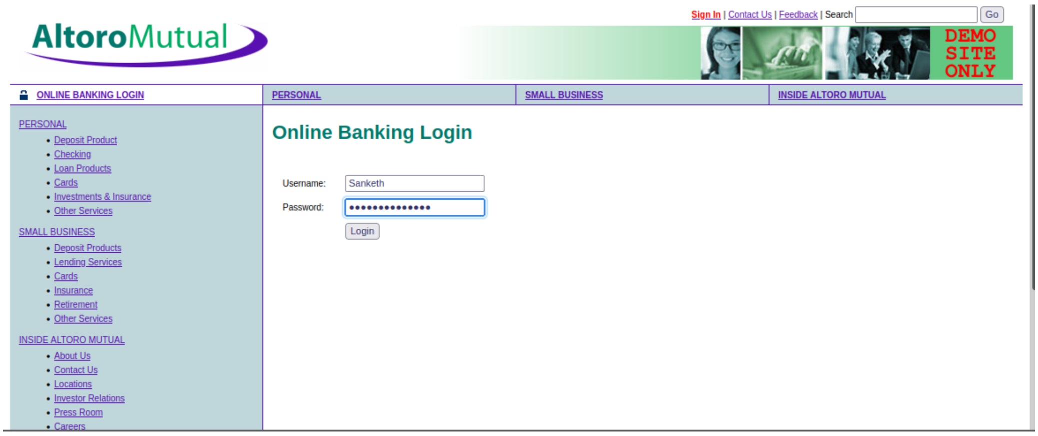
$ netdiscover –s 0.5



```
 Currently scanning: 192.168.20.0/16   |   Screen View: Unique Hosts

 6 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 360
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.78.1    00:50:56:c0:00:08      6      360  VMware, Inc.

zsh: suspended  sudo netdiscover -s 0,5

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

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 vulnarabilty in the configuration that could that could potentially be exploited by the attackers.



Online Banking Login

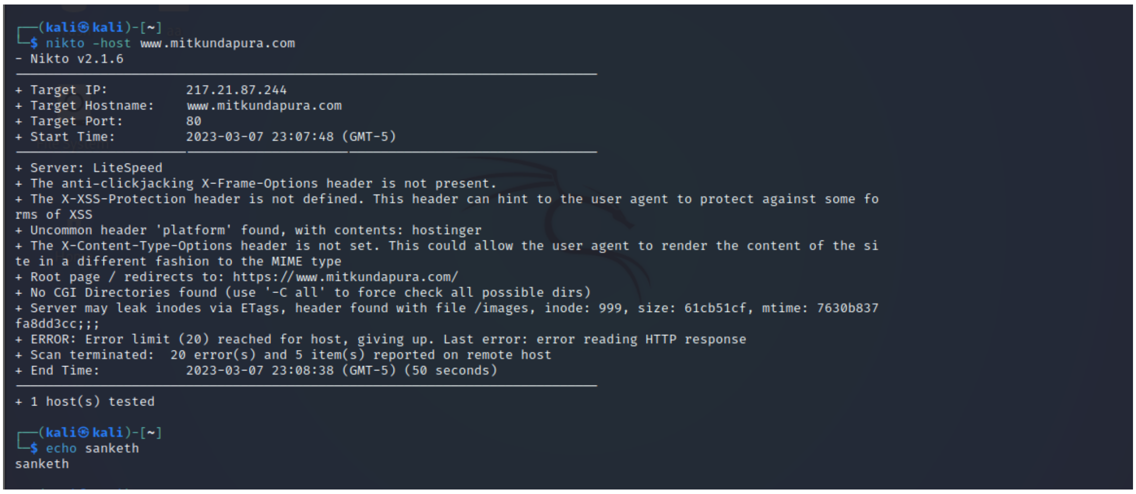
Username: Sanketh

Password: ••••••••••••••

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:

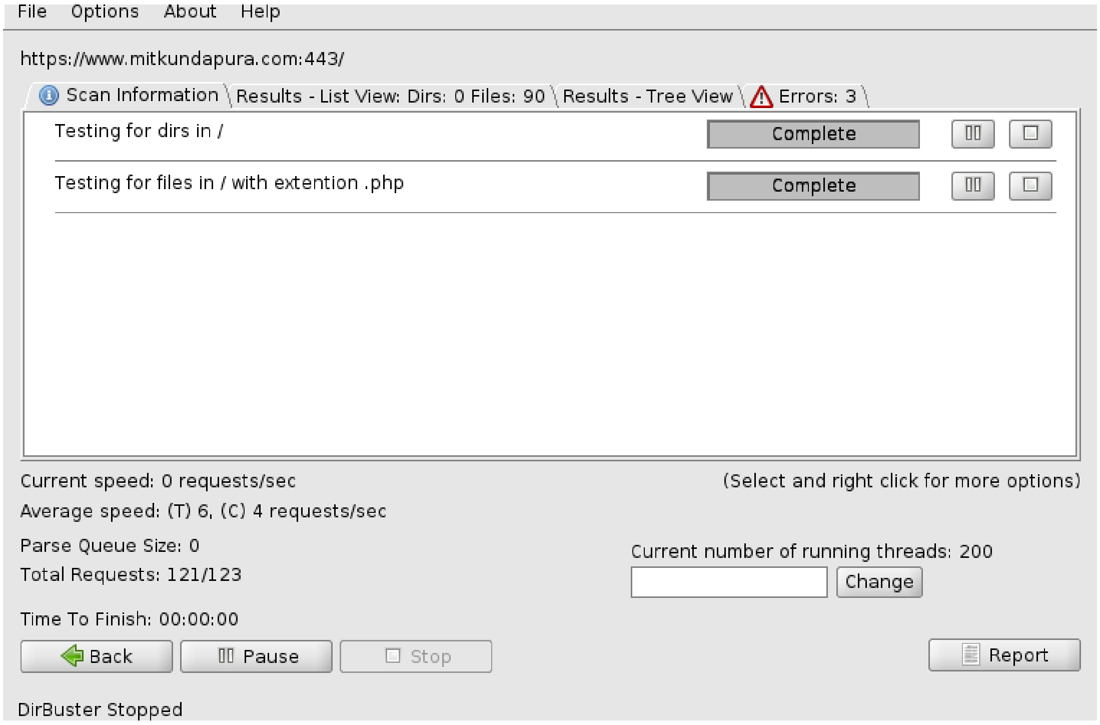
```
$ nikto  -host kali.org
```



```
┌──(kali㉿kali)-[~]
└─$ nikto -host www.mitkundapura.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          217.21.87.244
+ Target Hostname:    www.mitkundapura.com
+ Target Port:        80
+ Start Time:         2023-03-07 23:07:48 (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 fo
rms 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 si
te 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: 7630b837
fa8dd3cc;;;
+ 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:           2023-03-07 23:08:38 (GMT-5) (50 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

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

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.



https://www.mitkundapura.com:443/

Results - List View: Dirs: 0 Files: 90

Errors: 3

Testing for dirs in / Complete

Testing for files in / with extention .php Complete

Current speed: 0 requests/sec

(Select and right click for more options)

Average speed: (T) 6, (C) 4 requests/sec

Parse Queue Size: 0

Total Requests: 121/123

Current number of running threads: 200

Time To Finish: 00:00:00

DirBuster Stopped