Name: Sushma

Reg.No:145CS20020

Date:02-03-2023

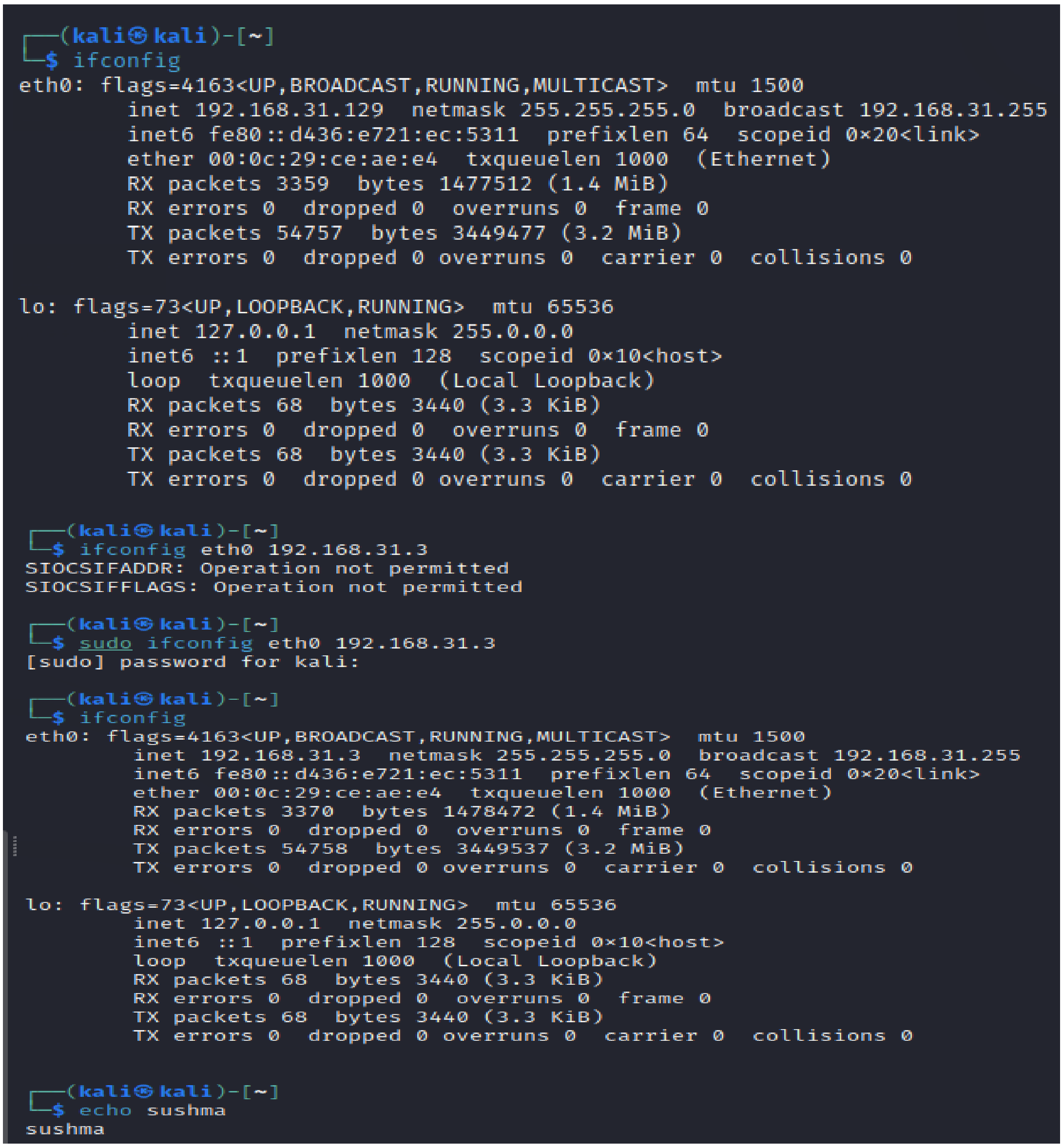
Task:2

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 form 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

$ ifconfig eth0 192.168.31.2



```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.31.129  netmask 255.255.255.0  broadcast 192.168.31.255
        inet6 fe80::d436:e721:ec:5311  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:ce:ae:e4  txqueuelen 1000  (Ethernet)
        RX packets 3359  bytes 1477512 (1.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 54757  bytes 3449477 (3.2 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 68  bytes 3440 (3.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 68  bytes 3440 (3.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~]
└─$ ifconfig eth0 192.168.31.3
SIOCSIFADDR: Operation not permitted
SIOCSIFFLAGS: Operation not permitted

┌──(kali㉿kali)-[~]
└─$ sudo ifconfig eth0 192.168.31.3
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.31.3  netmask 255.255.255.0  broadcast 192.168.31.255
        inet6 fe80::d436:e721:ec:5311  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:ce:ae:e4  txqueuelen 1000  (Ethernet)
        RX packets 3370  bytes 1478472 (1.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 54758  bytes 3449537 (3.2 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 68  bytes 3440 (3.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 68  bytes 3440 (3.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


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

2. Perform MAC address spoofing:

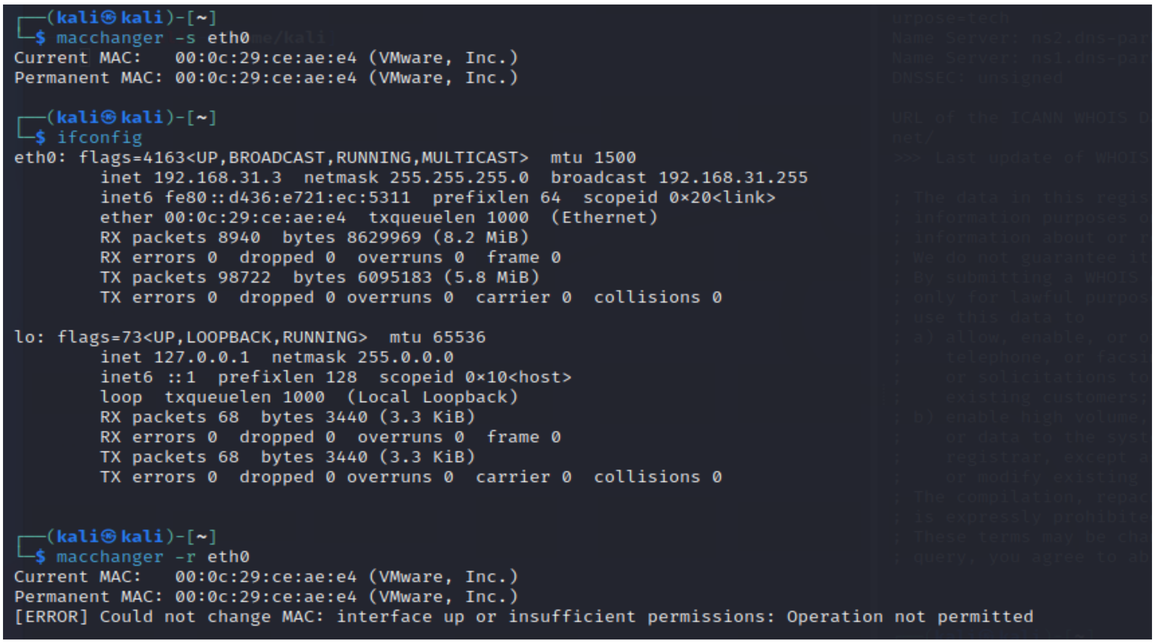
An attacker can mimic your MAC address and redirect data sent to your device to another and access your data. A MAC spoofing attack is when a hacker changes the MAC address of their device to match the MAC address of another on a network in order to gain unauthorized access or launch a Man-in-the-Middle attack.

$ macchanger –s eth0

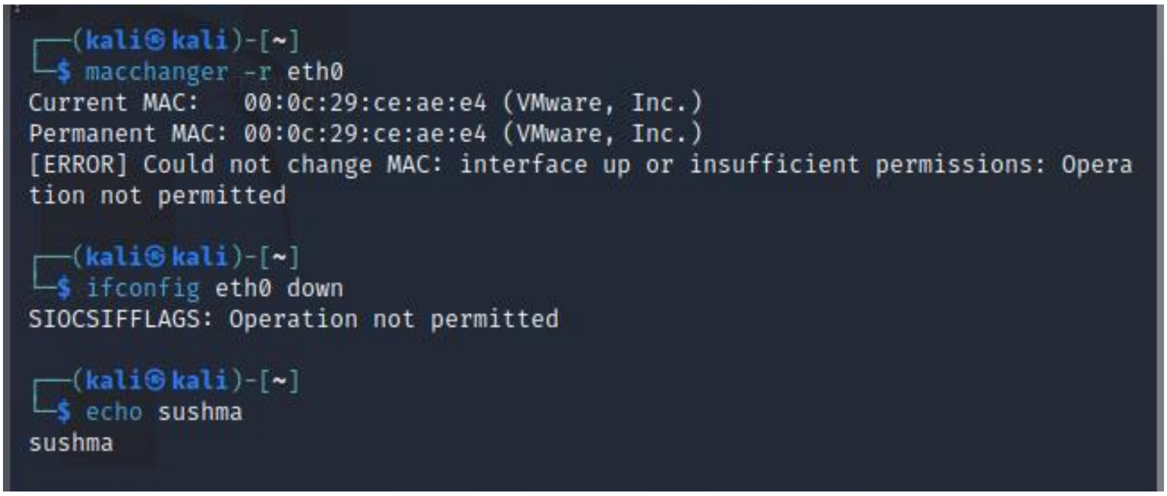
$ ifconfig

$ macchanger –r eth0

$ ifconfig eth0 down



```
┌──(kali㉿kali)-[~]
└─$ macchanger -s eth0
Current MAC:   00:0c:29:ce:ae:e4 (VMware, Inc.)
Permanent MAC: 00:0c:29:ce:ae:e4 (VMware, Inc.)

┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.31.3  netmask 255.255.255.0  broadcast 192.168.31.255
        inet6 fe80::d436:e721:ec:5311  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:ce:ae:e4  txqueuelen 1000  (Ethernet)
        RX packets 8940  bytes 8629969 (8.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 98722  bytes 6095183 (5.8 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 68  bytes 3440 (3.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 68  bytes 3440 (3.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ macchanger -r eth0
Current MAC:   00:0c:29:ce:ae:e4 (VMware, Inc.)
Permanent MAC: 00:0c:29:ce:ae:e4 (VMware, Inc.)
[ERROR] Could not change MAC: interface up or insufficient permissions: Operation not permitted
```



```
┌──(kali㉿kali)-[~]
└─$ macchanger -r eth0
Current MAC:   00:0c:29:ce:ae:e4 (VMware, Inc.)
Permanent MAC: 00:0c:29:ce:ae:e4 (VMware, Inc.)
[ERROR] Could not change MAC: interface up or insufficient permissions: Opera
tion not permitted

┌──(kali㉿kali)-[~]
└─$ ifconfig eth0 down
SIOCSIFFLAGS: Operation not permitted

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

3.Any 5 whatweb commands:

Basic scanning:

The most basic command to scan website with WhatWeb is:

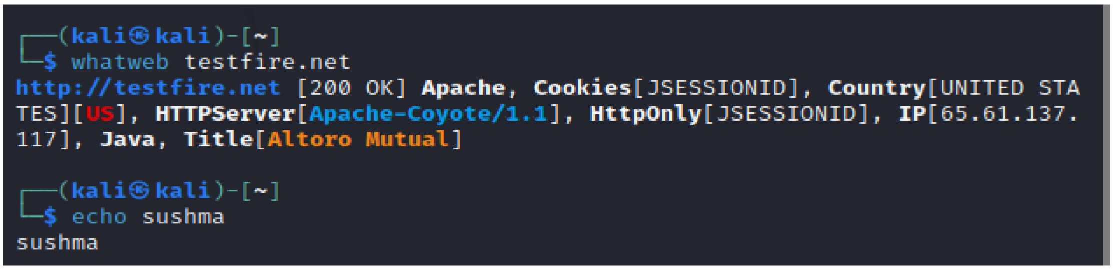
$ whatweb testfire.net

$whatweb –v testfire.net

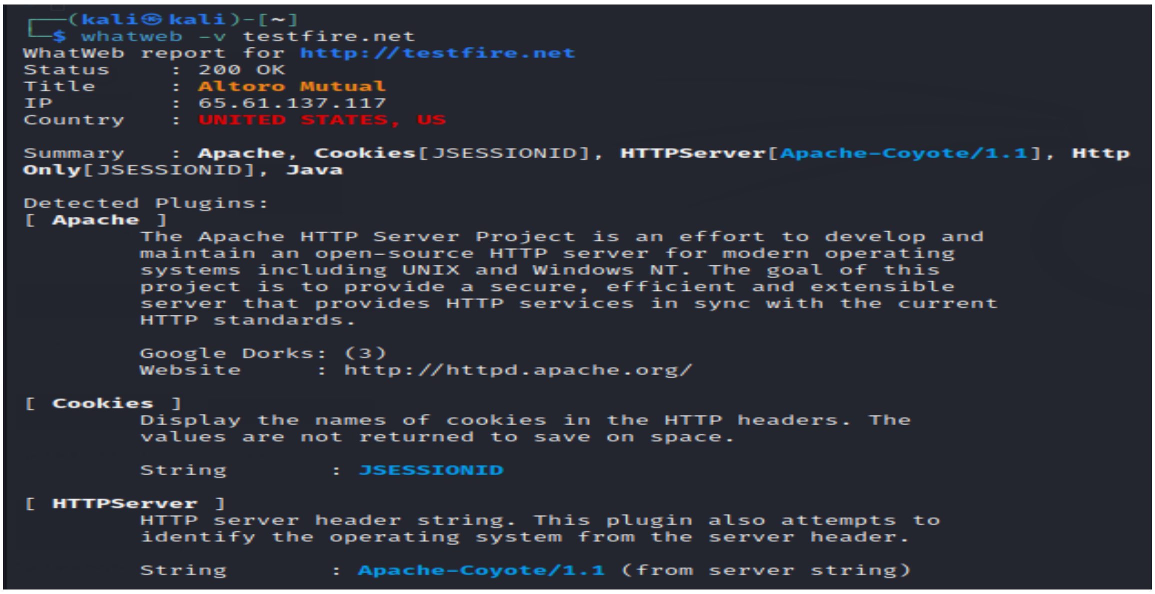
$ whatweb -a testfire.net

$ whatweb --max-redirect 2 testfire.net

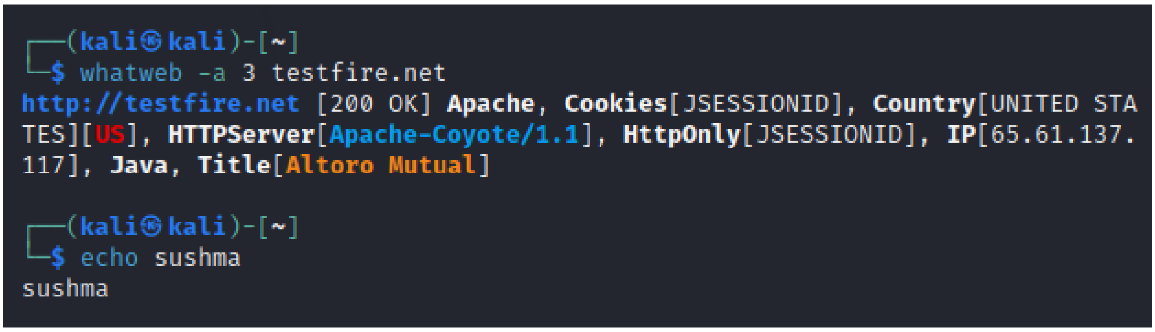
$ whatweb -v –a 3 testfire.net



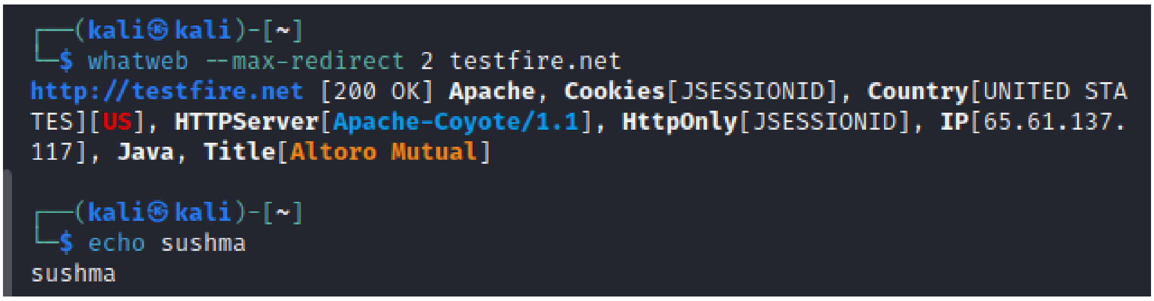
```
┌──(kali㉿kali)-[~]
└─$ whatweb testfire.net
http://testfire.net [200 OK] Apache, Cookies[JSESSIONID], Country[UNITED STA
TES][US], HTTPServer[Apache-Coyote/1.1], HttpOnly[JSESSIONID], IP[65.61.137.
117], Java, Title[Altoro Mutual]

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



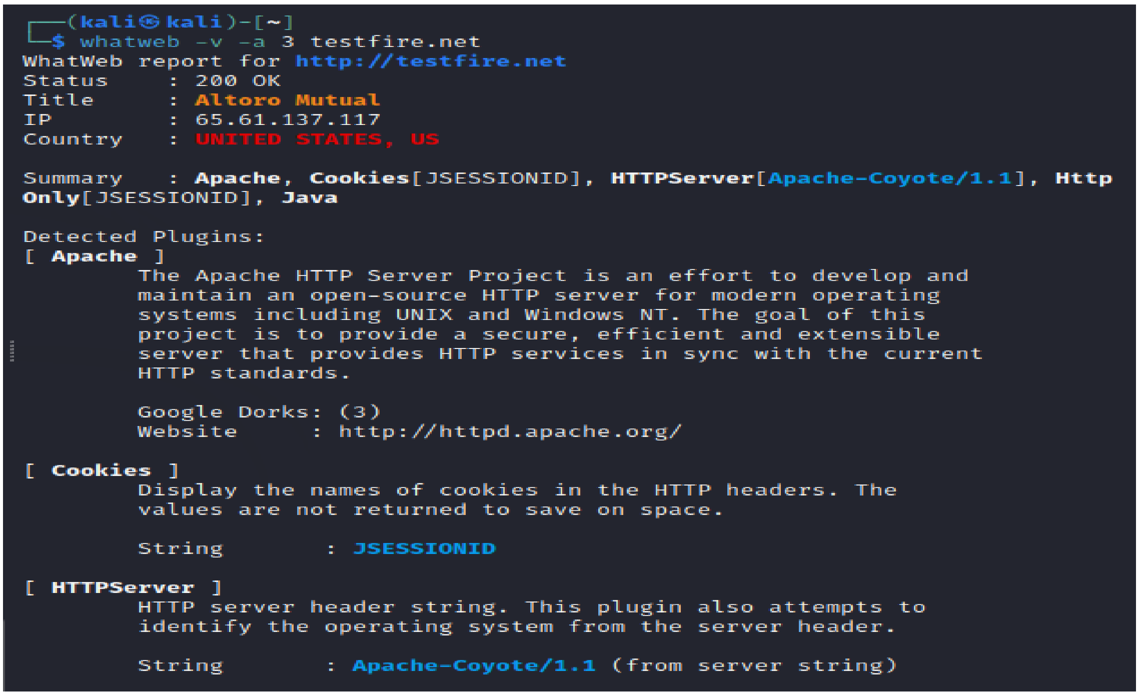
```
┌──(kali㉿kali)-[~]
└─$ whatweb -v testfire.net
WhatWeb report for http://testfire.net
Status    : 200 OK
Title     : Altoro Mutual
IP        : 65.61.137.117
Country   : UNITED STATES, US

Summary   : Apache, Cookies[JSESSIONID], HTTPServer[Apache-Coyote/1.1], Http
Only[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)
```



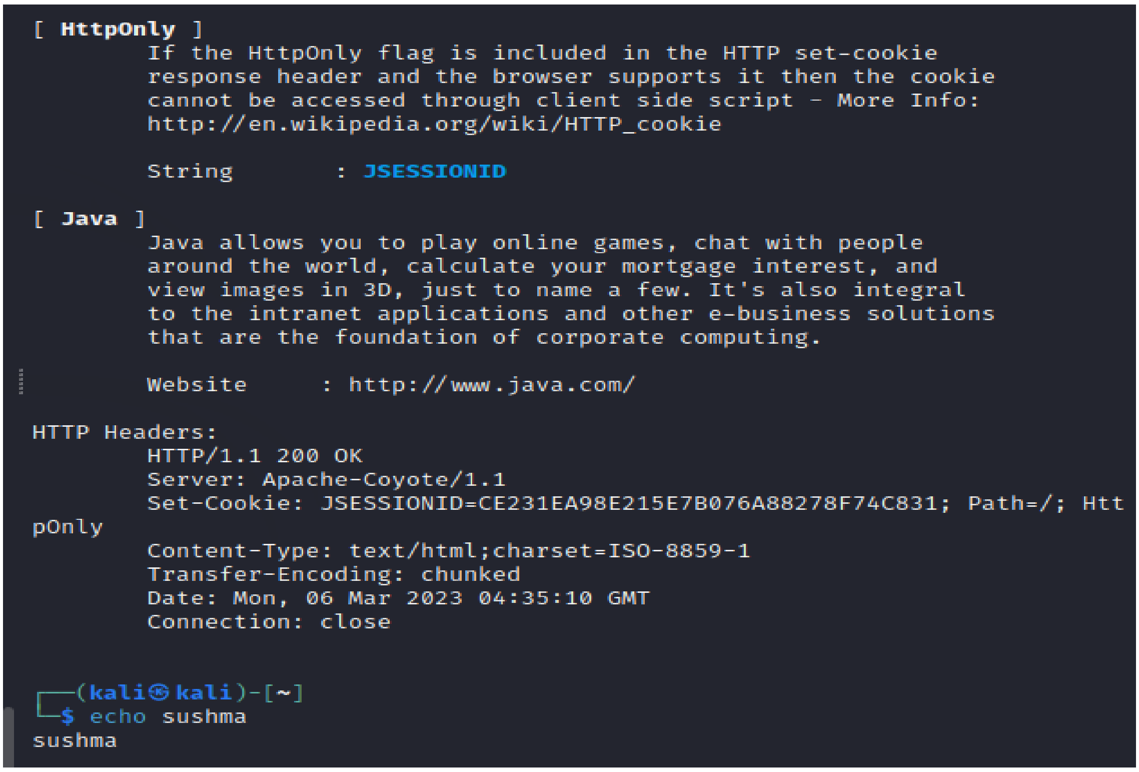
```
┌──(kali㉿kali)-[~]
└─$ whatweb -a 3 testfire.net
http://testfire.net [200 OK] Apache, Cookies[JSESSIONID], Country[UNITED STA
TES][US], HTTPServer[Apache-Coyote/1.1], HttpOnly[JSESSIONID], IP[65.61.137.
117], Java, Title[Altoro Mutual]

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



```
┌──(kali㉿kali)-[~]
└─$ whatweb --max-redirect 2 testfire.net
http://testfire.net [200 OK] Apache, Cookies[JSESSIONID], Country[UNITED STA
TES][US], HTTPServer[Apache-Coyote/1.1], HttpOnly[JSESSIONID], IP[65.61.137.
117], Java, Title[Altoro Mutual]

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



```
┌──(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], Http
Only[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 ]
        If the HttpOnly flag is included in the HTTP set-cookie
        response header and the browser supports it then the cookie
        cannot be accessed through client side script - More Info:
        http://en.wikipedia.org/wiki/HTTP_cookie

        String       : JSESSIONID

[ 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=CE231EA98E215E7B076A88278F74C831; Path=/; Htt
pOnly
        Content-Type: text/html;charset=ISO-8859-1
        Transfer-Encoding: chunked
        Date: Mon, 06 Mar 2023 04:35:10 GMT
        Connection: close


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

4.Any 5 nslookup commands:

Nslookup is a network administration command-line tool for querying the Domain Name System to obtain the mapping between domain name and IP address, or other DNS records.

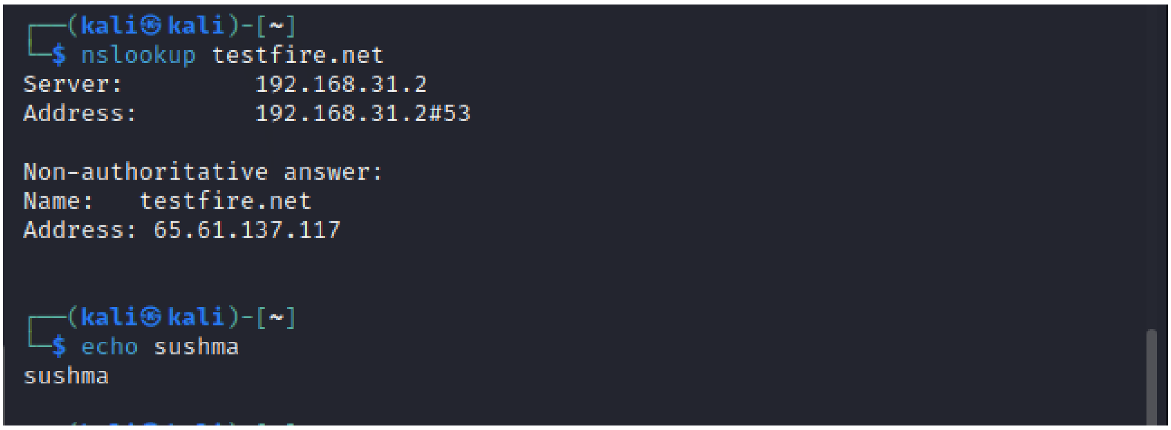
$ nslookup testfire.net

$ nslookup -type=mx testfire.net

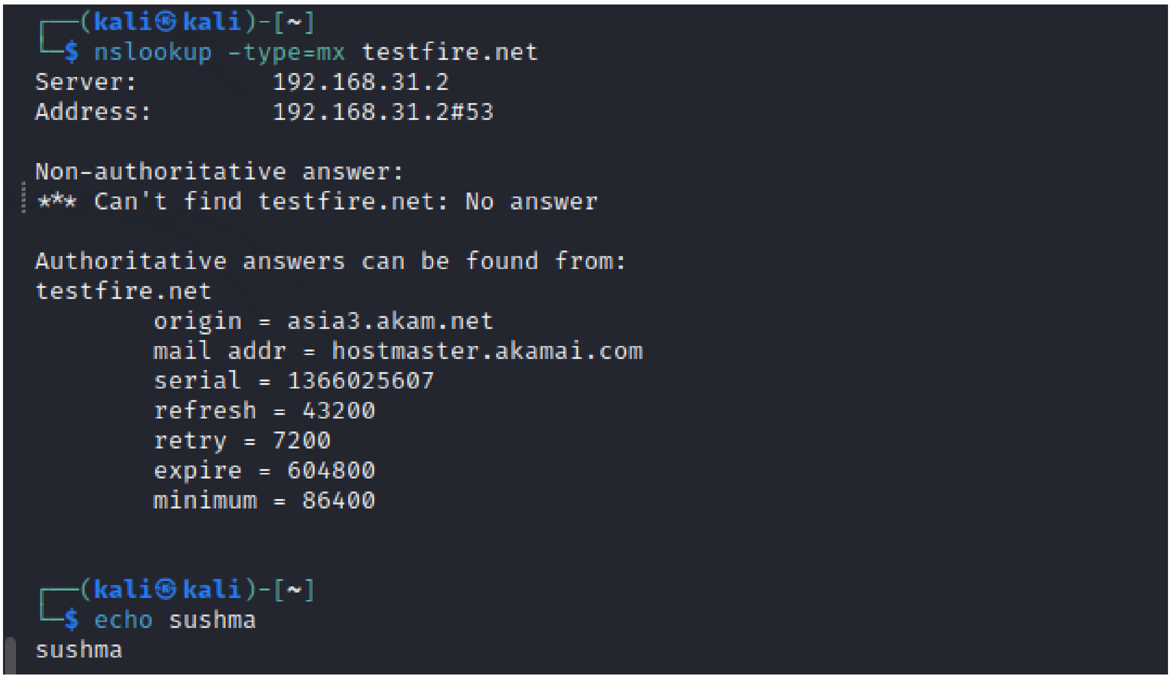
$ nslookup -type=ns testfire.net

$ nslookup -type=a testfire.net

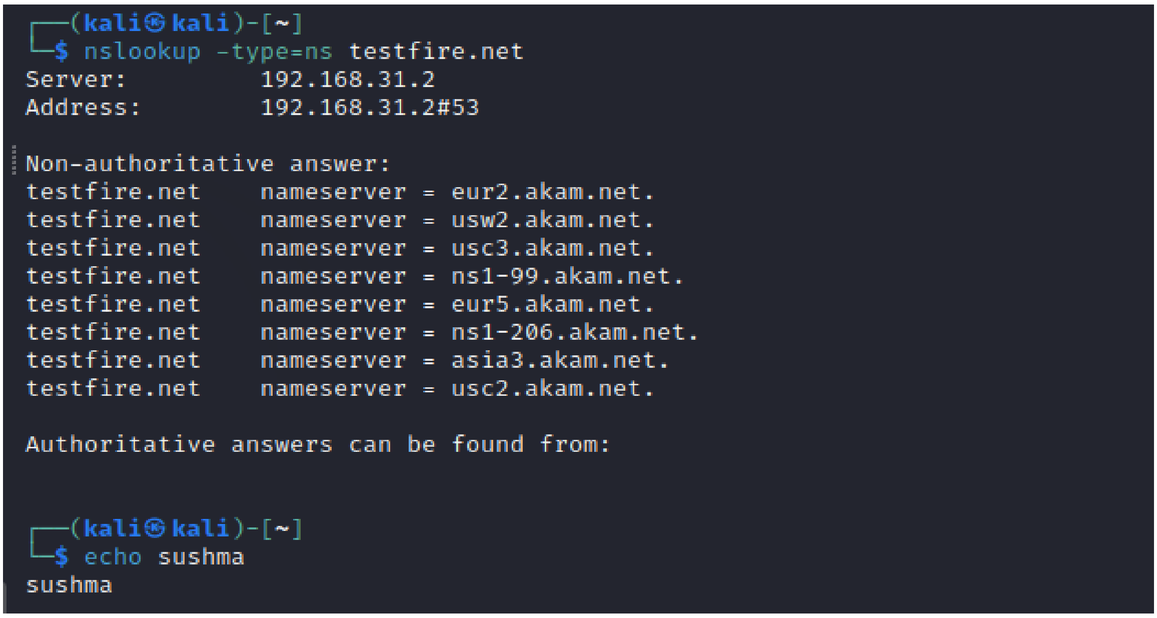
$ nslookup –type=aaaa mitkundapura.com



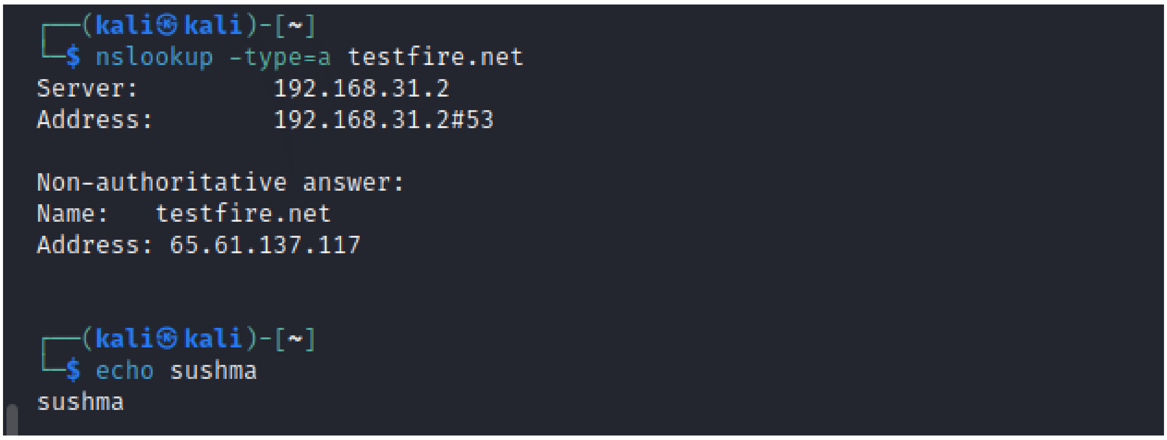
```
┌──(kali㉿kali)-[~]
└─$ nslookup testfire.net
Server:         192.168.31.2
Address:        192.168.31.2#53

Non-authoritative answer:
Name:   testfire.net
Address: 65.61.137.117


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



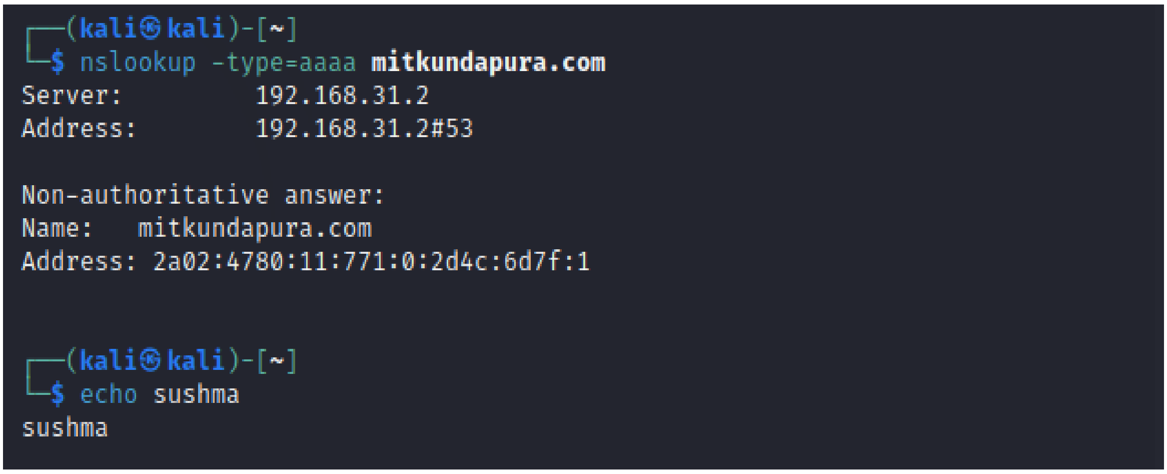
```
┌──(kali㉿kali)-[~]
└─$ nslookup -type=mx testfire.net
Server:         192.168.31.2
Address:        192.168.31.2#53

Non-authoritative answer:
*** Can't find testfire.net: No answer

Authoritative answers can be found from:
testfire.net
        origin = asia3.akam.net
        mail addr = hostmaster.akamai.com
        serial = 1366025607
        refresh = 43200
        retry = 7200
        expire = 604800
        minimum = 86400


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



```
┌──(kali㉿kali)-[~]
└─$ nslookup -type=ns testfire.net
Server:         192.168.31.2
Address:        192.168.31.2#53

Non-authoritative answer:
testfire.net    nameserver = eur2.akam.net.
testfire.net    nameserver = usw2.akam.net.
testfire.net    nameserver = usc3.akam.net.
testfire.net    nameserver = ns1-99.akam.net.
testfire.net    nameserver = eur5.akam.net.
testfire.net    nameserver = ns1-206.akam.net.
testfire.net    nameserver = asia3.akam.net.
testfire.net    nameserver = usc2.akam.net.

Authoritative answers can be found from:


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



```
┌──(kali㉿kali)-[~]
└─$ nslookup -type=a testfire.net
Server:         192.168.31.2
Address:        192.168.31.2#53

Non-authoritative answer:
Name:   testfire.net
Address: 65.61.137.117


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

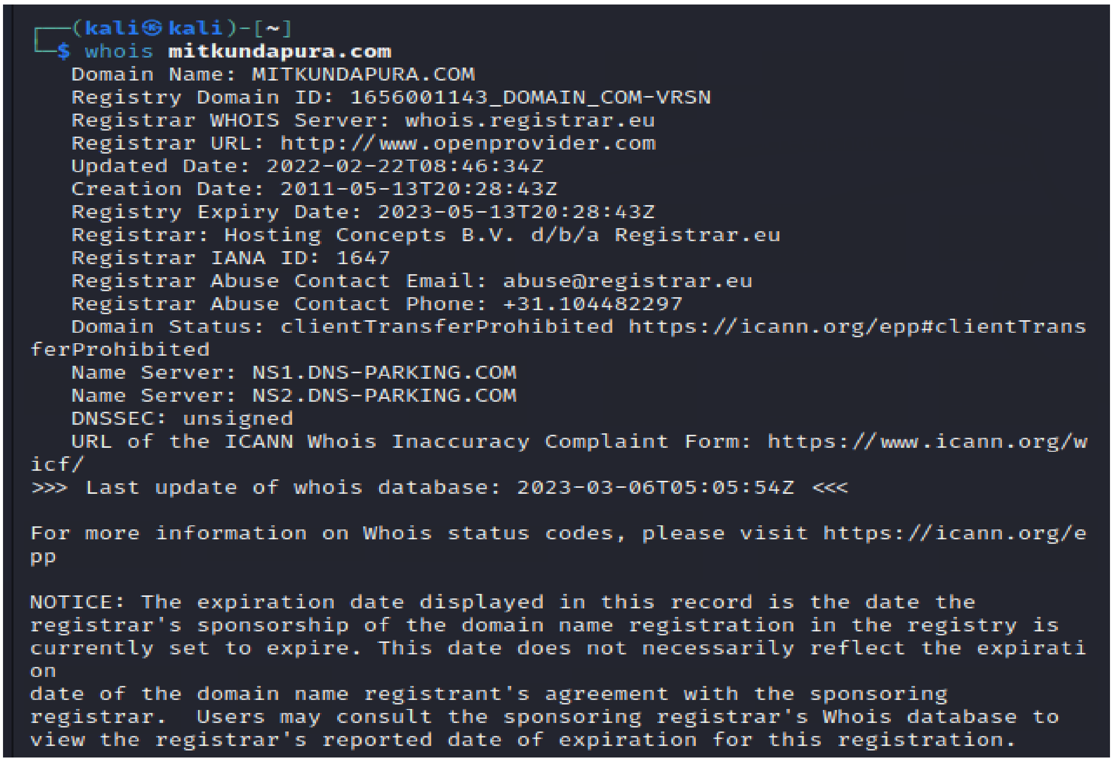


```
┌──(kali㉿kali)-[~]
└─$ nslookup -type=aaaa mitkundapura.com
Server:         192.168.31.2
Address:        192.168.31.2#53

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


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

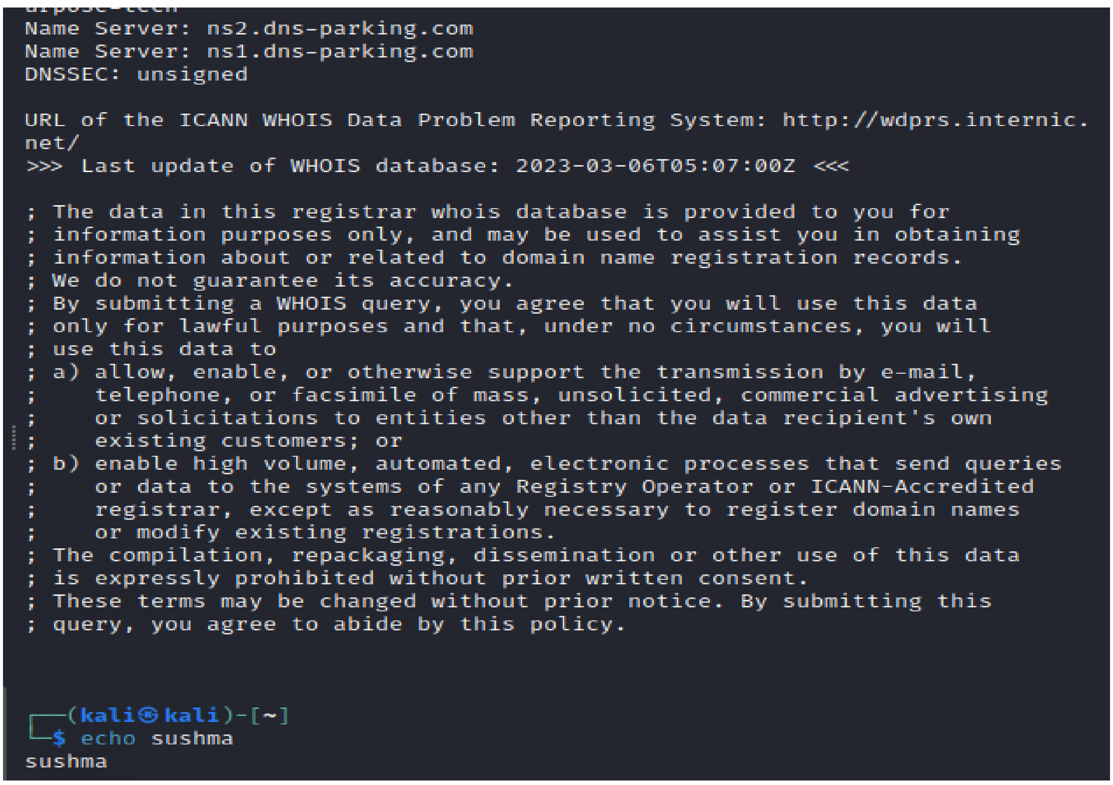
5. whois commands:

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



```
┌──(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#clientTrans
ferProhibited
   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/w
icf/
>>> Last update of whois database: 2023-03-06T05:05:54Z <<<

For more information on Whois status codes, please visit https://icann.org/e
pp

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 expirati
on
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.
```



```
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: 2023-03-06T05:07:00Z <<<

; 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 sushma
sushma
```

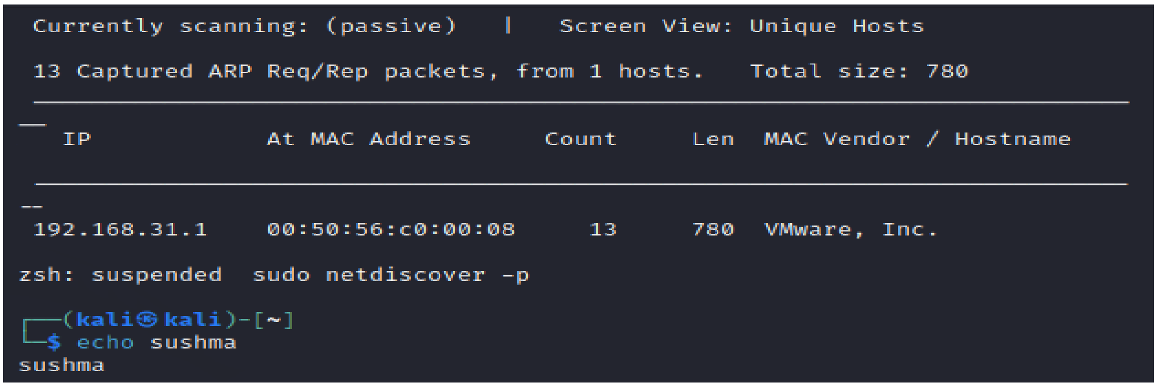
6. Find data packets using wireshark:

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 maon menu. Wireshark will open toolbar between the main toolbar and the packet list, “The “Find Packet”toolbar”.

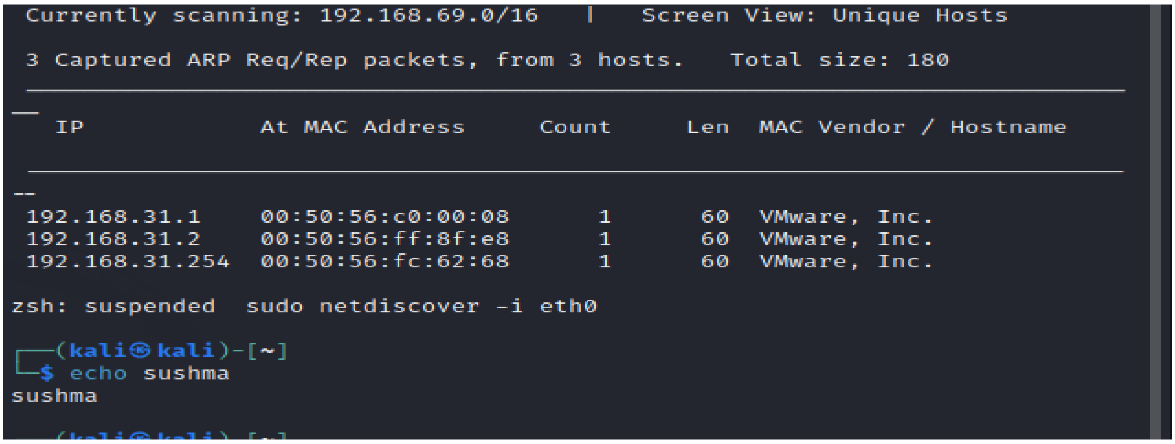
7.Any 5 netdiscover command:

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:

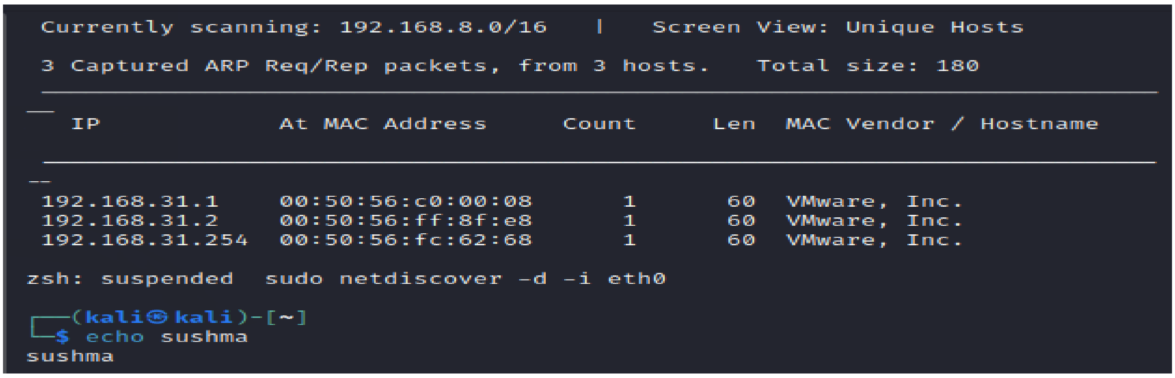
$ sudo netdiscover -p
$ sudo netdiscover -i eth0
$sudo netdiscover –d -i eth0



```
 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
 _____________________________________________________________________________
--
 192.168.31.1    00:50:56:c0:00:08     13     780  VMware, Inc.

zsh: suspended  sudo netdiscover -p

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



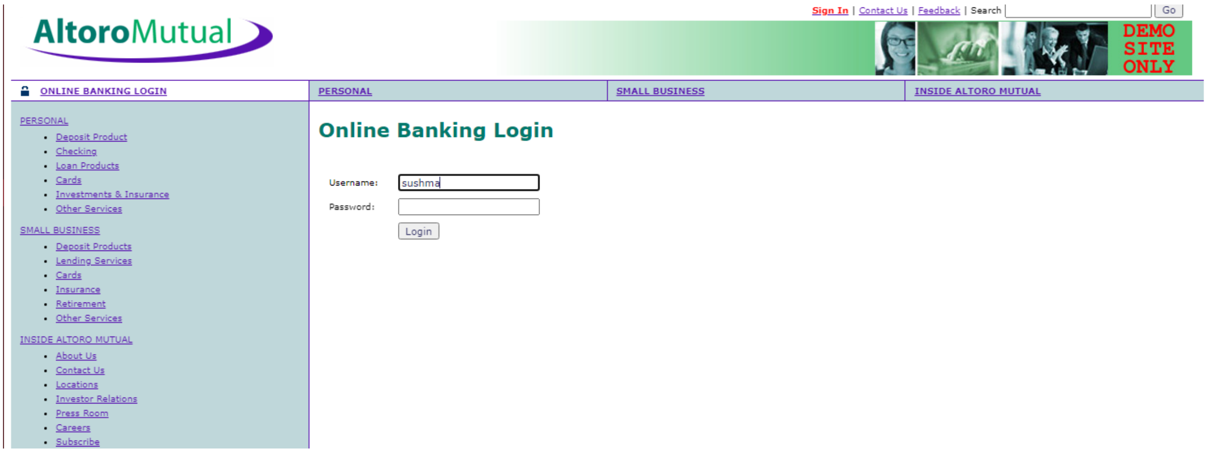
```
 Currently scanning: 192.168.69.0/16   |   Screen View: Unique Hosts

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
 _____________________________________________________________________________
__
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 _____________________________________________________________________________
--
 192.168.31.1    00:50:56:c0:00:08      1      60  VMware, Inc.
 192.168.31.2    00:50:56:ff:8f:e8      1      60  VMware, Inc.
 192.168.31.254  00:50:56:fc:62:68      1      60  VMware, Inc.

zsh: suspended  sudo netdiscover -i eth0

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



```
 Currently scanning: 192.168.8.0/16   |   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
 _____________________________________________________________________________
--
 192.168.31.1    00:50:56:c0:00:08      1      60  VMware, Inc.
 192.168.31.2    00:50:56:ff:8f:e8      1      60  VMware, Inc.
 192.168.31.254  00:50:56:fc:62:68      1      60  VMware, Inc.

zsh: suspended  sudo netdiscover -d -i eth0

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

8. CryptoConfiguration Flow:

CryptoConfiguration typically refers to the configuration of cryptographic protocols and algorithms used to protect sensitive data and communications. A flow is context cloud refers to a weakness or vulnerability in the configuration that cloud potentially be exploited by the attackers.



Online Banking Login

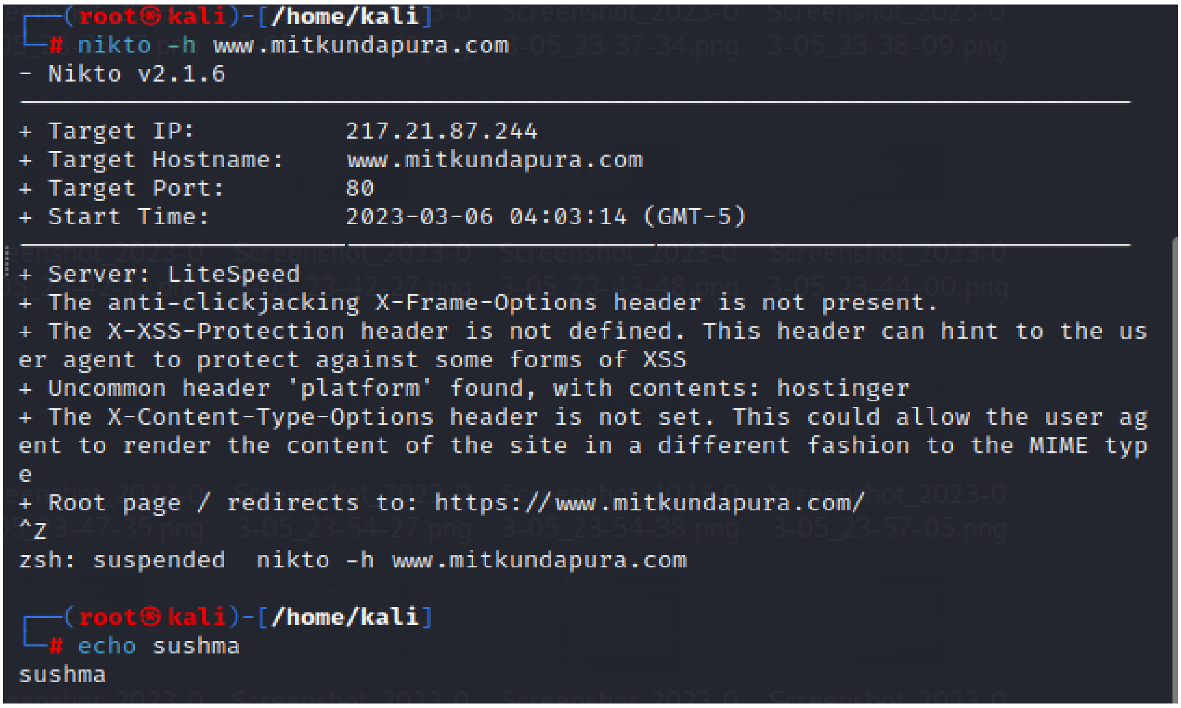
Username: sushma

Password:

Login

9. Nikto commands:

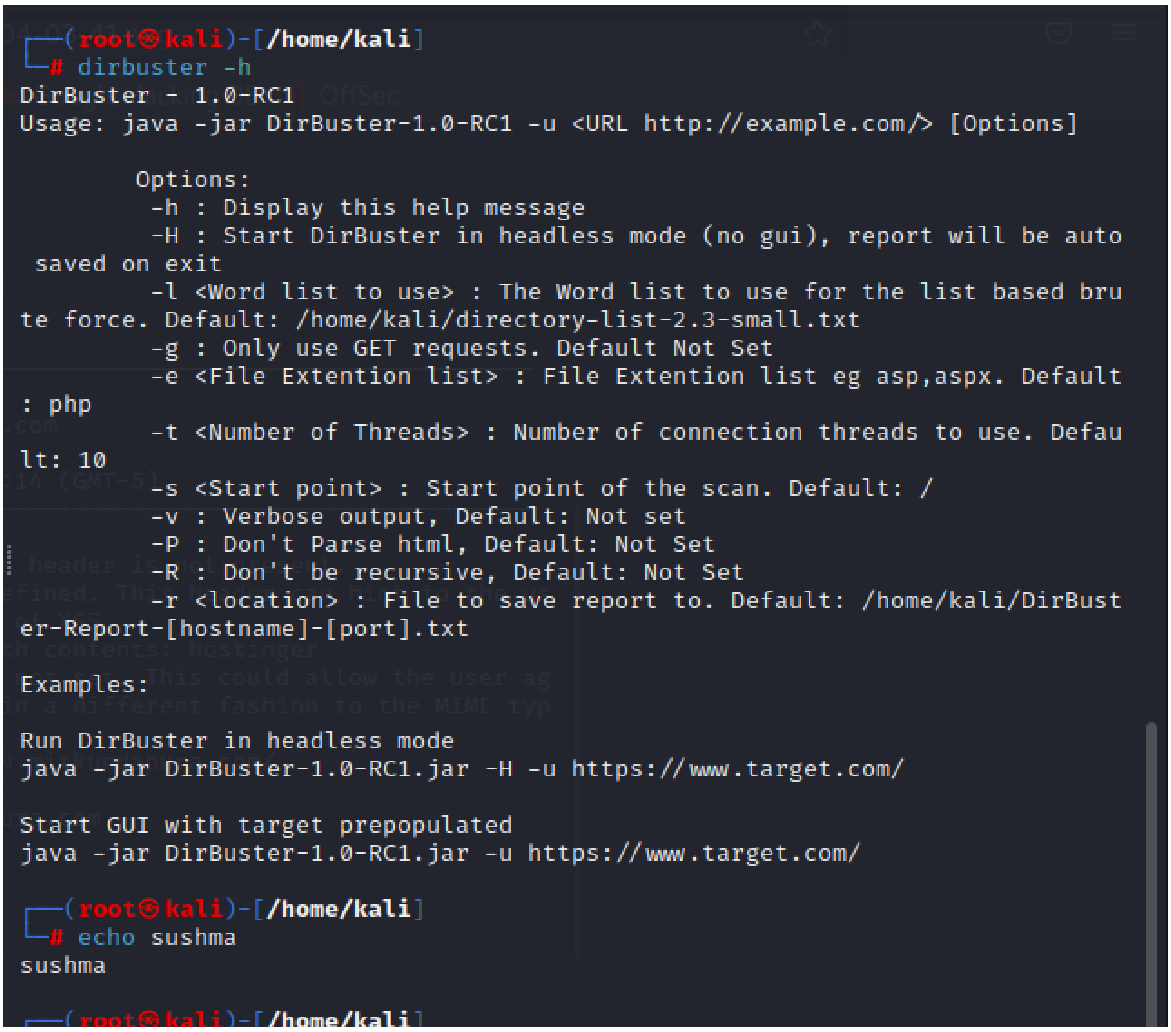
Nikto is a popular web server scanner that can help you identify potential vulnerabilities on a web serve. Here are some common Nikto commands:



```
┌──(root㉿kali)-[/home/kali]
└─# nikto -h 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 04:03:14 (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 us
er 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 ag
ent to render the content of the site in a different fashion to the MIME typ
e
+ Root page / redirects to: https://www.mitkundapura.com/
^Z
zsh: suspended  nikto -h www.mitkundapura.com

┌──(root㉿kali)-[/home/kali]
└─# echo sushma
sushma
```

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.



```
┌──(root㉿kali)-[/home/kali]
└─# dirbuster -h
DirBuster - 1.0-RC1
Usage: java -jar DirBuster-1.0-RC1 -u <URL http://example.com/> [Options]

        Options:
         -h : Display this help message
         -H : Start DirBuster in headless mode (no gui), report will be auto
 saved on exit
         -l <Word list to use> : The Word list to use for the list based bru
te force. Default: /home/kali/directory-list-2.3-small.txt
         -g : Only use GET requests. Default Not Set
         -e <File Extention list> : File Extention list eg asp,aspx. Default
: php
         -t <Number of Threads> : Number of connection threads to use. Defau
lt: 10
         -s <Start point> : Start point of the scan. Default: /
         -v : Verbose output, Default: Not set
         -P : Don't Parse html, Default: Not Set
         -R : Don't be recursive, Default: Not Set
         -r <location> : File to save report to. Default: /home/kali/DirBust
er-Report-[hostname]-[port].txt

Examples:

Run DirBuster in headless mode
java -jar DirBuster-1.0-RC1.jar -H -u https://www.target.com/

Start GUI with target prepopulated
java -jar DirBuster-1.0-RC1.jar -u https://www.target.com/

┌──(root㉿kali)-[/home/kali]
└─# echo sushma
sushma

┌──(root㉿kali)-[/home/kali]
```