Name:Darshan S Kundar

Date:02-03-2023

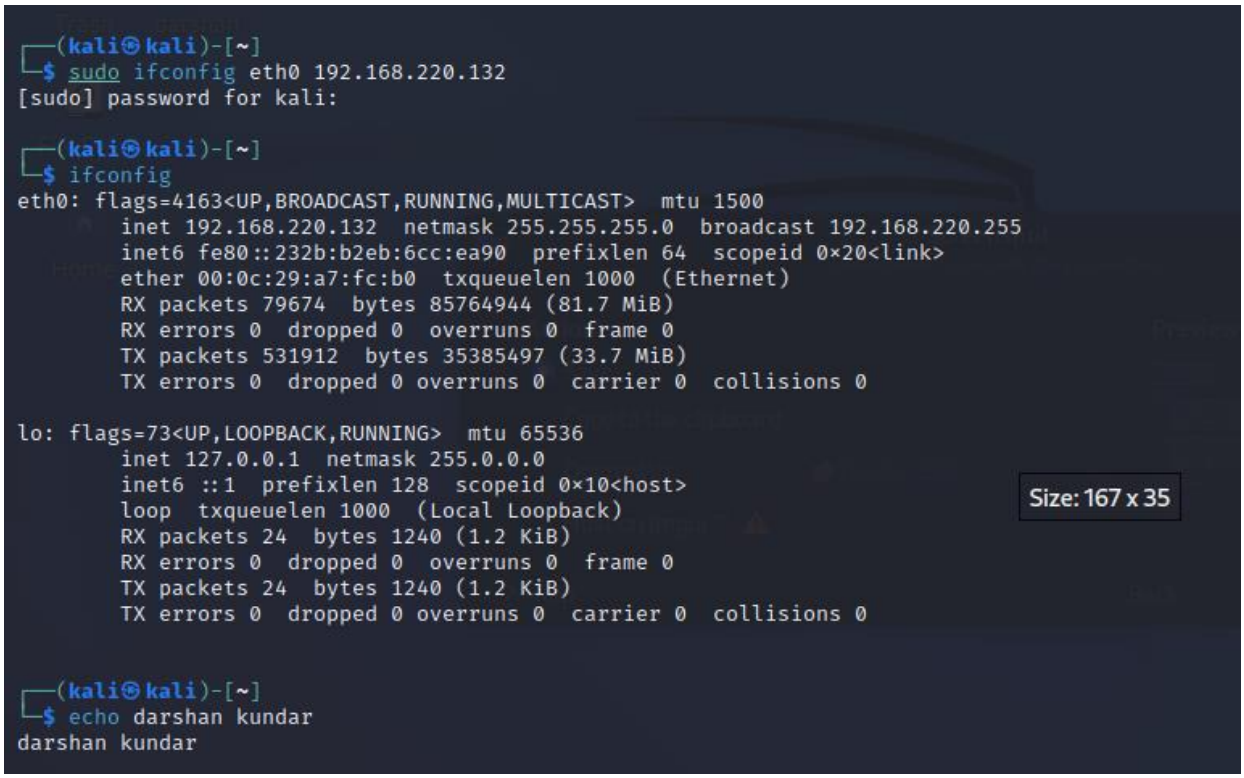
Task:2

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.

$ sudo ifconfig eth0 192.168.209.15

$ ifconfig



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.

$ sudo macchanger –s eth0

$ ifconfig

$ macchanger –r eth0

$ ifconfig eth0 down

```
┌──(kali㉿kali)-[~]
└─$ sudo macchanger -s eth0
Current MAC:   00:0c:29:a7:fc:b0 (VMware, Inc.)
Permanent MAC: 00:0c:29:a7:fc:b0 (VMware, Inc.)

┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.220.132  netmask 255.255.255.0  broadcast 192.168.220.255
        inet6 fe80::232b:b2eb:6cc:ea90  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:a7:fc:b0  txqueuelen 1000  (Ethernet)
        RX packets 79965  bytes 85799374 (81.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 531917  bytes 35386067 (33.7 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 24  bytes 1240 (1.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1240 (1.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ sudo macchanger -r eth0
Current MAC:   00:0c:29:a7:fc:b0 (VMware, Inc.)
Permanent MAC: 00:0c:29:a7:fc:b0 (VMware, Inc.)
New MAC:       ee:0e:42:37:74:2d (unknown)

┌──(kali㉿kali)-[~]
└─$ ifconfig
```

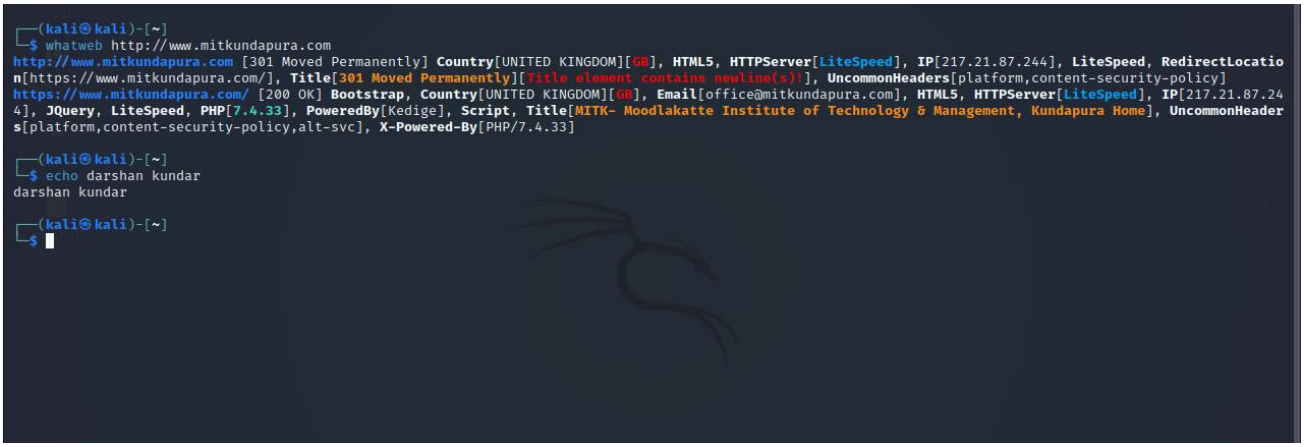
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.220.132  netmask 255.255.255.0  broadcast 192.168.220.255
        inet6 fe80::232b:b2eb:6cc:ea90  prefixlen 64  scopeid 0×20<link>
        ether ee:0e:42:37:74:2d  txqueuelen 1000  (Ethernet)
        RX packets 79965  bytes 85799374 (81.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 531920  bytes 35386247 (33.7 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 24  bytes 1240 (1.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1240 (1.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


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

3.Any 5 whatweb commands:

Basic scanning:

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

$ whatweb [website URL]

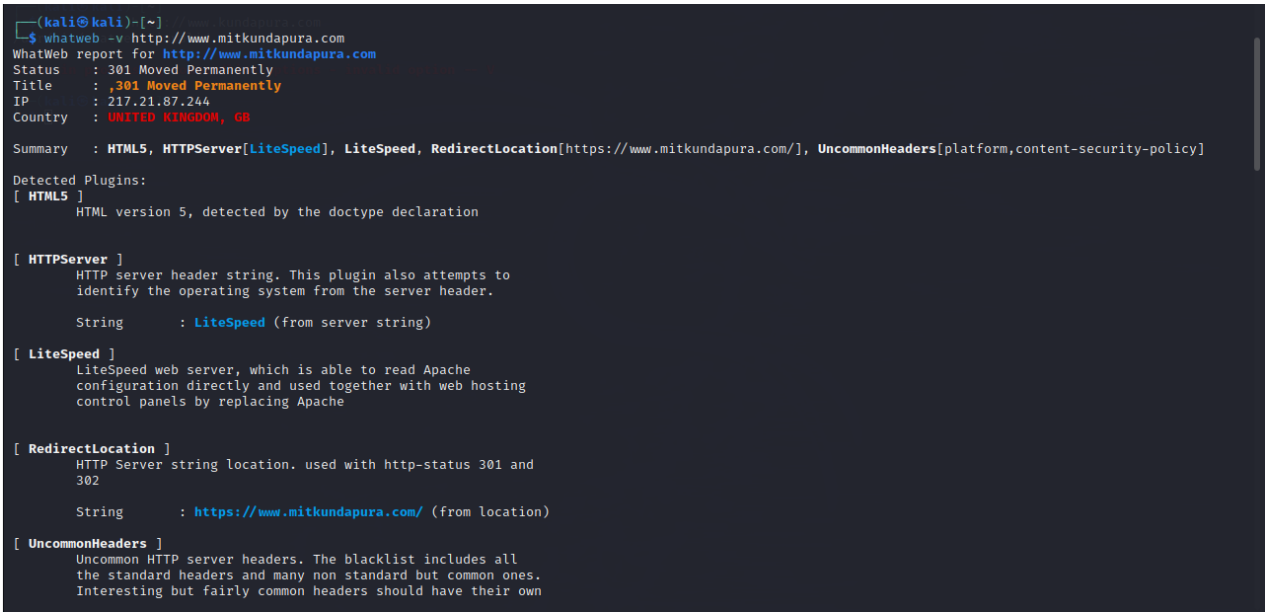


This will perform a default scan of the website and display the identified technologies.

Verbose scanning:

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

$ whatweb -v [website URL]



```
[ 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       : platform,content-security-policy,alt-svc (from headers)

[ 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 06:54:24 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"


┌──(kali㉿kali)-[~]
└─$ echo darshan kundar
darshan kundar

┌──(kali㉿kali)-[~]
└─$
```

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

$ whatweb –a 3 [website URL]

```
┌──(kali㉿kali)-[~]
└─$ whatweb -a 3 http://www.mitkundapura.com
http://www.mitkundapura.com [301 Moved Permanently] Country[UNITED KINGDOM][GB], HTML5, HTTPServer[LiteSpeed], IP[217.21.87.244], LiteSpeed, RedirectLocatio
ntains 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[217.21.87.24
lakatte Institute of Technology & Management, Kundapura Home], UncommonHeaders[platform,content-security-policy,alt-svc], X-Powered-By[PHP/7.4.33]

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

┌──(kali㉿kali)-[~]
└─$ whatweb -a 3 http://www.mitkundapura.com
http://www.mitkundapura.com [301 Moved Permanently] Country[UNITED KINGDOM][GB], HTML5, HTTPServer[LiteSpeed], IP[217.21.87.244], LiteSpeed, RedirectLocatio
n[https://www.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[217.21.87.24
4], JQuery, LiteSpeed, PHP[7.4.33], PoweredBy[Kedige], Script, Title[MITK- Moodlakatte Institute of Technology & Management, Kundapura Home], UncommonHeader
s[platform,content-security-policy,alt-svc], X-Powered-By[PHP/7.4.33]

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

$ whatweb --max –redirect 2 [website URL]

```
┌──(kali㉿kali)-[~]
└─$ whatweb --max-redirect 2 http://www.mitkundapura.com
http://www.mitkundapura.com [301 Moved Permanently] Country[UNITED KINGDOM][GB], HTML5, HTTPServer[LiteSpeed], IP[217.21.87.244], LiteSpeed, RedirectLocatio
ntains 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[217.21.87.24
lakatte Institute of Technology & Management, Kundapura Home], UncommonHeaders[platform,content-security-policy,alt-svc], X-Powered-By[PHP/7.4.33]

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

┌──(kali㉿kali)-[~]
└─$ whatweb --max-redirect 2 http://www.mitkundapura.com
http://www.mitkundapura.com [301 Moved Permanently] Country[UNITED KINGDOM][GB], HTML5, HTTPServer[LiteSpeed], IP[217.21.87.244], LiteSpeed, RedirectLocatio
n[https://www.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[217.21.87.24
4], JQuery, LiteSpeed, PHP[7.4.33], PoweredBy[Kedige], Script, Title[MITK- Moodlakatte Institute of Technology & Management, Kundapura Home], UncommonHeader
s[platform,content-security-policy,alt-svc], X-Powered-By[PHP/7.4.33]

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

$ whatweb –v –a 3 [website URL]

```
┌──(kali㉿kali)-[~]
└─$ whatweb -v -a 3 http://www.mitkundapura.com
WhatWeb report for http://www.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://www.mitkundapura.com/], UncommonHeaders[platform,content-security-policy]

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

[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : LiteSpeed (from server string)

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


[ RedirectLocation ]
        HTTP Server string location. used with http-status 301 and
        302

        String       : https://www.mitkundapura.com/ (from location)

[ 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
```

```
[ 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
        transfer-encoding: chunked
        content-encoding: gzip
        vary: Accept-Encoding
        date: Fri, 03 Mar 2023 07:40:52 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"


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

4.Any 5 nslookup commands:

$ nslookup google.com

```
┌──(kali㉿kali)-[~]
└─$ nslookup google.com
Server:         192.168.11.2
Address:        192.168.11.2#53

Non-authoritative answer:
Name:   google.com
Address: 172.217.166.46
Name:   google.com
Address: 2404:6800:4007:81f::200e


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

$ nslookup -type=mx [website URL]

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 mitkundapura.com
Server:         192.168.11.2
Address:        192.168.11.2#53

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

Authoritative answers can be found from:


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

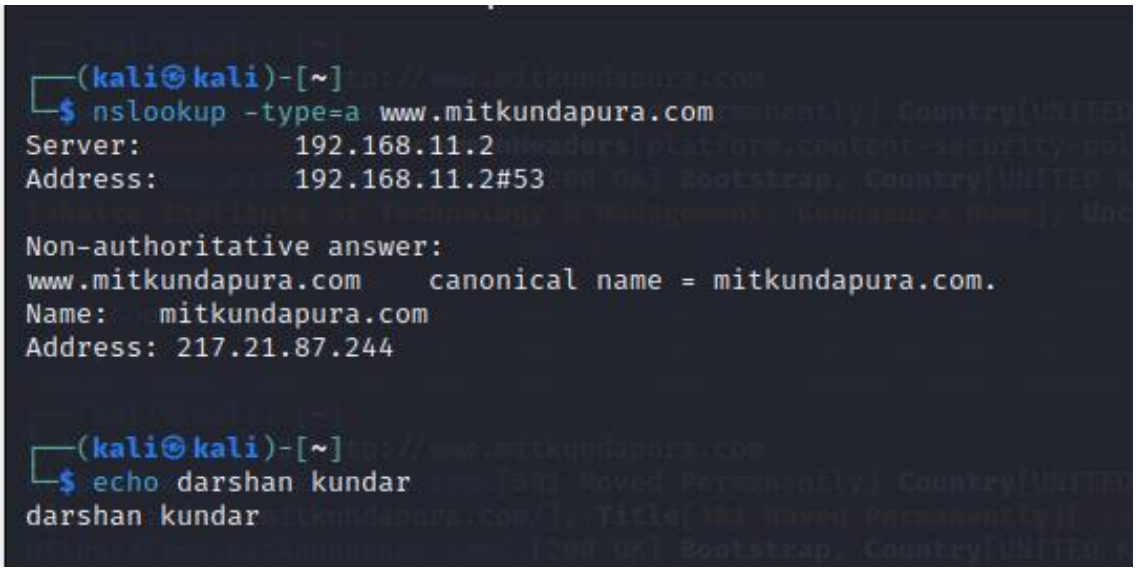
$ nslookup -type=ns [website URL]

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 mitkundapura.com
Server:         192.168.11.2
Address:        192.168.11.2#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 darshan kundar
darshan kundar
```

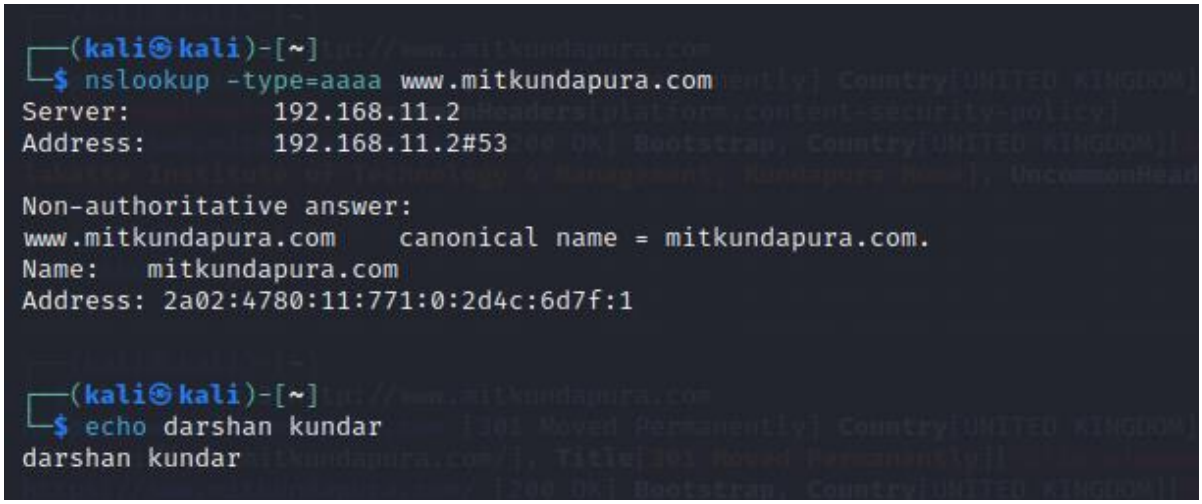
$ nslookup -type=a [website URL]

This command will perform a DNS lookup for the IPv4 address associated with the subdomain www.example.com.



$ nslookup -type=aaa [website URL]

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

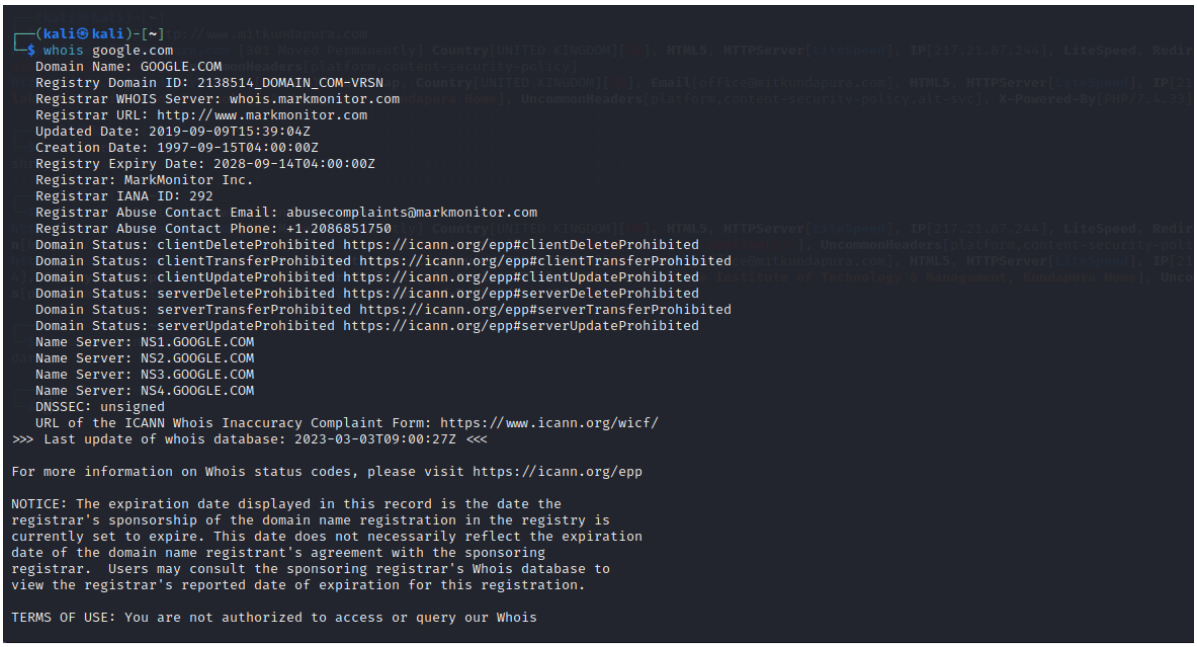


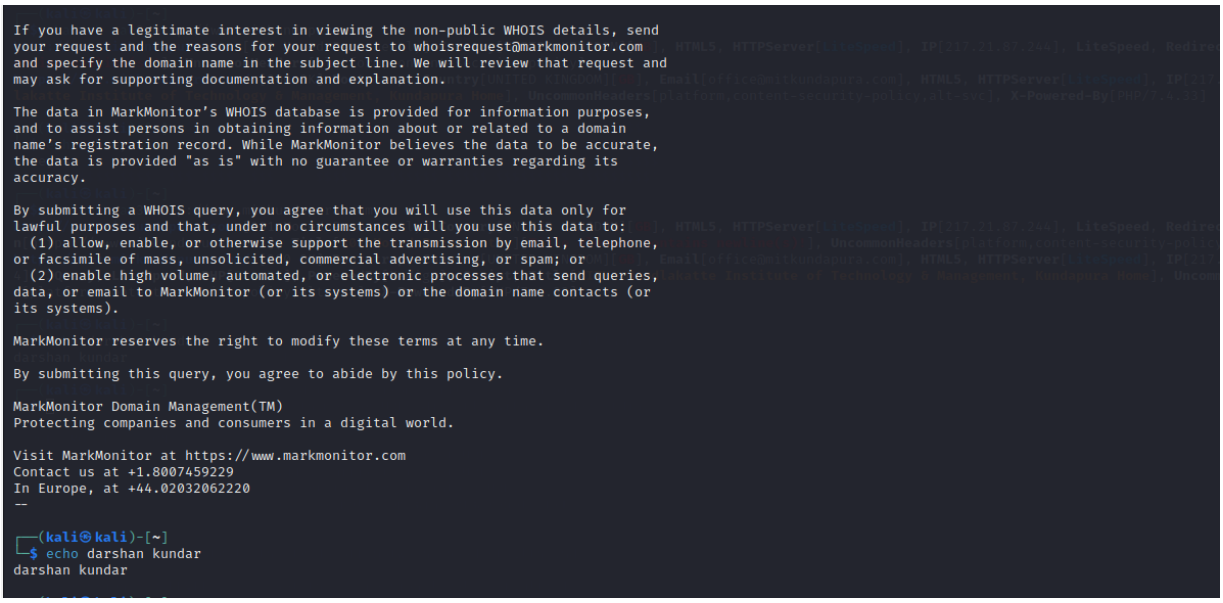
5.whois Commands:

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 [website URL]

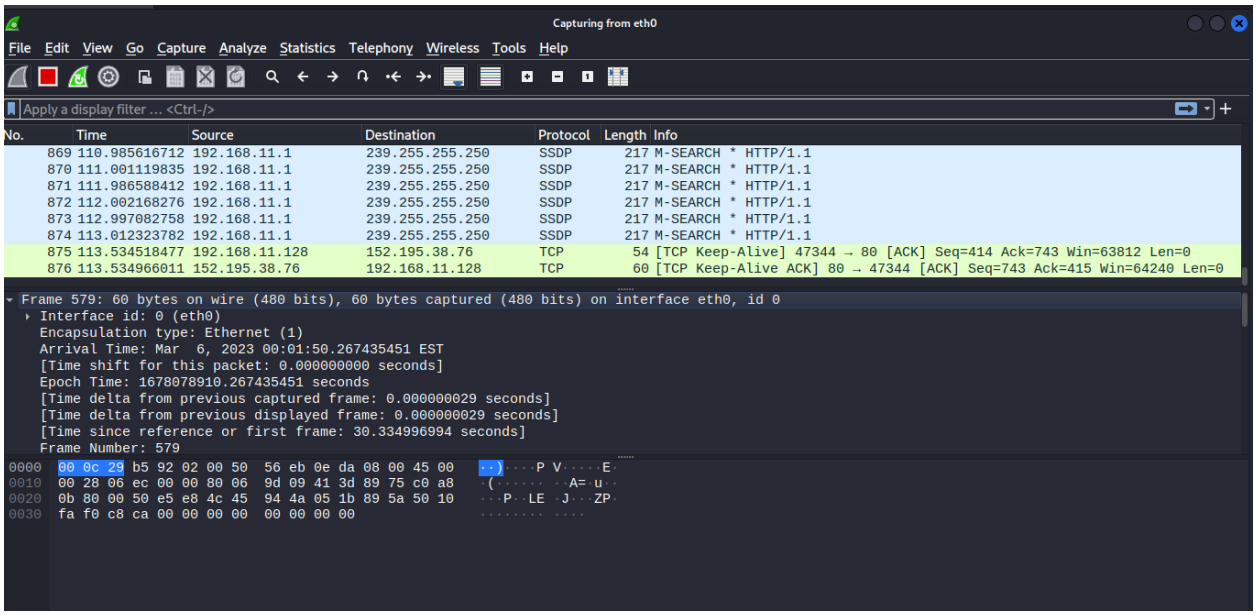
This command will display information about the domain name, such as the name of the registrant, the name servers, and the date of registration





6.Find data packets using wireshark:

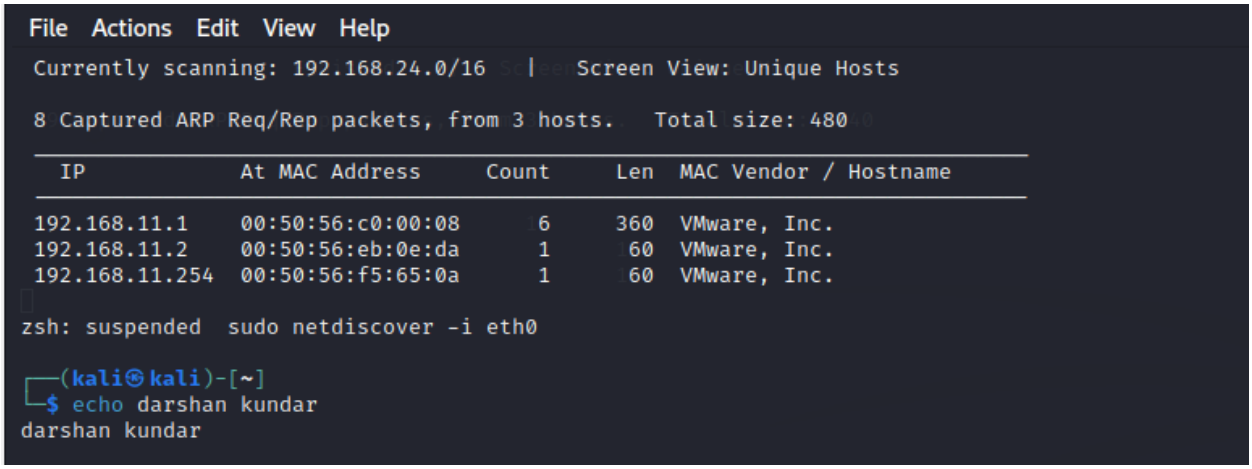
You can easily find packets once you have captured some packets or have read in a previously saved capture file. Simply select Edit Find Packet... in the main menu. Wireshark will open a toolbar between the main toolbar and the packet list, "The "Find Packet" toolbar".



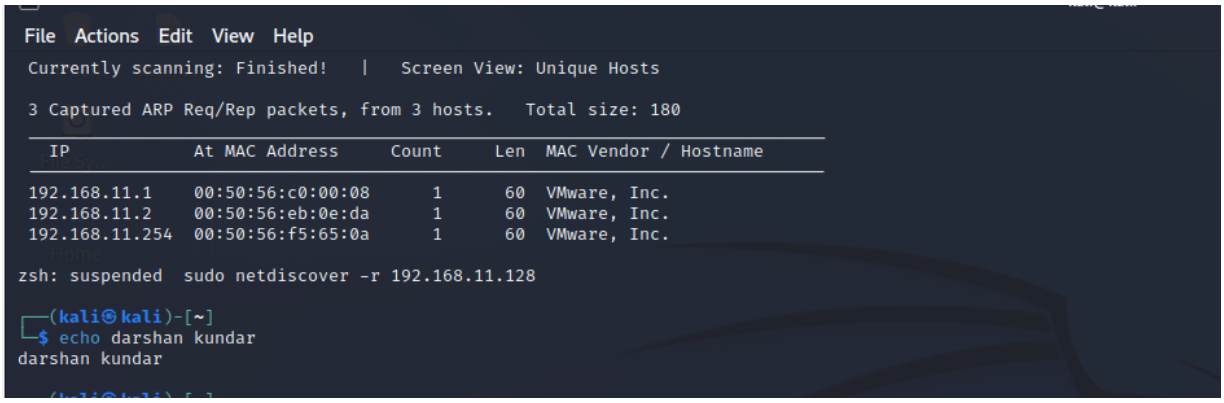
7.Any 5 netdiscover command:

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:

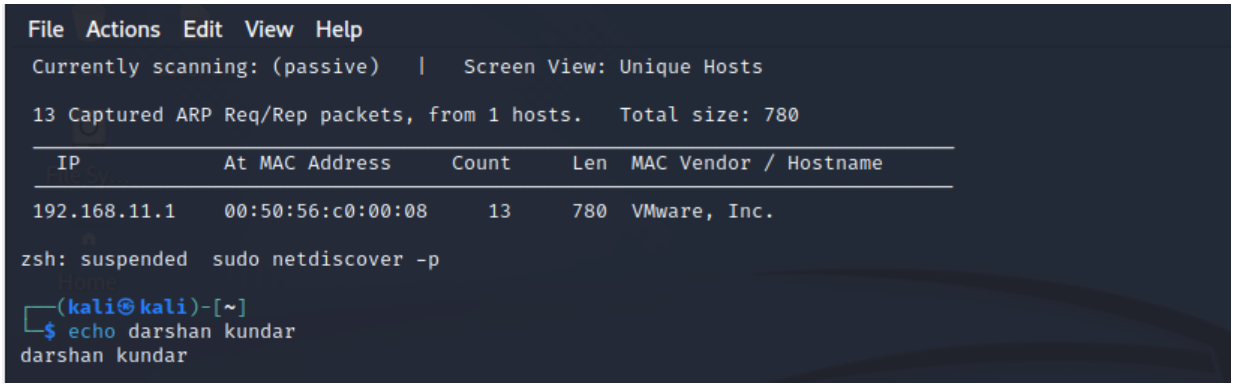
$ netdiscover -i eth0



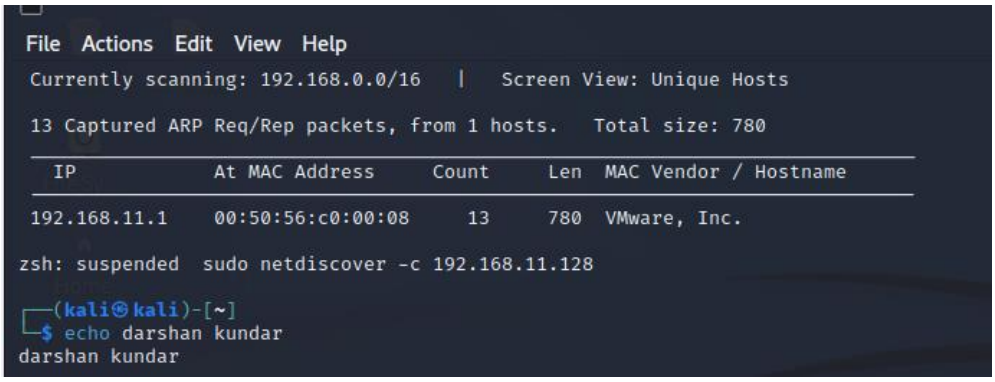
$ netdiscover -r 192.168.11.128



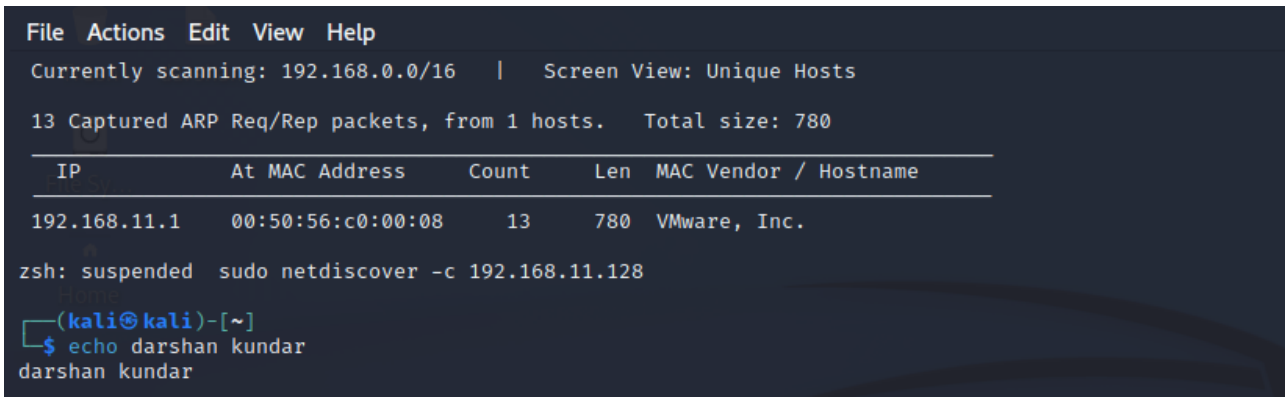
$ netdiscover -p



$ netdiscover -c 192.168.11.128

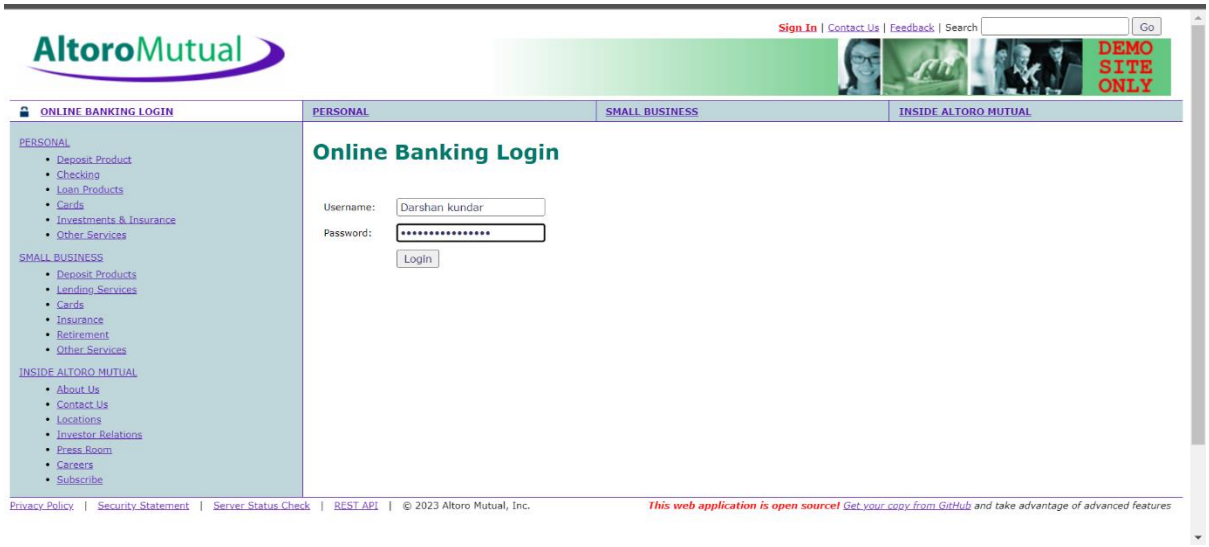


$ netdiscover –c 192.168.11.128



8.CryptoConfiguration Flaw:

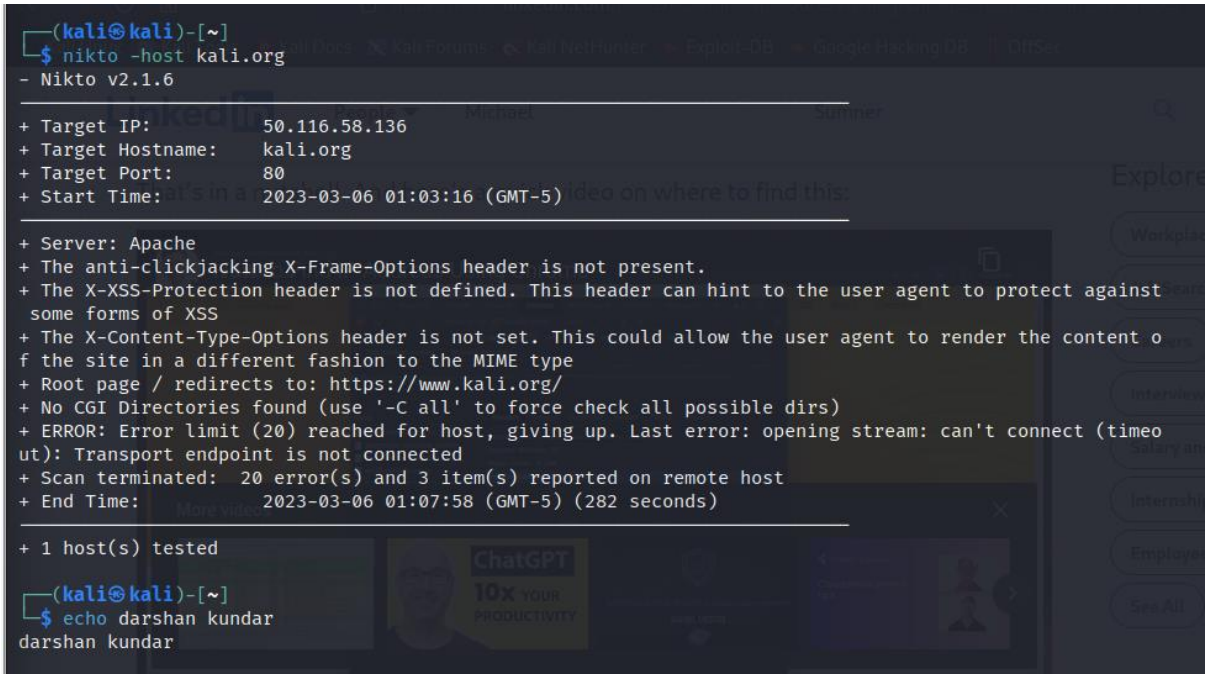
CryptoConfiguration typically refers to the configuration of cryptographic protocols and algorithms used to protect sensitive data and communications.A flaw is context could refers to a weakness or vulnarabilty in the configuration that could that could potentially be exploited by the attackers.



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



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.