Name:Ganesh Gowda

Reg No:145CS21702

Date:02-03-2023

Task:2

1.Perform IP address spoofing:

IP address spoofing is the act of falsifying the source IP address of a network packet to hide the identity of the sender or to impersonate another system.

$ ifconfig eth0 192.168.209.15

$ ifconfig

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.11.130  netmask 255.255.255.0  broadcast 192.168.11.255
        inet6 fe80::7b85:501d:ae77:6c46  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:7c:60:ab  txqueuelen 1000  (Ethernet)
        RX packets 204  bytes 12804 (12.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 42  bytes 4672 (4.5 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


┌──(kali㉿kali)-[~]
└─$ sudo ifconfig eth0 192.168.11.15
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.11.15  netmask 255.255.255.0  broadcast 192.168.11.255
        inet6 fe80::7b85:501d:ae77:6c46  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:7c:60:ab  txqueuelen 1000  (Ethernet)
        RX packets 204  bytes 12804 (12.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 42  bytes 4672 (4.5 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


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

2.Perform MAC address spoofing:

MAC address spoofing is the act of modifying the Media Access Control (MAC) address of a network interface to impersonate another device or to hide the identity of the sender.

$ macchanger -s eth0

$ ifconfig

$ macchanger -r eth0

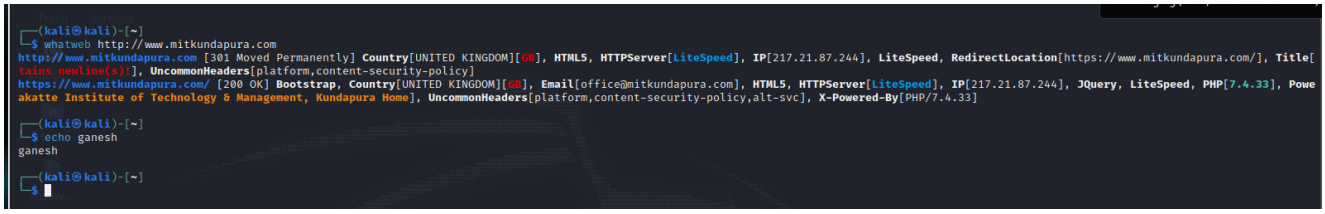
$ ifconfig eth0 down

3.Any 5 whatweb commands:

Basic scanning:

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

$ whatweb websiteURL

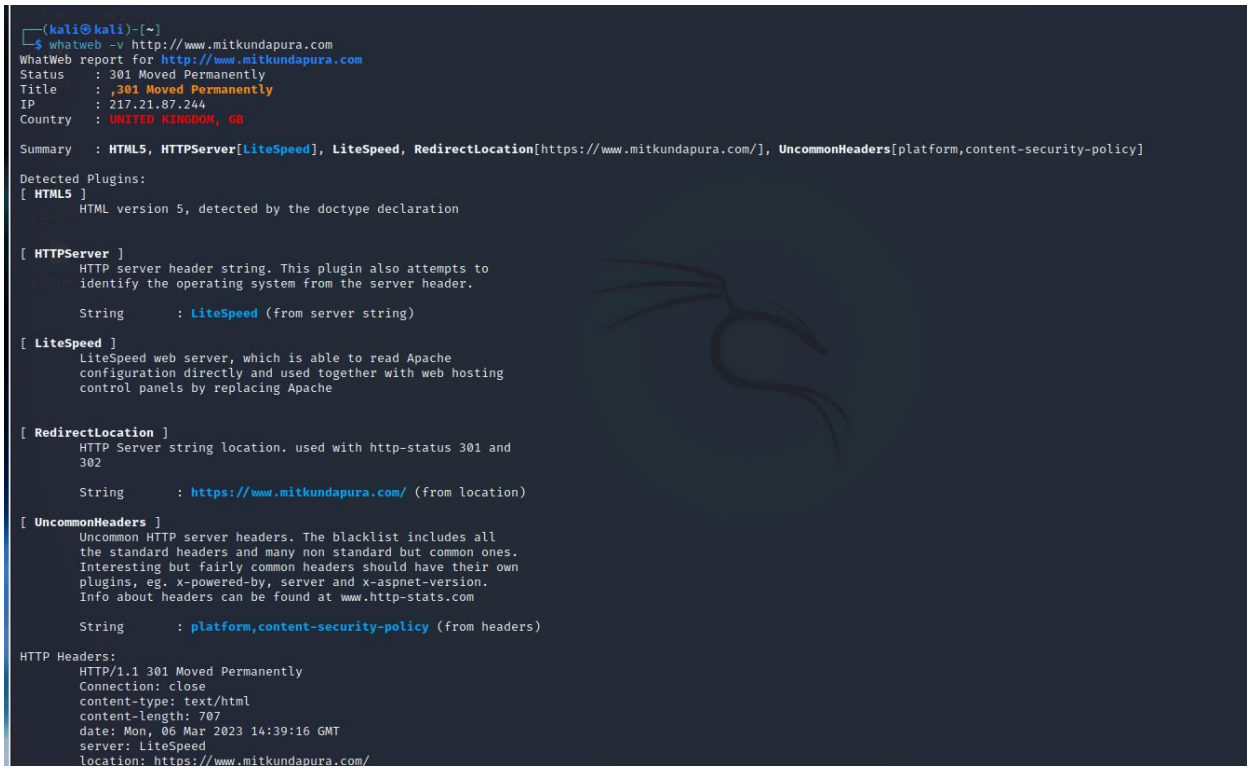


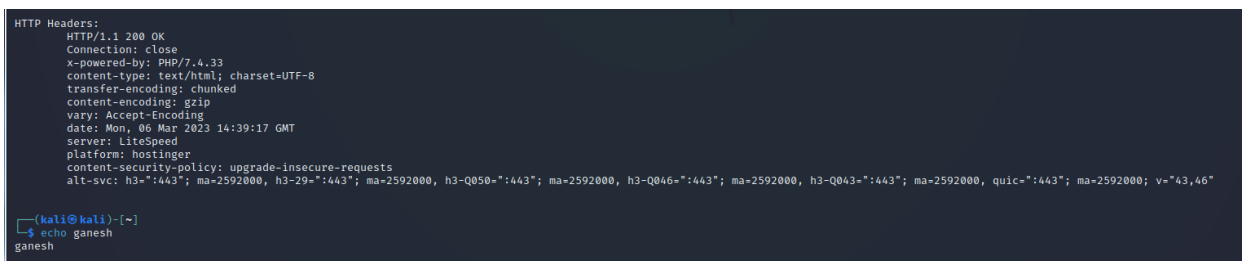
This will perform a default scan of the website and display the identified technologies.

Verbose scanning:

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

$ whatweb -v [website URL]



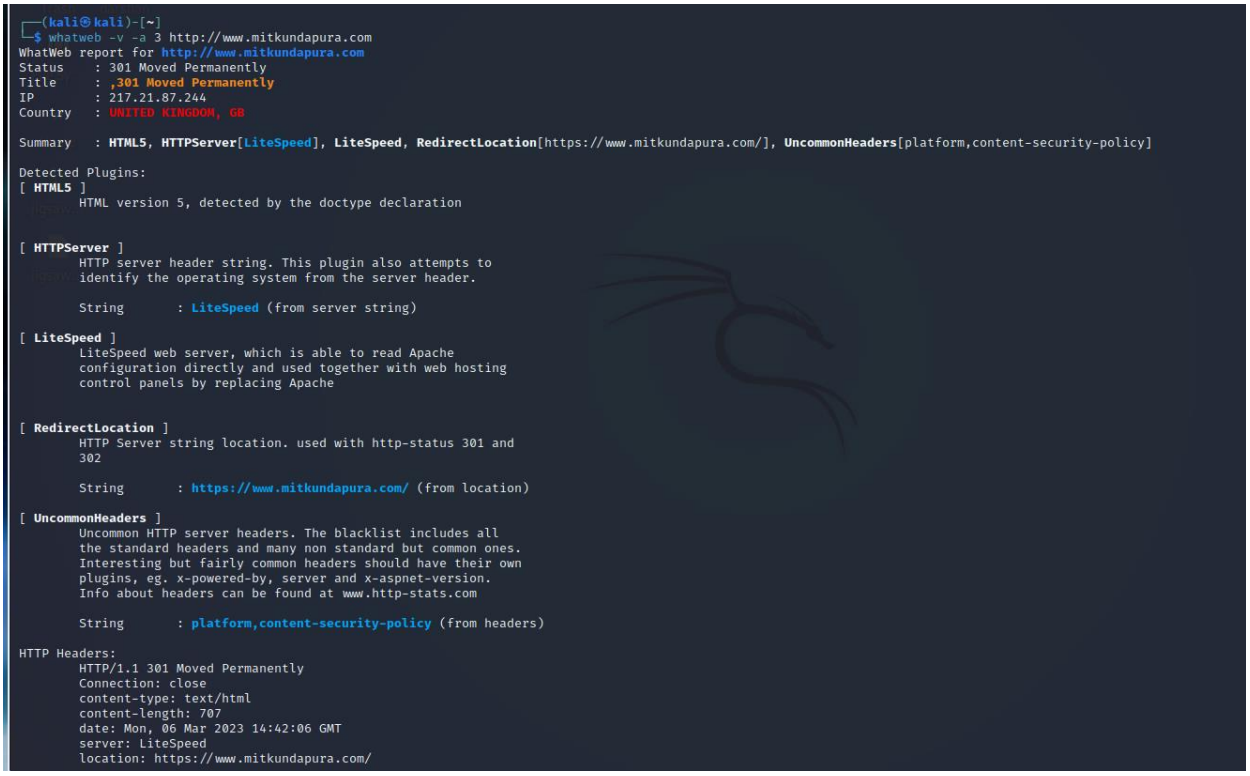


This will perform a more thorough scan and provide additional details, such as HTTP headers and server information.

$ whatweb –a 3 htttp://www.mitkundapura.com

$ whatweb --max –redirect 2 htttp://www.mitkundapura.com

$ whatweb –v –a 3 htttp://www.mitkundapura.com



4.Any 5 nslookup commands:

$ nslookup google.com

$ nslookup -type=mx mitkundapura.com

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

$ nslookup -type=ns mitkundapura.com

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

$ nslookup -type=a www.mitkundapura.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 ganesh
ganesh
```

$ nslookup -type=aaaa www.mitkundapura.com

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

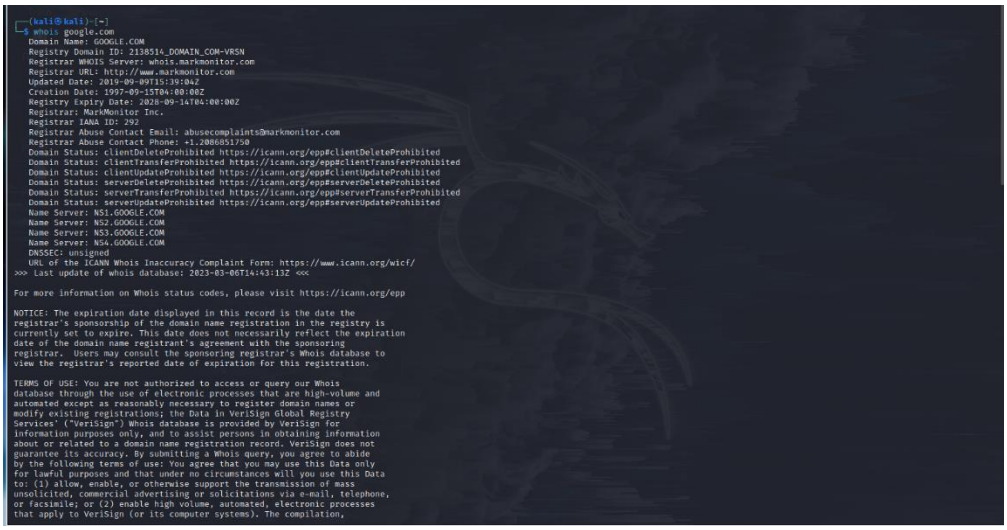
```
┌──(kali㉿kali)-[~]
└─$ nslookup -type=aaaa www.example.com
Server:         192.168.78.2
Address:        192.168.78.2#53

Non-authoritative answer:
Name:   www.example.com
Address: 2606:2800:220:1:248:1893:25c8:1946


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

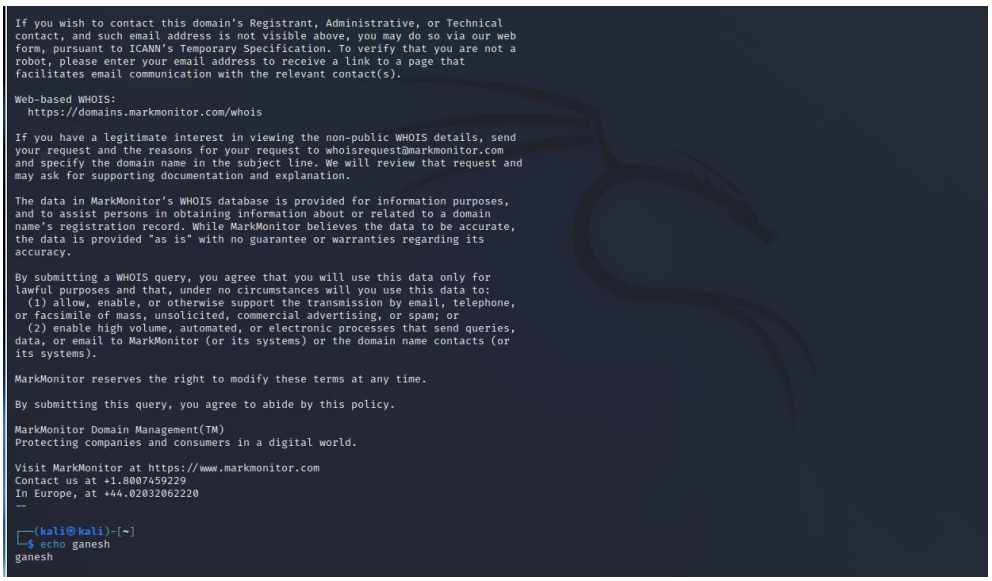
5.whois Commands:

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

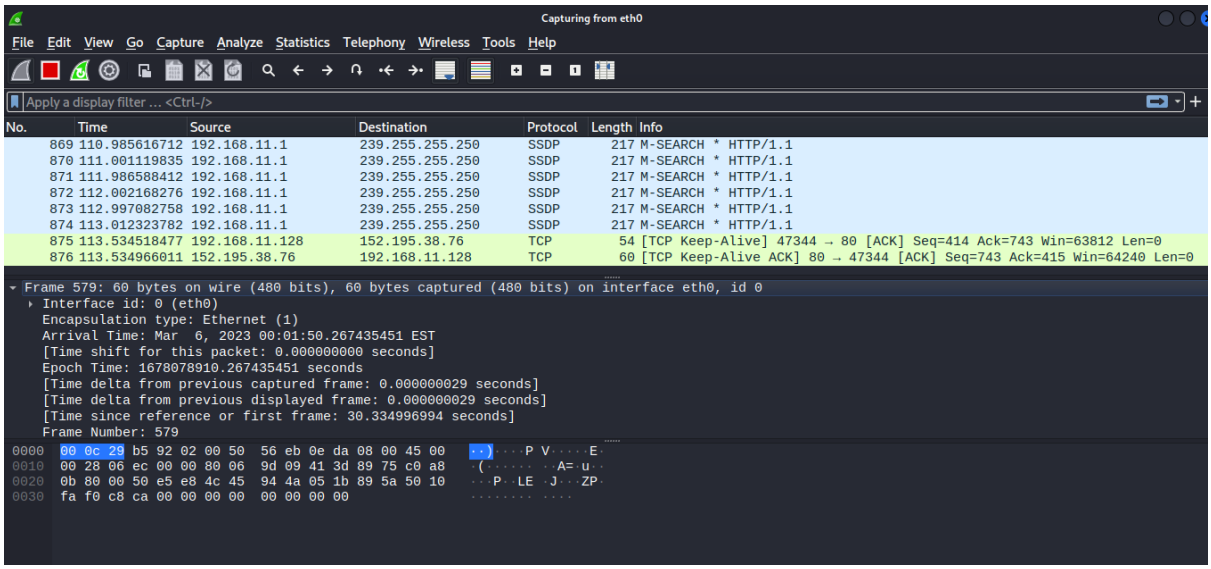




6.Find data packets using wireshark:

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".

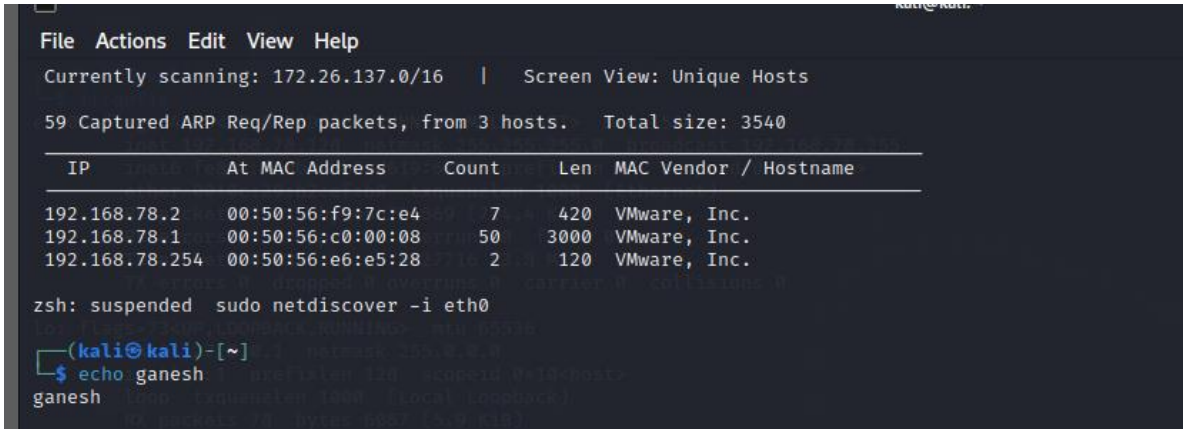
$wireshark



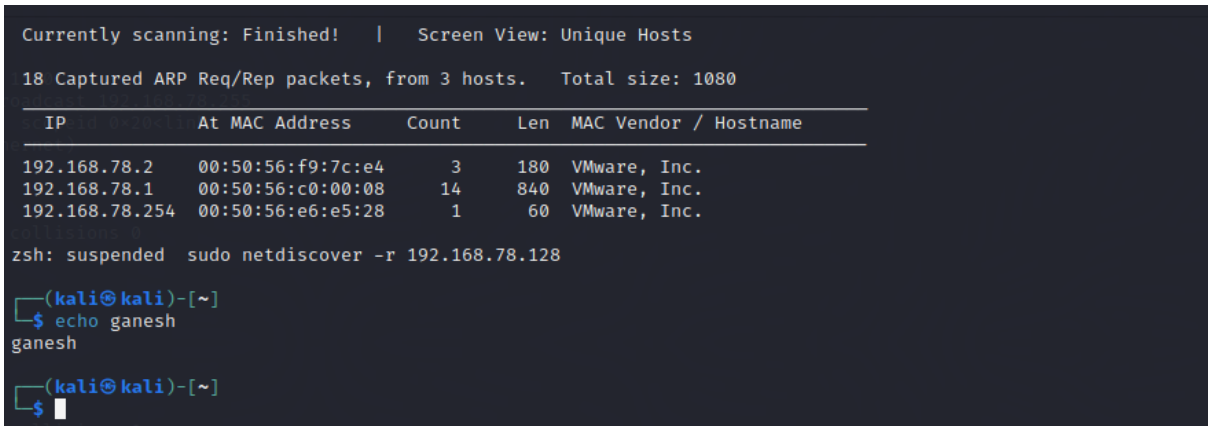
7.Any 5 netdiscover command:

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:

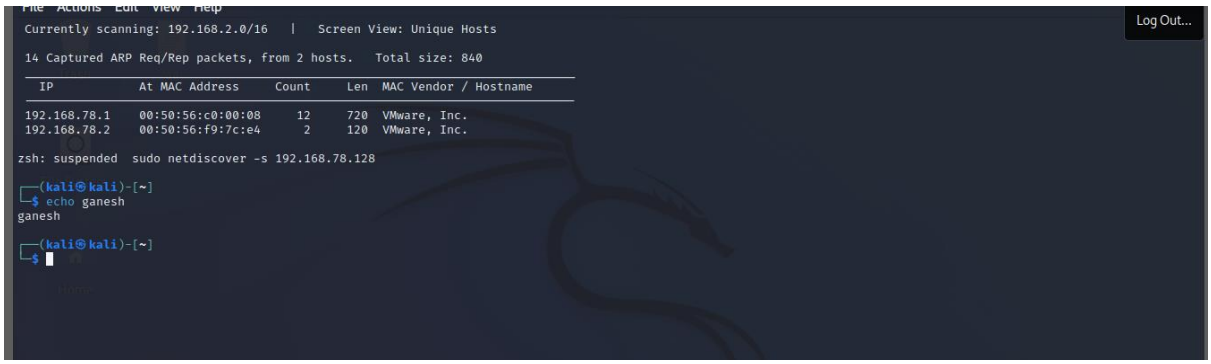
$ netdiscover -i eth0



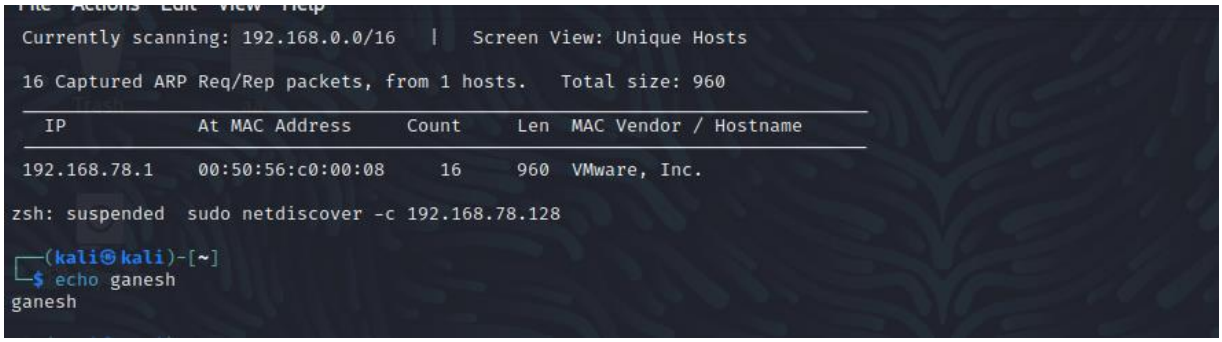
$ netdiscover -p



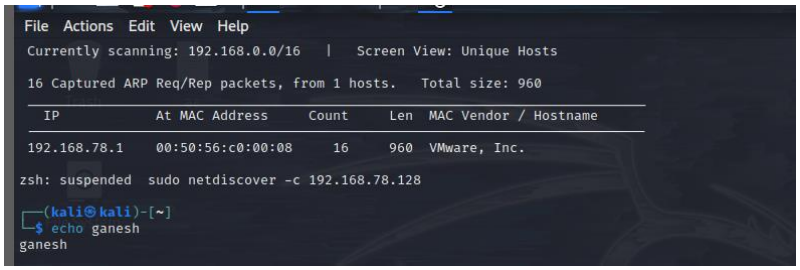
$ netdiscover -r 192.168.0.15



$ netdiscover -d -i eth0

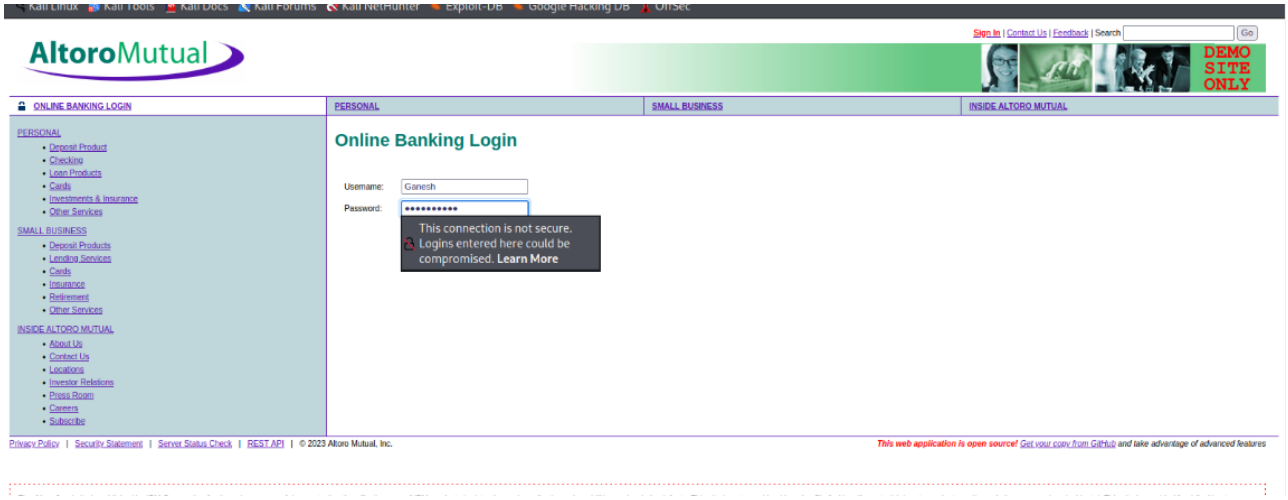


$ sudo netdiscover -c 192.168.11.128



8.CryptoConfiguration Flaw:

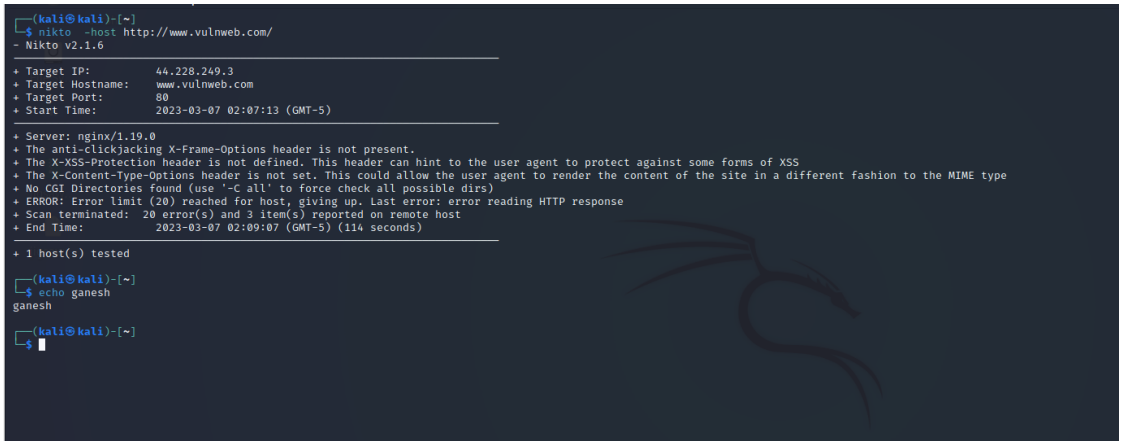
CryptoConfiguration typically refers to the configuration of cryptographic protocols and algorithms used to protect sensitive data and communications.A flaw is context could refers to a weakness or vulnarabilty in the configuration that could that could potentially be exploited by the attackers.



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 http://www.vulnweb.com/



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.