**University Cyber Attack**

**Task 1:** Obtaining a scanning the report of entire network and identifying how many terminals are connected with the Windows operating system and the Linux-based systems

**Solution:**

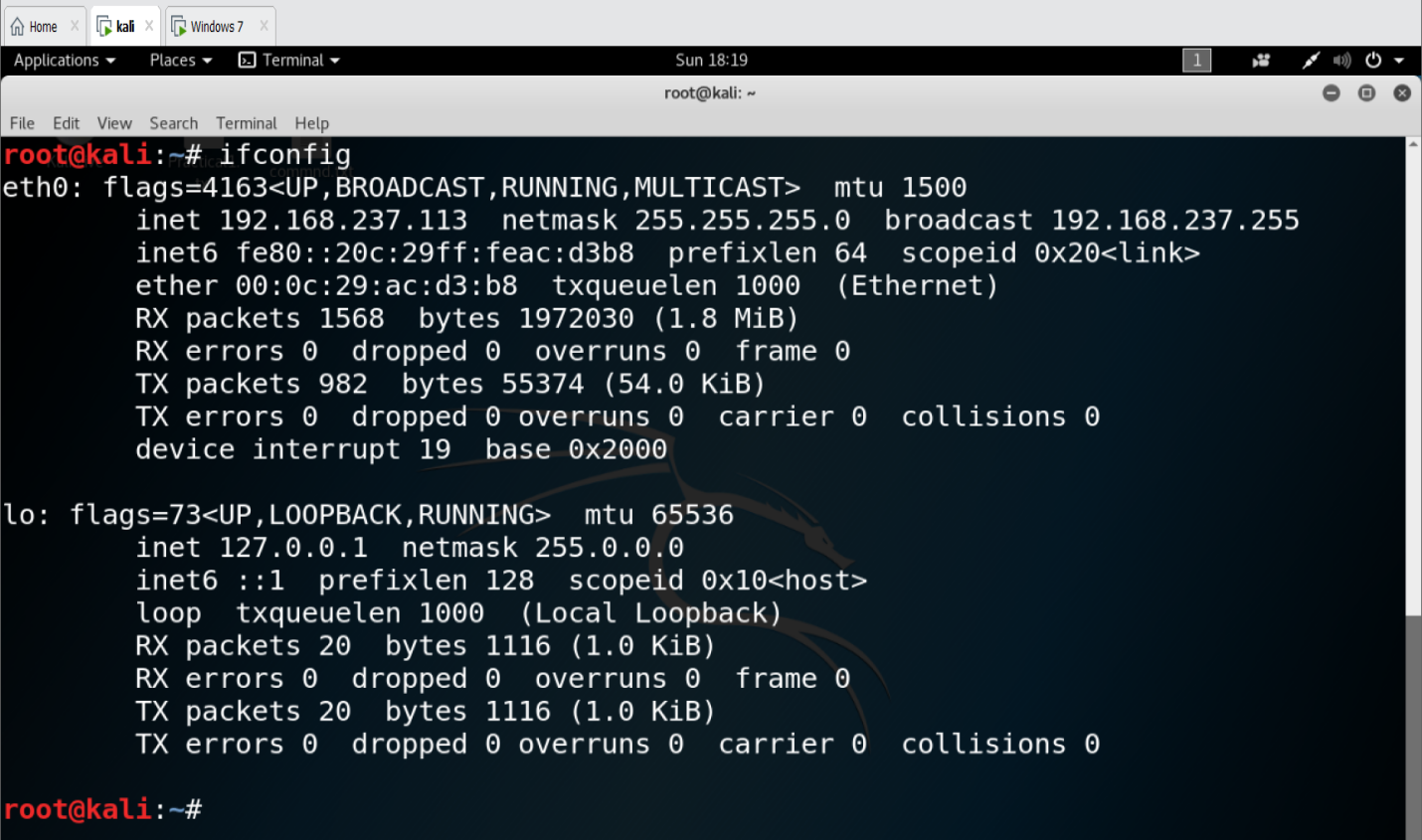
**A.**  Scang the server terminal for IP address and MAC address using the following command:

**# ifconfig**

IP address of Server

The screenshot of the output is given below:

MAC ID of Server

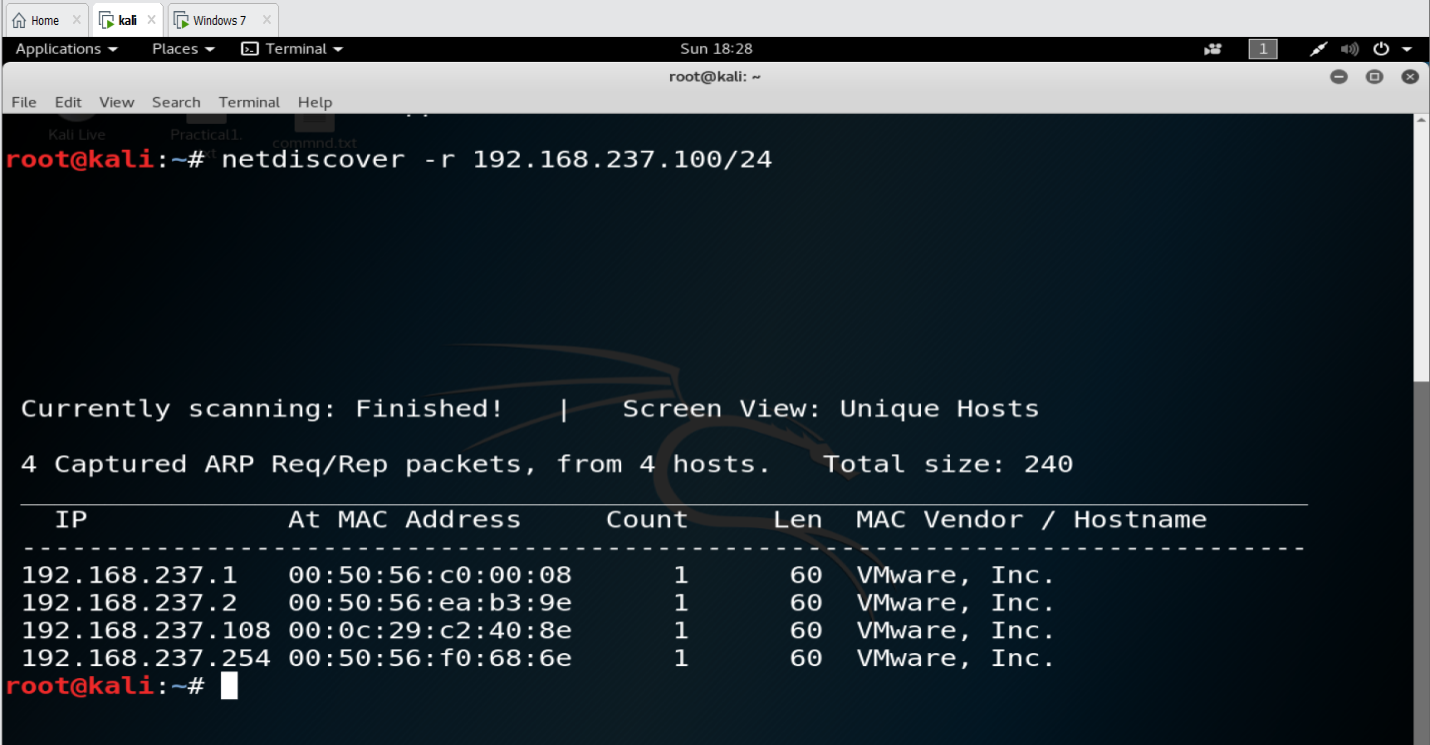


**B.** Run NET DISCOVER command for identifying all connected terminals with the server. .

**# netdiscover –r 192.168.237.100/24**

As the server IP is 192.168.237.113, which is a class C IP address, CIDR can be 24

The screenshot of the output is given below:



Default gateway of network is **192.168.237.2**

IP address of victim machine is **192.168.237.108**

Default IP of router is **192.168.237.1**

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

**#ping 192.168.237.108**

This command offers the No. of bytes sent by the server to the client and its ICMP sequence for every packet with its TTL value and time.

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 offers Windows Machines

TTL 63 offers Linux Machine

TTL 64 offers Mac Machine

TTL 40-55 offers Firewall

The screenshot of the output is given below:

****

**Summary:**

Server IP is **192.168.237.113**

Victim IP is **192.168.237.108**

**Total 1 terminal is connected with the server and the type of operating system is Windows**

**Task2:** Identify CVE score of victims vulnerability

Vulnerability search offers types of open ports and is available for use by anonymous users. To verify this, use following steps:

**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:**

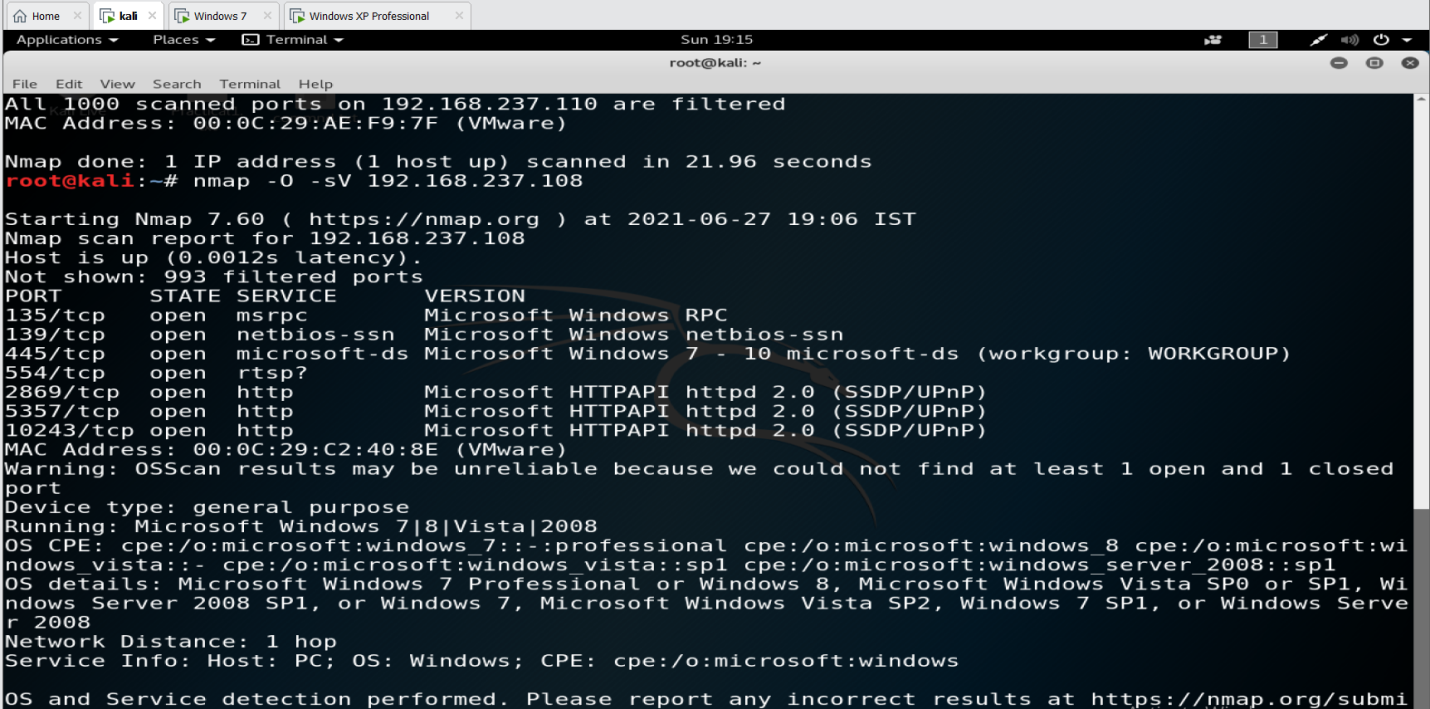
**#nmap target IP**

**#nmap 192.168.237.108**

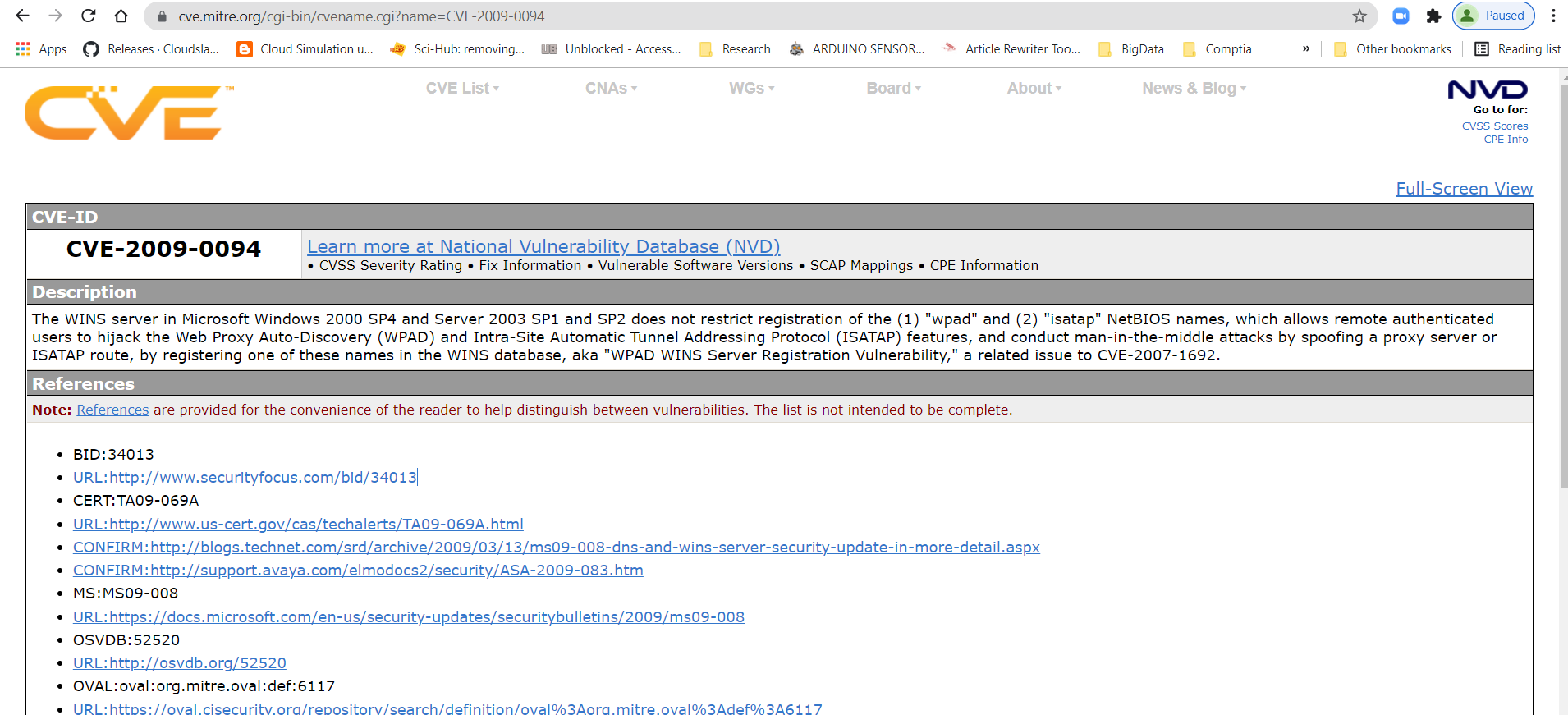
The screenshot of the output is given below:



**# Nmap –O –sV 192.168.237.108**

****

Check the CVE score for all open ports

****

**CVE -2009-0094 windows XP/2007 netBIOS**

**Score is 7**

**Task 3:** Identify whether the victims terminal is affected with MiMT attack or not and submit the incident report for the same.

As Samantha works in the university, and sometimes she would access the public network without the university VPN, it may be possible that her system could be affected by MiMT. To check this, the Incident Response Team was required to collect and check the footprinting of the victim's machine. To do the same, they had to follow the given steps:

**Possible conditions for an MiMT attack are:**

A. Unexpected or repeated disconnections of terminal with servers

B. Unknown or invalid addresses reported on URL bar

C. Connected with unsecure or open Wi-Fi

D. Network connections with unknown locations

**Possible checks to counter the above situations are:**

A. Regular inspections of Wi-Fi Connections

B. Routine Check of Malware

C. Use Network Sniffer tools

D. Apply Monitoring Scripts

**Using Wireshark to easily identify any unwanted sniffing into the network.**

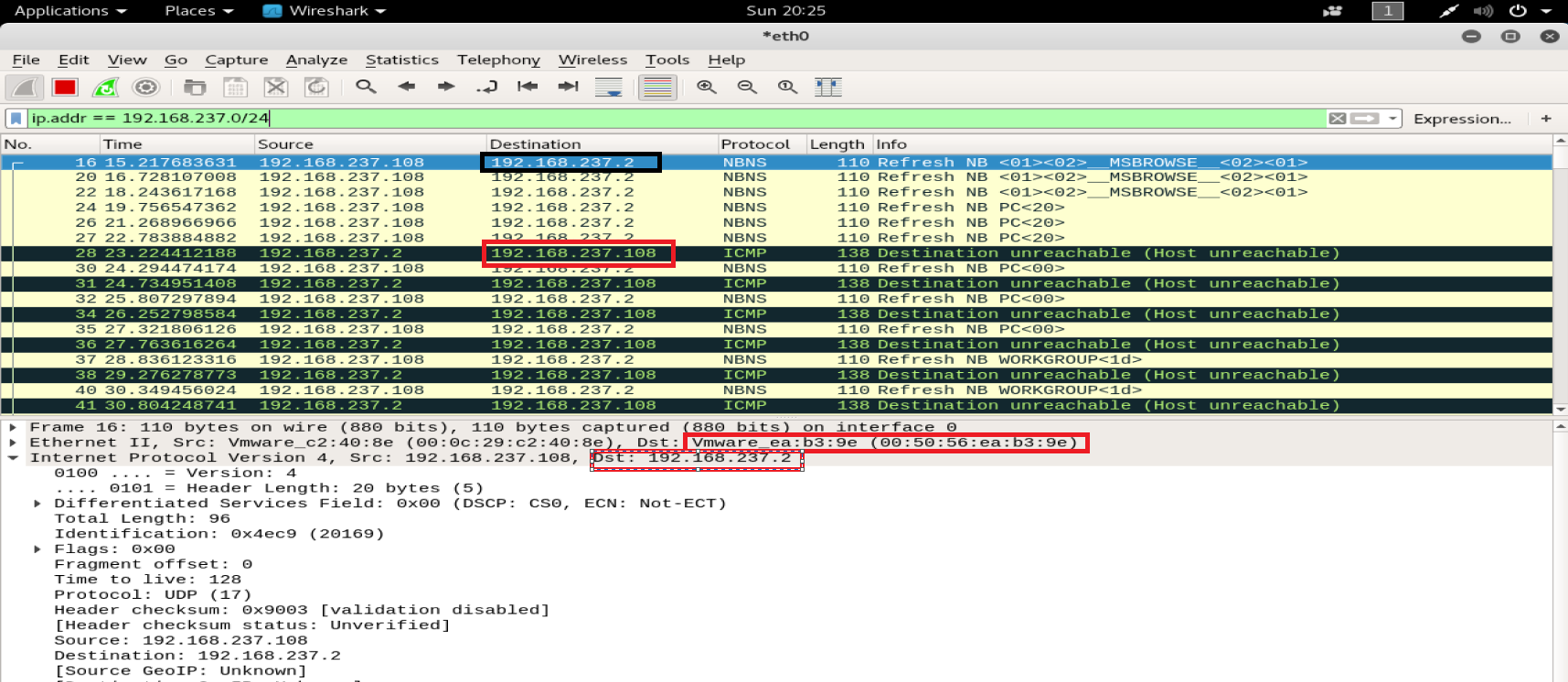
**Using the pcap file of the terminal, it was detected that if the condition is as following, then MiMT attack can be possible:**

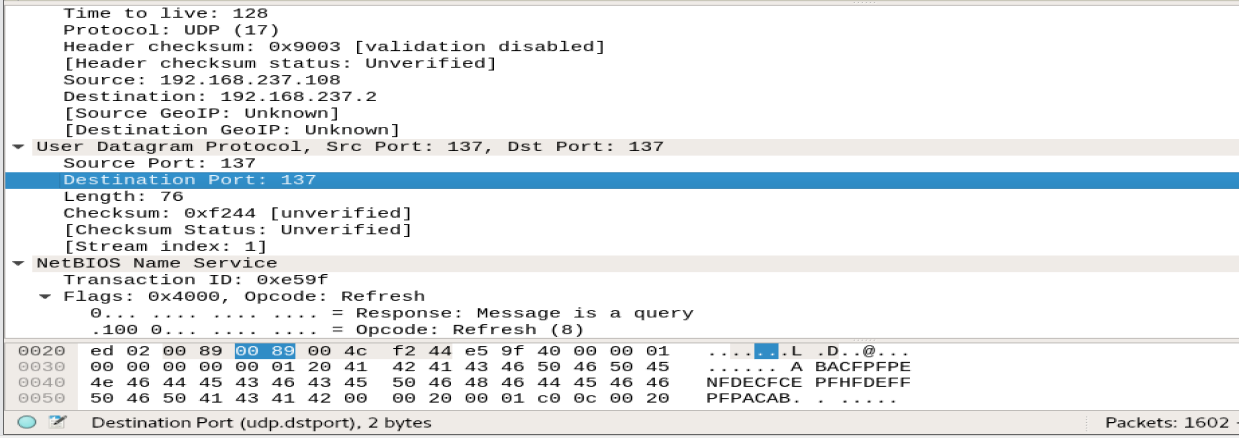
Default gateway IP is **192.168.237.2**

Victim machine IP is **192.168.237.108** (Marked as RED for MiMT attack as the message is 138 destination unreachable (Host Unreachable)

MAC address of source is **(00:0c:29:c2:40:8e)**

MAC address of destination is **(00:50:56:ea:b3:9e)**

****

****

**Entry port is 137. Therefore NetBIOS is used for entry.**

**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 192.168.237.113**

**Victim IP is 192.168.237.108**

**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 192.168.237.2**

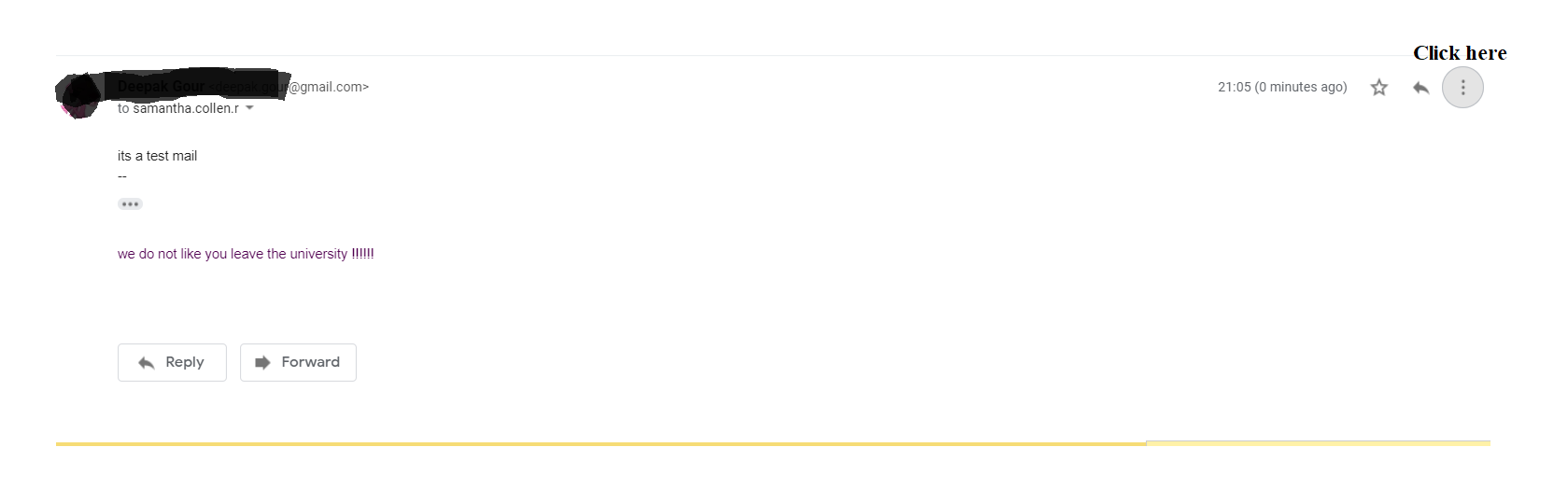
**Victim Machine IP is 192.168.237.108** (Marked as RED for MiMT attack as message is 138 Destination unreachable (Host Unreachable)

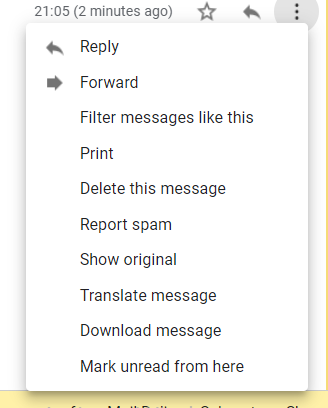
**MAC address of source is (00:0c:29:c2:40:8e)**

**MAC address of Destination is (00:50:56:ea:b3:9e)**

**Entry port is 137 (NetBIOS) is use for entry**

**Task 4:** Use email forensics analysis to identify the address location of sender’s IP

****

****

**It will offer following details:**

MIME-Version: 1.0

Date: Sun, 27 Jun 2021 21:05:56 +0530

References: <CAA7z9VfC4od73fdsFxwSu0=WzRuxxMFErbgwkXEwkyS\_x3sNtQ@mail.gmail.com>

In-Reply-To: <CAA7z9VfC4od73fdsFxwSu0=WzRuxxMFErbgwkXEwkyS\_x3sNtQ@mail.gmail.com>

Message-ID: <CAA7z9Vdv0OvSCQE6edHj0j9DB2cQ95iA-CVDhCYGn5AFa9OMmw@mail.gmail.com>

Subject: Fwd:

From: xxxxxxx <xxxx.xoxr@gmail.com>

To: samantha.collen.r@gmail.com

Content-Type: multipart/alternative; boundary="00000000000005a45905c5c12101"

--00000000000005a45905c5c12101

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

its a test mail

--

we do not like you leave the university !!!!!!

--00000000000005a45905c5c12101

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

Content-Transfer-Encoding: quoted-printable

<div dir=3D"ltr"><br>its a test mail=C2=A0<br><div class=3D"gmail\_quote"><d=

iv dir=3D"ltr" class=3D"gmail\_attr">--</div><br><div dir=3D"ltr">we do not =

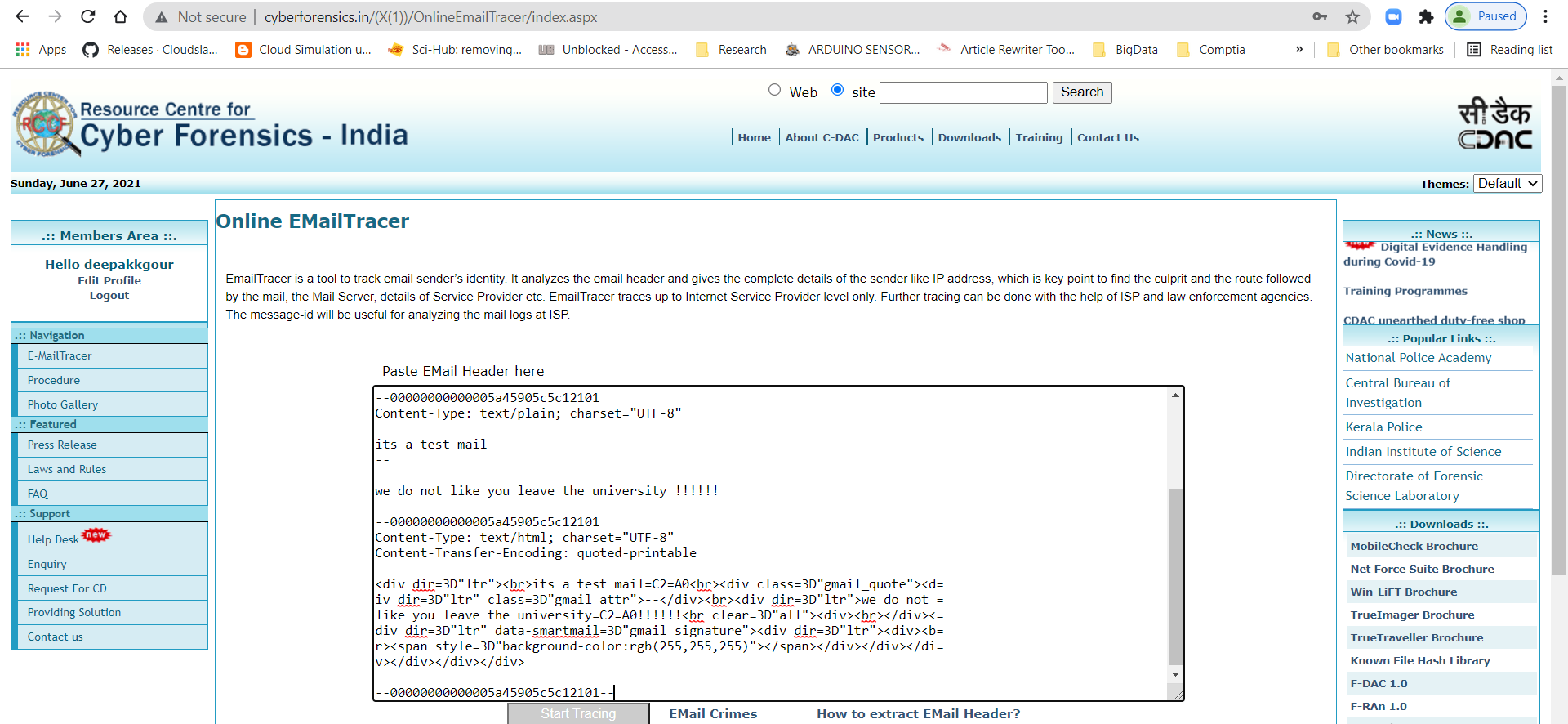
like you leave the university=C2=A0!!!!!!<br clear=3D"all"><div><br></div><=

div dir=3D"ltr" data-smartmail=3D"gmail\_signature"><div dir=3D"ltr"><div><b=

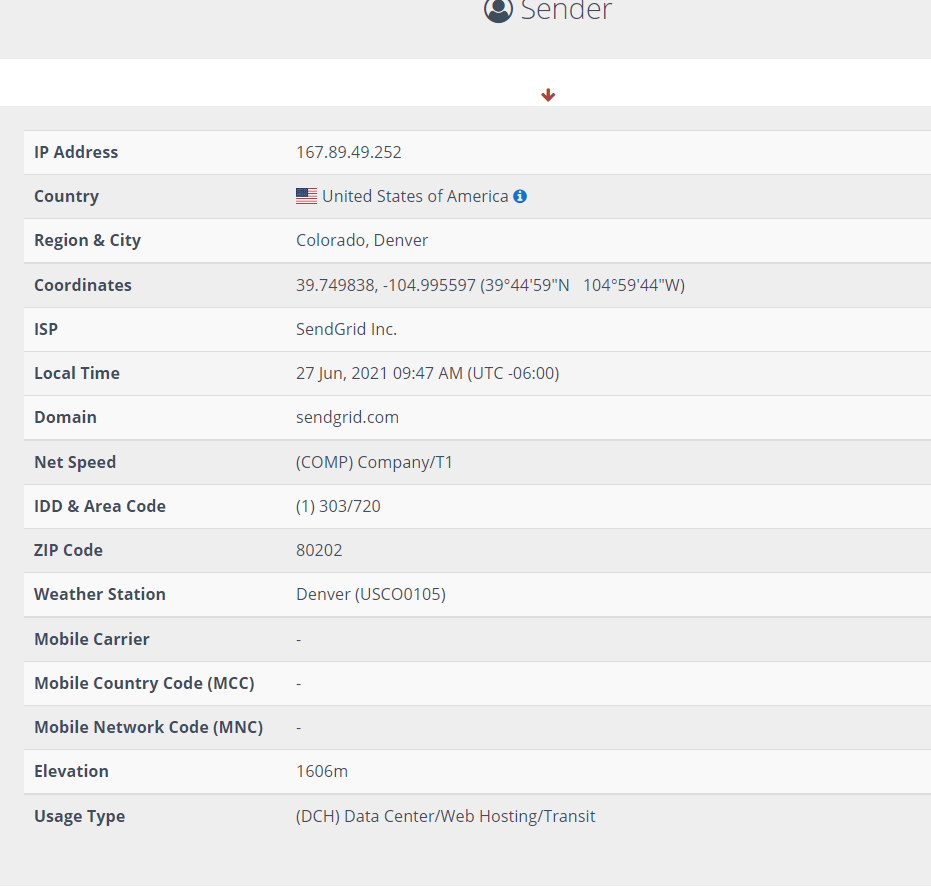
r><span style=3D"background-color:rgb(255,255,255)"></span></div></div></di=

v></div></div></div>

--00000000000005a45905c5c12101--

****

**It offers the following response:**

****

**Task5:** Submit complete incident report

**Incident Description:**

|  |  |
| --- | --- |
| **Threat Description** | Credential hijacking using Man-in-the-Middle attack |
| **Threat Target** | University faculty Samantha |
| **Attack Techniques** | Social Engineering and Footprinting with Man-in-the-Middle Attack (MiMT) |
| **Controls/**  **Countermeasures** | Banner grabbing and identifying vulnerable ports, Compromising victim’s machine with MiMT attack and hijacking of credentials |
| **Artifact Hijacked** | Personal email ID of victim ( samantha.collen.r@gmail.com) |
| **Threat Statement** |  |
| **Collected Artifacts From Incident Response Team Other Collected Artifacts** | Server IP is **192.168.237.113**  Victim IP is **192.168.237.108**  **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 **192.168.237.2**  Victim Machine IP is **192.168.237.108** (Marked as RED for MiMT attack as message is 138 Destination unreachable (Host Unreachable)  MAC address of source is **(00:0c:29:c2:40:8e)**  MAC address of Destination is **(00:50:56:ea:b3:9e)**  **Entry port is 137. Therefore, NetBIOS is used for entry** |
| **Attacker Email Summary** | **Email forensic analysis with original source:** |
| **E-Mail Forensic Summary** |  |