Date:05/05/2023

Created By

SABIH KHAN

Cyber Security Project

(Simplilearn)

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: For successful attainment of IRT, you need to perform the following actions:

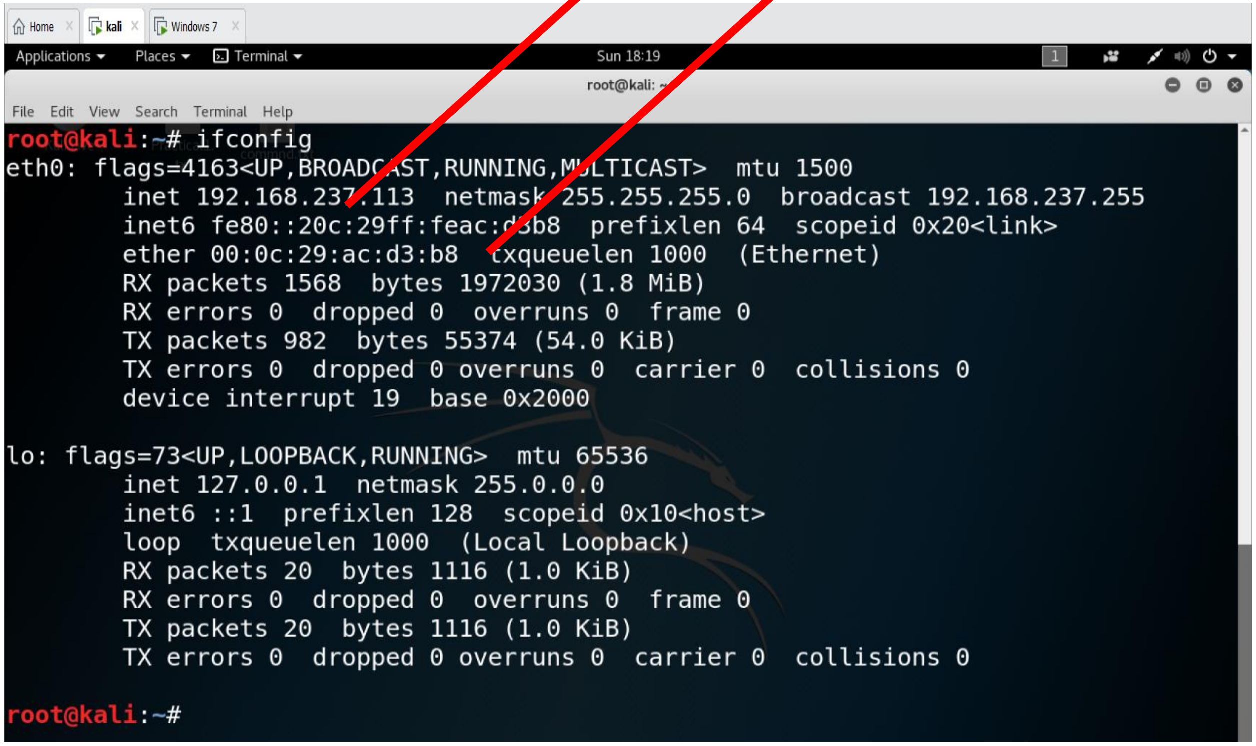
A. Scang the server terminal for IP address and MAC address using the following command:

ifconfig

The screenshot of the output is given below:

IP address of Server

MAC ID of Server



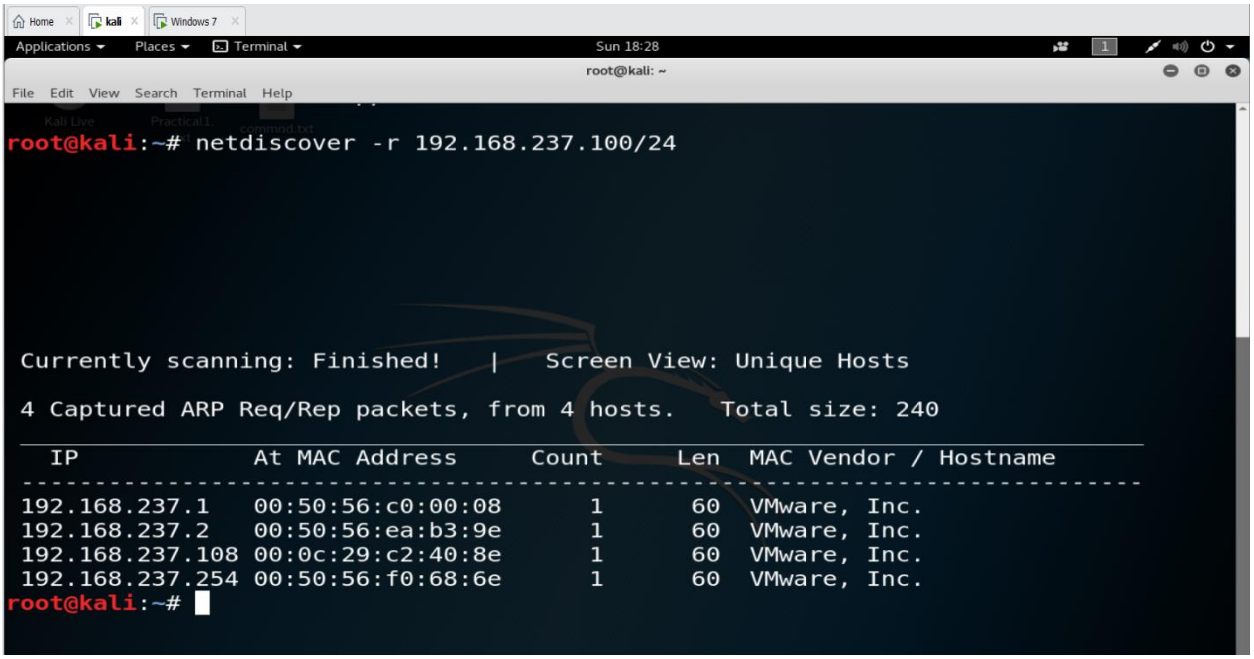
```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.237.113  netmask 255.255.255.0  broadcast 192.168.237.255
        inet6 fe80::20c:29ff:feac:d3b8  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:ac:d3:b8  txqueuelen 1000  (Ethernet)
        RX packets 1568  bytes 1972030 (1.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 982  bytes 55374 (54.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  base 0x2000

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 20  bytes 1116 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1116 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~#
```

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:



```
root@kali:~# netdiscover -r 192.168.237.100/24

 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
 -----------------------------------------------------------------------------
 192.168.237.1   00:50:56:c0:00:08      1      60  VMware, Inc.
 192.168.237.2   00:50:56:ea:b3:9e      1      60  VMware, Inc.
 192.168.237.108 00:0c:29:c2:40:8e      1      60  VMware, Inc.
 192.168.237.254 00:50:56:f0:68:6e      1      60  VMware, Inc.
root@kali:~# 
```

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.

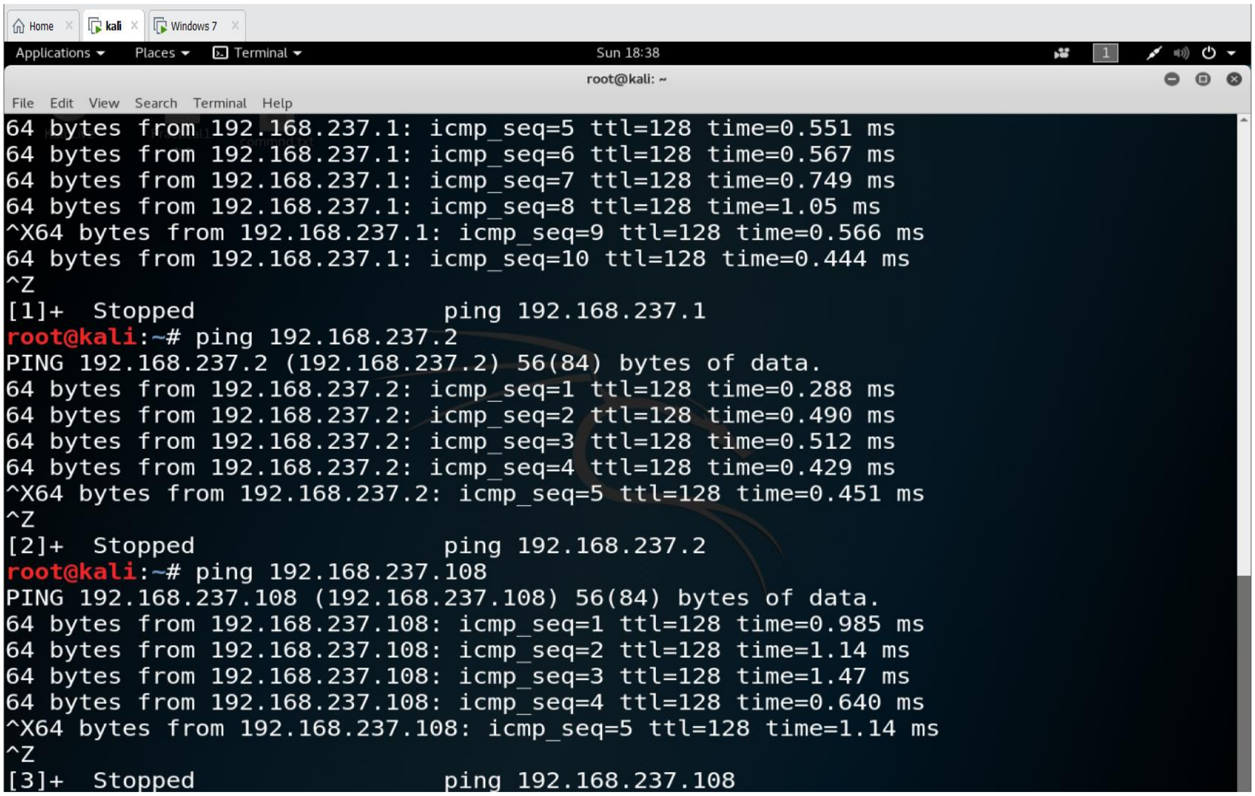
#ping 192.168.237.108

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:



```
64 bytes from 192.168.237.1: icmp_seq=5 ttl=128 time=0.551 ms
64 bytes from 192.168.237.1: icmp_seq=6 ttl=128 time=0.567 ms
64 bytes from 192.168.237.1: icmp_seq=7 ttl=128 time=0.749 ms
64 bytes from 192.168.237.1: icmp_seq=8 ttl=128 time=1.05 ms
^X64 bytes from 192.168.237.1: icmp_seq=9 ttl=128 time=0.566 ms
64 bytes from 192.168.237.1: icmp_seq=10 ttl=128 time=0.444 ms
^Z
[1]+  Stopped                 ping 192.168.237.1
root@kali:~# ping 192.168.237.2
PING 192.168.237.2 (192.168.237.2) 56(84) bytes of data.
64 bytes from 192.168.237.2: icmp_seq=1 ttl=128 time=0.288 ms
64 bytes from 192.168.237.2: icmp_seq=2 ttl=128 time=0.490 ms
64 bytes from 192.168.237.2: icmp_seq=3 ttl=128 time=0.512 ms
64 bytes from 192.168.237.2: icmp_seq=4 ttl=128 time=0.429 ms
^X64 bytes from 192.168.237.2: icmp_seq=5 ttl=128 time=0.451 ms
^Z
[2]+  Stopped                 ping 192.168.237.2
root@kali:~# ping 192.168.237.108
PING 192.168.237.108 (192.168.237.108) 56(84) bytes of data.
64 bytes from 192.168.237.108: icmp_seq=1 ttl=128 time=0.985 ms
64 bytes from 192.168.237.108: icmp_seq=2 ttl=128 time=1.14 ms
64 bytes from 192.168.237.108: icmp_seq=3 ttl=128 time=1.47 ms
64 bytes from 192.168.237.108: icmp_seq=4 ttl=128 time=0.640 ms
^X64 bytes from 192.168.237.108: icmp_seq=5 ttl=128 time=1.14 ms
^Z
[3]+  Stopped                 ping 192.168.237.108
```

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

Once you identify the relevant information about the environment, it's time to perform an autopsy of the victim's machine.

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

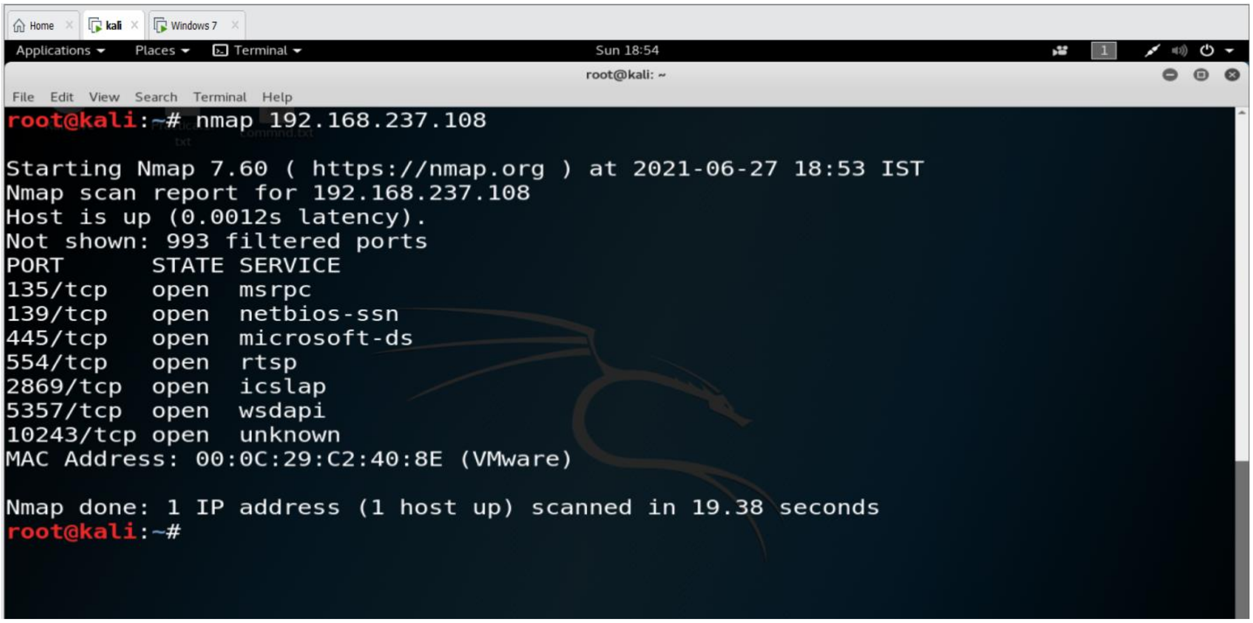
B. Once you receive the port information, check the type of vulnerability with the CVE score portal of the NVD.

Commands:

#nmap target IP

#nmap 192.168.237.108

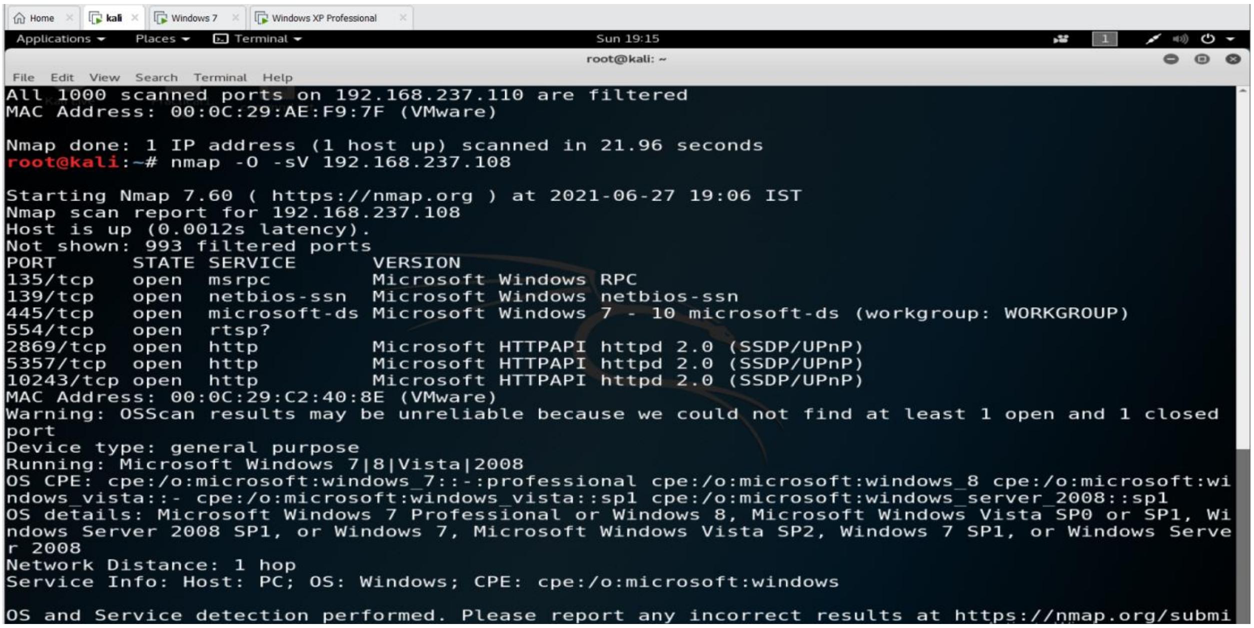
The screenshot of the output is given below:



```
root@kali:~# nmap 192.168.237.108

Starting Nmap 7.60 ( https://nmap.org ) at 2021-06-27 18:53 IST
Nmap scan report for 192.168.237.108
Host is up (0.0012s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
MAC Address: 00:0C:29:C2:40:8E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 19.38 seconds
root@kali:~#
```

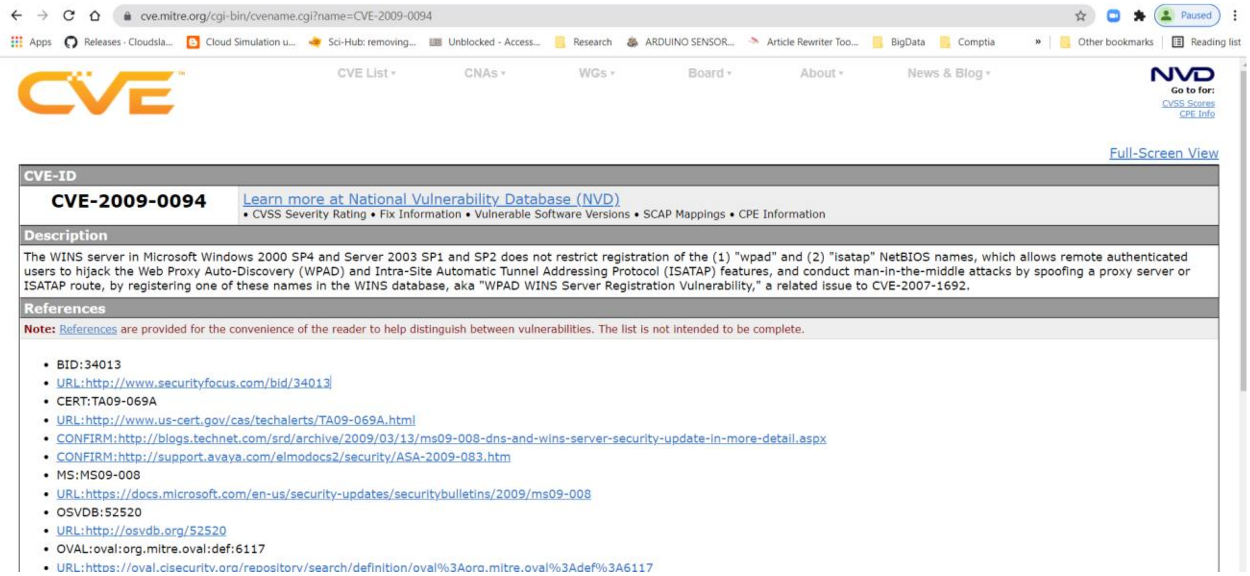
Use the following command to check the vulnerability:

# Nmap –O –sV 192.168.237.108



```
All 1000 scanned ports on 192.168.237.110 are filtered
MAC Address: 00:0C:29:AE:F9:7F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.96 seconds
root@kali:~# nmap -O -sV 192.168.237.108

Starting Nmap 7.60 ( https://nmap.org ) at 2021-06-27 19:06 IST
Nmap scan report for 192.168.237.108
Host is up (0.0012s latency).
Not shown: 993 filtered ports
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)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 00:0C:29:C2:40:8E (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed
port
Device type: general purpose
Running: Microsoft Windows 7|8|Vista|2008
OS CPE: cpe:/o:microsoft:windows_7::-:professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:wi
ndows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1
OS details: Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Vista SP0 or SP1, Wi
ndows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Serve
r 2008
Network Distance: 1 hop
Service Info: Host: PC; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submi
```

Check the CVE score for all open ports



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
- OVAL:oval:org.mitre.oval:def:6117
- URL:https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A6117

CVE -2009-0094 windows XP/2007 netBIOS
Source link: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0094
Score is 5.5 According to CVSS 2.0

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:

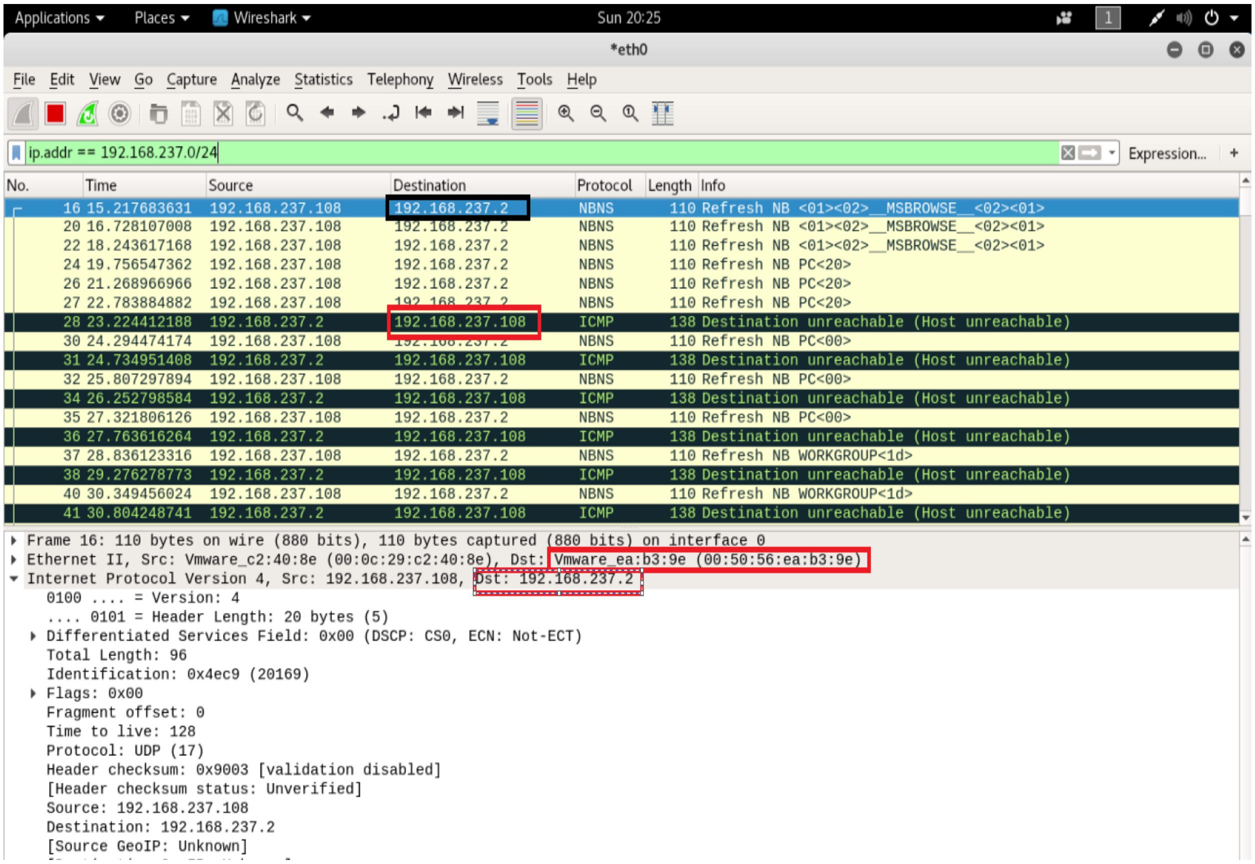
Possible conditions for an MiMT attack are:
A. Unexpected or repeated disconnections of terminal with servers
B. Unknown or invalid addresses reported on URL bar
C. Connected with unsecure or open Wi-Fi
D. Network connections with unknown locations

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

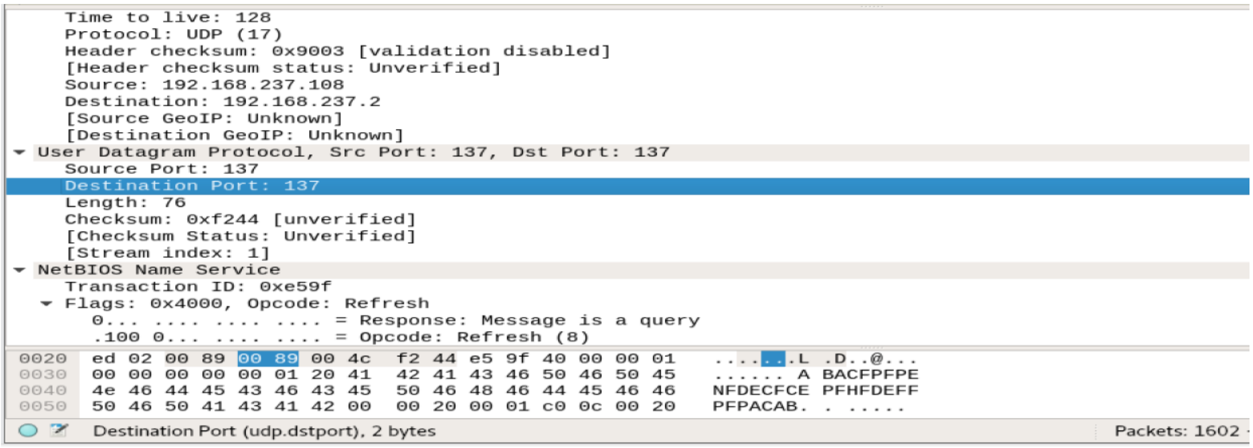
Note: Using Wireshark allows you to easily identify any unwanted sniffing into the network.

For Example: 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)**


Applications
Places
Wireshark
Sun 20:25
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

```
ip.addr == 192.168.237.0/24

No.  Time           Source           Destination      Protocol Length Info
  16 15.217683631  192.168.237.108  192.168.237.2    NBNS      110 Refresh NB <01><02>__MSBROWSE__<02><01>
  20 16.728107008  192.168.237.108  192.168.237.2    NBNS      110 Refresh NB <01><02>__MSBROWSE__<02><01>
  22 18.243617168  192.168.237.108  192.168.237.2    NBNS      110 Refresh NB <01><02>__MSBROWSE__<02><01>
  24 19.756547362  192.168.237.108  192.168.237.2    NBNS      110 Refresh NB PC<20>
  26 21.268966966  192.168.237.108  192.168.237.2    NBNS      110 Refresh NB PC<20>
  27 22.783884882  192.168.237.108  192.168.237.2    NBNS      110 Refresh NB PC<20>
  28 23.224412188  192.168.237.2    192.168.237.108  ICMP      138 Destination unreachable (Host unreachable)
  30 24.294474174  192.168.237.108  192.168.237.2    NBNS      110 Refresh NB PC<00>
  31 24.734951408  192.168.237.2    192.168.237.108  ICMP      138 Destination unreachable (Host unreachable)
  32 25.807297894  192.168.237.108  192.168.237.2    NBNS      110 Refresh NB PC<00>
  34 26.252798584  192.168.237.2    192.168.237.108  ICMP      138 Destination unreachable (Host unreachable)
  35 27.321806126  192.168.237.108  192.168.237.2    NBNS      110 Refresh NB PC<00>
  36 27.763616264  192.168.237.2    192.168.237.108  ICMP      138 Destination unreachable (Host unreachable)
  37 28.836123316  192.168.237.108  192.168.237.2    NBNS      110 Refresh NB WORKGROUP<1d>
  38 29.276278773  192.168.237.2    192.168.237.108  ICMP      138 Destination unreachable (Host unreachable)
  40 30.349456024  192.168.237.108  192.168.237.2    NBNS      110 Refresh NB WORKGROUP<1d>
  41 30.804248741  192.168.237.2    192.168.237.108  ICMP      138 Destination unreachable (Host unreachable)

▸ Frame 16: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
▸ Ethernet II, Src: Vmware_c2:40:8e (00:0c:29:c2:40:8e), Dst: Vmware_ea:b3:9e (00:50:56:ea:b3:9e)
▾ Internet Protocol Version 4, Src: 192.168.237.108, Dst: 192.168.237.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 96
    Identification: 0x4ec9 (20169)
  ▸ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0x9003 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.237.108
    Destination: 192.168.237.2
    [Source GeoIP: Unknown]
```



```
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0x9003 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.237.108
    Destination: 192.168.237.2
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▾ User Datagram Protocol, Src Port: 137, Dst Port: 137
    Source Port: 137
    Destination Port: 137
    Length: 76
    Checksum: 0xf244 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
▾ NetBIOS Name Service
    Transaction ID: 0xe59f
  ▾ Flags: 0x4000, Opcode: Refresh
      0... .... .... .... = Response: Message is a query
      .100 0... .... .... = Opcode: Refresh (8)

0020  ed 02 00 89 00 89 00 4c  f2 44 e5 9f 40 00 00 01   .......L .D..@...
0030  00 00 00 00 00 01 20 41  42 41 43 46 50 46 50 45   ...... A BACFPFPE
0040  4e 46 44 45 43 46 43 45  50 46 48 46 44 45 46 46   NFDECFCE PFHFDEFF
0050  50 46 50 41 43 41 42 00  00 20 00 01 c0 0c 00 20   PFPACAB. . .....

Destination Port (udp.dstport), 2 bytes                                   Packets: 1602
```

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

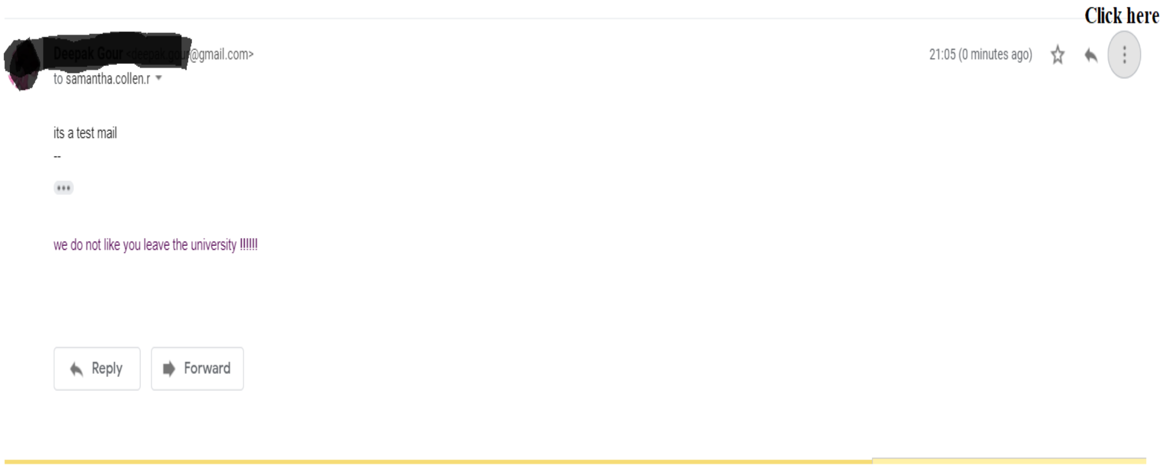
Summary:

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

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

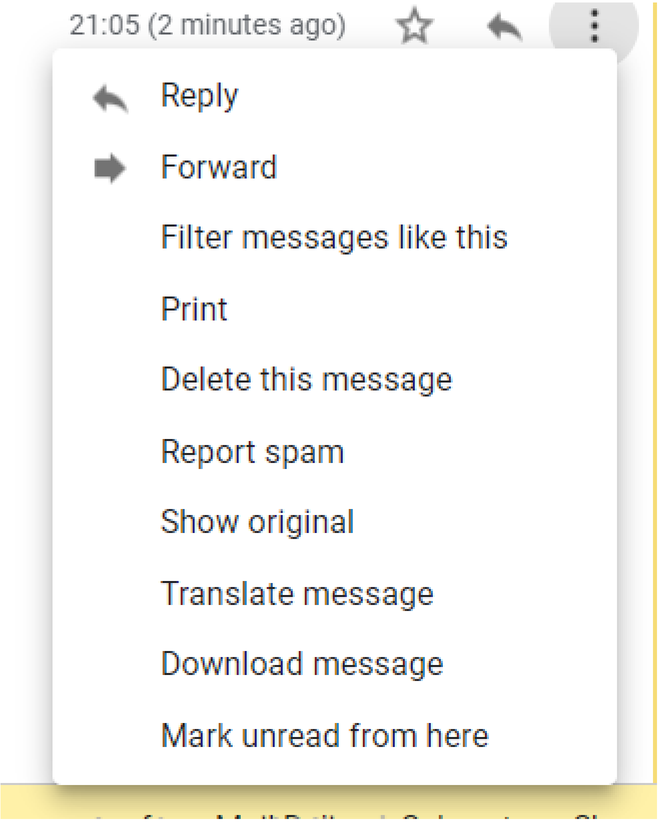


[redacted]@gmail.com>
to samantha.collen.r

its a test mail
--

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

- **Click on Show original option.**



It will offer following details:

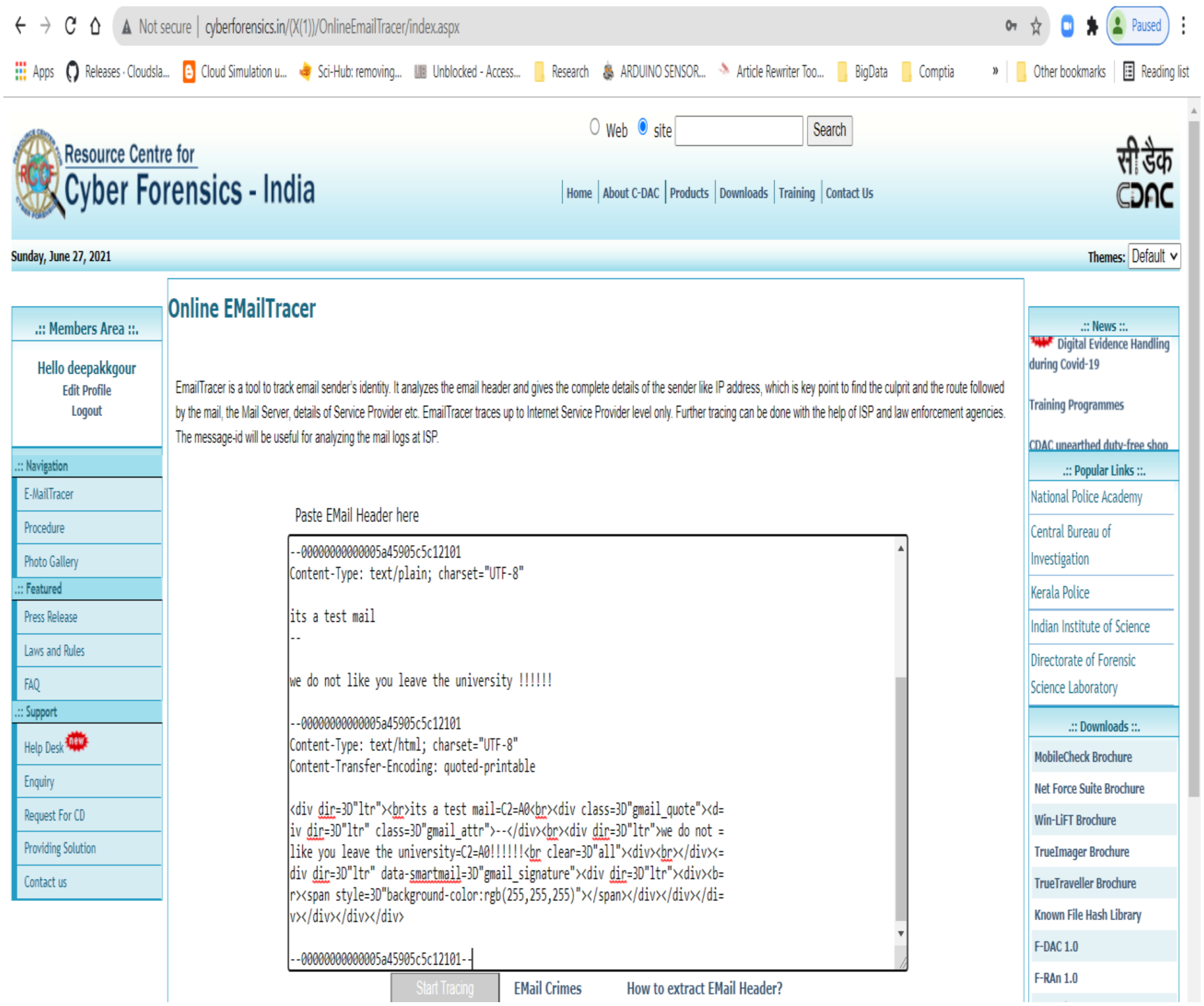
MIME-Version: 1.0
Date: Sun, 27 Jun 2021 21:05:56 +0530

Created by Sabih Khan - CEH

```
References:
<CAA7z9VfC4od73fdsFxwSu0=WzRuxxMFErbgwkXEwkyS_x3sNtQ@mail.gmail.co
m>
In-Reply-To:
<CAA7z9VfC4od73fdsFxwSu0=WzRuxxMFErbgwkXEwkyS_x3sNtQ@mail.gmail.co
m>
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--
```

- **Go to any online tracer website and paste above original message**

It will offer the IP address of the sender. Users can use any IP tracer website for the address and identification of threat attacker.



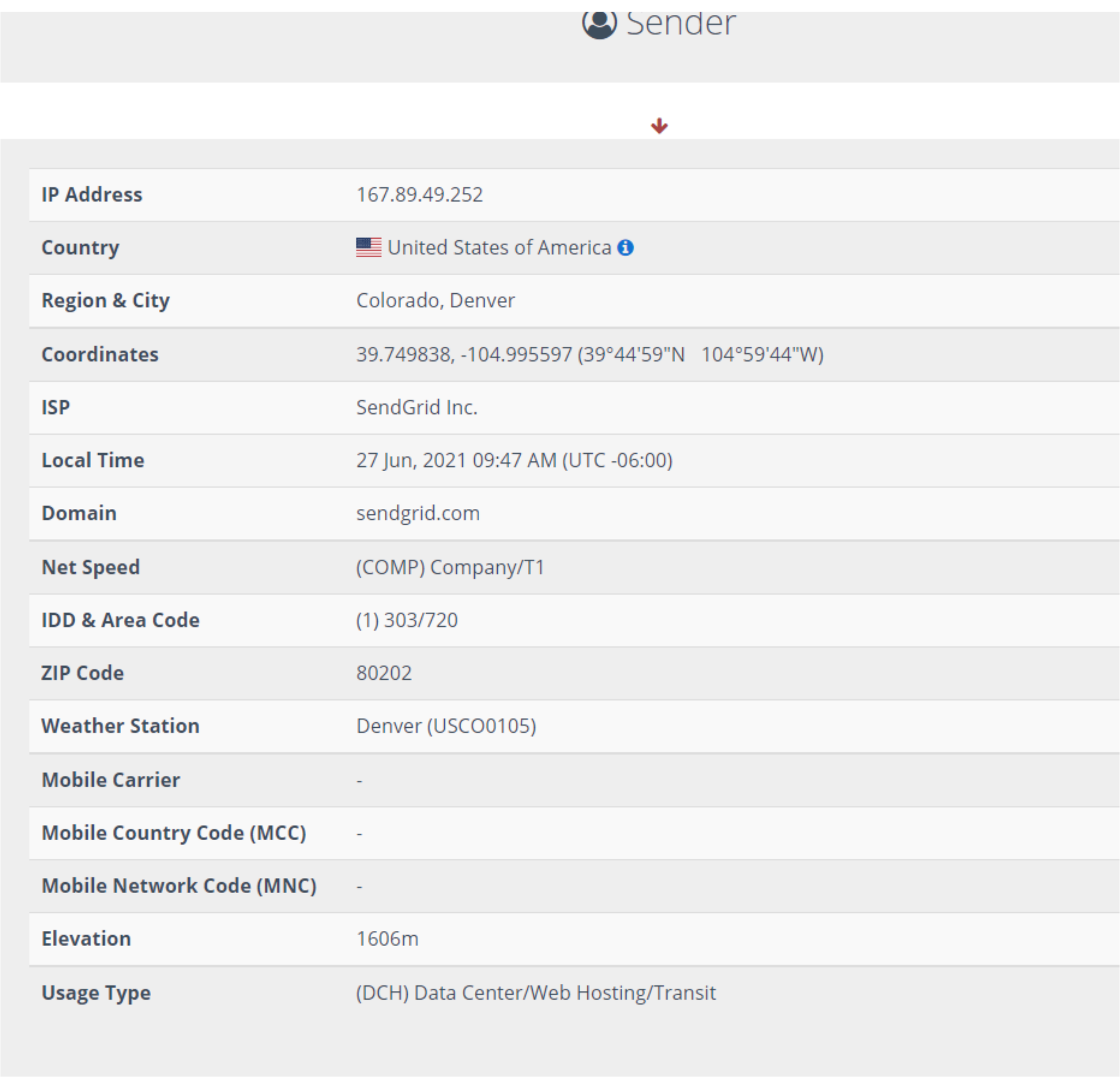
Online EMailTracer

EmailTracer is a tool to track email sender's identity. It analyzes the email header and gives the complete details of the sender like IP address, which is key point to find the culprit and the route followed by the mail, the Mail Server, details of Service Provider etc. EmailTracer traces up to Internet Service Provider level only. Further tracing can be done with the help of ISP and law enforcement agencies. The message-id will be useful for analyzing the mail logs at ISP.

Paste EMail Header here

```
--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:



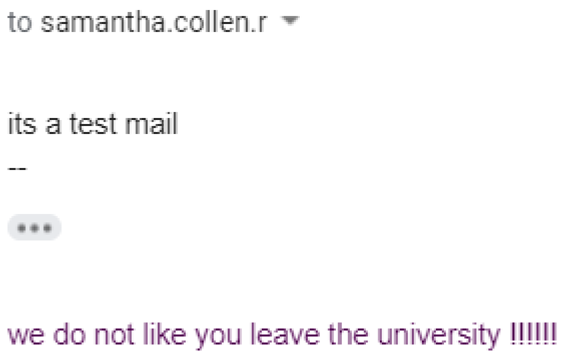
Sender

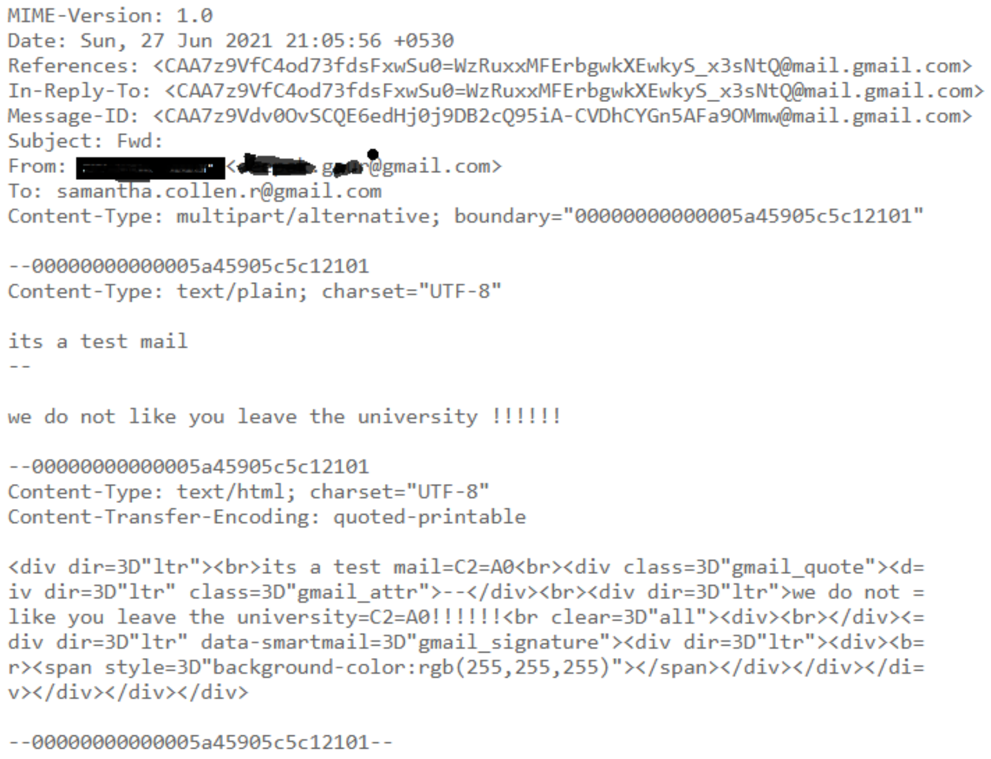
IP Address	167.89.49.252
Country	🇺🇸 United States of America ℹ
Region & City	Colorado, Denver
Coordinates	39.749838, -104.995597 (39°44'59"N 104°59'44"W)
ISP	SendGrid Inc.
Local Time	27 Jun, 2021 09:47 AM (UTC -06:00)
Domain	sendgrid.com
Net Speed	(COMP) Company/T1
IDD & Area Code	(1) 303/720
ZIP Code	80202
Weather Station	Denver (USCO0105)
Mobile Carrier	-
Mobile Country Code (MCC)	-
Mobile Network Code (MNC)	-
Elevation	1606m
Usage Type	(DCH) Data Center/Web Hosting/Transit

Task5: Submit complete incident report

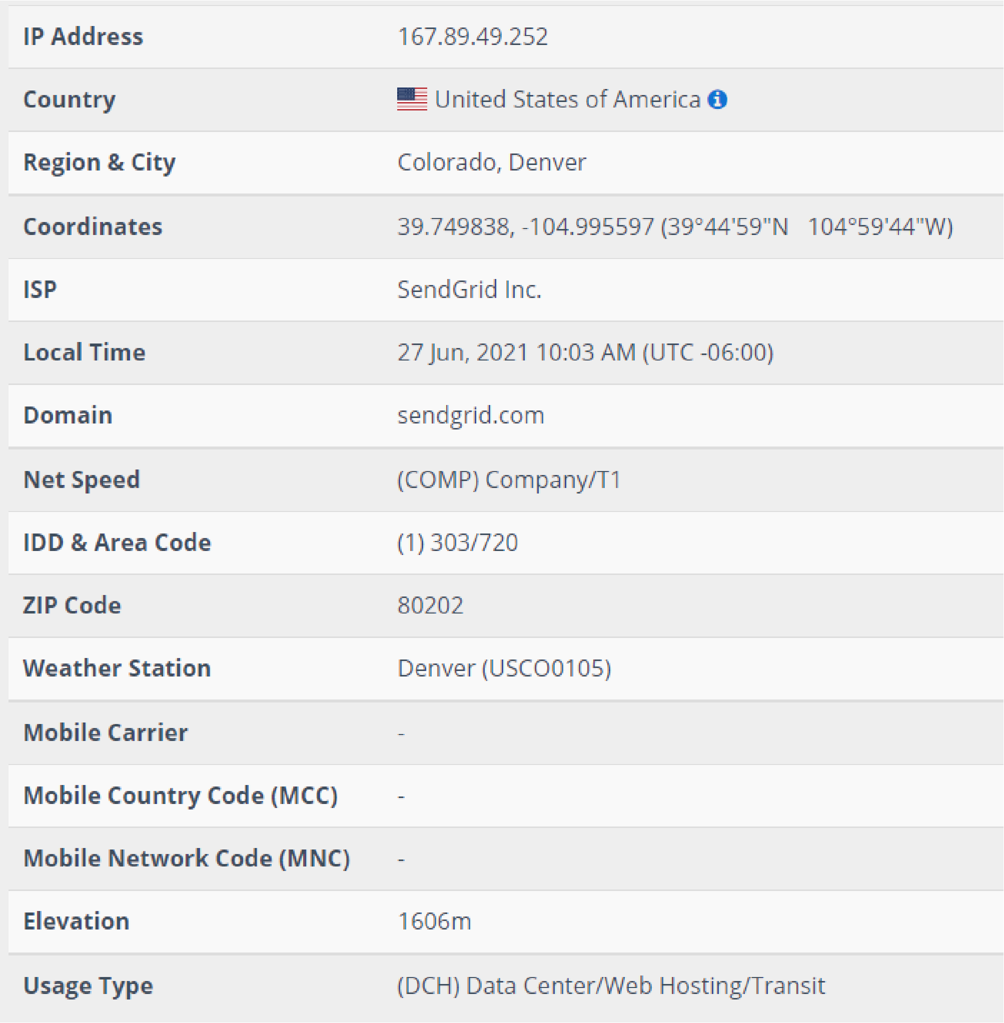
Incident Description:

Created by Sabih Khan - CEH

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	 to samantha.collen.r ▾ its a test mail -- ••• we do not like you leave the university !!!!!!
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:**  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: [redacted]<[redacted]@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"> its a test mail=C2=A0 <div class=3D"gmail_quote"><d= iv dir=3D"ltr" class=3D"gmail_attr">--</div> <div dir=3D"ltr">we do not = like you leave the university=C2=A0!!!!!!<br clear=3D"all"><div> </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--

E-Mail Forensic Summary



IP Address	167.89.49.252
Country	United States of America
Region & City	Colorado, Denver
Coordinates	39.749838, -104.995597 (39°44'59"N 104°59'44"W)
ISP	SendGrid Inc.
Local Time	27 Jun, 2021 10:03 AM (UTC -06:00)
Domain	sendgrid.com
Net Speed	(COMP) Company/T1
IDD & Area Code	(1) 303/720
ZIP Code	80202
Weather Station	Denver (USCO0105)
Mobile Carrier	-
Mobile Country Code (MCC)	-
Mobile Network Code (MNC)	-
Elevation	1606m
Usage Type	(DCH) Data Center/Web Hosting/Transit

Created by Sabih Khan - CEH