CompTIA Security+ (SYO 601) Course Project

Taaha Siddiqui Mohammed

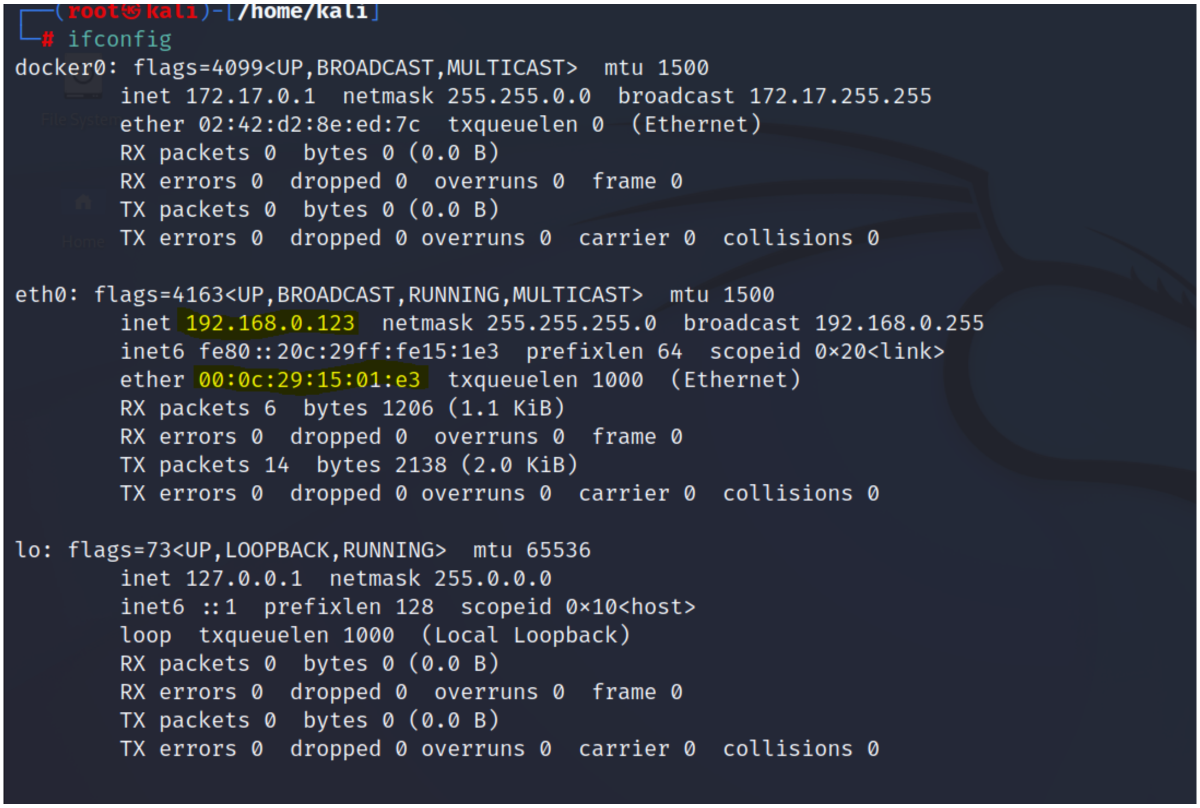
University Cyber Attack

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.

I have used Kali Linux.

Procedure:

1. Firstly, we need to get the IP address of our network. For this I have used the **'ifconfig'** command in the terminal.



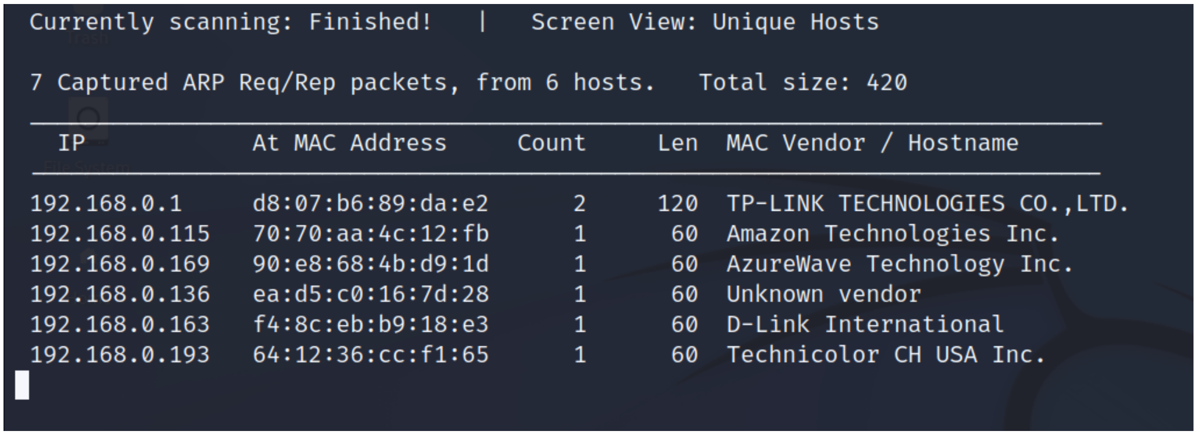
```
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:d2:8e:ed:7c  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.123  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::20c:29ff:fe15:1e3  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:15:01:e3  txqueuelen 1000  (Ethernet)
        RX packets 6  bytes 1206 (1.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14  bytes 2138 (2.0 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 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

I have highlighted the machine IP as well as the MAC address.

IP address = 192.168.0.123

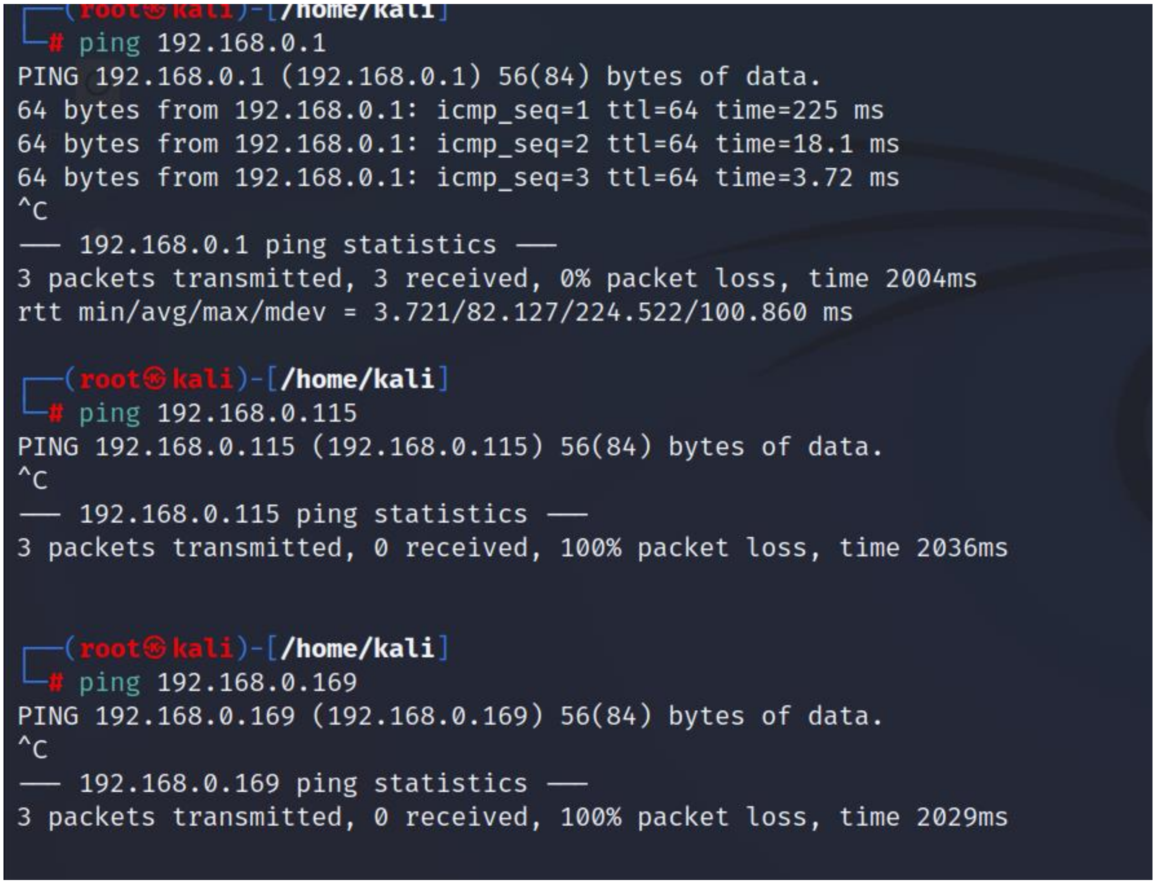
2. Now we need to get all the open terminals in our network. We can use the ‘netdiscover’ command as follows;

netdiscover –r 192.168.0.123/24

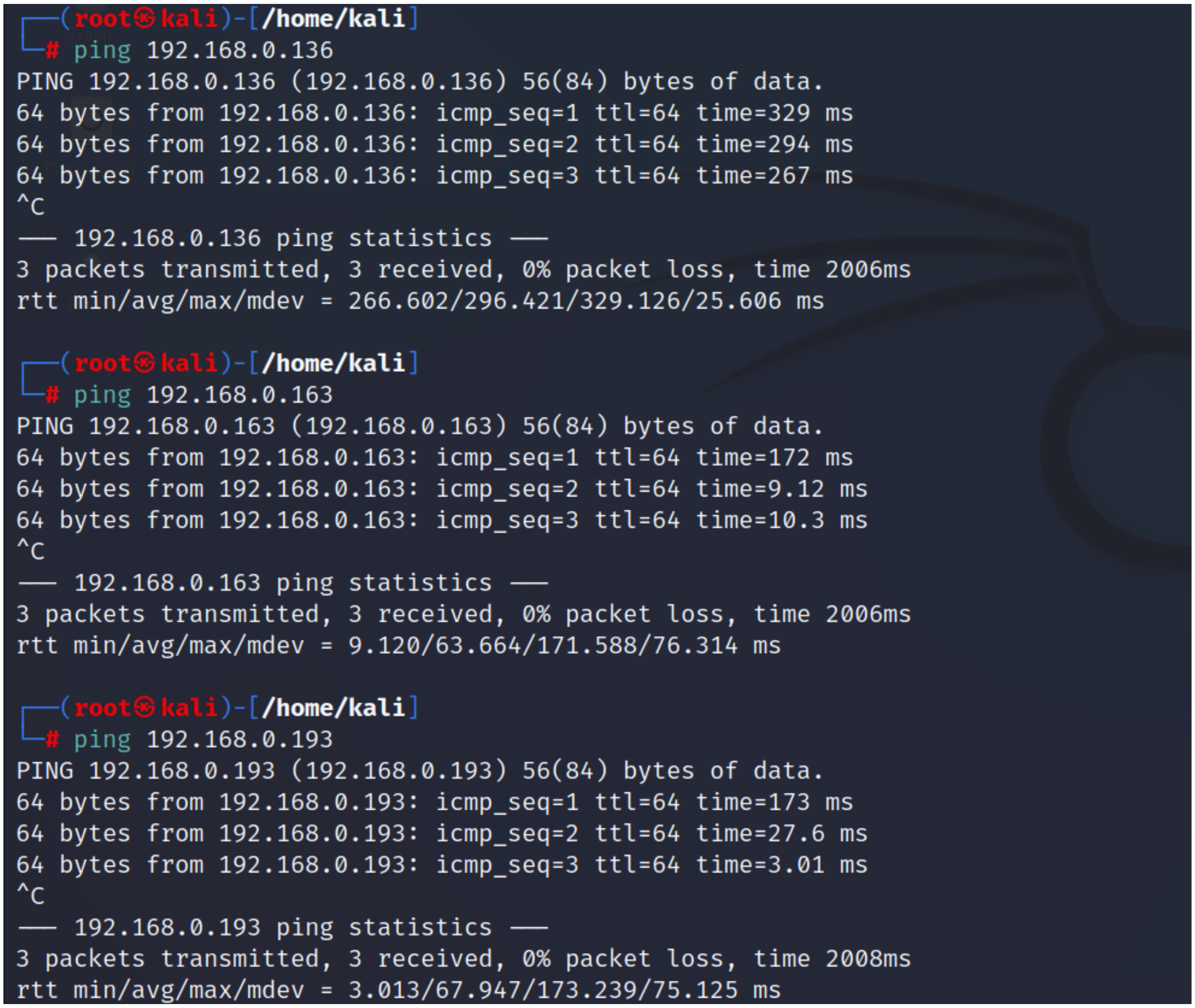


```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 7 Captured ARP Req/Rep packets, from 6 hosts.   Total size: 420
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 _____________________________________________________________________________

 192.168.0.1     d8:07:b6:89:da:e2      2     120  TP-LINK TECHNOLOGIES CO.,LTD.
 192.168.0.115   70:70:aa:4c:12:fb      1      60  Amazon Technologies Inc.
 192.168.0.169   90:e8:68:4b:d9:1d      1      60  AzureWave Technology Inc.
 192.168.0.136   ea:d5:c0:16:7d:28      1      60  Unknown vendor
 192.168.0.163   f4:8c:eb:b9:18:e3      1      60  D-Link International
 192.168.0.193   64:12:36:cc:f1:65      1      60  Technicolor CH USA Inc.
```

We can see that there are 6 live hosts in the network. 192.168.0.1 is the IP of the network gateway. Let us ping to see which terminals are active.



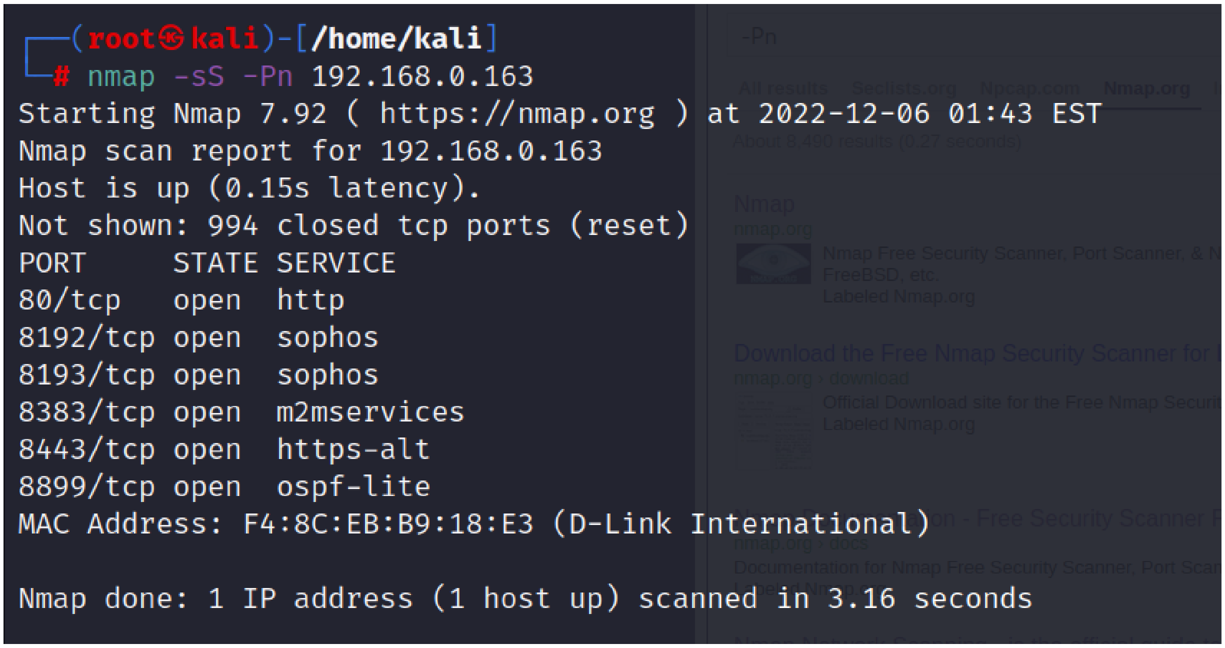
```
┌──(root㉿kali)-[/home/kali]
└─# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=225 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=18.1 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=3.72 ms
^C
── 192.168.0.1 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 3.721/82.127/224.522/100.860 ms

┌──(root㉿kali)-[/home/kali]
└─# ping 192.168.0.115
PING 192.168.0.115 (192.168.0.115) 56(84) bytes of data.
^C
── 192.168.0.115 ping statistics ──
3 packets transmitted, 0 received, 100% packet loss, time 2036ms


┌──(root㉿kali)-[/home/kali]
└─# ping 192.168.0.169
PING 192.168.0.169 (192.168.0.169) 56(84) bytes of data.
^C
── 192.168.0.169 ping statistics ──
3 packets transmitted, 0 received, 100% packet loss, time 2029ms
```



```
┌──(root㉿kali)-[/home/kali]
└─# ping 192.168.0.136
PING 192.168.0.136 (192.168.0.136) 56(84) bytes of data.
64 bytes from 192.168.0.136: icmp_seq=1 ttl=64 time=329 ms
64 bytes from 192.168.0.136: icmp_seq=2 ttl=64 time=294 ms
64 bytes from 192.168.0.136: icmp_seq=3 ttl=64 time=267 ms
^C
── 192.168.0.136 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2006ms
rtt min/avg/max/mdev = 266.602/296.421/329.126/25.606 ms

┌──(root㉿kali)-[/home/kali]
└─# ping 192.168.0.163
PING 192.168.0.163 (192.168.0.163) 56(84) bytes of data.
64 bytes from 192.168.0.163: icmp_seq=1 ttl=64 time=172 ms
64 bytes from 192.168.0.163: icmp_seq=2 ttl=64 time=9.12 ms
64 bytes from 192.168.0.163: icmp_seq=3 ttl=64 time=10.3 ms
^C
── 192.168.0.163 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2006ms
rtt min/avg/max/mdev = 9.120/63.664/171.588/76.314 ms

┌──(root㉿kali)-[/home/kali]
└─# ping 192.168.0.193
PING 192.168.0.193 (192.168.0.193) 56(84) bytes of data.
64 bytes from 192.168.0.193: icmp_seq=1 ttl=64 time=173 ms
64 bytes from 192.168.0.193: icmp_seq=2 ttl=64 time=27.6 ms
64 bytes from 192.168.0.193: icmp_seq=3 ttl=64 time=3.01 ms
^C
── 192.168.0.193 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2008ms
rtt min/avg/max/mdev = 3.013/67.947/173.239/75.125 ms
```

Out of 6, only 4 have responded to our ping. Let us scan and see which of the 3 (except the gateway IP) has open ports.

We can use Nmap scans for seeing open ports.



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -Pn 192.168.0.163
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-06 01:43 EST
Nmap scan report for 192.168.0.163
Host is up (0.15s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
8192/tcp open  sophos
8193/tcp open  sophos
8383/tcp open  m2mservices
8443/tcp open  https-alt
8899/tcp open  ospf-lite
MAC Address: F4:8C:EB:B9:18:E3 (D-Link International)

Nmap done: 1 IP address (1 host up) scanned in 3.16 seconds
```

On scanning I got open ports only for ‘**192.168.0.163**’ device which is another router available in my network.

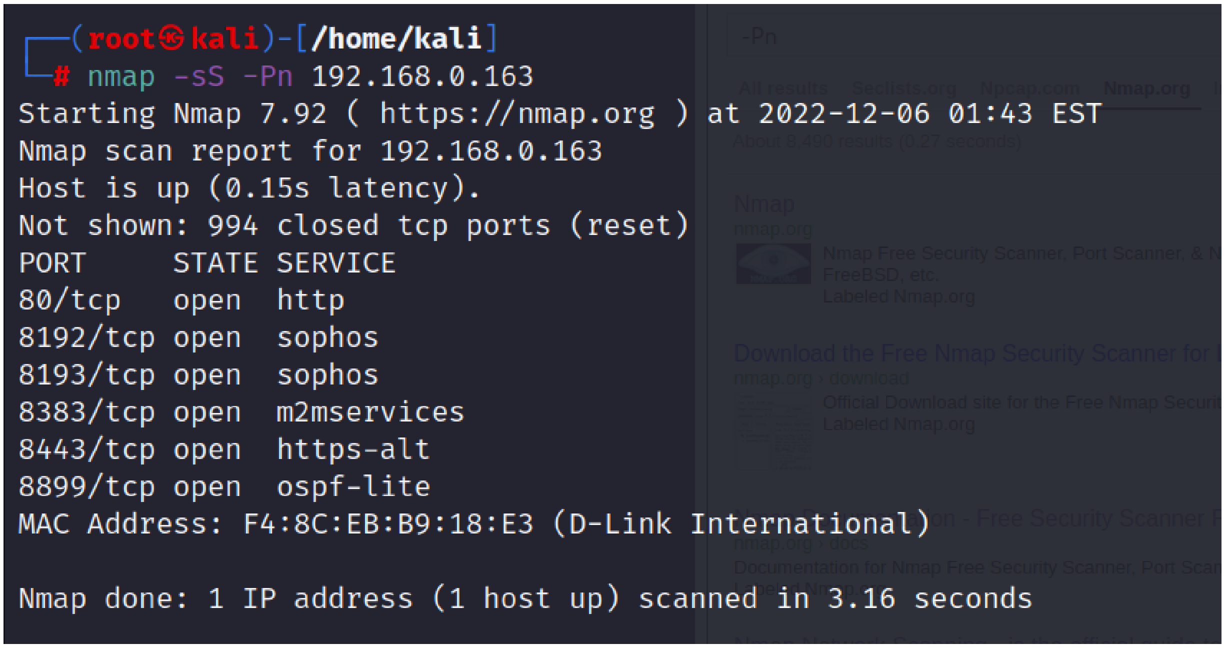
So, concluding Task-1;

Server IP = 192.168.0.123

Victim IP = 193.168.0.163

==

Task 2: Identify CVE score of the victim’s vulnerability.

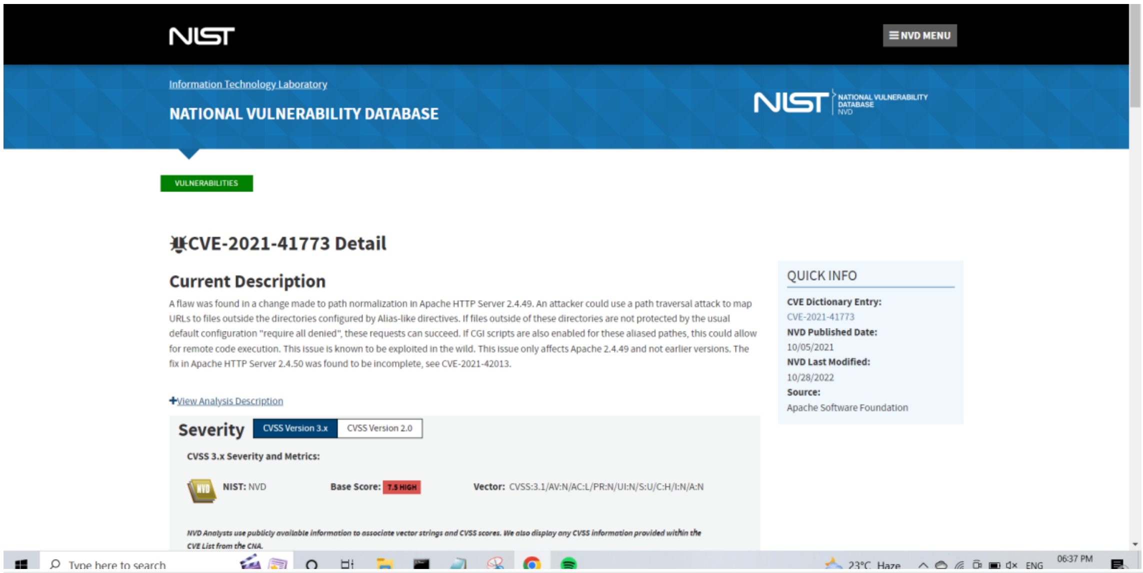


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -Pn 192.168.0.163
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-06 01:43 EST
Nmap scan report for 192.168.0.163
Host is up (0.15s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
8192/tcp open  sophos
8193/tcp open  sophos
8383/tcp open  m2mservices
8443/tcp open  https-alt
8899/tcp open  ospf-lite
MAC Address: F4:8C:EB:B9:18:E3 (D-Link International)

Nmap done: 1 IP address (1 host up) scanned in 3.16 seconds
```

Let us look at exploits for each port if there is any available.

1. **Port 80 – http**

   a. CVE-2021-41773 - Apache HTTP Server Path Traversal Vulnerability

b. 

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

VULNERABILITIES

CVE-2021-41773 Detail

Current Description

A flaw was found in a change made to path normalization in Apache HTTP Server 2.4.49. An attacker could use a path traversal attack to map URLs to files outside the directories configured by Alias-like directives. If files outside of these directories are not protected by the usual default configuration "require all denied", these requests can succeed. If CGI scripts are also enabled for these aliased pathes, this could allow for remote code execution. This issue is known to be exploited in the wild. This issue only affects Apache 2.4.49 and not earlier versions. The fix in Apache HTTP Server 2.4.50 was found to be incomplete, see CVE-2021-42013.

+View Analysis Description

Severity CVSS Version 3.x | CVSS Version 2.0

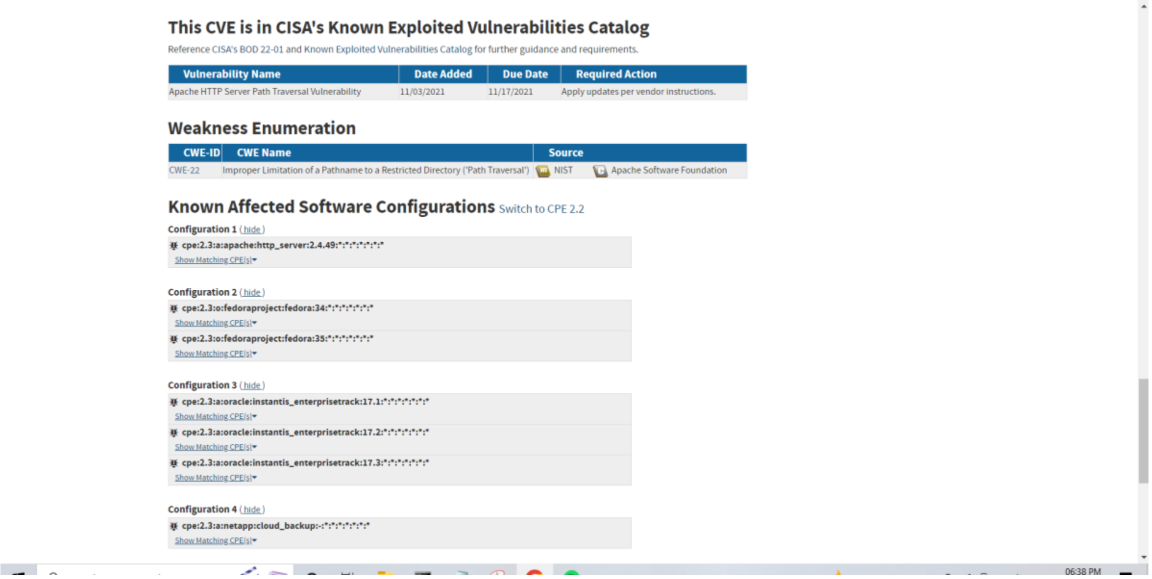
CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 7.5 HIGH **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

QUICK INFO

CVE Dictionary Entry:
CVE-2021-41773
NVD Published Date:
10/05/2021
NVD Last Modified:
10/28/2022
Source:
Apache Software Foundation



This CVE is in CISA's Known Exploited Vulnerabilities Catalog

Reference CISA's BOD 22-01 and Known Exploited Vulnerabilities Catalog for further guidance and requirements.

Vulnerability Name	Date Added	Due Date	Required Action
Apache HTTP Server Path Traversal Vulnerability	11/03/2021	11/17/2021	Apply updates per vendor instructions.

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	NIST Apache Software Foundation

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

```
cpe:2.3:a:apache:http_server:2.4.49:*:*:*:*:*:*:*
```
Show Matching CPE(s)▾

Configuration 2 (hide)

```
cpe:2.3:o:fedoraproject:fedora:34:*:*:*:*:*:*:*
```
Show Matching CPE(s)▾

```
cpe:2.3:o:fedoraproject:fedora:35:*:*:*:*:*:*:*
```
Show Matching CPE(s)▾

Configuration 3 (hide)

```
cpe:2.3:a:oracle:instantis_enterprisetrack:17.1:*:*:*:*:*:*:*
```
Show Matching CPE(s)▾

```
cpe:2.3:a:oracle:instantis_enterprisetrack:17.2:*:*:*:*:*:*:*
```
Show Matching CPE(s)▾

```
cpe:2.3:a:oracle:instantis_enterprisetrack:17.3:*:*:*:*:*:*:*
```
Show Matching CPE(s)▾

Configuration 4 (hide)

```
cpe:2.3:a:netapp:cloud_backup:-:*:*:*:*:*:*:*
```
Show Matching CPE(s)▾

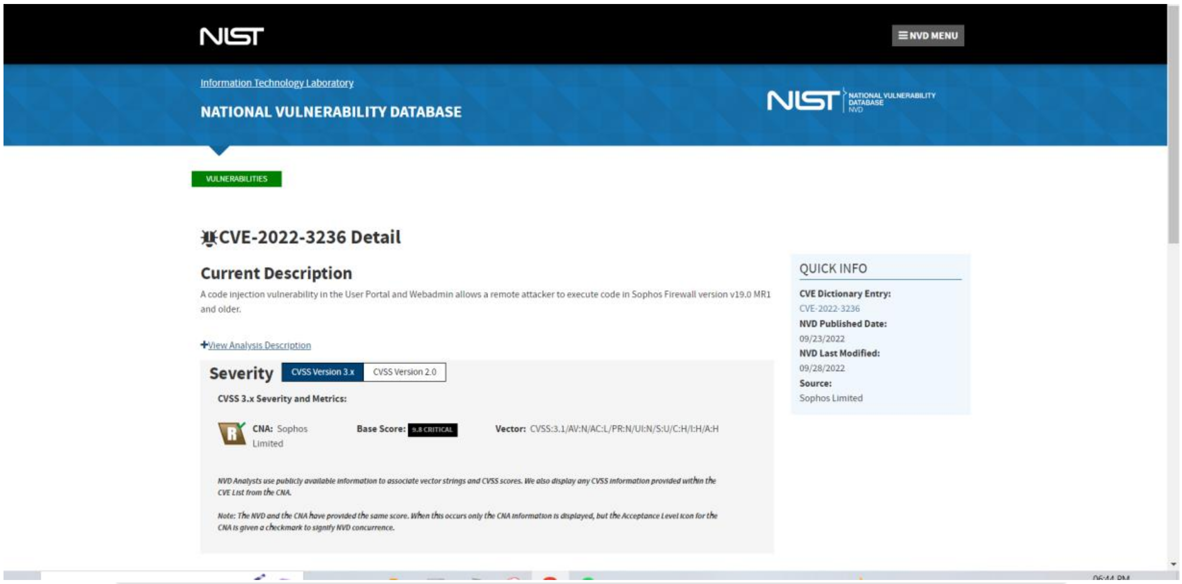
c. https://nvd.nist.gov/vuln/detail/CVE-2021-41773

d. CVE Score given by National Vulnerability Database is **7.5 (HIGH).**

2. Ports 8192/8193 - Sophos

a. CVE-2022-3236 - Sophos Firewall Code Injection Vulnerability

b.


NIST
≡ NVD MENU
Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE
NIST NATIONAL VULNERABILITY DATABASE NVD
VULNERABILITIES

CVE-2022-3236 Detail

Current Description

A code injection vulnerability in the User Portal and Webadmin allows a remote attacker to execute code in Sophos Firewall version v19.0 MR1 and older.

+View Analysis Description

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

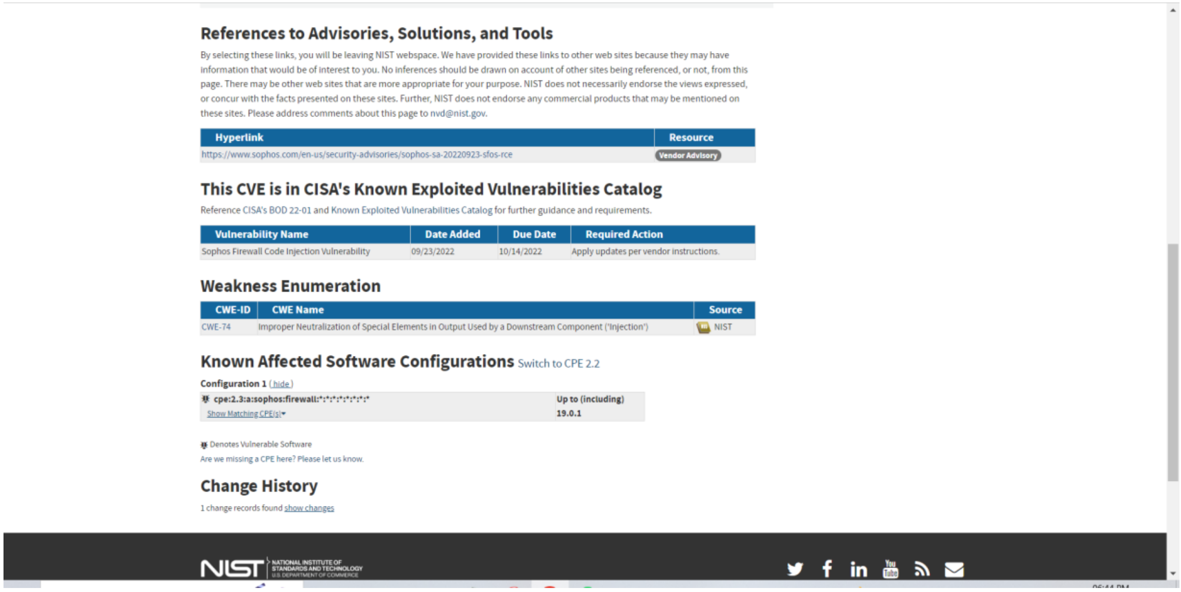
CNA: Sophos Limited **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: The NVD and the CNA have provided the same score. When this occurs only the CNA information is displayed, but the Acceptance Level icon for the CNA is given a checkmark to signify NVD concurrence.

QUICK INFO

CVE Dictionary Entry:
CVE-2022-3236
NVD Published Date:
09/23/2022
NVD Last Modified:
09/28/2022
Source:
Sophos Limited



References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://www.sophos.com/en-us/security-advisories/sophos-sa-20220923-sfos-rce	Vendor Advisory

This CVE is in CISA's Known Exploited Vulnerabilities Catalog

Reference CISA's BOD 22-01 and Known Exploited Vulnerabilities Catalog for further guidance and requirements.

Vulnerability Name	Date Added	Due Date	Required Action
Sophos Firewall Code Injection Vulnerability	09/23/2022	10/14/2022	Apply updates per vendor instructions.

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	NIST

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:a:sophos:firewall:*:*:*:*:*:*:*:* Show Matching CPE(s)▾	**Up to (including)** **19.0.1**

Denotes Vulnerable Software
Are we missing a CPE here? Please let us know.

Change History

1 change records found show changes

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

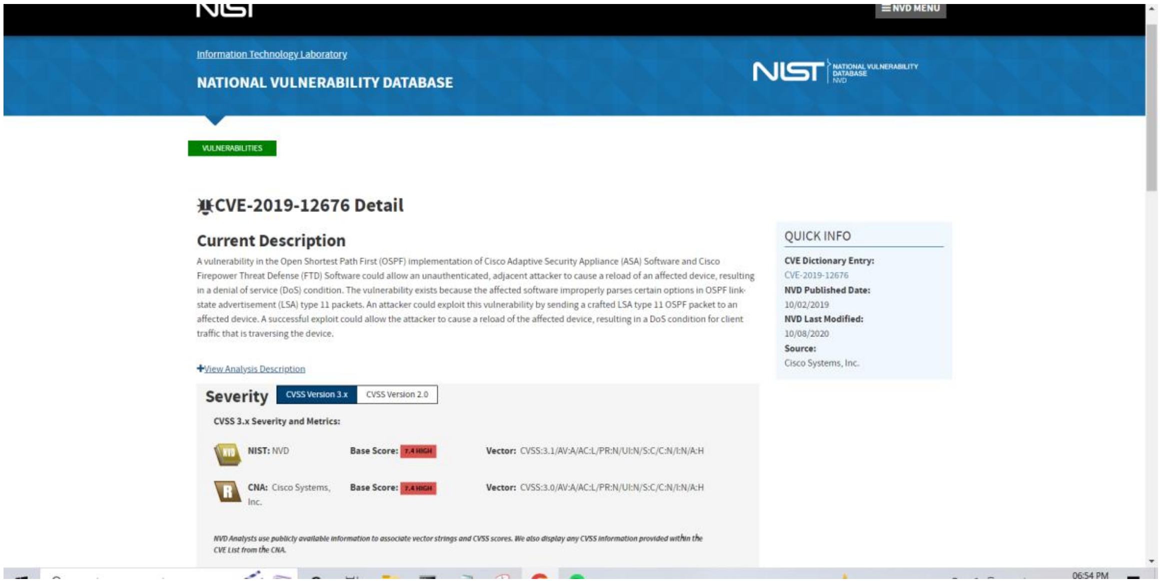
c. https://nvd.nist.gov/vuln/detail/CVE-2022-3236

d. CVE Score given by National Vulnerability Database is **9.8 (Critical)**

3. Port 8899 – OSPF-Lite

a. CVE-2019-12676

b.


NVD MENU
Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE
NIST NATIONAL VULNERABILITY DATABASE NVD
VULNERABILITIES
06:54 PM

CVE-2019-12676 Detail

Current Description

A vulnerability in the Open Shortest Path First (OSPF) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability exists because the affected software improperly parses certain options in OSPF link-state advertisement (LSA) type 11 packets. An attacker could exploit this vulnerability by sending a crafted LSA type 11 OSPF packet to an affected device. A successful exploit could allow the attacker to cause a reload of the affected device, resulting in a DoS condition for client traffic that is traversing the device.

QUICK INFO

CVE Dictionary Entry:
CVE-2019-12676
NVD Published Date:
10/02/2019
NVD Last Modified:
10/08/2020
Source:
Cisco Systems, Inc.

+View Analysis Description

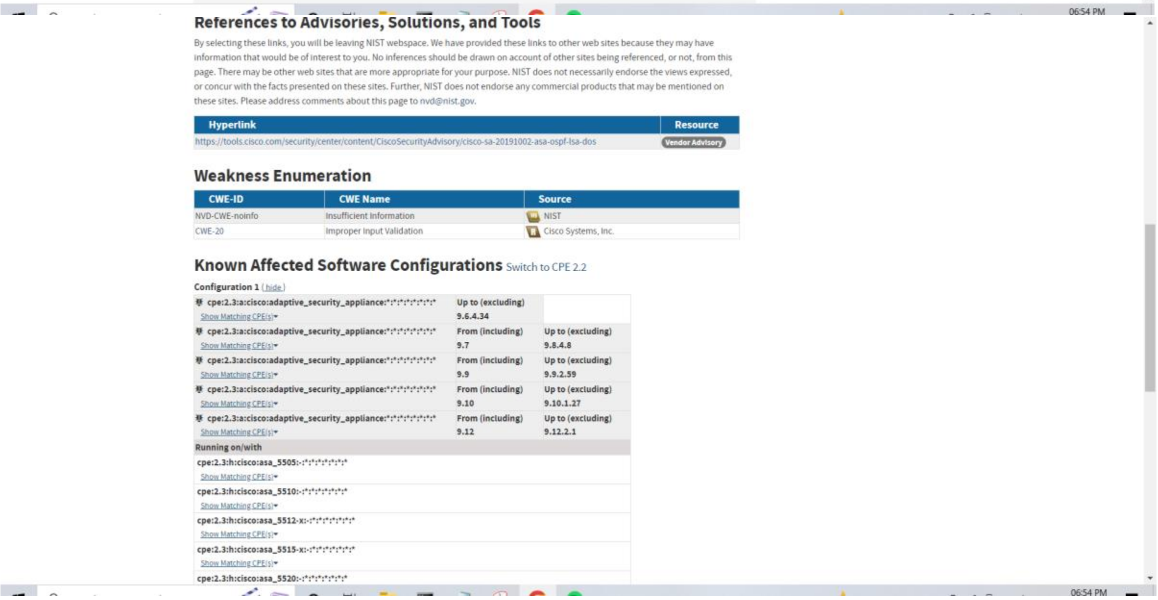
Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD	**Base Score:** 7.4 HIGH	**Vector:** CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H
CNA: Cisco Systems, Inc.	**Base Score:** 7.4 HIGH	**Vector:** CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.



References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-asa-ospf-lsa-dos	Vendor Advisory

Weakness Enumeration

CWE-ID	CWE Name	Source
NVD-CWE-noinfo	Insufficient Information	NIST
CWE-20	Improper Input Validation	Cisco Systems, Inc.

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:a:cisco:adaptive_security_appliance:*:*:*:*:*:*:*:* Show Matching CPE(s)▾	Up to (excluding) 9.6.4.34	
cpe:2.3:a:cisco:adaptive_security_appliance:*:*:*:*:*:*:*:* Show Matching CPE(s)▾	From (including) 9.7	Up to (excluding) 9.8.4.8
cpe:2.3:a:cisco:adaptive_security_appliance:*:*:*:*:*:*:*:* Show Matching CPE(s)▾	From (including) 9.9	Up to (excluding) 9.9.2.59
cpe:2.3:a:cisco:adaptive_security_appliance:*:*:*:*:*:*:*:* Show Matching CPE(s)▾	From (including) 9.10	Up to (excluding) 9.10.1.27
cpe:2.3:a:cisco:adaptive_security_appliance:*:*:*:*:*:*:*:* Show Matching CPE(s)▾	From (including) 9.12	Up to (excluding) 9.12.2.1
Running on/with		
cpe:2.3:h:cisco:asa_5505:-:*:*:*:*:*:*:* Show Matching CPE(s)▾		
cpe:2.3:h:cisco:asa_5510:-:*:*:*:*:*:*:* Show Matching CPE(s)▾		
cpe:2.3:h:cisco:asa_5512-x:-:*:*:*:*:*:*:* Show Matching CPE(s)▾		
cpe:2.3:h:cisco:asa_5515-x:-:*:*:*:*:*:*:* Show Matching CPE(s)▾		
cpe:2.3:h:cisco:asa_5520:-:*:*:*:*:*:*:*		

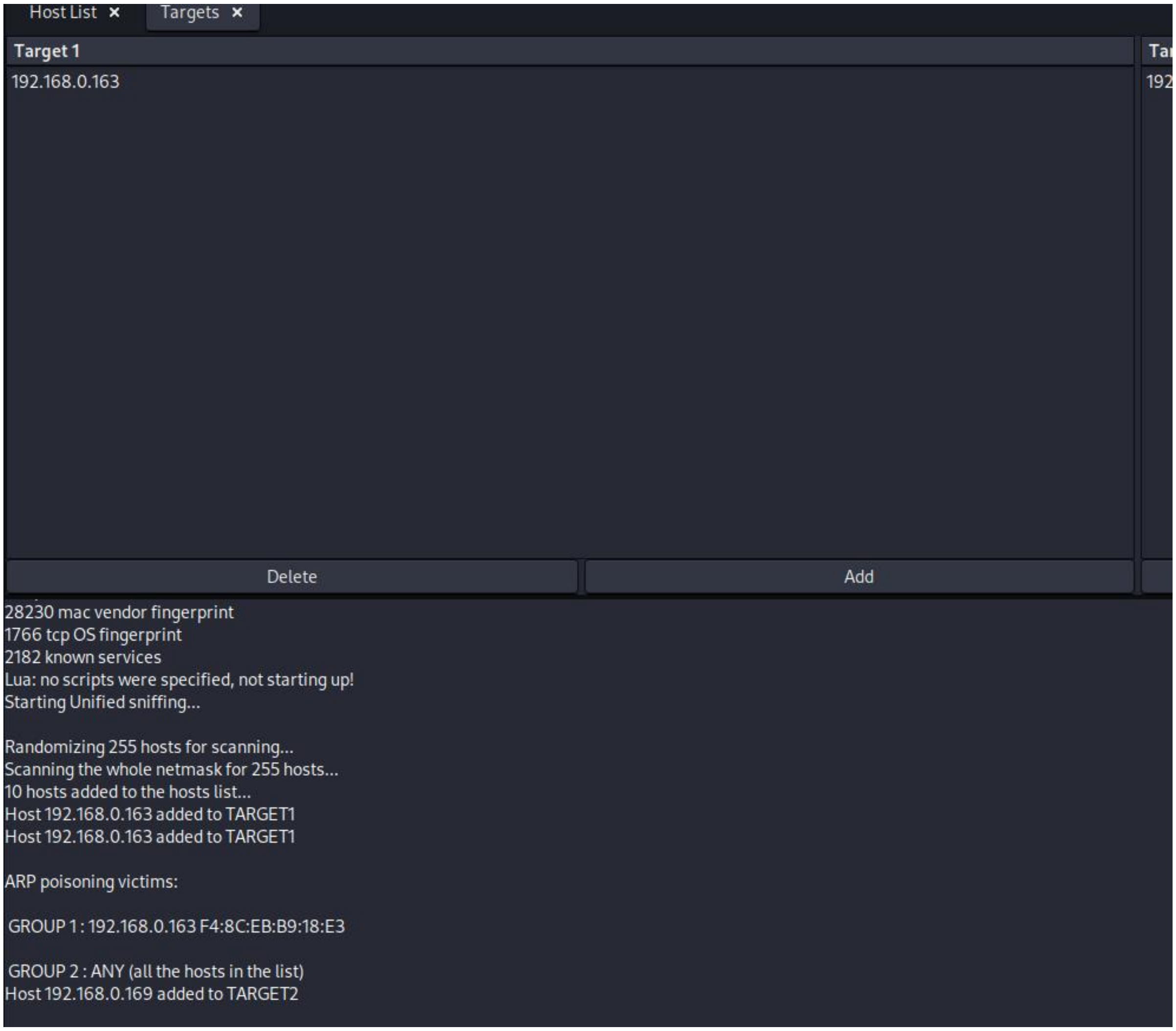
c. https://nvd.nist.gov/vuln/detail/CVE-2019-12676

d. CVE Score given by National Vulnerability Database is **7.4 (HIGH).**

==

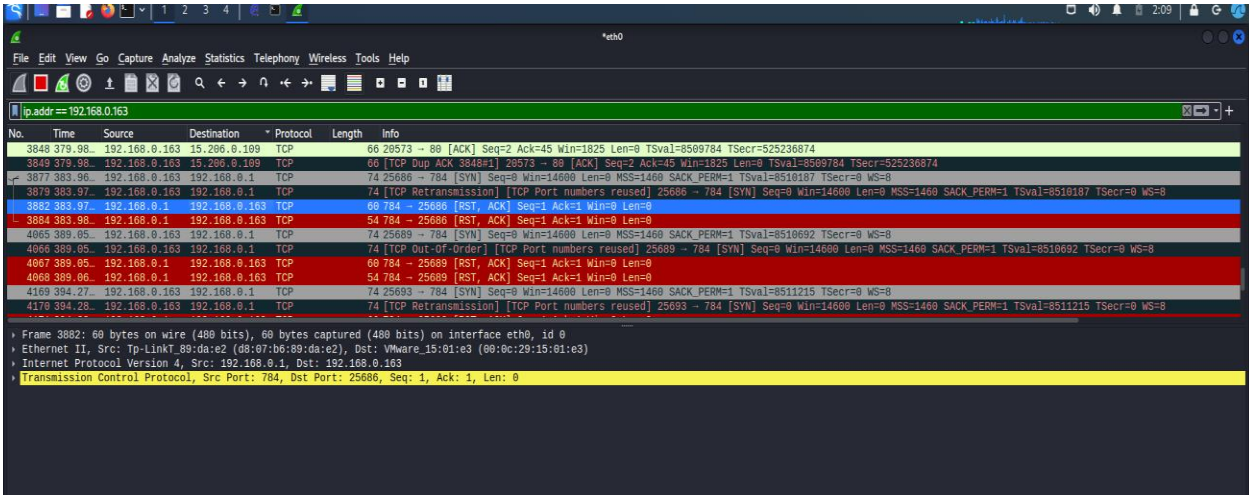
Task 3: Identify whether the victim's terminal is affected with MiMT attack or not and submit the incident report for the same.

1. In-order to check if MITM attacks are possible on this device, we can take help of Ettercap-graphical for ARP Poisoning the target.

2. 

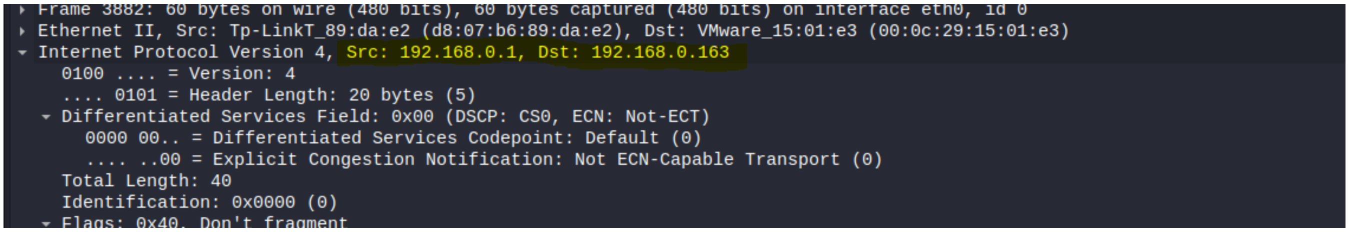
```
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
10 hosts added to the hosts list...
Host 192.168.0.163 added to TARGET1
Host 192.168.0.163 added to TARGET1

ARP poisoning victims:

 GROUP 1 : 192.168.0.163 F4:8C:EB:B9:18:E3

 GROUP 2 : ANY (all the hosts in the list)
Host 192.168.0.169 added to TARGET2
```

3. And to check the result we will use Wireshark to see the effect on the target.

4. 
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 192.168.0.163
```

```
No.   Time      Source         Destination    Protocol Length Info
 3848 379.98…  192.168.0.163  15.206.0.109   TCP      66 20573 → 80 [ACK] Seq=2 Ack=45 Win=1825 Len=0 TSval=8509784 TSecr=525236874
 3849 379.98…  192.168.0.163  15.206.0.109   TCP      66 [TCP Dup ACK 3848#1] 20573 → 80 [ACK] Seq=2 Ack=45 Win=1825 Len=0 TSval=8509784 TSecr=525236874
 3877 383.96…  192.168.0.163  192.168.0.1    TCP      74 25686 → 784 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=8510187 TSecr=0 WS=8
 3879 383.97…  192.168.0.163  192.168.0.1    TCP      74 [TCP Retransmission] [TCP Port numbers reused] 25686 → 784 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=8510187 TSecr=0 WS=8
 3882 383.97…  192.168.0.1    192.168.0.163  TCP      60 784 → 25686 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 3884 383.98…  192.168.0.1    192.168.0.163  TCP      54 784 → 25686 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 4065 389.05…  192.168.0.163  192.168.0.1    TCP      74 25689 → 784 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=8510692 TSecr=0 WS=8
 4066 389.05…  192.168.0.163  192.168.0.1    TCP      74 [TCP Out-Of-Order] [TCP Port numbers reused] 25689 → 784 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=8510692 TSecr=0 WS=8
 4067 389.05…  192.168.0.1    192.168.0.163  TCP      60 784 → 25689 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 4068 389.06…  192.168.0.1    192.168.0.163  TCP      54 784 → 25689 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 4169 394.27…  192.168.0.163  192.168.0.1    TCP      74 25693 → 784 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=8511215 TSecr=0 WS=8
 4170 394.28…  192.168.0.163  192.168.0.1    TCP      74 [TCP Retransmission] [TCP Port numbers reused] 25693 → 784 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=8511215 TSecr=0 WS=8

▸ Frame 3882: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
▸ Ethernet II, Src: Tp-LinkT_89:da:e2 (d8:07:b6:89:da:e2), Dst: VMware_15:01:e3 (00:0c:29:15:01:e3)
▸ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.163
▸ Transmission Control Protocol, Src Port: 784, Dst Port: 25686, Seq: 1, Ack: 1, Len: 0
```



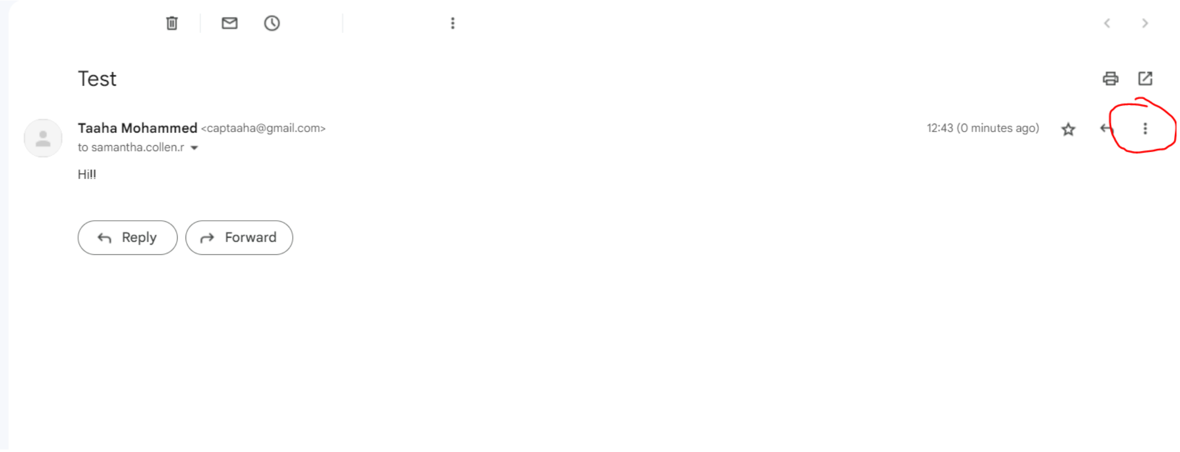
```
▸ Frame 3882: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
▸ Ethernet II, Src: Tp-LinkT_89:da:e2 (d8:07:b6:89:da:e2), Dst: VMware_15:01:e3 (00:0c:29:15:01:e3)
▾ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.163
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▾ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 40
    Identification: 0x0000 (0)
  ▾ Flags: 0x40, Don't fragment
```

5. Hence, we see the effect. We can conclude that MITM attacks are possible on the target.

==

Task 4: Use email forensics analysis and identify the sender's IP address

1. I have sent a sample email to Samantha on her personal email.

2. 

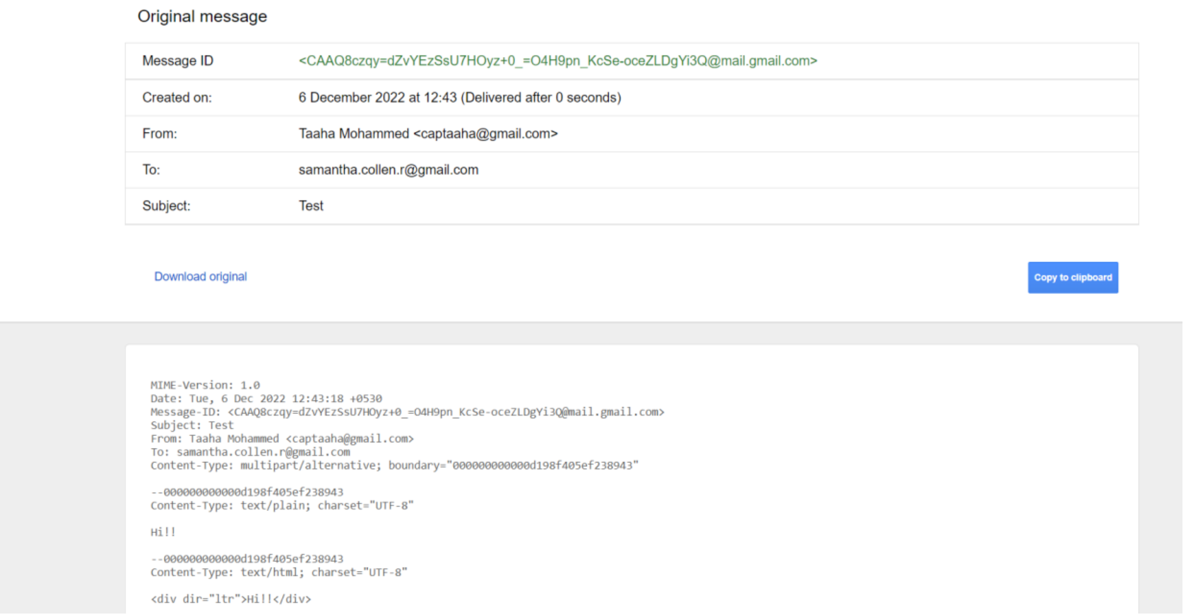
Test

Taaha Mohammed <captaaha@gmail.com>
to samantha.collen.r

12:43 (0 minutes ago)

Hi!!

3. We click on the 3 dots and select the show original option. We get the following details;

4. 

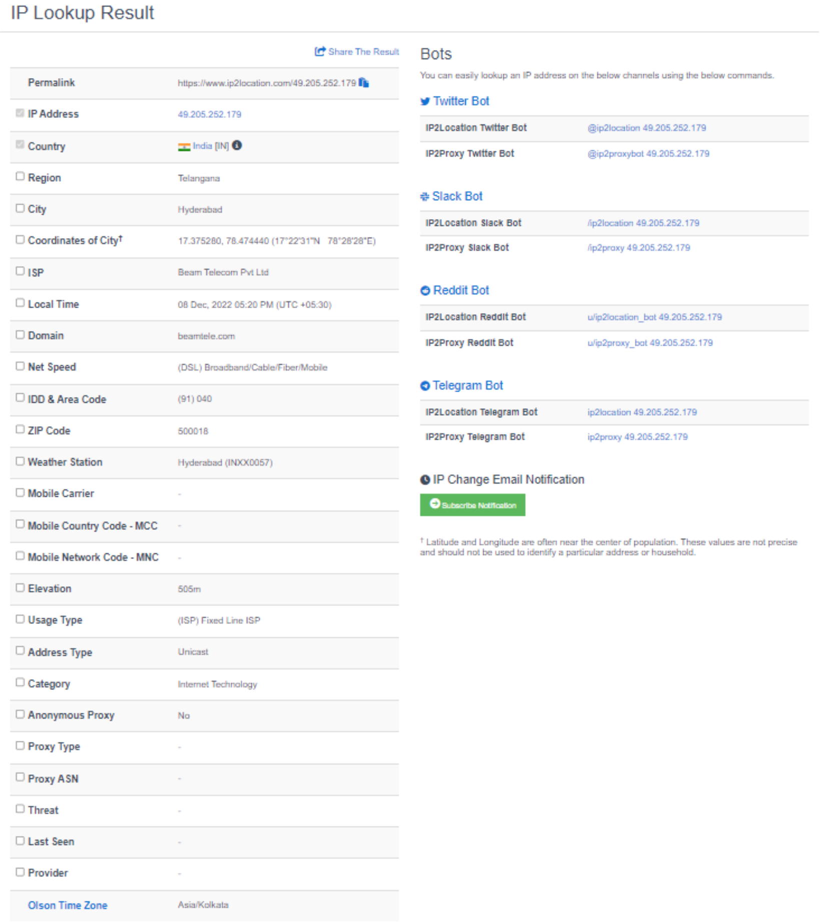
Original message

Message ID	<CAAQ8czqy=dZvYEzSsU7HOyz+0_=O4H9pn_KcSe-oceZLDgYi3Q@mail.gmail.com>
Created on:	6 December 2022 at 12:43 (Delivered after 0 seconds)
From:	Taaha Mohammed <captaaha@gmail.com>
To:	samantha.collen.r@gmail.com
Subject:	Test

```
MIME-Version: 1.0
Date: Tue, 6 Dec 2022 12:43:18 +0530
Message-ID: <CAAQ8czqy=dZvYEzSsU7HOyz+0_=O4H9pn_KcSe-oceZLDgYi3Q@mail.gmail.com>
Subject: Test
From: Taaha Mohammed <captaaha@gmail.com>
To: samantha.collen.r@gmail.com
Content-Type: multipart/alternative; boundary="000000000000d198f405ef238943"

--000000000000d198f405ef238943
Content-Type: text/plain; charset="UTF-8"

Hi!!

--000000000000d198f405ef238943
Content-Type: text/html; charset="UTF-8"

<div dir="ltr">Hi!!</div>
```

5. Let us take this into an Email tracing tool;

6.



IP Lookup Result

Permalink	https://www.ip2location.com/49.205.252.179
☑ IP Address	49.205.252.179
☑ Country	India [IN]
☐ Region	Telangana
☐ City	Hyderabad
☐ Coordinates of City[†]	17.375280, 78.474440 (17°22'31"N 78°28'28"E)
☐ ISP	Beam Telecom Pvt Ltd
☐ Local Time	08 Dec, 2022 05:20 PM (UTC +05:30)
☐ Domain	beamtele.com
☐ Net Speed	(DSL) Broadband/Cable/Fiber/Mobile
☐ IDD & Area Code	(91) 040
☐ ZIP Code	500018
☐ Weather Station	Hyderabad (INXX0057)
☐ Mobile Carrier	-
☐ Mobile Country Code - MCC	-
☐ Mobile Network Code - MNC	-
☐ Elevation	505m
☐ Usage Type	(ISP) Fixed Line ISP
☐ Address Type	Unicast
☐ Category	Internet Technology
☐ Anonymous Proxy	No
☐ Proxy Type	-
☐ Proxy ASN	-
☐ Threat	-
☐ Last Seen	-
☐ Provider	-
Olson Time Zone	Asia/Kolkata

Bots

You can easily lookup an IP address on the below channels using the below commands.

Twitter Bot

IP2Location Twitter Bot	@ip2location 49.205.252.179
IP2Proxy Twitter Bot	@ip2proxybot 49.205.252.179

Slack Bot

IP2Location Slack Bot	/ip2location 49.205.252.179
IP2Proxy Slack Bot	/ip2proxy 49.205.252.179

Reddit Bot

IP2Location Reddit Bot	u/ip2location_bot 49.205.252.179
IP2Proxy Reddit Bot	u/ip2proxy_bot 49.205.252.179

Telegram Bot

IP2Location Telegram Bot	ip2location 49.205.252.179
IP2Proxy Telegram Bot	ip2proxy 49.205.252.179

IP Change Email Notification

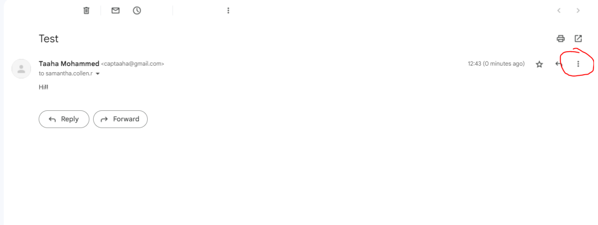
[†] Latitude and Longitude are often near the center of population. These values are not precise and should not be used to identify a particular address or household.

7. https://www.ip2location.com/49.205.252.179

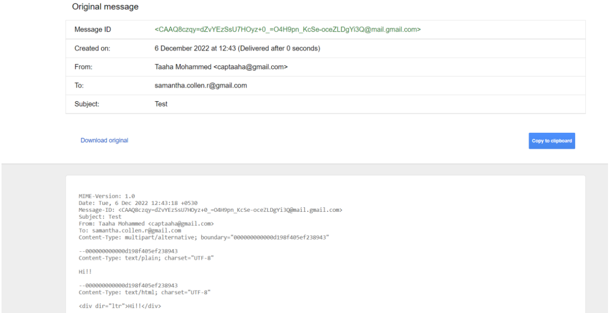
===

Task5: Submit the complete incidence report

Incident Report:

Threat Description	Credential Hijacking using MITM attack
Threat Target	Samantha Collen R. - University Faculty
Attack Techniques	Social Engineering and Footprinting with MITM attack
Control/ Countermeasures	Banner Grabbing and identifying vulnerable ports of the target device
Artifact Hijacked	Personal email ID of victim – samantha.collen.r@gmail.com
Threat Statement	 Test Taaha Mohammed <captaaha@gmail.com> to samantha.collen.r 12:43 (0 minutes ago) Hi!!
Collected Artifacts from Incident Response Team/ Other Artifacts	1. Server IP = 192.18.0.123 2. Victim IP = 192.168.0.163 3. CVE-2021-41773 - Apache HTTP Server Path Traversal Vulnerability 4. Score is 7.5 5. Default Gateway IP is 192.168.0.1 6. Victim machine IP is 192.168.0.163 (Marked as red for MITM attack) 7. MAC address of source is 90-E8-68-4B-D9-1D 8. MAC address of Destination is 00-0C-29-15-01-E3

Attacker Email Summary

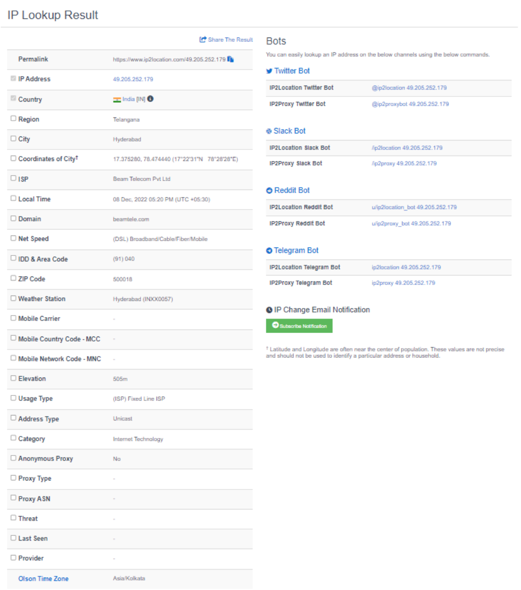


Original message

Message ID	<CAAQ8czqy=dZvYEzSsU7HOyz+0_=O4H9pn_KcSe-oceZLDgYi3Q@mail.gmail.com>
Created on:	6 December 2022 at 12:43 (Delivered after 0 seconds)
From:	Taaha Mohammed <captaaha@gmail.com>
To:	samantha.collen.r@gmail.com
Subject:	Test

```
MIME-Version: 1.0
Date: Tue, 6 Dec 2022 12:43:18 +0530
Message-ID: <CAAQ8czqy=dZvYEzSsU7HOyz+0_=O4H9pn_KcSe-oceZLDgYi3Q@mail.gmail.com>
Subject: Test
From: Taaha Mohammed <captaaha@gmail.com>
To: samantha.collen.r@gmail.com
Content-Type: multipart/alternative; boundary="000000000000d198f405ef238943"

--000000000000d198f405ef238943
Content-Type: text/plain; charset="UTF-8"

Hi!!

--000000000000d198f405ef238943
Content-Type: text/html; charset="UTF-8"

<div dir="ltr">Hi!!</div>
```

Email Forensic Summary



IP Lookup Result

Permalink	https://www.ip2location.com/49.205.252.179
☑ IP Address	49.205.252.179
☑ Country	India [IN]
□ Region	Telangana
□ City	Hyderabad
□ Coordinates of City†	17.375280, 78.474440 (17°22'31"N 78°28'28"E)
□ ISP	Beam Telecom Pvt Ltd
□ Local Time	08 Dec, 2022 05:20 PM (UTC +05:30)
□ Domain	beamtele.com
□ Net Speed	(DSL) Broadband/Cable/Fiber/Mobile
□ IDD & Area Code	(91) 040
□ ZIP Code	500018
□ Weather Station	Hyderabad (INXX0057)
□ Mobile Carrier	-
□ Mobile Country Code - MCC	-
□ Mobile Network Code - MNC	-
□ Elevation	505m
□ Usage Type	(ISP) Fixed Line ISP
□ Address Type	Unicast
□ Category	Internet Technology
□ Anonymous Proxy	No
□ Proxy Type	-
□ Proxy ASN	-
□ Threat	-
□ Last Seen	-
□ Provider	-
Olson Time Zone	Asia/Kolkata

Bots

You can easily lookup an IP address on the below channels using the below commands.

Twitter Bot

IP2Location Twitter Bot	@ip2location 49.205.252.179
IP2Proxy Twitter Bot	@ip2proxybot 49.205.252.179

Slack Bot

IP2Location Slack Bot	/ip2location 49.205.252.179
IP2Proxy Slack Bot	/ip2proxy 49.205.252.179

Reddit Bot

IP2Location Reddit Bot	u/ip2location_bot 49.205.252.179
IP2Proxy Reddit Bot	u/ip2proxy_bot 49.205.252.179

Telegram Bot

IP2Location Telegram Bot	ip2location 49.205.252.179
IP2Proxy Telegram Bot	ip2proxy 49.205.252.179

IP Change Email Notification

† Latitude and Longitude are often near the center of population. These values are not precise and should not be used to identify a particular address or household.