Project Report

Man In the Middle Attack

CompTIA Security+ (SY0-601)

Submitted To : Simplilearn Solutions Pvt. Ltd.

Dated : 16-10-2022

PROJECT 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.

As an investigator, your task is to identify the following:

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.

Solution: Start with a check of IP address on Kali linux machine (attacker machine) by using following command on terminal

#ifconfig

```
Shell No. 1        Shell No. 2        Shell No. 3

root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.4  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe47:3409  prefixlen 64  scopeid 0x20<li
        ether 08:00:27:47:34:09  txqueuelen 1000  (Ethernet)
        RX packets 35764  bytes 45105426 (43.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 25198  bytes 1516586 (1.4 MiB)
        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 125  bytes 12858 (12.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 125  bytes 12858 (12.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~#
```

IP address of Kali Linux machine is : 10.0.2.4

Now scan the entire network by using command netdiscover to find the IP addresses of all the terminals connected with network.

#netdiscover

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

25 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 1500
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.0.2.1        52:54:00:12:35:00      9     540  Unknown vendor
10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.3        08:00:27:fa:65:77      8     480  PCS Systemtechnik GmbH
10.0.2.15       08:00:27:67:2b:0b      7     420  PCS Systemtechnik GmbH
```

IP address of Virtual Box NIC : 10.0.2.3

IP Address of Victim machine (Windows) : 10.0.2.15

Give a try to ping the machine to confirm the connectivity of the 10.0.2.15 machine to find that host is reachable or not.

#ping 10.0.2.15

```
root@kali:~# ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=128 time=0.676 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=128 time=0.823 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=128 time=0.881 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=128 time=0.805 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=128 time=0.736 ms
^C
--- 10.0.2.15 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4066ms
rtt min/avg/max/mdev = 0.676/0.784/0.881/0.071 ms
root@kali:~#
```

Host is reachable. TTL details shows that host machine **TTL value is 128** . Which describes that it could be a windows machine. So to confirm the OS and other details of this machine, Perform the NMAP scan.

#nmap –A 10.0.2.15

-A : Aggressive scan.

```
root@kali:~# nmap -A 10.0.2.15
Starting Nmap 7.91 ( https://nmap.org ) at 2022-10-16 01:51 EDT
Nmap scan report for 10.0.2.15
Host is up (0.00051s latency).
Not shown: 996 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?
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-server-header: Microsoft-HTTPAPI/2.0
| http-title: Service Unavailable
MAC Address: 08:00:27:67:2B:0B (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: general purpose
Running (JUST GUESSING): Microsoft Windows XP|7|2008 (89%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2
Aggressive OS guesses: Microsoft Windows XP SP3 (89%), Microsoft Windows XP SP2 (87%), Microsoft Windows 7 (85%), Microsoft Windows Server 2008 SP1 or Windows Server 2008
R2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| nbstat: NetBIOS name: DESKTOP-QTFASVJ, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:67:2b:0b (Oracle VirtualBox virtual NIC)
| smb2-security-mode:
|   2.02:
|     Message signing enabled but not required
| smb2-time:
|   date: 2022-10-16T05:51:39
|_  start_date: N/A
```

Perform the OS and services versions scan on the windows machine.

#nmap –sV –O 10.0.2.15

-sV : versions of services

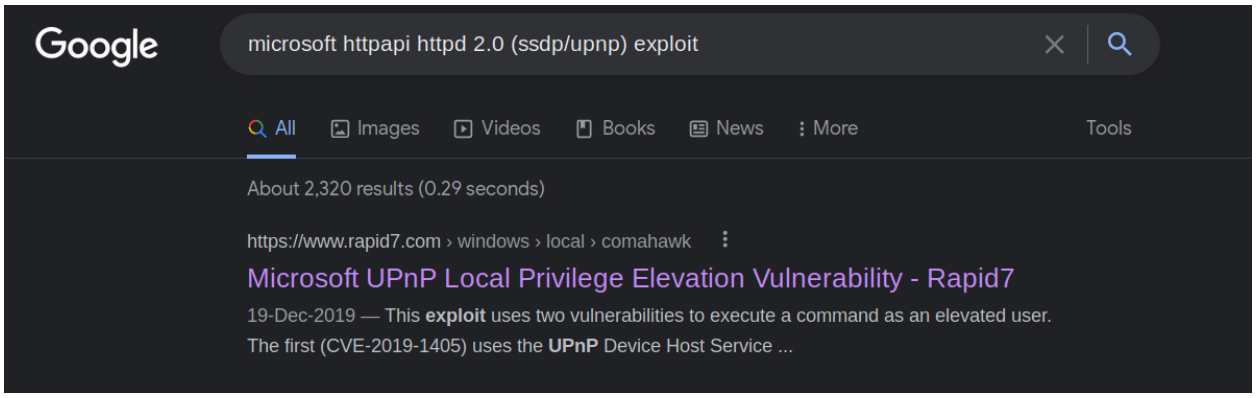
-O : for operating system scan.

```
root@kali:~# nmap -sV -O 10.0.2.15
Starting Nmap 7.91 ( https://nmap.org ) at 2022-10-16 02:01 EDT
Nmap scan report for 10.0.2.15
Host is up (0.00054s latency).
Not shown: 996 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?
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:67:2B:0B (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: general purpose
Running (JUST GUESSING): Microsoft Windows XP|2008|7 (87%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windo
ws_7
Aggressive OS guesses: Microsoft Windows XP SP3 (87%), Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2 (86%), Microsoft Windows XP SP
2 (85%), Microsoft Windows 7 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

From above scan we got the result that port **nos. 135, 139, 445, 5357 are open.**

On port no. 5357 : http service is running.

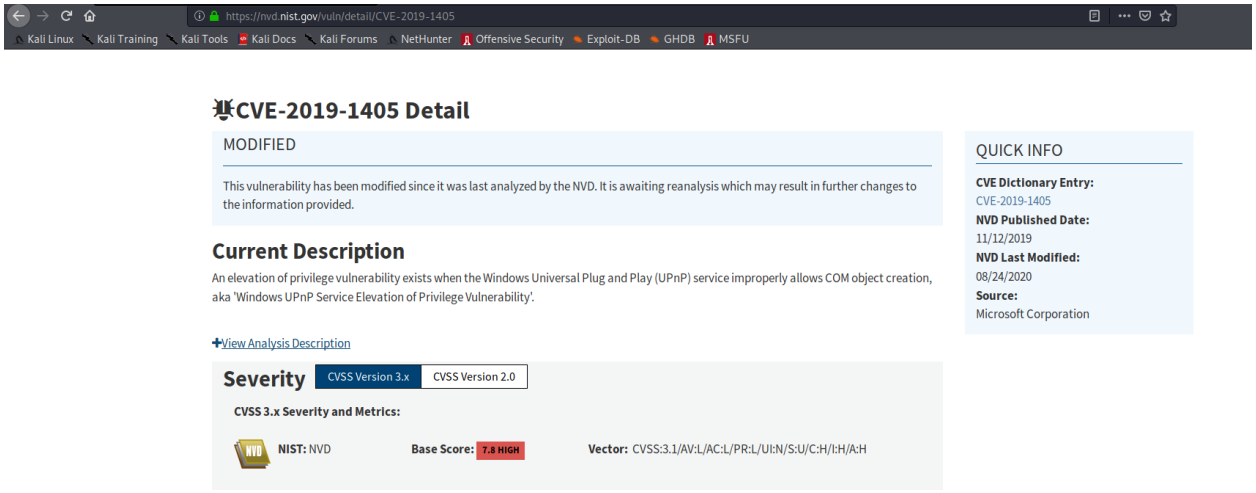
As We know this is not a secure protocol for web server. So we will target this service to find the vulnerability into this service. On this port service Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) is running. Now we will find the exploit against this service which ensures the vulnerability about this service by using google.



Find that using google about http service we found this service is vulnerable to **CVE-2019-1405 .**

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

Solution : Now we need to find the CVE score of this vulnerability by using https://nvd.nist.gov/



Got the result about this vulnerability **.**

CVE Score is 7.8 High.

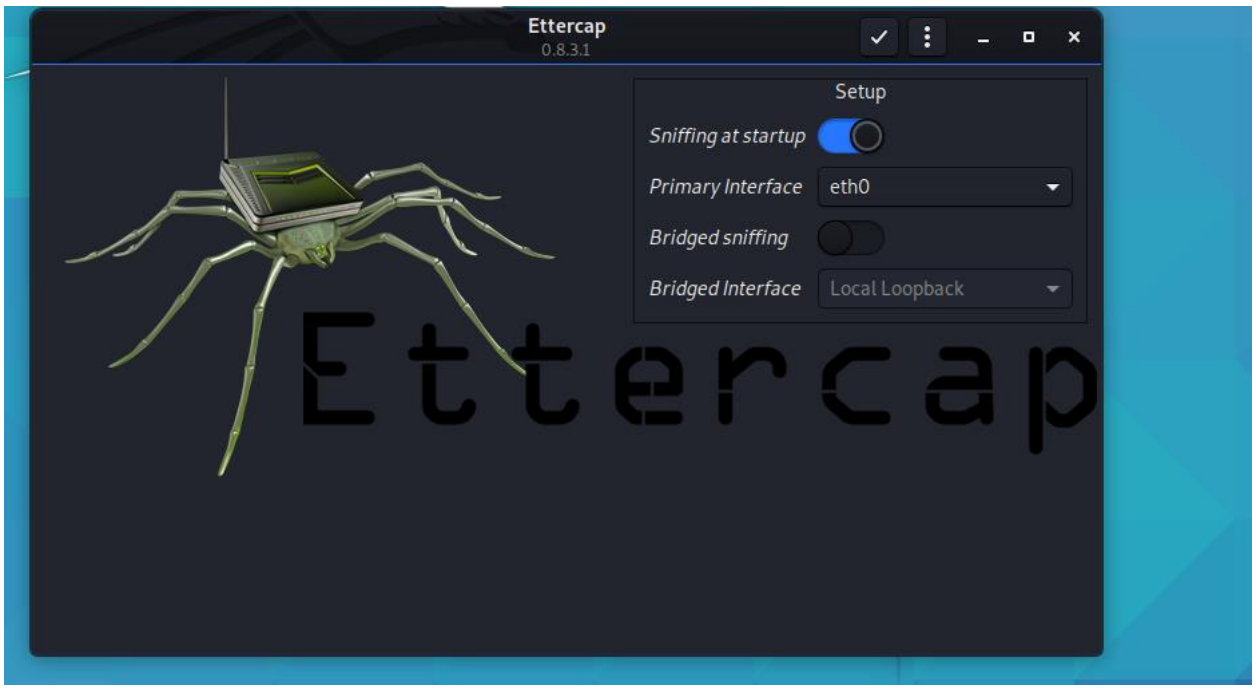
Which describes this is a critical vulnerability.

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

Solution : Victim system is vulnerable to MITM attack. For identification of this , we will perform following steps for MITM attack on victim system.

Step 1 : To ensure the packet flow through attacker system. We will perform the following command on attacker machine (kali terminal)

2. Start the **Ettercap** tool on Kali machine.



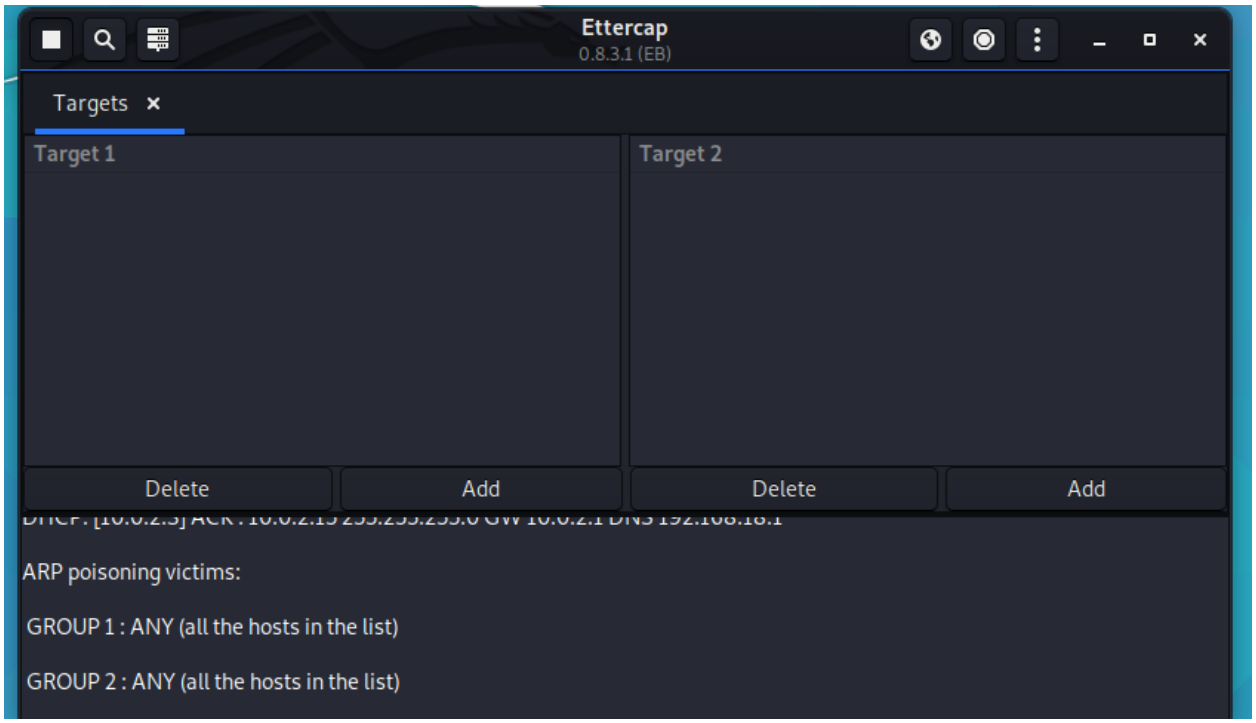
3. Set the interface as your interface name .

In my case name of Interface : eth0

4. Select the targets :

Target 1 : Interface Ip address : 10.0.2.1

Target 2 : Victim Machine IP Address (Windows Machine) : 10.0.2.15



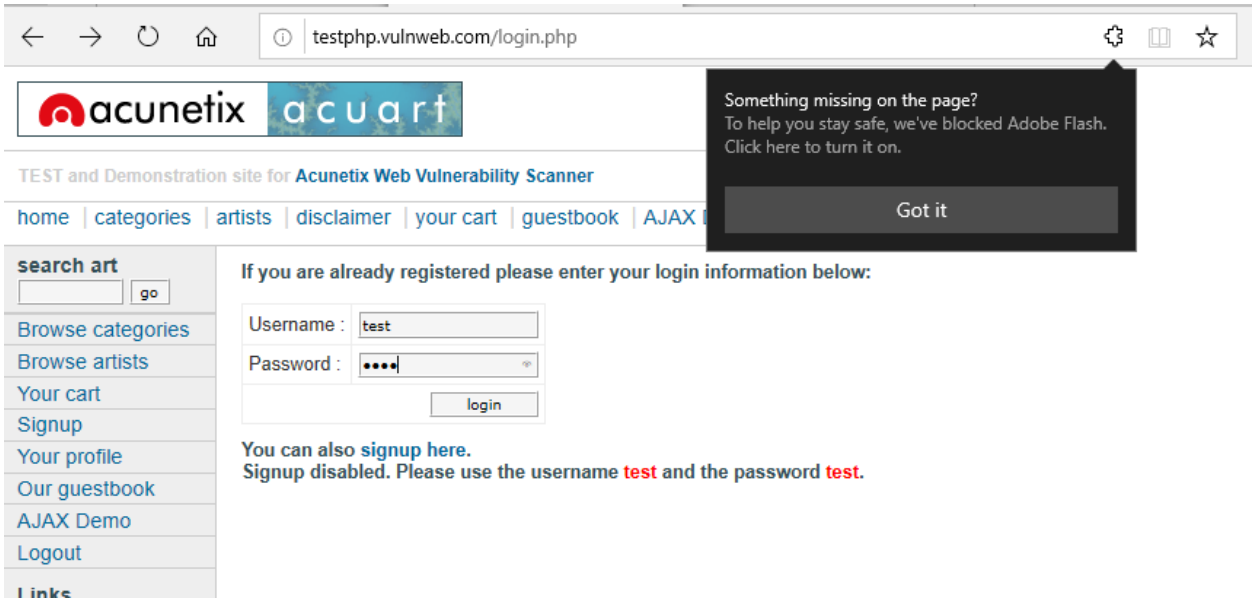
5. After selecting the target Select the **ARP Poisoning** from MITM menu.

6. For sniffing the target we can start **Wireshark packet sniffing tool** on Kali Linux (attacker machine)

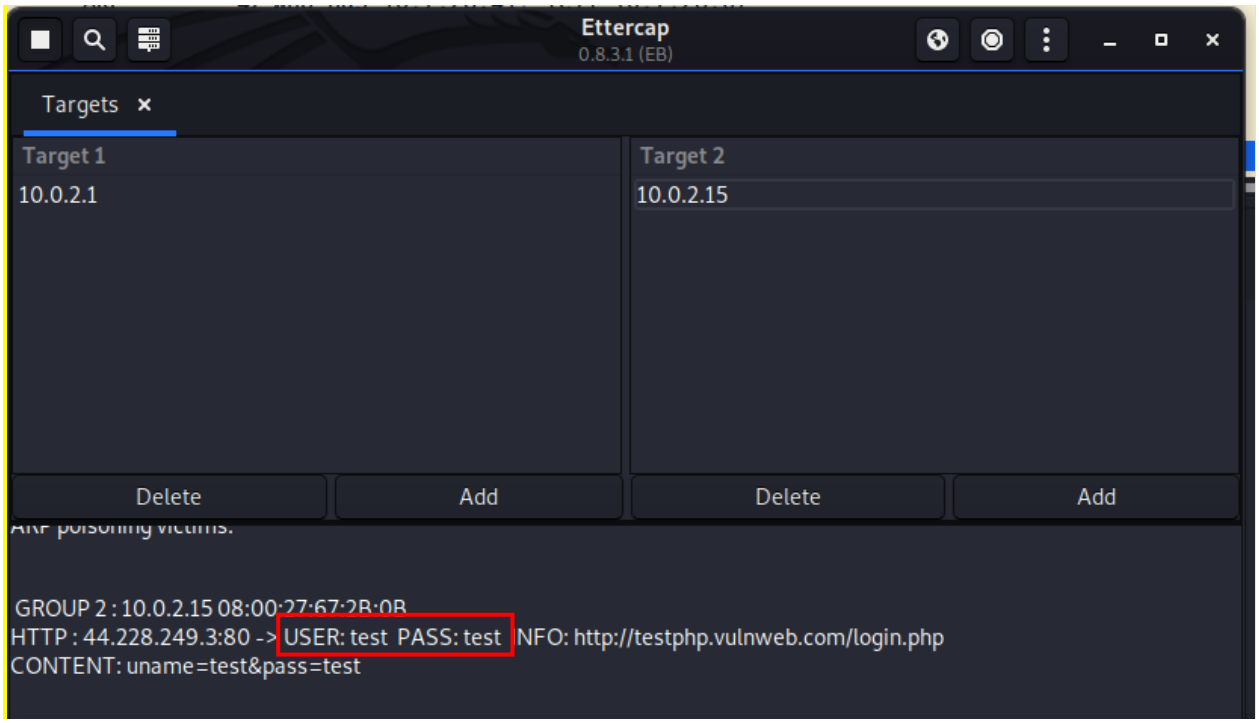
7. Now on victim machine, Open a website and put the credentials for logging in :

User name : test

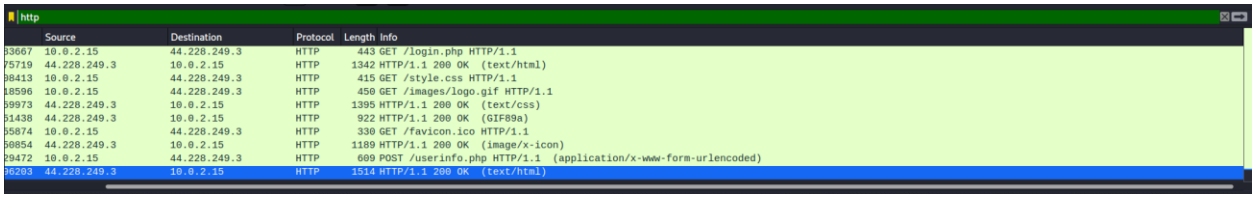
Password : test



8. We can see the hard coded credentials in Ettercap window on attacker machine and also from wireshark packet capture of http.



Wireshark screen shot below for packet sniffing :



http

	Source	Destination	Protocol	Length	Info
33667	10.0.2.15	44.228.249.3	HTTP	443	GET /login.php HTTP/1.1
75719	44.228.249.3	10.0.2.15	HTTP	1342	HTTP/1.1 200 OK (text/html)
38413	10.0.2.15	44.228.249.3	HTTP	415	GET /style.css HTTP/1.1
18596	10.0.2.15	44.228.249.3	HTTP	450	GET /images/logo.gif HTTP/1.1
39973	44.228.249.3	10.0.2.15	HTTP	1395	HTTP/1.1 200 OK (text/css)
31438	44.228.249.3	10.0.2.15	HTTP	922	HTTP/1.1 200 OK (GIF89a)
55874	10.0.2.15	44.228.249.3	HTTP	330	GET /favicon.ico HTTP/1.1
60854	44.228.249.3	10.0.2.15	HTTP	1189	HTTP/1.1 200 OK (image/x-icon)
29472	10.0.2.15	44.228.249.3	HTTP	609	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
96203	44.228.249.3	10.0.2.15	HTTP	1514	HTTP/1.1 200 OK (text/html)

```
⊞ Frame 42851: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface eth0, id 0
⊞ Ethernet II, Src: RealtekU_12:35:00 (52:54:00:12:35:00), Dst: PcsCompu_67:2b:0b (08:00:27:67:2b:0b)
⊞ Internet Protocol Version 4, Src: 44.228.249.3, Dst: 10.0.2.15
⊞ Transmission Control Protocol, Src Port: 80, Dst Port: 50458, Seq: 8361, Ack: 952, Len: 1460
⊞ [2 Reassembled TCP Segments (2920 bytes): #42850(1460), #42851(1460)]
⊟ Hypertext Transfer Protocol
  ⊞ HTTP/1.1 200 OK\r\n
    Server: nginx/1.19.0\r\n
    Date: Sun, 16 Oct 2022 07:07:40 GMT\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    Transfer-Encoding: chunked\r\n
    Connection: keep-alive\r\n
    X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1\r\n
    Set-Cookie: login=test%2Ftest\r\n
    Content-Encoding: gzip\r\n
    \r\n
    [HTTP response 2/2]
```

We can see the plaintext credentials in highlighted area . It ensures that MITM attack on Victim machine .

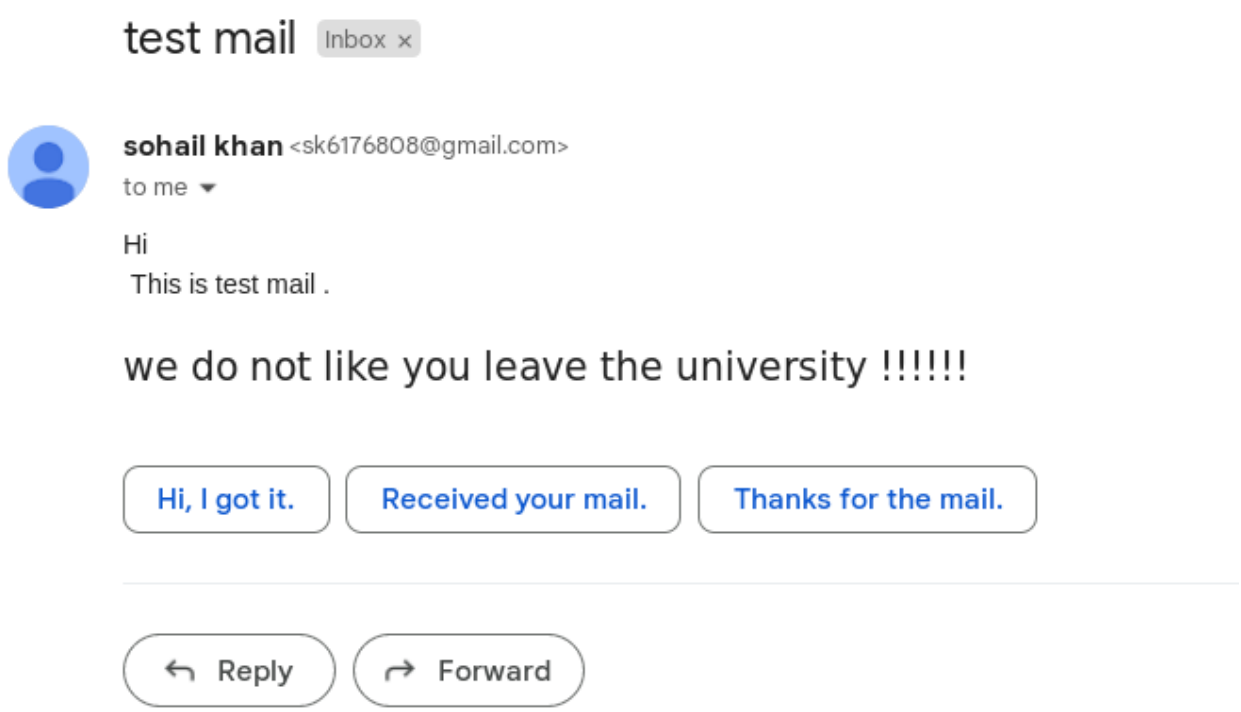
Task 4: **Use email forensics analysis and identify the sender's IP address**

(For project purpose I am using following dummy email ids:

dummy email id for student **: sk6176808@gmail.com**

Dummy email id for teaching staff member : **Samantha6176808@gmail.com**

Solution :

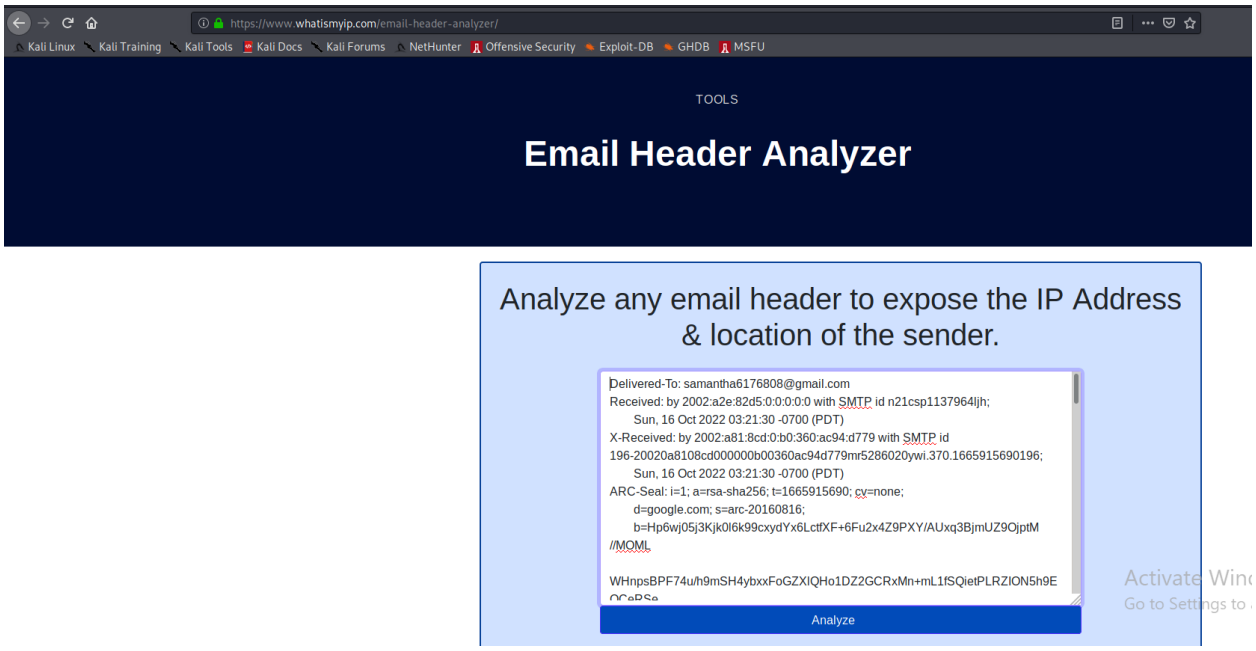


Now **Click on the Three dots on the right corner** of email. And Click on the option : **Show original**

It will display the following screen.

```
Delivered-To: samantha6176808@gmail.com
Received: by 2002:a2e:82d5:0:0:0:0:0 with SMTP id n21csp1137964ljh;
        Sun, 16 Oct 2022 03:21:30 -0700 (PDT)
X-Received: by 2002:a81:8cd:0:b0:360:ac94:d779 with SMTP id 196-20020a8108cd000000b00360ac94d779mr5286020ywi.370.1665915690196;
        Sun, 16 Oct 2022 03:21:30 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1665915690; cv=none;
        d=google.com; s=arc-20160816;
        b=Hp6wj05j3Kjk0l6k99cxydYx6LctfXF+6Fu2x4Z9PXY/AUxq3BjmUZ9OjptM//MOML
         WHnpsBPF74u/h9mSH4ybxxFoGZXlQHo1DZ2GCRxMn+mL1fSQietPLRZION5h9EOCeRSe
         qcpzUjKb3KU9qDdwYmepW9zPMoQP0FnutDZfy2ByhKh4h39bBYthzt6xHji9Sq/6h2KI
         WBMIAXdzKVB1w4vtj0PyfiS2SH5dOnjWa+4wtNVGKvh5bfNLFP9Reg3ApebNVlyMggdm
         dUdaV704RbtFTKc48J94QWyttOxEoRkuq4MZoMi4L22AS1y1SaJITtuyUtLG33X2T08R
         XwtQ==
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=iAbkVHfMThVUokHDvt2E9ykxQkKFQL31CxBzeWhzgzM=;
        b=bqGICtLcZ11Iigr3KnpHjRR5/JCdZ+TbIIdbI00XAefMVwdkryBJrvVkVMPvkCg2cH
         vyIw4A/uEBVNitVoId5L0NZs9VwcxndB95mlDBaMG89XiHKyJAipTt495wJRH1LTNu+F
         m8ndxn/80rlnUKITp2MSPhQmz/ic7fvMOF3JdIf1WG+bVjfHns3Go7wNMOLQqEUoHty+
         PeVaTGj5+ZoGu8Mz6JfcJ0H7upRno/ubxNXt3Dc9qnx26ztxLRfLgGbCZFR30IyxWU7y
         DPij/LHf/6GxqrP8fK+YWNhhzrUG29t8B23cXrgnxSwt/wKbqpgPWZree/9na4tA0Z3T
         gndQ==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@gmail.com header.s=20210112 header.b=AmIEiith;
       spf=pass (google.com: domain of sk6176808@gmail.com designates 209.85.220.41 as permitted sender) smtp.mailfrom=sk6176808@gmail.com;
       dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
Return-Path: <sk6176808@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 n10-20020a5b048a000000b006bebad9accasor2730754ybp.56.2022.10.16.03.21.30
        for <samantha6176808@gmail.com>
        (Google Transport Security);
        Sun, 16 Oct 2022 03:21:30 -0700 (PDT)
Received-SPF: pass (google.com: domain of sk6176808@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=20210112 header.b=AmIEiith;
       spf=pass (google.com: domain of sk6176808@gmail.com designates 209.85.220.41 as permitted sender) smtp.mailfrom=sk6176808@gmail.com;
       dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
```


Copy the above mentioned data and use and **online email tracker** to identify the **IP Address of Sender.**



Email Source IP Info

The email source IP address is 209.85.220.41

The email source IP hostname is mail-sor-f41.google.com.

City:

Country: South Korea

Latitude: 36.5

Longitude: 127.75

By using online email tracker ,

we got the IP address of sender is : 209.85.220.41

THANK YOU