PROJECT #1

TABLE OF CONTENTS

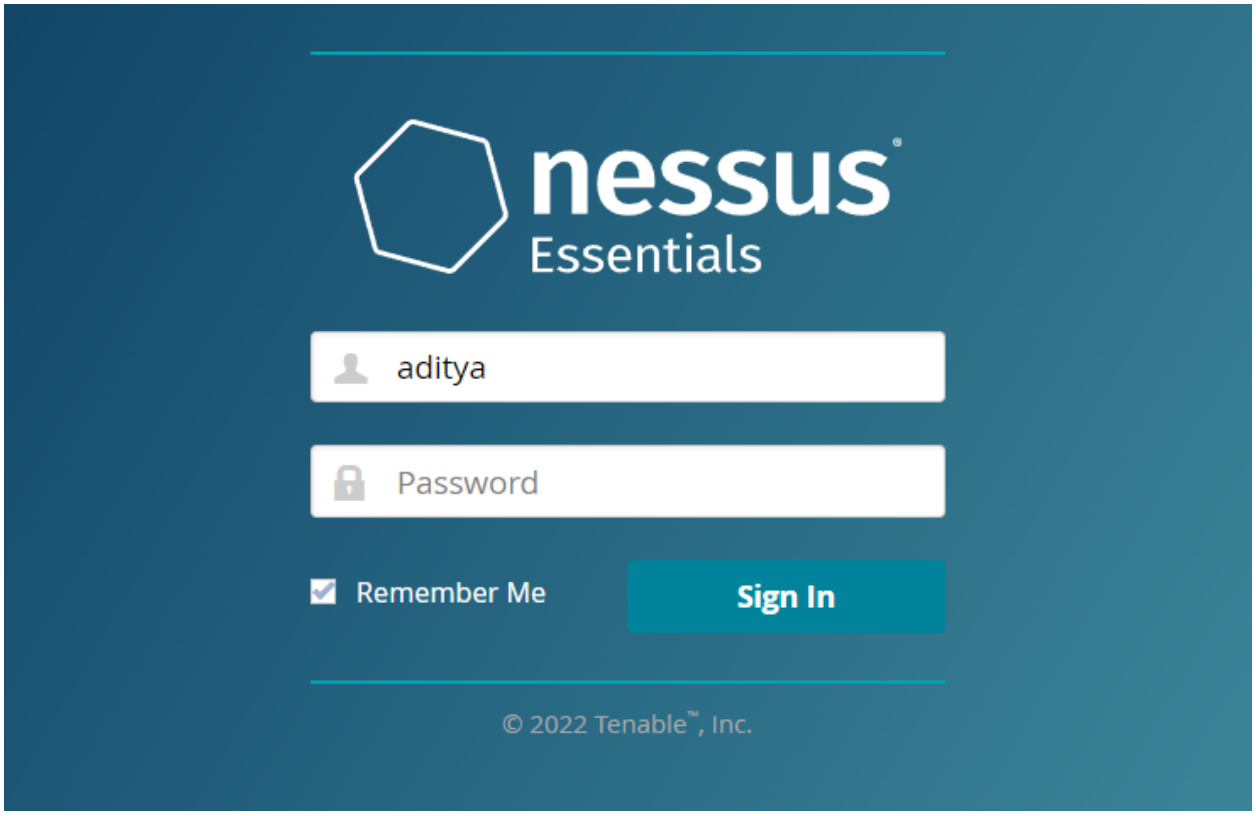
DELIVERABLE 1 :

The first deliverable focuses on finding vulnerabilities in the organization's websites.

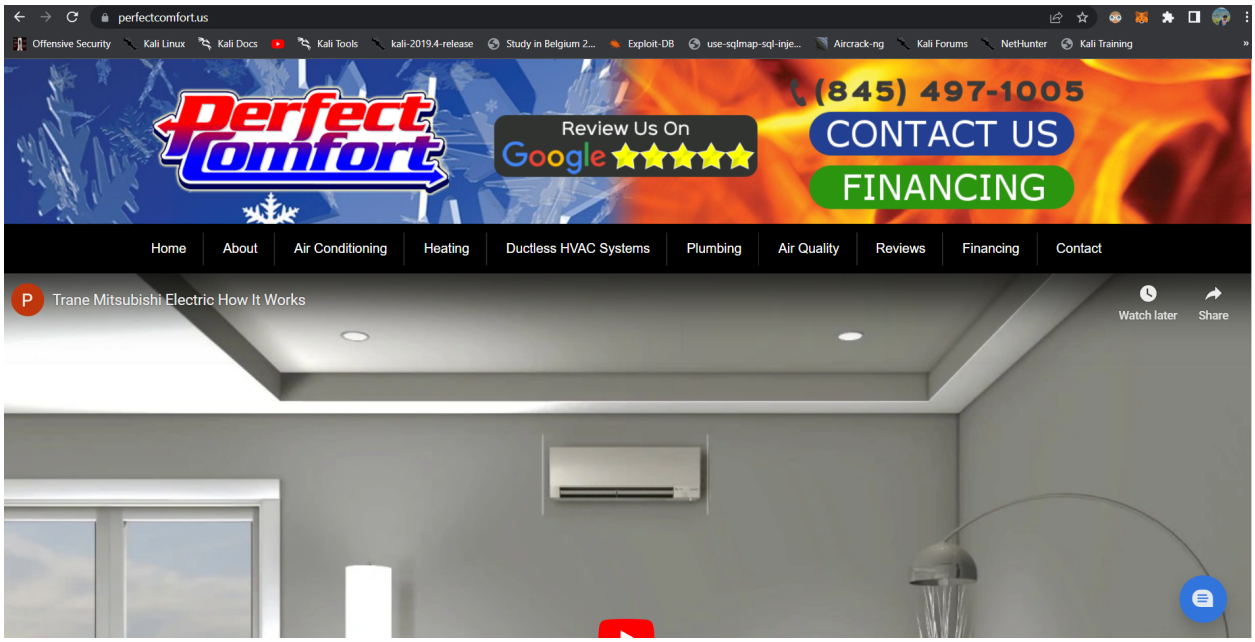
Tools Used -

- **Nessus Vulnerability Scanner**

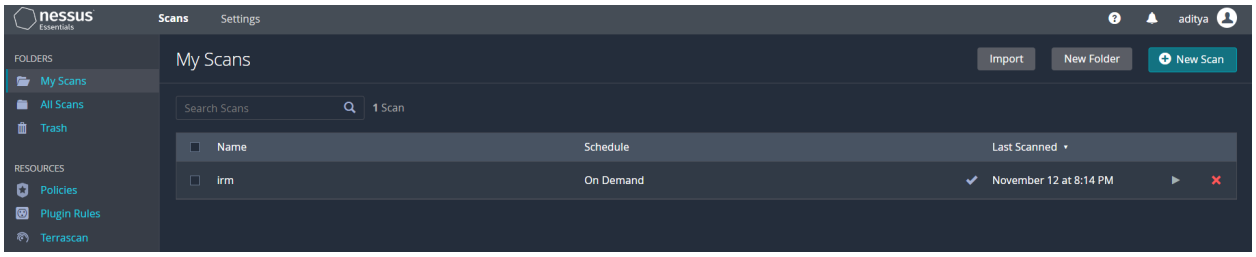
  An open-source network vulnerability scanner is called Nessus. This is employed to identify widespread network vulnerabilities. Nessus Attack Scripting Language (NASL), a scripting language used by the Nessus, is used to specify specific threats and potential attacks. [**Nessus Scan -** Basic Scan.]



Victim Website : https://www.perfectcomfort.us/

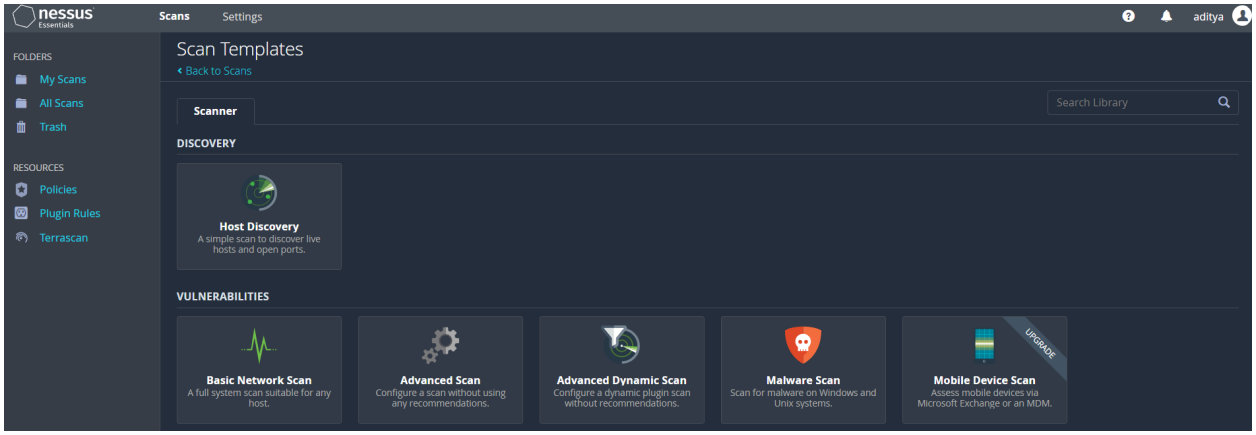


Scanning a website:



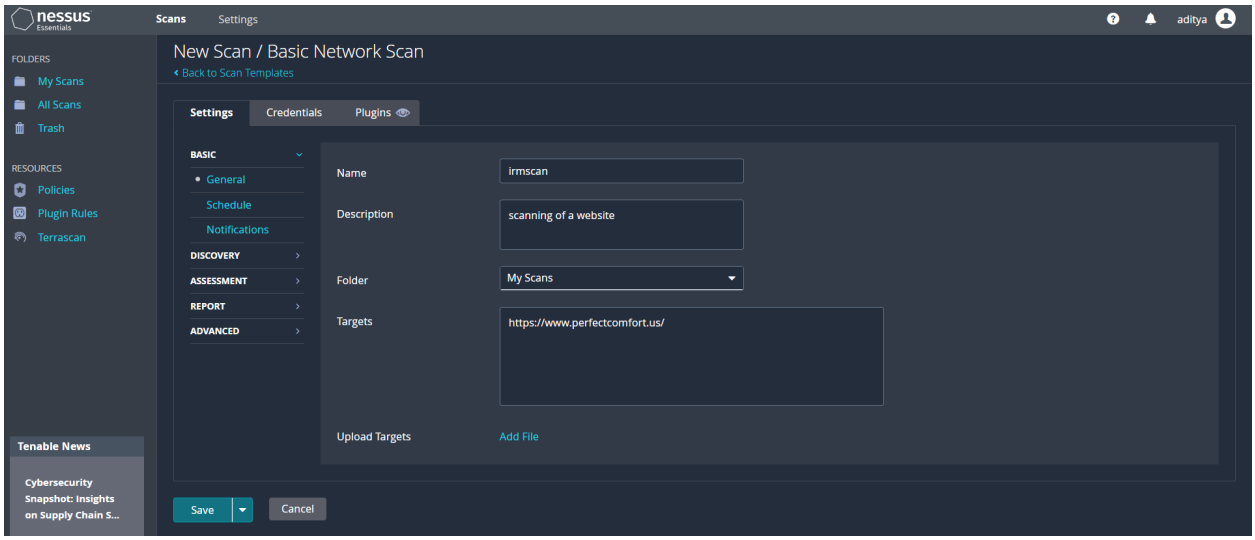
1. Click on the new scan on the top right corner to implement a new scan for a website.

Network Scanning :



1. Click on the Basic network scan. This would allow us to follow through the sequence of steps.

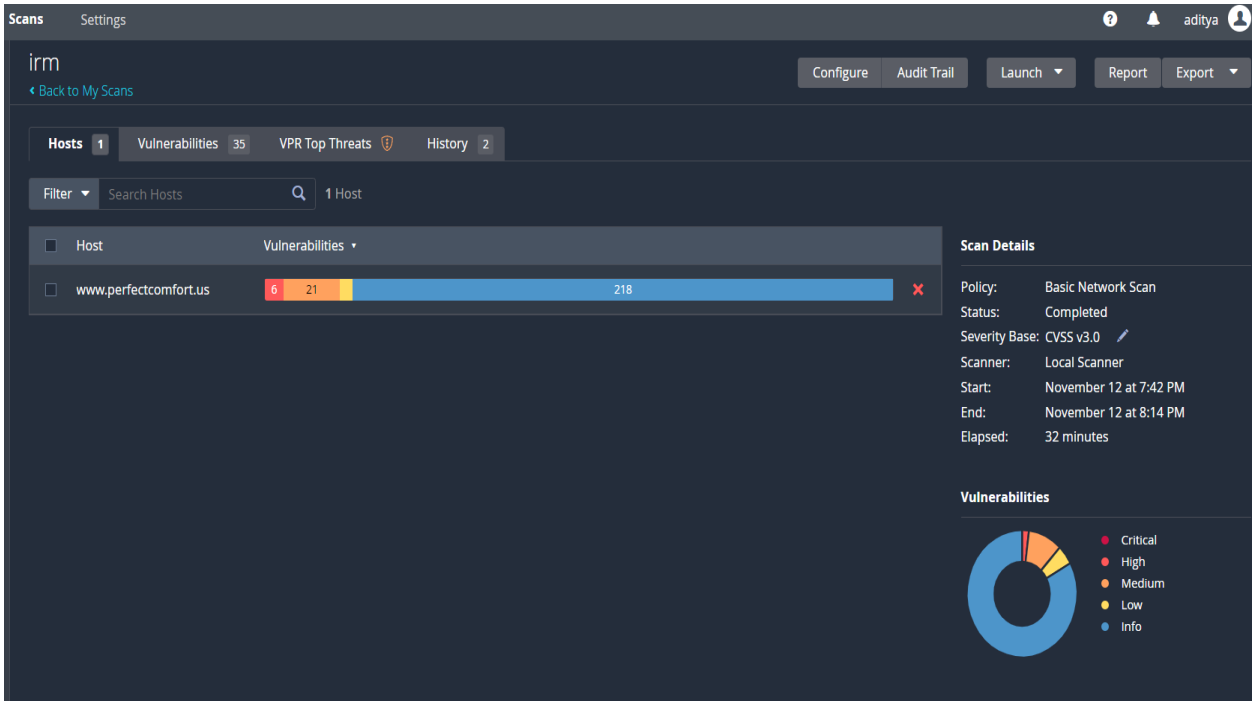
Network Scan II -



1. By clicking on the network scan it would further take us to the page to include information about the target.
2. This includes fields such as -
    - Name
    - Description
    - Folder
    - Targets
3. Click on the save option to save and run the scanner.

EXECUTIVE ANALYSIS :

The target organization is called Perfect Comfort. They sell supplies for different home equipment such as heating, air conditioning, plumbing, and air quality. This website would be essential to grab information about the users who are opting for the service and can be easily targeted.

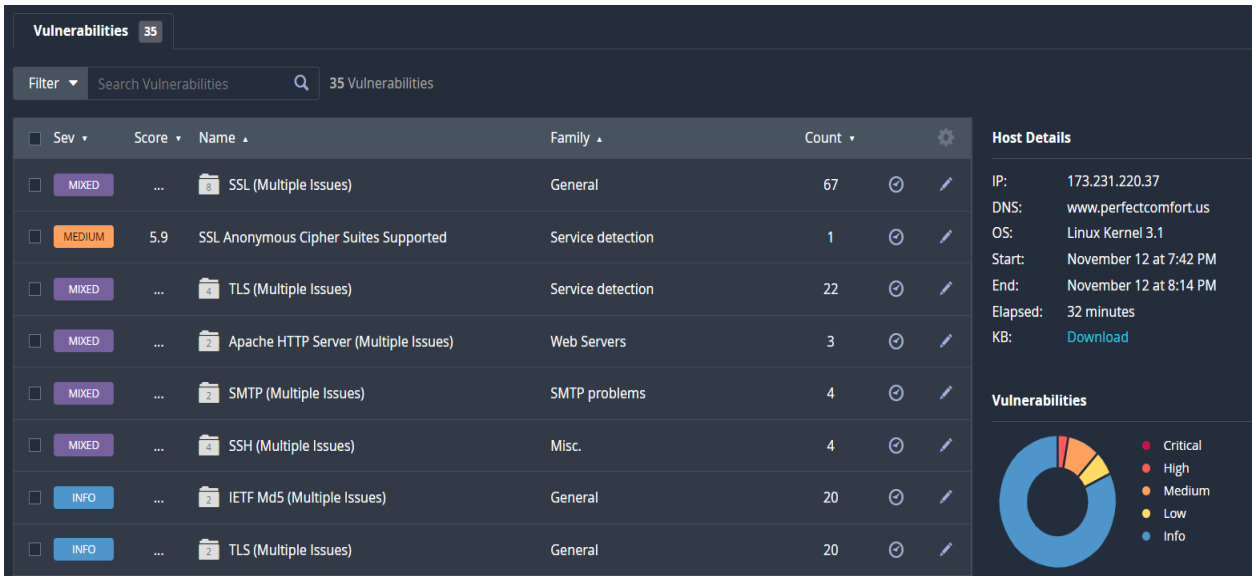


☐ After a successful nessus scan on the website we can observe that the -

- Total number of high vulnerabilities - 6
- Total number of medium vulnerabilities - 21

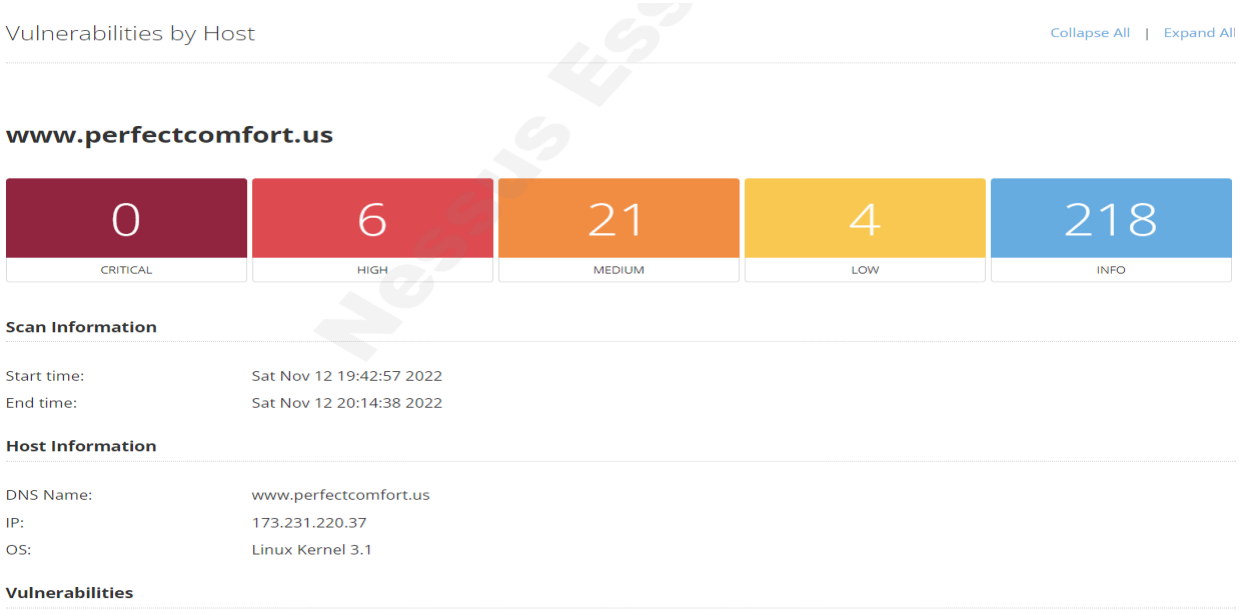
  These can be used to exploit a system or even take control of it.

★ This report would be sent to the following CISO for further inspection.



- ☐ The following image provides us with information regarding the vulnerabilities and other key components. It can also be observed that the "**host details**" provide us with information regarding the host. The details that can be found are -
    - IP
    - DNS
    - OS
    - START
    - END
    - ELAPSED
    - KB

List Of Vulnerabilites :



The given picture describes the vulnerabilities of perfectcomfort.us with both scan information and host information.

CVE	VULNERABILITY NAME	PRIORITY
CVE-2016-2183	42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	1
CVE-2013-2566	65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	2
CVE-2008-5161	70658 - SSH Server CBC Mode Ciphers Enabled	3
CVE-2007-1858	31705 - SSL Anonymous Cipher Suites Supported	4

CVE-1999-0524	10114 - ICMP Timestamp Request Remote Date DisclosureAX	5

PATCHING OF VULNERABILITIES :

- CVE-2016-2183 - TLS, SSH (secure shell), and IPSec are just a few of the protocols that utilize ciphers like DES and triple DES. When used against these lengthy encrypted sessions, a birthday assault by the remote attackers makes it simple to retrieve cleartext. The term "Sweet32" is also used to describe these.

  The CVSS score of the vulnerability is 7.5.
- CVE-2013-2566 - This is an RC4 algorithm; these are used in the TLS and SSl protocols. These consist of single-byte biases, which make it easier for the remote attackers to use plaintext-recovery attacks via ciphertext in a large number of sessions that also use the same plaintext.

  The CVSS score of the vulnerability is 4.3
- CVE-2008-5161 - When utilizing specific algorithms, such as the block cipher algorithm in cipher block chaining (CBC) mode, these are related to error handling in the SSH protocol. It makes it simpler for remote attackers to use unidentified attack vectors to decipher a block of ciphertext in an SSH session and recover specific plaintext data from it.

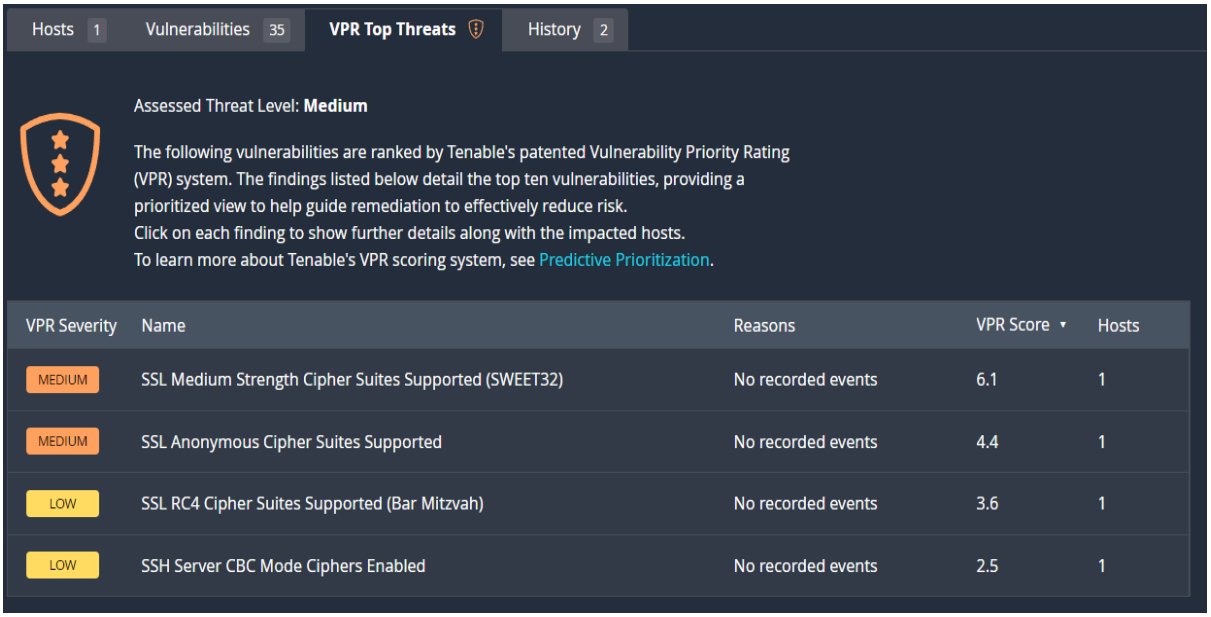
  The CVSS score of the vulnerability is 2.6.
- CVE-2007-1858 - The Apache Tomcat application comes with the standard SSL cipher setup. These employ a number of insurance ciphers, including anonymous ciphers. These make it possible for remote attackers to gather private data.

The CVSS score of the vulnerability is 2.6.

- CVE-1999-0524 - Any host is allowed to send ICMP data like the timestamp and netmask.

  The CVSS score for the vulnerability is 0.0.

➔ All the vulnerabilities have to be addressed. These information are provided in the report file generated with the help of nessus.



VPR Severity	Name	Reasons	VPR Score	Hosts
MEDIUM	SSL Medium Strength Cipher Suites Supported (SWEET32)	No recorded events	6.1	1
MEDIUM	SSL Anonymous Cipher Suites Supported	No recorded events	4.4	1
LOW	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	No recorded events	3.6	1
LOW	SSH Server CBC Mode Ciphers Enabled	No recorded events	2.5	1

The VPR Top threats follows a series of tests, where it assesses the level of threat for the organization. given the specific operations that are performed. The assessed threat level is medium. The further analysation of each and every vulnerabilities can be accessed as -

- Click on vulnerabilities.
- Click on respective vulnerabilities.
- This would further provide respective information about the attack.

MEDIUM SSL Anonymous Cipher Suites Supported

Description

The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

Solution

Reconfigure the affected application if possible to avoid use of weak ciphers.

See Also

http://www.nessus.org/u?3a040ada

Output

```
The following is a list of SSL anonymous ciphers supported by the remote TCP server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                        Code            KEX          Auth     Encryption            MAC
    ----------------------      ----------      ---          ----     --------------------  ---
    ADH-DES-CBC3-SHA            0x00, 0x1B      DH           None     3DES-CBC(168)         SHA1
    AECDH-DES-CBC3-SHA          0xC0, 0x17      ECDH         None     3DES-CBC(168)         SHA1

more...
```

Plugin Details

Severity:	Medium
ID:	31705
Version:	1.30
Type:	remote
Family:	Service detection
Published:	March 28, 2008
Modified:	February 3, 2021

Risk Information

Risk Factor: Low

CVSS v3.0 Base Score 5.9

CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v3.0 Temporal Vector:
CVSS:3.0/E:U/RL:O/RC:C

CVSS v3.0 Temporal Score: 5.2

CVSS v2.0 Base Score: 2.6

CVSS v2.0 Temporal Score: 1.9

CVSS v2.0 Vector:
CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

CVSS v2.0 Temporal Vector:
CVSS2#E:U/RL:OF/RC:C

All the vulnerabilities that do not make it into the top 5 have to be addressed individually, although some vulnerabilities can be easily mitigated. These vulnerabilities also provide information on various sessions and can be helpful in understanding the organization's network.

DELIVERABLE 2 :

This deliverable would provide information on both sides of the red team and blue team developments. Given the scenario to choosing a host, the process is done through 2 systems -

1. **Kali linux** (attacker)
2. **Windows system** (host)

Red Team Scenario :

Given two systems for both attacking and getting information, The given systems are -

Windows IP : 192.168.1.250

Kali Linux IP : 192.168.1.89

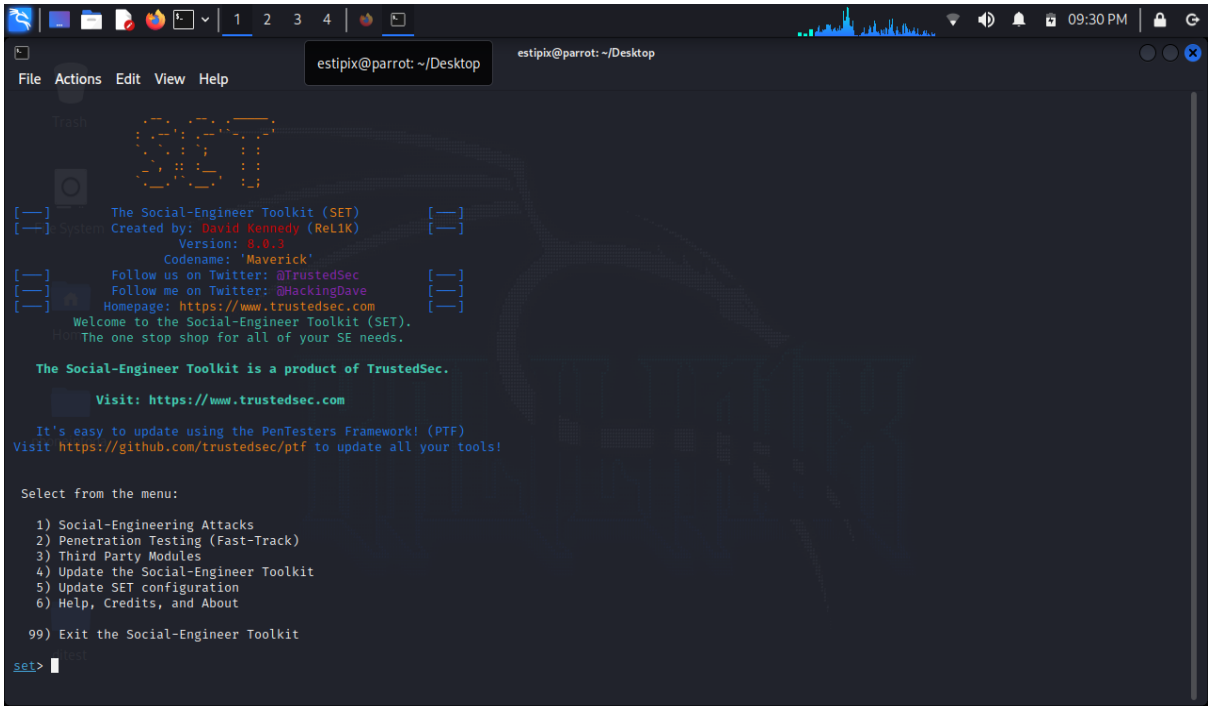
These IP addresses are specific to the systems that are on the same network. These can also be remotely accessed through different means, such as ngrok. This is a service that can be accessed through the command-line interface (terminal).

Attack Scenario (Credential Harvesting) :

The attack is performed through a Kali Linux system. This is a Debian-based penetration testing operating system, and all the operations are performed through the command line interface (Terminal).

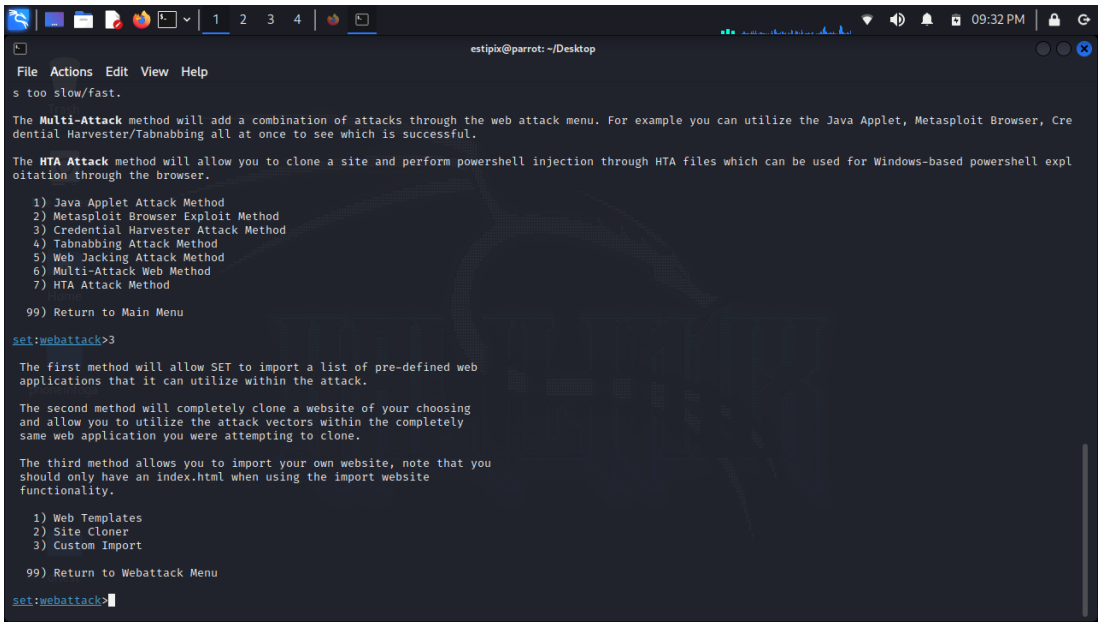
The tools used in the attack scenario are -

- Social engineering attack
- Wireshark



1. The social engineering toolkit is enabled through the command line interface.

   Command - Sudo setoolkit. The sudo command gives the superuser access to the system.

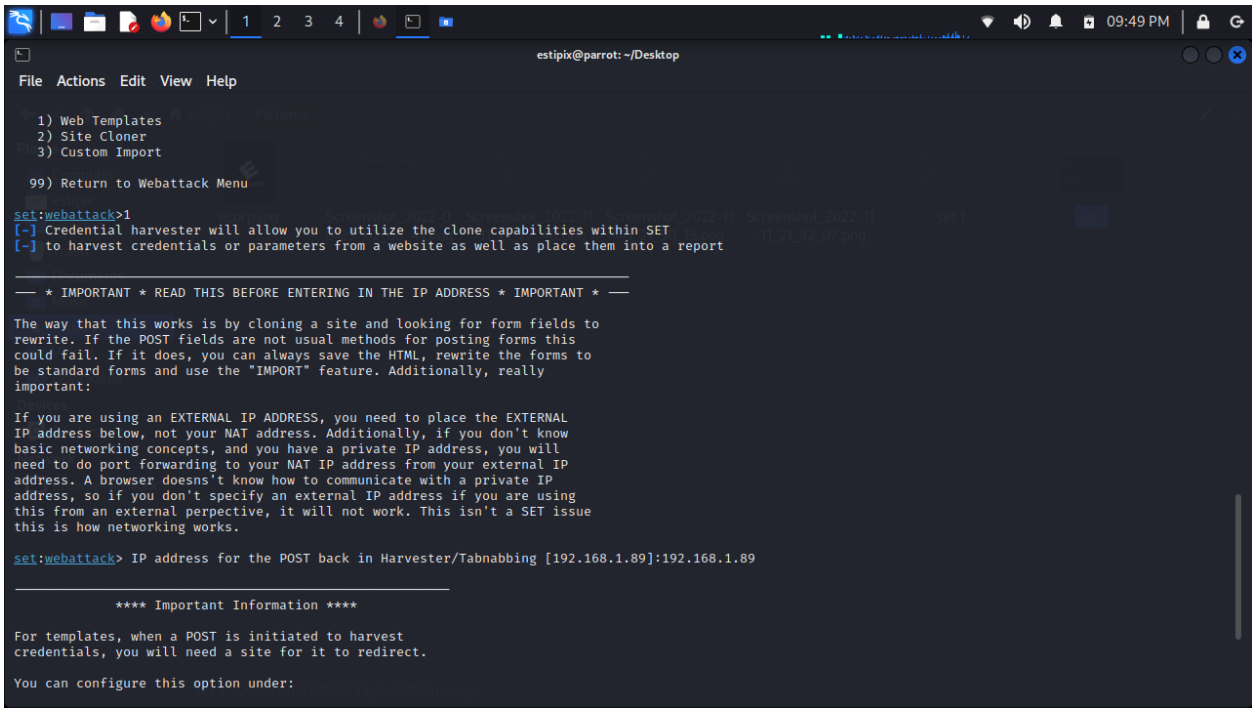


2. The “Social engineering attacks “ are chosen from the list. (option 1)

   This provides additional attack scenarios that can be carried out through the system. Here we would follow a method called “Credential Harvesting."

   Credential Harvesting: This attack would clone a website login page. This includes any page with a login and creates a phishing link that hooks back to the system. This generally gives the attacker the required login credentials to login to the user accounts. This includes -

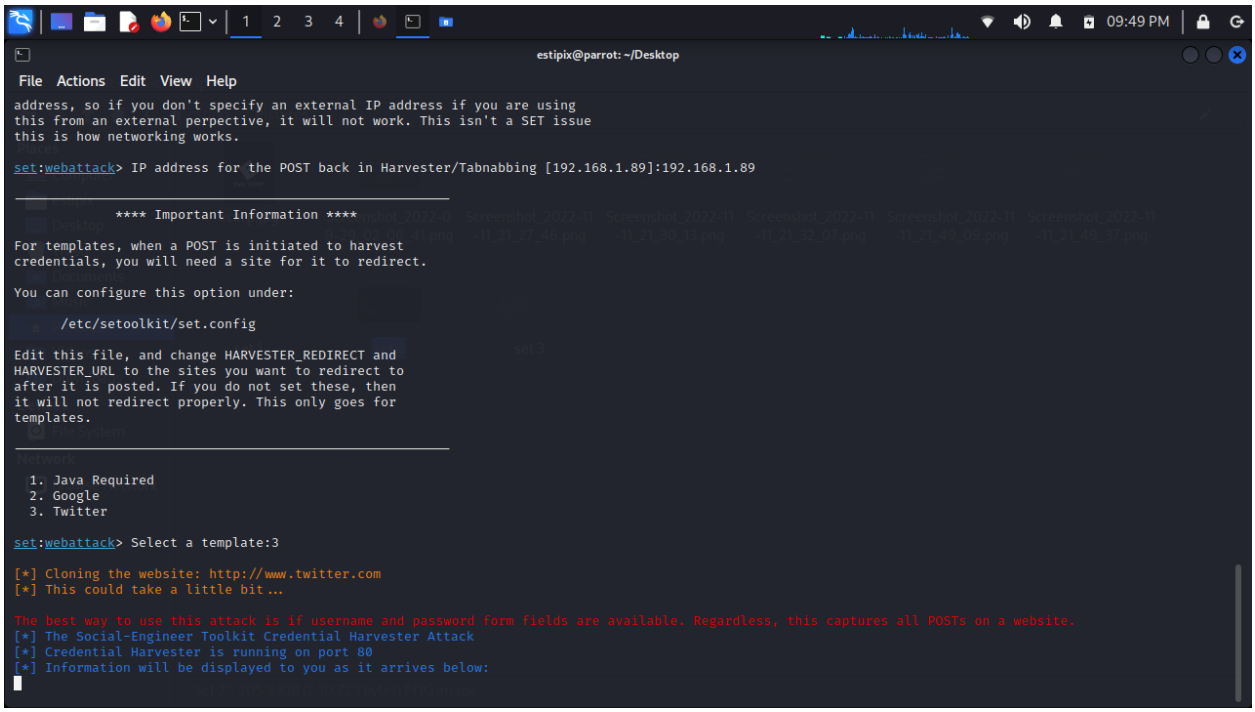
   - Social web pages
   - Corporate login pages
   - Emails
   - Bank page logins



3. Here the credential harvesting page is selected and further gives out the option to enter the IP address for the call back. Here the functionalities of the attack are vast. With the given option of web templates. Here the basic functionality of this selection would clone a web site to create a new one.

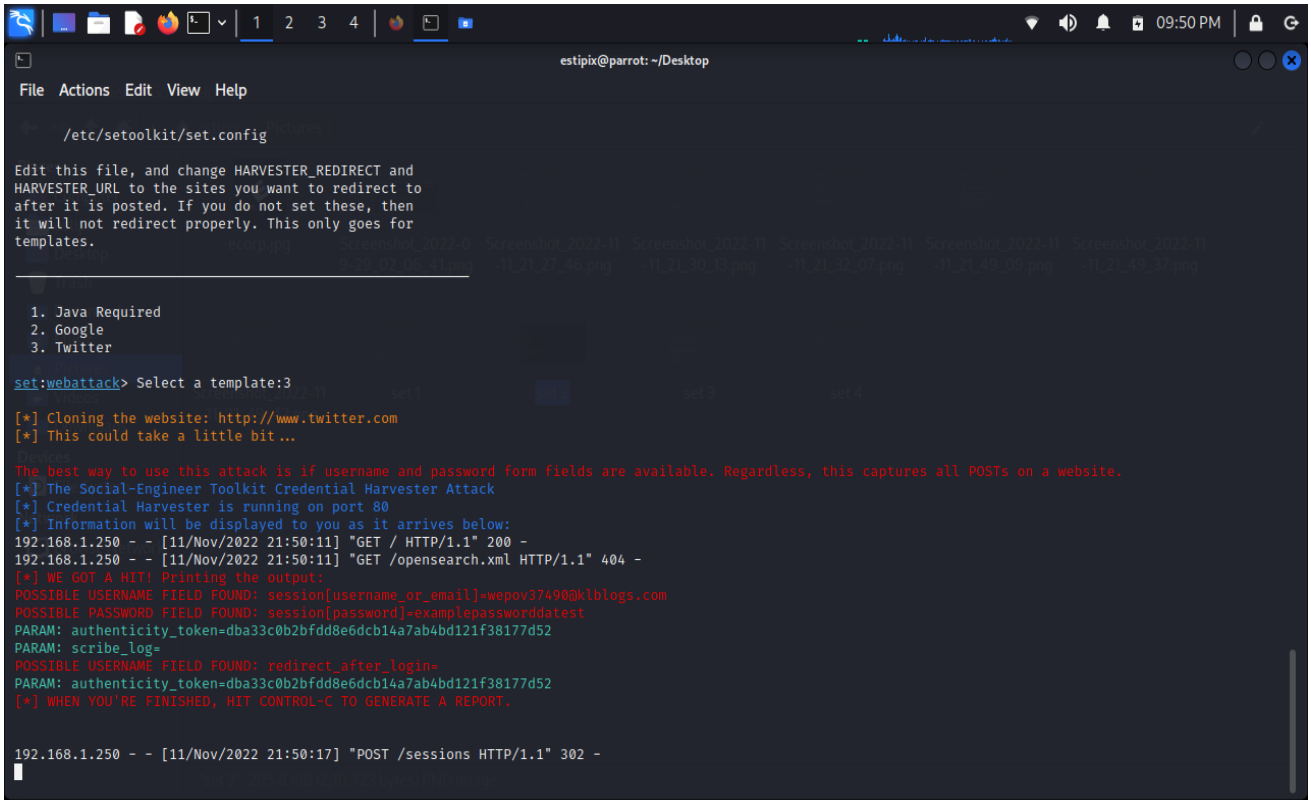
   The “Site cloner” option would also provide the opportunity to enter any login page url, which can be cloned in seconds.

   The Harvester/Tabnabbing IP address is enabled at 192.168.1.89, which is the attacker's machine to receive the information.



4. Here the web template selected is the “twitter” page. This creates a Twitter page login phishing link with the attacker ip address.

   This can be modified through services such as “bit.ly” to create an authentic url to send out to the victim.



5. Here the attack is performed and the phishing link is sent to the victim. Here the victim accessed the login page and has entered the details. The information has come back to the attacker as the attacker placed a harvester IP for the information.

ATTACK REPORT :

- Attack tye - Phishing
- Source - Twitter Login Page
- Feature - Credential Harvesting
- Details - Email : wepov37490@klblogs.com

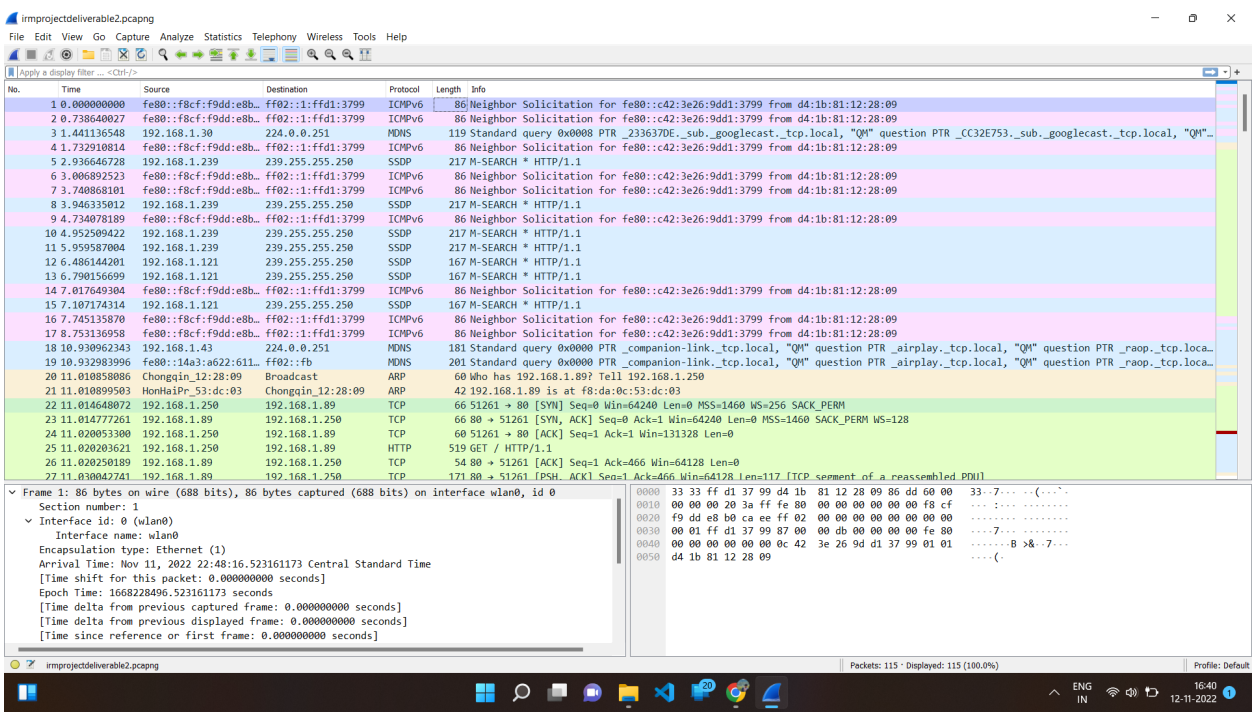
  Password : examplepassworddatest
- Attack status : Successful ✅

Blue Team Scenario :

The network of the company has come under attack. This can subsequently develop in a variety of malicious attacks on the system software, such as privilege escalation and RAT, which would cause the company to suffer enormous financial loss. The blue team has created a report. The following is stated:

INCIDENT : #NTWRKATTCK10-52-86

A certain PCAP file is generated by the network team, and is further processed to be assessed by the blue team.



The given file is the pcap file for the incident, which have

- 155 lines of traffic
- Have different protocols.

  The further implementations and details are provided below -

ARTIFACT LISTING :

The artifact listing has several information regarding the incident, these are -

- Time
- Source IP - 192.168.1.89
- Destination IP - 192.168.1.250
- Protocol
- Length
- Information

ACTIONS TAKEN :

Actions performed in response to the issue must go through specialized teams; this includes setting various priorities, forming teams, and updating software.

Finding Red Flags -

Few of the websites, such as those of banks or businesses, will ask for a particular set of information. This is generally done through sources such as email. If they receive any email requesting certain information on the fields, this has to be treated with suspicion and marked with a red flag.

Password Policies :

Phishing attacks usually make use of human error. These errors are frequently the cause of phishing. Passwords should be updated on a frequent basis to avoid this. By making sure the passwords are well protected, this would give the business defense against phishing scams and malicious actors. One of the best practices would be to use two-factor authentication.

Secure Browsers -

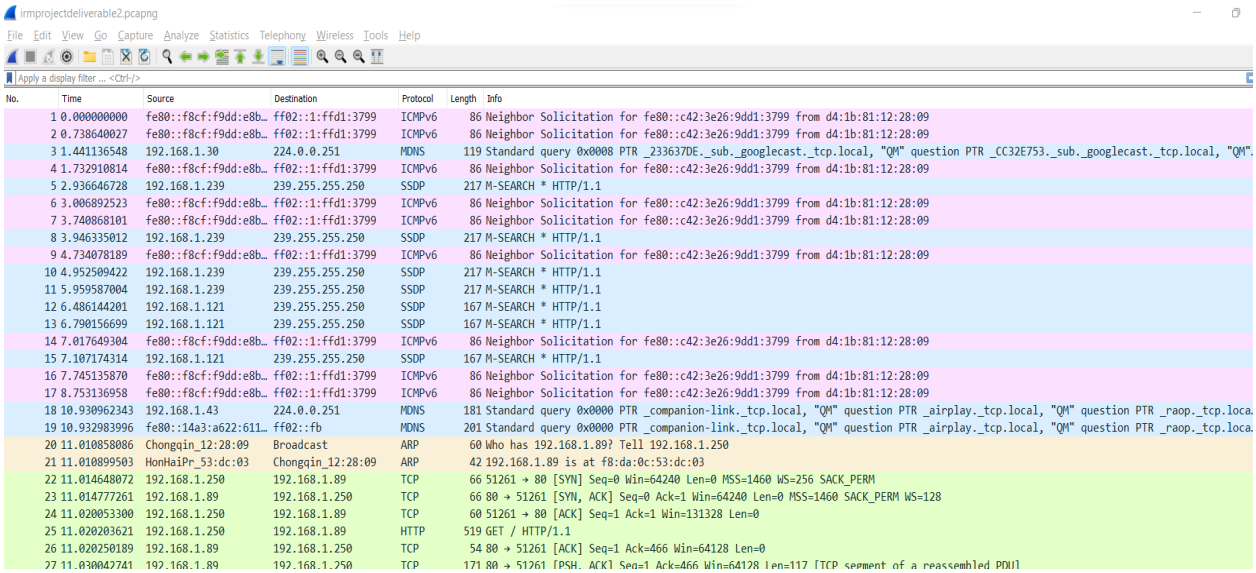
Employee browsers are one of the most important things to consider when preventing phishing attacks. Certain sensitive information, such as cookies and credentials, is at risk of being exploited. The data that the browser stores is one of the key vulnerabilities to be found in the zone of security.

Encryption -

The best way to reduce the possibility of phishing attacks is to encrypt important data. One of the finest ways to use various algorithms to safeguard sensitive data and stop various forms of data breaches is encryption.

<u>ANALYSIS :</u>

Looking at the pcap file has given us a ton of information on various connections, including TCP, IPv4, and ARP.



irmprojectdeliverable2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::f8cf:f9dd:e8b…	ff02::1:ffd1:3799	ICMPv6	86	Neighbor Solicitation for fe80::c42:3e26:9dd1:3799 from d4:1b:81:12:28:09
2	0.738640027	fe80::f8cf:f9dd:e8b…	ff02::1:ffd1:3799	ICMPv6	86	Neighbor Solicitation for fe80::c42:3e26:9dd1:3799 from d4:1b:81:12:28:09
3	1.441136548	192.168.1.30	224.0.0.251	MDNS	119	Standard query 0x0008 PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _CC32E753._sub._googlecast._tcp.local, "QM".
4	1.732910814	fe80::f8cf:f9dd:e8b…	ff02::1:ffd1:3799	ICMPv6	86	Neighbor Solicitation for fe80::c42:3e26:9dd1:3799 from d4:1b:81:12:28:09
5	2.936646728	192.168.1.239	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
6	3.006892523	fe80::f8cf:f9dd:e8b…	ff02::1:ffd1:3799	ICMPv6	86	Neighbor Solicitation for fe80::c42:3e26:9dd1:3799 from d4:1b:81:12:28:09
7	3.740868101	fe80::f8cf:f9dd:e8b…	ff02::1:ffd1:3799	ICMPv6	86	Neighbor Solicitation for fe80::c42:3e26:9dd1:3799 from d4:1b:81:12:28:09
8	3.946335012	192.168.1.239	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
9	4.734078189	fe80::f8cf:f9dd:e8b…	ff02::1:ffd1:3799	ICMPv6	86	Neighbor Solicitation for fe80::c42:3e26:9dd1:3799 from d4:1b:81:12:28:09
10	4.952509422	192.168.1.239	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
11	5.959587004	192.168.1.239	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
12	6.486144201	192.168.1.121	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
13	6.790156699	192.168.1.121	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
14	7.017649304	fe80::f8cf:f9dd:e8b…	ff02::1:ffd1:3799	ICMPv6	86	Neighbor Solicitation for fe80::c42:3e26:9dd1:3799 from d4:1b:81:12:28:09
15	7.107174314	192.168.1.121	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
16	7.745135870	fe80::f8cf:f9dd:e8b…	ff02::1:ffd1:3799	ICMPv6	86	Neighbor Solicitation for fe80::c42:3e26:9dd1:3799 from d4:1b:81:12:28:09
17	8.753136958	fe80::f8cf:f9dd:e8b…	ff02::1:ffd1:3799	ICMPv6	86	Neighbor Solicitation for fe80::c42:3e26:9dd1:3799 from d4:1b:81:12:28:09
18	10.930962343	192.168.1.43	224.0.0.251	MDNS	181	Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR _airplay._tcp.local, "QM" question PTR _raop._tcp.loca
19	10.932983996	fe80::14a3:a622:611…	ff02::fb	MDNS	201	Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR _airplay._tcp.local, "QM" question PTR _raop._tcp.loca
20	11.010858086	Chongqin_12:28:09	Broadcast	ARP	60	Who has 192.168.1.89? Tell 192.168.1.250
21	11.010899503	HonHaiPr_53:dc:03	Chongqin_12:28:09	ARP	42	192.168.1.89 is at f8:da:0c:53:dc:03
22	11.014648072	192.168.1.250	192.168.1.89	TCP	66	51261 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
23	11.014777261	192.168.1.89	192.168.1.250	TCP	66	80 → 51261 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
24	11.020053300	192.168.1.250	192.168.1.89	TCP	60	51261 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
25	11.020203621	192.168.1.250	192.168.1.89	HTTP	519	GET / HTTP/1.1
26	11.020250189	192.168.1.89	192.168.1.250	TCP	54	80 → 51261 [ACK] Seq=1 Ack=466 Win=64128 Len=0
27	11.030042741	192.168.1.89	192.168.1.250	TCP	171	80 → 51261 [PSH, ACK] Seq=1 Ack=466 Win=64128 Len=117 [TCP segment of a reassembled PDU]

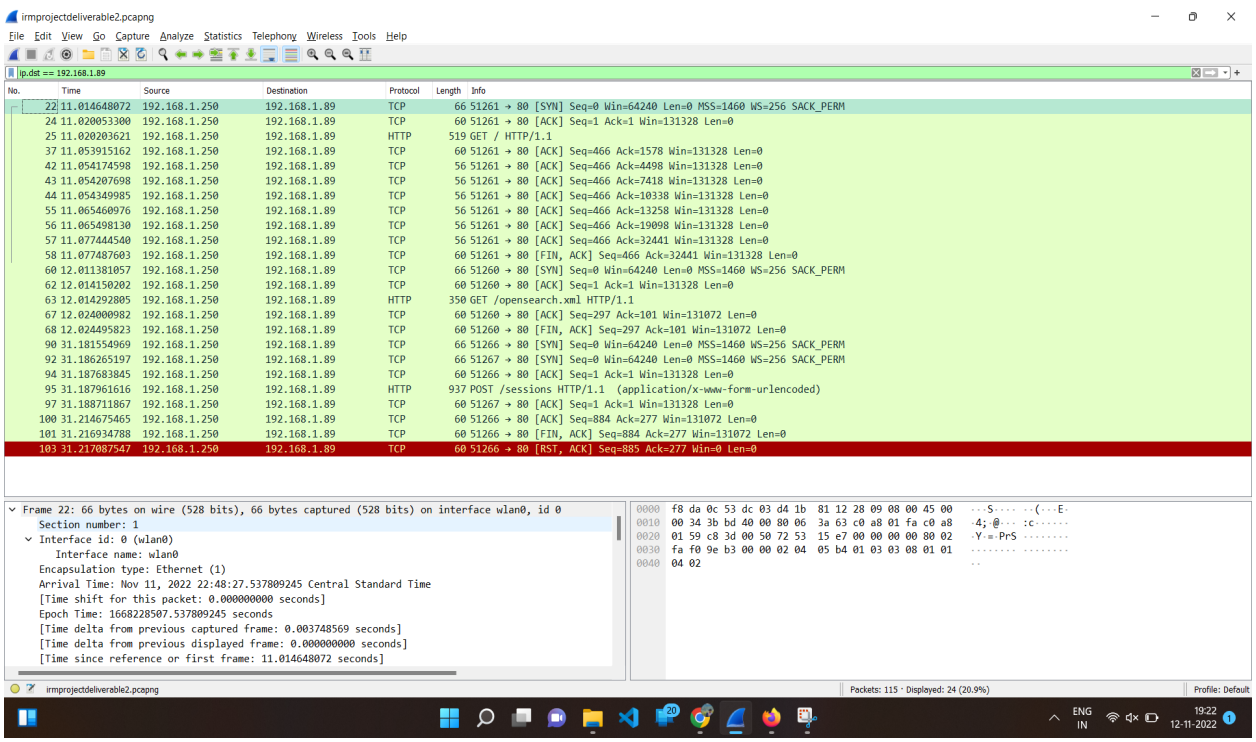
The connections have a lot of transmissions where, the IP addresses from source to destination which are present for a valid amount of time are -

- 192.168.1.89
- 192.168.1.250

These connections have a lot of different transmissions and some of the key details that are to be observed are -

Line 22 - The first handshake

A handshake connection between the source and the destination IP addresses is formed below.



The command for the wireshark, “ ip.dst == 192.168.1.89,” gives out a filter for the data. which provides us with all the destination connections for the IP 192.168.1.89.

Some of the other information regarding the Pcap file is provided below -

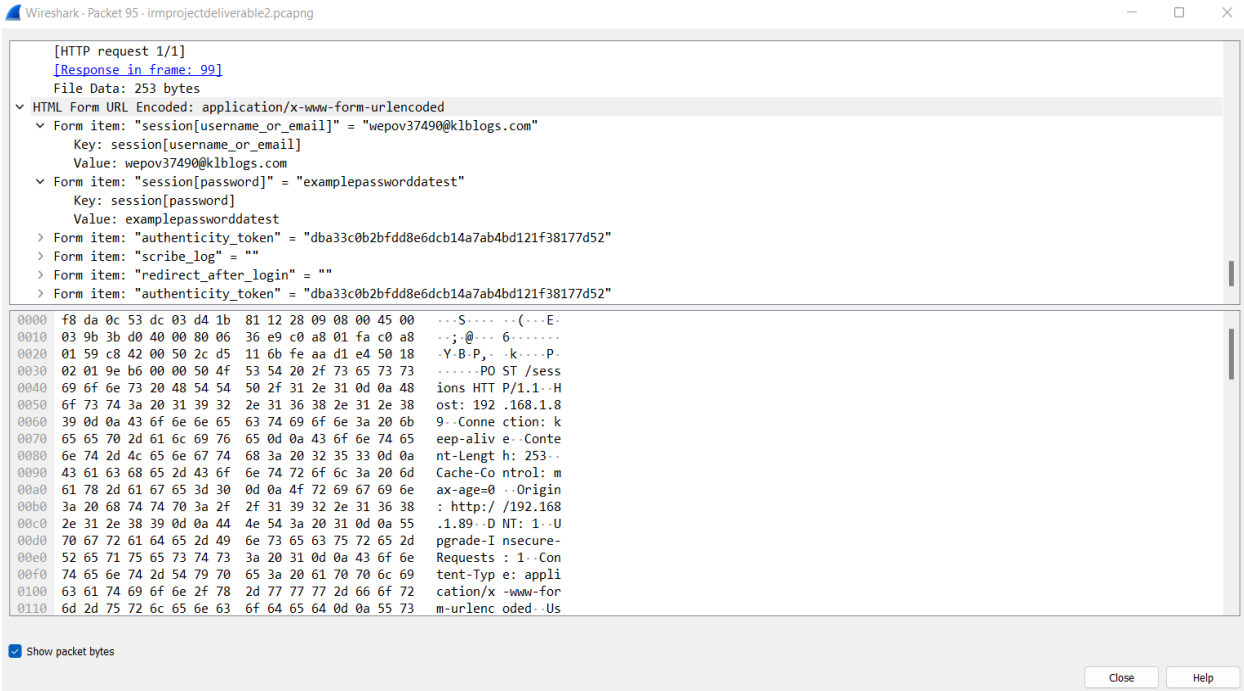
PACKET	DIRECTION	DESCRIPTION
25	192.168.1.250 -> 192.168.1.89	HTTP/1.1 is the most recent version. This runs on top of the TCP/IP suite.
84	Chongquin -> Broadcast	The packet is regarded as broadcast traffic because it is meant for every station in the network. The ARP protocol typically uses something like this.
95	192.168.1.250 -> 192.168.1.89	This gives details on the post-session. This has identified a login attempt from a user on a fake page.
103	192.168.1.250 -> 192.168.1.89	Here, the TCP session is ended. The packet concludes the same session with a RST (reset) message after acknowledging the previous packet in the data stream.

Here, the TCP session has ended. The packet concludes the same session with a RST (reset) message after acknowledging the previous packet in the data stream.

To find out a neighbor's link layer address or to see if the neighbor is available or not, the neighbor solicitation message is sent through the stream. This is also observed through the pcap file provided. The packets such as 1, 2, 4, 6, and 7 provide the information through wireshark.

MAJOR FINDINGS :

One of the major findings in this scenario is the packet capture for the line - 95.



Here we can easily grasp the information that -

- The user account has been compromised.
- The sensitive login information is breached.
- The phishing link is exploited through the victim

<u>CONCLUSION :</u>

Additionally, the IT network team would be given a new assignment for this incident in order to do additional analysis and gather specifics for the report.

The PCAP file has been extensively examined and mined for pertinent information based on the attack. The blue team has prepared the incident report successfully. These attacks can be

defended against in a number of ways. The firms follow thorough incident response plans as well as a variety of procedures to assess functions.

Additionally, the incident has been closed by the respective team, the source and motivation of the attack have been found, and certain measures have been put in place.