INTERNSHIP REPORT

- By Pravesh N

INTRODUCTION:

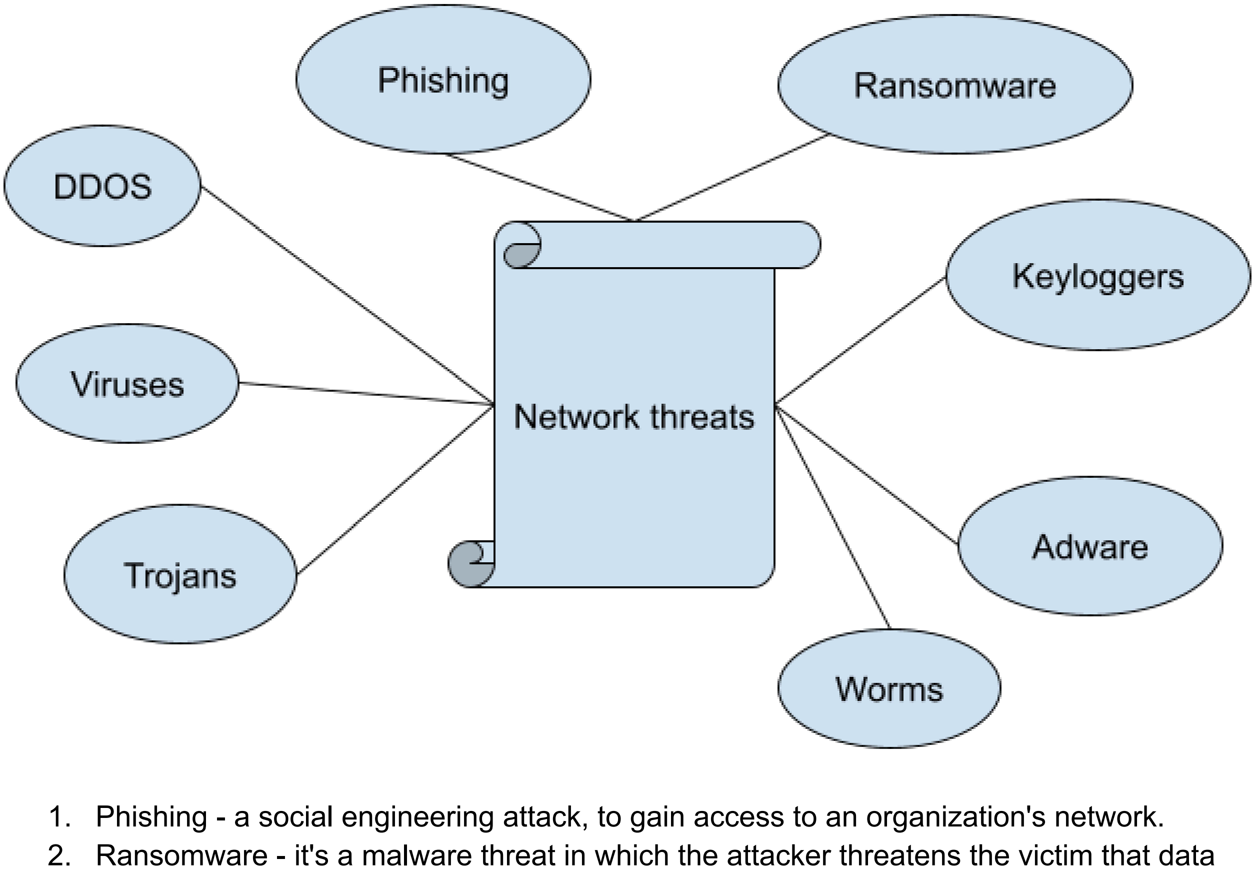
The project which had worked on is basics like setting up a home lab to capture the networks/protocols using the Wireshark tool, to analyze unusual/malicious traffic. Another project which covers web application security (i.e. scanned the website using OWASP Zed Attack Proxy tool to find the attacks/vulnerabilities, also manually exploited and tested the vulnerability in the web application.)

The purpose of my project is to become aware of real-time scenario-based tasks with hands-on practice. So, capable of analyzing the PCAP files on its own and manually exploiting the web application.

TASK OVERVIEW:

TASK - 1(Network security)

Network threats:



1. Phishing - a social engineering attack, to gain access to an organization's network.
2. Ransomware - it's a malware threat in which the attacker threatens the victim that data will leak if a ransom is not paid.

3. DDOS attack - the principle behind it is the flooding of requests sent to the target system/network to stagger the n/w and can easily make the victim's system vulnerable.
4. Viruses - a type of malware that can spread with external action. It is dangerous too and makes it more complex for security professionals to contain the system.
5. Worms - a type of malware that can spread without human interaction. It spreads to new computers through unpatched/compromised accounts if there is a clear entry point.
6. Trojans - also a malware that relies on deception. it can be a virtual legitimate file, users might download and execute it of their violation. Another way of attack is to gain initial access to target network..
7. Keyloggers, infostealers - a collection of sensitive info from an infected computer.
8. Adware and cryptojackers - would use infected machines to earn money for an attacker.

Security measures implemented:(in the system)

- Enabled firewall and WPA2(personal) for network encryption.
- Reason - firewall is to allow only authorised apps and networks into the system and block unauthorized connection requests. WPA2 is the second generation of wifi-protected access, to ensure the network with encrypted and more secure.

The objective was to capture packets and find unusual threats in the home networks. I used the Wireshark tool and analyzed basic network protocols like HTTP, DNS, and TCP.

Steps taken:

1. Constructed the home networks for scanning.

2. In the Wireshark, captured the wireless network which had shown in the tab.

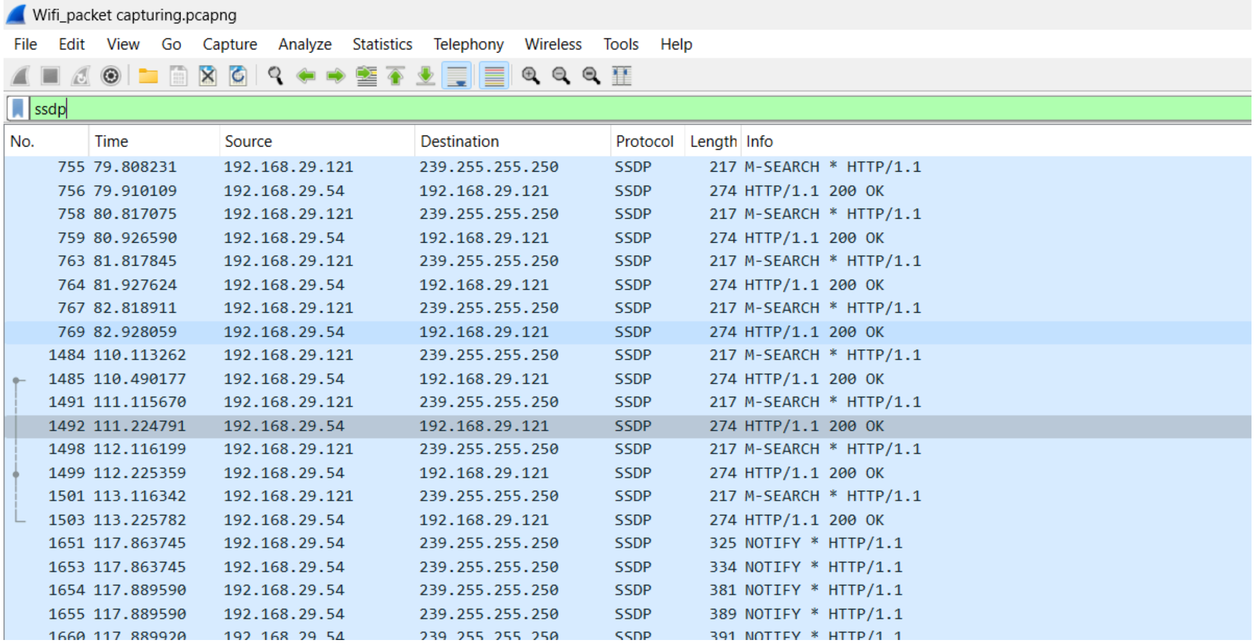
3. Extracted and downloaded as the PCAP file

4. Used basic protocols like HTTP, TCP and DNS which unusual threats might occur.

5. Checked these protocols whether the malicious files uploaded, exhausting traffic occurred in particular IP or not, time duration mismatch and unusual message in encrypted form.

Wireshark(Network monitoring tool):-

>>> Captured my home network traffic using the Wireshark tool.

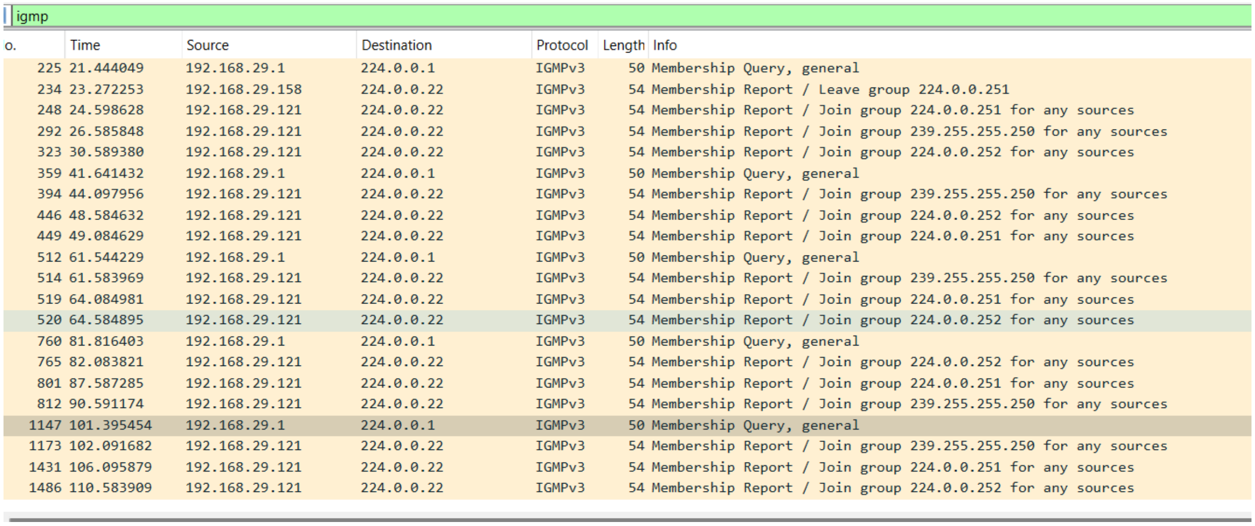


ssdp

No.	Time	Source	Destination	Protocol	Length	Info
755	79.808231	192.168.29.121	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
756	79.910109	192.168.29.54	192.168.29.121	SSDP	274	HTTP/1.1 200 OK
758	80.817075	192.168.29.121	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
759	80.926590	192.168.29.54	192.168.29.121	SSDP	274	HTTP/1.1 200 OK
763	81.817845	192.168.29.121	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
764	81.927624	192.168.29.54	192.168.29.121	SSDP	274	HTTP/1.1 200 OK
767	82.818911	192.168.29.121	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
769	82.928059	192.168.29.54	192.168.29.121	SSDP	274	HTTP/1.1 200 OK
1484	110.113262	192.168.29.121	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
1485	110.490177	192.168.29.54	192.168.29.121	SSDP	274	HTTP/1.1 200 OK
1491	111.115670	192.168.29.121	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
1492	111.224791	192.168.29.54	192.168.29.121	SSDP	274	HTTP/1.1 200 OK
1498	112.116199	192.168.29.121	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
1499	112.225359	192.168.29.54	192.168.29.121	SSDP	274	HTTP/1.1 200 OK
1501	113.116342	192.168.29.121	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
1503	113.225782	192.168.29.54	192.168.29.121	SSDP	274	HTTP/1.1 200 OK
1651	117.863745	192.168.29.54	239.255.255.250	SSDP	325	NOTIFY * HTTP/1.1
1653	117.863745	192.168.29.54	239.255.255.250	SSDP	334	NOTIFY * HTTP/1.1
1654	117.889590	192.168.29.54	239.255.255.250	SSDP	381	NOTIFY * HTTP/1.1
1655	117.889590	192.168.29.54	239.255.255.250	SSDP	389	NOTIFY * HTTP/1.1
1660	117.889920	192.168.29.54	239.255.255.250	SSDP	391	NOTIFY * HTTP/1.1

- In the above picture - SSDP(simple service discovery protocol) requests are more, it shows this protocol is vulnerable to Denial of Service attacks.

- Basic filters like HTTP, DNS, and TCP - there is no vulnerability/unusual traffic found.



igmp

o.	Time	Source	Destination	Protocol	Length	Info
225	21.444049	192.168.29.1	224.0.0.1	IGMPv3	50	Membership Query, general
234	23.272253	192.168.29.158	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.251
248	24.598628	192.168.29.121	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.251 for any sources
292	26.585848	192.168.29.121	224.0.0.22	IGMPv3	54	Membership Report / Join group 239.255.255.250 for any sources
323	30.589380	192.168.29.121	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
359	41.641432	192.168.29.1	224.0.0.1	IGMPv3	50	Membership Query, general
394	44.097956	192.168.29.121	224.0.0.22	IGMPv3	54	Membership Report / Join group 239.255.255.250 for any sources
446	48.584632	192.168.29.121	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
449	49.084629	192.168.29.121	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.251 for any sources
512	61.544229	192.168.29.1	224.0.0.1	IGMPv3	50	Membership Query, general
514	61.583969	192.168.29.121	224.0.0.22	IGMPv3	54	Membership Report / Join group 239.255.255.250 for any sources
519	64.084981	192.168.29.121	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.251 for any sources
520	64.584895	192.168.29.121	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
760	81.816403	192.168.29.1	224.0.0.1	IGMPv3	50	Membership Query, general
765	82.083821	192.168.29.121	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
801	87.587285	192.168.29.121	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.251 for any sources
812	90.591174	192.168.29.121	224.0.0.22	IGMPv3	54	Membership Report / Join group 239.255.255.250 for any sources
1147	101.395454	192.168.29.1	224.0.0.1	IGMPv3	50	Membership Query, general
1173	102.091682	192.168.29.121	224.0.0.22	IGMPv3	54	Membership Report / Join group 239.255.255.250 for any sources
1431	106.095879	192.168.29.121	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.251 for any sources
1486	110.583909	192.168.29.121	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources

- In the above screenshot - IGMP(Internet Group Management Protocol) - flooding of requests in the router side. It might be vulnerable to a DDOS attack if an attacker found this.

- Basic security measures like network scanning, enabling the firewall, and encrypted protocol access make a network secure at both personal(home) and business levels.

Additional security measures:

1. Should monitor the network routinely to avoid any threats, we can also automate this process.
2. Make strict firewall rules and encrypted protocol access.
3. Segment the subnet to enable the different security standards for each level. This would make it easy to isolate any vulnerable segments without affecting the whole system.
4. Device hardening is a must for large and complex networks. Referring NIST and MITRE ATT&CK framework, configuration and security patches should be upgraded wisely.

Network security in everyday use:

Everyone should be educated on network security through a short video through their organisation. Students
should be taught not to misuse hacking tools to avoid legal action. At the organisational level, each employee should be taught the different types of malware so that they would be aware and informed of any priority attacks. Also, they should know to isolate the vulnerable spots to avoid system failure. Teach them how to mitigate immediately with various processes.

Challenges faced:

- I faced a challenge in finding the unusual threat in the packet and rectified this by consulting with my mentor (the red users)
- Finally, I completed my task by myself without any delay. I also noted down each point with screenshots and zipped.