Network Security and Penetration Testing

Prateek Pulastya
MSc. In Cybersecurity
National College of Ireland
Dublin, Ireland
x21112541@student.ncirl.ie

***Abstract*— This research aims to identify the various vulnerabilities that affect the network setup. Through the use of tools such as penetration testing, we can easily identify these issues and implement effective security measures to make our network secure.**

Keywords—Penetration Testing, Network, Security, DoS, XSS, ACE,

I. EXECUTIVE SUMMARY

A penetration test is a type of cybersecurity technique that involves testing the security of a system by identifying and highlighting the vulnerabilities. It can be carried out on various types of computers, servers, and devices. The tester has to perform a series of tasks and operations in order to mimic the actions of an attacker. Although penetration tests are usually performed by professionals, they can be very time-consuming and challenging. During a penetration test, the tester tries to identify and exploit various vulnerabilities in a network. Due to the complexity of a network, it can be very challenging for a professional to carry out a penetration test. Doing so not only helps the organization identify potential security issues, but also provides them with the necessary tools and resources to prevent attacks.

The objective of this report is to analyze the network security of a real-world network setup and to perform penetration testing on it using various tools and techniques. After successfully performing the test, the researcher will be able to identify the security vulnerabilities in the network.

The network is very important when it comes to performing penetration testing. It should be secure, well-maintained, and should allow devices to connect to the internet while the test is being conducted. Due to the rise in cyber-attacks, there has been a need to expand the security measures for networks. A network is a type of communication that connects various devices and allows them to share information or data. This process can be done over a network regardless of whether it's a wired or Wi-Fi connection. When one device connects to the internet, the data that's stored on that device's server is transferred to the other devices.

I choose the private home network to undertake penetration testing and security vulnerability checks on my network. I have many wireless routers for my home network, and they may be abused if not adequately protected. I picked this network because it has all of the necessary equipment, switches, routers, and cables, and if the pen test is performed on my network, I will be able to make it more secure, and the test results will reveal any security weaknesses. There are four people in my house who are connected to the network, one of whom uses a desktop, switches, repeaters, and new cables, so it makes sense for me to utilize my own home network for this research.

This study describes the security vulnerabilities for the private home network configuration, how these attacks are identified using penetration testing, and how they may be mitigated and documented in the networks for future reference using various tools and approaches. Some of the devices linked to my home network are out of date, while others are easily hacked. With the aid of this study, I was able to determine which gadgets needed to be replaced or altered.

Following the release of the latest security reports, I would like to suggest that all network devices be regularly updated to the latest security frameworks. Also, when a device is not working properly, it should be immediately removed or changed.

II. NETWORK SETUP

A network is composed of various devices that are used for various tasks such as transferring data or sharing resources. After conducting research, I get to know about the various devices in the network and their compatibility. This helps me make informed decisions regarding the security of my home network. Through the research, I also learn if a penetration test can be performed on a home network that's composed of such devices.

It was decided that a home network setup should be set up with multiple devices connected to it. This setup should be very complex as there are so many different types of devices (such as routers, switches, and IoT devices) that can be attached to it. To make this setup more real, the latest routers and switches have been added to it.

My home network setup comprised of:

- A Cisco router
- A FortiGate firewall
- A HPE switch
- A Tp-Link wireless access point
- 1 Laptop with windows 10
- 1 Laptop with windows 11
- 1 Smartphones (One plus8t: Android 12)
- 1 Amazon Alexa (IOT device)
- 1 Speaker
- 1 Sony PlayStation 4 gaming console
- 1 Canon printer

Below is the diagram of my home network setup:

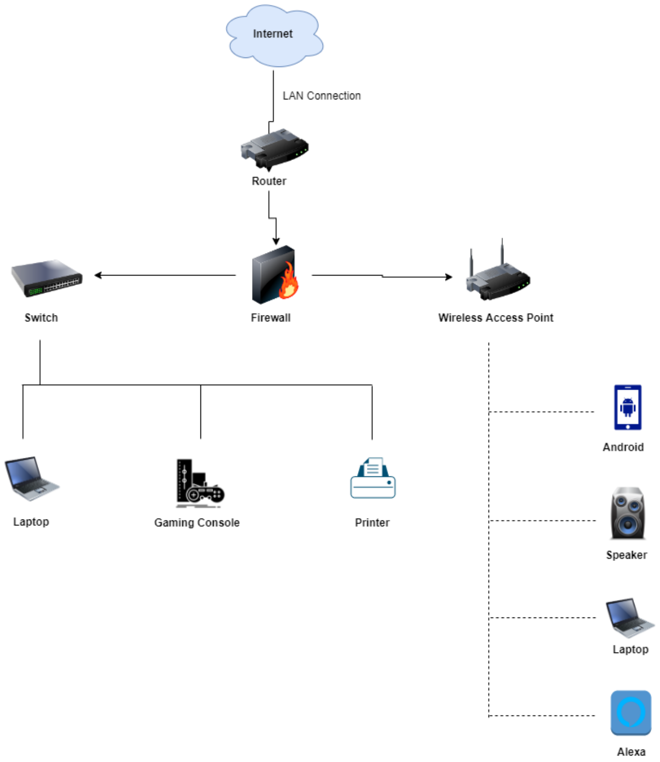

Fig. 1. Network Diagram (Home Network Setup)

The network setup I created is a home network that's connected to a LAN connection. It's made up of various devices, such as smartphones, IoT devices, and other network peripherals. Each of these has its own specification, making it incredibly complex to set up. Aside from being able to perform a pen test, the network setup also serves as a good starting point for testing various security features and updates. The test is carried out in five phases, each of which involves planning, preparation, execution, analysis, and reporting. One of the main goals of the pen test is to determine when it can be run and what type of test can be performed. Aside from this, the network setup also has to be considered. Before establishing a network, research is conducted to identify the various points that will affect its operation.

The table below summarizes all of the network's primary devices:

TABLE I. SUMMARY TABLE I

Hardware Specifications			
Device	***Model Number***	***Manufacturer***	***Release Date***
Router	RV340	Cisco	Feb, 2017
Firewall	Fortinet 80F	FortiGate	July, 2020
Switch	AurbaOS-S	HPE	Feb, 2017
Wireless AP	AC1750	Tp-Link	Oct, 2018
Laptop	Nitro 5	Acer	April, 2019
Laptop	Pavilion	HP	April, 2016
Smartphone	KB2001	One plus	Oct, 2020
IOT device	B8R75E	Amazon	Oct, 2020
Gaming Console	CUH-1023	Sony	Nov, 2020
Printer	LBP2900B	Canon	Sept, 2014

TABLE II. SUMMARY TABLE II

Software Specifications			
Device	***Model Name***	***OS/Firmware Version***	***Release Date***
Router	RV340	Cisco	Feb, 2017
Firewall	Fortinet 80F	FortiOS	July, 2020
Switch	AurbaOS-S	AurbaOS-CX OS	Feb, 2017
Wireless AP	AC1750	Tp-Link	Oct, 2018
Laptop	Nitro 5	Windows 11(22H2)	April, 2019
Laptop	Pavilion	Windows 10 (21H2)	April, 2016
Smartphone	KB2001	Android 12	Oct, 2020
IOT device	B8R75E	Fire OS 5.0	Oct, 2020
Gaming Console	CUH-1023	Orbis OS	Nov, 2020
Printer	LBP2900B	Canon	Sept, 2014

This method is more realistic as most of the devices that are connected to the network have the latest operating systems and software versions. Software companies are not providing patches or updates for older models as they are focused on their sales. Recently, Blackberry sent out a message to its customers stating that after Jan 2022, all of its devices will no longer work. After receiving the same message, I decided to remove the Windows 7 software from my device. According to the research, there are about 200 million Windows 7 users who still use the software as their daily drivers.

My network consists of various devices, such as a dual-WAN Gigabit VPN router and a firewall. First, I will talk about the Cisco RV340 Dual-WAN VPN router, which provides a secure and reliable connection to the Internet. Second, at my apartment, there's also a FortiGate Fortinet 80F firewall router for network security that is linked by my other flat mate because he operates from home and has his office established within my house. I have also used a combination of devices, such as the HPE switch and the Tp-Link wireless access point, to connect various devices. The wireless access point allows me to connect various devices, such as smartphones and laptops, to the Internet.

III. ATTACK VECTORS

An attack vector is a technique used by cybercriminals to obtain illegal access to a network or system. They then use this access to steal various valuable information such as banking credentials and personal data. It is important to implement effective security measures to prevent data breaches.

Most of the attack vectors used by cybercriminals are viruses, email attachments, and web pages. In today's world, attackers are constantly looking for vulnerabilities that can be exploited. Due to the increasing number of attacks, users no longer rely on antivirus protection. Due to the increasing number of attacks, it is important that the proper strategy is implemented to minimize the risks associated with these types of attacks.

I have chosen 3 attack vectors which are **ACE (Arbitrary Code Execution) Attack**, **DOS (Denial of Service)**, and **Cross-Site Scripting (XSS) attack.**The three vectors are very different in terms of their techniques and targets. For instance, the ACE technique is more complex than the DoS attack. Different devices such as Cisco Router are being attacked by these three vectors. Their motive is similar to stealing the private information and files of users.

The table below summarizes all of the main characteristics of the attack vectors;

TABLE III. SUMMARY TABLE III

Name	***Arbitrary Code Execution***	***Denial of Service (DOS)***	***Cross-Site Scripting Attack (XSS)***
Techniques	Authentication Bypass	Buffer Overflow	Malicious Script Inject
Devices	Router	PlayStation	Switch
Affect	Steals sensitive user information	Stealing credentials	Stealing personal Data
CVE ID	CVE-2022-20708 [1]	CVE-2022-28085 [2]	CVE-2021-29148 [3]
Exploit	Success	Success	Success
Brief Description	ACE attack is the ability of an attacker to execute any code or instructions of the attacker's choice on a target system without the owner's knowledge.	DOS is a type of attack that targets a network or machine with a huge amount of traffic.	XSS is a type of attack that exploits a website's built-in security features to secretly install malicious scripts.

A. ACE Attack

ACE (Arbitrary Code Execution) attack is the ability of an attacker to execute any code or instructions of the attacker's choice on a target system without the owner's knowledge. In ACE attack, arbitrary code installs a backdoor into a system, steals important user information (such as passwords), or disables security safeguards. The arbitrary code execution vulnerability implies that an attacker might exploit a vulnerability to upload malicious code to a system and deceive the remote system into executing that code.

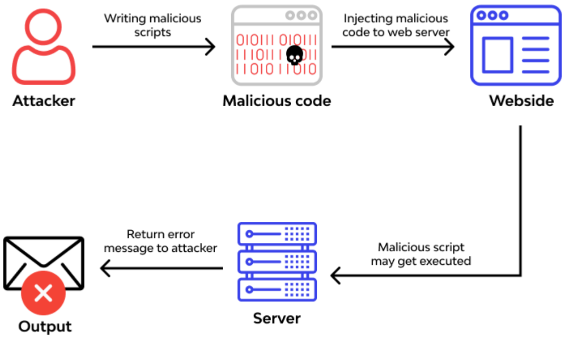
Writing malicious scripts
Injecting malicious code to web server
Attacker
Malicious code
Webside
Return error message to attacker
Malicious script may get executed
Output
Server

Fig. 2. ACE Attack

Motive: The motive behind an attack like this is not always clear. It can be motivated by financial or ideological reasons, and it can also be carried out for personal pleasure. Hackers can also steal or modify sensitive data, and sell it on the black market. The overall purpose is to render internet resources inert or non-responsive.

Techniques: The ACE Attack employs a one-of-a-kind approach in which the attacker gains access to the backend server and steals the sensitive information. The most common forms of ACE attacks include:

- *Deserialization*

Insecure deserialization is when a user takes unserialized data and consumes it without ensuring that it's valid. This process can be performed by implementing serialization, which is a type of data conversion that allows programmers to easily send and receive complex data. A user might intervene in this process and submit incorrect or unexpected data. [4]

- *Type Confusion*

In type confusion, a program's code can be complex, which can lead to subtle conflicts. A hacker can then step in and try to solve the problem. In addition, when a program uses an incompatible type, it could cause logical errors. In programming languages without memory safety, type confusion leads to out-of-bounds memory access and arbitrary code execution.

- *Memory Safety/Corruption*

A memory corruption vulnerability can affect a computer system by altering its memory without an explicit assignment. This vulnerability can be exploited by an attacker to execute arbitrary code. Memory safety refers to the state of being secure from different software faults and security flaws while dealing with memory access.

Target Devices/technologies: The Cisco Small Business RV340 router is the device targeted by the Home Network Setup.

Vulnerabilities: After researching and getting information about a vulnerability in Cisco's RV340 router which is CVE ID: CVE-2022-20708, I noticed that its web-based management interface has multiple vulnerabilities that can allow remote attackers to execute code on the device.

The vulnerability can be exploited by sending an HTTP request that contains a self-written script. An attacker can then execute arbitrary code on the device by loading the malicious code into its operating system which results in stealing the sensitive information of the devices which are connected to the router.

Exploits: An arbitrary code execution attack may be readily exploited by a cyber expert, and the assault's impact on my router is successful.

The rise of the Advanced Cybersurfing attack, ACE has been discussed in various reports about the digital marketing industry. According to a report by Portswigger, in January 2022, it showed that the first quarter of the year was the most common time when it comes to the number of attacks. The report also noted that many large organizations globally are the victims of the attack. [4]

In April 2022, Cisco was the victim of an ACE attack after it was discovered that it had a known vulnerability in a Java library. The attacker exploited this vulnerability by accessing it through the Cisco Nexus Dashboard. He then abused another vulnerable part of the library to perform code execution. [5]

B. DOS (Denial of Service) Attack

A distributed denial-of-service attack, also referred to as a DoS attack, is a type of attack that targets a network or machine with a huge amount of traffic. It then tries to prevent its users from accessing the services or resources they need. In both cases, the attackers prevent legitimate users from accessing the services or resources they expected. Most DoS attacks are directed at high-profile organizations, such as banks and media companies. Although they usually do not steal valuable information, they can cost the victim a lot of money and time.

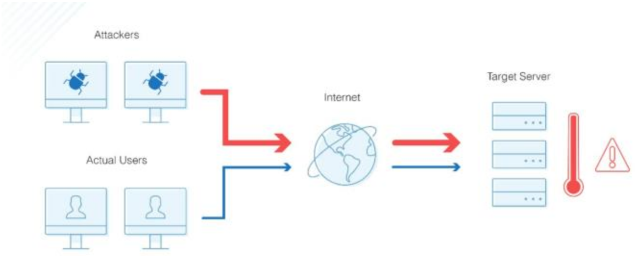

Fig. 3. Denial of Service Attack

Motive: The motive behind a DoS attack may vary depending on the nature of the attack and the benefit it seeks. For instance, it can be motivated by revenge or ideological beliefs. After all, the ultimate goal of the attacker is to completely disable all online resources.

Techniques: DDoS attacks employ a one-of-a-kind approach in which the attacker repeatedly sends data requests to a web server until he gains access to it. The following are examples of common DDoS attacks:

- *Buffer Overflow*

The most common DoS attack is when a network receives more traffic than it can handle. It involves sending more traffic to a different address than the system that's designed to handle it.

- *ICMP Flood or Volume-Based Attacks*

The term ping of death refers to a type of distributed denial of service attack that uses a network device to send fake packets to various computers on the targeted network. This attack then triggers the network to amplify the traffic. The attacker utilizes a large volume of false traffic in this form of attack to determine the state of the website or server. [6]

- *SYN Flood or Protocol Attacks*

A denial-of-service attack occurs when a user tries to connect to a server, but the request is not completed. It then continues until all ports are full, causing no legitimate users to be able to connect. The main goal of this attack is to consume all the resources of the firewalls and load balancers. [6]

Target Devices/technologies: The Sony PlayStation linked via LAN is the device targeted by the Home Network Setup.

Vulnerabilities: After getting information about the CVE ID: 2022-28085, Sony's PlayStation gaming console has multiple vulnerabilities that can allow a remote attacker to execute code on the device. A vulnerability in the input values supplied by users can be exploited by an attacker to access a device's resources. An attacker can send a self-made HTTP request in order to access the device's data. If the response is successful, the attacker would then reload the malicious code.

Exploits: DOS attacks are easily manipulated by cyber professionals, and the attack's influence on my switch is successful.

A report released in March 2022 states that Israel's government websites were affected by distributed denial of service attacks. According to a report released by Cloudflare, the first quarter of the year is the most common time for attacks. The report also states that in China, the number of DoS victims decreased. [8]

C. Cross-Site Scripting Attack (XSS)

Cross-site scripting is a web security issue that allows an attacker to take over a vulnerable application's interactions with its users. XSS attacks usually involve sending malicious code to a user in a browser-side script. The output of a web application that uses input from a user is then used to send the requested code. This type of attack is different from other types of attacks as it targets the entire web application. However, in other attacks, such as SQL injection, the users are at risk. This can be very dangerous and can ruin the whole business.

Motive: The goal of the attacker is to collect the personal information of the user, such as their name, address, and email address. Doing so would allow him or her to access the website and gain control of it.

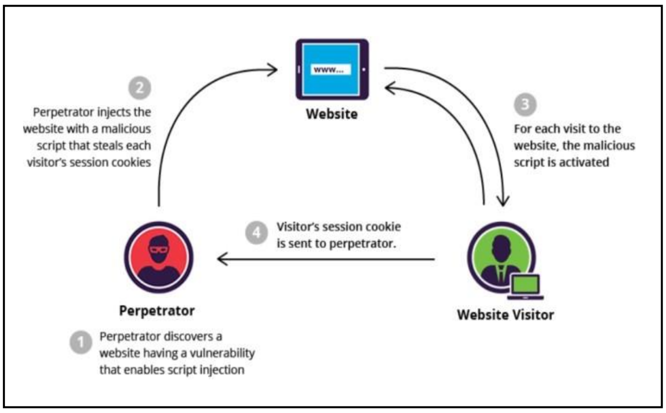
Website
www...
2
Perpetrator injects the website with a malicious script that steals each visitor's session cookies
3
For each visit to the website, the malicious script is activated
4
Visitor's session cookie is sent to perpetrator.
Perpetrator
Website Visitor
1
Perpetrator discovers a website having a vulnerability that enables script injection

Fig. 4. Cross-Site Scripting Attack

Techniques: XSS attacks are usually carried out by a cybercriminal who has to find a way to inject a malicious script or a crafted code into a web page that a user visits. After that, the attacker will collect all the details and entries from the victim.

If the attack failed, the attacker will try to use social engineering techniques to trick the victim into clicking on a link or sending a malicious email. Cross-Site Scripting is mainly of three types:

➢ *Stored XSS*

Stored XSS or Persistent XSS is a type of cross-site scripting that injects a malicious script into a vulnerable web application or website. The victim then retrieves the contents of the injected script from the servers. These are typically attacks that target servers that have a database containing information, such as a visitor log.

➢ *Reflected XSS*

A reflective attack occurs when an injected script is reflected off of a web server, for example in an error message or a search result. It can be delivered to the targeted users through an e-mail message or other website. The attack takes advantage of the unsafe way an application compiles data after receiving an HTTP request.

➢ *DOM Based XSS*

A type of attack known as a DOM-based XSS occurs when an application uses client-side JavaScript to process data from an untrusted source. Instead of writing the data back to the original destination, the application uses the client-side code to run in an unpredictable manner.

Target Devices/technologies: The HPE AurbaOS-S switch is the device targeted by the Home Network Setup.

Vulnerabilities: After getting information about the CVE ID: 2021-29148, it was discovered that certain products of HPE, such as routers, switches, and Wi-Fi systems, are prone to being affected by the XSS. Due to these issues, the company issued a security advisory, which tells the users to update the firmware.

Exploits: Reflected XSS attacks are easily manipulated by cyber professionals, and the attack's influence on my switch is successful.

In April 2022, Google released a vulnerability in Chrome that could allow an attacker to run malicious HTML code in the New Tab. The vulnerability was fixed by the company's security team. [9]

Last week, Rain loop released several fixes for vulnerabilities in some of its plugins that can allow an attacker to take over a user's system after they open an email. These vulnerabilities can be exploited by an attacker to install a malicious JavaScript payload on the user's system. [10]

IV. Mitigation Solutions

After the network has been established and the attack vulnerabilities have been identified, the next step is to implement effective mitigation strategies. This process involves conducting penetration tests on various network devices:

➢ NMAP Network Scanner

➢ Acunetix Vulnerability Scanner

➢ Kali Linux (Virtual Machine)

➢ Metasploit framework

➢ Windows utility tools (Wireshark, ping, etc.)

➢ BurpSuite

➢ XSS Hunter

First, we will discuss some of the most prevalent mitigation measures that are necessary for improved network security.

➢ This process involves conducting regular audits and monitoring the network to identify potential security issues.

➢ Having a good firewall and an antivirus are also important for a successful network setup.

➢ For security professionals, the goal is to create a schedule for the updates and patches that are needed. One should also regularly monitor the traffic on the network. Having a plan in place should allow the security professionals to respond quickly to an attack.

Preventive Measures against Arbitrary Code Execution attack:

❖ Sanitizing user input. This is sometimes difficult to perform due to the abundance of pre-installed bypasses and limits. Any special characters or function names are actively blacklisted. This, like sanitizing user input, should be avoided. [11]

❖ If you see an unusual number of users, immediately remove them. Also, it's important to have only one administrator and set other roles to the lowest privileges.

❖ Regularly schedule scans for vulnerabilities and malware. Doing so will allow you to identify potential security issues before they become too critical.

❖ Even if you don't use software that's vulnerable, make sure that you patch it regularly. Doing so will prevent the exploitation of known vulnerabilities.

- Aside from regularly checking the software, make sure that your anti-malware tools are also up to date. Having the latest version of these tools can help prevent the exploitation of certain vulnerabilities.

Preventive Measures against Denial-of-Service attack:

- Network administrators can monitor and analyze network traffic using a firewall or an intrusion detection system. They can also set rules that will alert them about traffic sources and drop network packets that meet certain criteria.
- To improve their security posture, organizations should regularly update their antivirus software and firewalls, and install and maintain other security tools. They should also regularly monitor and manage their internet-facing devices.
- Through a service that monitors traffic, network administrators can prevent unauthorized traffic from entering their networks. It can also redirect or detect anomalous traffic flows. [12]
- A disaster recovery plan should also be created to address the various aspects of a DoS attack. This should include planning for communication and mitigation.
- The use of firewalls and other network security tools is also important to prevent DoS attacks. These can help prevent unauthorized traffic from entering the network.

Preventive Measures against Cross-Site Scripting attack (XSS):

- Some of the mitigation strategies that can be used to prevent a web app from being attacked are using a firewall, having a content security policy, and ensuring that the cookies are secure.
- Keep in mind that your applications and software are always up-to-date. Having a firewall is also important to prevent unauthorized access to your network.
- When receiving user input, filter it according to what's expected and valid. This ensures that the application doesn't get flooded with irrelevant input.
- When the user-controlled data is output in response, ensure that it's encoded to prevent it from being considered active content. This can be done by implementing various encoding methods such as HTML, JavaScript, and CSS. [13]
- To prevent XSS in web responses that don't contain JavaScript or HTML, use the appropriate response headers. These headers ensure that browsers interpret the content in the way that you intend.

V. CONCLUSION

This research aims to analyze the security vulnerabilities in the home network setup. Through the penetration testing, I was able to identify the most common attacks that can be carried out on the network. Also, with the help of various tools and techniques, I was able to identify the devices that need to be replaced or changed. After conducting the penetration testing, I discovered that the network devices are prone to being attacked. To minimize the risk of exploitation, it is important that the devices are updated to the latest security frameworks. This can be done through regular audits and the removal of outdated or not working properly hardware.

Due to the existence of various vulnerabilities in my network, I have limited resources to deploy effective security measures. After conducting research, I came across many useful devices that can be used to secure my network. The main findings of the study are the characteristics of the network, attack vectors, and techniques used to secure it. This research expands my knowledge of network security and penetration testing significantly. While conducting research, I learned about new tools, network equipment, and how to set up a home network.

References

[1] Tennable, "Tennable Blog," Tennable, [Online]. Available: https://www.tenable.com/blog/cve-2022-20699-cve-2022-20700-cve-2022-20708-critical-flaws-in-cisco-small-business-rv-series. [Accessed 3 May 2022].

[2] National Vulnerability Database, "CVE-2022-28085 Detail," NIST, [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2022-28085. [Accessed 3 May 2022].

[3] National Vulnerability Database, "CVE-2021-29148 Detail," NIST, [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2021-29148#vulnCurrentDescriptionTitle. [Accessed 3 May 2022].

[4] Okta, "Arbitrary Code Execution(ACE)," [Online]. Available: https://www.okta.com/identity-101/arbitrary-code-execution/. [Accessed 05 May 2022].

[5] PortSwigger, "The Daily Swig," PortSwigger, [Online]. Available: https://portswigger.net/daily-swig/rce. [Accessed 4 May 2022].

[6] PortSwigger, "Cisco software update blocks exploit chain in network management software," 04 April 2022. [Online]. Available: https://portswigger.net/daily-swig/cisco-software-update-blocks-exploit-chain-in-network-management-software. [Accessed 04 May 2022].

[7] paloalto, "What is a denial of service attack (DoS)," [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos. [Accessed 05 May 2022].

[8] J. Haworth, "The Daily Swig," 2022 march 15. [Online]. Available: https://portswigger.net/daily-swig/israeli-government-websites-temporarily-knocked-offline-by-massive-cyber-attack. [Accessed 5 May 2022].

[9] A. Hashim, "Chromium Devs Fixed a crazy HTML bug," 04 April 2022. [Online]. Available: https://latesthackingnews.com/2022/04/04/chromium-devs-fixed-a-crazy-html-parser-bug/. [Accessed 05 May 2022].

[10] A. Hashim, "XSS Vulnerability in RainLoop Webmail," 01 May 202. [Online]. Available: https://latesthackingnews.com/2022/05/01/researchers-found-xss-vulnerability-in-rainloop-webmail/. [Accessed 05 May 2022].

[11] A. KL, "What Is Arbitrary Code Execution? How To Prevent Arbitrary Code Execution?," [Online]. Available: https://thesecmaster.com/what-is-arbitrary-code-execution/. [Accessed 05 May 2022].

[12] S. Overby, "DOS Attacks Explained," 03 Aug 2021. [Online]. Available: https://www.mimecast.com/blog/what-is-dos-attack-and-how-to-prevent-it/. [Accessed 05 May 2022].

[13] PortSwigger, "Cross SIte Scripting," [Online]. Available: https://portswigger.net/web-security/cross-site-scripting. [Accessed 05 May 2022].

[14] Portswigger, "The Daily Swig," [Online]. Available: https://portswigger.net/daily-swig/cyber-attacks. [Accessed 30 April 2022].