LONDON METROPOLITAN UNIVERSITY

islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CC5004NI Security in Computing

Assessment Weightage & Type

30% Individual Coursework 02

Year and Semester

2021 -22 Spring Semester

Student Name: Kushal Poudel

London Met ID: 21049723

College ID: np01nt4a210077@islingtoncollege.edu.np

Assignment Due Date: 2023-07-28

Assignment Submission Date: 2023-07-28

Word Count (Where Required): 4689

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

Table of Contents

List of Figures

Acknowledgement

I would like to thank the module leader of Security in Computing, Ms. Suruchi Shrestha, for helping me understand and learn the concept for my topic making it as convenient as possible.

Abstract

In this report, we delve into the realm of Denial-of-Service (DoS) attacks, with a particular emphasis on Distributed Denial-of-Service (DDoS) attacks. By researching, analysing, and evaluating the techniques employed, we aim to understand the impact of these malicious assaults on information technology devices and systems. Practical demonstrations of a DDoS attack, specifically the Slow Loris method, will shed light on its intricacies. Moreover, we explore effective mitigation strategies to safeguard against these disruptive cyber threats, underlining the significance of fortifying defences in the face of evolving cyber threats.

1. Introduction

In today's technologically advanced world, where digital interconnection between devices and systems is the backbone of businesses, communication, and daily life, the integrity and availability of information technology systems are paramount. Unfortunately, malevolent actors continuously seek to exploit vulnerabilities in these systems, threatening the seamless flow of data and services. Among the most insidious weapons in their arsenal are Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks, which have the power to bring down entire networks, cripple critical infrastructures, and disrupt the livelihoods of individuals and organizations. Typically, this is done by saturating the targeted host or network with traffic until it becomes unresponsive or fails. DoS assaults can last anywhere from a few hours to several months, costing businesses and customers money and effort while their tools and services are down (Frankenfield, 2023).

Figure 1 DDoS Attack

As the name implies, denial-of-service (DoS) attacks involve a malicious actor attempting to prevent authorized users from accessing a particular resource, network, or service. This is accomplished by flooding the target with malicious traffic or many requests, which renders the system unavailable and denies service to genuine users. Distributed Denial-of-Service (DDoS) assaults, in contrast, increase the maliciousness by utilizing several sources and staging a coordinated attack on the target. DDoS assaults are particularly sneaky because they can overload even strong infrastructures by generating enormous volumes of traffic from botnets or hacked devices. Denial of Service Attacks involve preventing authorized Internet and network users from using the server's or network's services. It basically means starting an attack that will temporarily prevent authorized users from accessing the Network's services (Warburton, 2022).

Some of the key flaws that allow devices or systems to become vulnerable to DDoS attacks include:

- Exhaustion of Bandwidth: Many networks and systems have constrained bandwidth capacity, which implies that at any one time, they can only manage a specific volume of incoming data. DDoS assaults exceed the target's bandwidth capacity by saturating it with a huge amount of traffic, which causes the system to stop sluggishly or completely responding the legitimate requests.

- Resource Depletion: DDoS assaults can deplete system resources like CPU, memory, and disk space by sending out requests repeatedly that demand a lot of processing and memory. As these resources are used up, the system's performance declines, which denies service to authorized users.

- Protocol Exploitation: To bombard their target with malicious traffic, DDoS attackers use flaws in network protocols including TCP, UDP, and ICMP. SYN flood attacks, for instance, take advantage of the TCP three-way

handshake procedure, whereas UDP flood attacks transmit a lot of UDP packets without waiting for a reply.

- Inadequate Traffic Filtering: A network is more susceptible to DDoS attacks if a system doesn't have enough rate-limiting and traffic filtering systems in place. Filtering that is properly configured can assist in separating harmful from normal traffic and lessen the impact of the assault (Geenens, 2022).

1.1 Aim of the Attack

DoS and DDoS assaults are primarily intended to interfere with the regular operation and accessibility of specific information technology resources. These attacks may be carried out by cybercriminals to do financial harm, obtain a competitive edge, steal data, encourage espionage, further ideological goals, exact revenge, or act as a diversion from more sinister activity.

1.2 Objectives of the Attack

The following objectives may be the part of a DDoS attack:

- Inflict financial losses on targeted organizations, leading to potential economic ramifications.
- Discredit the reputation and credibility of the targeted entity, eroding user trust and confidence.
- Extract sensitive information or intellectual property through diversionary tactics.
- Undermine the accessibility of critical online services, impacting productivity and business continuity.
- Create distractions or smokescreens to facilitate other malicious activities, such as data breaches.

2. Background

Distributed Denial of Service (DDoS) attacks have become one of the most pervasive and disruptive threats in the field of cybersecurity. Through a significant

flow of traffic, these attacks seek to interfere with the normal operation and accessibility of targeted information technology resources. DDoS attacks are distinguished by their distributed nature, in which many infected machines, known as bots or zombies, are coordinated by a centralized command-and-control server to jointly carry out the attack. The attackers take advantage of security flaws in different computer systems, infecting them with malware or evading authentication checks to build a potent botnet.

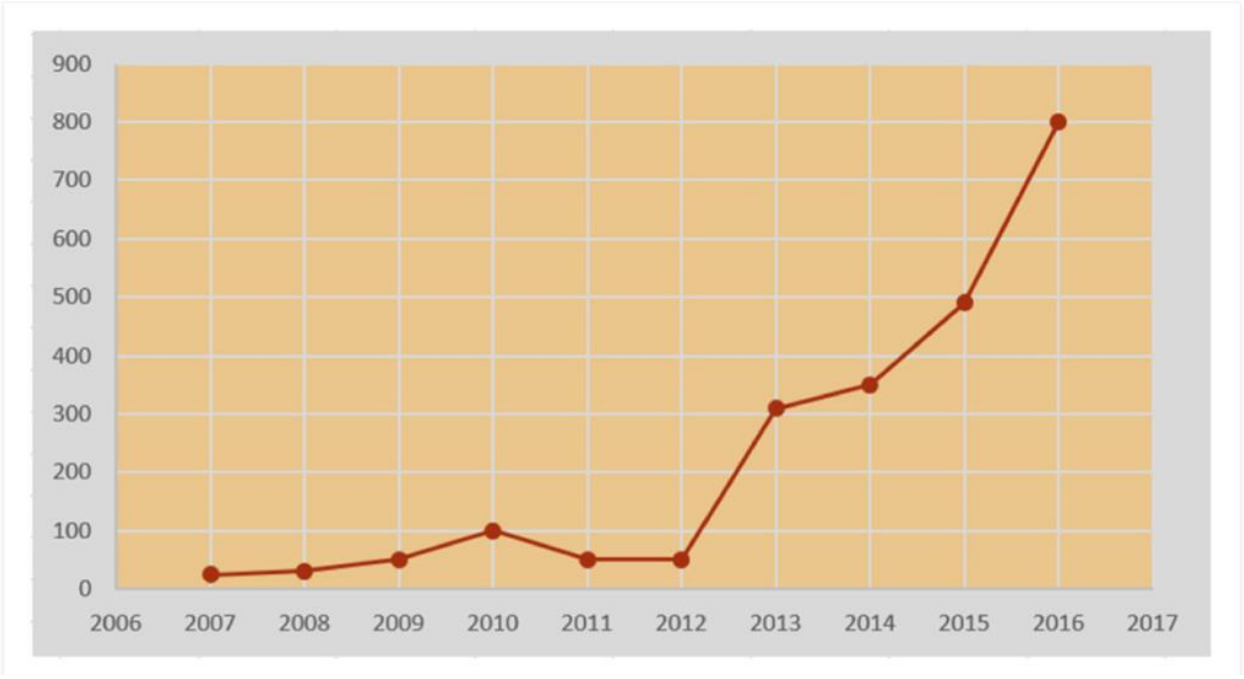

Figure 2 Growth of DDoS Assaults in recent years

The above chart only represents the data till 2017 which is far more back from the present date. It clearly is terrifying to observe the growth of such assaults even in those years as it would have a devastating outcome to even imagine how far the count might have exceeded in the present context (Tansuva Mahjabin, 2017).

2.1 Functioning of DDoS

DDoS assaults are meticulously planned actions that entail a series of tactical moves intended to deplete the target's resources. The first step in the procedure is to identify susceptible computer systems, often known as "attack masters." These systems are picked because of their lax authentication measures or security flaws, which make them vulnerable. A botnet is created, or many existing

zombie devices are implemented for the attack when an attacker takes control of one susceptible machine and spreads the infection to additional targets. The DDoS attack's foot soldiers are these infected devices, or bots. The botnet acts as an effective network of dispersed attack sources that may be used at the attacker's command remotely (Jena, 2022).

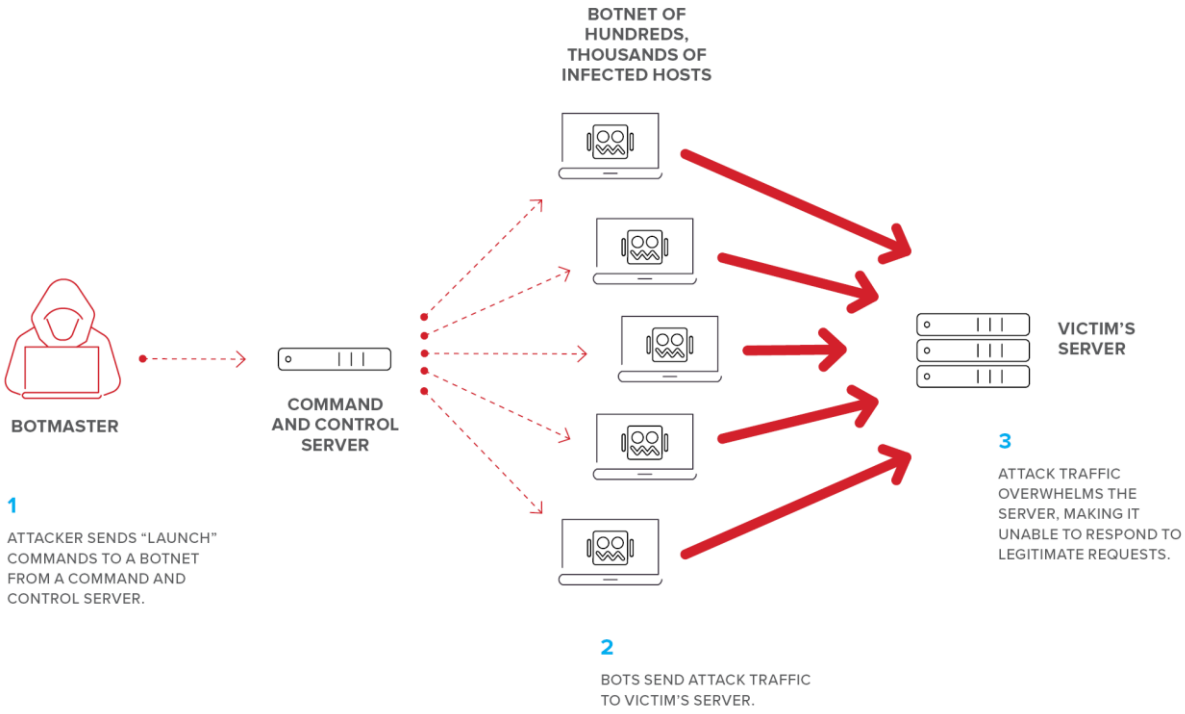

Figure 3 Basic Working Mechanism of DDoS Attack

Zombies, a network of remotely managed, organized, and dispersed nodes, perform DDoS attacks. With the help of zombies, the assailant starts an assault. Such injected or remotely accessed devices and systems can be referred as secondary victims in technical terms for clarity.

DDoS attacks can be broadly classified into three main types, each targeting different aspects of the victim's infrastructure:

- Network-Centric or Volumetric Attacks: In these attacks, the primary objective is to overwhelm the target's network resources by consuming all available bandwidth with an enormous volume of packets. One common example is the Domain Name System (DNS) amplification attack, where the

attacker sends requests to a DNS server using the target's IP address, prompting the server to flood the target with responses, leading to service disruption (Kime, 2022).

- Protocol Attacks: This type of attack exploits flaws in network layer or transport layer protocols to exhaust targeted resources. An infamous example is the SYN flood attack, where the attacker floods the target IP addresses with a high volume of "initial connection request" packets using spoofed source IP addresses. As a result, the Transmission Control Protocol(TCP) handshake is unable to complete due to the constant influx of requests, rendering the target unavailable to legitimate users.

- Application Layer Attacks: These attacks target the application services or databases of the victim by bombarding them with an excessive number of application calls. The HTTP flood attack is an example of an application layer attack, where the attacker simulates numerous simultaneous webpage refreshes, overloading the server and causing denial of service (DDoS-Guard, 2023).

2.2 Impacts of the Attack

A DDoS assault can have a big and broad impact, changing many different regular operating components of the system, functioning’s, network, or the organization targeted. The size and length of the assault, as well as the victim's resources and defences, all influence how severe the impact will be.

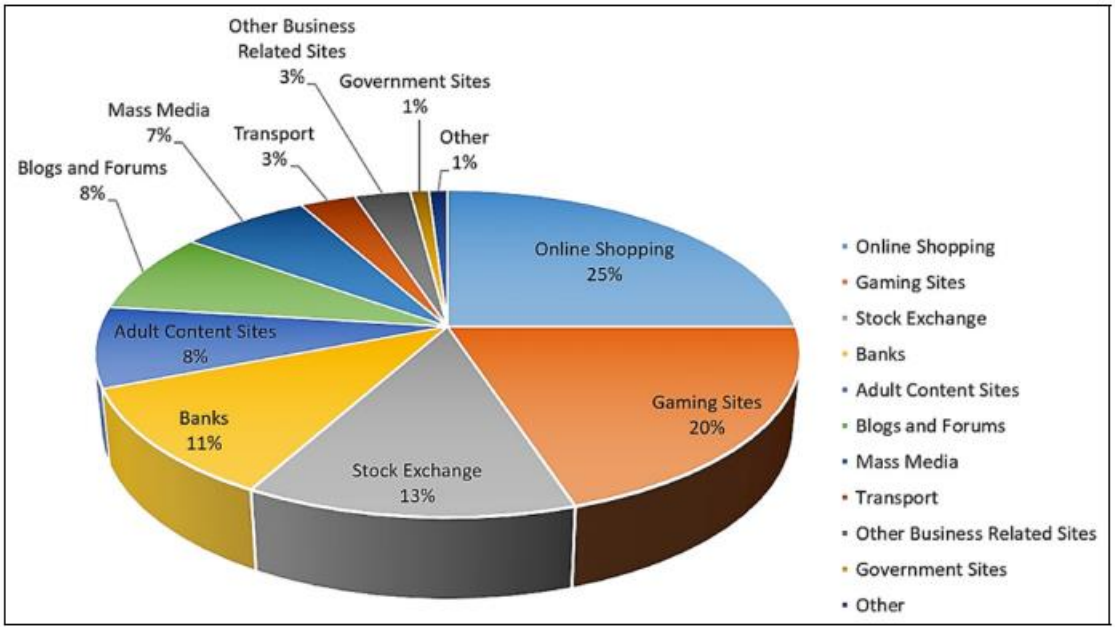

Figure 4 Representation of the Sectors Affected

- Service Disruption: The primary impact of a successful DDoS attack is the disruption of services. By overwhelming the target's resources with an excessive amount of traffic, the attacker can make legitimate user requests unable to reach the server, resulting in service unavailability. This can lead to the temporary or complete shutdown of websites, online services, or network resources, causing inconvenience to users and financial losses to businesses that heavily rely on those services.

- Loss of Revenue and Productivity: Downtime caused by a DDoS attack can result in direct financial losses for businesses, especially e-commerce platforms, as they miss out on potential sales during the unavailability period. Additionally, employees' productivity may suffer if internal systems are impacted, leading to delays in operations and workflow disruptions (McCollin, 2023).

- Immediate Reputation Damage: The public perception of an organization can be severely impacted by a DDoS attack. Customers and users may lose trust in the company's ability to maintain secure and reliable services,

leading to reputational damage. This loss of trust can be long-lasting and may drive customers away to competitors.

- Operational Costs: Organizations affected by a DDoS attack may incur additional operational costs to mitigate the attack and restore services. This could involve investing in better security infrastructure, hiring cybersecurity experts, and conducting investigations to understand the extent of the damage.

- Resource Exhaustion: DDoS attacks can exhaust various system resources, such as bandwidth, CPU, memory, and network connections. This not only impacts the targeted systems but also potentially affects other devices and services within the same network, leading to collateral damage.

- Distraction from Other Threats: A massive DDoS attack can act as a smokescreen for other malicious activities, diverting the organization's attention and resources away from detecting and mitigating other cyber threats that might be occurring simultaneously (Kaspersky, 2023).

2.3 Concept of the Attack

The Slow Loris attack is a type of application-layer denial-of-service (DDoS) attack that exploits the way web servers handle concurrent connections. Unlike traditional flood attacks that rely on overwhelming network resources with high traffic volumes, Slow Loris capitalizes on the servers' processing capacity and connection-handling mechanisms. The attack works by sending partial HTTP requests to the target server, deliberately keeping each connection open with slow data transmission. This method allows the attacker to hold numerous connections open simultaneously, consuming the server's resources such as available connections, threads, and memory.

During a Slow Loris attack, the target server allocates resources for each incomplete connection, expecting the request to complete eventually. However,

the attacker continuously sends minimal amounts of data at regular intervals, preventing the connections from timing out. As a result, the server's resources become tied up in handling these partially open connections, which exhausts its capacity to serve legitimate requests. The Slow Loris attack's stealthy and low-bandwidth nature makes it difficult to detect and defend against, as it may not trigger traditional rate-based or threshold-based security measures. It sends the crafted HTTP requests to the target server, simulating the slow data transmission behaviour. The attack can be executed from a single machine or coordinated through a botnet of compromised devices, further amplifying its impact (Pilcher, 2022).

The Slow Loris attack can significantly impact the target server's performance and availability. As the server dedicates resources to handle each slow connection, it becomes overwhelmed, leading to service degradation or even complete denial of service to legitimate users. The attack does not require a massive amount of bandwidth, making it particularly insidious, as it can be carried out with relatively low resources compared to other DDoS attacks. Furthermore, Slow Loris can exploit web servers regardless of their underlying operating systems or security configurations, making it a versatile and challenging threat to mitigate because of its unique undetectable characteristics which implies on the fact that many requests can be sent at the same time to the server just from a single device acting as requests from many different Ips to disguise from the security measures which the server may have implemented for their security.

2.4 Tools utilized for the Attack

In the context of this DDoS attack, keeping the nature of the concept of the method of the attack in mind, a secure virtual environment was established using Oracle VMware, a robust virtualization platform. Within this virtual environment, a web server was set up using Windows Server 2022 enabling to host a website locally to perform the attack. This configuration facilitated the execution of the Slow Loris attack on a controlled environment, ensuring the safety and integrity of the experiment. The controlled environment provided valuable insights into the

behaviour and impact of this unique DoS technique, enabling a safe and learning-oriented exploration of the attack's mechanics without disrupting anyone’s personal content over the internet which wasn’t necessary as this provides a real-time event of the attack which may take place in any kind of other websites.

- **Oracle VM VirtualBox**

  Oracle VM VirtualBox is a virtualization platform that enables you to run multiple virtual machines (VMs) on a single physical server. It provides a sandboxed environment to host various operating systems and applications, allowing you to carry out experiments and tests safely. In your experiment, Oracle VMware allows you to set up the target server and run the Slow Loris attack in an isolated and controlled environment (Oracle, 2022).

- Windows Server 2022

  Windows Server 2022 is a robust server operating system that provides essential services and functionalities for enterprise environments. By using Windows Server 2022 in your experiment, you can deploy and configure the web server that will be the target of the Slow Loris attack. This allows you to observe the attack's impact on a real-world server setup and evaluate its effects on system resources (Microsoft, 2021).

Other Tools for Real-Time Attacks

In the realm of real-time DDoS attacks, various tools and botnets are available that can be used to carry out similar attacks on live targets. Some commonly known DDoS attack tools include:

a. LOIC (Low Orbit Ion Cannon): A popular open-source DDoS tool that allows attackers to launch flood attacks from multiple sources simultaneously.
b. Xerxes: A powerful DDoS tool known for its multi-threaded and multi-platform capabilities, capable of overwhelming target resources.
c. Hulk: Another tool used for HTTP flood attacks, specifically targeting web servers' resources.
d. Mirai: A well-known botnet used for launching DDoS attacks, primarily targeting IoT devices.

3. Attack Demonstration

Slow Loris attack, an application layer DDoS attack which uses partial HTTP requests to open connections between a single computer and a targeted Web server, then keeping those connections open for as long as possible, thus overwhelming and slowing down the target. This program is used to attack a website hosted on device created in a virtual environment created with the help of Oracle VM VirtualBox and Windows Server 2022. By establishing connections with a targeted Web server and then maintaining those connections for as long as possible, the attack works. It is a simple but effective in the same way as it can easily disrupt the service of targeted host without being detected. The loopholes and vulnerabilities in a system allows it to operate smoothly. Slow Loris offered a unique and stealthy approach to launching a DoS attack, focusing on exploiting the server's connection-handling mechanisms rather than overwhelming network resources with high traffic volumes. This low and slow approach made it an intriguing choice, as it allowed for a more targeted and controlled attack, capable of bypassing traditional rate-based or threshold-based security measures.

Moreover, by performing the Slow Loris attack on a locally hosted website in a secure virtual environment, I could gain a deeper understanding of the attack's intricacies without posing any risk to external systems. The controlled setup allowed for precise observation and analysis of the impact on the website's performance and resource consumption, leading to a safer yet highly educational experience.

To verify the success of the attack on the system, the procedures carried out during the attack has been expressed stepwise below:

Step 1: Environment Setup

The first step involved setting up a virtual environment using Oracle VM VirtualBox with Windows Server 2022 installed as the guest operating system. The virtual machine was configured to ensure smooth performance and seamless internet connectivity. The resources has been allocated in a manner which surpasses the general and small capacity of request processing mechanism which other virtual machines usually represent making it easier for the attack.

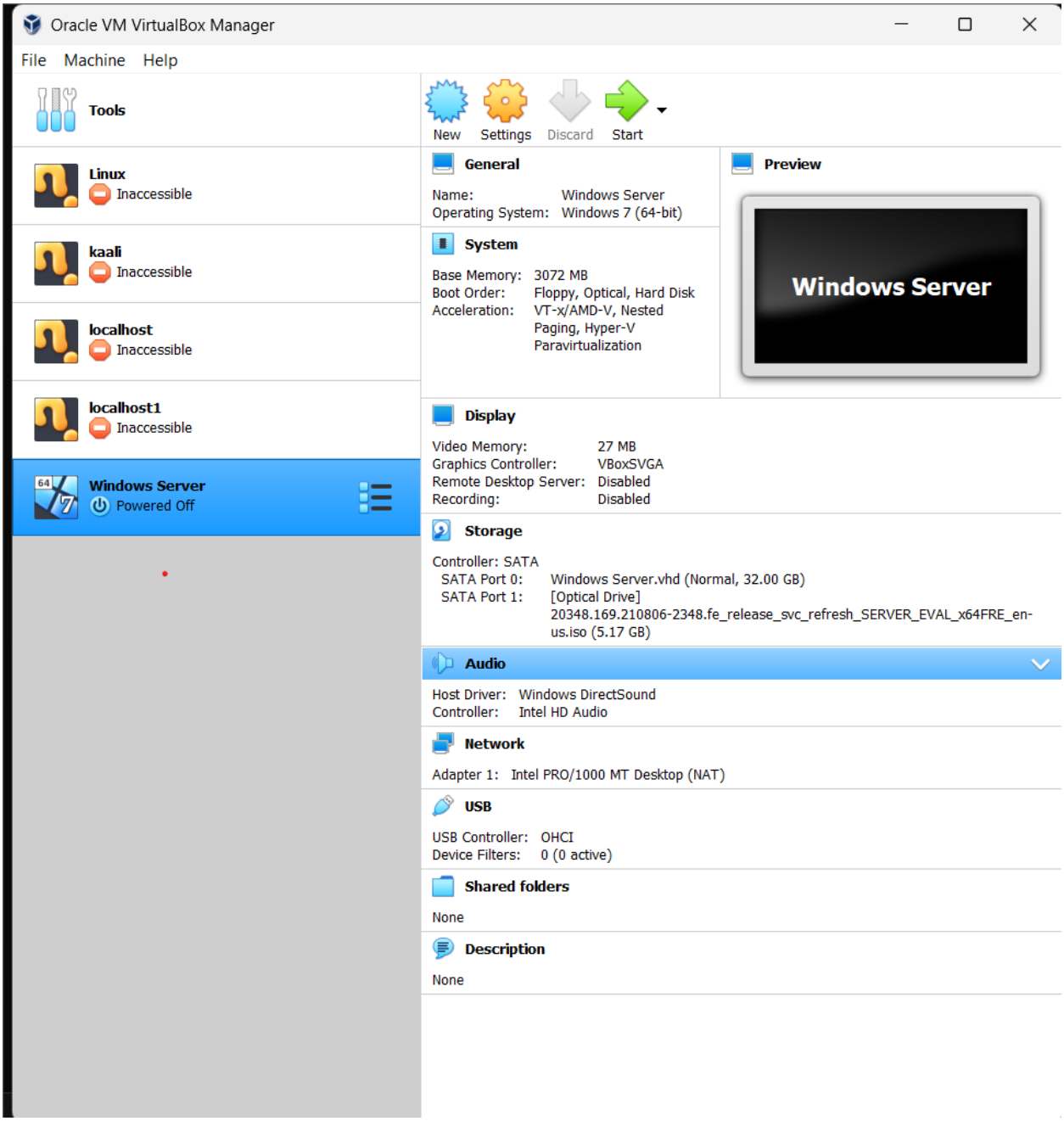

Figure 5 Creation of Virtual Environment

Step 2: Python Installation

Next, Python 3.11 was installed on the Windows Server 2022 virtual machine to access the standard repository and leverage the Slow Loris script using pip, a package manager for Python which offers various modules to install in a device. It

has enabled to install slow loris module in the system to acquire the mechanisms conveniently to perform the attack. It was installed using Command Prompt.

Step 3: Linux WSL Integration

Linux WSL (Windows Subsystem for Linux) was installed in the virtual machine's command prompt to access Linux commands and distributions conveniently during the attack. It was installed using a command: wsl –install

Step 4: Slow Loris Installation

The Slow Loris attack tool was then installed on the virtual machine using the Python package manager which is a standard repository for installing Slow Loris module. The following command was executed to accomplish this:

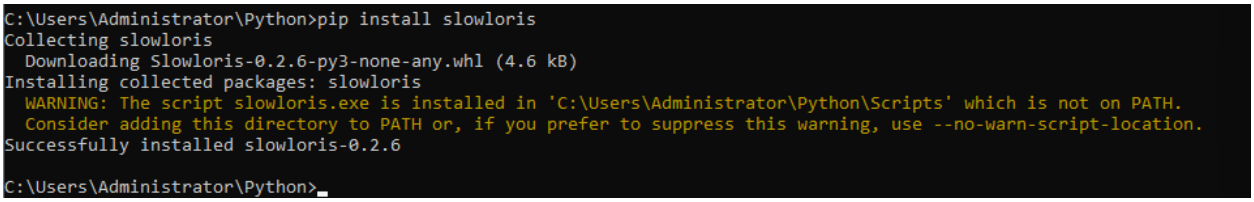

Figure 6 Installation of Slow Loris

Step 5: Slow Loris Configuration

After the installation, we need to verify if the program has been functioning properly by checking the script file. Using the command prompt, the Slow Loris command was executed in the command prompt to explore its available services and understand the parameters required for launching the attack. Key information included the hostname (IP address of the target), sockets count (which exceed the server's capacity), and the port used (default is port 80).

```
C:\Users\Administrator\Python>cd scripts

C:\Users\Administrator\Python\Scripts>slowloris
usage: slowloris.exe [-h] [-p PORT] [-s SOCKETS] [-v] [-ua] [-x] [--proxy-host PROXY_HOST] [--proxy-port PROXY_PORT]
                     [--https] [--sleeptime SLEEPTIME]
                     [host]

Slowloris, low bandwidth stress test tool for websites

positional arguments:
  host                  Host to perform stress test on

options:
  -h, --help            show this help message and exit
  -p PORT, --port PORT  Port of webserver, usually 80
  -s SOCKETS, --sockets SOCKETS
                        Number of sockets to use in the test
  -v, --verbose         Increases logging
  -ua, --randuseragents
                        Randomizes user-agents with each request
  -x, --useproxy        Use a SOCKS5 proxy for connecting
  --proxy-host PROXY_HOST
                        SOCKS5 proxy host
  --proxy-port PROXY_PORT
                        SOCKS5 proxy port
  --https               Use HTTPS for the requests
  --sleeptime SLEEPTIME
                        Time to sleep between each header sent.

C:\Users\Administrator\Python\Scripts>
```

Figure 7 Displaying the Slow Loris Standard Repository

Step 6: Initializing the Slow Loris Attack

The Slow Loris attack was executed on the locally hosted website by providing the information concerning the targeted website.

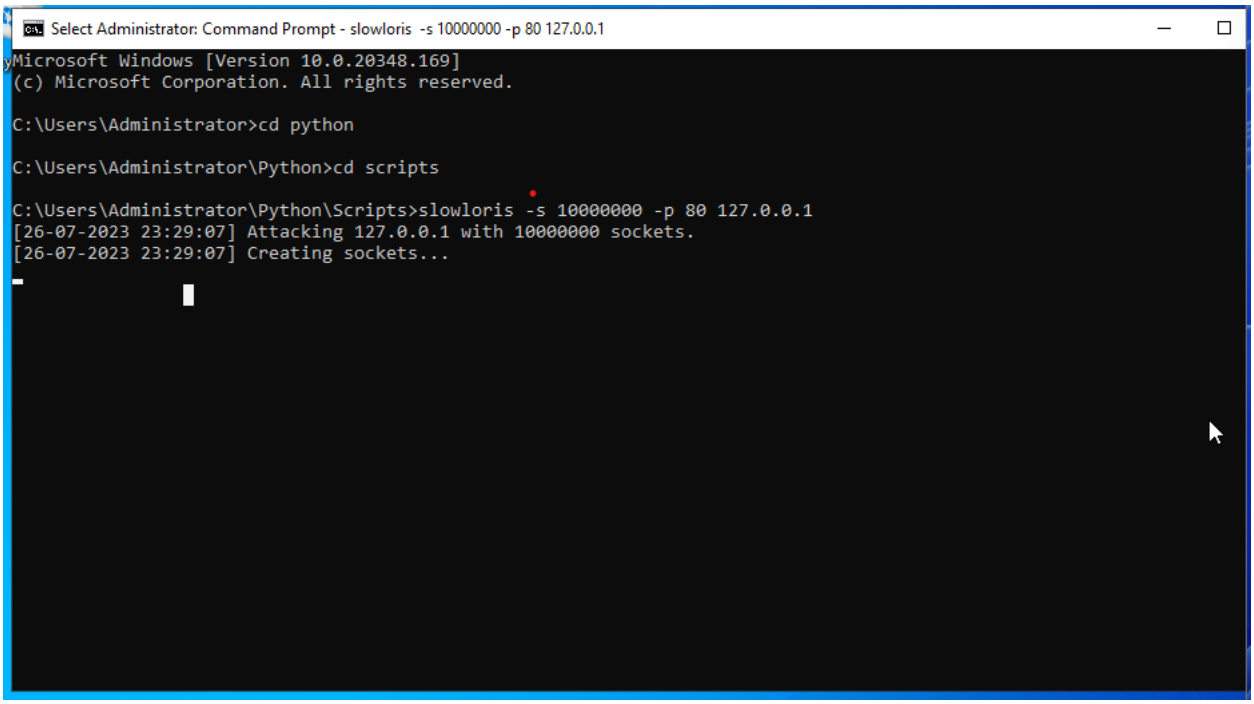

Figure 8 Initializing the Slow Loris Attack

The attack employed 10,000,000 sockets (-s) and targeted port 80 (-p) on the local IP address 127.0.0.1, representing the locally hosted website named index.local.

Step 7: Observing the Attack in Action

As the Slow Loris attack commenced, the program employed the specified number of sockets to overwhelm the server's capacity to respond. The command prompt displayed the socket count completed by the server, although this count could not be calculated precisely due to the high number of sockets used which indicates the exhaustion of the server handling all the sockets which counts to 10000000 resulting the server to malfunction the hosting of the website.

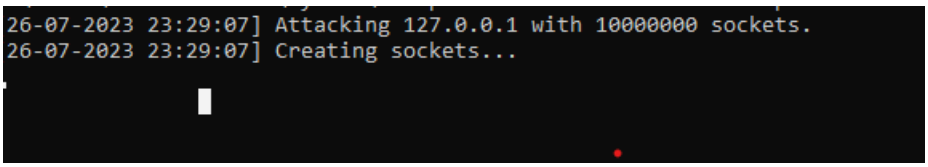

Figure 9 Processing the Attack in Action

Step 8: Verification of Attack Impact

During the attack, attempts were made to access the locally hosted website through a browser. It became evident that the website experienced severe performance issues, including unresponsiveness, significant delays and eventually the server failed to respond the request made from the browser during the attack. The Slow Loris attack effectively disrupted the website's normal operation.

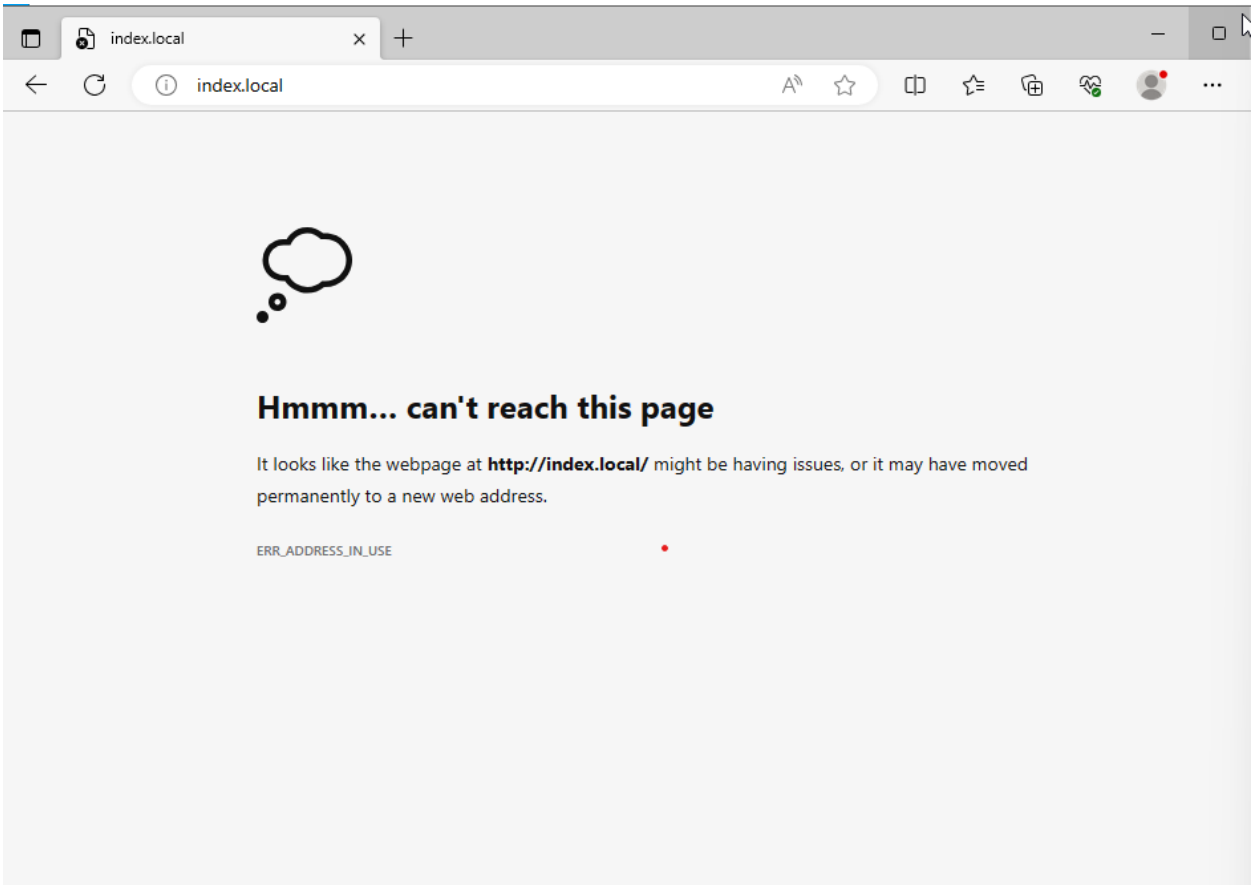

Figure 10 Impact of Slow Loris on the Target

Step 9: Optional - Lowering Sockets Count

To demonstrate the impact of reduced sockets, a second attack was conducted with a lower socket count, such as 1,000,000 sockets. Observations were made regarding the website's performance under this altered attack configuration. The

socket count was being responded by the server normally without disrupting the function to access the website.

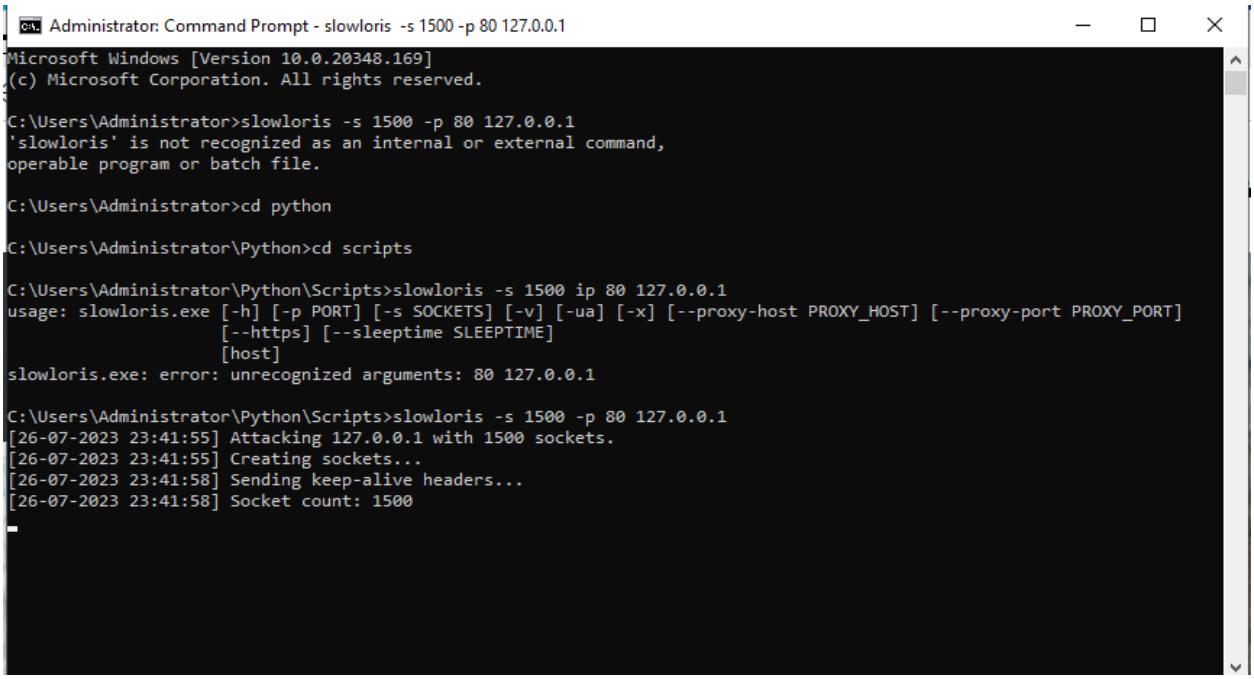

Figure 11 Unsuccessful Slow Loris Attack

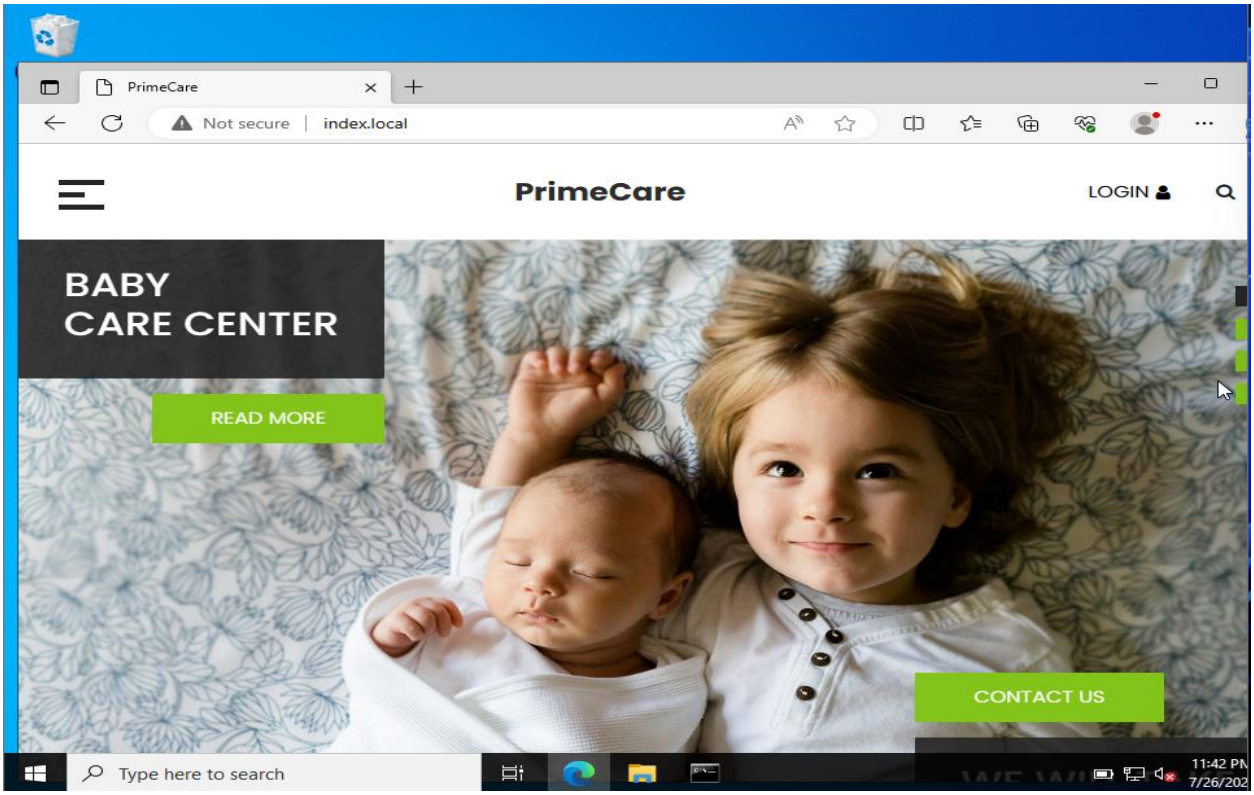

Figure 12 Website being Accessed

In conclusion, the demonstration of the Slow Loris attack provided valuable insights into the world of DDoS attacks and their potential impact on web servers. By utilizing a unique application-layer attack strategy, Slow Loris showcased how exploiting server connection-handling mechanisms can lead to service disruption without relying on massive traffic volumes. This attack method proved to be stealthy and challenging to detect, making it a significant threat to web servers across various platforms and configurations which even penetrated through the capacity of handling mechanisms of one of the renowned hosting virtual server indeed the task was proved to be overwhelming for Windows Server 2022 to handle the attack.

4. Mitigation

Mitigating the risks posed by Slow Loris and other DDoS attacks is a paramount concern for organizations that rely heavily on the availability and stability of their online services. These attacks, which can exploit the vulnerabilities in web servers and network infrastructure, pose significant challenges for defenders due to their

stealthy and low-bandwidth nature. To safeguard against such threats effectively, organizations must adopt a multi-faceted approach, integrating various mitigation strategies to create a robust defence. A DDoS attack can be mitigated in several ways. Certain remedial security measures that have been suggested may contribute to prevent a DDoS assault before it reaches the target service (Giobbi, 2009).

- Web Application Firewall (WAF):
  A Web Application Firewall serves as the frontline defence against Slow Loris and application layer DDoS attacks. It acts as a filter between the user's request and the web server, inspecting incoming traffic and identifying malicious patterns. By analysing HTTP requests, the WAF can block Slow Loris attack patterns, protecting the server from exhaustion. It also enables rule-based detection, allowing organizations to customize rules that specifically target Slow Loris attack signatures. Moreover, advanced WAF solutions can leverage machine learning algorithms to detect anomalous behaviour, ensuring a proactive defence against evolving attack techniques.

- Purchase More Bandwidth:
  Ensuring ample bandwidth capacity is the first step in building DDoS-resistant infrastructure. While it may not entirely thwart the attack, having sufficient bandwidth raises the bar for attackers, making it harder for them to overwhelm your network. Although not a standalone solution, having extra bandwidth serves as a vital safety measure.

- Network Hardware Configuration:
  Simple hardware configuration changes can provide some level of protection against certain types of DDoS attacks. For instance, configuring routers or firewalls to drop incoming DNS responses or ICMP packets can help in preventing specific DNS and ping-based volumetric attacks.

- Transparent Mitigation:
  Implementing transparent mitigation techniques is essential to keep your website accessible to users during a DDoS attack. Utilizing advanced mitigation technologies ensures that users can access the site without disruptions or outdated cached content. When attackers observe that their efforts are ineffective, they may cease the attack, preserving the user experience.

- Anti-DDoS Hardware and Software Modules:
  Combining network firewalls and web application firewalls with load balancers and specialized DDoS prevention software modules enhances protection against Slowloris and other DDoS attacks. Web servers can be equipped with modules like mod_reqtimeout in Apache 2.2.15, which safeguards against Slowloris-style application-layer attacks. These modules keep connections open for legitimate users while detecting and mitigating malicious activities.

- Hardware Modules for Protocol Attacks:
  To defend against protocol-based DDoS attacks like SYN floods, hardware modules can be employed to monitor and manage incomplete connections. These modules detect unusual connection patterns and flush incomplete connections once a configurable threshold is reached, thereby preventing the server from being overwhelmed (Norton, 2022).

5. Evaluation

5.1 Pros of the applied mitigated strategies:

- Effectiveness: The implemented mitigation strategy has demonstrated effectiveness in mitigating Slow Loris DDoS attacks. By utilizing specialized hardware and software modules, the strategy effectively detects and thwarts Slow Loris attack attempts. It successfully identifies the prolonged

connection openings and slow data transmission behaviour characteristic of Slow Loris, allowing for timely response and resource allocation to legitimate users.

- Scalability: The mitigation strategy is scalable and can accommodate the organization's growing needs. As the business expands, the hardware and software can be upgraded or expanded to handle higher volumes of traffic and more sophisticated attack attempts.

- Quick Response: The strategy ensures a quick response to Slow Loris attacks, minimizing the downtime experienced by the web server. The detection mechanisms trigger prompt actions, mitigating the impact of the attack on the server's performance and availability.

- Enhanced Resilience: By incorporating specialized detection mechanisms tailored to Slow Loris behaviour, the mitigation strategy enhances the organization's resilience against this particular attack vector. It strengthens the overall security posture and protects against potential reputational damage caused by prolonged service disruption.

5.2 Cons of the applied mitigation strategies

- Cost: The primary drawback of the implemented mitigation strategy is the initial investment cost. Acquiring anti-DDoS hardware, software modules, and employing cybersecurity experts can impose a significant financial burden, especially for smaller organizations with limited budgets.

- False Positives: While the strategy effectively detects Slow Loris attacks, it may occasionally generate false positives, misidentifying legitimate user

traffic as malicious. These false alarms can lead to unnecessary traffic diversion or temporary service disruptions, impacting the user experience.

- Resource Intensive: The implementation and maintenance of the mitigation strategy require dedicated resources and expertise. Cybersecurity experts must continuously monitor and fine-tune the system to adapt to evolving attack techniques, which can strain the organization's IT resources (Norton, 2022).

- Complexity: Integrating and configuring the various components of the mitigation strategy may pose challenges, particularly for organizations without in-house cybersecurity expertise. The complexity of the solution might necessitate additional training or outsourced support.

5.3 Cost-Benefit Analysis (CBA)

Scenario:

The "ABC" company, an online e-commerce book website, fell victim to a Slow Loris DDoS attack that resulted in a significant disruption of their services. During the attack, customers were unable to access the website or complete book purchases, leading to substantial financial losses. To assess the cost-effectiveness of implementing a Slow Loris DDoS mitigation strategy, a Cost Benefit Analysis (CBA) was conducted.

Annual Loss Expectancy (ALE) Calculation:

The average duration of downtime after a Slow Loris DDoS attack was found to be 30 minutes, with an estimated cost of $1800 per minute of disruption. Considering the potential for such attacks to occur throughout the year, the ALE prior to implementing any security measures was calculated as follows:

ALE(Prior) = 1800 * 30 * 365 (per annum)
= $19,710,000

Annual Cost of Safeguard (ACS):
In response to the Slow Loris DDoS attack, the "ABC" company decided to invest in DDoS mitigation tools and specialized personnel. The cost of hiring and maintaining four IT operations personnel, with a fully burdened average compensation of $80,000 per year for each specialist, was taken into account. Therefore, the ACS was calculated as:

ACS (Annual Cost of Safeguard) = $80,000 * 4
= $320,000

Post Annual Loss Expectancy (ALE):
After implementing the Slow Loris DDoS mitigation strategy and having the IT personnel actively involved in safeguarding against such attacks, the annual loss expectancy was significantly reduced to $60,000.

Cost Benefit Analysis (CBA) Calculation:
The CBA was conducted to compare the ALE before and after implementing the Slow Loris DDoS mitigation strategy and assess the effectiveness of the security measures. The calculation is as follows:

CBA = ALE(Prior) - ALE(Post) - ACS
= $19,710,000 - $60,000 - $320,000
= $19,330,000

Based on the Cost Benefit Analysis, it is evident that the cost of investing in DDoS mitigation tools and hiring IT specialists to protect against Slow Loris attacks is significantly lower than the potential loss expectancy resulting from such an attack. The "ABC" company's decision to implement

preventive and detection measures against Slow Loris DDoS attacks is highly justified, as it proves to be a valuable investment in safeguarding their online book website and preserving customer trust.

6. Conclusion

The Internet is dynamic and evolving continually in a rapid turn of evolving technologies in present context. Therefore, DDoS mitigation measures quickly become insignificant. Online providers constantly introduce new services, while attackers constantly try to prevent customers from accessing those services. The crucial query, however, is whether DDoS attacks indicate a network issue, a human issue, or both. we delved into the realm of Distributed Denial of Service (DDoS) attacks, with a particular focus on the intriguing Slow Loris attack. Through an in-depth exploration of the concepts, classifications, and functioning of DDoS attacks, we gained valuable insights into the disruptive nature of these cyber threats. The primary aim of DDoS attacks, whether network-centric, protocol-based, or application-layer, is to overwhelm target resources, rendering them inoperable and causing widespread disruption. Slow Loris, as a unique application-layer attack, stands out for its low and slow traffic approach, making it particularly challenging to detect and mitigate. we explored various mitigation strategies to safeguard against DDoS attacks and specifically targeted the Slow Loris attack. Strategies like purchasing additional bandwidth, network hardware configuration, and protecting DNS servers serve as proactive measures to fortify the infrastructure against potential attacks. Moreover, transparent mitigation techniques and the use of anti-DDoS hardware and software modules prove effective in ensuring uninterrupted access to services during an attack. We investigated many DDoS mitigation techniques and primarily focused on the Slow Loris assault and the mitigating measures were wisely evaluated for the least damage and prevention of bearing severe damages from the assault.

These innovative concepts were accepted in this study providing a critical insight needed to develop safe and normal operable approaches.

7. References

DDoS-Guard, 2023. *DDoS Attack Classification: A Complete Guide to DDoS Attack Types.* [Online]
Available at: https://ddos-guard.net/en/blog/classification-of-ddos-attacks
[Accessed 21 07 2023].

Frankenfield, J., 2023. *Denial-of-Service (DoS) Attack: Examples and Common Targets.* [Online]
Available at: https://www.investopedia.com/terms/d/denial-service-attack-dos.asp#:~:text=In%20a%20DoS%20attack%2C%20the,or%20CPU%20of%20the%20server.
[Accessed 16 07 2023].

Geenens, P., 2022. *What Drives DDoS Attacks and Why it Should be a Concern.* [Online]
Available at: https://www.radware.com/blog/ddos-protection/2022/01/what-drives-ddos-attacks-and-why-it-should-be-a-concern/
[Accessed 16 07 2023].

Giobbi, R., 2009. *Mitigating Slowloris.* [Online]
Available at: https://insights.sei.cmu.edu/blog/mitigating-slowloris/
[Accessed 22 07 2023].

Jena, B. K., 2022. *What Is a DDoS Attack and How Can It Be Fended Off?.* [Online]
Available at: https://www.simplilearn.com/tutorials/cryptography-tutorial/ddos-attack
[Accessed 21 07 2023].

Kaspersky, 2023. *Distributed Denial of Service: Anatomy and Impact of DDoS Attacks.* [Online]
Available at: https://usa.kaspersky.com/resource-center/preemptive-safety/how-does-ddos-attack-work
[Accessed 21 07 2023].

Kime, C., 2022. *Complete Guide to the Types of DDoS Attacks.* [Online]
Available at: https://www.esecurityplanet.com/networks/types-of-ddos-attacks/
[Accessed 21 07 2023].

McCollin, R., 2023. *DDoS Attacks Explained: Causes, Effects, and How to Protect Your Site.* [Online]
Available at: https://kinsta.com/blog/what-is-a-ddos-attack/#:~:text=A%20DDoS%20attack%20could%20render,of%20action%20by%20the

%20attack.
[Accessed 21 07 2023].

Microsoft, 2021. *Windows Server 2022.* [Online]
Available at: https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2022
[Accessed 21 07 2023].

Norton, Z., 2022. *How to Mitigate a Slowloris DDoS Attack.* [Online]
Available at: https://brilliancesecuritymagazine.com/cybersecurity/how-to-mitigate-a-slowloris-ddos-attack/
[Accessed 22 07 2023].

Oracle, 2022. *Changelog for VirtualBox 6.1.* [Online]
Available at: https://www.virtualbox.org/
[Accessed 21 07 2023].

Pilcher, H., 2022. *What is a slow loris? Everything you need to know about this cute but venomous primate.* [Online]
Available at: https://www.sciencefocus.com/nature/slow-loris/
[Accessed 21 07 2023].

Tansuva Mahjabin, Y. X. G. S. W. J., 2017. A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *International Journal of Distributed,* 13(12), p. 33.

Warburton, D., 2022. *2022 Application Protection Report: DDoS Attack Trends.* [Online]
Available at: https://www.f5.com/labs/articles/threat-intelligence/2022-application-protection-report-ddos-attack-trends
[Accessed 16 07 2023].