



Analysis of cyber-attacks through simulation

Fatmir Basholli¹, Dolantina Hyka², Albina Basholli³, Adisa Daberdini⁴, Besjana Mema¹

¹Albanian University, Department of Engineering, Tirana, Albania, fatmir.basholli@albanianuniversity.edu.al; b.mema@albanianuniversity.edu.al

²Mediterranean University of Albania, Department of Information Technology, Albania, dolantina.hyka@umsh.edu.al

³Polytechnic University of Tirana, Faculty of Mathematics Engineering and Physics Engineering, Tirana, Albania, a.basholli@fimif.edu.al

⁴Aleksander Xhuvani University, Informatics Department, Elbasan, adisa.daberdini@uniel.edu.al

Cite this study: Basholli, F., Hyka, D., Basholli, A., Daberdini, A., & Mema, B. (2023). Analysis of cyber-attacks through simulation. *Advanced Engineering Days*, 7, 120-122

Keywords

Simulation
Technology
Institutions
Cyber systems

Abstract

Nowadays, the development of information technology has brought radical changes in every aspect of people's lives and this has made our lives have a lot of access to information. Users should be very careful when using social networks, various applications and navigating the Internet world because the risk of cyber-attacks by irresponsible persons with malicious intentions is very frequent. This paper aims to provide the necessary information for cyber-attacks, where we will use for simulation tools from the Metasploit library which is a framework that makes hacking simpler and is also an essential tool for many attackers and defender.

Introduction

Since the early days of the Internet, there have been cyber attackers with the motto "Hit and Go". Later, these attacks were aimed at modifying documents and most of them were carried out for fame and reputation, where at that time most organizations only had a firewall between the organization's network and the Internet. Today in the trend of attacks are social networks, banks, businesses, institutions and every day they are increasing, and with this development the insecurity of the users of these networks is also increasing. Now cyberattacks are modified and well-organized which are analyzed and prepared in a special way for the organization they target, modern attacks are undertaken from which hackers benefit materially or financially [1-3]. So, the best protection against Internet attacks is achieved when we understand how cyber-attacks actually work and, in the following, we will clarify the types of cyber-attacks and what we currently have available for the protection and avoidance of these attacks.

Material and Methods

The most common are Viruses, which are a piece of computer code that is attached to an application program or a file. Some viruses can cause damage, such as damage programs, delete programs, delete files and even the entire contents of the hard drive. The main goal of a cyber-attack in most cases is to steal and expose sensitive data [4]. Some of the types of cyber-attacks are:

Ransomware; "Brute-force" attack; "keylog" attack; Spear phishing; Phishing clones; Whaling; Rogue Wifi; Zero-Day Attacks.

DDoS is short for Distributed Denial of Service attacks, which occurs when a server is attacked by sending it more requests than it can respond to, causing an overload on that server that makes it impossible to respond to legitimate requests. DoS attacks are among the simplest attacks that do not aim to steal, modify or destroy information, but aim to prevent a user from using a job [5]. The method of creating a Metasploit project. Metasploit is basically a versatile testing and penetration framework, it can perform literally all the tasks involved in a testing lifecycle. Also, since it is a complete Framework and not just an application, it can be customized and extended according to our requirements [6]. Metasploit is used to test and analyze the vulnerabilities of computer systems for access to system control and is among the main tools of Ethical Hackers

or White Hat's or groups responsible for cyber security, not only for identifying any errors or defects. The special thing is that it allows you to be a step or two ahead of ordinary attackers.

Results and Discussions

We must note that there is no one-size-fits-all security solution, so in advance we must make a risk assessment that is preferably done by a specialized external firm and after the risk and ways of solving it have been well analyzed to decide on the best possible alternative [7].

Experimentation of DoS attacks through Simulation. The DoS attack starts when the client tries to connect to the system using the TCP protocol (HTTP or HTTPS), where it first requires handshakes to be performed before exchanging data between them. So, before we start the simulation, we identify the attacker and the victim where both use Windows operating systems and the steps we have to follow to simulate the attack are the commands after opening the Metasploit Framework.

Now we will illustrate the steps of the simulation through figures step by step:

1-Msfconsole is the command that activates the Metasploit Framework, see Figure 1.

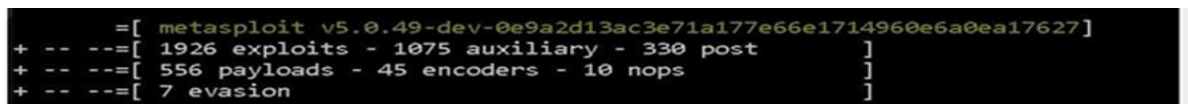


```

C:\metasploit-framework>msfconsole
  
```

Figure 1. Msfconsole command view

2-In Figure 2 (second image) Metasploit is activated with 1926 exploits- 1075 auxiliary- 330 post, 556 payloads - 45 encoders- 10 nops, 7 evasion.

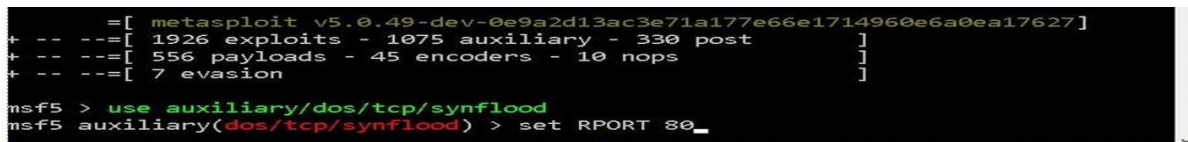


```

=[ metasploit v5.0.49-dev-0e9a2d13ac3e71a177e66e1714960e6a0ea17627 ]
+ -- --=[ 1926 exploits - 1075 auxiliary - 330 post ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops ]
+ -- --=[ 7 evasion ]
  
```

Figure 2. Metasploit view

3-Use the command "use auxiliary/dos/tcp/synflood", Figure 3 to demonstrate the DoS attack -"set RPORT 80" sets port 80 for synflood in Metasploit



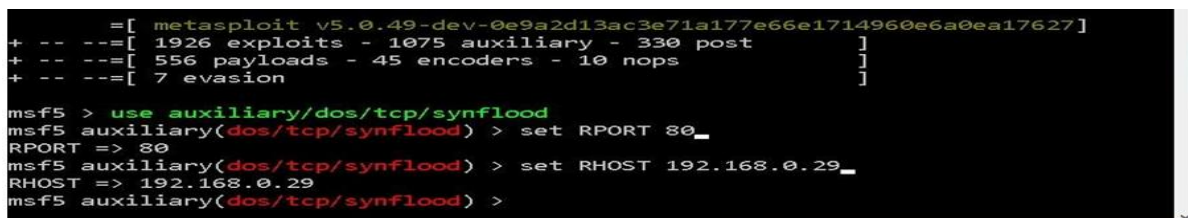
```

=[ metasploit v5.0.49-dev-0e9a2d13ac3e71a177e66e1714960e6a0ea17627 ]
+ -- --=[ 1926 exploits - 1075 auxiliary - 330 post ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops ]
+ -- --=[ 7 evasion ]

msf5 > use auxiliary/dos/tcp/synflood
msf5 auxiliary(dos/tcp/synflood) > set RPORT 80_
  
```

Figure 3. Metasploit view after using the "auxiliary" command

4-"set RHOST 192.168.0.29" sets the IP (Figure 4) as the destination for executing the DoS attack



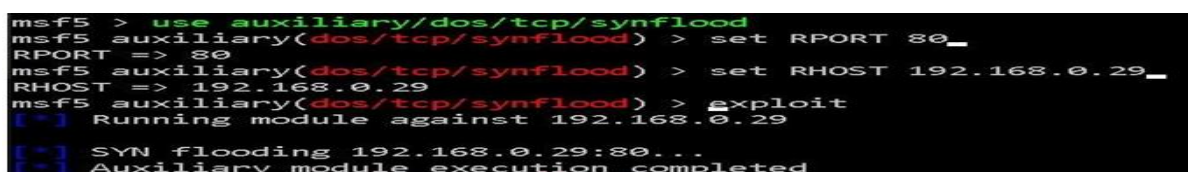
```

=[ metasploit v5.0.49-dev-0e9a2d13ac3e71a177e66e1714960e6a0ea17627 ]
+ -- --=[ 1926 exploits - 1075 auxiliary - 330 post ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops ]
+ -- --=[ 7 evasion ]

msf5 > use auxiliary/dos/tcp/synflood
msf5 auxiliary(dos/tcp/synflood) > set RPORT 80_
RPORT => 80
msf5 auxiliary(dos/tcp/synflood) > set RHOST 192.168.0.29_
RHOST => 192.168.0.29
msf5 auxiliary(dos/tcp/synflood) >
  
```

Figure 4. Results of the "auxiliary" command

5- "exploit" executes the DoS attack on the IP, the specified port (Figure 5) with the exploit provided by Metasploit. This section shows how the execution of the SYNflooding Auxiliary module is completed for the IP and port specified above.



```

msf5 > use auxiliary/dos/tcp/synflood
msf5 auxiliary(dos/tcp/synflood) > set RPORT 80_
RPORT => 80
msf5 auxiliary(dos/tcp/synflood) > set RHOST 192.168.0.29_
RHOST => 192.168.0.29
msf5 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 192.168.0.29
[*] SYN flooding 192.168.0.29:80...
[*] Auxiliary module execution completed
  
```

Figure 5. Execution of the "exploit"; Execution of the "Auxiliary" module of "SYNflooding"

6- "exit" command closes the processes of Metasploit Framework (Figure 6) and with this ends the simulation of DoS SYNflood cyber-attack according to Metasploit

```

[*] SYN flooding 192.168.0.29:80...
[*] Auxiliary module execution completed
msf5 auxiliary(dos/tcp/synflood) > exit

```

Figure 6. Execution of the "exit" command

After the DoS SYNflood cyberattack on Metasploit towards the Windows operating system with IP Address 192.168.0.29 and with port 80, to analyze the effects of the simulation on the above-mentioned host we used WireShark software and taskmanager to see the effects caused by the simulation of demonstrated above with Metasploit. So, the administrator is able to identify the attack based on TCP Traffic which has been overloaded [8- 10]. Figure 7 shows the normal state of the CPU and RAM before the DoS TCP Syn Flood attack, as well as how the DoS attack on the CPU and RAM affects the System resources, Figure 8.

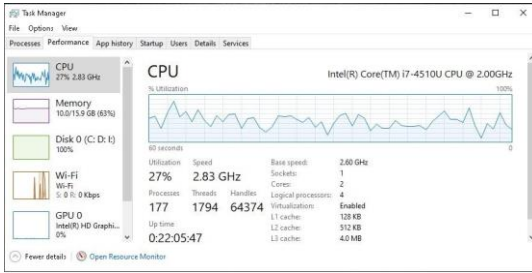


Figure 7. State of CPU and RAM before attack

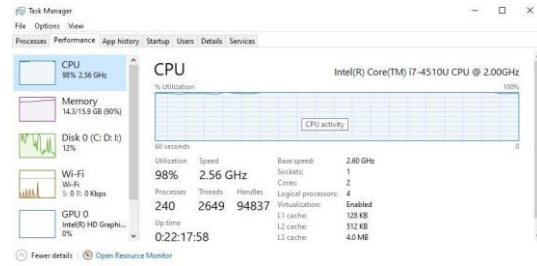


Figure 8. State of CPU and RAM after attack

From these illustrations, it was demonstrated how a TCP SYN Flood DoS cyberattack was carried out with MetaSploit, from the Windows operating system, using WireShark with filters for review and clarification.

Conclusion

Cyber-attacks include a field for which we must work and study a lot, in order to fundamentally understand the problems that this phenomenon can cause. Keep software up to date; Educate employees; Implement formal security policies; Save data (Backup); Use encryption software to protect sensitive data.

References

1. Rahalkar, S. (2017). Metasploit for Beginners. UK.
2. Basholli, F., (2022). Cyber warfare, a new aspect of modern warfare. International Scientific Journal Security & Future, Publisher: Scientific Technical Union of Mechanical Engineering Industry-4.0, 72-75
3. Malware, 2019. http://cyberalbania.al/?page_id=632.
4. Johnson, M., (2021). The Role of Education in Cybersecurity: A Systematic Literature Review. International Journal of Cybersecurity Education, Research and Practice.
5. Basholli, F., Daberdini, A., & Basholli, A. (2023). Detection and prevention of intrusions into computer systems. Advanced Engineering Days (AED), 6, 138-141.
6. Denial-of-service attack, (2019). https://en.wikipedia.org/wiki/Denial-of-service_attack.
7. Hyka, D., & Basholli, F. (2023). Health care cyber security: Albania case study. Advanced Engineering Days (AED), 6, 121-123.
8. Phishing, (2019) <https://sq.wikipedia.org/wiki/Phishing>.
9. Smith, J., Johnson, A., & Brown, L. (2022). The Role of Education in Cyber Hygiene: A Systematic Review. International Journal of Cybersecurity Education, Research, and Practice
10. Daberdini, A., Basholli, F., Metaj, N., & Skenderaj, E. (2022). Cyber security in mail with Fortiweb and Fortinet for companies and institutions. Advanced Engineering Days (AED), 5, 81-83.