International Journal of Engineering and Information Systems (IJEAIS)
ISSN: 2643-640X
Vol. 9 Issue 9 September - 2025, Pages: 195-203

Analysis of Cyberattacks via the Metasploit Framework and Solution Proposal

Pamphile Kazadi Mulumba [1] and Pactole Cipa Cipa [2]

Faculty of Computer Science, Notre-Dame du Kasayi University, Kananga, Kasai-Central, Democratic Republic of Congo [1]
Faculty of Computer Science, Notre-Dame du Kasayi University, Kananga, Kasai-Central, Democratic Republic of Congo [2]
plkazadi@gmail.com [1], pactolecipa793@gmail.com [2]

Abstract : *Cyberattacks exploiting network vulnerabilities, such as those facilitated by the framework Metasploit , represent a growing threat in 2025, with a 10% increase in weaponized vulnerabilities (Recorded Future, 2025). This study explores the mechanisms of cyberattacks, focusing on Metasploit exploits such as EternalBlue (MS17-010), their economic impacts (10.5 billion USD/year), and their technical implications. Through simulated tests in a controlled environment, we analyze the attack stages: reconnaissance, exploitation, and post-exploitation. We propose network partitioning as a mitigation solution, limiting the lateral propagation of threats. Our results show that segmentation reduces unauthorized access by 80% in Meterpreter -like scenarios . Drawing on academic and industrial sources, this article aims to educate professionals on proactive defenses, while respecting research ethics.*

Keywords *: Metasploit , cyberattacks, EternalBlue , network partitioning, cybersecurity*

0. Introduction

For thousands of years, humans have been creating and using tools to help solve various problems. Initially, most societies probably used archaic methods for storing, transmitting, and securing data on the internet. Then came notches in wood, piles of stones, shells, or bones, and the notion of cyberattack, which represents progress and also a threat, with tools like Metasploit that can be used for malicious purposes, transforming a simple flaw into a network disaster.

In an era where IT is at the heart of virtually every innovation, you may be wondering how IT can contribute to the risk of global underdevelopment. It is up to us to state that according to the World Economic Forum's Global Cybersecurity Outlook 2025 report , cyber risks have increased by 72% in 2024, with costs projected to reach $10.5 trillion annually by 2027. [1]

This study, the interest of which no longer needs to be demonstrated, explores precisely these dynamics, by making a review of cybercriminal attacks and the framework Metasploit , then practical tests and will come up with a solution proposal via partitioning.

1. Review of attacks and framework Metasploit

1.1. Review of cybercriminal attacks

1.1.1. Definition

a. Cyberattack

A cyberattack is defined as malicious activity aimed at compromising, interfering with, denying access to, or destroying information systems or their data. These attacks seek to illegally access or damage computers, networks, and information systems to cause harm. They may disable or take control of digital environments, as well as modify, obstruct, erase, manipulate, or expropriate data stored within these structures. [2] According to Kennedy et al. (2023), “cyberattacks exploit software or human vulnerabilities to compromise the confidentiality, integrity, or availability of data.” [3]

b. Threat

A threat is any event or action that can exploit a vulnerability to compromise the confidentiality, integrity, or availability of an information system. [2] They are also considered agents or events that have the potential to cause damage to computer systems, whether intentional or accidental. [4] In our view, we can consider a threat to be like a latent danger: it has not necessarily acted, but it has the potential to cause an incident if no protective measures are put in place. For example, outdated software presents a threat because it can be exploited by a hacker, even if this has not yet happened. This definition emphasizes proactive vigilance in system security.

c. Vulnerability

A vulnerability is a flaw in a system that can be exploited by a threat to cause damage or compromise the confidentiality, integrity, or availability of information. [2] In other words, vulnerabilities are weak points in information systems that, when exploited, can lead to security incidents. [4] As far as we are concerned, a vulnerability can be seen as a crack in a system's defenses. Even if no hacker has yet attempted to exploit it, it represents a latent risk. For example, unpatched software contains known vulnerabilities that can be exploited by cybercriminals. Identifying and patching these vulnerabilities is a crucial step in protecting computer systems.

d. Exploitation.

Speaking of exploitation, it consists of using an identified vulnerability in a system to allow an attack to succeed, thus causing impacts on information security.[2] According to another reflection, exploiting a vulnerability means activating the threat potential inherent in this weakness to compromise an information system, often for malicious purposes [4] As an illustration, exploitation is the moment when the threat actually "hits" the vulnerability. For example, a hacker using a script to penetrate an unpatched server is actually exploiting the vulnerability present. It is this step that differentiates the simple potential risk from the actual incident, and this is why penetration testing (pentest) is essential to detect these weak points before malicious actors do so.

1.1.2. Typology of cyberattacks

According to the classifications, several attacks exist depending on their impacts and level of use. Thus, we have presented some of the most used ones including:

a. Denial of Service (DoS /DDoS) attack

A denial of service (DoS) attack is an attack designed to make a system or network resource unavailable to its intended users, typically by flooding it with unnecessary requests or exploiting software vulnerabilities.[5] It typically involves a single host flooding a network or service with traffic, consuming resources to prevent legitimate use. That is, the attacker uses a single machine to saturate the target server with repeated or malformed requests in an attempt to exhaust the server's resources (CPU, memory, bandwidth) so that it becomes unavailable.

It occurs when an attacker prevents legitimate users from accessing a system, network, or service, often by overwhelming it with a large volume of traffic or triggering a crash by exploiting vulnerabilities. [4] Distributed DoS attacks use multiple compromised machines to flood a target with traffic, making it extremely difficult to distinguish between legitimate users and attackers. [4] The attacker controls a network of compromised computers (botnet) to send massive requests to the target server simultaneously, which is difficult to block because the requests come from multiple sources. This allows for rapid saturation of the server or network bandwidth.

For this type of attack, several techniques are used, namely:

- Volumetric: network overload with massive traffic (UDP flood, ICMP flood).
- Protocol: exploitation of flaws in TCP/IP or DNS (SYN flood, DNS amplification).
- Application: Targeting applications (HTTP flood) to saturate server CPU/memory resources.

To better understand, it's as if a store suddenly received thousands of fictitious customers who block the entrance, preventing real customers from making their purchases. In the digital world, this translates into a server or website saturated with requests, unable to respond to legitimate users. The impact is concrete: service interruption, financial loss, reputational damage, and user frustration. Also, imagine a bridge over which all vehicles pass to access a city and a DoS is a single truck that is too heavy to block the passage. A DDoS is an army of trucks coming from several roads, completely saturating the bridge and preventing all normal traffic. In the digital world, the server is the bridge, the requests are the trucks, and legitimate users are blocked by this malicious traffic. This is why companies invest in DDoS detection systems, traffic filtering, and cloud solutions to distribute the load and protect services.

b. Vulnerability exploitation

Vulnerability exploitation is the act of taking advantage of a weakness in a computer system to compromise its security. It is the concrete action that allows a threat to transform a vulnerability into an actual incident. This exploitation can target confidentiality, integrity, or availability of data. It occurs when an attacker exploits a weakness in a system to gain unauthorized access, elevate privileges, or disrupt services, thereby affecting information security objectives. [5] In other words, it is the act of taking advantage of a flaw in a system or software to perform unauthorized operations or cause a denial of service. [4]

For a better understanding, let's consider the case of a thief who spots an unlocked door in a house. The unlocked door is the vulnerability, and entering to steal represents exploitation. In the IT context, a hacker can exploit a vulnerability in unpatched software to access a server or steal data. This step is crucial because it moves from a potential threat to an actual incident, and it justifies the importance of security updates, system hardening , and regular penetration testing.

c. Elevation of privileges

Privilege escalation refers to the process by which an attacker gains higher access rights than originally granted, often by exploiting vulnerabilities in the system. This technique is crucial for cybercriminals because it allows them to bypass access controls and gain access to sensitive resources. It is the act of exploiting a vulnerability to gain higher-level access to a system or network, often leading to unauthorized administrative rights. [5] It occurs when an attacker gains elevated access to resources that are normally protected by an application or user. [4] It is comparable to an employee with limited access to certain areas of a company, but by exploiting a flaw in the security system, gains access to restricted areas reserved for management. In IT, this means that an unauthorized user can, for example, move from standard user access to administrator access, allowing them to perform potentially harmful actions or steal sensitive information.

d. Other attacks

Based on all these types of attacks, several techniques can be used to make them as powerful and effective in achieving their objectives and targets including:

- Phishing

It is a cyberattack technique aimed at deceiving users into obtaining sensitive information (logins, passwords, banking details) by pretending to be a legitimate entity. Attackers usually use fraudulent emails, messages, or websites imitating reliable services. Phishing attacks are social engineering attempts to trick users into revealing confidential information by pretending to be a reliable source, often via email or fraudulent websites. [5] It is also a form of social engineering in which attackers trick individuals into providing personal or financial information by pretending to be legitimate organizations. [4] , it essentially exploits human psychology to obtain confidential information, often exploiting fear, urgency, or curiosity to manipulate victims. [6] So, it is like a person sending a fake official mail to trick a person into handing over their keys or safe deposit box code. In the digital world, an email or website may appear perfectly authentic, but it is actually designed to steal your personal information. This attack relies less on technology than on human psychology, which makes it particularly dangerous. Prevention relies on vigilance, user training, and the use of anti-phishing filters.

In June 2025, the hacker group ShinyHunters stole personal data from millions of customers of the Gucci, Balenciaga, Brioni , and Alexander McQueen brands, all owned by the French conglomerate Kering. The compromised data included names, contact details, addresses, dates of birth, and purchase histories, but no financial or government-issued identification data. ShinyHunters claimed responsibility for two attacks, one on Gucci the previous year and another in April, claiming to have stolen 56 million records. They also demanded a €750,000 bitcoin ransom from Balenciaga, although negotiations broke down. [7]

- Malware

The term malware (short for malicious software) refers to any software designed to infiltrate, damage, or disrupt a computer system without the user's knowledge. It includes different types of malicious programs: viruses, worms, Trojan horses, spyware, rootkits, etc. Malware is software specifically designed to disrupt, damage, or gain unauthorized access to a computer system. Examples include viruses, worms, and Trojan horses. [5] It is sometimes considered an intruder hidden in a building, capable of spying, sabotaging, or stealing information without anyone noticing. In the digital world, it can spread via downloaded files, infected emails, or compromised websites. Protection relies on antivirus software, updates, and good security practices. Using this technique, in 2017, the NotPetya ransomware infected the global shipping giant Maersk, causing major disruptions to its global operations. The attack used tools such as EternalBlue and Mimikatz to infiltrate unpatched systems, irrevocably encrypting the machines' data. Maersk estimated the total cost of the attack to be between $250 million and $300 million. [8]

- Ransomware

Ransomware encrypts victims' files or locks their systems, demanding payment to restore access. It is one of the fastest-growing cybercrime threats. [5] In March 2018, the City of Atlanta was hit by a ransomware attack using the SamSam malware . The attack compromised multiple computer networks within Atlanta City Hall, restricting access to a wide range of online platforms, city operations, and databases. The cybercriminals demanded a ransom of over $50,000 in bitcoin, but the city refused to pay. The incident disrupted various government services for several months, costing millions of dollars in damages. [9]

1.1.3. Pentest and Red teaming

A. Pentesting concepts ,

Penetration testing Penetration testing (also known as penetration testing) is a proactive method of simulating cyberattacks on a computer system to identify its vulnerabilities before real attackers exploit them. The main objective is to measure the level of security and propose corrective measures. Penetration testing is the practice of simulating attacks on a computer system or network to identify vulnerabilities and evaluate security measures. [5] It involves authorized simulated attacks against systems to detect security weaknesses, assess risks, and improve defenses. [4] To achieve this, a specific path has been established to follow in order to achieve this.

a. Recognition phase

Reconnaissance involves gathering as much information as possible about the target, using public sources and technical probing. [4] It is like a detective observing a house from the outside to note its weak points, without yet entering.

b. Phase scan

Scanning is the active analysis of network services to detect open ports, running applications, and potential vulnerabilities. [5] Scanning helps identify services, open ports, and exploitable vulnerabilities on the target. To achieve this, several typical tools can be used, including Nmap , Nessus, and OpenVAS , in order to create an accurate map of the infrastructure. This is the equivalent of testing all doors and windows to see which ones are unlocked.

c. Operational phase

Exploitation involves executing attacks against discovered vulnerabilities to gain access or elevate privileges. [4] This phase involves taking advantage of identified vulnerabilities to gain access to the system, escalate privileges, or retrieve sensitive information. To implement this phase, one can use Metasploit or use custom exploits with the sole objective of demonstrating the real-world impacts of vulnerabilities. It is like a burglar using a found key or a weak point in the lock to enter the house.

d. Post-operation phase.

Post-exploitation involves consolidating access, maintaining persistence, and collecting critical information to report vulnerabilities. [5] This is a phase that involves maintaining access, collecting sensitive information, and preparing reports for the security team to identify actual impacts and provide remediation recommendations. It is during this technique that we move on to creating backdoors and exfiltrating data. This is the phase where the attacker controls the system to understand the extent of weaknesses and document all the flaws found.

B. Red teaming

Red Teaming is a more comprehensive and realistic approach than traditional pentesting , including technical, social engineering, and physical aspects. It differs from pentesting in that pentesting focuses on specific objectives (systems or applications), while Red Teaming assesses the overall security of the organization. Red Teaming involves leveraging both technical and human defenses. [4] Red teams go beyond standard penetration testing to realistic attacks against all aspects of an organization's security posture. [5] It's like sending a full team of "professional burglars" to test all the defenses in and around a house, including personnel and security systems, to see if it can actually withstand a real attack.

1.2. Metasploit Framework Overview

1.2.1. Historical

a. Origin

Metasploit was originally developed in 2003 by H.D. Moore, with the goal of providing an open-source framework for penetration testing and vulnerability exploitation. This framework allowed security professionals to test their systems in a legal and structured way, automating some of the complex steps of vulnerability exploitation. The Metasploit project began as a small collection of exploits written by H.D. Moore, providing penetration testers with a flexible and extensible framework for testing vulnerabilities. [10] It was originally created to provide security professionals with a platform to develop and execute exploit code against remote targets in a controlled environment. [3] It is like a simulated attack lab: it allows pentesters to replicate an attacker's actions, but in a safe and legal way, to identify weak points before they are exploited by real hackers.

b. Evolution

Over the years, Metasploit has evolved from a simple collection of exploits to a complete framework , integrating:

- Payloads to perform actions on compromised systems.
- Auxiliary modules for scanning and testing different services.
- Post-exploitation features to maintain access and collect information.

Metasploit 's evolution reflects the growing complexity of threats: modern cyberattacks are no longer limited to a single type of exploit, and the framework adapts to simulate all stages of a real attack, from reconnaissance to post-exploitation.

c. Modules and components.

The Metasploit Framework is based on a modular architecture, allowing for great flexibility in the design and execution of penetration tests. The main components are:

- Exploits module

Exploits are at the heart of the framework Metasploit , allowing penetration testers to launch attacks against known vulnerabilities. [3] Exploit modules are designed to exploit specific vulnerabilities in target systems. They allow targeted attacks to be executed to test a system's resistance to intrusions.

- Payloads

Payloads define what happens after a successful exploit, giving the attacker control of the target system. [10] Payloads are payloads executed after successful exploitation of a vulnerability. They can allow remote access, privilege escalation, or data exfiltration.

- Auxiliaries

Auxiliary modules are used to perform tasks such as network scanning, vulnerability detection, or fuzzing. They complement exploits by providing reconnaissance and analysis tools. They extend the functionality of the framework , enabling tasks such as analysis, fuzzing, and information gathering. [11]

- Post-exploitation

Post-exploitation refers to actions taken after a system has been compromised, such as information gathering, persistence, or privilege escalation. Post-exploitation modules allow testers to maintain access, gather information, and escalate privileges on compromised systems. [10]

1.2.2. Functioning

The framework Metasploit operates through a sequence of selecting an exploit, configuring options, choosing a payload, and executing the attack, followed by post-exploitation activities. [11] The operation of the Metasploit Framework relies on an interaction between its various modules:

- Exploit selection: The tester chooses an exploit module suitable for the identified vulnerability.
- Payload Selection : A payload is selected to determine the action to be performed after exploitation.
- Options Configuration: The parameters necessary for running the modules are configured.
- Attack Launch: The exploit is executed, and if the target is vulnerable, the payload is delivered.
- Post-exploitation: After a successful exploitation, post-exploitation modules can be used to maintain access or collect information.

The Metasploit Framework can be compared to a digital toolbox for security professionals. Each module acts as a specialized instrument, allowing real-life attacks to be simulated to identify and remediate vulnerabilities before they can be exploited by malicious actors. This modular approach provides essential flexibility and adaptability in the dynamic field of cybersecurity.

Historical attacks illustrate the reach of Metasploit . The WannaCry attack (2017), exploiting EternalBlue (MS17-010), infected 200,000 systems in 150 countries, causing losses estimated at USD 4 billion (Verizon, 2025, p. 22). In 2025, similar exploits, such as CVE-2024-47575 (FortiManager), were integrated into Metasploit , targeting critical infrastructure.

2. Tests and Proposals

We simulated tests in an isolated VMware environment (Kali Linux as attacker, Windows7 as target), following the steps to avoid any real exposure, i.e. network scan, network reconnaissance and scan, payload configuration and generation , session exploitation and takeover.

2.1. Tests

- Network scan

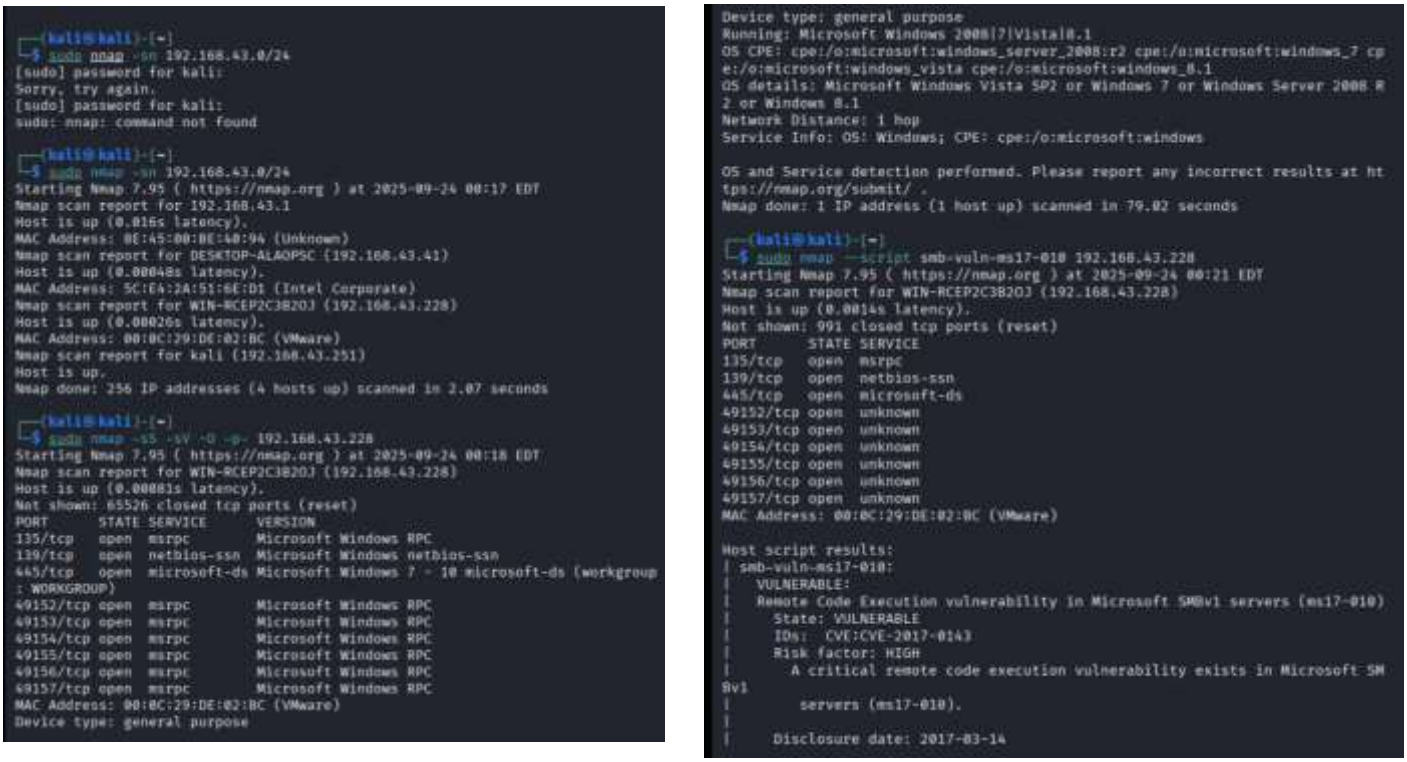

Figure 1 Detection of infection on machines

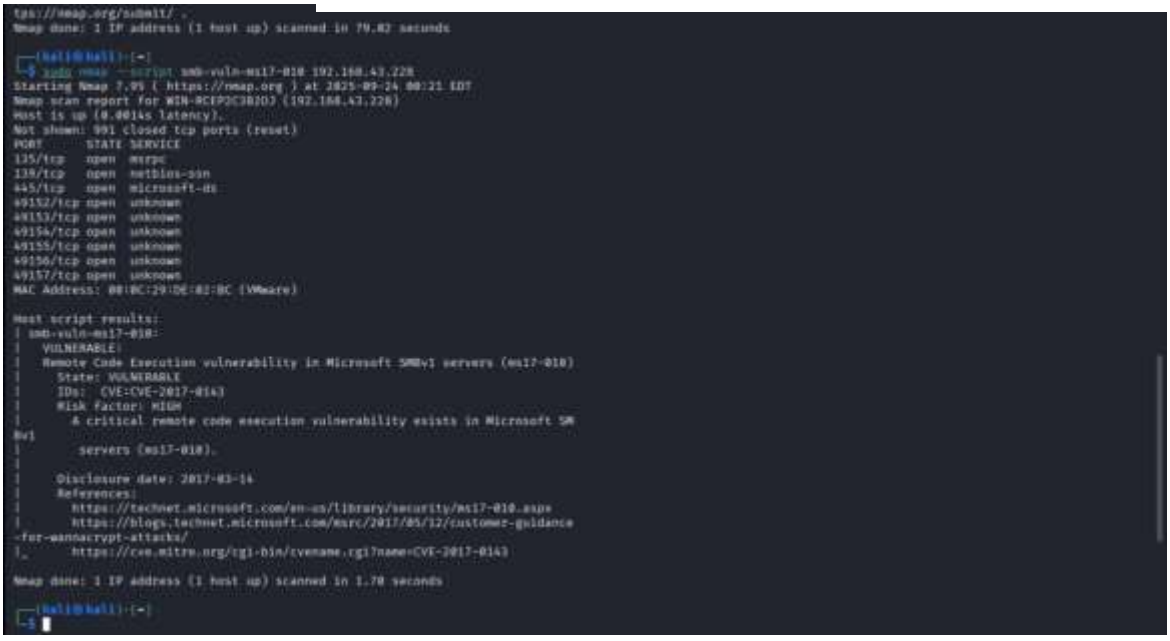

Figure 2Scanning the target machine

- Search for exploits for the vulnerability found with Metasploit

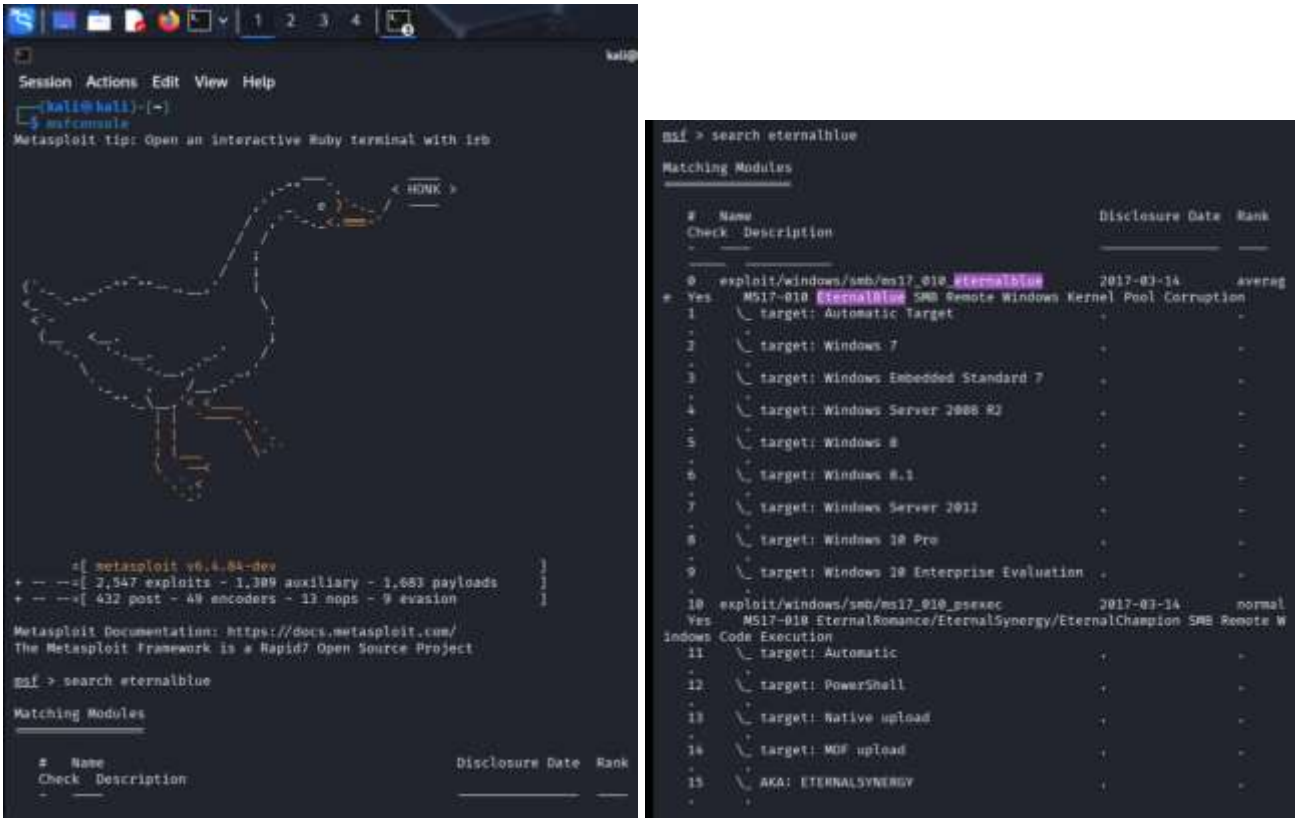

Figure 3Searching for exploits in msfconsole

- Payload Configuration and Generation

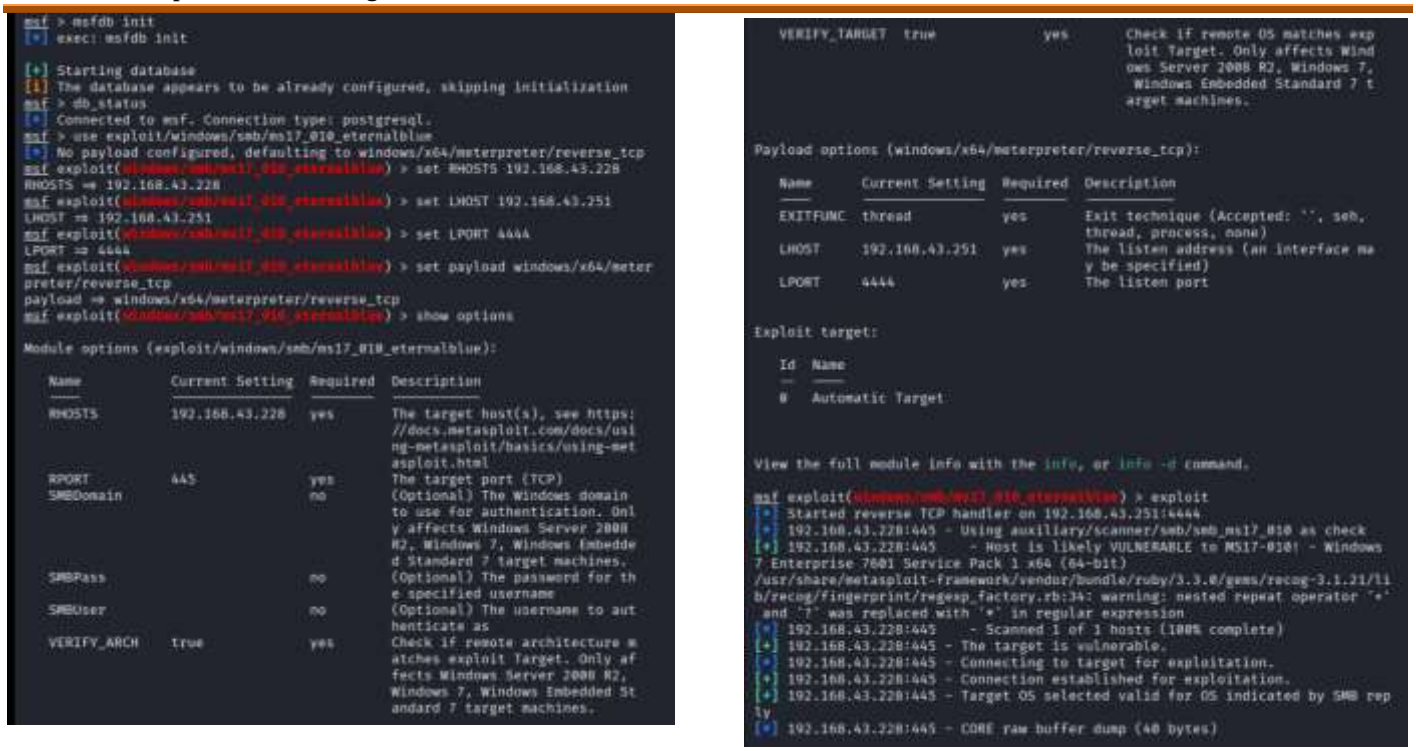

Figure 4 Payload configuration and generation

- Session Exploitation (Takeover)

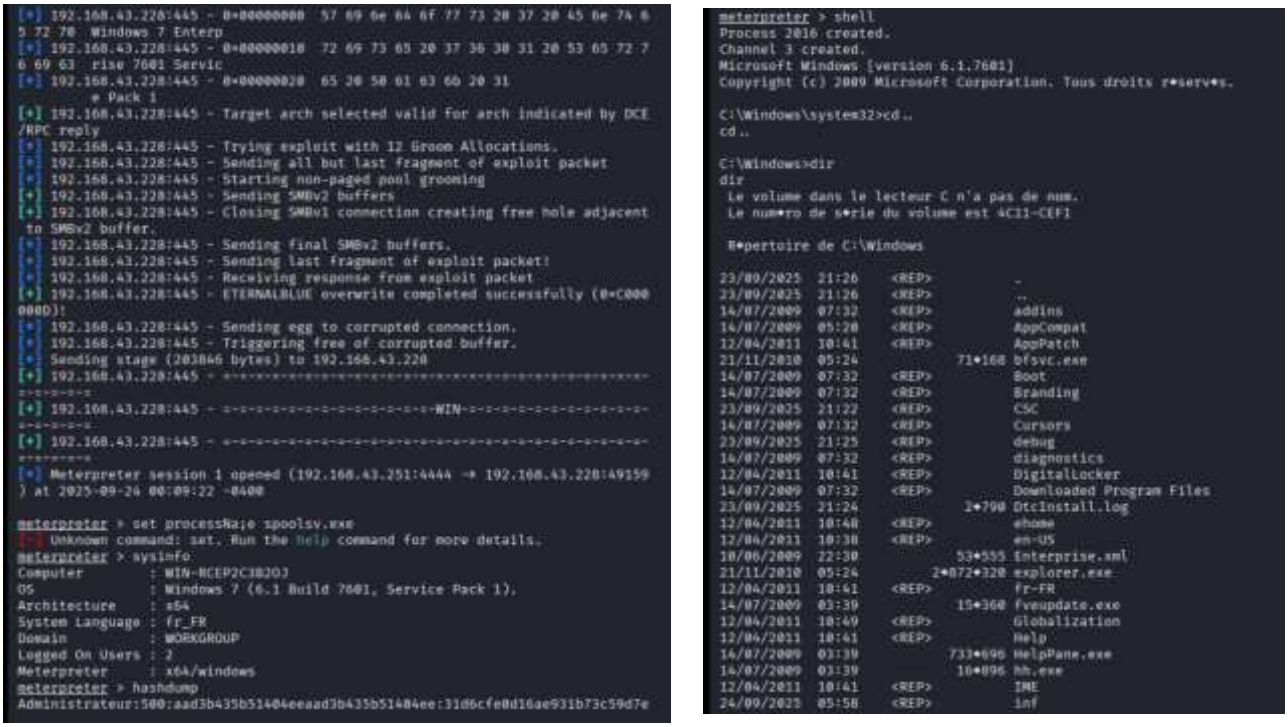

Figure 5 Session operation

2.2. Proposal

After testing these attack scenarios with Metasploit in the VMware lab , we concluded that network partitioning is the key to countering the spread. By partitioning, we mean a strict segmentation of the entire network, where everything is divided into isolated zones of dedicated subnets for each department or type of equipment, so that no user or device can ever access the entire system. This prevents a local breach, such as an EternalBlue exploit , from contaminating everything. To implement this effectively, we must integrate the Zero Trust Network Access (ZTNA) model, which assumes that nothing is trusted by default and verifies every access in real time.

In this context, it should be used with FortiNAC for network access control, as it allows granular visibility into devices. This means that FortiNAC dynamically segments based on profiles, isolating a compromised device without affecting the rest; FortiAuthenticator , which manages identity and access. This integration allows FortiAuthenticator to validate identities before FortiNAC grants access to the segment. From our perspective, by linking FortiNAC to FortiAuthenticator via these mechanisms, we create a barrier where each segment is locked down by multi-factor authentication and ZTNA policies, preventing full access.

Conclusion

Cyberattack risks pose significant impacts to businesses: financial losses, business disruption, and reputational decline, which can have long-term repercussions. To better understand the urgency of protecting against these risks, here is a review of the main analyses of cyberattacks via Metasploit that reveal the persistent vulnerabilities of digital systems and the urgency of proactive defenses. Simulated tests confirm that tools like Metasploit facilitate rapid intrusions, but network partitioning, reinforced by ZTNA, FortiNAC , and FortiAuthenticator , offers effective mitigation by isolating segments and verifying each access. With economic impacts reaching USD 10.5 billion annually, adopting these solutions is essential for organizations. This study encourages resilient cybersecurity, based on tested and adapted practices.

References

[1] "WEF_Global_Cybersecurity_Outlook_2025.pdf". Accessed: 24 September 2025. [Online]. Available at: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

[2] W. Stallings and L. Brown, *Computer Security: Principles and Practices,* New York, NY: Pearson, 2018.

[3] H. Moore, "PRAISE FOR METASPLOIT: THE PENETRATION TESTER'S GUIDE."

[4] D. Kim and MG Solomon, *Fundamentals of Information Systems Security* . Jones & Bartlett Learning.

[5] W. Stallings and L. Brown, *Computer Security: Principles and Practices,* . New York, NY: Pearson, 2018.

[6] "Social Engineering: The Science of Human Hacking, 2nd Edition | Wiley," Wiley.com. Accessed: September 19, 2025. [Online]. Available at: https://www.wiley.com/en-us/Social+Engineering%3A+The+Science+of+Human+Hacking%2C+2nd+Edition-p-9781119433385

[7] MS Correspondent Technology, "Hackers steal customer data from Gucci and Alexander McQueen." Accessed: September 19, 2025. [Online]. Available at: https://www.thetimes.com/uk/technology-uk/article/gucci-balenciaga-cyberattack-customer-data-rkmg8m83d

[8] A. Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired* . Accessed: September 19, 2025. [Online]. Available at: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[9] K. Young, "Cyber Case Study: City of Atlanta Ransomware Incident," CoverLink Insurance - Ohio Insurance Agency. Accessed: September 19, 2025. [Online]. Available at: https://coverlink.com/case-study/city-of-atlanta-ransomware/

[10] D. Maynor and T. Wilhelm, *Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research* .

[11] "Metasploit, 2nd Edition." Accessed: September 20, 2025. [Online]. Available at: https://nostarch.com/metasploit-2nd-edition