**EXPLOITING MS17\_010\_ETERNALBLUE ON WINDOWS 7**

**Digital Security Final Report (2023)**

****

**Text

Description automatically generatedA picture containing logo

Description automatically generated**

**Student Name: Ekata Ghimire**

**LBU Id: 77261096**

**TBC ID: 6091**

**Table of contents**

**Abstract**

This report provides an overview of ethical hacking using the Metasploit Framework ms17 to exploit vulnerabilities in Windows 7 systems. The objective is to demonstrate the capabilities of this framework for identifying and addressing security weaknesses before malicious hackers can exploit them. The report includes a detailed analysis of the steps involved in conducting the hack, the tools used, and the results obtained. The importance of ethical hacking is also discussed, including improved security, innovation, compliance, and cost savings. Finally, the report addresses the importance of protecting the system against such attacks.

**1.0 Introduction**

**As modern technologies continue to emerge**, so do the associated vulnerabilities. Therefore, it is essential to be aware of potential security breaches before they happen. This is where the concept of ethical hacking comes into play. The practice of identifying and exploiting vulnerabilities in computer systems and networks in a lawful and ethical manner is known as ethical hacking. It is also known as “penetration testing”.

**1.1 Importance of Ethical hacking:**

1. Improved Security: This is accomplished by detecting and exploiting system weaknesses in computer networks and systems.
2. Innovation: By identifying vulnerabilities and developing new defense mechanisms, organizations can remain ahead of the constantly changing threat landscape.
3. Compliance: Many organizations are legally obligated, or industry regulations require them to conduct regular security assessments, including penetration testing. Ethical hacking ensures that they adhere to these requirements.
4. Cost savings: Identifying security vulnerabilities ahead of time can save organizations from costly data breaches and other security incidents.

**This report is intended** to provide an overview of the techniques used to exploit vulnerabilities in Windows 7 using Metasploit Framework ms17, and how these vulnerabilities can be leveraged to gain authorized access to a system.

**The main objective** of this report is to demonstrate the capabilities of using Metasploit Framework Ms17 for ethical hacking purposes, specifically targeting the vulnerabilities in Windows 7 systems. The report includes a detailed analysis of the steps involved in carrying out the hack, the tools used, and the results obtained. Additionally, the report could include how to protect the system so that hacking is not possible.

**The** **tools** used in the exploitation are nmap, Metaspploit framework (msf version6).

**2.0 Types of Hackers:**

**White Hat** Hackers, also called ethical hackers, utilize their hacking abilities to identify and correct security vulnerabilities in computer systems and networks. They are employed to evaluate the security defenses and ensure that they are robust enough to withstand attacks.

**Black Hat** Hackers are individuals who use their hacking abilities for malevolent purposes. They exploit security gaps in computer systems and networks to steal data, introduce malware, and cause harm.

**Grey Hat** Hackers are not malicious, but they do not have the authorization to access the systems they hack. They may hack for amusement or to reveal vulnerabilities in a system, but their actions can be against the law.

**Hacktivists** are hackers who employ their abilities to promote a political or social cause. They may deface websites, steal data, or launch denial-of-service attacks to make a statement or draw attention to an issue.

**Script Kiddies** are amateur hackers who use pre-written scripts and tools to launch attacks. They frequently lack a deep understanding of hacking and are motivated by the desire to showcase to their friends.

**State-Sponsored** Hackers are hackers employed by governments who utilize their skills to conduct espionage, steal intellectual property, and disrupt the operations of other countries.

**3.0 Vulnerability Description, Attack and Exploit Software.**

The emergence of MS17-010 EternalBlue was due to the detection of a crucial vulnerability in Microsoft Windows operating systems. The infamous WannaCry ransomware attack in 2017 first took advantage of this vulnerability, causing extensive damage across various organizations and countries.

The MS17-010 EternalBlue vulnerability is found in the implementation of the Server Message Block (SMB) protocol in Microsoft Windows, allowing attackers to execute any code on a targeted system by sending a specially crafted packet to the SMBv1 server. Its ability to be remotely exploited without user interaction or authentication poses a significant threat.

While Microsoft patched the vulnerability in March 2017, unpatched or outdated systems remain vulnerable to attacks using this exploit. Since the initial attack, various malware and ransomware families have utilized this exploit to infect systems worldwide.

The significance of regular vulnerability assessments and penetration testing to detect and remediate such vulnerabilities before they can be exploited by attackers is emphasized by the MS17-010 EternalBlue vulnerability. It also highlights the importance of following security best practices, such as keeping systems updated and employing strong authentication mechanisms to protect against potential attacks.

The report includes a detailed analysis of the steps involved in carrying out the hack by using the Metasploit framework Ms17\_010\_Eternalblue and nmap.

**4.0 Anatomy of Attack:**

**4.1 Enumeration**

Actively probing a target system or network to extract specific details about it is known as enumeration. This process enables cybersecurity professionals to gather valuable information about the target system, including open ports, running services, installed software, usernames, and other system details that are valuable in identifying potential vulnerabilities or attack vectors. Analyzing this information is crucial in securing the target system or network against potential cyber threats.

**4.2 Network reconnaissance**

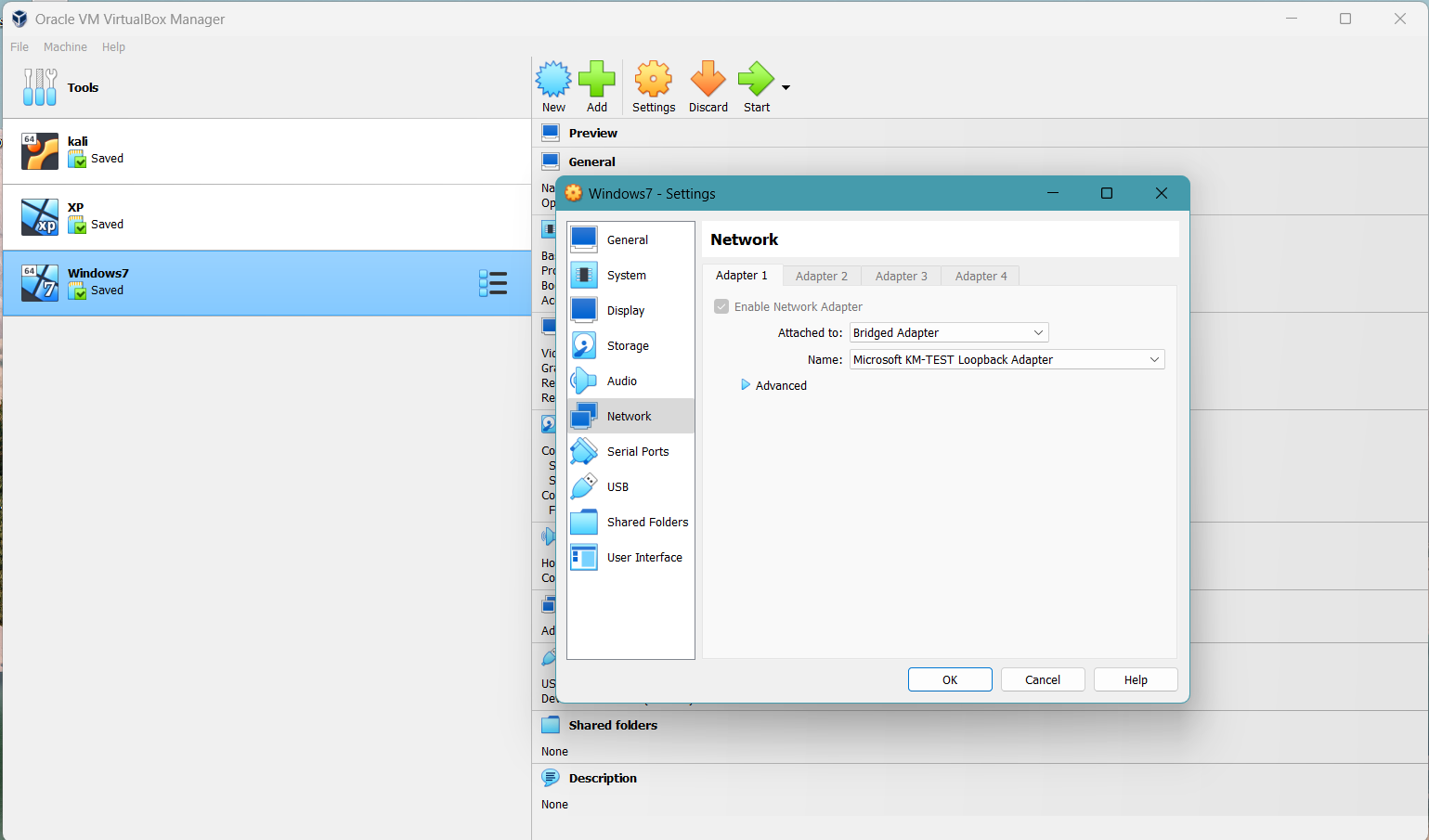
When aiming to exploit a system, the first action is to conduct a network scan to gather details about the system's structure, OS, IP addresses, open ports, active services, and whether the firewalls are activated or not. This data aids in identifying any weaknesses that can be utilized to infiltrate the target.

First it is important to be on the same network system to be able to hack. For that in the virtual box windows 7 and kali Linux has been installed and configured.

**4.2.1 Configuring same Network on the Targeting Machine and Targeted Machine.**

**4.2.1.1 Windows 7 (Target Machine):**

Setting up Network and Ip address to 172.16.33.4.

Graphical user interface, text, application, email

Description automatically generated

**4.2.1.2 Kali configuration (Targeting Machine):**

Setting up Network and Ip address to 172.16.33.3.

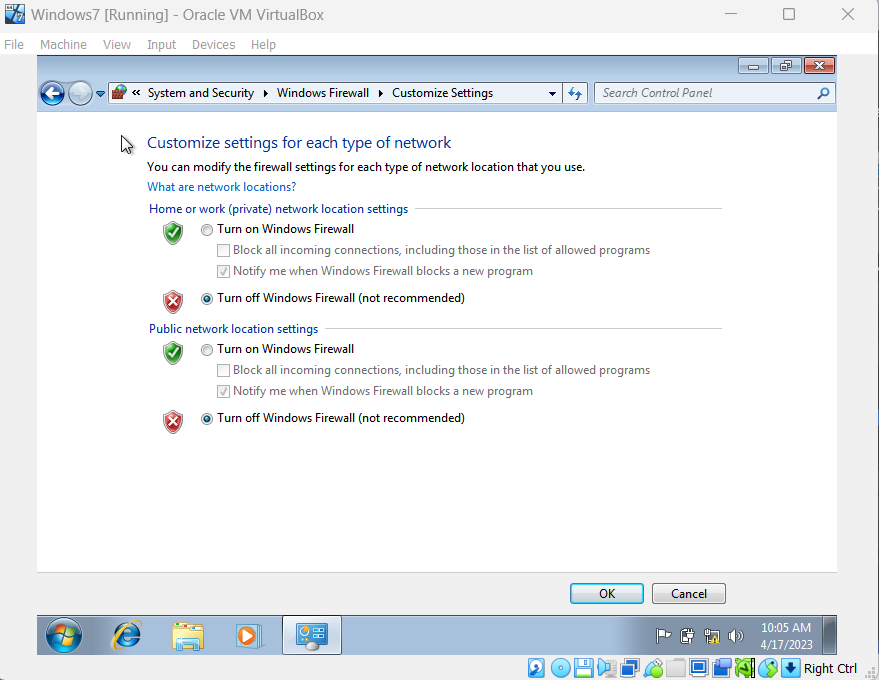
Graphical user interface, application

Description automatically generated

Graphical user interface, application

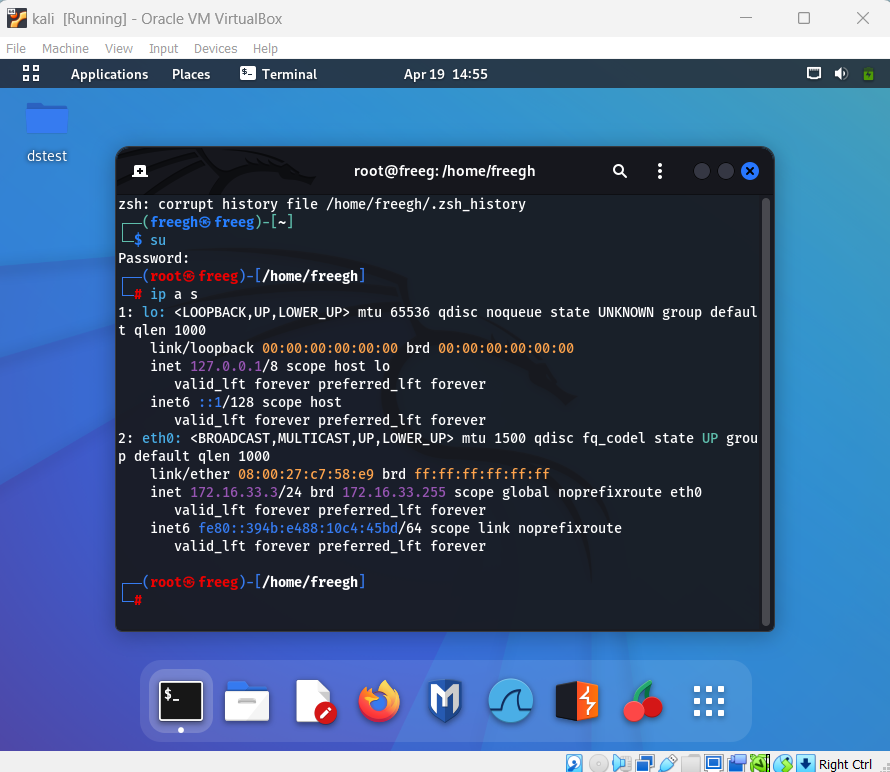
Description automatically generated

**4.2.1.4 Setting up the windows 7 firewall off**



**4.2.2 Knowing the Ip address of targeting Machine.**

Since we set the same network for the target machine and the targeting machine, checking the Ip address of the targeting machine(kali).



**4.2.3 Attack** **Anatomy table**

|  |  |  |  |
| --- | --- | --- | --- |
| Purpose | Machines | Network Adapter | Ip address |
| Targeting Machine | Kali | Bridge Adapter, NIC  Microsoft KM-TEST Loopback Adapter | 172.16.33.3/24 |
| Target Machine | Windows 7 | Bridge Adapter  Microsoft KM-TEST Loopback Adapter | 172.16.33.4/24 |

**4.2.4 Network scanning**

**Nmap**, short for Network Mapper, is a free and open-source software tool used for network exploration, management, and security auditing. It is a command-line utility that can be used to scan networks and hosts, and retrieve information such as open ports, running services, operating systems, and other details. Nmap is a valuable tool for network discovery, vulnerability assessment, and penetration testing, making it a popular choice among security professionals and network administrators. Its strong features and versatility allow users to evaluate and improve the security of a network. Here nmap is used to scan the possible networks available.

Graphical user interface, text

Description automatically generated

Three Ip addresses are scanned which are inside the same network among which we will target the machine with the Ip address 172.16.33.4.

**4.2.5 Checking network connection with the targeted machine**

Network connectivity checking on the targeting machine with the targeted machine Ip address.

Graphical user interface, text

Description automatically generated

**4.2.6 Checking the open port, operating system, and versions.**

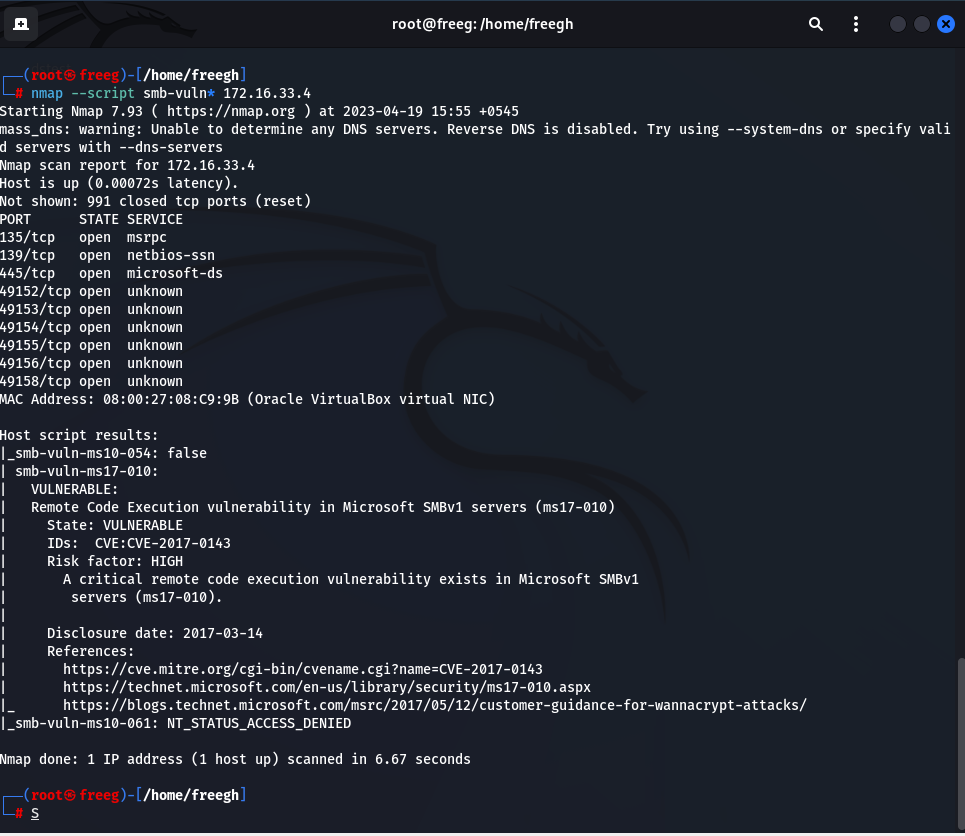
Text

Description automatically generated

By using the command "nmap -sv 172.16.33.4", Nmap is instructed to scan the IP address 172.16.33.4 and identify any open ports. The scan results reveal that there are nine TCP ports that are open on the targeted machine, including ports 135, 139, 445, 49152, 49153, 49154, 49155, 49156 and 49158. This information could be used by an attacker to identify potential vulnerabilities and plan a targeted attack on the system.

**4.2.7 Detect specific vulnerabilities related to the Server Message Block (SMB) protocol.**

The "nmap --script smb-vuln\* 172.16.33.4" command makes use of a set of Nmap scripts referred to as smb-vuln\* to pinpoint weaknesses linked to the Server Message Block (SMB) protocol, which is integral to file sharing and network communication in Windows-operated systems. Upon running this command against a specified IP address, one can establish the existence of any SMB vulnerabilities flagged by the smb-vuln\* script on the target system. This information can be leveraged to address and rectify the vulnerabilities, thwarting any attempts by malicious actors to exploit them.

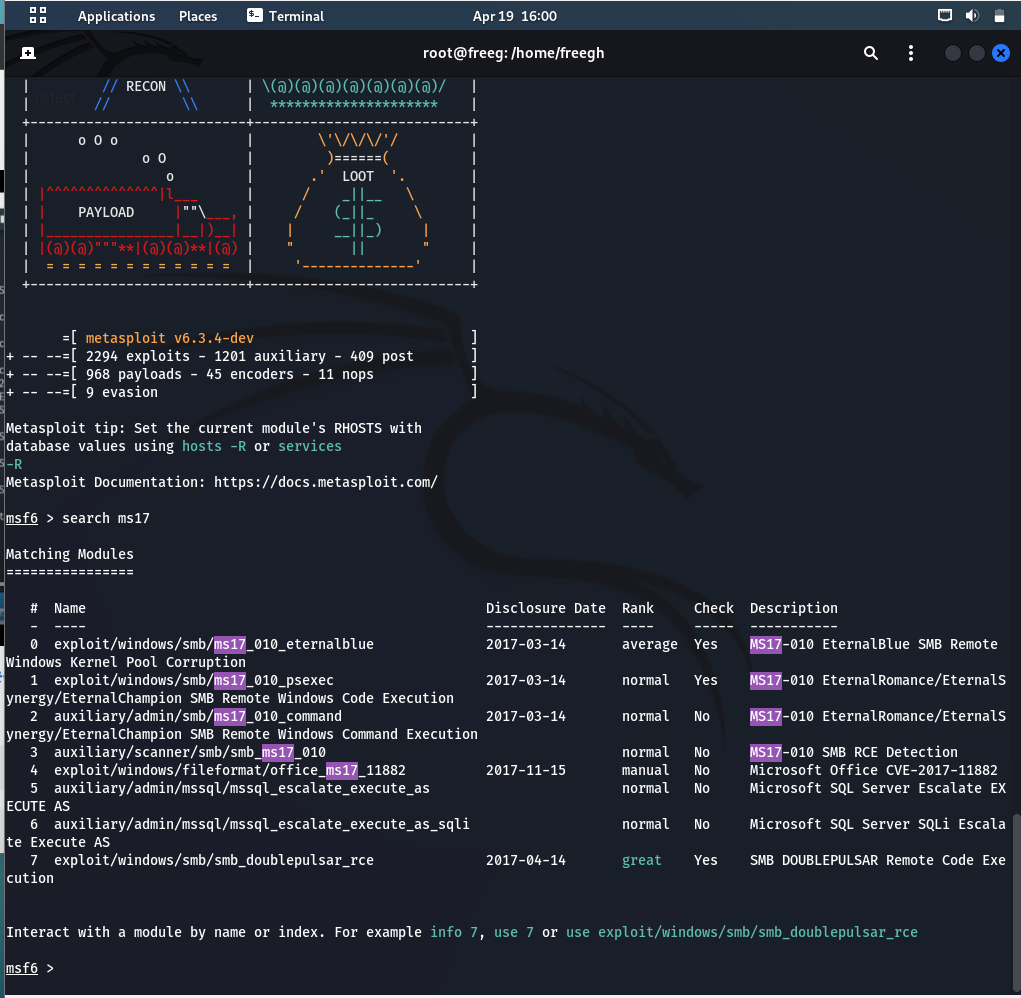


This shows that the output "\_smb\_vuln\_ms10\_054: false" means that the Nmap script did not find any vulnerability related to MS10-054 on the target system, which affects certain versions of Windows through the SMB protocol. The value "false" indicates that the target system is not susceptible to this exploitation.

On the other hand, the output "\_smb\_vuln\_ms10\_010:" shows that the script has detected the presence of vulnerability MS10-010, which also relates to the SMB protocol in Windows.

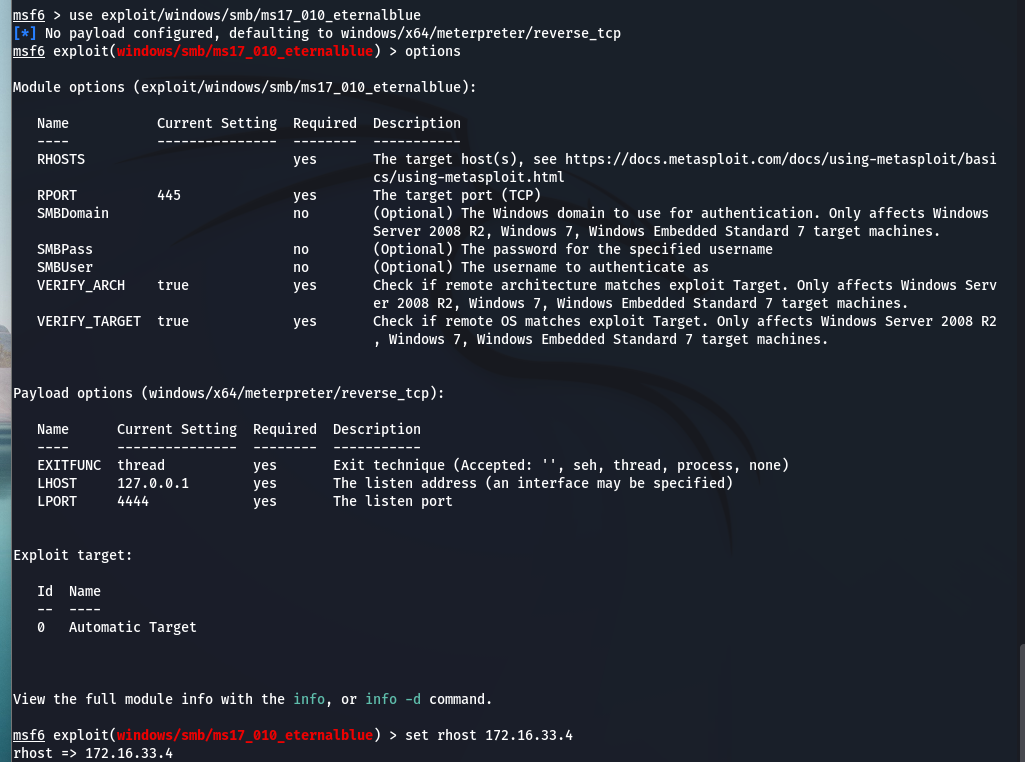
**4.2.8 Exploitation of the Targeted Machine.**

**4.2.8.1 Searching the available ms17 exploits in the msfconsole**

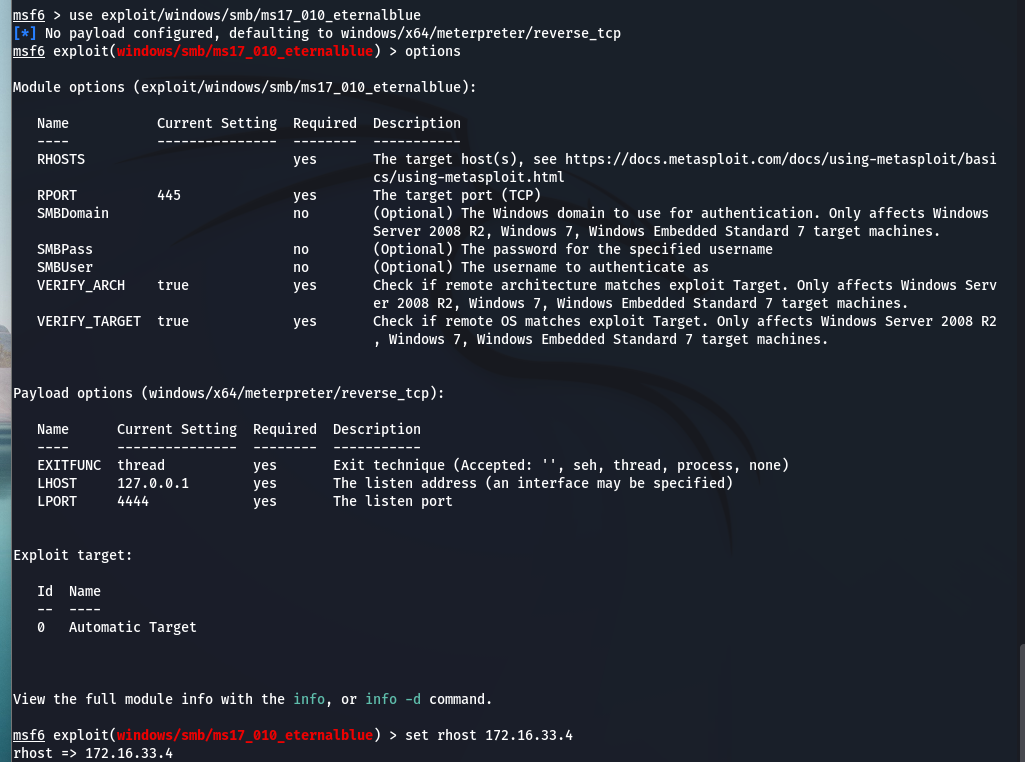


After the “search ms17” in msfconsole it will search for any modules or exploits in the Metasploit framework related to vulnerabilities with identifier “MS17”.

I decided to use the **exploit/windows/smb/ms17\_010\_eternalblue** exploit.



**4.2.8.2 Payload configuration (RHOST and LHOST)**

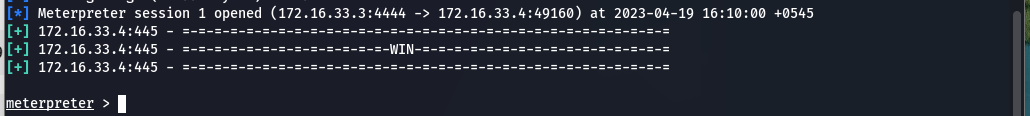




**4.2.8.3 Beginning the exploitation.**



After successful exploitation you will see a view like this:



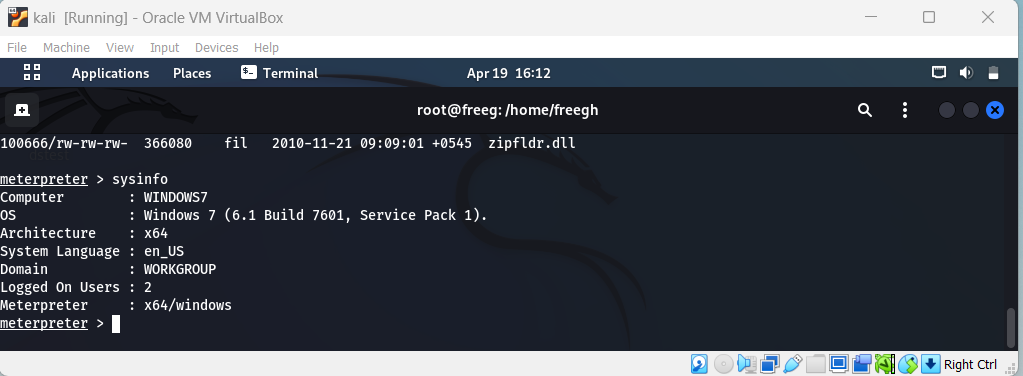
The Windows 7 has been successfully Hacked using the MetaSploit Framework:

**exploit/windows/smb/ms17\_010\_eternalblue.**

**4.2.9 Post Exploitation**

Post-exploitation is a phase of a cyber-attack that occurs after an attacker has successfully breached a target system. In this phase, the attacker attempts to maintain their access and escalate their control over the target system to achieve their ultimate objectives, which may include stealing sensitive information, spreading malware, or launching further attacks.

**4.2.9.1 Extracting information of the Exploited Machine**



This sysinfo provides system information about the exploited machine which can be used by an attacker to extract important information about the OS, hardware and configuration.

**4.2.9.2 Shell Session**

A screenshot of a computer

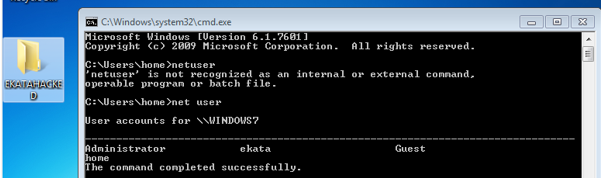
Description automatically generated with medium confidence

Obtaining a shell through the Meterpreter payload.

**4.2.9.3 Creation of the new user**

Graphical user interface

Description automatically generated with medium confidence



A new user ekata has been created in windows 7 from the exploited shell of the kali machine.

**4.2.9.4 Checking the Ip configuration from the extracted shell.**

**Text

Description automatically generated**

**4.2.9.5 Folder Creation inside the desktop**

A screenshot of a computer

Description automatically generated with medium confidence

**4.2.9.6 Creating a file.**



Graphical user interface, text, application, Word

Description automatically generated

The Figure above shows that a new txt file has been created and that has some context written on it.

**4.2.9.7 Deletion of the folder**

Deletion of the existing folder Hello.



**6.0 Related Software**

In addition to the software mentioned in this report, there are other programs that perform similar functions.

Icon

Description automatically generated with medium confidence

**Zenmap** is a user-friendly software that provides a graphical user interface for Nmap, which can be beneficial for non-technical users. Zenmap provides a user-friendly point-and-click interface that presents Nmap results in an easily understandable format. It also offers additional features such as network topology mapping and graphical representations of network data.

**Nessus** is a vulnerability scanner that detects weaknesses in network devices using a database of known vulnerabilities.

**Wireshark** is a network protocol analyzer that captures and analyzes network traffic to identify network problems and troubleshoot issues.

A picture containing text, web

Description automatically generated

**Armitage** is a graphical user interface (GUI) for Metasploit that

simplifies and automates several hacking tasks like network

mapping, vulnerability scanning, and exploitation. For novice

and non-technical users who may be intimidated by the

command-line interface of Metasploit, Armitage is a useful tool.

Armitage simplifies attack launches by enabling users to select targets from a graphical interface and provides visualization and collaboration features to streamline the hacking process.

**Cobalt Strike** is a commercial software that enhances the capabilities of Metasploit by adding advanced features such as social engineering campaigns, post-exploitation tools, and team collaboration.

**Canvas** is a commercial penetration testing platform that offers Metasploit integration and other tools like network mapping, vulnerability scanning, and exploit development. These software tools can be useful in detecting and exploiting vulnerabilities to evaluate and improve the security of a network.

**5.0 Defensive tactics to prevent exploitation.**

The attacks can be prevented from happening using various techniques and technologies. There are several ways to do that. One of them is Ensuring that the system is regularly updated with the most recent security patches and updates issued by the vendor. Such updates may involve patches specifically designed to tackle the EternalBlue vulnerability.

To maintain the security of your system, it's important to have control over who can **access** it and to **authenticate** their identity. Additionally, using security systems can aid in identifying and blocking malicious traffic while network segmentation can reduce attacker mobility. Keeping **anti-malware** software up-to-date and regularly conducting security assessments and tests can help detect and resolve vulnerabilities. There are different types of anti-malware software like: Signature-based detection. Heuristics-based detection, Sandboxing, Machine learning, Behavioral analysis, and many others.

Graphical user interface, text, application

Description automatically generated

**Firewalls** serve as a shield that separates a secure internal network from untrusted external networks, such as the Internet. They are effective in preventing malicious attacks by denying unauthorized access attempts to a network or system. Firewalls can also prevent the propagation of malware by blocking malicious traffic or communication from compromised systems. Moreover, they can enhance security by logging and reporting suspicious network activity and intrusion attempts.

**IronPort** is a protection solution against email and web-based threats such as viruses, spam, and phishing attacks. It uses content filtering, reputation filtering, and virus scanning to prevent harmful traffic from entering the network.

**6.0 Critical Reflection**

The exploit utilized in this case serves the purpose of showcasing the process of device scanning, the steps involved in exploiting vulnerabilities, and the possible security measures that can be taken to prevent such attacks. Although ethical hacking aims to uncover and address security weaknesses in networks and systems, it is crucial to acknowledge the potential negative consequences that may arise from utilizing such techniques. The primary threat is the possibility of malicious actors exploiting the same vulnerabilities found during ethical hacking for their own gain. Therefore, it is important to utilize these techniques with caution and responsibility to prevent any harm that may occur. Even though the exploit has legitimate applications, such as penetration testing and identifying security weaknesses, it can also be used by malicious actors to carry out harmful attacks on individuals or organizations. Hence, it is essential to consider the potential ramifications of using such tools and ensure that they are used ethically and responsibly. Furthermore, it is crucial to acknowledge that the discovery of vulnerabilities and the development of exploits should be geared towards improving system security by identifying and addressing weaknesses, rather than compromising them.

**7.0 Conclusion**

8.0 Bibliography