**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: Ethical hacking can help organizations to identify and address security weaknesses before malicious hackers can exploit them by identifying and exploiting vulnerabilities in computer systems.
2. Innovation: Organizations can stay ahead of the constantly evolving threat landscape by identifying vulnerabilities and developing new defense mechanisms beforehand.
3. Compliance: Many organizations are required by law or industry regulations to conduct regular security assessments, including penetration testing. Ethical hacking ensures that that they are meeting those requirements.
4. Cost savings: Having identified the security vulnerability beforehand can prevent costly data breaches and other security incidents that can damage an organization’s reputation and bottom line.

**1.2 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.

**1.3 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.

**2.0 Types of Hackers:**

**2.1 White Hat Hackers:** Also known as ethical hackers, they use their skills to identify and fix security vulnerabilities in computer systems and networks. They are hired to test their security defenses and ensure that they are strong enough to resist attacks.

**2.2 Black Hat Hackers**: These are the bad guys, who use their hacking skills for malicious purposes. They exploit vulnerabilities in computer systems and networks to steal data, plant malware, and cause damage.

**2.3 Grey Hat Hackers**: These hackers do not have malicious intent, but they do not have permission to access the systems they hack. They may hack for fun or to expose security flaws in a system, but their actions can still be illegal.

**24 Hacktivists**: These are hackers who use their skills to promote a political or social cause. They may deface websites, steal data, or launch denial-of-service attacks to make a statement or bring attention to a cause.

**2.5 Script Kiddies**: These are amateur hackers who use pre-written scripts and tools to launch attacks. They often do not have a deep understanding of hacking and are motivated by the desire to show off to their friends.

**2.6 State-Sponsored Hackers**: These hackers work for governments and use 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**

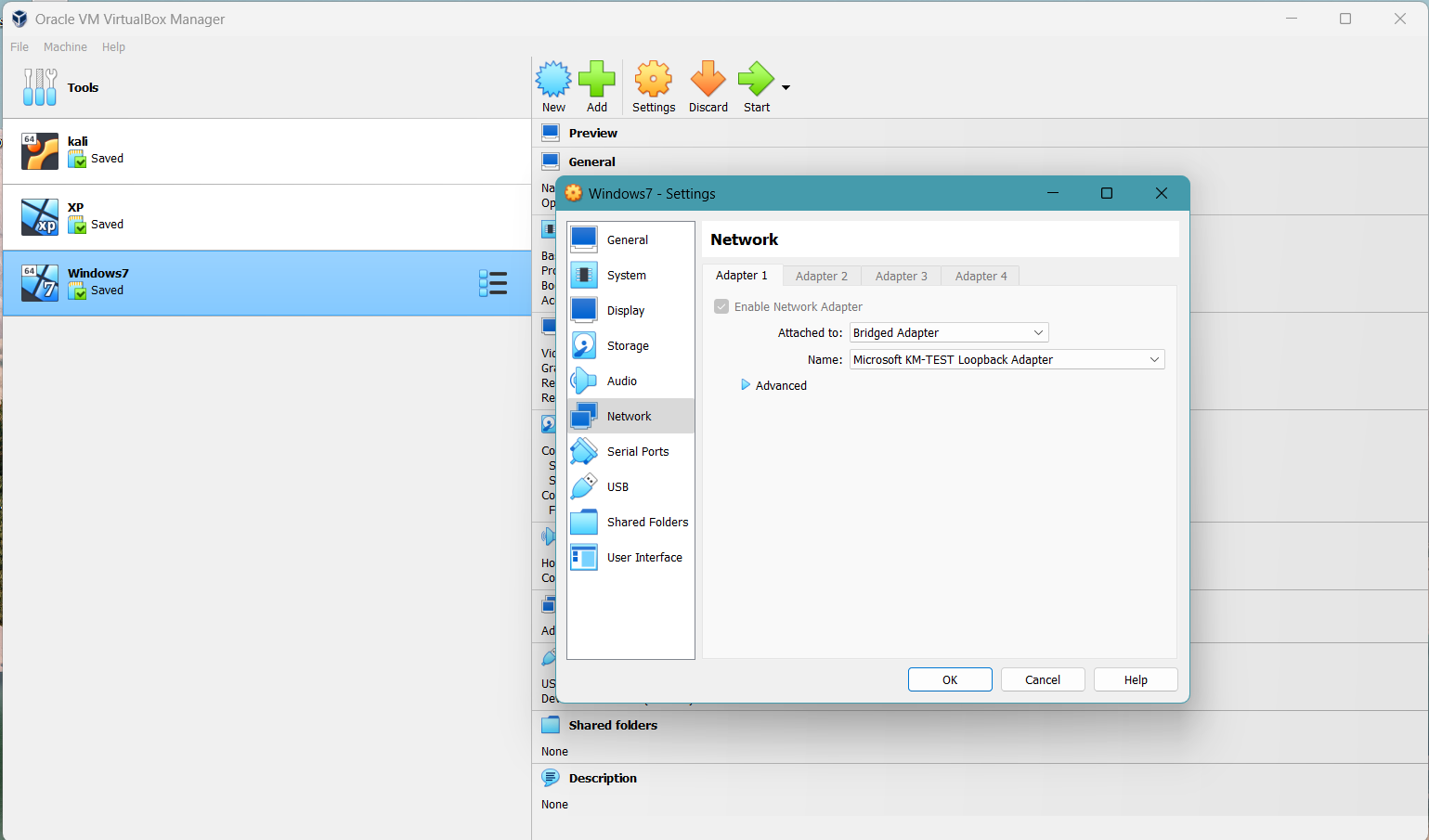
When aiming to exploit a system, the first action is to conduct a network scan to gather details about the system's structure, OS, IP addresses, open ports, active services, and whether the firewalls are activated or not. This data aids in identifying any weaknesses that can be utilized to infiltrate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

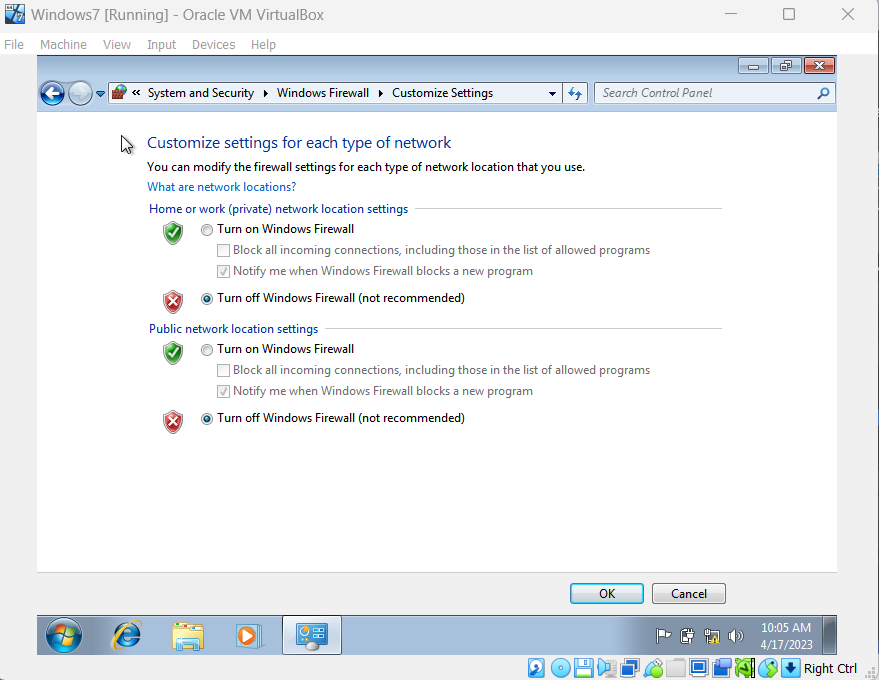
Graphical user interface, application

Description automatically generated

Graphical user interface, application

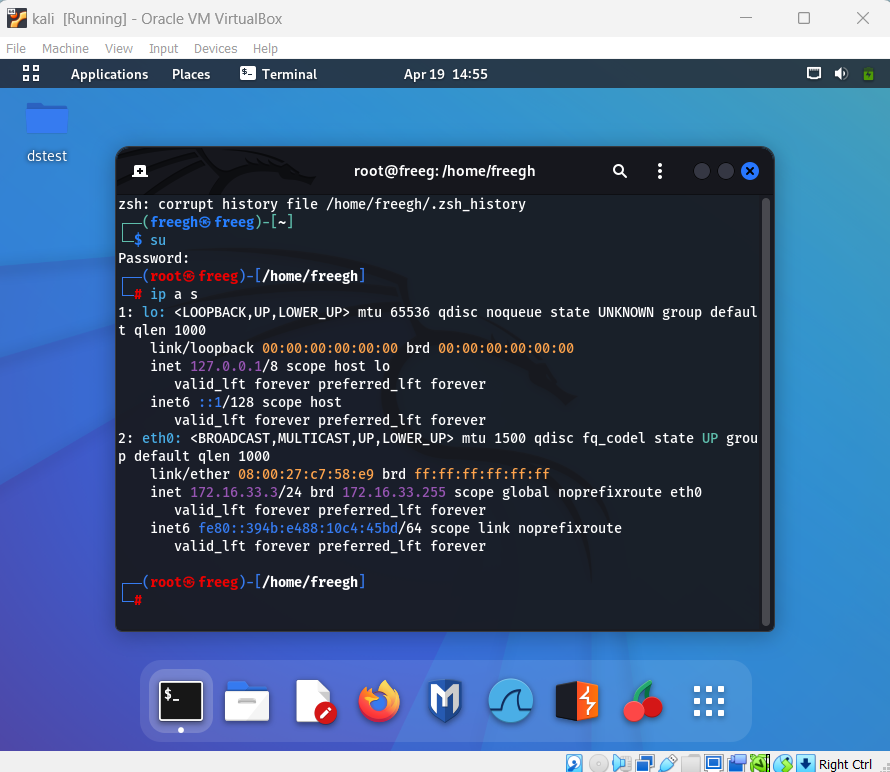
Description automatically generated

**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 Network scanning**

Graphical user interface, text

Description automatically generated

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

**4.2.3 Checking if network connection**

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

Graphical user interface, text

Description automatically generated

**4.2.4 Checking the open port, operating system,**

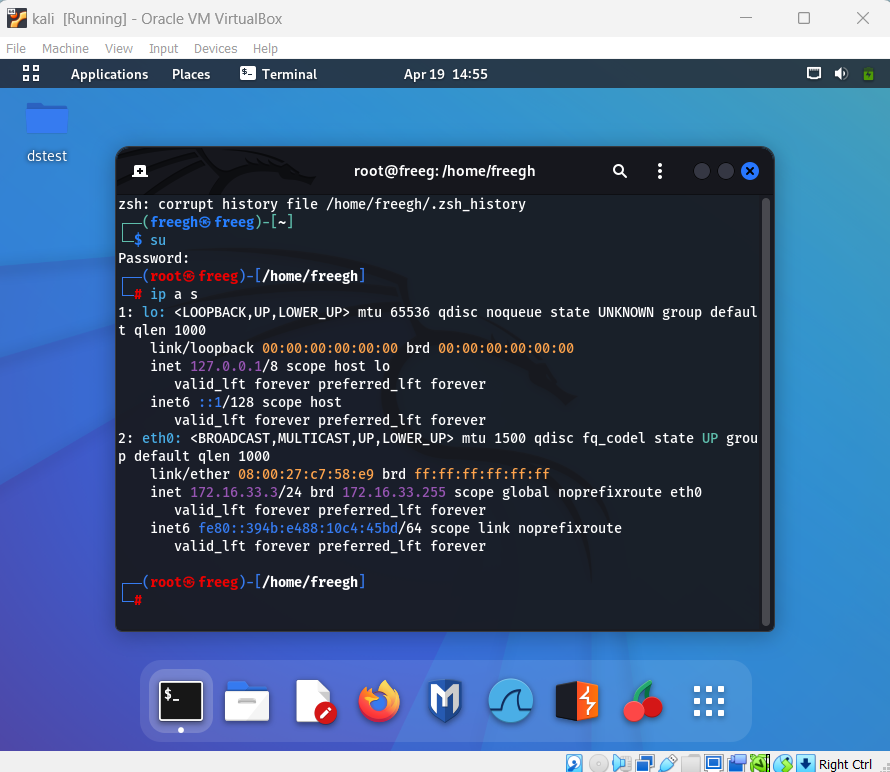
172.16.33.1 – pc ko ip address

Windows 7 ko configuration change

Kali ko configuration

Ip addres milako on windows 11 – own pc

Windows 7 firewall off

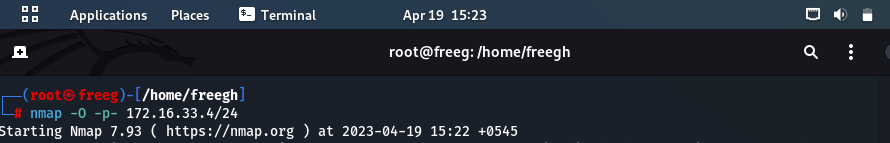


Ping reply

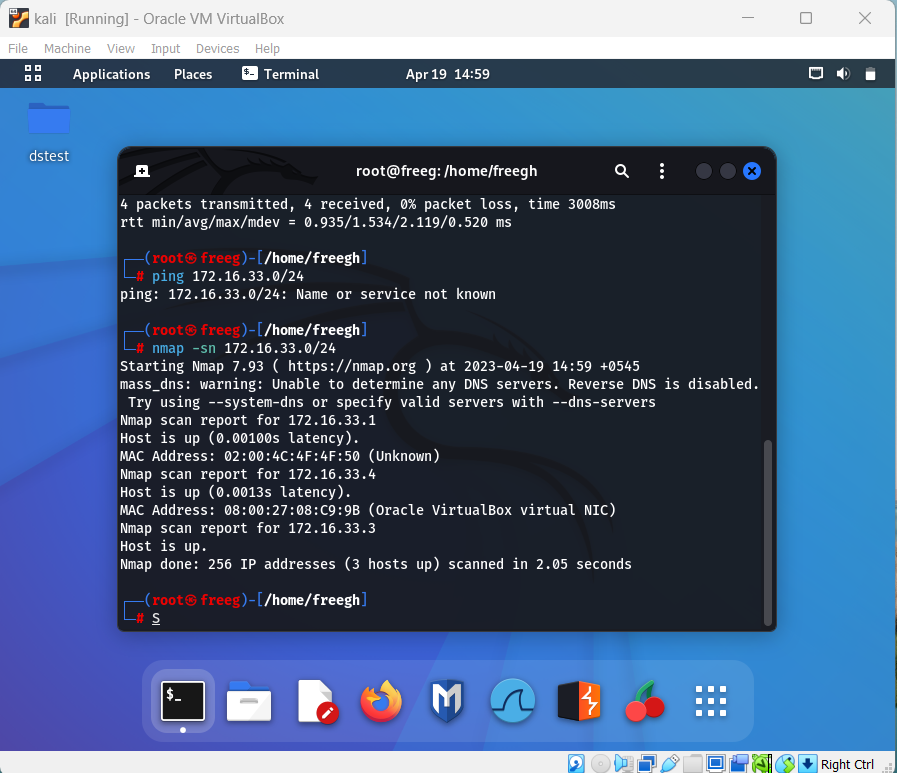
Graphical user interface, text

Description automatically generated

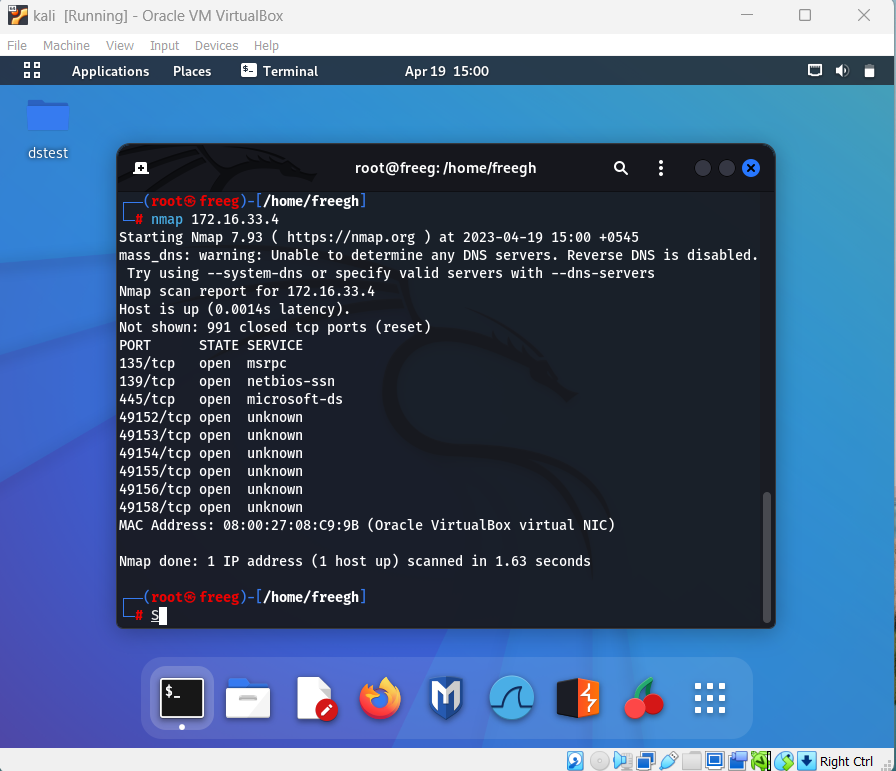
Knowing the open port and the operating system of the hacking pc

Text

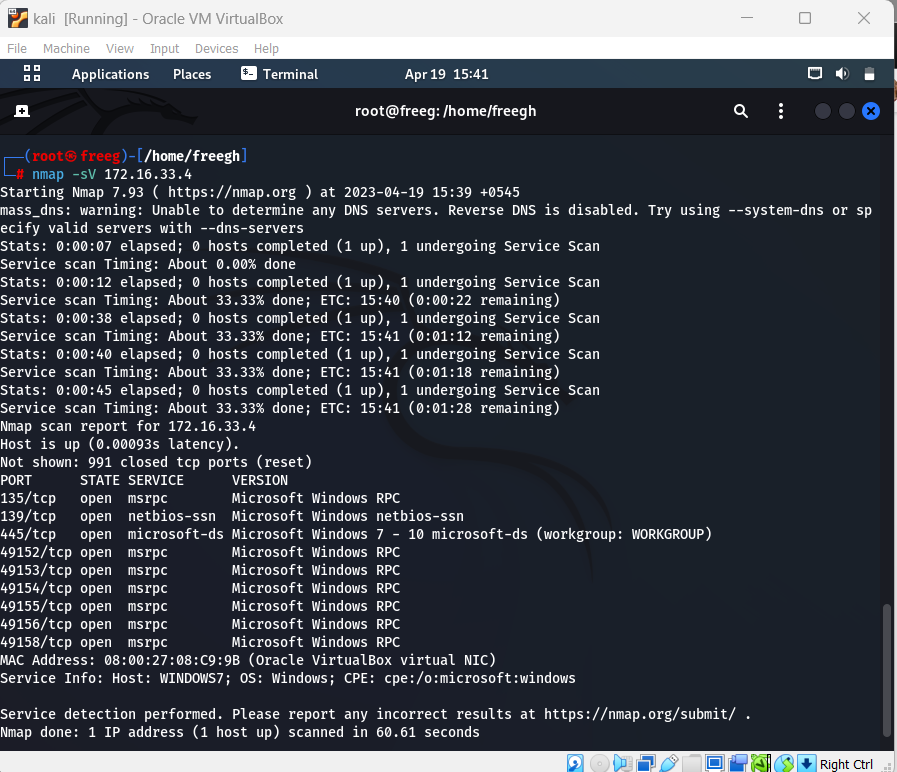
Description automatically generated

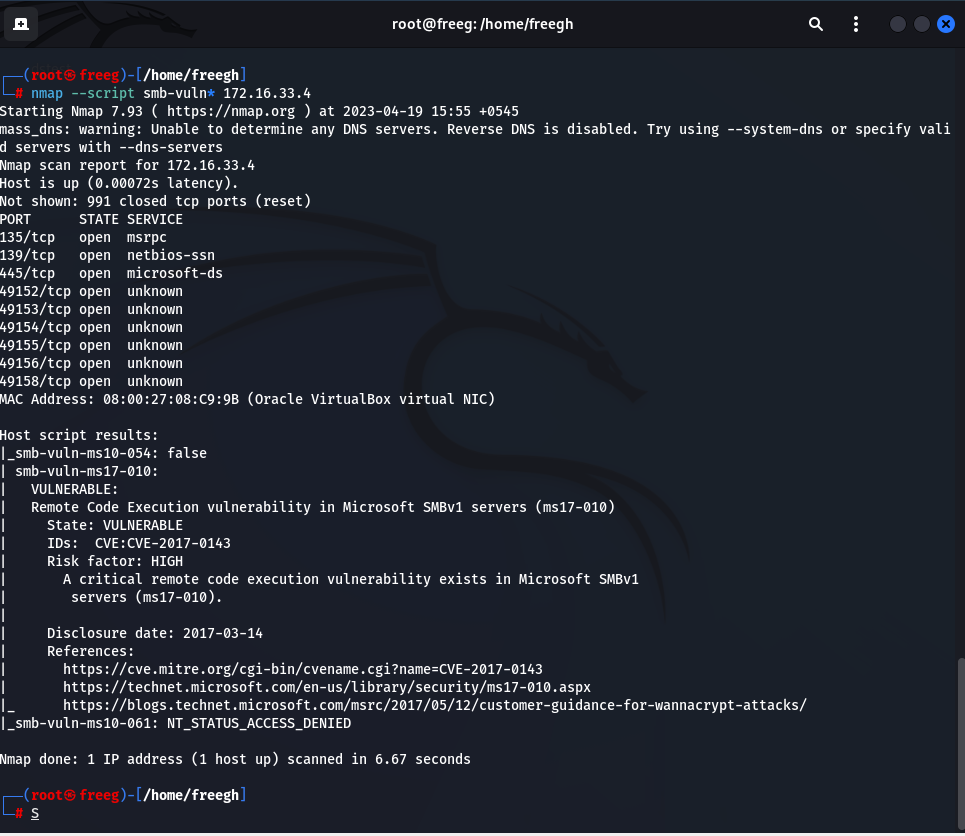


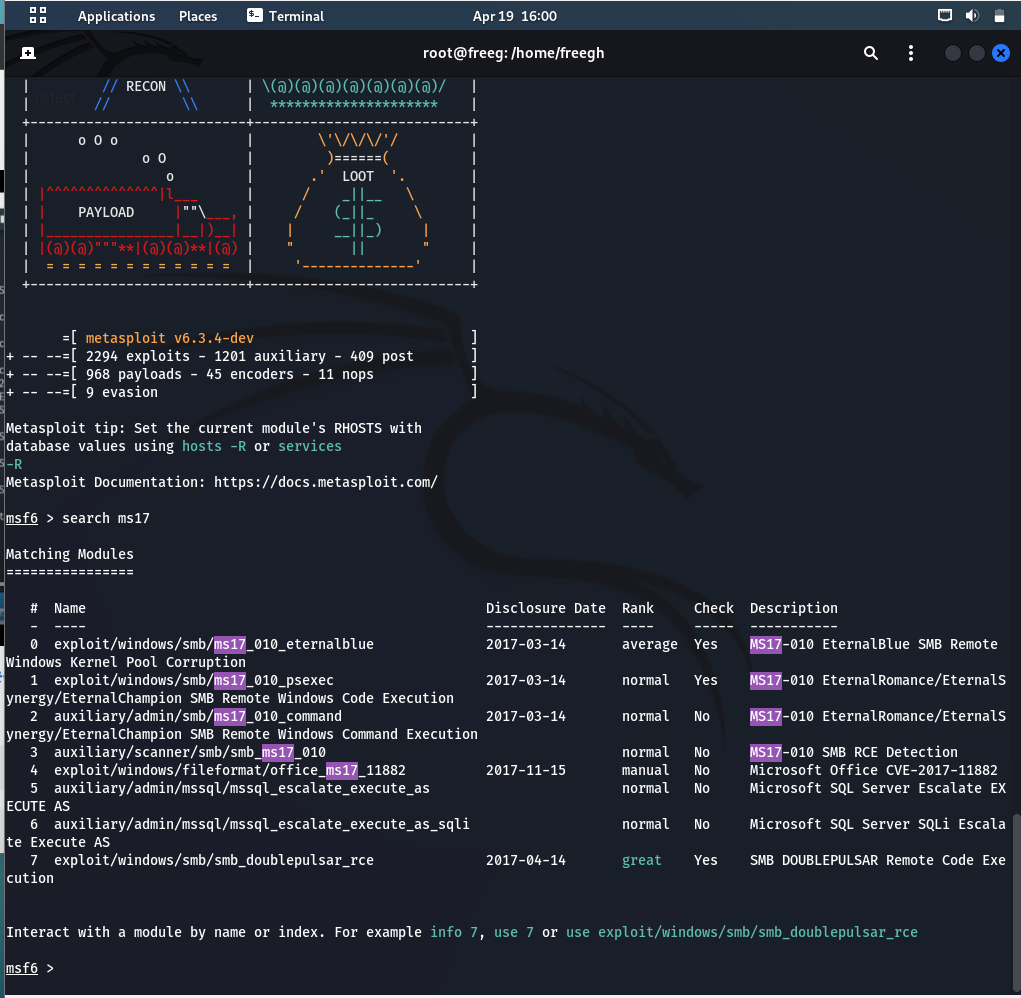
Open port tha paune

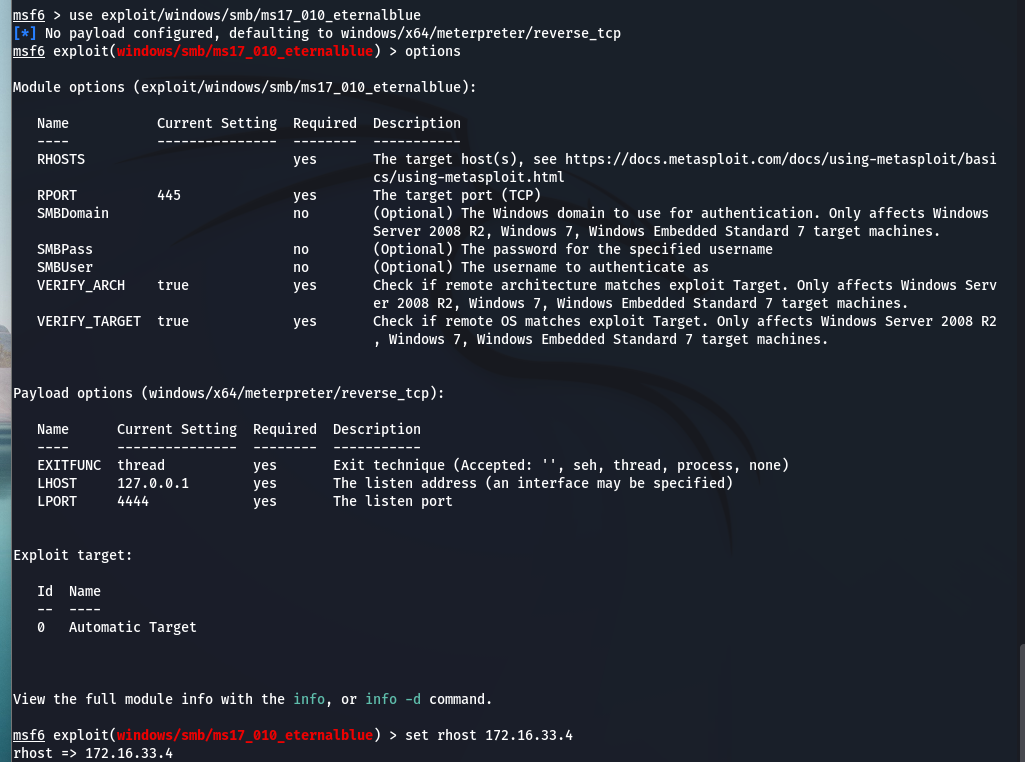


Which pc I am going to exploit tesko os soas sab dkhaidinxa

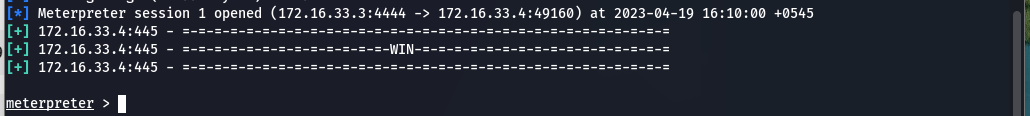


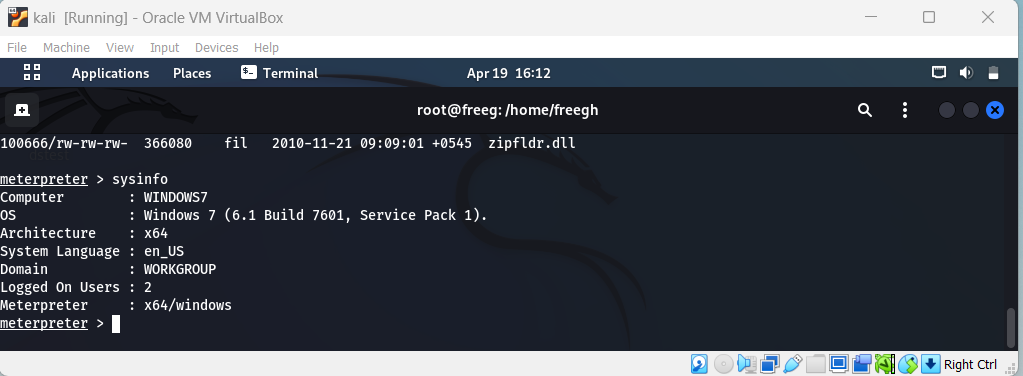
Script   








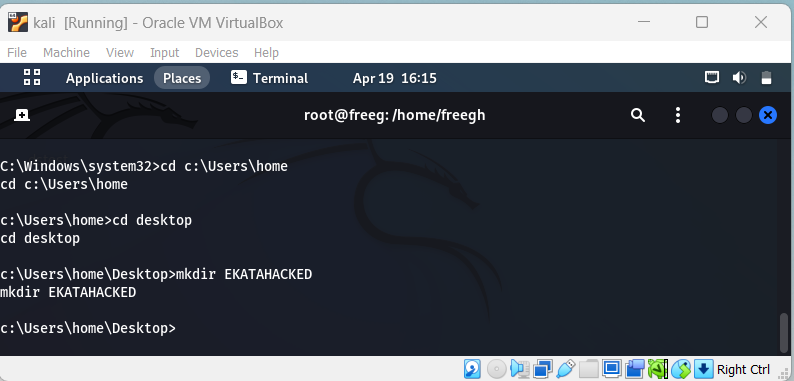




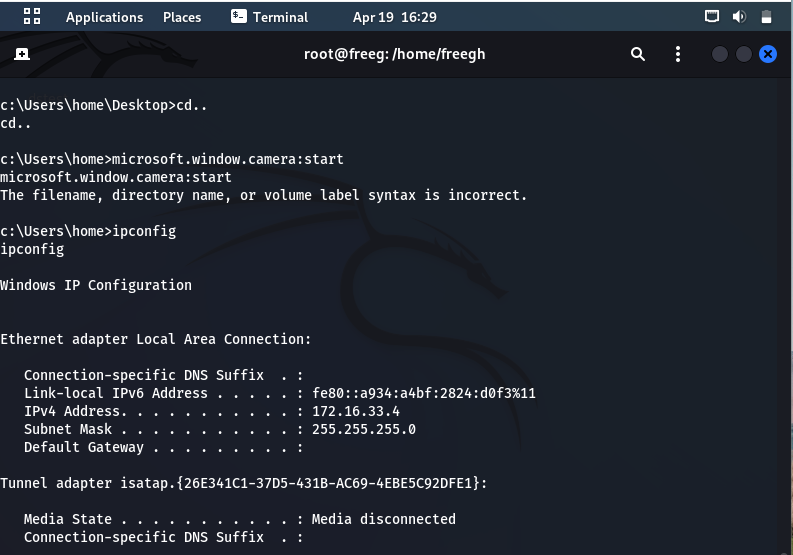
A screenshot of a computer

Description automatically generated with medium confidence

Cd desktop folder creation







New user created from the hacked shell.

Graphical user interface

Description automatically generated with medium confidence

Graphical user interface

Description automatically generated

Creating the file:



Graphical user interface, text, application, Word

Description automatically generated

A picture containing icon

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence