**Executive Summary**

This assessment aimed to evaluate the security vulnerabilities of a Windows 7 virtual machine configured with IP address 10.0.2.15. The machine was scanned using **Nmap** for open ports and running services. The scan revealed that the target was running SMB services on ports **139** and **445**, commonly associated with file sharing and remote access on Windows systems.

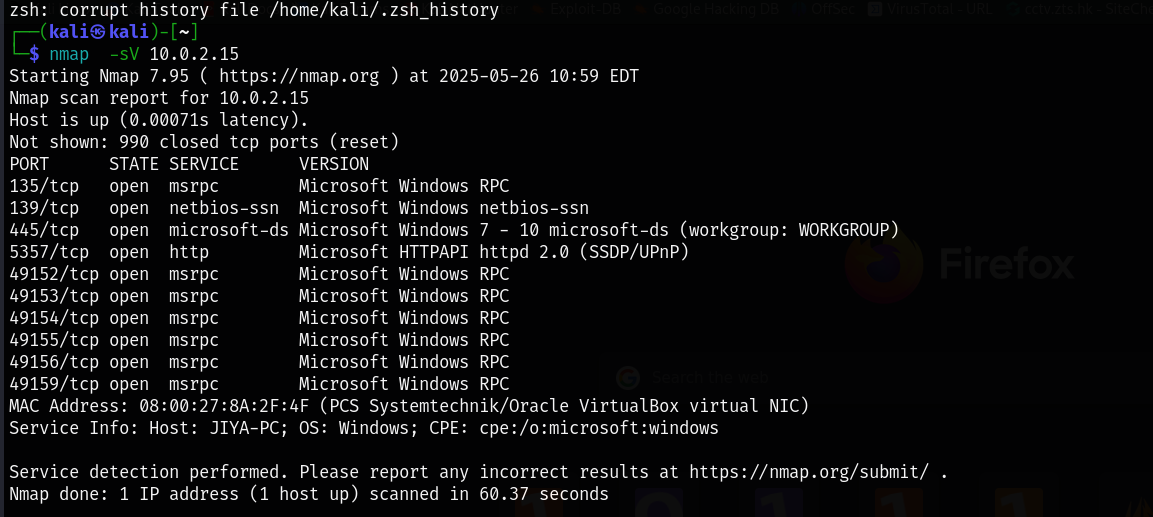
Upon further inspection using vulnerability scanning scripts, the system was found to be **vulnerable to MS17-010**, also known as **EternalBlue**, a critical SMBv1 flaw that allows **unauthenticated remote code execution**.

Using the **Metasploit Framework**, this vulnerability was successfully exploited. The attacker was able to gain a **remote shell with system-level access**, demonstrating complete compromise of the target host.

This test confirms the critical nature of unpatched SMB vulnerabilities and emphasizes the need for proactive patch management and service hardening.

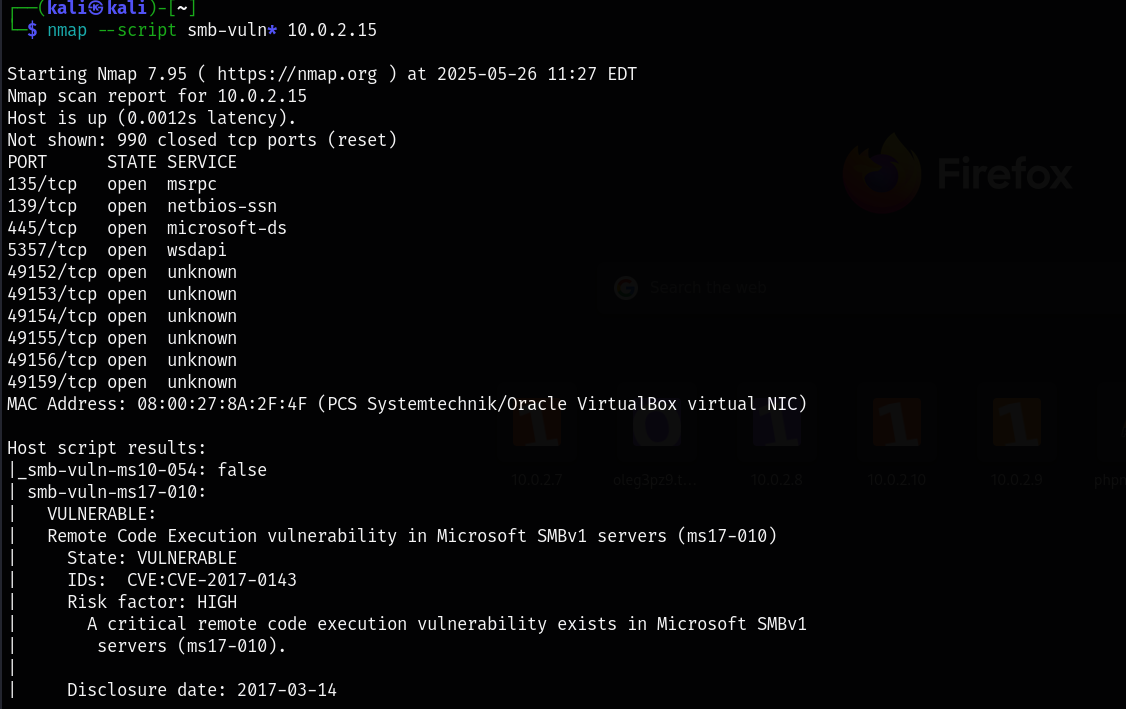
**Step 1: Nmap Scan Overview**

**🔹 Command Used:** nmap -sV 10.0.2.15



**Inference:**

* The presence of port **445** with **SMB service** suggests the system may be vulnerable to **EternalBlue (MS17-010)**.
* The system is likely running **Windows 7**, which is historically vulnerable to this exploit if unpatched.



**Step 3: Using Metasploit to Exploit EternalBlue**

Once the target is confirmed to be vulnerable to **MS17-010**, you can exploit it via Metasploit.

**🔹 Steps:**

1. **Start Metasploit:**

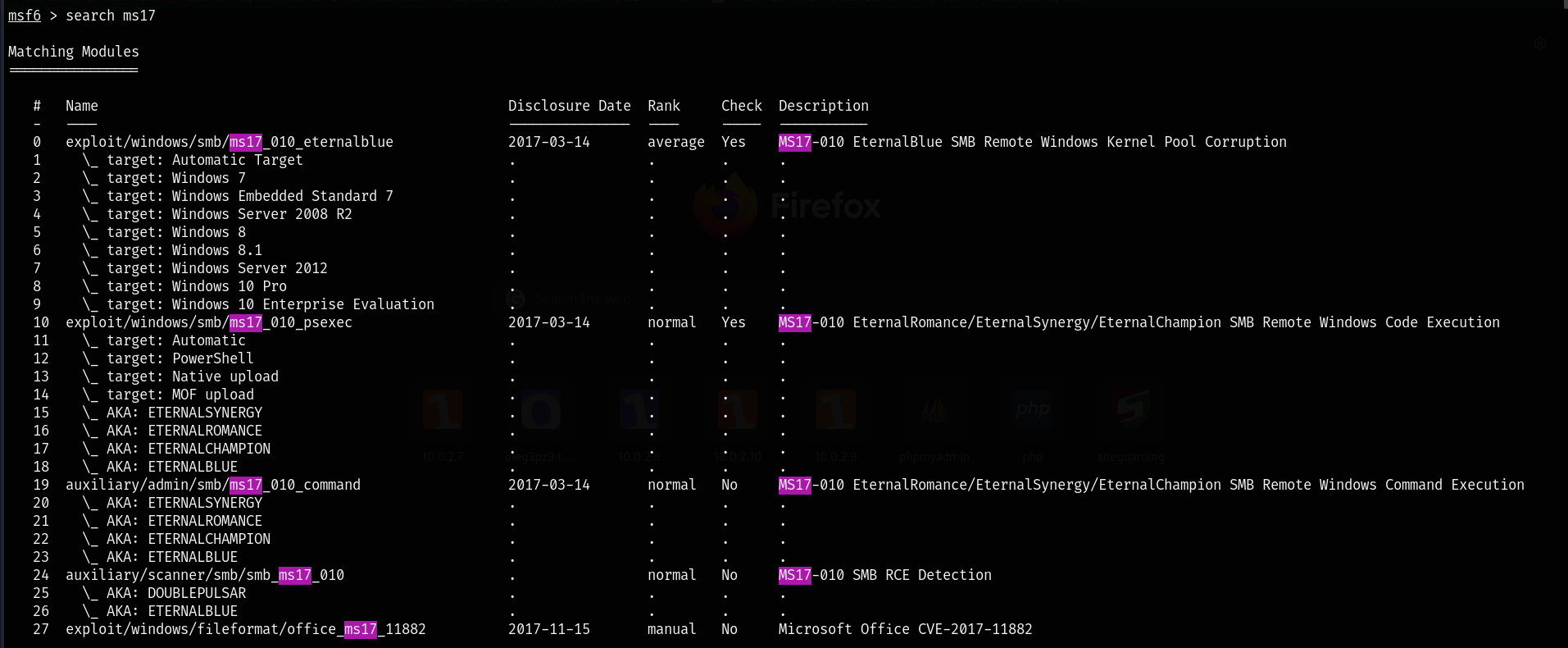
msfconsole

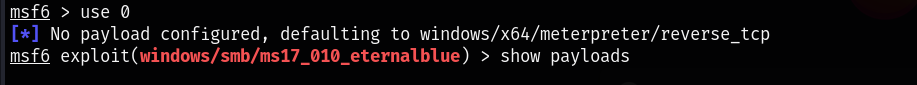
1. **Search for the exploit:**

search ms17\_010

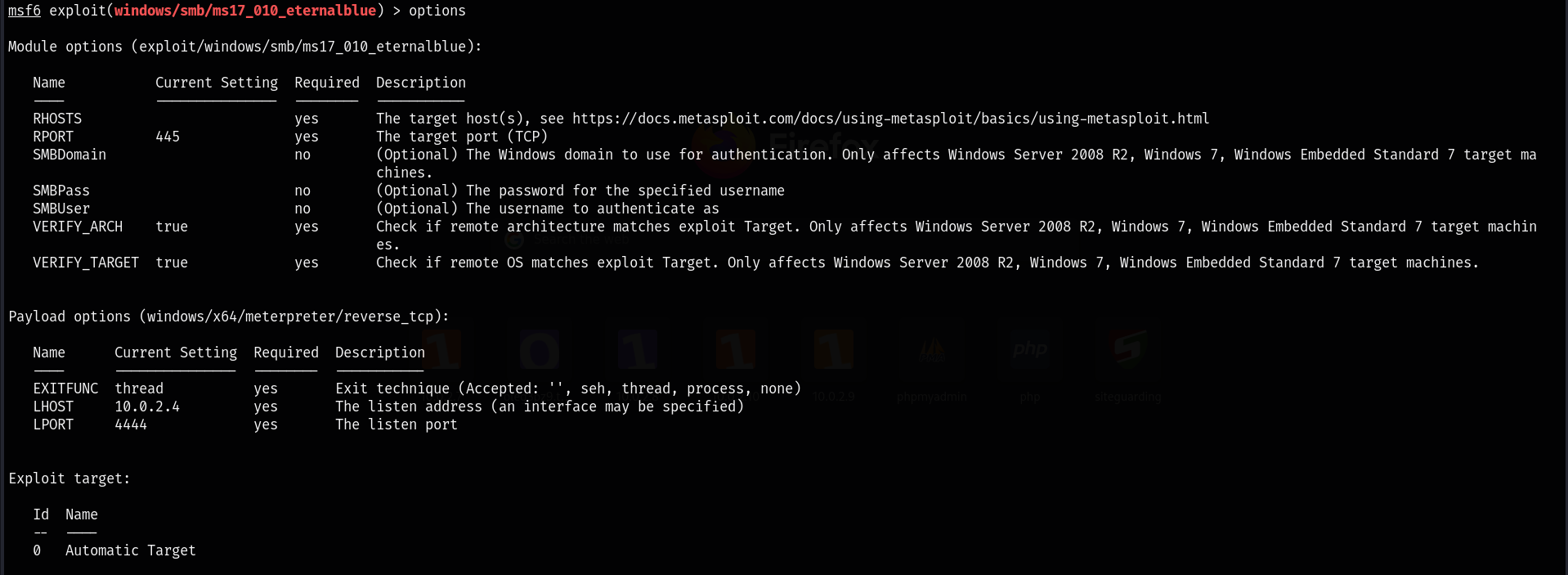
1. **Use the EternalBlue module:**

use exploit/windows/smb/ms17\_010\_eternalblue

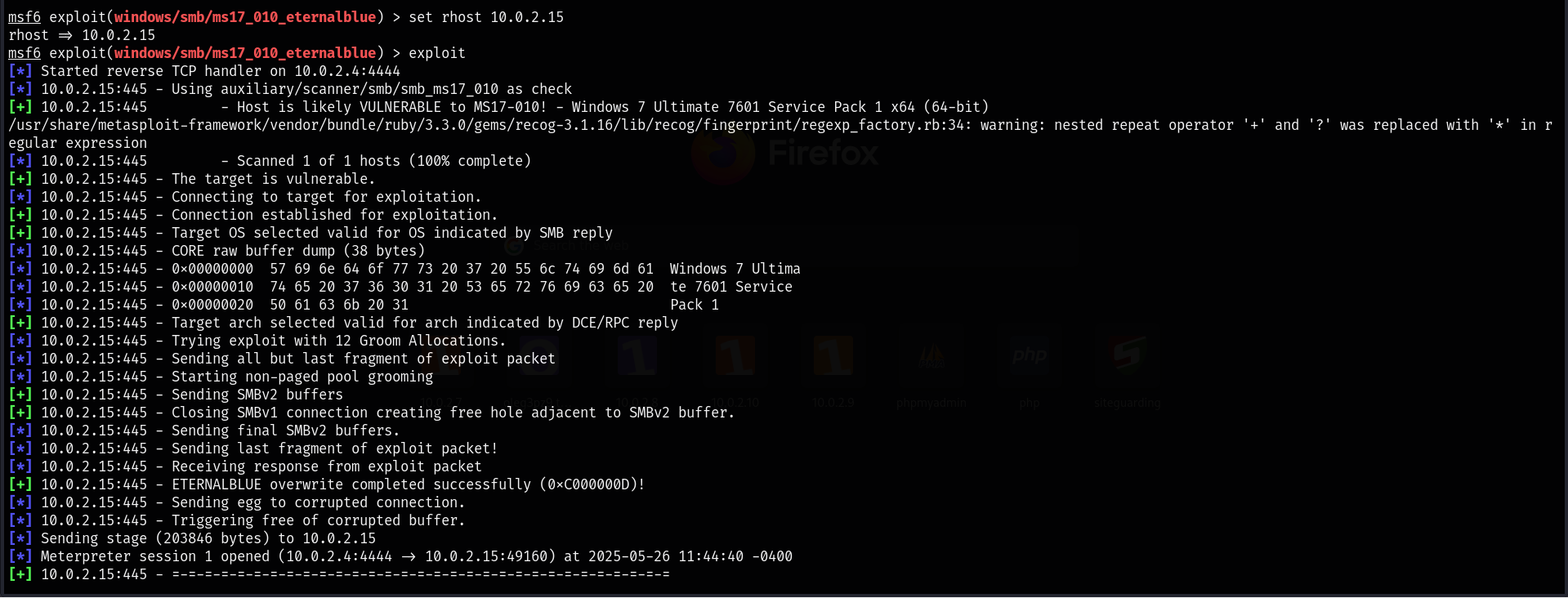




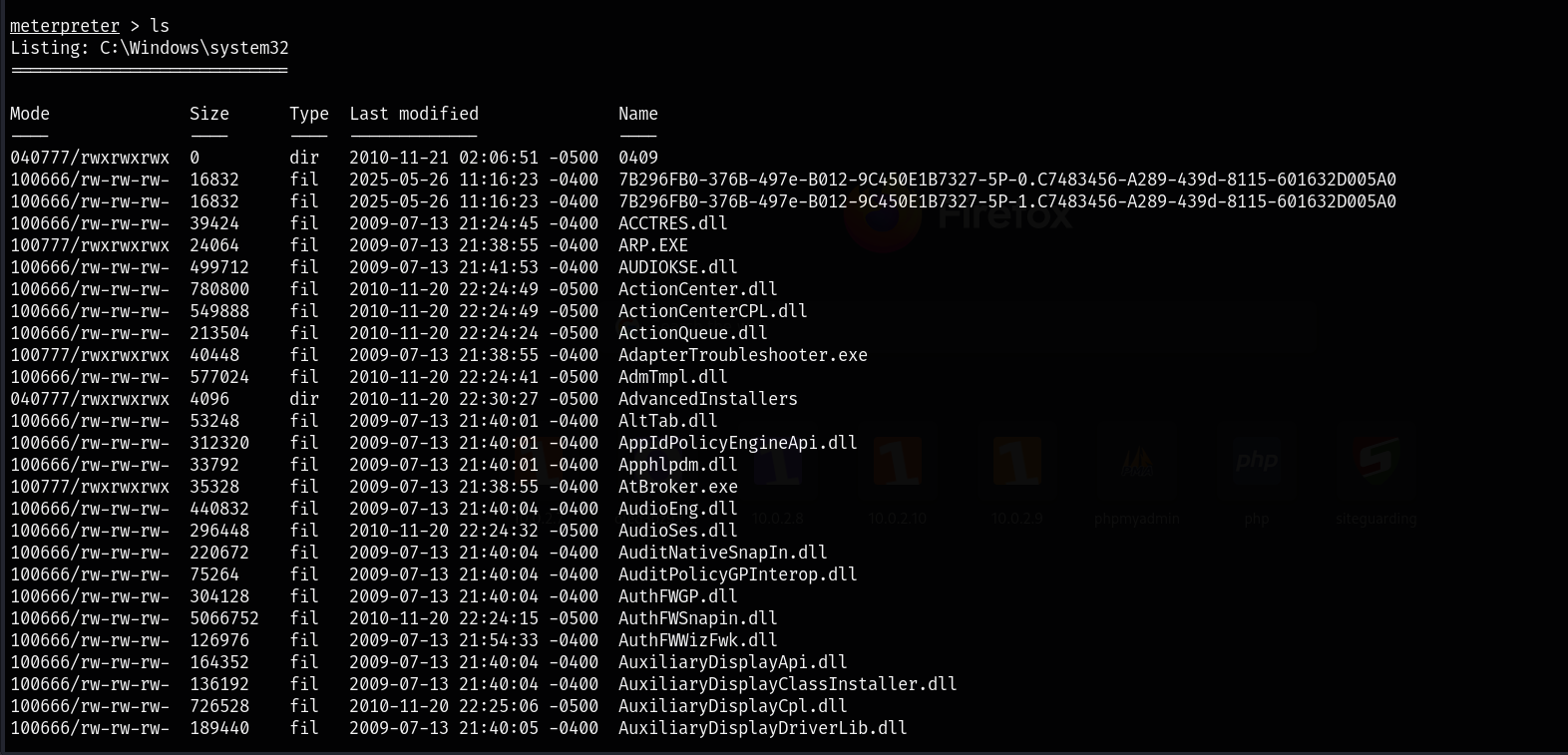
Lets use the exploit of eternal blue.



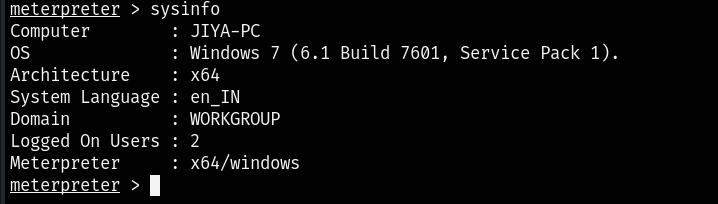
Set the rhost has the ip address of the victim.



We cracked it..







**Important Notes:**

* EternalBlue affects unpatched Windows 7, 8, Server 2008.
* Always verify legality and authorization before performing exploits.
* Consider using smb-check-vulns.nse for targeted checks without launching full exploitation.

**. Recommendations & Remediations**

To mitigate the risk associated with SMB exploitation, the following actions are strongly recommended:

**🔧 Patch and System Updates**

* **Apply the MS17-010 patch** available from Microsoft for CVE-2017-0144.
* Perform a **full system update** via Windows Update to resolve any other missing patches.

**Disable SMBv1 Protocol**

* SMBv1 is deprecated and insecure. Disable it via :

Set-SmbServerConfiguration -EnableSMB1Protocol $false

**Firewall and Network Segmentation**

* **Restrict inbound access** to ports 135, 139, and 445 using the host firewall.
* Only allow SMB traffic within trusted internal networks.
* Use VLANs or subnets to isolate high-value or legacy systems.

**Continuous Monitoring**

* Deploy **Host-based Intrusion Detection Systems (HIDS)** and monitor SMB traffic.
* Use Security Information and Event Management (SIEM) tools to detect exploit patterns.

**Additional Security Controls**

* Enforce **strong password policies** to reduce post-exploitation lateral movement.
* Enable **Windows Defender / Endpoint Protection** with real-time scanning.
* Regularly perform **vulnerability scans** with tools like Nessus or OpenVAS.

**Conclusion**

* This penetration test demonstrates a **full compromise** of the target Windows 7 VM due to an **unpatched critical vulnerability (MS17-010)**. The attacker was able to gain **system-level access** and perform post-exploitation activities, validating the severity of this issue.
* It is strongly advised that all remediation steps outlined above be followed immediately to mitigate this risk and prevent real-world exploitation.