Sections

Nmap Scan

Enumeration

Vulnerabilities

Exploitation

Privilege Escalation

Vulnerability Assessment

In this phase, we used the results from our Nmap and Enumeration steps to identify potential vulnerabilities.

- We discovered port **445 (SMB)** was open and the OS matched **Windows 7/Server 2008**.
- These findings were consistent with known vulnerabilities, including **MS17-010 (EternalBlue)**.
- We verified the vulnerability using **Rapid7's exploit database** and selected the Metasploit module `exploit/windows/smb/ms17_010_eternalblue`.
- This confirmed a critical remote code execution path was available with no authentication required.

Highlighted Nmap Vulnerability

Download Vulnerability Report (PDF)