Penetration Testing Report

Ethical Hacking – Black Box Simulation

📡 **Target Network:** `192.168.225.0/24`

💻 **Environment: Host-only Virtual Lab with Two Remote Virtual Machines**

📁 **Engagement Type: Black-Box Network Penetration Test**

Prepared by:-

Rohan Arora
B.Tech CSE (Cybersecurity) – SRM University
arorarohanx@gmail.com
https://www.linkedin.com/in/rohan-arora-x/

📘 Executive Summary

Project Title:
Penetration Testing Simulation – Ethical Hacking Assignment

Objective:
To simulate a real-world black-box penetration test on two virtual machines in a segmented 192.168.225.0/24 network and identify exploitable vulnerabilities without using direct console access.

Environment:

- 2 remote virtual machines (Linux + Windows 7)
- Host-only networking on VirtualBox
- Attacker machine: Kali Linux

Tools Used:

- 🛠️ Nmap – Port & service scanning
- 🛠️ Netdiscover – Live host identification
- 🛠️ SMBClient – File share enumeration

- 🛠️ Metasploit Framework – Exploitation (MS17-010)
- 🛠️ Kali Linux – Attack platform

Key Vulnerabilities Identified:

- MS17-010 (EternalBlue) — Remote Code Execution on Windows 7
- Anonymous SMB Share Access — Unauthenticated file exposure on CentOS

Exploitation Highlights:

- Gained reverse Meterpreter shell with SYSTEM privileges on the Windows host
- Extracted non-public files from Linux SMB shares using unauthenticated access

Risk & Impact:

- Demonstrated full system compromise risk due to outdated SMBv1 protocol
- Exposed data from misconfigured file shares poses privacy & integrity threats

Skills Demonstrated:

- Reconnaissance and enumeration
- Exploitation of known CVEs
- Report writing, risk analysis, and remediation planning
- Professional documentation

Deliverables:

- 📄 PDF report (this document)
- 📁 Saved Nmap scan outputs
- 📸 Screenshots of each step

Table of Contents

Introduction

This penetration test was conducted as part of an ethical hacking engagement involving two virtual machines in an isolated lab environment. Two virtual machines on a private network (192.168.225.0/24) were analyzed as remote targets. The objective was to identify vulnerabilities, exploit them ethically, and document the attack path without using direct console access.

Methodology

The penetration test was conducted using a structured and ethical approach, which is as follows :

Reconnaissance – Performed network scanning and service enumeration using Nmap to identify live hosts and open ports

Enumeration – Conducted in-depth analysis of exposed services (e.g., SMB) to identify potential misconfigurations and vulnerabilities

Vulnerability Assessment – Identifying known exploits applicable to discovered services.

Exploitation – Gaining unauthorized access via the EternalBlue (MS17-010) vulnerability. (Which was discovered in the windows)

Post-Exploitation – Conducted post-access analysis to identify system risks and potential data exposure vectors.

Reporting – Documenting every step, result, and recommended mitigation strategies.

Tools and Technologies Used:-

Nmap – for reconnaissance and service detection.
smbclient – for SMB enumeration.
Metasploit Framework – for exploiting MS17-010.
Kali Linux is the attacking platform.

Netdiscover - To identify live hosts on the network

VirtualBox - A Virtualization platform to host a lab environment

Key Achievements:-

- Successfully identified SMBv1 vulnerability on one target machine.
- Verified anonymous access to shared folders via SMB.
- Exploited the system using the EternalBlue vulnerability with Metasploit.
- Demonstrated the real-world impact of unpatched systems.

Scope of Engagement

The purpose of this penetration testing is to assess the security of two target machines within a controlled virtual network environment (192.168.225.0/24). This simulates a real-world black-box attack scenario where the attacker has no internal access and must rely solely on external remote exploitation techniques to compromise the target systems.

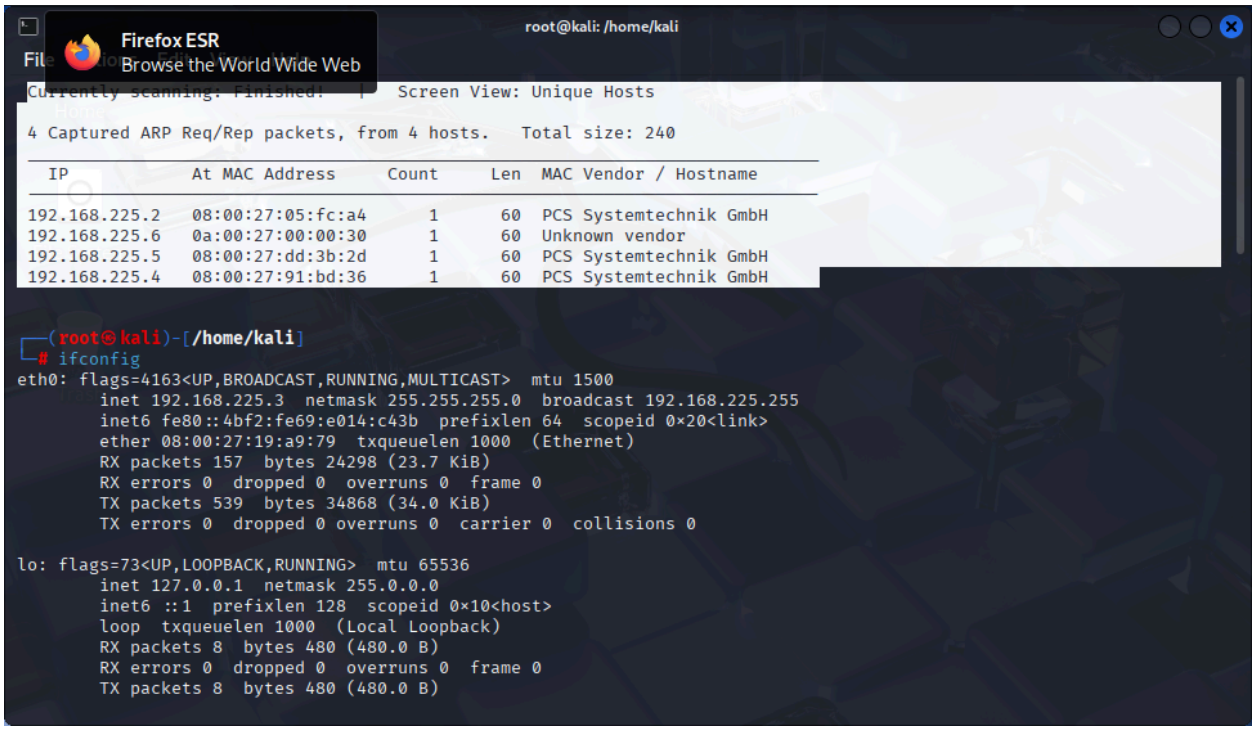
Parameter	Description
Network Range	192.168.225.0/24
Total Machines	2 Target Virtual Machines
Operating Systems	Windows (Version not initially disclosed) and Linux Server
Network Type	Host-only (Virtualized Lab)
Accessible Ports	To be discovered via the reconnaissance phase

Reconnaissance

The goal of this phase was to identify live hosts, detect open ports, detect services, and gather preliminary information about the target machines in the 192.168.225.0/24 lab network.

Host discovery was initiated using the following Netdiscover command: **netdiscover -r 192.168.255.0/24**

To discover all the hosts that are live and running

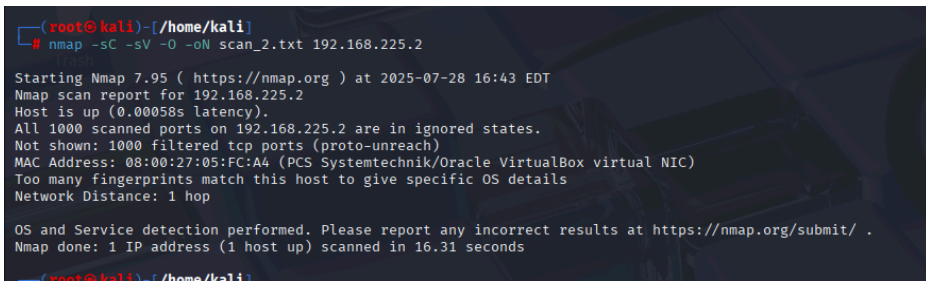


1.1 Host Discovery on the same network

The scan results revealed a total of four live hosts on the network; the attacking machine was identified as **192.168.255.3.**

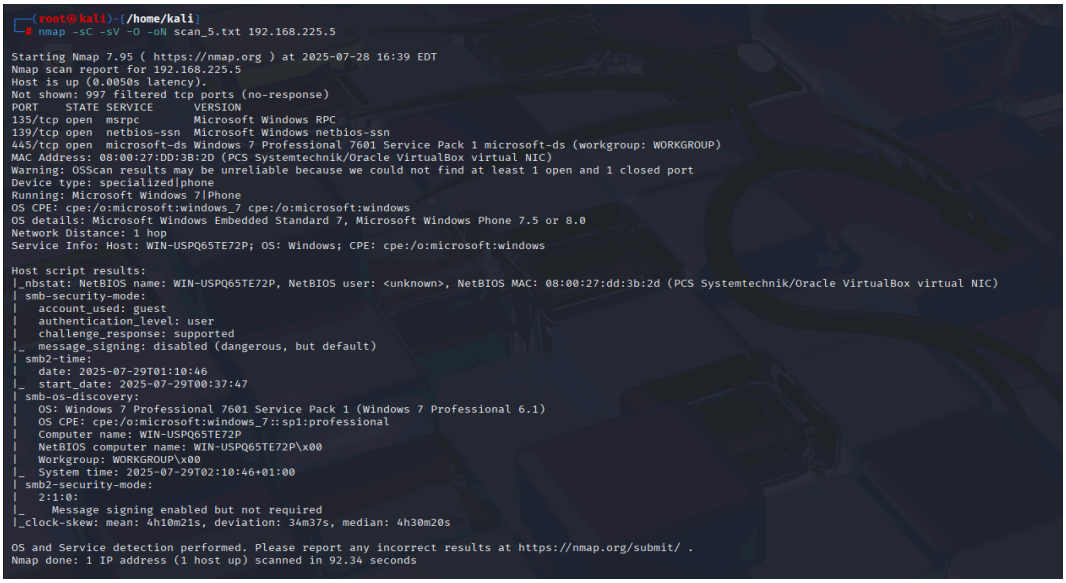
Subsequently, Nmap scans were conducted on all discovered IPs to enumerate services and identify OS-level fingerprints. Used these command of Nmap:-

nmap -sC -sV -O -oN scan_2.txt 192.168.255.2
nmap -sC -sV -O -oN scan_4.txt 192.168.255.4
nmap -sC -sV -O -oN scan_5.txt 192.168.255.5
nmap -sC -sV -O -oN scan_6.txt 192.168.255.6



1.2 Nmap scan of 192.168.255.2

1.3 Nmap scan of 192.168.255.4



1.4 Nmap scan of 192.168.255.5

1.5 Nmap scan of 192.168.255.6

These scans helped identify open ports, services, and operating system information. Based on this, **192.168.255.4** was identified as a Linux server and **192.168.255.5** as a Windows host.

Enumeration

The enumeration phase aims to extract detailed information about services running on the identified hosts from the reconnaissance phase. The goal is to uncover potential vulnerabilities, user accounts, shared resources, and misconfigurations that can be exploited during penetration testing.

Target 1: 192.168.255.4 (Linux Machine – CentOS)

Nmap Scan Results (From Screenshot of Nmap of 192.168.255.4)

Key Open Ports:

- 22/tcp – OpenSSH 7.4 (CentOS default)
- 80/tcp – Apache 2.4.6 (CentOS) with PHP/5.4.16
- 445/tcp – Samba SMB 4.8.3
- 139/tcp – NetBIOS Session Service

The presence of SMB services and guest access suggests a potential for unauthenticated enumeration and data leakage.

Target 2: 192.168.255.5 (Windows Machine)

Nmap Scan Results (From Screenshot of Nmap of 192.168.255.5)

Key Open Ports:

- 445/tcp – Microsoft SMB
- 139/tcp – NetBIOS Session Service
- 3389/tcp – RDP (Remote Desktop Protocol)

Target OS (Windows 7/Server 2008) is potentially vulnerable to **EternalBlue (MS17-010)**.

Additionally, SMB services on the Windows host may allow similar enumeration techniques as used against the Linux server.

Exploitation and Post-Exploitation

The exploitation phase aimed to gain unauthorized access to the identified vulnerable systems by leveraging the information discovered during reconnaissance and enumeration. Two systems were targeted:

- **192.168.255.5** — exploited using **EternalBlue (MS17-010)**
- **192.168.255.4** — exploited via **SMB enumeration**

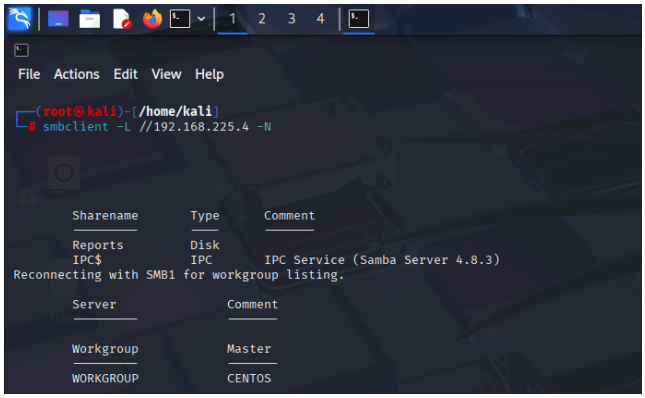
Target 1: 192.168.255.4 – Server (SMB Enumeration Exploit)

Vulnerability Identified

- **Open Ports:** 139, 445
- **Service:** Samba (SMB)
- **Shared Folders:** Enumerated successfully using smbclient

Enumeration was performed using the following smbclient command :-

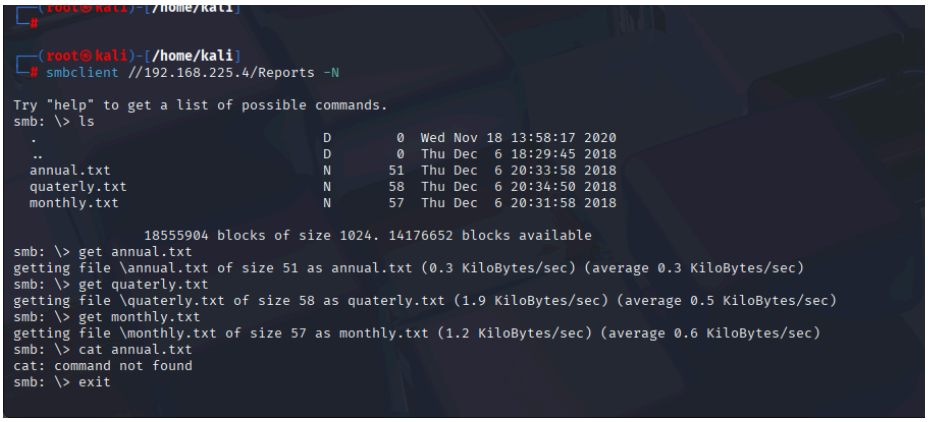
smbclient -L //192.168.255.4 -N



1.6 Using smbclient to enumerate

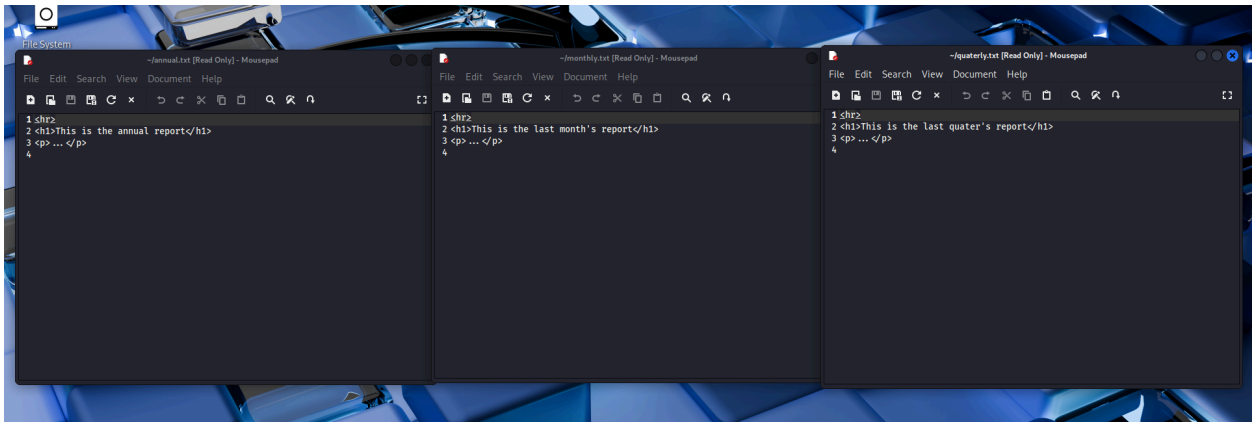
Execution of the above command revealed several shared directories available over SMB, shared in the above screenshot and the 'Reports' share was further enumerated using the same smbclient syntax :-

smbclient -L //192.168.255.4/Reports -N



1.7 Enumerating again with a Sharename

The enumeration revealed several shared files, potentially containing sensitive, non-public information. These files were accessible without authentication, posing a security risk (attached screenshot below):-



1.8 Text-Reports which were on the server

Target 2: 192.168.255.5 – Windows (EternalBlue Exploit)

Vulnerability Identified

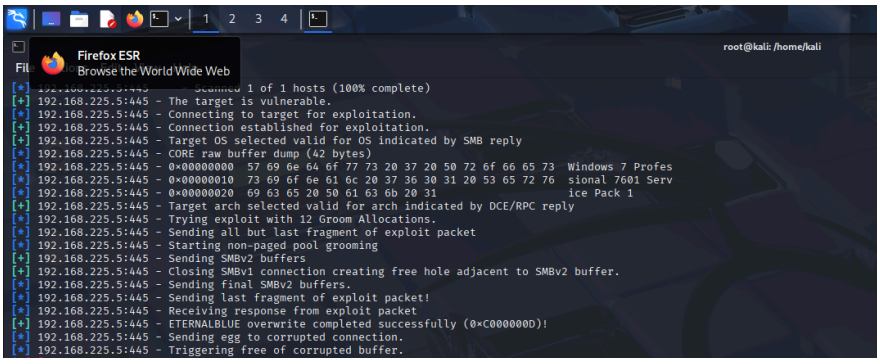
- Open Ports: 445, 139, 3389
- OS Detection: Windows 7 / Server 2008 R2
- Vulnerability: SMBv1 enabled

Based on these, the host was determined to be vulnerable to **MS17-010 (EternalBlue).**

The Metasploit Framework (**msfconsole**) was used to validate the presence of the MS17-010 vulnerability on the Windows target.

1.9 Starting the Metasploit and setting up the Target

In the msfconsole, I searched for smb_ms17_010 and used it then afterwards I set 192.168.255.5 as the RHOSTS, as it is the target IP, and he module confirmed the target system as vulnerable to MS17-010, enabling remote code execution through Metasploit . Subsequently, the target system was exploited using Metasploit's MS17-010 module and a reverse TCP payload and A reverse TCP payload (windows/x64/meterpreter/reverse_tcp) was configured to establish a remote Meterpreter session



2.0 Exploiting the windows 7 using metasploit

Risk Assessment and Impact Analysis

The purpose of this section is to assess the severity, likelihood, and impact of the vulnerabilities discovered and exploited during the penetration test. This analysis provides context for the business and technical risks associated with each compromised system and helps prioritize remediation efforts.

Target IP	Vulnerability	CVSS Score	Severity	Risk Level	Exploited Successfully
192.168.255.5	MS17-010 (EternalBlue)	9.8	**Critical**	**High**	Yes
192.168.255.4	Anonymous SMB Share Access	6.5	**Medium**	**Medium**	Yes

MS17-010 (EternalBlue) is a widely known Remote Code Execution vulnerability affecting SMBv1 on older Windows systems.

Successful exploitation of this vulnerability by an adversary may result in a production environment:

- All data on the system can be stolen or encrypted (e.g., ransomware)
- The system could potentially be used as a pivot point for a broader domain compromise
- Could result in data breaches, regulatory non-compliance, or reputational damage.

SMB shares are misconfigured to allow **anonymous access** without authentication. Read access to potentially sensitive files.

- Violates basic security principles (confidentiality, access control)
- May be used by an attacker to escalate privileges, impersonate users, or deliver malware

Recommendations and Remediation Plan

This section outlines a prioritized and practical remediation strategy for the vulnerabilities discovered during the penetration test. The goal is to help the organization reduce risk, prevent exploitation, and enhance its overall cybersecurity posture through patching, configuration changes, and policy enforcement.

Recommendations for Target: 192.168.255.4

Vulnerability: Anonymous SMB Share Access
Impact: Unauthorized file access, information disclosure

Recommendation	Description
Disable Anonymous SMB Access	Configure SMB to deny guest or anonymous logins completely.
Implement Access Controls	Use NTFS permissions and user-level authentication for shared access.
Sanitize SMB Shares	Audit and remove unnecessary or sensitive files from publicly accessible directories.

Recommendations for Target: 192.168.255.5

Vulnerability: MS17-010 (EternalBlue)

Impact: Full remote code execution with SYSTEM privileges

Recommendation	Description
Apply Critical Patch (MS17-010)	Install the official Microsoft patch for MS17-010 to eliminate the flaw.
Disable SMBv1 Protocol	Disable SMBv1 if not required. Prefer SMBv2/3 for secure file sharing.
Restrict Port 445 Access	Block SMB ports (TCP 445) at the firewall level, especially from external networks.
Enable Host-Based Firewalls	Enforce Windows Firewall to allow only required inbound/outbound communication.
Conduct Routine Vulnerability Scans	Schedule regular scans to detect missing patches and outdated software.

Remediation Prioritization Table

Priority	Target IP	Vulnerability	Recommended Fix	Deadline
High	192.168.255.5	EternalBlue (MS17-010)	Patch MS17-010, disable SMBv1	Within 24 hours
Medium	192.168.255.4	Anonymous SMB Access	Reconfigure SMB shares, apply ACLs	Within 3 days

The penetration test successfully identified critical and medium-severity vulnerabilities across two hosts. These weaknesses are exploitable in real-world attack scenarios and could lead to full system compromise or sensitive data leakage.

Timely remediation, combined with improved system hardening and security monitoring, will significantly reduce the organization's exposure to threats and align its defenses with industry standards.

Conclusions

This ethical hacking engagement involved a comprehensive penetration test of two systems in a controlled /24 lab network, the assessment simulated real-world attack scenarios targeting two hosts—192.168.255.5 (Windows 7 Professional) and 192.168.255.4 (CentOS Linux)—within a segmented /24 lab network, simulating real-world attack scenarios focused on vulnerability identification, exploitation, and post-exploitation analysis.

The Windows 7 target was confirmed to be vulnerable to MS17-010 (EternalBlue)—a critical SMBv1 flaw (CVE-2017-0143) that enables remote code execution. Metasploit was used to launch multiple exploitation attempts, which confirmed the system's susceptibility to the EternalBlue vulnerability

In parallel, the Linux target (192.168.255.4) was evaluated through SMB enumeration and null session access, revealing exposed file shares without authentication. Without authentication, the server exposed readable shares, allowing access to confidential files via smbclient. This vulnerability allowed passive data extraction without credentialed access.

Security Recommendations

- Patch MS17-010 immediately (Windows KB4013389) and disable SMBv1 across endpoints

- On Linux systems, enforce access controls on SMB shares and disable guest/null sessions