

WinRM Service

```
Enter-PSSession -ComputerName 192.168.56.103 -Credential theshyhat
```

The Windows Remote Management (WinRM) service provides PowerShell terminal access to a Windows server

WinRM Service

```
Enter-PSSession -ComputerName 192.168.56.103 -Credential theshyhat
```

WinRM access is usually limited to administrator-level users, but it's not guaranteed

WinRM Service

```
└─$ evil-winrm -i 192.168.56.115 -u "nica" -p "password"

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby
ction_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: http
rs/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\nica\Documents> 
```

The typical method of access WinRM is through a PowerShell terminal, but Linux users can use the Evil-WinRM program to interact with the service

Privilege Escalation

SeImpersonate Privilege

```
Nombre de privilegio
=====
SeAssignPrimaryTokenPrivilege
SeIncreaseQuotaPrivilege
SeAuditPrivilege
SeChangeNotifyPrivilege
SeImpersonatePrivilege
SeCreateGlobalPrivilege
```

The SeImpersonate privilege is a feature which allows a user to perform commands in the context of other users

Privilege Escalation

SelImpersonate Privilege

```
c:\windows\system32\inetsrv>whoami  
whoami  
iis apppool\defaultapppool
```

This privilege is typically associated with service accounts, like IIS, SQL Server, and with Administrator accounts

Privilege Escalation

SeImpersonate Privilege

```
Nombre de privilegio
=====
SeAssignPrimaryTokenPrivilege
SeIncreaseQuotaPrivilege
SeAuditPrivilege
SeChangeNotifyPrivilege
SeImpersonatePrivilege
SeCreateGlobalPrivilege
```

Using SeImpersonate, attackers can elevate privileges to SYSTEM or Administrator level, either through Token Theft and / or Named Pipes

Selmpersonate – Potato Exploit

The Potato-family of Windows exploits all leverage the Selmpersonate privilege in different ways to achieve elevated access on Windows targets



Potato Exploit – JuicyPotato

Which Potato exploit to use on a target largely depends on the version of Windows being used. In this case, we'll be using the Juicy Potato variant

