

Description from ATT&CK

Adversaries may use [Valid Accounts](<https://attack.mitre.org/techniques/T1078>) to interact with remote systems using Windows Remote Management (WinRM). The adversary may then perform actions as the logged-on user.

WinRM is the name of both a Windows service and a protocol that allows a user to interact with a remote system (e.g., run an executable, modify the Registry, modify services).(Citation: Microsoft WinRM) It may be called with the `winrm` command or by any number of programs such as PowerShell.(Citation: Jacobsen 2014) WinRM can be used as a method of remotely interacting with [Windows Management Instrumentation](#). (Citation: MSDN WMI)

Atomic Tests

[atomic-red-team](#) / [atomics](#) / [T1021.006](#) / [T1021.006.md](#)

[↑ Top](#)

Preview

Code

Blame

139 lines (72 loc) · 3.64 KB

Raw



- Atomic Test #3 - WinRM Access with Evil-WinRM

Atomic Test #1 - Enable Windows Remote Management

Powershell Enable WinRM

Upon successful execution, powershell will "Enable-PSRemoting" allowing for remote PS access.

Supported Platforms: Windows

auto_generated_guid: 9059e8de-3d7d-4954-a322-46161880b9cf

























Attack Commands: Run with `powershell` ! Elevation Required (e.g. root or admin)

Enable-PSRemoting -Force



Atomic Test #2 - Invoke-Command

Execute Invoke-command on remote host.

- >  T1016
 - >  T1018
 - >  T1020
 - >  T1021.001
 - >  T1021.002
 - >  T1021.003
 - ✓  T1021.006
 -  T1021.006.md
 -  T1021.006.yaml
 - >  T1027.001
 - >  T1027.002
 - >  T1027.004
 - >  T1027
 - >  T1030
 - >  T1033
 - >  T1036.003
 - >  T1036.004
 - >  T1036.005
 - >  T1036.006
 - >  T1036
 - >  T1037.001
 - >  T1037.002
 - >  T1037.004
 - >  T1037.005

Upon successful execution, powershell will execute ipconfig on localhost using `invoke-command`.

Supported Platforms: Windows

auto_generated_guid: 5295bd61-bd7e-4744-9d52-85962a4cf2d6

Inputs:

Name	Description	Type	Default Value
host_name	Remote Windows Host Name	String	localhost
remote_command	Command to execute on remote Host	String	ipconfig

Attack Commands: Run with powershell!

```
invoke-command -ComputerName #{host_name} -scriptblock {#{remote_command}}
```

Atomic Test #3 - WinRM Access with Evil-WinRM

An adversary may attempt to use Evil-WinRM with a valid account to interact with remote systems that have WinRM enabled

Supported Platforms: Windows

auto_generated_guid: efe86d95-44c4-4509-ae42-7bfd9d1f5b3d

Inputs:

Name	Description	Type	Default Value
user_name	Username	String	Domain\Administrator
destination_address	Remote Host IP or Hostname	String	Target
password	Password	String	P@ssw0rd1

Attack Commands: Run with powershell! Elevation Required (e.g. root or admin)

```
evil-winrm -i #{destination_address} -u #{user_name} -p #{password}
```

Dependencies: Run with `powershell`!

Description: Computer must have Ruby Installed

Check Prereq Commands:

```
try {if (ruby -v) {exit 0} else {exit 1}} catch {exit 1}
```

Get Prereq Commands:

```
Invoke-WebRequest -OutFile $env:Temp\rubyinstaller-2.7.1-1-x64.exe http
$file1= $env:Temp + "\rubyinstaller-2.7.1-1-x64.exe"
Start-Process $file1 /S;
```

Description: Computer must have Evil-WinRM installed

Check Prereq Commands:

```
try {if (evil-winrm -h) {exit 0} else {exit 1}} catch {exit 1}
```



Get Prereq Commands:

```
gem install evil-winrm
```

