

# T1021.006 - Windows Remote Management

# **Description from ATT&CK**

Adversaries may use [Valid Accounts](<a href="https://attack.mitre.org/techniques/T1078">https://attack.mitre.org/techniques/T1078</a>) 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 Test #1 Enable Windows Remote Management
- Atomic Test #2 Invoke-Command
- 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

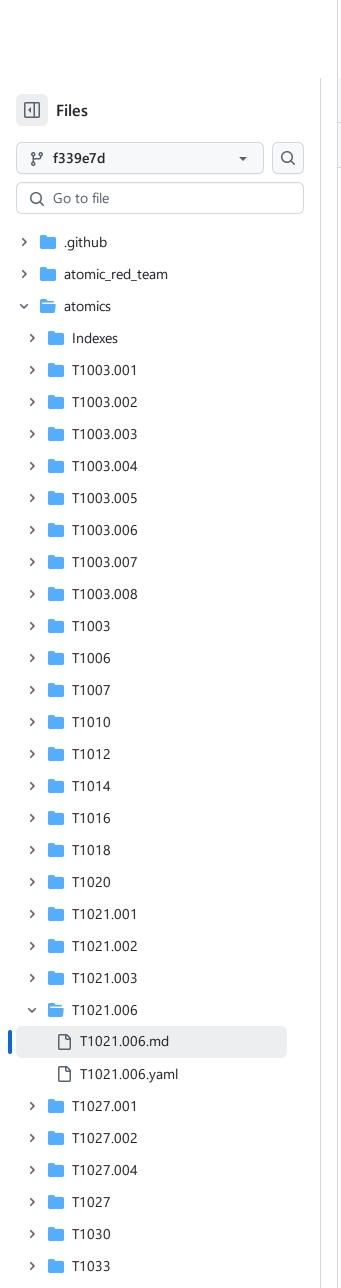
auto\_generated\_guid: 9059e8de-3d7d-4954-a322-46161880b9cf

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.



T1036.003

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	Туре	Default Value
host_name	Remote Windows Host Name	String	localhost

atomic-red-team / atomics / T1021.006 / T1021.006.md

Preview Code | Blame 139 lines (72 loc) ⋅ 3.64 KB Raw □ ⋅ □ ⋅ □ ⋅ □

 $invoke-command - Computer Name \ \#\{host\_name\} - scriptblock \ \{\#\{remote\_command \ \Box \ \Box \ Barrier \} \}$ 

↑ Top

Q

Q

### 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	Туре	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:** 



