

📁

redcanaryco / atomic-red-team

Public

🔔

Notifications

🍴

Fork2.8k

★

Star9.7k

<>

Code

🔗

Issues6

🔗

Pull requests5

▶️

Actions

📖

Wiki

🛡️

Security

📊

Insights

atomic-red-team / atomics / T1021.001 / T1021.001.md

⌵

🐙

Atomic Red Team doc generat...Generated docs from job=generate-d...819934c · 2 years ago

🕒

History

PreviewCodeBlame202 lines (115 loc) · 6.11 KB

Raw📄⬇️☰

T1021.001 - Remote Desktop Protocol

Description from ATT&CK

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to log into a computer using the Remote Desktop Protocol (RDP). The adversary may then perform actions as the logged-on user.

Remote desktop is a common feature in operating systems. It allows a user to log into an interactive session with a system desktop graphical user interface on a remote system. Microsoft refers to its implementation of the Remote Desktop Protocol (RDP) as Remote Desktop Services (RDS).(Citation: TechNet Remote Desktop Services)

Adversaries may connect to a remote system over RDP/RDS to expand access if the service is enabled and allows access to accounts with known credentials. Adversaries will likely use Credential Access techniques to acquire credentials to use with RDP. Adversaries may also use RDP in conjunction with the [Accessibility Features](#) or [Terminal Services DLL](#) for Persistence.(Citation: Alperovitch Malware)

Atomic Tests

- [Atomic Test #1 - RDP to DomainController](#)
- [Atomic Test #2 - RDP to Server](#)
- [Atomic Test #3 - Changing RDP Port to Non Standard Port via Powershell](#)
- [Atomic Test #4 - Changing RDP Port to Non Standard Port via Command_Prompt](#)

Atomic Test #1 - RDP to DomainController

Attempt an RDP session via Remote Desktop Application to a DomainController.

Supported Platforms: Windows

auto_generated_guid: 355d4632-8cb9-449d-91ce-b566d0253d3e

Inputs:

Name	Description	Type	Default Value
logonserver	ComputerName argument default %logonserver%	String	\$ENV:logonserver.TrimStart("\")
domain	domain argument default %USERDOMAIN%	String	\$Env:USERDOMAIN

Files

f339e7d

🔍

Go to file

> .github

> atomic_red_team

> atomics

> Indexes

> T1003.001

> T1003.002

> T1003.003

> T1003.004

> T1003.005

> T1003.006

> T1003.007

> T1003.008

> T1003

> T1006

> T1007

> T1010

> T1012

> T1014

> T1016

> T1018

> T1020

> T1021.001

📄 T1021.001.md

📄 T1021.001.yaml

> T1021.002

> T1021.003

> T1021.006

> 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

username	Username argument default %username%	String	\$ENV:USERNAME
password	Password	String	1password2!

Attack Commands: Run with powershell!

```
$Server=#{logonserver}
$User = Join-Path #{domain} #{username}
$Password=#{password}"
cmdkey /generic:TERMSRV/$Server /user:$User /pass:$Password
mstsc /v:$Server
echo "RDP connection established"
```



Cleanup Commands:

```
$p=Tasklist /svc /fi "IMAGENAME eq mstsc.exe" /fo csv | convertfrom-csv
if(-not ([string]::IsNullOrEmpty($p.PID))) { Stop-Process -Id $p.PID }
```



Dependencies: Run with powershell!

Description: Computer must be domain joined

Check Prereq Commands:

```
if((Get-CIMInstance -Class Win32_ComputerSystem).PartOfDomain) { exit 0}
```



Get Prereq Commands:

```
Write-Host Joining this computer to a domain must be done manually
```



Atomic Test #2 - RDP to Server

Attempt an RDP session via Remote Desktop Application over Powershell

Supported Platforms: Windows

auto_generated_guid: 7382a43e-f19c-46be-8f09-5c63af7d3e2b

Inputs:

Name	Description	Type	Default Value
logonserver	ComputerName	String	WIN-DC
username	Username	String	Administrator
password	Password	String	1password2!

Attack Commands: Run with powershell!

```
$Server=#{logonserver}"
$User=#{username}"
$Password=#{password}"
cmdkey /generic:TERMSRV/$Server /user:$User /pass:$Password
mstsc /v:$Server
echo "RDP connection established"
```



Cleanup Commands:

```
$p=Tasklist /svc /fi "IMAGENAME eq mstsc.exe" /fo csv | convertfrom-csv
if(-not ([string]::IsNullOrEmpty($p.PID))) { Stop-Process -Id $p.PID }
```



Atomic Test #3 - Changing RDP Port to Non Standard Port via Powershell

Changing RDP Port to Non Standard Port via Remote Desktop Application over Powershell

Supported Platforms: Windows

auto_generated_guid: 2f840dd4-8a2e-4f44-beb3-6b2399ea3771

Inputs:

Name	Description	Type	Default Value
OLD_Remote_Port	Default RDP Listening Port	String	3389
NEW_Remote_Port	New RDP Listening Port	String	4489

Attack Commands: Run with powershell !

```
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal :
New-NetFirewallRule -DisplayName 'RDPPORTLatest-TCP-In' -Profile 'Public
```



Cleanup Commands:

```
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal :
Remove-NetFirewallRule -DisplayName "RDPPORTLatest-TCP-In" -ErrorAction
```



Atomic Test #4 - Changing RDP Port to Non Standard Port via Command_Prompt

Changing RDP Port to Non Standard Port via Command_Prompt

Supported Platforms: Windows

auto_generated_guid: 74ace21e-a31c-4f7d-b540-53e4eb6d1f73

Inputs:

Name	Description	Type	Default Value
OLD_Remote_Port	Default RDP Listening Port	String	3389
NEW_Remote_Port	New RDP Listening Port	String	4489

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

```
reg add "HKLM\System\CurrentControlSet\Control\Terminal Server\WinStatio
netsh advfirewall firewall add rule name="RDPPORTLatest-TCP-In" dir=in a
```



Cleanup Commands:

```
reg add "HKLM\System\CurrentControlSet\Control\Terminal Server\WinStatio
```



```
netsh advfirewall firewall delete rule name="RDPPORTLatest-TCP-In" >nul .
```