T1021.002 - SMB/Windows Admin Shares

Description from ATT&CK

> Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to interact with a remote network share using Server Message Block (SMB). The adversary may then perform actions as the logged-on user.
> SMB is a file, printer, and serial port sharing protocol for Windows machines on the same network or domain. Adversaries may use SMB to interact with file shares, allowing them to move laterally throughout a network. Linux and macOS implementations of SMB typically use Samba.
>
> Windows systems have hidden network shares that are accessible only to administrators and provide the ability for remote file copy and other administrative functions. Example network shares include `C$`, `ADMIN$`, and `IPC$`. Adversaries may use this technique in conjunction with administrator-level Valid Accounts to remotely access a networked system over SMB,(Citation: Wikipedia Server Message Block) to interact with systems using remote procedure calls (RPCs),(Citation: TechNet RPC) transfer files, and run transferred binaries through remote Execution. Example execution techniques that rely on authenticated sessions over SMB/RPC are Scheduled Task/Job, Service Execution, and Windows Management Instrumentation. Adversaries can also use NTLM hashes to access administrator shares on systems with Pass the Hash and certain configuration and patch levels.(Citation: Microsoft Admin Shares)

Atomic Tests

- Atomic Test #1 - Map admin share
- Atomic Test #2 - Map Admin Share PowerShell
- Atomic Test #3 - Copy and Execute File with PsExec
- Atomic Test #4 - Execute command writing output to local Admin Share

Atomic Test #1 - Map admin share

Connecting To Remote Shares

Supported Platforms: Windows

auto_generated_guid: 3386975b-367a-4fbb-9d77-4dcf3639ffd3

Inputs:

Name	Description	Type	Default Value
user_name	Username	String	DOMAIN\Administrator
share_name	Examples C$, IPC$, Admin$	String	C$
password	Password	String	P@ssw0rd1
computer_name	Target Computer Name	String	Target

Attack Commands: Run with `command_prompt`!

```
cmd.exe /c "net use \\#{computer_name}\#{share_name} #{password} /u:#{us
```

Atomic Test #2 - Map Admin Share PowerShell

Map Admin share utilizing PowerShell

Supported Platforms: Windows

auto_generated_guid: 514e9cd7-9207-4882-98b1-c8f791bae3c5

Inputs:

Name	Description	Type	Default Value
share_name	Examples C$, IPC$, Admin$	String	C$
map_name	Mapped Drive Letter	String	g
computer_name	Target Computer Name	String	Target

Attack Commands: Run with `powershell`!

```
New-PSDrive -name #{map_name} -psprovider filesystem -root \\#{computer_
```

Atomic Test #3 - Copy and Execute File with PsExec

Copies a file to a remote host and executes it using PsExec. Requires the download of PsExec from https://docs.microsoft.com/en-us/sysinternals/downloads/psexec.

Supported Platforms: Windows

auto_generated_guid: 0eb03d41-79e4-4393-8e57-6344856be1cf

Inputs:

Name	Description	Type	Default Value
command_path	File to copy and execute	Path	C:\Windows\System32\cmd.exe
remote_host	Remote computer to receive the copy and execute the file	String	\\localhost
psexec_exe	Path to PsExec	string	C:\PSTools\PsExec.exe

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

```
#{psexec_exe} #{remote_host} -accepteula -c #{command_path}
```

Dependencies: Run with `powershell`!

Description: PsExec tool from Sysinternals must exist on disk at specified location (#{psexec_exe})

Get Prereq Commands:

```
Invoke-WebRequest "https://download.sysinternals.com/files/PSTools.zip"
Expand-Archive $env:TEMP\PsTools.zip $env:TEMP\PsTools -Force
New-Item -ItemType Directory (Split-Path "#{psexec_exe}") -Force | Out-N
Copy-Item $env:TEMP\PsTools\PsExec.exe "#{psexec_exe}" -Force
```

Atomic Test #4 - Execute command writing output to local Admin Share

Executes a command, writing the output to a local Admin Share. This technique is used by post-exploitation frameworks.

Supported Platforms: Windows

auto_generated_guid: d41aaab5-bdfe-431d-a3d5-c29e9136ff46

Inputs:

Name	Description	Type	Default Value
output_file	Remote computer to receive the copy and execute the file	String	output.txt
command_to_execute	Command to execute for output.	String	hostname

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

```
cmd.exe /Q /c #{command_to_execute} 1> \\127.0.0.1\ADMIN$\#{output_file}
```