

Ex080

Joshua Main-Smith

2020-10-21

Contents

Technical Report	2
Finding: Default Router Credentials Used	2
Risk Assessment	2
Vulnerability Description	2
Mitigation or Resolution Strategy	2
Attack Narrative	2
Accessing PfSense	2
Accessing Herd	3
KEY	4
Zoom Links	4

Technical Report

Finding: Default Router Credentials Used

Risk Assessment

With the PfSense router containing the default login credentials and it being open to the wide area network gives an attacker control over packets passing through the router.

Vulnerability Description

The company router uses the default login credentials and is reachable to those outside the network.

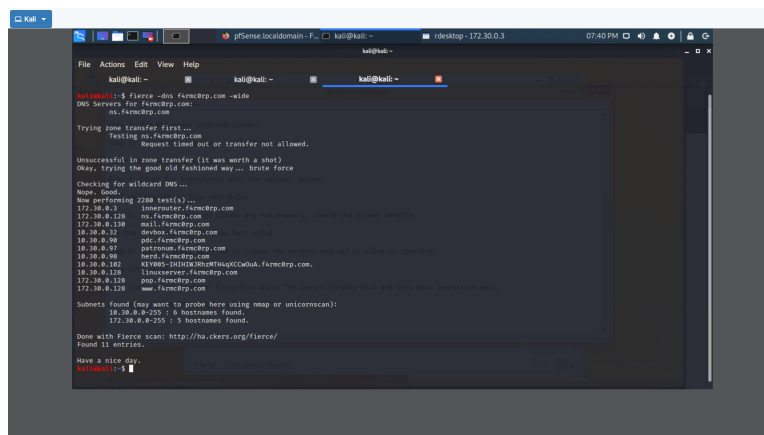
Mitigation or Resolution Strategy

This issue can be resolved by changing the default login credentials and removing the router from the WAN to LAN.

Attack Narrative

Accessing PfSense

As had been mentioned previously we scanned the F4rmC0rp network to find potential hosts that may be providing web servers with the command **fierce -dns f4rmc0rp.com -wide**.



```
kali@kali:~$ fierce -dns f4rmc0rp.com -wide
DNS Servers for f4rmc0rp.com:
ms.f4rmc0rp.com

Trying some transfer first...
Testing ms.f4rmc0rp.com
Request timed out or transfer not allowed.
Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
None found.
Now performing 2208 test(s)...
172.30.0.2 jameson.f4rmc0rp.com
172.30.0.128 ms.f4rmc0rp.com
172.30.0.128 mail.f4rmc0rp.com
18.30.0.32 devbox.f4rmc0rp.com
18.30.0.97 patronus.f4rmc0rp.com
18.30.0.98 herb.f4rmc0rp.com
18.30.0.182 XIV805-1H1H4W307H4qKCuab.f4rmc0rp.com
18.30.0.128 linuxserver.f4rmc0rp.com
172.30.0.128 pnp.f4rmc0rp.com
172.30.0.128 ms.f4rmc0rp.com

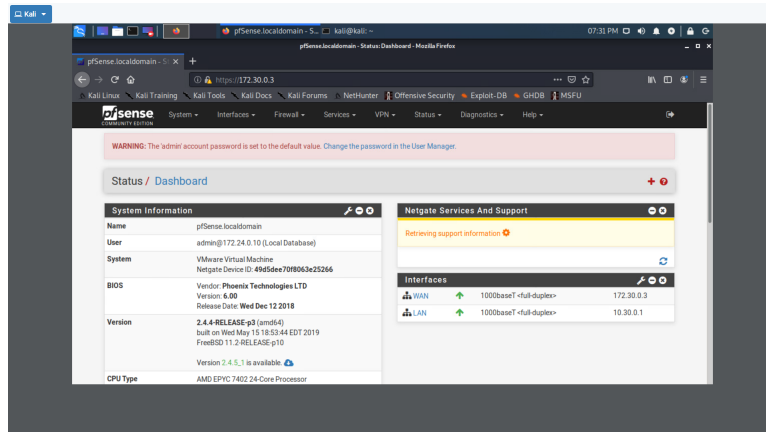
Subnets found (you want to probe here using nmap or unicornscan):
18.30.0.0-255 : 6 hostnames found.
172.30.0.0-255 : 3 hostnames found.

Done with Fierce scan: http://ho.ckers.org/fierce/
Found 11 entries.

Have a nice day.
exitcode: 0
```

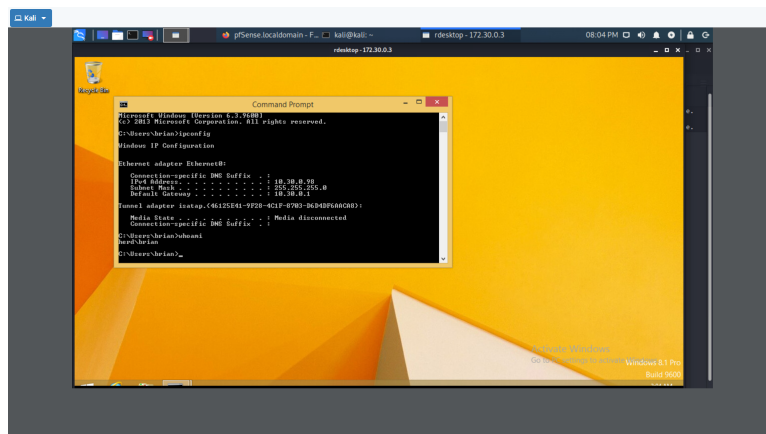
Several hosts with internal IP addresses were found that are directly inaccessible. Additionally, we performed an nmap scan of the ISP network to see if the router is accessible on the WAN. Using the Linux command **nmap -sV 172.30.0.0/24** we found a machine named **innerrouter.f4rmc0rp.com** located at

172.30.0.3. This device only had one port open, **443** running an **ssl/http** service of **nginx**. We successfully accessed the PfSense router at **https://172.30.0.3** and we were able to login with the default credentials.



Accessing Herd

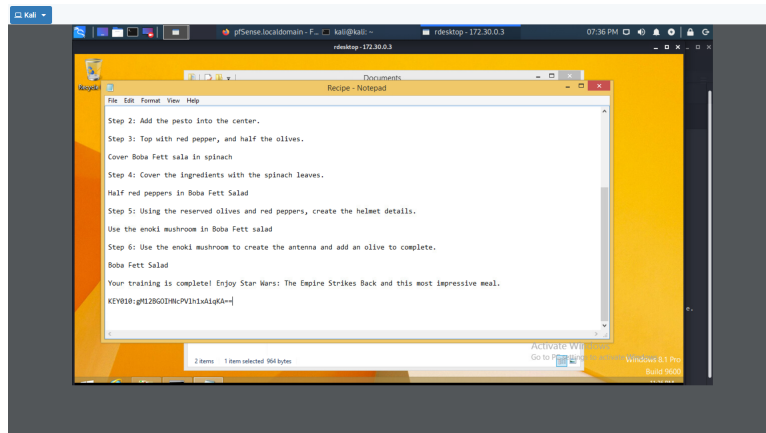
From here, we were able to set up a port forward to an internal machine and possibly connect if the hosts port is open. We found that MS RDP is open on **herd.f4rmc0rp.com** (10.30.0.98). We were then able to set up a port forward to the default port of MS RDP (3389) by going to **Firewall -> NAT** then clicking **Add**. We then set the destination and redirect ports to **3389** and the redirect IP address to **10.30.0.98**. After saving this configuration, we performed an nmap scan on **172.30.0.3** and found that port 3389 was open. So, we were then able to connect to port 3389 using **rdesktop** from our attack box. After issuing the command **rdesktop -g95% 172.30.0.3**, we were able to connect to the herd login screen.



From previous reconnaissance, we were able to find what appeared to be a password under Brian's account from the **www** host. Using this under Brian's username granted us access to Brian's account.

KEY

While looking around in Brian's Documents folder, we discovered a key.



The value of this key is **KEY010:gM12BGOIHNCpVlh1xAiqKA==**.

Zoom Links

[October 16, 2020](#)