Ex080 - ThroughTheGate

Simon Tobon

2021-07-08

Contents

Technical Report

Introduction

For this exercise, we were tasked to exploit infrastructure misconfigurations, and connect to a desktop on the herd.f4rmc0rp.com machine via Microsoft Remote Desktop.

Finding: Description of finding

Risk Rating

There are some risks that come with RDP. If the connection is not properly secured it is fairly easy to inject ransomware.

Vulnerability Description

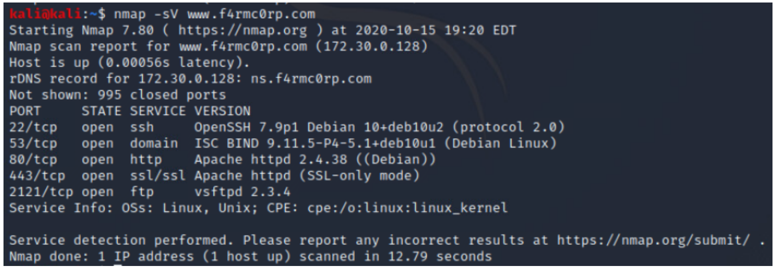
- pfSense - Defaults
  - If the admin username and password are not changed from the defaults, i.e., admin/pfsense then it is VERY easy for someone to log in to your host.

Mitigation or Resolution Strategy

This kind of exploit can be mitigated by changing the default login credentials for pfsense on the router. This will make it much harder for someone to login and have full control over the system. It can also be mitigated by blocking traffic on port 3389 with a firewall.

Attack Narrative

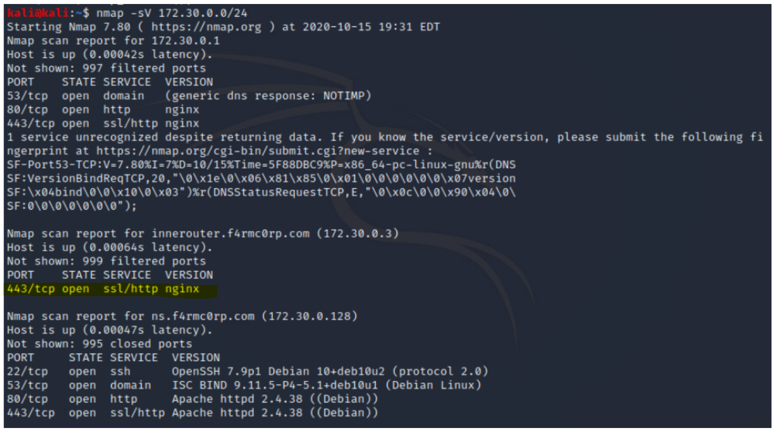
To begin with I ran a nmap version scan on f4rmc0rp.com. **nmap -sV www.f4rmc0rp.com** This yielded the following:



```
kali@kali:~$ nmap -sV www.f4rmc0rp.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-15 19:20 EDT
Nmap scan report for www.f4rmc0rp.com (172.30.0.128)
Host is up (0.00056s latency).
rDNS record for 172.30.0.128: ns.f4rmc0rp.com
Not shown: 995 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
53/tcp   open  domain  ISC BIND 9.11.5-P4-5.1+deb10u1 (Debian Linux)
80/tcp   open  http    Apache httpd 2.4.38 ((Debian))
443/tcp  open  ssl/ssl Apache httpd (SSL-only mode)
2121/tcp open  ftp     vsftpd 2.3.4
Service Info: OSs: Linux, Unix; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.79 seconds
```

This shows that www.f4rmc0rp.com address is 172.30.0.128. Using this information I then ran the following **nmap -sV 172.30.0.0/24** to find a host that was providing a web service.



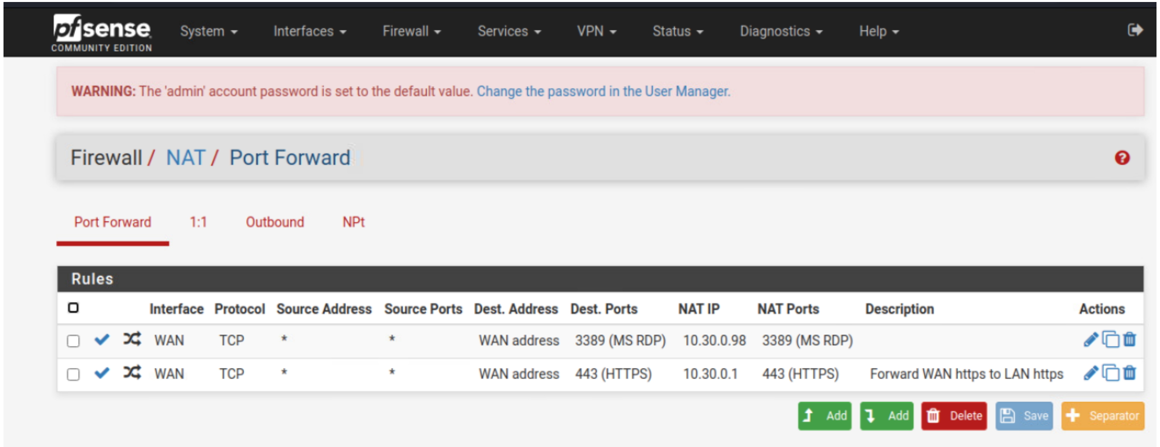
```
kali@kali:~$ nmap -sV 172.30.0.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-15 19:31 EDT
Nmap scan report for 172.30.0.1
Host is up (0.00042s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE  VERSION
53/tcp  open  domain   (generic dns response: NOTIMP)
80/tcp  open  http     nginx
443/tcp open  ssl/http nginx
1 service unrecognized despite returning data. If you know the service/version, please submit the following fi
ngerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=10/15%Time=5F88DBC9%P=x86_64-pc-linux-gnu%r(DNS
SF:VersionBindReqTCP,20,"\0\x1e\0\x06\x81\x85\0\x01\0\0\0\0\0\0\x07version
SF:\x04bind\0\0\x10\0\x03")%r(DNSStatusRequestTCP,E,"\0\x0c\0\0\x90\x04\0\
SF:0\0\0\0\0\0\0");

Nmap scan report for innerouter.f4rmc0rp.com (172.30.0.3)
Host is up (0.00064s latency).
Not shown: 999 filtered ports
PORT    STATE SERVICE  VERSION
443/tcp open  ssl/http nginx

Nmap scan report for ns.f4rmc0rp.com (172.30.0.128)
Host is up (0.00047s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
53/tcp   open  domain   ISC BIND 9.11.5-P4-5.1+deb10u1 (Debian Linux)
80/tcp   open  http     Apache httpd 2.4.38 ((Debian))
443/tcp  open  ssl/http Apache httpd 2.4.38 ((Debian))
```

.

I suspect that 172.30.0.3 has to be the host were interested in since it is the innerouter. It is hinted that we must port forward a port from the 172.30.0.0/24 network to the 10.30.0.0/24 network. This is done by navigating to **https://172.30.0.3:443** using a web browser. This brings us to the pfsense login page, using the default credentials: admin/pfsense we were able to log-in and set a Forwarding Rule. The following rule is created (the top one):



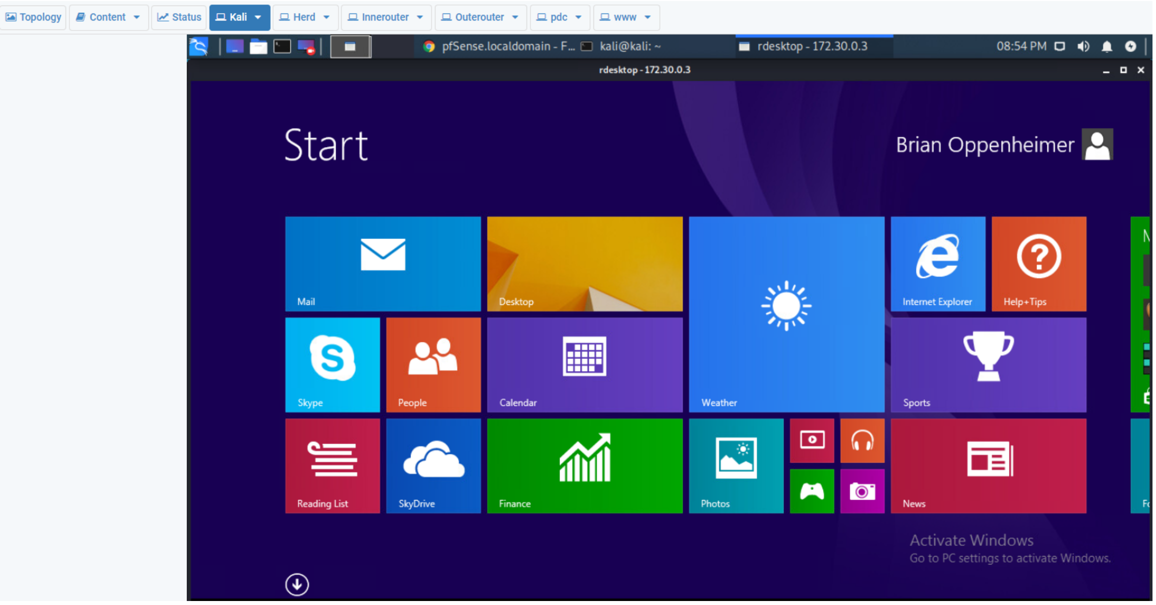
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / NAT / Port Forward

Rules

☐			Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
☐	✓	⤮	WAN	TCP	*	*	WAN address	3389 (MS RDP)	10.30.0.98	3389 (MS RDP)		
☐	✓	⤮	WAN	TCP	*	*	WAN address	443 (HTTPS)	10.30.0.1	443 (HTTPS)	Forward WAN https to LAN https	

With this new port forwarding rule in place, we should now be able to connect to the herd.f4rmc0rp.com machine via rdp.
This was achieved by running **rdesktop -g95% 172.30.0.3**
Now was also hinted that information we found in a previous ”attack” could be useful for logging in to the HERD machine. From Ex080 there was a directory called secrets in this directory the phrase Sw0rdF!sh was seen. Sure enough I was able to log in to the HERD machine with username **brian** and password **Sw0rdF!sh**.


Topology
Content
Status
Kali
Herd
Innerouter
Outerouter
pdc
www
pfSense.localdomain - F...
kali@kali: ~
rdesktop - 172.30.0.3
08:54 PM
rdesktop - 172.30.0.3
Start
Brian Oppenheimer
Mail
Desktop
Internet Explorer
Help+Tips
Skype
People
Calendar
Weather
Sports
Reading List
SkyDrive
Finance
Photos
News
Activate Windows
Go to PC settings to activate Windows.