Ex0b0 - NetcatPivot

Simon Tobon

2021-07-08

Contents

Technical Report

Introduction

For this exercise we were tasked to connect to a normally inaccessible web server by creating a netcat pivot on plunder.pr0b3.com.

Finding: Description of finding

Vulnerability Description

A web server can be accessible from an outside machine via Netcat. This enables attackers to exfiltrate potentially disclosed information, and learn more about the network.

Mitigation or Resolution Strategy

This attack can be mitigated by closing port 80. It can also be mitigated by locking all web pages under an administrative login.

Attack Narrative

To begin we Connected to Plunder via SSH. This was done by the following: **ssh stobon@plunder.pr0b3.com**.

From there, on Plunder, we ran **ip a** to see all the network interfaces on Plunder. We were using interface ens33 (45.79.141.233), from here on referred to as Interface 1, Another instance of Plunder is also ran on ens160 (45.79.140.233), referred to as Interface 2.

```
stobon@plunder:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:50:56:87:e5:56 brd ff:ff:ff:ff:ff:ff
    inet 45.79.140.233/24 brd 45.79.140.255 scope global noprefixroute ens160
       valid_lft forever preferred_lft forever
    inet6 fe80::fefe:724f:8a1b:2ba1/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:50:56:87:79:14 brd ff:ff:ff:ff:ff:ff
    inet 45.79.141.233/24 brd 45.79.141.255 scope global noprefixroute ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe87:7914/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

From here I created a shell script with the following source:

```
 GNU nano 3.2                                                scan.sh

#/bin/bash

for i in {1..255}
do
nc -v -z -w 0.001 45.79.140.$i 80

done
```

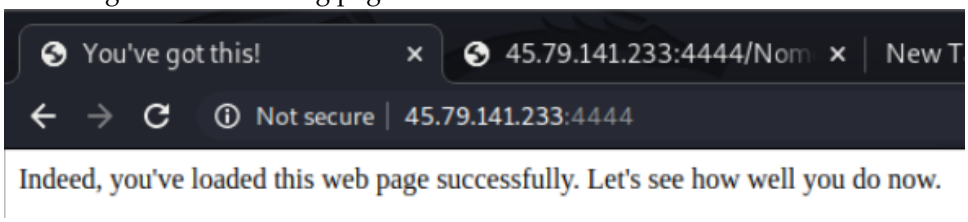
When executed on Plunder, it runs the netcat command to connect to port 80. It cycles through ip ranges: 45.79.140.**1-255**. The only IP address that succeeded on port 80 was 45.79.140.13.

```
Ncat: Connected to 45.79.140.13:80.
Ncat: 0 bytes sent, 0 bytes received in 0.01 seconds.
```

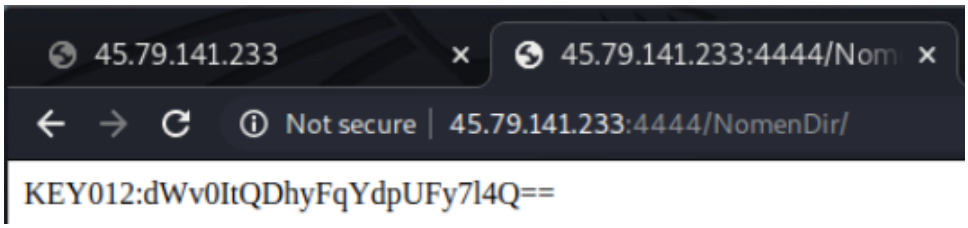
This command also confirmed that port 80 was open on that machine.

From here, we ran the following commands to establish a netcat listener connector pivot.
mknod /tmp/door p and **nc 45.79.140.13 80 </tmp/door — nc -k -l -p 4444 >/tmp/door**

Immediately after, we open a web browser on our Kali machine and navigated to 45.79.141.233:4444. This is the address for Plunder, we connect to it since we issued the command on Plunder and it uses that address as the listener. This will bring us to this landing page:



With deeper digging, we are able to find a KEY. This is done by looking at the source code of the webpage. From there we find some portion of code that is commented out that redirects to the NomenDir subpage. We can navigate to this page by going to 45.79.141.233:4444/NomenDir, it will prompt us to login, we can login with previously exfiltrated credentials: n.nomen/Satoshi1 on this page we can find the KEY:



This concludes the report.