Ex0b0

Joshua Main-Smith

2020-11-02

Contents

Technical Report

Finding: Hyperlinks to Sensitive Data

Risk Assessment

A commented out hyperlink to a directory was found in the page source of the web page on **45.79.140.13:80**. Access to the directory was password protected, indicating the presence of sensitive information. Exploitation could lead attackers in viewing or exfiltrating said sensitive information.

Vulnerability Description

Viewing the page source of **45.79.140.13:80** shows the pathway to a directory that has been commented out. Attackers having in possession of the proper credentials can connect to the directory.

Mitigation or Resolution Strategy

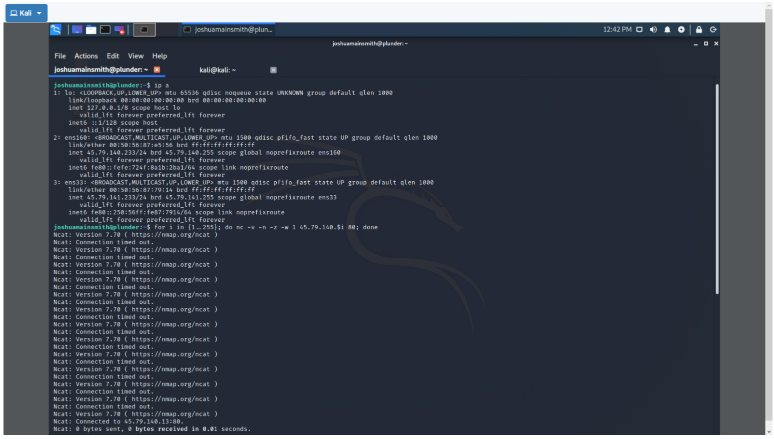
If the pathway to the directory isn't intended for public knowledge, then the hyperlink should be deleted rather than commented out.

Attack Narrative

Connecting to Foreign Machine

After connecting to Plunder with **ssh name@plunder.pr0b3.com**, we can see the network devices connected on the machine by using **ip a**. There were two interfaces attached to Plunder with the IP addresses of **45.79.140.233/24** and **45.79.141.233/24**. From our Kali host, we can ping the machine with **ping plunder.pr0b3.com** and this will tell us the IP address of the machine we connected to, which is **45.79.141.233**. So, we're interested in finding any web pages connected to **45.79.140.233:80**.

We didn't have access to nmap on Plunder, but we were able to scan the network for listening connections of port 80 on the network using a one line script utilizing Netcat, which is **for i in {1..255}; do nc -v -n -z -w 1 45.79.140.$i 80; done**. We found that the only machine available was at **45.79.140.13:80**, as seen in the image below.


Kali
joshuamainsmith@plun...
12:42 PM
joshuamainsmith@plunder: ~
File Actions Edit View Help
joshuamainsmith@plunder: ~
kali@kali: ~

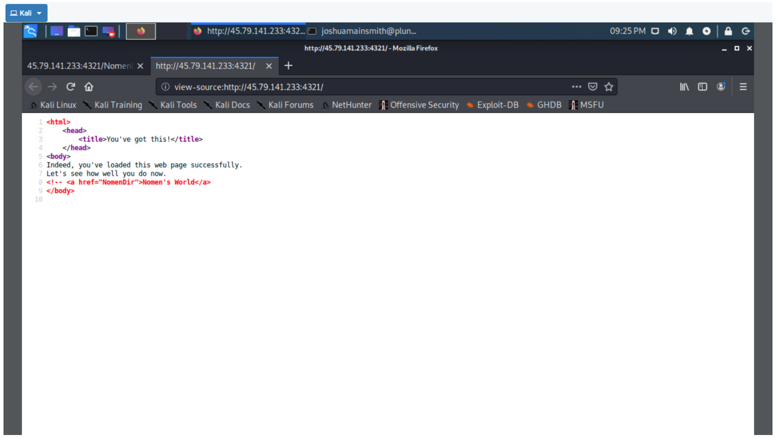
```
joshuamainsmith@plunder:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       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
joshuamainsmith@plunder:~$ for i in {1..255}; do nc -v -n -z -w 1 45.79.140.$i 80; done
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connection timed out.
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connection timed out.
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connection timed out.
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connection timed out.
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connection timed out.
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connection timed out.
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connection timed out.
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connection timed out.
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connection timed out.
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connection timed out.
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connection timed out.
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connection timed out.
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 45.79.140.13:80.
Ncat: 0 bytes sent, 0 bytes received in 0.01 seconds.
```

We then connected to the web page from our Kali host to the foreign address on our web browser using a listener/connector pivot on Plunder. First, we made a FIFO file that we'll use as input for the connector and output as the listener with **mknod bp p**. We then set up our listener/connector with **nc 45.79.140.13 80 <bp | nc -l -k -p 8080 >bp** (the **-l** opens a listener, **-k** keeps listening for connections and **-p** specifies the port).

We can then connect to the machine on **45.79.140.13:80** on the web browser from our Kali host by going to the address **45.79.141.13:8080**. We were greeted with an encouraging message **You've got this!** and **Indeed, you've loaded this web page successfully. Let's see how well you do now**.

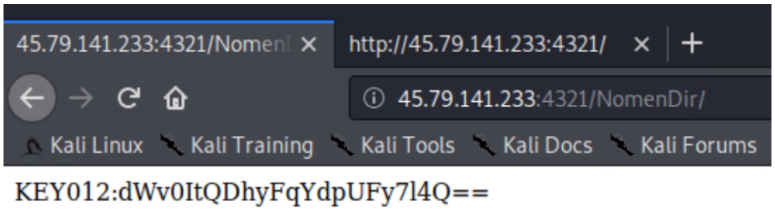
KEY

Viewing the page source, it appears that that there was a hyperlink to a directory that has since been commented out.



```
<html>
    <head>
        <title>You've got this!</title>
    </head>
<body>
Indeed, you've loaded this web page successfully.
Let's see how well you do now.
<!-- <a href="NomenDir">Nomen's World</a>
</body>
```

Navigating to 45.79.141.13:8080/NomenDir we were greeted with a prompt to enter username and password credentials. We attempted the credentials we discovered from cracking hashes we discovered earlier on Herd, successfully granting us access to KEY012.



KEY012:dWv0ItQDhyFqYdpUFy7l4Q==

Zoom Link

October 29, 2020