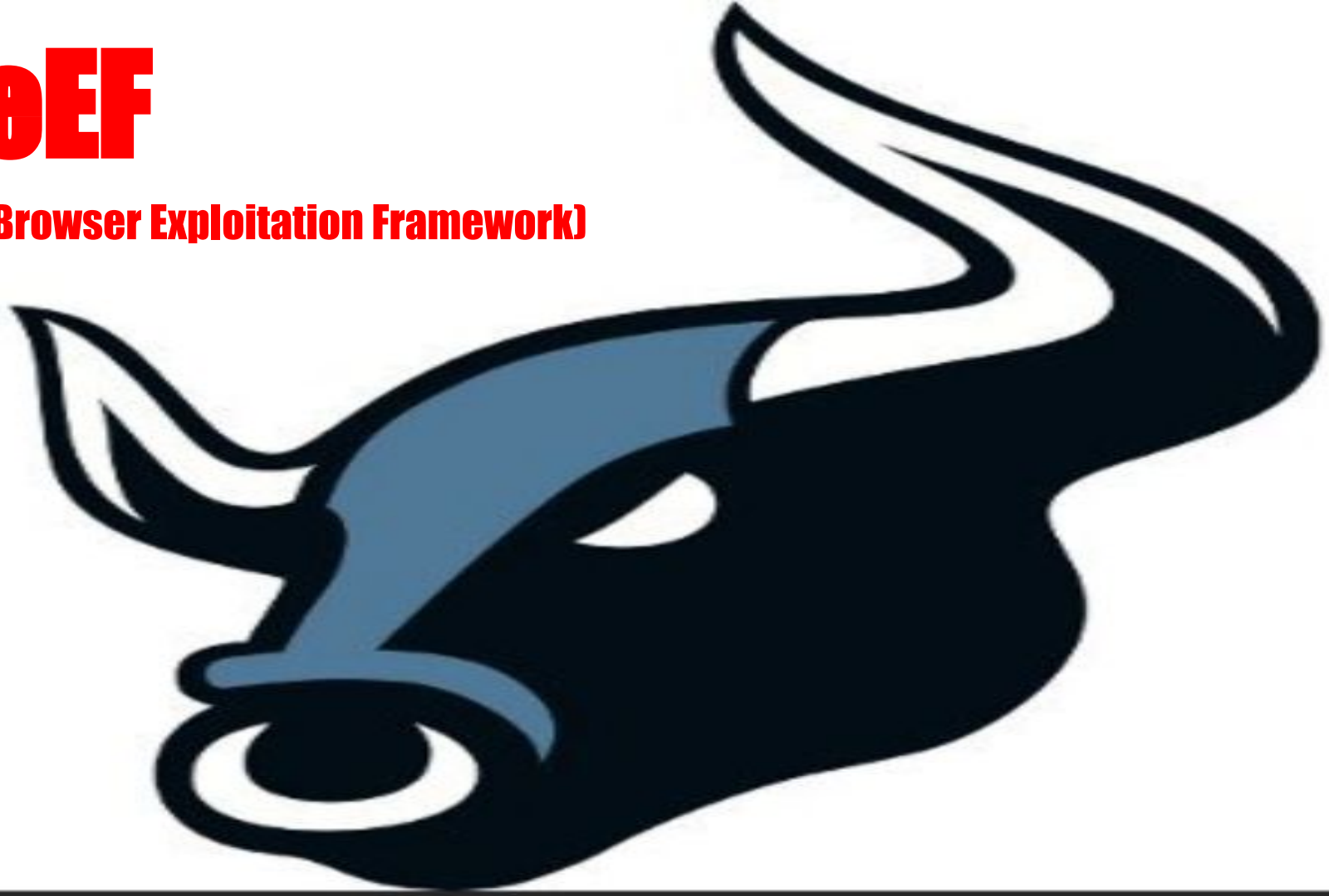
BeEF

(The Browser Exploitation Framework)



Rethinking Beef: Ethics on Your Plate

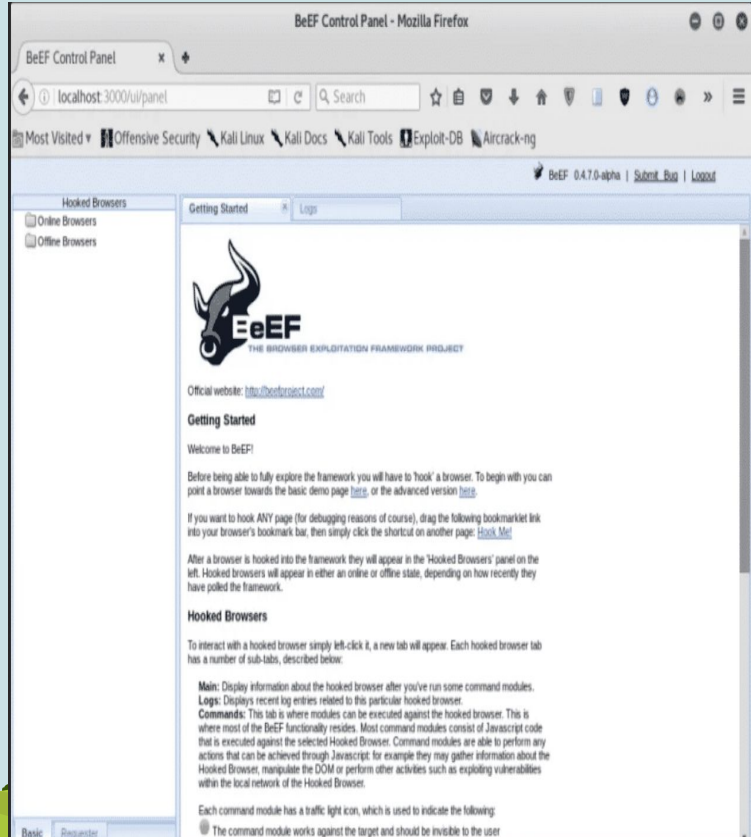
Introduction to BoEF

What Is BeEF?

- BeEF is short for Browser Exploitation Framework. It is an open source penetration testing tool focused on exploiting vulnerabilities in the web browser.
- Can be done via Phishing attack
- Perfect for social engineering or keylogging
- Coded in Ruby

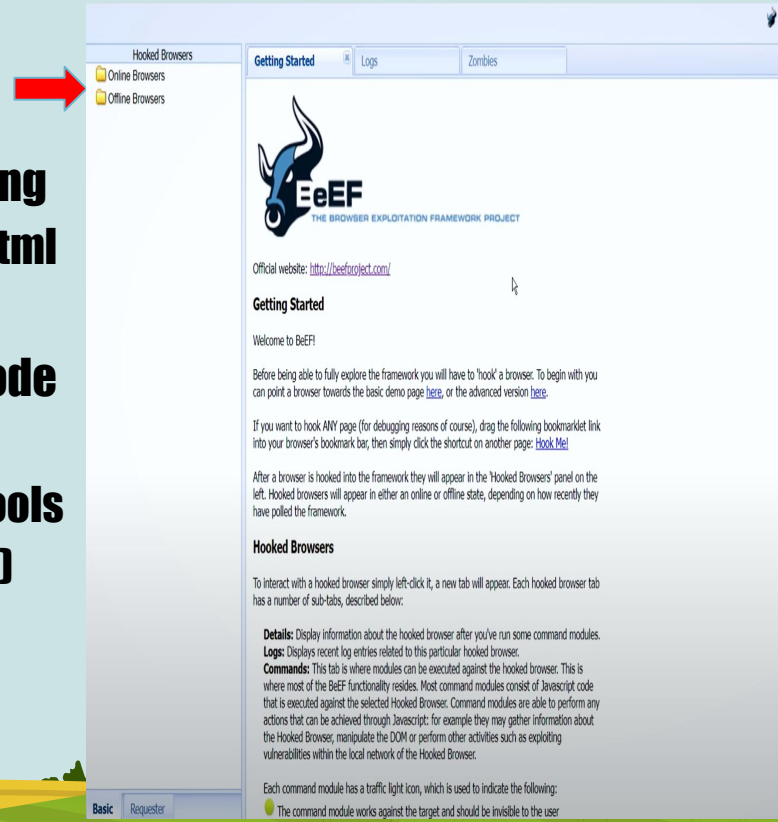
Installation and setup

-`sudo apt install beef-xss`
-`Ip a or Ifconfig`- This will get your IP Address
-`sudo beef-xss`
-`sudo beef-xss-stop`-This will stop BeEF if needed
-Username is beef, Password: Whatever you want



Directions for BeEF

- You will see online and offline browsers
- Enable bi-drectional clipboard in Virtualbox
- Copy the second “Here” link then send the following
  - http://<your IP>:3000/demos/butcher/index.html
- If you want make a website with the BeEF script
- A website can hide the BeEF script in its source code
- If using a VM set network to “Bridged Adapter”
- UML blocks Kali Linux so use a VPN when installing tools
- MUST be on SAME NETWORK as your victim (EDUROAM)



What to do Next

- When someone clicks on link they are “Hooked”
  - Hoooked means that victims browsers are now under your control.
- Click on the hooked IP address and go to commands
- You will have a large list of exploits you can use
- Choose an exploit on the dedicated IP and execute it
- When viewing exploits `green` means likely to work, `orange` means may work, `red` means it probably won't work.
  - You can also have pop-up messages made by you

Objective

Your objective is to gather the following information:

1. Get Noah's browser history
2. View IP address, browser, OS of victim
3. Get cookies of victim
4. Man-In-The-Browser
5. Confirm close Tab
6. DOS user
7. Use the Proxy to ping google
8. Use XSS Rays (Cross site scripting)

For extra credit:

1. Integrate BeEF with metasploit.
2. Use your victimes browser as a proxy
3. Utilize a JavaScript XSS