BeEF framework

Browser exploitation framework allows us to launch a number of attacks on a hooked target. Targets are hooked once they load a hook url.

→ start beef: kali → beef start
→ open it
→ it'll open beef on browser, login (user: beef)
→ On the left are some online & offline browsers (previously hooked) that you can control.

★ In order to hook a browser, you need to get it execute a specific JS code.
→ if you are MITM then a dns spoof can be done to redirect user to the link of js.
→ or you can inject js code that we learnt earlier.
→ or you can exploit XSS vulnerability
→ or do social engineering.

Subject :

PAGE NO
DATE

☆ Lets try to hook.
☆ Copy the js script from terminal.
→ go to var/www/html
→ write click & open index.html via text editor
→ place hook code <script ..... >
→ replace the ip with kali's ip.
☆ if anyone now loads our ip. The hook code will execute automatically.

→ Start the webserver
→ go to windows VM & go to our ip
→ Currently since its us, no dns spoof is required
→ now, if you go to beef.
→ the browser is hooked.
→ Now you can do various things
↳ In details → generic info is found
↳ In logs → logs of events are shown
↳ In commands tab, you can run various commands.
↳ In Proxy tab → configure & use browser as a proxy
→ logout once done.

☆ Now that we have hooked a browser, there's a better way to do it if you are MITM.
→ download custom js code. (✓)
→ ~~copy it~~ modify it :
→ enter your ip. & save
→ put location of this file in hstscaplet. (usr/1000/1/share/bettercap)
→ modify payloads
→ put our js. ☆ : root/Downloads/inject-beef.js

Subject :

PAGE NO
DATE

→ now if you run bettercap, any site that user loads will get us hooked to their browser.
→ ∴ run arpspoof
→ load hstshijack.
→ go to target & load any website.
→ We have hooked the target now
★ Now we can inject our codes

★ Go to beef → commands
★ There are many things you can do.
★ Click on module → execute.
↳ lets try alert
↳ go to Create Alert Dialog & execute.
↳ go to Raw JavaScript → use any code you want
↳ go to Spyder Eye → get screenshot of the user pc (it might fail)
↳ go to Redirect Browser
↳ redirects target to any url

★ Now lets have a look over social engineering plugin.
→ go to Social Engineering → go to Pretty Theft
→ Dialog Type (select) → Backing (default)
→ execute.

———— ∝ ———— ∝ ———— ∝ ————

★ Now lets try to gain full meterpreter control over the target.
→ go to Social Engineering
→ go to Fake Notification Bar
→ this will tell user to install a plugin (which is our backdoor)
→ give its full address in the URL box
→ give the notification text
→ before running, open the port to listen in metasploit.