# Bettercap Web GUI

Contents

[Bettercap Web GUI 1](#_Toc84705819)

[Lab Requirements 1](#_Toc84705820)

[Bettercap Web GUI 1](#_Toc84705821)

[1. View Local IP Address Information 1](#_Toc84705822)

[2. bettercap Web GUI 2](#_Toc84705823)

[Assignment Submission 3](#_Toc84705824)

Time required: 30 minutes

# Lab Requirements

This lab can disrupt network communications on a production network. We want to do this lab in a completely virtual environment.

1. Kali Linux VM
2. Windows VM with Google Chrome
3. Both VM’s on same NAT network

# Bettercap Web GUI

We know how to be the man in the middle and capture all the packets from a victim. We can do this from a GUI interface.

Connect both VM’s to the NAT network we created earlier.

# 1. View Local IP Address Information

On your Kali Linux: run the following command in the terminal to find out the name and IP address of the network interface that you’re using. It is commonly eth0.

|  |
| --- |
| ip a |

**Insert a screenshot:**

Click or tap here to enter text.

# 2. bettercap Web GUI

Bettercap that comes installed with Kali Linux doesn’t work right. It does if we do a clean build direct from the bettercap github.

1. Type the following commands separately at the terminal to do a clean install of bettercap.

|  |
| --- |
| sudo apt update  sudo apt install -y golang git libusb-1.0-0-dev libpcap-dev libnetfilter-queue-dev  git clone https://github.com/bettercap/bettercap.git  cd bettercap  go install  go build  sudo ./bettercap  caplets.update  ui.update |

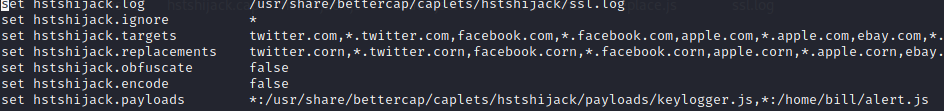
1. Quit bettercap.
2. Enter the following command to open the hstshijack.cap for editing.

|  |
| --- |
| sudo geany /usr/local/share/bettercap/caplets/hstshijack/hstshijack.cap |

This is the contents of the alert.js file we created earlier

|  |
| --- |
| alert('You have been hacked!') |

1. Go to the **set hstshijack.payloads** line shown at the bottom, add the path to your **alert.js** file.



|  |
| --- |
| ,\*:/home/user/alert.js |

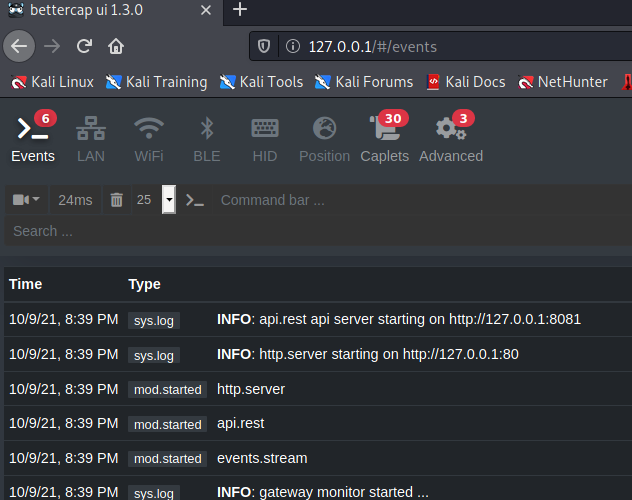
1. Run the following commands to start bettercap and the web ui.

|  |
| --- |
| cd ./bettercap  sudo ./bettercap -iface eth0  http-ui |

1. **Insert a screenshot:**

Click or tap here to enter text.

1. In your web browser: go to **localhost**
2. You should see the bettercap web ui.
3. Username: **user** Password: **pass**

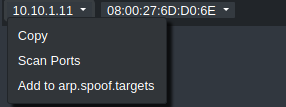


1. Click the **LAN** tab. Click the play button for **net.probe.** This will automatically start **net.recon**. Those are the play buttons to the right of the trash can.

Graphical user interface, application

Description automatically generated

1. You should see your gateway, your Kali machine, .3 is the VirtualBox DHCP server and the victim computer’s IP address.
2. Click the downward pointing triangle next to the victim computer’s IP address 🡪 **Add to arp.spoof.targets**.



1. Click **full-duplex spoofing**. Click **Start arp.spoof**.
2. You will see a little red icon indicating that you are spoofing the target.
3. Go to your Windows victim machine. At a command prompt: **ping google.com**
4. Run **arp -a** You should see that the gateway MAC address is the same as the Kali machine.
5. **Insert a screenshot:**

Click or tap here to enter text.

1. On Kali: Click the **Caplets** tab. Click **hstshijack**
2. Click the play button above the display of the **hstshijack.cap** file.
3. Go to [www.vulnweb.com](http://www.vulnweb.com) 🡪 Click one of the websites to see the javascript file showing an alert.
4. **Insert a screenshot:**

Click or tap here to enter text.

1. Close the web browser. Type **quit** to stop bettercap.

## Assignment Submission

Attach this completed document to the assignment in Blackboard.