ETHICAL HACKING V2
LAB SERIES

Lab 12: ARP Spoofing and MiTM Attacks

Document Version: 2020-08-24

Material in this Lab Aligns to the Following	
Books/Certifications	**Chapters/Modules/Objectives**
All-In-One CEH Chapters ISBN-13: 978-1260454550	6: Web-Based Hacking: Servers and Applications
EC-Council CEH v10 Domain Modules	13: Hacking Webservers 14: Hacking Web Applications 15: SQL Injection
CompTIA Pentest+ Objectives	3.2: Given a scenario, exploit network-based vulnerabilities 4.2: Compare and contrast various use cases of tools
CompTIA All-In-One PenTest+ Chapters ISBN-13: 978-1260135947	7: Network-Based Attacks

Contents

Introduction

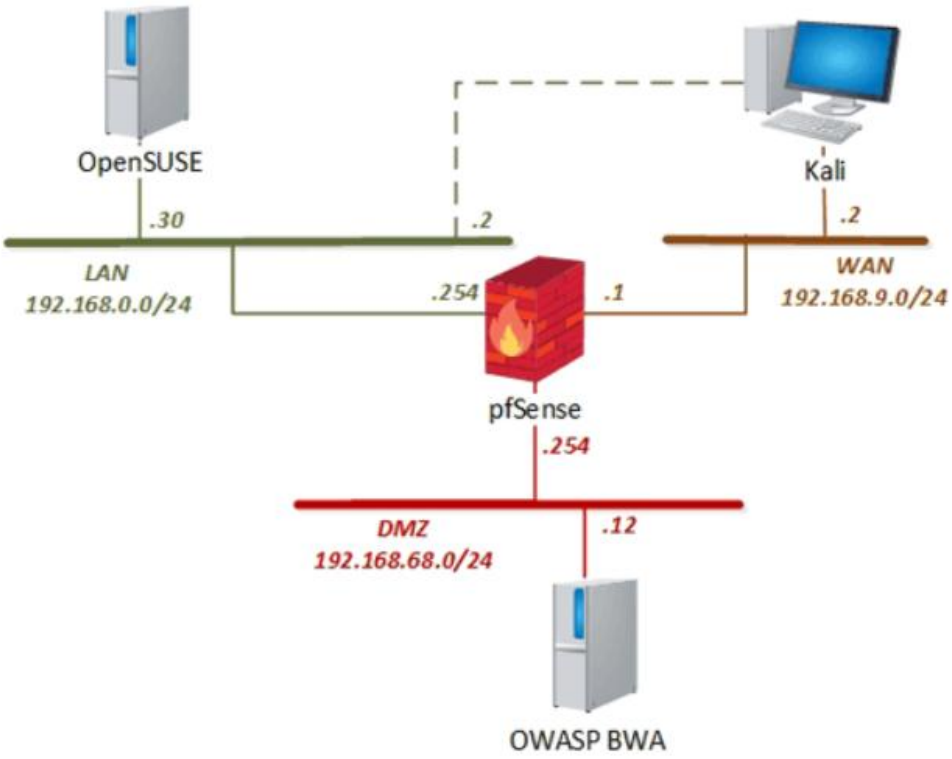
In this lab, you will explore ARP spoofing and doing Man-in-The-Middle (MiTM) attacks.

Objective

In this lab, you will be conducting ethical hacking practices using various tools. You will be performing the following tasks:

1. ARP Spoofing with Ettercap
2. Capturing web username and passwords
3. Manipulating HTTP images
4. Manipulating Javascript

Pod Topology



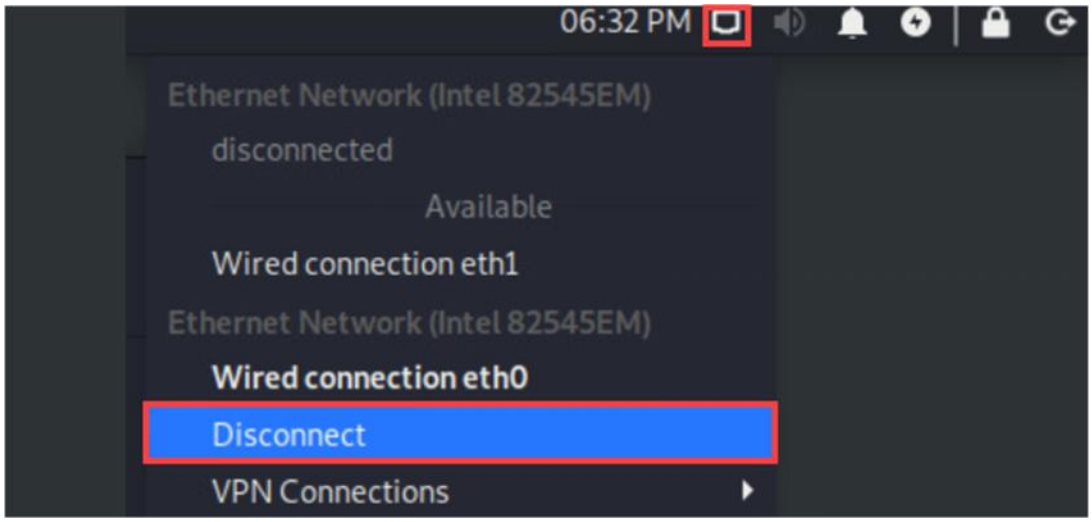
Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

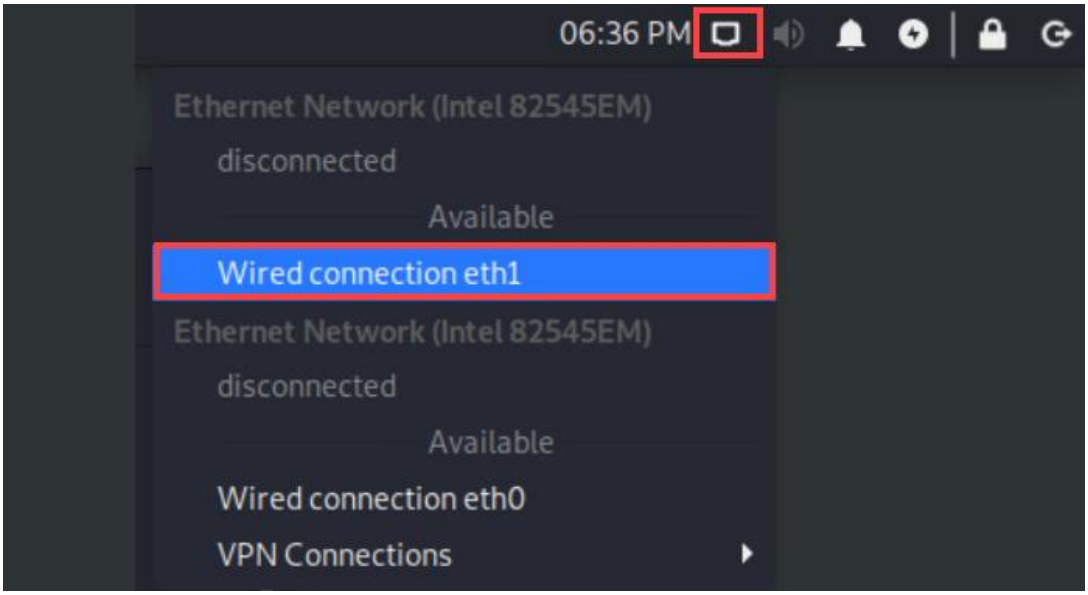
Virtual Machine	**IP Address**	**Account** (if needed)	**Password** (if needed)
Kali Linux	192.168.9.2 192.168.0.2	root	toor
pfSense	192.168.0.254 192.168.68.254 192.168.9.1	admin	pfsense
OWASP Broken Web App	192.168.68.12	root	owaspbwa
OpenSUSE	192.168.0.30	osboxes	osboxes.org

1 ARP Spoofing with ettercap

1. Click on the **Kali** tab.
2. Click within the console window and press **Enter** to display the login prompt.
3. Enter **`root`** as the *username*. Press **Tab**.
4. Enter **`toor`** as the *password*. Click **Log In**.
5. For this lab, you need to disable eth0 and enable eth1. By connecting eth1, you put the Kali machine on the LAN network, with an IP address of 192.168.0.2. To disable eth0, click on the network icon in the upper-right, then click on **Disconnect** below *Wired connection eth0*.



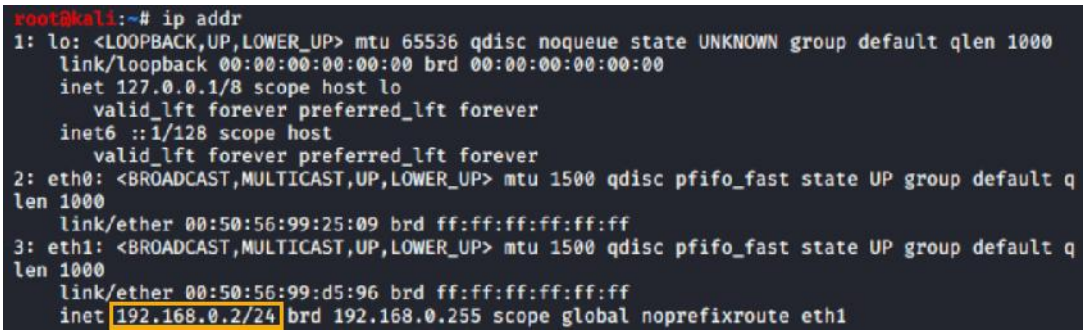
6. To enable eth1, click on the network icon in the upper-right, then click on **Wired connection eth1**.



7. Open the *Terminal* by clicking on the **Terminal** icon located at the top of the page, if not already open.

8. Confirm your IP address on eth1 by typing the following command and pressing **Enter.**

```
ip addr
```



Review eth1 and notice the inet address of 192.168.0.2/24.

9. Launch *Ettercap* in its graphical view by typing the command below and pressing **Enter.**

```
ettercap -G
```

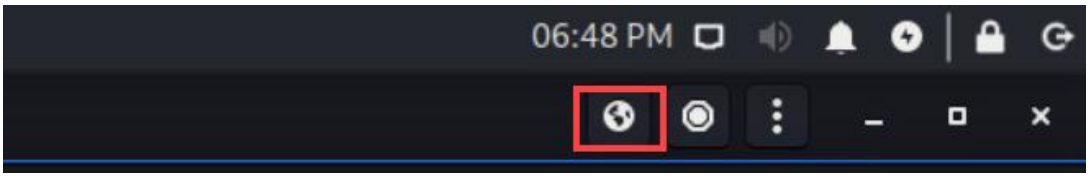
It is strongly recommended that you maximize the Ettercap interface by clicking the maximize button in the upper-right (looks like a square).

10. Change the *Primary Interface* dropdown to **eth1.**
11. Click the **checkmark** in the upper-right to accept changes.
12. Ettercap is now sniffing traffic. However, we need to select a target that we want to spoof. To scan for hosts on the same network, click the **magnifying glass** in the upper-left.

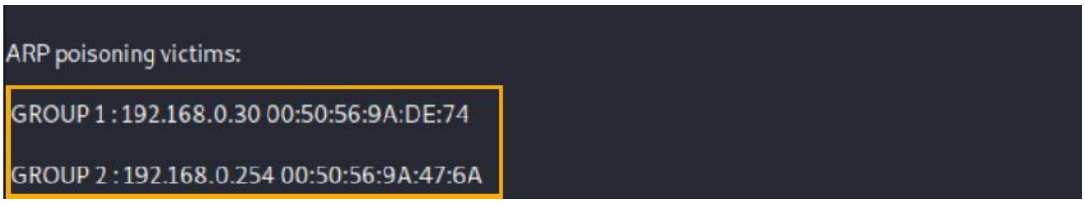
Review the output at the bottom of the screen. This is where you can monitor what the program is doing. Notice that hosts have been added to the hosts list.

13. To view the Host list, click the icon to the right of the magnifying glass.
14. You want to target the OpenSUSE machine, so click on **192.168.0.30.** Then click on **Add to Target 1**.
15. You also want to target only the pfsense firewall. If you do not select the firewall, *ettercap* will end up poisoning all hosts in the list. Click on **192.168.0.254** and click on **Add to Target 2.**

16. You are now able to sniff traffic but have not actually poisoned ARP. To start ARP poisoning, click on the **MITM** (Man-In-The-Middle) icon at the top-right.



17. Select **ARP Poisoning.**
18. Leave the default option to *Sniff remote connections* and click **OK.**
19. At this point, you have poisoned the ARP table. Traffic from OpenSUSE is being directed to the Kali machine.



Review the output at the bottom of the screen. You can confirm the two victims you selected.

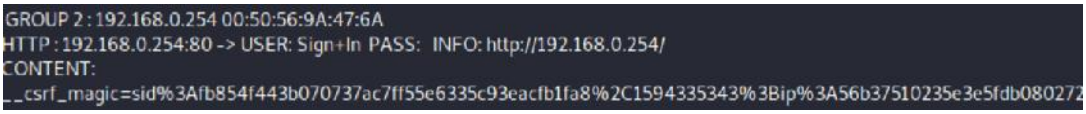
20. Leave the window open for the next task.

2 Capturing web username and passwords

1. By default, Ettercap will look for people logging into HTTP websites and record usernames/passwords. Note, this is happening at the packet level on the wire. To test this, click on the **OpenSUSE** tab at the top.
2. Enter **`osboxes.org`** as the *password*. Then press **Enter**.
3. Open the **Firefox** web browser.
4. You will be logging into the pfSense web interface. In the address bar, type the following and press **Enter:**

```
http://192.168.0.254
```

5. Enter **`admin`** as the *username*.
6. Enter **`pfsense`** as the *password*. Click **Sign In**.
7. Click on the **Kali** tab.



Review the output at the bottom of the screen. You may need to scroll to the right. Notice that it captured the username and password. In this current configuration, this will only work for HTTP websites. To capture HTTPS traffic requires more configuration and is beyond the scope of this lab.

8. Leave the window open for the next task.

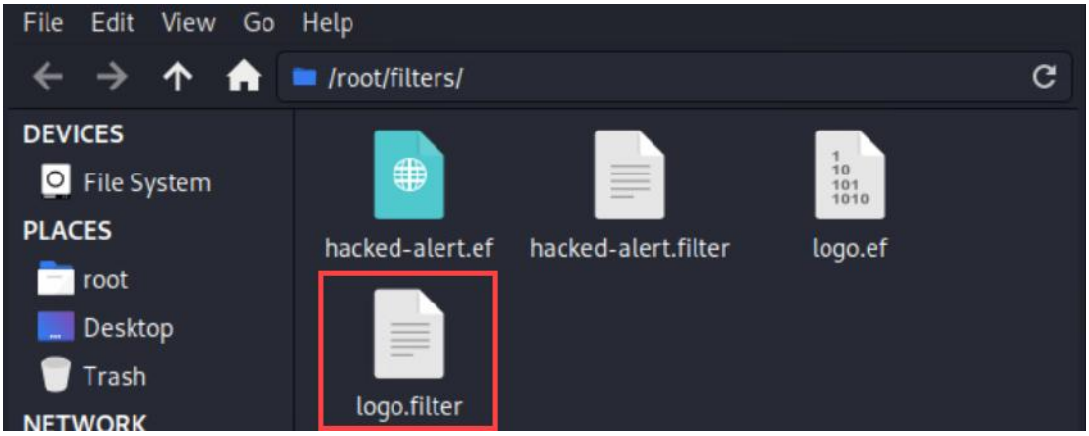
3 Manipulating HTTP Images

Capturing usernames and passwords is fun, but wouldn't it be more fun to mess with the user? *Ettercap* is monitoring HTTP traffic to and from the OpenSUSE machine. *Ettercap* can use filters to manipulate the traffic as it passes through the Kali box. How about you change all the images to an image of your own?!

1. Click on the **OpenSUSE** tab at the top.
2. Firefox should still be open. If not, relaunch Firefox. You will browse the OWASP machine's webpage. Type the following in the address bar and press **Enter**.

```
http://192.168.68.12
```

3. Review the page, taking notice of the graphics. Then, close the Firefox web browser.
4. Click on the **Kali** tab at the top.
5. Before we can enable the filter, take a look at what the filter does by clicking on the **File Browser** icon, then click on **filters** and finally click on **Open Folder.**
6. Inside this folder, you will see files that end with **.ef** and **.filter.** The **.ef** files are the compiled versions of the filter. You will use these later. The first one you want to look at is **logo.filter,** and you can do that by double-clicking on it.



7. The first **if** statement is looking for traffic that has a protocol of TCP and where it is destined for port 80. Here the filter will trash the Accept-Encoding, which allows the filter to modify the HTML.
8. The second **if** statement is then looking for traffic that has a protocol of TCP and a source of port 80. The filter will look for **<img src>** tags in the html and replace them with http://192.168.0.2/logo.jpg. This is a file we will host locally on the Kali system. You can close the **Mousepad** window and the **File Manager** window.

Note you could replace the logo.jpg file located in /var/www/html with any file you want. You would need to make sure the filename stays the same or you will be forced to recompile the filter before using it.

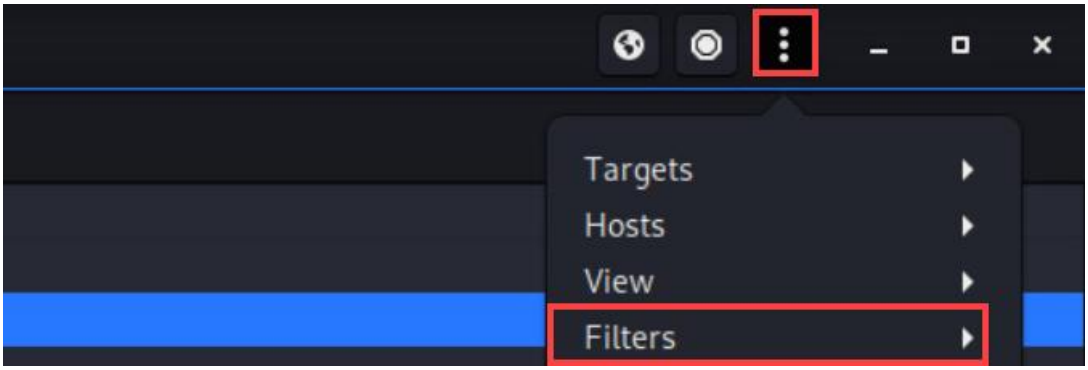
9. To start, you need to launch the webserver on Kali to host the image. Open a new **Terminal** window by clicking on the icon.
10. To start the *Apache* webserver, type the following and press **Enter**.

```
service apache2 start
```

```
root@kali:~# service apache2 start
root@kali:~# service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
     Active: active (running) since Thu 2020-07-09 19:10:09 EDT; 1min 1s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 2053 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
```

There is no confirmation the service started. To confirm, you can type **`service apache2 status`** and note the active line shows it is running. Press **q** to exit the status window.

11. Click the **X** to close this terminal window.
12. The *Ettercap* window should be displayed. If not, click on the application at the top.
13. Click on the *Ettercap* menu icon and click on **Filters**.



14. Click on **Load a filter…**
15. In the *Select a precompiled filter file….* window, click on the **Home.**
16. Double-click on the **filters** folder.
17. Click on **logo.ef** and then click on **OK**.

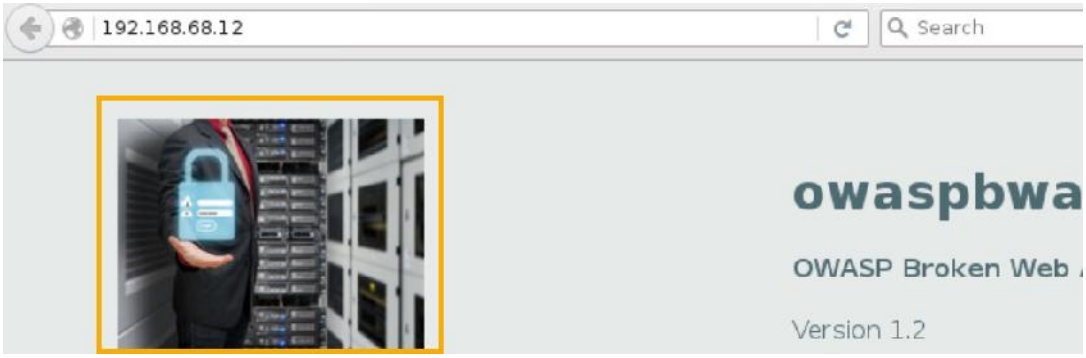
In the status window, make sure the content filter loaded successfully.

The logo.ef is a compiled filter for ettercap. The logo.filter is a text file with the ettercap filter script you examined earlier.

18. With the filter loaded, it is time to test it. Click on the **OpenSUSE** tab at the top.
19. Launch *Firefox* by clicking on the icon.

20. In the address bar, you will browse back to the OWASP webpage by typing the following and pressing **Enter:**

```
http://192.168.68.12
```



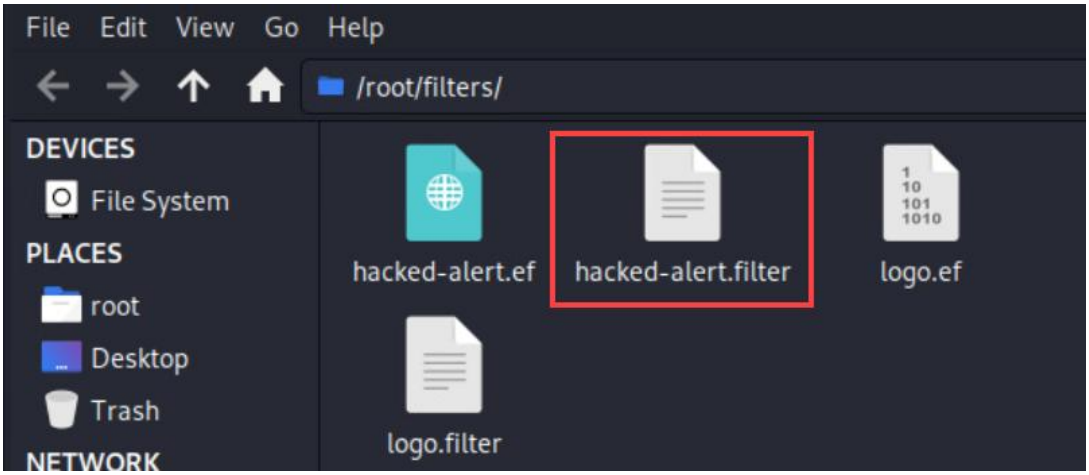
Notice that every image on the page has been changed.

21. Close the Firefox browser.

4 Manipulating Javascript

Normally, a hacker would not try to expose themselves in this manner, and certainly wouldn't do this during an audit. However, adding a Javascript alert into the HTML is a simple way to demonstrate injecting Javascript into an HTML page, causing the code to execute. The user thinks they are just going to a legitimate web site and has no other indication that they are being attacked.

1. Click on the **Kali** tab at the top.
2. First, review the filter you are about to apply by clicking on the **File Browser** icon, then click on **filters** and finally click on **Open Folder.**
3. The first one you want to look at is **hacked-alert.filter,** and you can do that by double-clicking on it.

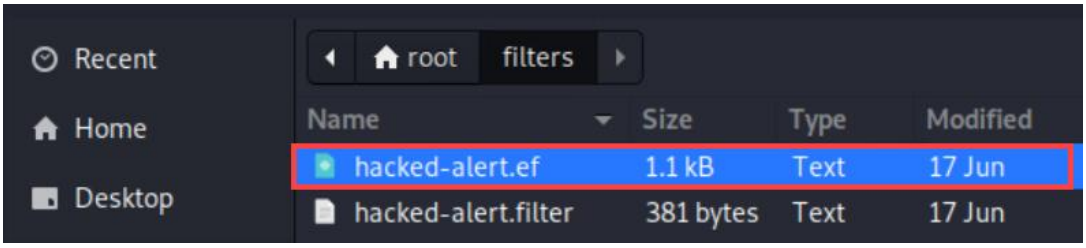


4. Like the last filter, the first **if** statement allows us to manipulate HTML. The second **if** statement will search the HTML for the closing </head> tag. It will then add a simple Javascript alert. You can close the **Mousepad** window and the **File Manager** window.

> Remember, this is non-malicious code. The Javascript here could be part of an infection from something like BeEF (The Browser Exploitation Framework), which allows a hacker to hook a browser and launch further attacks against the system from within the browser.

5. The *Ettercap* window should be displayed. If not, click on the application at the top.
6. Click on the *Ettercap* menu icon and click on **Filters**.
7. Click on **Load a filter…**
8. In the *Select a precompiled filter file….* window, click on **Home.**
9. Double-click on the **filters** folder.

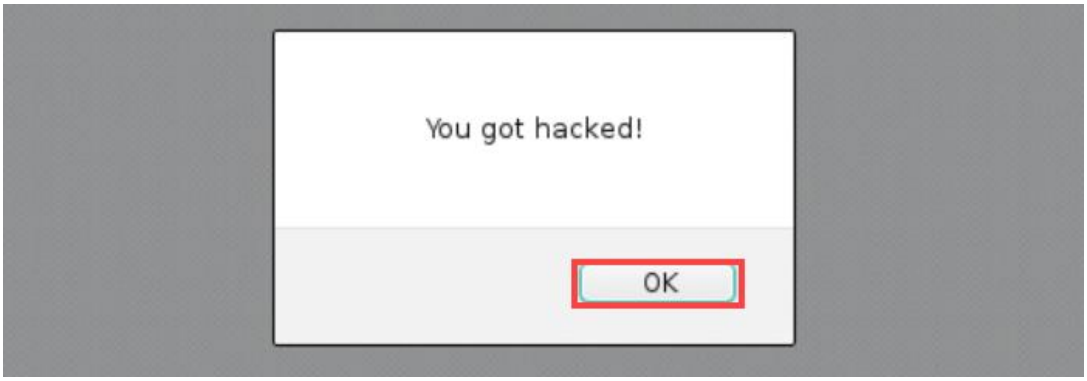
10. Click on **hacked-alert.ef** and then click on **OK**.



In the status window, make sure the content filter loaded successfully.

11. With the filter loaded, it is time to test it. Click on the **OpenSUSE** tab at the top.
12. Launch *Firefox* by clicking on the icon.
13. In the address bar, you will browse back to the OWASP webpage by typing the following and pressing **Enter:**

```
http://192.168.68.12
```



Notice the popup alert. Click on **OK.** Notice the images are still changed from the last filter. You can use several filters at once, allowing you to keep each filter small, so you can chain them together as needed.

14. You may now end your reservation.

