ETHICAL HACKING
LAB SERIES

Lab 11: Network Analysis

Material in this Lab Aligns to the Following Certification Domains/Objectives	
Certified Ethical Hacking (CEH) Domains	Offensive Security (PWK) Objectives
8: Sniffers	3: The Essential Tools (netcat, ncat, wireshark, tcpdump)

Document Version: 2016-03-09

Contents

Introduction

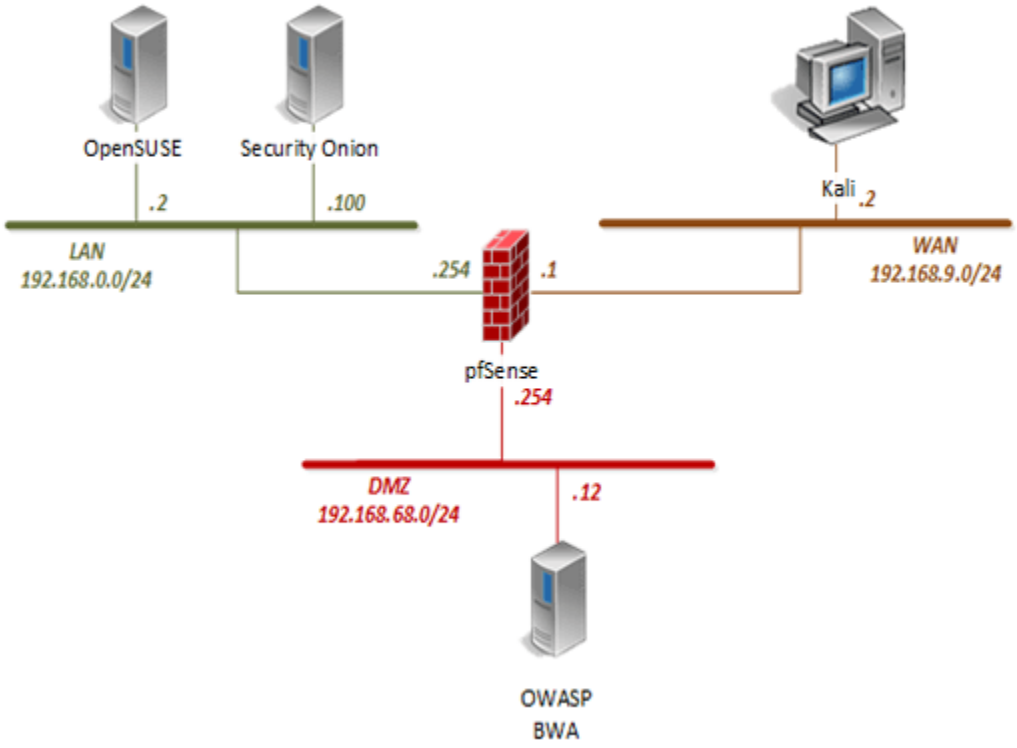
The ability to capture and analyze packets is an important skill when performing a security assessment or investigating a potential network breach. This lab will demonstrate how to capture and analyze network packets.

Objective

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

1. Capturing Traffic with tcpdump
2. Analyzing Traffic with Wireshark
3. Analyzing Traffic with Xplico

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	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	192.168.0.2	osboxes	osboxes.org
Security Onion	192.168.0.100	ndg	password123

1 Capturing Traffic with tcpdump

1. Click on the **Kali** graphic on the *topology page*.
2. Click anywhere within the *Kali* console window and press **Enter** to display the login prompt.
3. Enter `root` as the *username*. Click **Next**.
4. Enter `toor` as the *password*. Click **Sign In**.
5. Open the *Terminal* by clicking on the **Terminal** icon located on the left panel.

6. In the new *Terminal* window, type the command below to get familiarized with the *tcpdump* command options. Press Enter.

```
man tcpdump
```

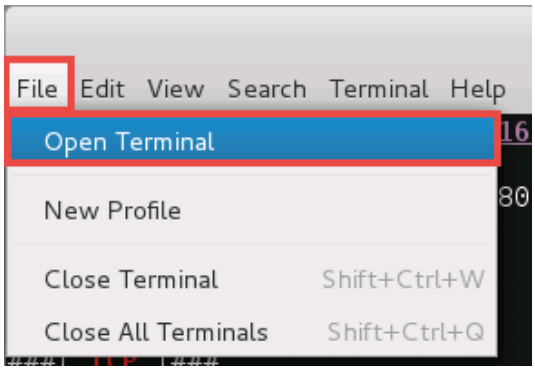
Press the **Spacebar** to skip to the next page or the **Enter** key to skip by each line. Press **Q** to quit at any given time and to receive the prompt back.

7. With *tcpdump*, collection of raw traffic is made possible which can then be used with applications such as *Wireshark* and *Xplico* to perform an analysis. Enter the command below to start capturing packets and saving them as a .pcap format which is acceptable by both *Wireshark* and *Xplico*.

```
tcpdump -i eth0 -s0 -w testdump.pcap
```

Leave the command running uninterrupted.

8. Launch a new **Terminal** by clicking the **File** drop-down menu option from the already existing *Terminal* window and select **Open Terminal**.



9. Generate some traffic with the *OWASP* VM by entering the command below in the new *Terminal* window.

```
smbclient -L 192.168.68.12
```

10. When prompted for *root's password*, type **`owaspbwa`**. Press **Enter**.

```
root@Kali2:~# smbclient -L 192.168.68.12
Enter root's password:
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.4.7]

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        apache          Disk      Apache Web Server Root
        tomcat          Disk      Tomcat6 Root
        var             Disk      /var
        etc             Disk      /etc
        usr             Disk      /usr
        owaspbwa        Disk      /owaspbwa
        IPC$            IPC       IPC Service (owaspbwa server (Samba, Ubuntu))
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.4.7]

        Server               Comment
        ---------            -------
        OWASPBWA             owaspbwa server (Samba, Ubuntu)

        Workgroup            Master
        ---------            -------
        WORKGROUP            OWASPBWA
```

11. Access the **owaspbwa** *SMB* share by typing the command below followed by pressing the **Enter** key.

```
smbclient \\\\192.168.68.12\\owaspbwa
```


12. When prompted for *root's password*, type **owaspbwa**. Press **Enter**.

```
root@Kali2:~# smbclient \\\\192.168.68.12\\owaspbwa
Enter root's password:
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.4.7]
smb: \>
```

13. Enter the **help** command.

```
help
```

14. List the files and directories in the current directory.

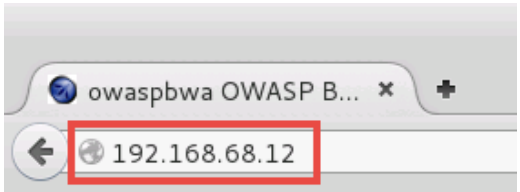
```
ls
```

15. Exit from the SMB client.

```
exit
```

16. Open the *Iceweasel* browser by clicking on the **Iceweasel** icon located on the left panel.

17. While viewing the *Iceweasel* browser, type **192.168.68.12** into the address field. Press the **Enter** key.



18. Once the page loads its contents, scroll downwards about halfway and click on the **Tiki Wiki** link.

19. Navigate back to the **Terminal** window where *tcpdump* is running.
20. Press **CTRL+C** to stop the *tcpdump* that is currently running.

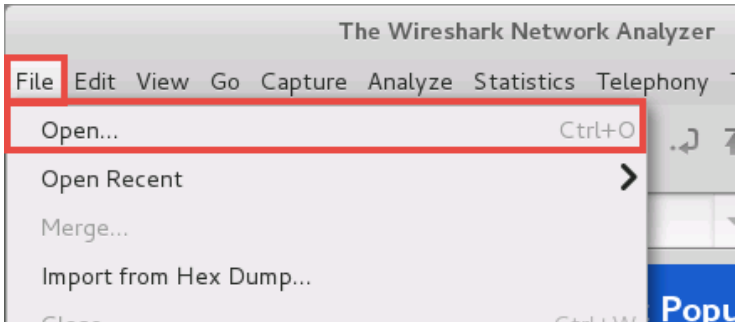
```
root@Kali2:~# tcpdump -i eth0 -s0 -w testdump.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 byt
es
^C1397 packets captured
1397 packets received by filter
0 packets dropped by kernel
```


2 Analyzing Traffic with Wireshark

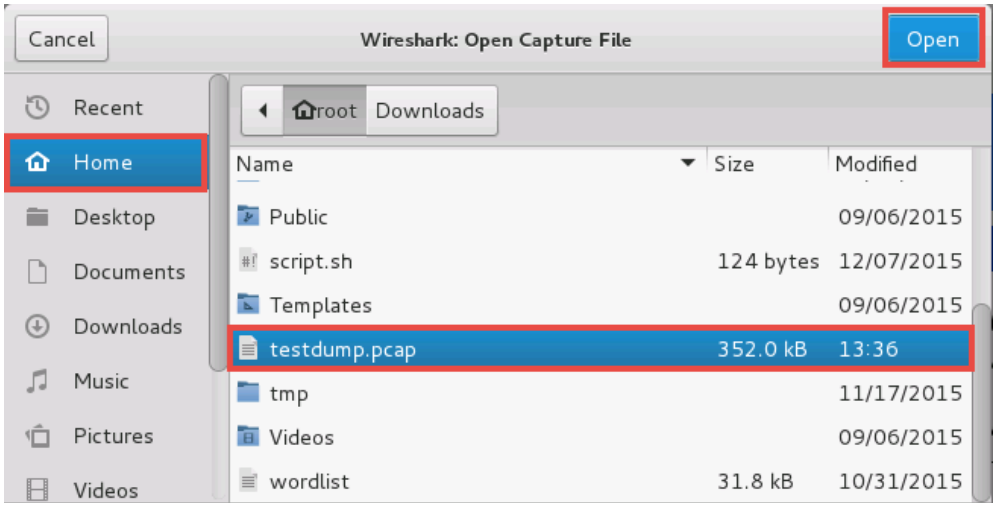
1. Launch the **Wireshark** application by typing the command below into the *Terminal*.

```
wireshark
```

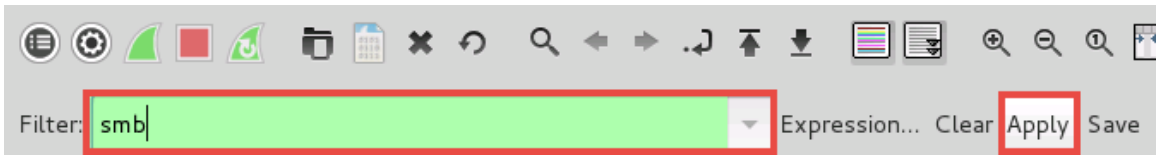
2. Click **OK** if prompted with an error message to continue.
3. If prompted with a warning message about running *Wireshark* as the root user, click **OK**.
4. In the *Wireshark* window, click on **File** in the top panel and select **Open**.



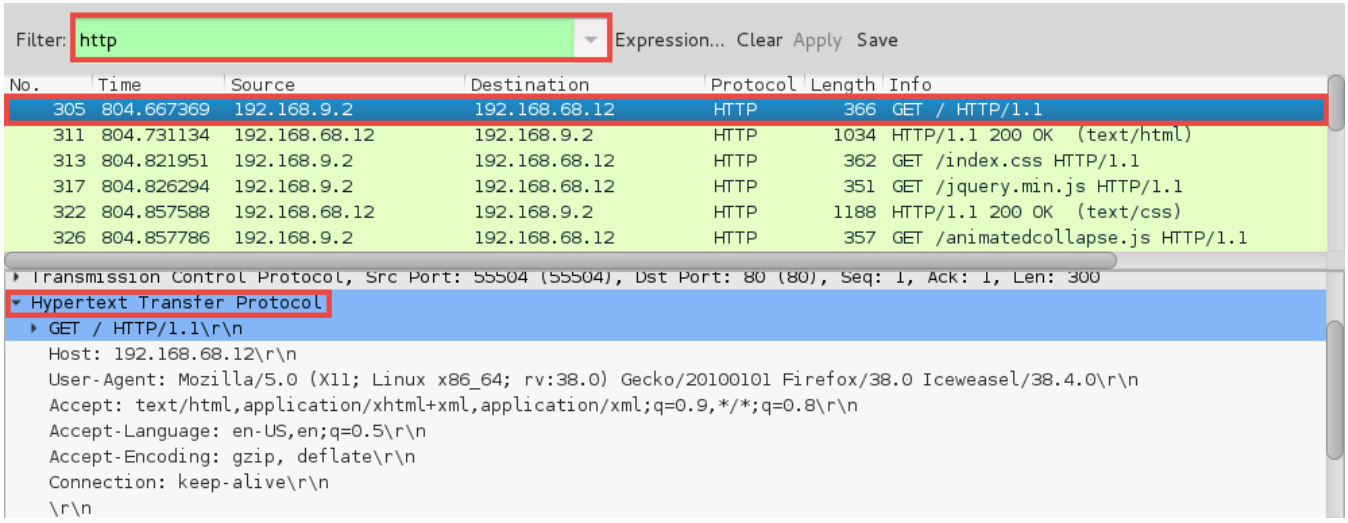
5. Click the **Home** icon located on the left panel.
6. Select **testdump.pcap** from the file list and click the **Open** button located top-right corner.



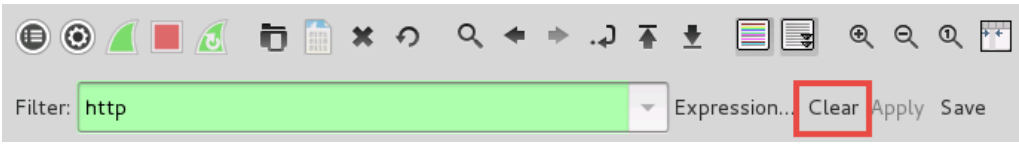
7. Narrow the captured traffic to only show SMB traffic by typing `smb` into the *Filter* text field and click **Apply**.



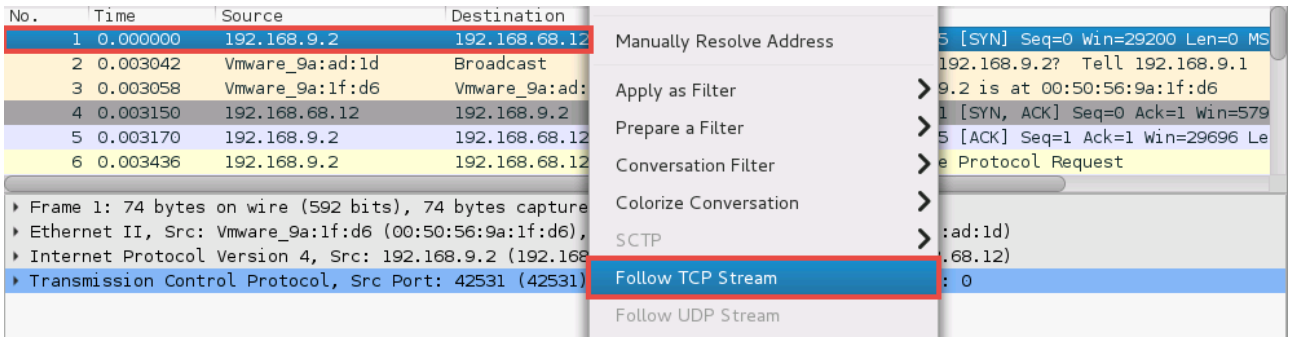
8. Analyze the captured *SMB* share traffic.
9. Filter the captured traffic with *HTTP*. Type `http` into the *Filter* text field and click **Apply**.
10. Select any **GET** packet from the list and analyze the frame in the bottom panel.
11. In the middle panel, expand the HTTP information by clicking on the arrow to the left of *Hypertext Transfer Protocol*.



12. In the top panel, click the **Clear** button next to the *Filter* field.



13. Right-click on the first TCP packet and click **Follow TCP Stream**.



14. Using the *Follow TCP Stream* feature, a conversation can be followed from start to finish given a TCP connection. Close the **Follow TCP Stream** window.
15. Close the **Wireshark** window.

3 Analyzing Traffic with Xplico

1. Navigate back to the **Terminal** and type the command below followed by pressing the **Enter** key.

```
xplico -m pcap -f testdump.pcap
```

```
root@Kali2:~# xplico -m pcap -f testdump.pcap
xplico v1.1.0
Internet Traffic Decoder (NFAT).
See http://www.xplico.org for more information.

Copyright 2007-2013 Gianluca Costa & Andrea de Franceschi and contributors.
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

This product includes GeoLite data created by MaxMind, available from http://www
.maxmind.com/.
Limits changed
Configuration file (/opt/xplico/cfg/xplico_cli.cfg) found!
```

Xplico has several modules for analyzing *pcap* file containing dissectors. The general *pcap* module will be used against the *testdump.pcap* file. Wait a few seconds until the prompt returns.

2. Enter the command below to change to the **/root/xdecode** directory.

```
cd xdecode
```

3. List the files and directories.

```
ls
```

Notice two directories, *arp* and *dig*. *Xplico* extracted an image in the *dig* directory and *ARP* messages in the *arp* directory. The *geomap….* files are for *Google Earth*.

4. For additional training, there are several *pcap* files in the */root/Downloads* directory for packet analysis.
5. Close the **Kali** PC viewer.

