ETHICAL HACKING V2
LAB SERIES

Lab 06: Network Analysis

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	4: Sniffing and Evasion
EC-Council CEH v10 Domain Modules	8: Sniffing
CompTIA Pentest+ Objectives	2.1: Given a scenario, conduct information gathering using appropriate techniques 4.2: Compare and contrast various use cases of tools
CompTIA All-In-One PenTest+ Chapters ISBN-13: 978-1260135947	3: Network Scanning and Enumeration 7: Network-Based Attacks

Contents

Introduction

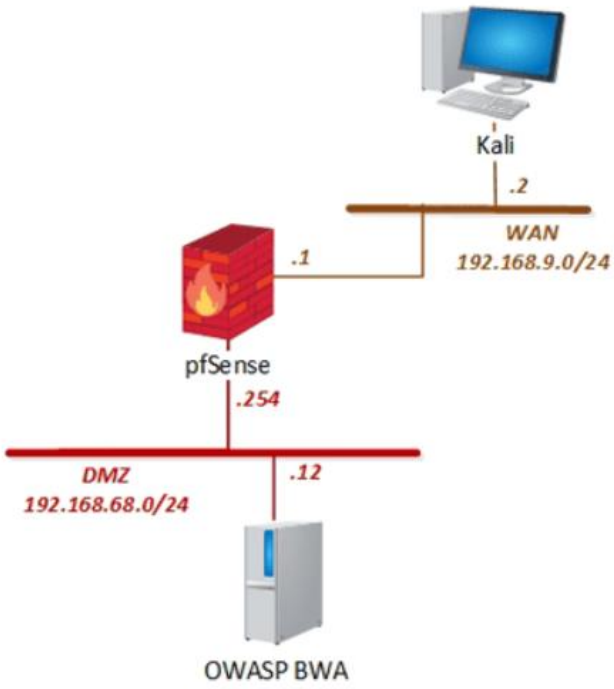
The ability to capture and analyze packets is an important skill when performing a security assessment or investigating a potential network breach. This lab will demonstrate how to capture and analyze network packets.

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

Pod Topology



Lab Settings

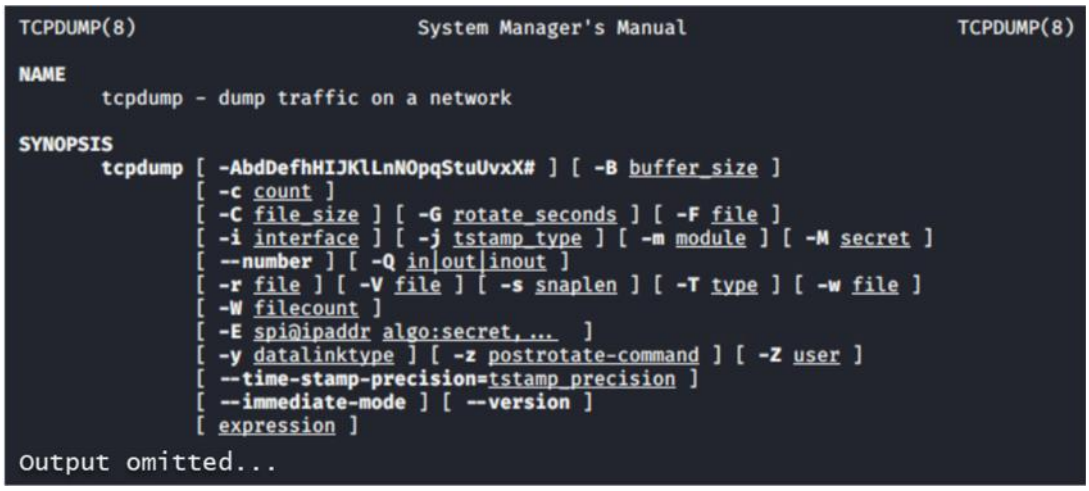
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

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

1 Capturing Traffic with tcpdump

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. Open a new terminal by clicking on the **Terminal** icon located at the top of the page, if the terminal is not already opened.
6. In the new *Terminal* window, type the command below to get familiarized with the *tcpdump* command options. Press **Enter**.

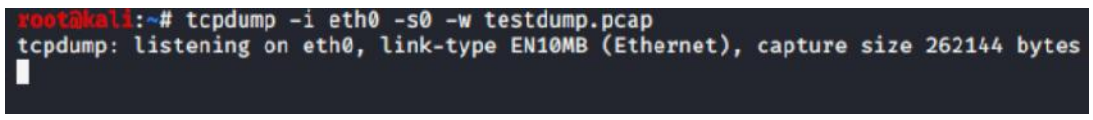
```
man tcpdump
```



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.

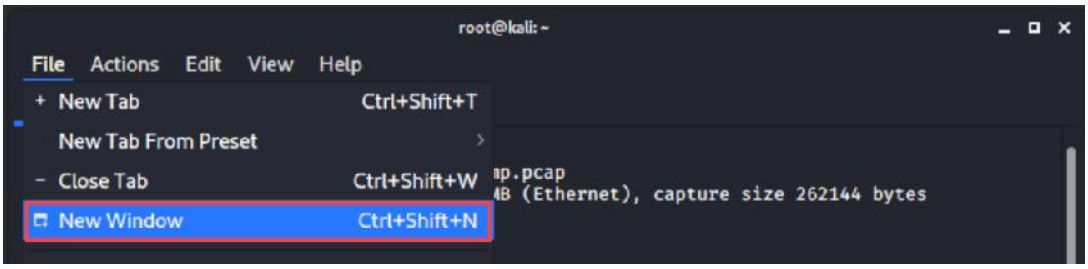
7. With *tcpdump*, collection of raw traffic is made possible, which can then be used with applications such as *Wireshark* and *Xplico* to perform an analysis. Enter the command below to start capturing packets and saving them as a .pcap format, which is acceptable by both *Wireshark* and *Xplico*.

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



Leave the command running uninterrupted.

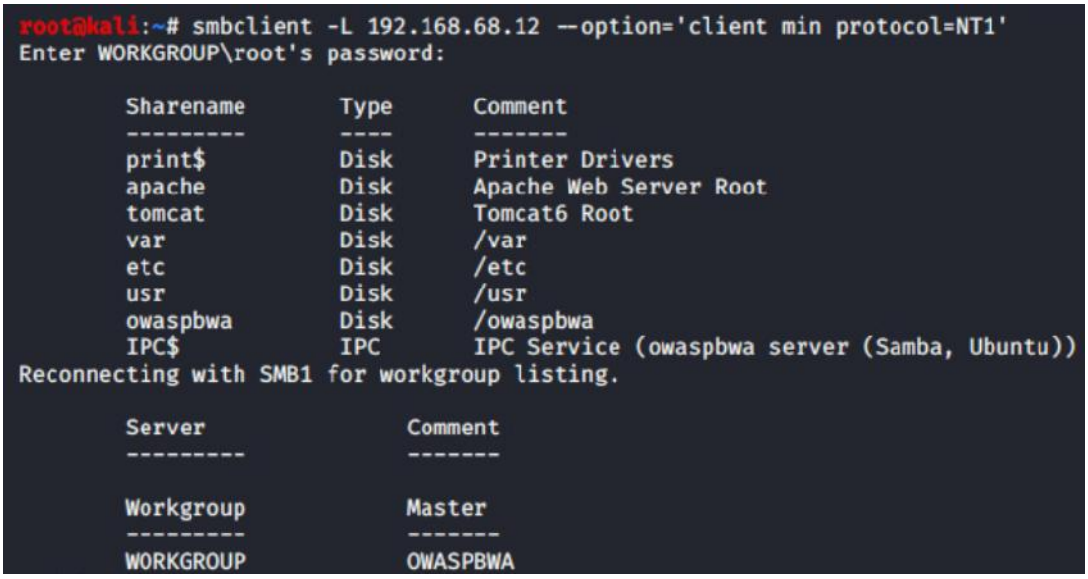
8. Launch a new **Terminal** by clicking the **File** dropdown menu option from the already existing *Terminal* window and select **New Window**.



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

```
smbclient -L 192.168.68.12 --option='client min protocol=NT1'
```

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



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

```
smbclient \\\\192.168.68.12\\owaspbwa --option='client min protocol=NT1'
```


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

```
root@kali:~# smbclient \\\\192.168.68.12\\owaspbwa --option='client min protocol=NT1'
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \>
```

13. Enter the **help** command.

```
help
```

```
smb: \> help
?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          del            deltree        dir
du             echo           exit           get            getfacl
geteas         hardlink       help           history        iosize
lcd            link           lock           lowercase      ls
l              mask           md             mget           mkdir
more           mput           newer          notify         open
posix          posix_encrypt  posix_open     posix_mkdir    posix_rmdir
posix_unlink   posix_whoami   print          prompt         put
pwd            q              queue          quit           readlink
rd             recurse        reget          rename         reput
rm             rmdir          showacls       setea          setmode
scopy          stat           symlink        tar            tarmode
timeout        translate      unlock         volume         vuid
wdel           logon          listconnect    showconnect    tcon
tdis           tid            utimes         logoff         ..
!
smb: \>
```

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

```
ls
```

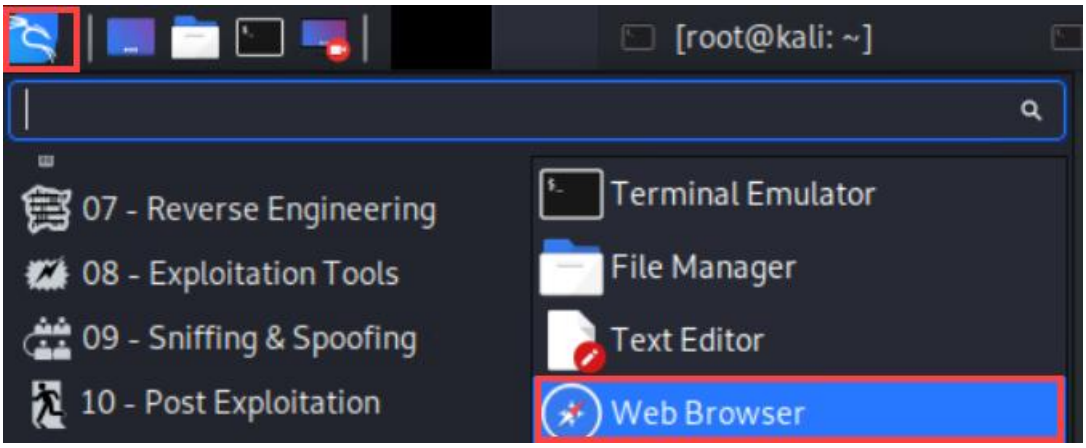
```
smb: \> ls
  .                                   D        0  Thu Jun 18 23:21:56 2015
  ..                                  D        0  Sun Jun 28 12:51:29 2020
  bwapp-git                           D        0  Thu May 14 22:35:28 2015
  owasp-zap-wave-svn                  D        0  Sun May  1 21:16:30 2011
  bodgeit-svn                         D        0  Tue May  5 21:06:19 2015
  railsgoat-git-1.2rc1                D        0  Mon Mar 17 01:45:18 2014
  WackoPicko-relative_urls-git        D        0  Tue May 17 21:32:16 2011
  webgoat.net-git                     D        0  Fri Mar 14 10:27:02 2014
  mutillidae-git                      D        0  Tue Jul 28 22:44:52 2015
  WebGoat-svn                         D        0  Fri Jun 29 15:39:36 2012
  MCIR-git                            D        0  Thu Jun 18 22:12:33 2015
  railsgoat-git-1.1.1                 D        0  Mon Mar 17 00:07:03 2014
  railsgoat-git                       D        0  Mon Mar 17 01:45:18 2014
  owasp-1-liner-git-modified-for-owaspbwa      D        0  Fri Feb  1 16:48:05 2013
Output omitted...
```

15. Exit from the SMB client.

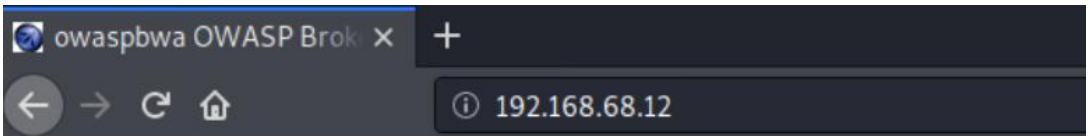
```
exit
```

```
smb: \> exit
root@kali:~#
```


16. Open the *Web Browser* by clicking on the **Application Menu > Web Browser** icon located on the left panel.

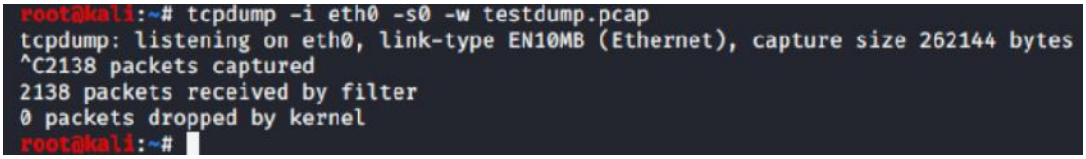


17. While viewing the *Mozilla Firefox* browser, type **`192.168.68.12`** into the address field. Press the **Enter** key.



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.

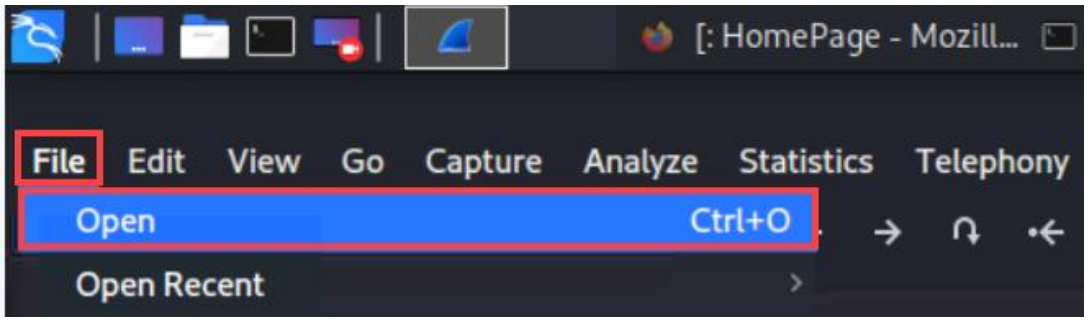


2 Analyzing Traffic with Wireshark

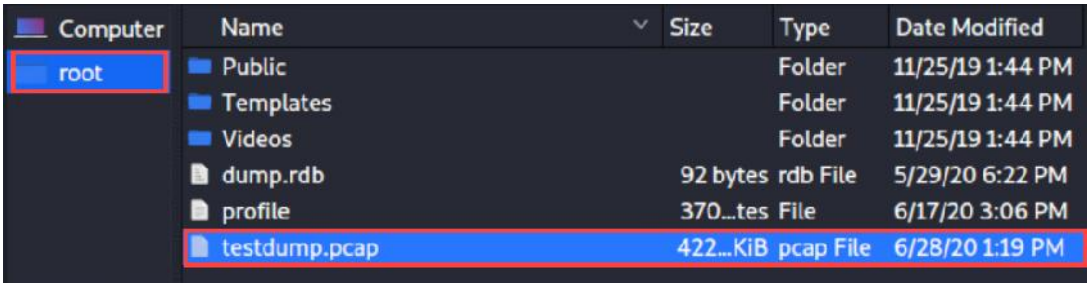
1. Launch the *Wireshark* application by typing the command below into the *Terminal*.

```
wireshark
```

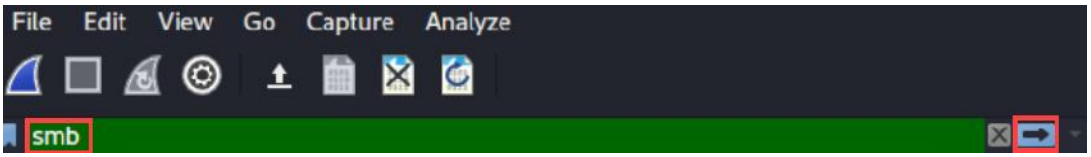
2. In the *Wireshark* window, click on **File** in the top panel and select **Open**.



3. Click the **root** folder located on the left panel.
4. Scroll down and select **testdump.pcap** from the file list and click the **Open** button located in the lower-right corner.

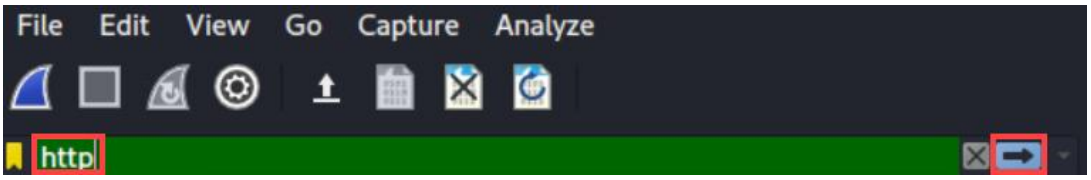


5. Narrow the captured traffic to only show SMB traffic by typing **`smb`** into the *Filter* text field and click the **Apply** icon.



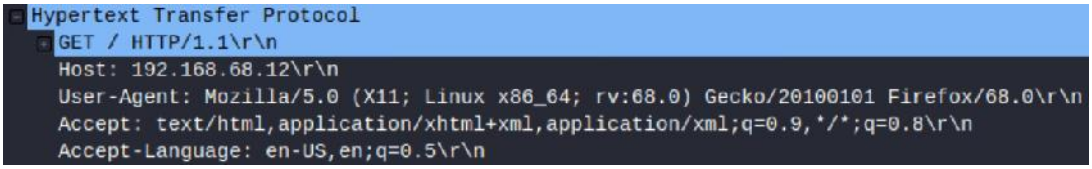
6. Analyze the captured *SMB* shared traffic.

7. Filter the captured traffic with *HTTP*. Type **`http`** into the *Filter* text field and click **Apply**.



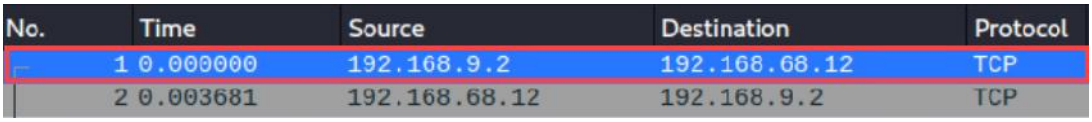
8. Select any **GET** packet from the list and analyze the frame in the bottom panel.

9. In the middle panel, expand the HTTP information by clicking on the arrow to the left of *Hypertext Transfer Protocol*.



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

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



12. 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.
13. Close the **Wireshark** window.
14. You may now end your reservation.

