**OBJECTIVES**

GENERAL

Develop offensive skills using a Kali Linux distribution

SPECIFIC:

Understand the concept of a CTF (Capture the Flag) exercise

Get different flags related with identification of a target

Launch different exploits to get confidential information of a target

This laboratory is intended to be developed**individually**.

Contents

PREPARING ENVIRONMENT1

Kali Linux Virtual Machine1

Server Zico2 Virtual Machine3

Kali Linux Introduction4

FLAG 1: Discover the IP of ZICO server virtual machine5

FLAG 2: Identify a vulnerability in the ZICO server6

FLAG 3: Identify all the resources in the ZICO server virtual machine7

# PREPARING ENVIRONMENT

### Kali Linux Virtual Machine

Download the Kali Linux distribution for Virtual Box from the following link

https://images.offensive-security.com/virtual-images/kali-linux-2018.4-vbox-i386.ova

Import the kali-linux-2018.4-vbox-i386.ova file in Virtual Box

Validate in network setting that “Host-Only Adapter” option stays selected

Start the virtual machine using credentials root/toor

### Server Zico2 Virtual Machine

Download the Server Zico from the following linkhttps://www.dropbox.com/s/dhidaehguuhyv9a/zico2.ova

Import the zico2.ova file in Virtual Box

Validate in network setting that “Host-only Adapter” option stays selected

Start the Virtual Machine

# Kali Linux Introduction

To guarantee that there it not copy in the answers of this laboratory, please change the terminal background using this procedure:

Open a terminal in Kali linux and execute the following command:

sudo apt install xfce4-terminal

After installation is done, open the xfce4-terminal application and open preferences -> appearance->Background image and select a file that you choose.

Background images should allow to read the text in the console. Some background images can be found here:https://www.pexels.com/search/background/

All the screenshots that you execute should have that image as background, and all commands should be executed over a xfce terminal.

Put here the screenshot of the terminal xfce4-terminal with the background image that you have selected:

Select one of the tools available in Kali Linux and documents its functionality mentioning: purpose of the tool and an example of the tool utility.

**Insert your answer here(Write at least 5 lines):**

# FLAG 1: Discover the IP of ZICO server virtual machine

We are in charge of attack a web server of an e-shop company called ZICO. Our attacker host (Kali Linux) isin the same network than ZICO serverbut we do not know the IP address of ZICO server, so our first task is to discover the ZICO server IP address.

Discover the IP of ZICO server virtual machine. Try with these commands:

netdiscover -r 192.168.56.0/24

nmap -sn 192.168.56.1-254

Note: 192.168.56.0/24 is equivalent to 192.168.56.1-254

Explain here what**netdiscover**does and what is the purpose of the argument**-r(Write at least 3 lines):**

Explain here what**nmap**does and what is the purpose of the arguments**s**and**n(Write at least 3 lines):**

Put here the screenshot of the execution of netdiscover:

Put here the screenshot of the execution of nmap:

With the previous commands you discovered the hosts in the network 192.168.56.0, now for each host discovered do a more exhaustive scanning using the command:

nmap --top-ports 10 --open -Pn -n**192.168.56.X**

Explain here what**nmap**does and what is the purpose of the arguments --top-ports 10, --open, -Pn, -n**(Write at least 5 lines):**

Put here the screenshots of the execution of nmap for all the hosts you found**(You should had discovered at least 2 hosts):**

As our target probably is a web server, it has the port TCP/80 opened, so try in a browser the IPs that you found which have the port TCP/80 opened. Try all the IPs until you find the webpage of ZICO’s shop:

Put here the screenshot of ZICO’s shop opened from a browser (Mozilla/Chrome):

What have weachieved until now? We have discovered hosts in our network, and we have identified the address of our target (ZICO’s shop). The ZICO IP was the**first flag**!

# FLAG 2: Identify a vulnerability in the ZICO server

Now that we have discovered the IP address of ZICO server, let’s find a vulnerability. The CMS (Content Management System) behind Zico has a vulnerability consisting in the access to files using URL parameters. This is evident when accessing to**ip-zico/view.php?page=tools.html.**

Using this vulnerability is possible to access to the passwd file

Replace this screenshot with yours:

Explain the meaning of the file passwd**(Write at least 5 lines):**

How many users do ZICO has?, How many users groups ZICO has?, Passwords are accessible?

Do a research about how this vulnerability (Operative System Command Injection) can be mitigated**(Write at least 5 lines):**

What have we achieved until now? We have discovered that ZICO has a vulnerability called**Operative System Command Injection**and we are able to read any file from the operative system. The recovery of the passwd file was the**Second flag**!

# FLAG 3: Identify all the resources in the ZICO server virtual machine

Run a web content scanner to discover the resources that ZICO server offers. Try with command:

dirbhttp://192.168.56.101/usr/share/dirb/wordlists/common.txt

Explain here what**dirb**does and what for a wordlist is used**(Write at least 5 lines):**

Replace this screenshot with yours

DIRC help us to identify the URLS that ZICO server may have. So, TRY to access to them through a web server and see if you find someone interesting.

Put here some screenshots you have tried**(at least 3 screenshots):**

Actually, there is one service that may be interesting for us, it is called phpLiteAdmin. Try to login in phpLiteAdmin using different passwords. At last try with the most obvious password: “admin”

Replace this screenshot with yours

What have we achieved until now? We have discovered that ZICO has a database manager application called**PhpLiteAdmin**and we were able to get in and even explore the database. The access to this database was the**Third flag**!

If you get to this point you have captured the first three flags of the CTF.**Congratulations!**