

Laboratorio N° 1 – Ethical Hacking

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**.

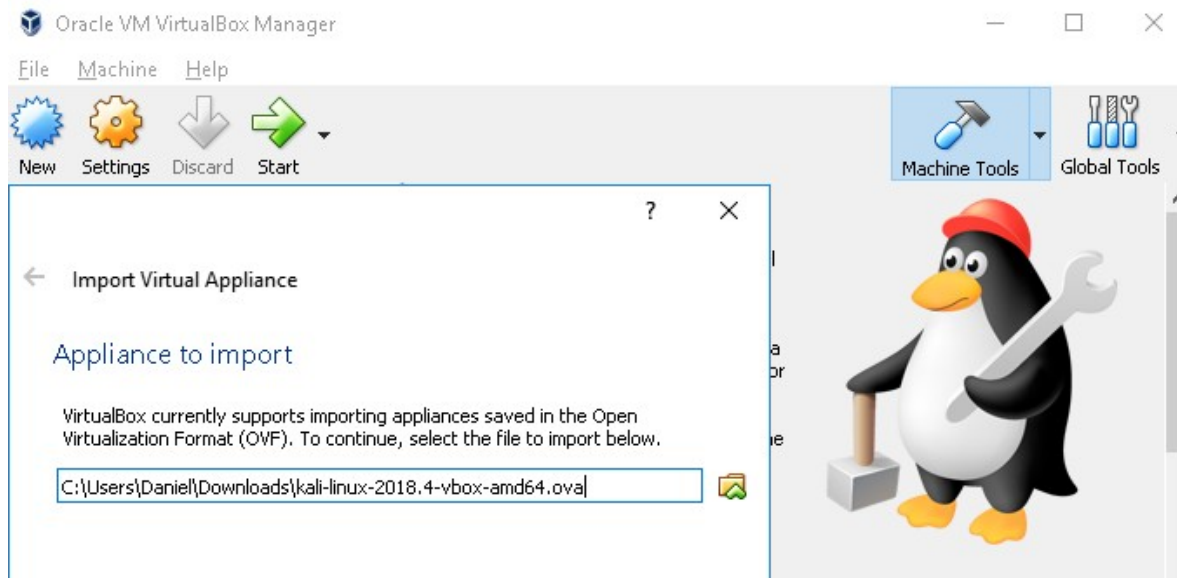
Contents

PREPARING ENVIRONMENT.....	1
Kali Linux Virtual Machine.....	1
Server Zico2 Virtual Machine.....	3
Kali Linux Introduction.....	4
FLAG 1: Discover the IP of ZICO server virtual machine.....	5
FLAG 2: Identify a vulnerability in the ZICO server.....	6
FLAG 3: Identify all the resources in the ZICO server virtual machine.....	7

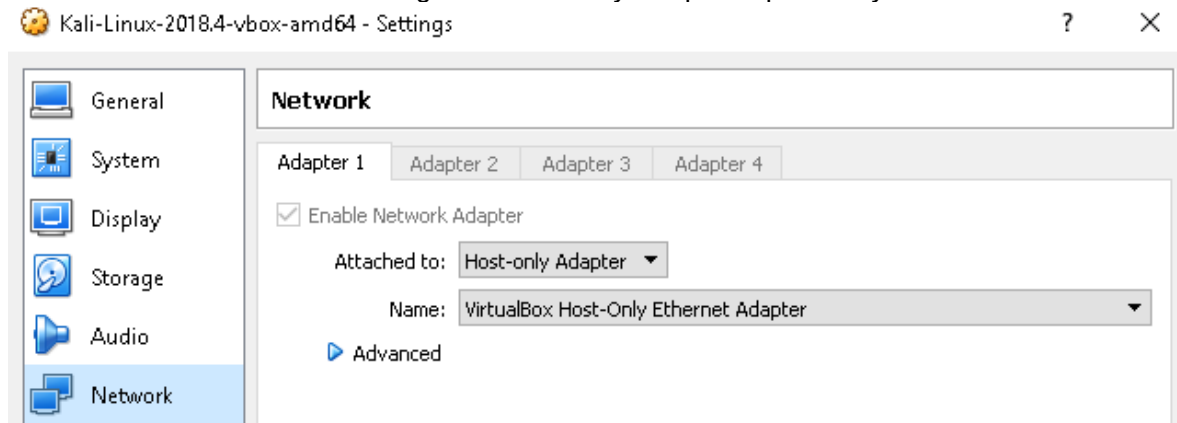
PREPARING ENVIRONMENT

Kali Linux Virtual Machine

1. 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>
2. Import the kali-linux-2018.4-vbox-i386.ova file in Virtual Box

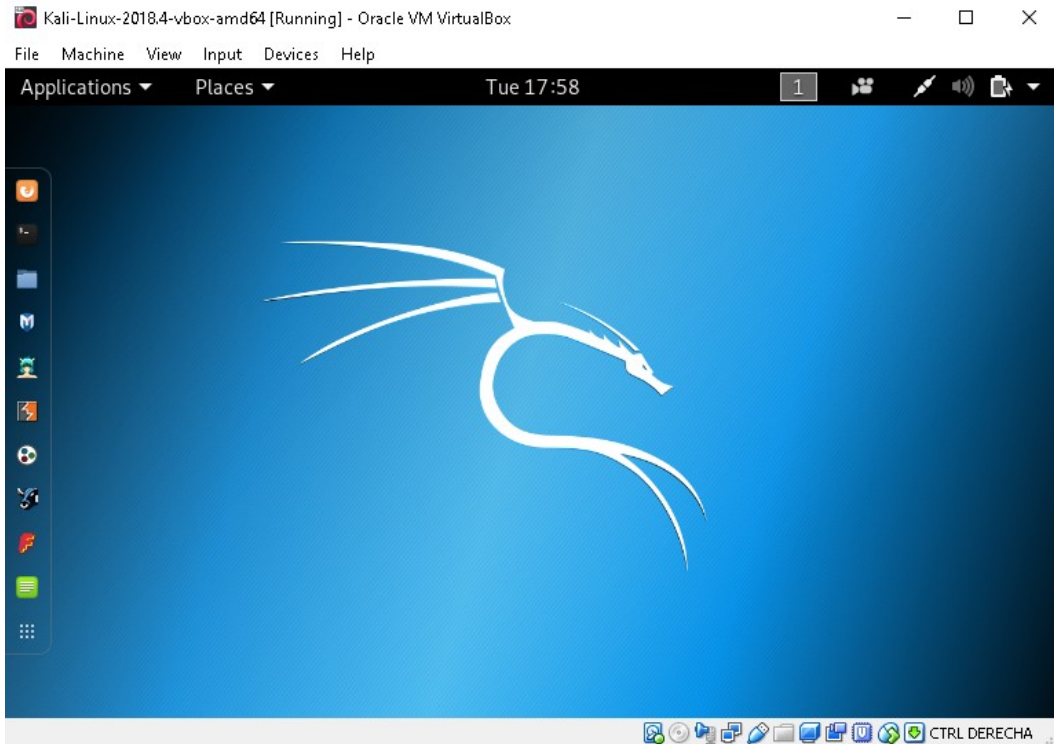


3. Validate in network setting that “Host-Only Adapter” option stays selected



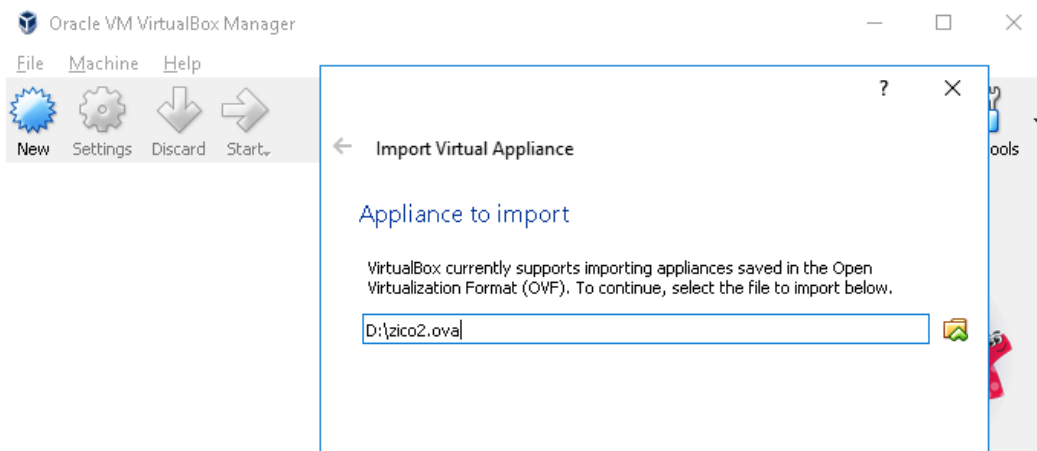
4. Start the virtual machine using credentials root/toor

Laboratorio N° 1 – Ethical Hacking



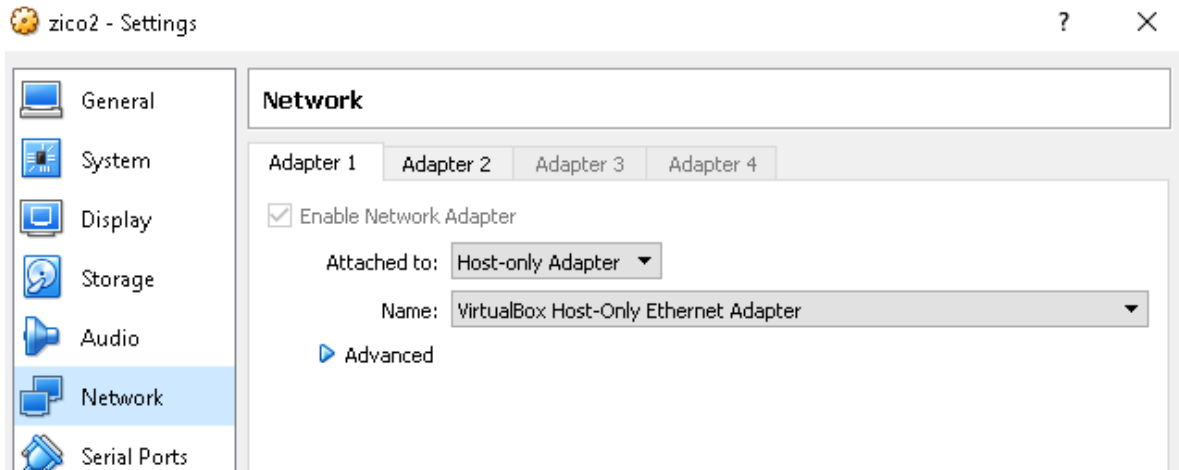
Server Zico2 Virtual Machine

1. Download the Server Zico from the following link
<https://www.dropbox.com/s/dhidaehguuhyv9a/zico2.ova>
2. Import the zico2.ova file in Virtual Box



3. Validate in network setting that "Host-only Adapter" option stays selected

Laboratorio N° 1 – Ethical Hacking



4. Start the Virtual Machine



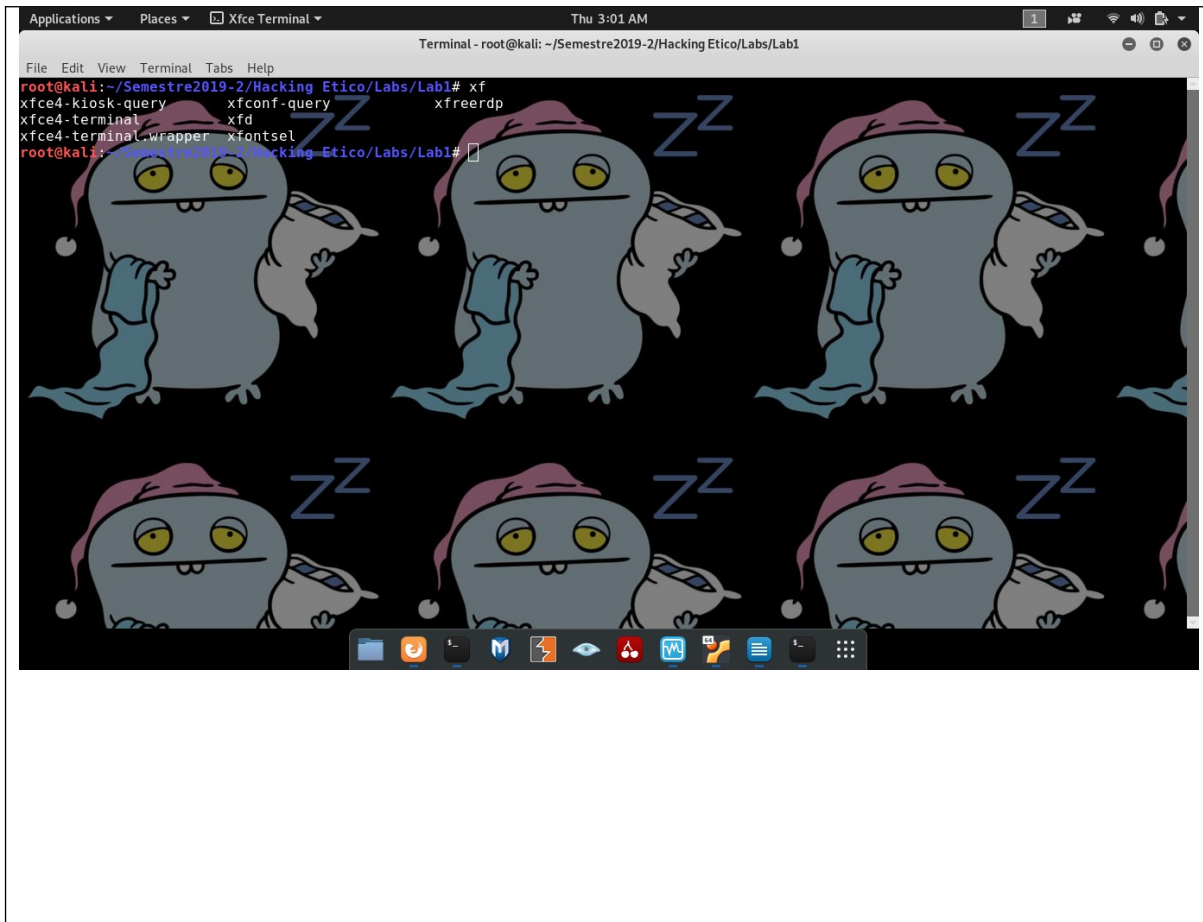
Kali Linux Introduction

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:
 - o `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.

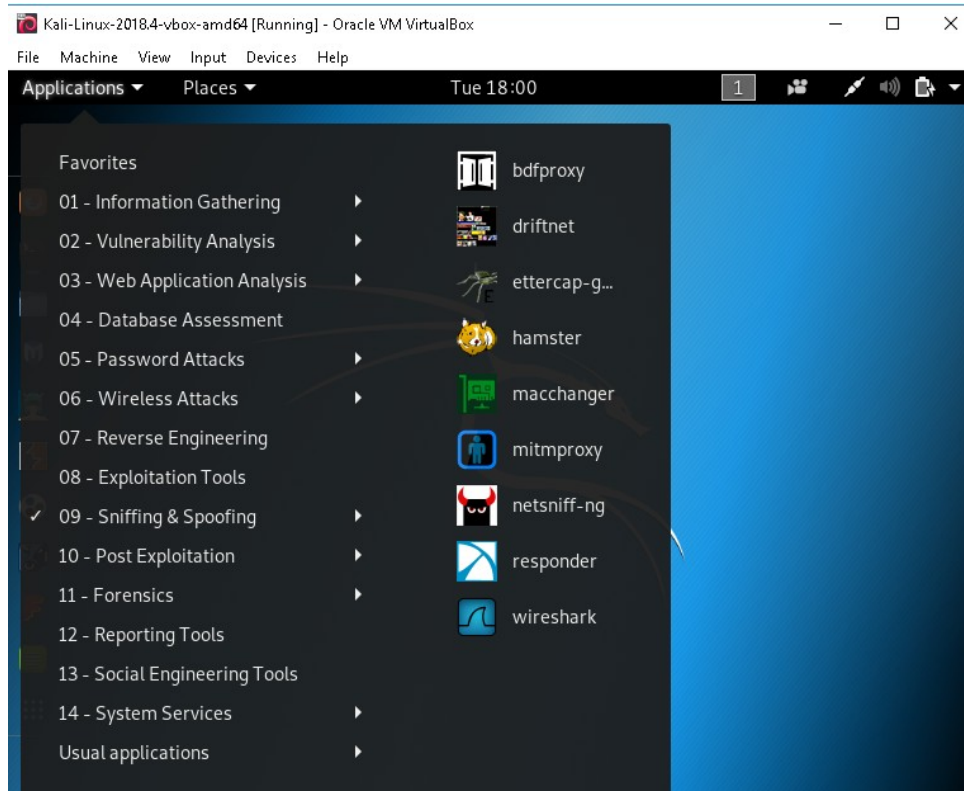
Put here the screenshot of the terminal xfce4-terminal with the background image that you have selected:

Laboratorio N° 1 – Ethical Hacking



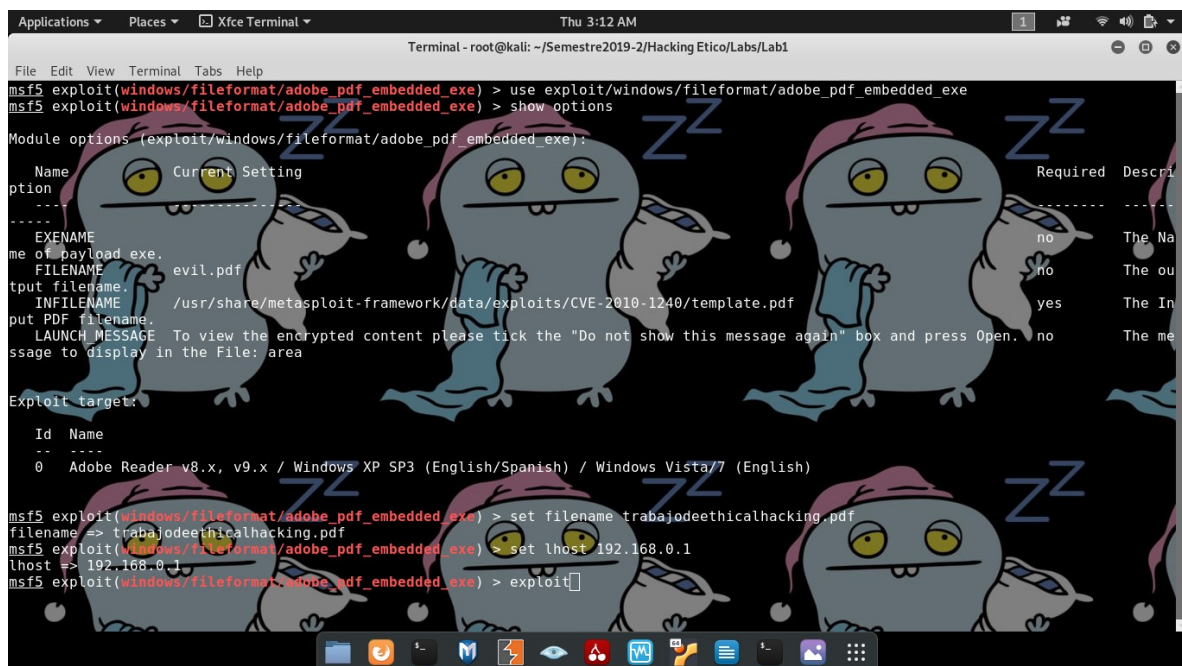
Select one of the tools available in Kali Linux and documents its functionality mentioning: purpose of the tool and an example of the tool utility.

Laboratorio N° 1 – Ethical Hacking



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

Para este trabajo escogí estratégicamente a metasploit framework, es un framework diseñado para hacer test de penetración , hoy en día dispone mas de 1900 exploit y mas de 500 payloads , además, permite interactuar con herramientas externas , como nmap, por ejemplo, seleccionaré un exploit viejo de pdf para windows, llenaré las opciones que tiene y crearé el archivo



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) is **in the same network than ZICO server** but 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:

- a. `netdiscover -r 192.168.56.0/24`
- b. `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):

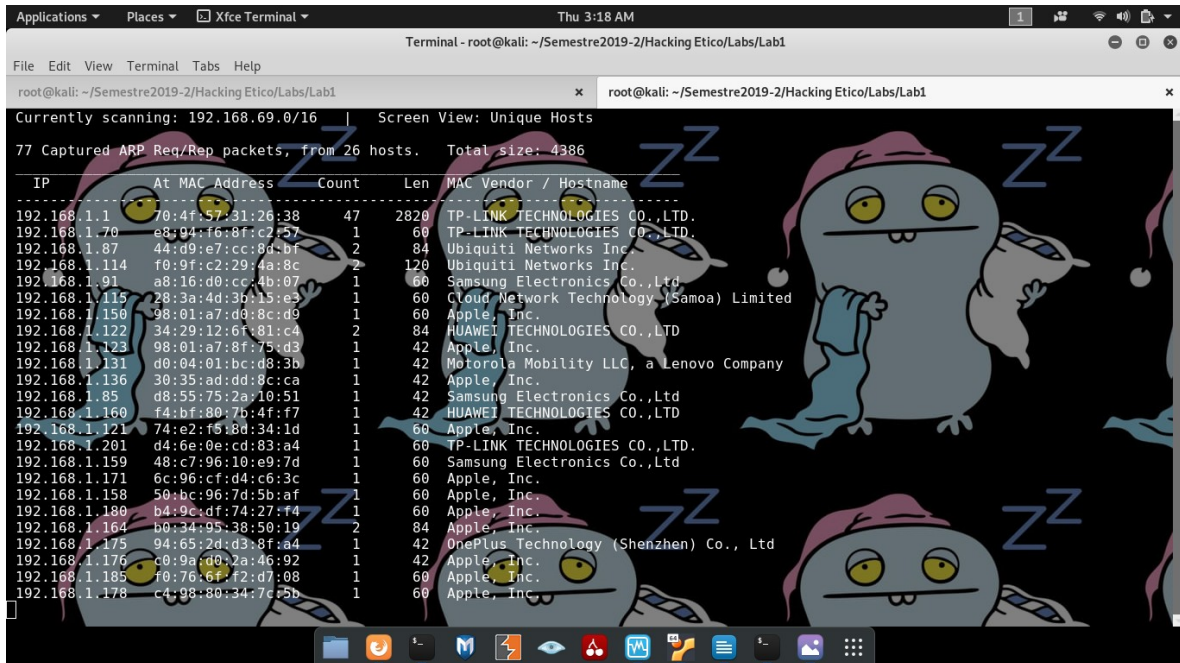
Tanto netdiscover como Nmap son herramientas para hacer escaneo de redes , el flag -r en netdiscover refiere al rango de ips el cual el usuario desee escanear

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

el flag -s hace referencia a seleccionar una fila, el -n lo dejo de tarea para preguntar mañana

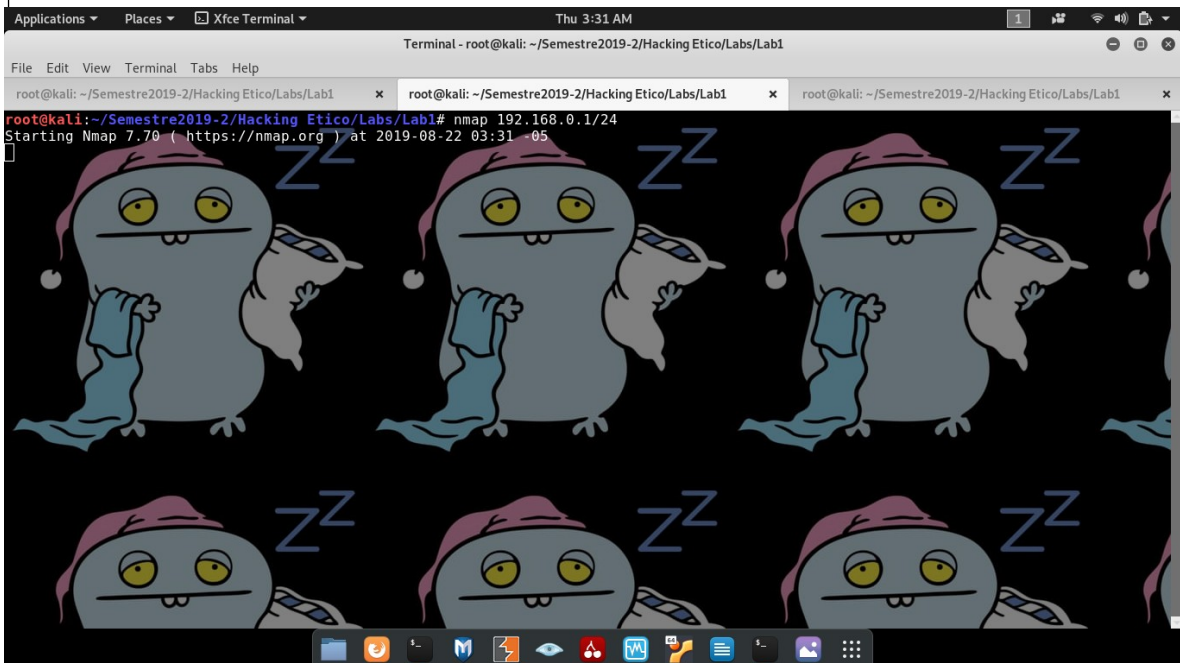
Put here the screenshot of the execution of netdiscover:

Laboratorio N° 1 – Ethical Hacking



```
Applications ▾ Places ▾ Xfce Terminal ▾ Thu 3:18 AM 1
Terminal - root@kali: ~/Semestre2019-2/Hacking Etico/Labs/Lab1
root@kali: ~/Semestre2019-2/Hacking Etico/Labs/Lab1
Currently scanning: 192.168.69.0/16 | Screen View: Unique Hosts
77 Captured ARP Req/Rep packets, from 26 hosts. Total size: 4386
IP At MAC Address Count Len MAC Vendor / Hostname
-----
192.168.1.1 70:4f:57:31:26:38 47 2820 TP-LINK TECHNOLOGIES CO.,LTD.
192.168.1.70 e8:04:f6:8f:c2:57 1 60 TP-LINK TECHNOLOGIES CO.,LTD.
192.168.1.87 44:d9:e7:cc:8d:bf 2 84 Ubiquiti Networks Inc.
192.168.1.114 f0:9f:c2:29:4a:8c 2 120 Ubiquiti Networks Inc.
192.168.1.91 a8:16:d0:cc:4b:07 1 60 Samsung Electronics Co.,Ltd
192.168.1.115 28:3a:4d:3b:15:e3 1 60 Cloud Network Technology (Samoa) Limited
192.168.1.150 98:01:a7:d0:8c:d9 1 60 Apple, Inc.
192.168.1.122 34:29:12:6f:81:c4 2 84 HUAWEI TECHNOLOGIES CO.,LTD
192.168.1.123 98:01:a7:8f:75:d3 1 42 Apple, Inc.
192.168.1.131 d0:04:01:bc:d8:3b 1 42 Motorola Mobility LLC, a Lenovo Company
192.168.1.136 30:35:ad:dd:8c:ca 1 42 Apple, Inc.
192.168.1.85 d8:55:75:2a:10:51 1 42 Samsung Electronics Co.,Ltd
192.168.1.160 f4:bf:80:7b:4f:f7 1 42 HUAWEI TECHNOLOGIES CO.,LTD
192.168.1.121 74:e2:f5:8d:34:1d 1 60 Apple, Inc.
192.168.1.201 d4:6e:0e:cd:83:a4 1 60 TP-LINK TECHNOLOGIES CO.,LTD.
192.168.1.159 48:c7:96:10:e9:7d 1 60 Samsung Electronics Co.,Ltd
192.168.1.171 6c:96:cf:d4:c6:3c 1 60 Apple, Inc.
192.168.1.158 50:bc:96:7d:5b:af 1 60 Apple, Inc.
192.168.1.180 b4:9c:df:74:27:f4 1 60 Apple, Inc.
192.168.1.164 b0:34:95:38:50:19 2 84 Apple, Inc.
192.168.1.175 94:65:2d:d3:8f:a4 1 42 OnePlus Technology (Shenzhen) Co., Ltd
192.168.1.176 c0:9a:d0:2a:46:92 1 42 Apple, Inc.
192.168.1.185 f0:76:6f:f2:d7:08 1 60 Apple, Inc.
192.168.1.178 c4:98:80:34:7c:5b 1 60 Apple, Inc.
```

Put here the screenshot of the execution of nmap:



```
Applications ▾ Places ▾ Xfce Terminal ▾ Thu 3:31 AM 1
Terminal - root@kali: ~/Semestre2019-2/Hacking Etico/Labs/Lab1
root@kali: ~/Semestre2019-2/Hacking Etico/Labs/Lab1
root@kali:~/Semestre2019-2/Hacking Etico/Labs/Lab1# nmap 192.168.0.1/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-22 03:31 -05
```


Laboratorio N° 1 – Ethical Hacking

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:

a. `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):**

hay una cantidad de puertos que son importantes, como el 80, o el 22, pues, si intentara escanear todos los puertos, el algoritmo sería muy ruidoso y muy demorado, por lo tanto, la cantidad de to-ports lo que hace es escanear los puertos importantes, y el argumento que recibe es la cantidad, por ejemplo --top-ports 10 lo que hace es escanear 10 puertos importantes

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

Lo hice con usted profe, en su oficina

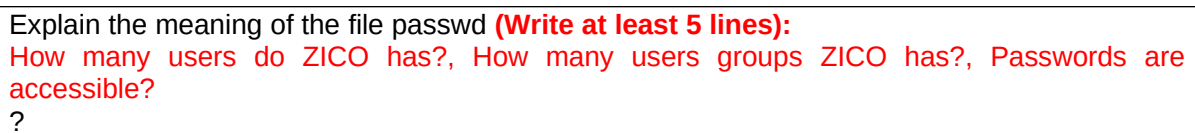
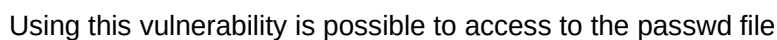
As our target probably is a web server, it has the port TCP/80 opened, so try in a browser the IPs that you found which have the port TCP/80 opened. Try all the IPs until you find the webpage of ZICO's shop:

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

What have we achieved 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**.



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:

a) dirb <http://192.168.56.101> /usr/share/dirb/wordlists/common.txt

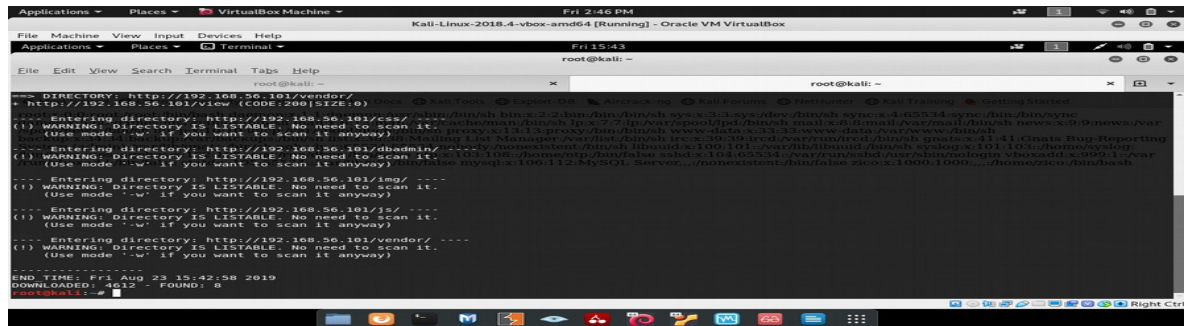
Explain here what **dirb** does and what for a wordlist is used **(Write at least 5 lines):**

Dirb es un escaneador de contenido de red, lo que hace es buscar por objetos que estén así sea escondidos enviando requests y analizando las respuestas de cada request, todo esto, funciona bajo un ataque de diccionario

un ataque de diccionario lo que hace es recibir un archivo txt que contiene todas las posibles respuestas o una cantidad grande , e intentar una por una

Laboratorio N° 1 – Ethical Hacking

Replace this screenshot with yours

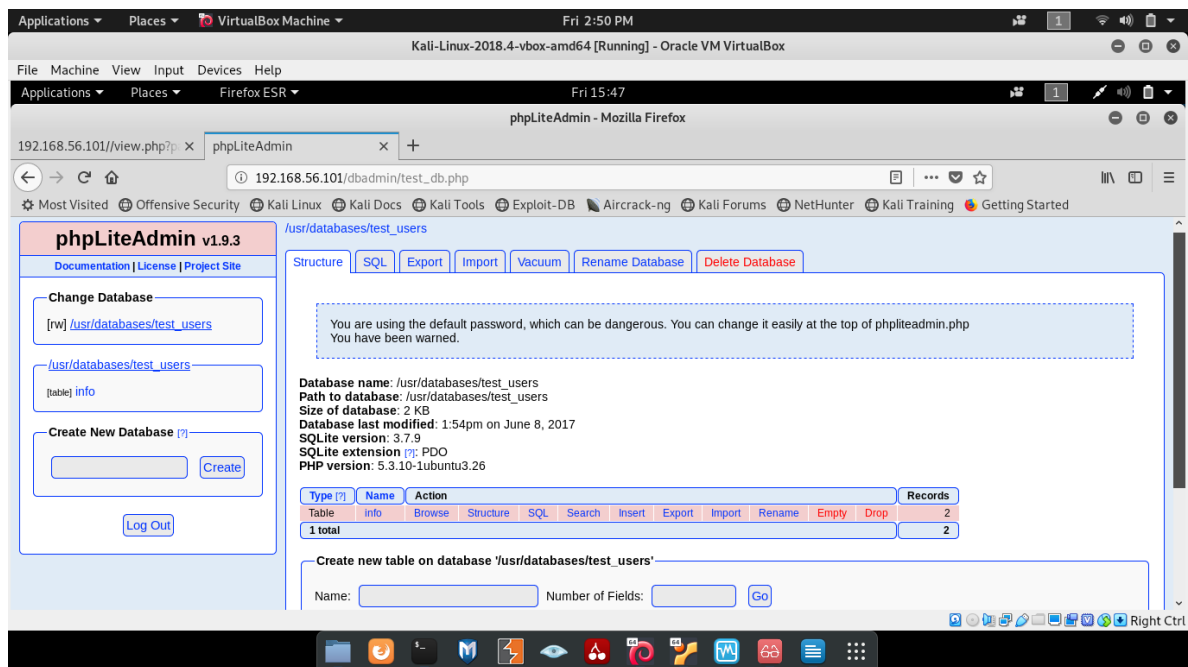


```
root@kali: ~  
--s DIRECTORY: http://192.168.56.101/vendor/ --s  
+ http://192.168.56.101/view (CODE:200) [SIZE:0]  
---- Entering directory: http://192.168.56.101/css/ ----  
(i) WARNING: Directory is LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)  
---- Entering directory: http://192.168.56.101/js/ ----  
(i) WARNING: Directory is LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)  
---- Entering directory: http://192.168.56.101/img/ ----  
(i) WARNING: Directory is LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)  
---- Entering directory: http://192.168.56.101/vendor/ ----  
(i) WARNING: Directory is LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)  
-----  
END TIME: Fri Aug 23 15:42:58 2019  
DOWNLOADED: 4612 - FOUND: 8
```

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)**:

Laboratorio N° 1 – Ethical Hacking



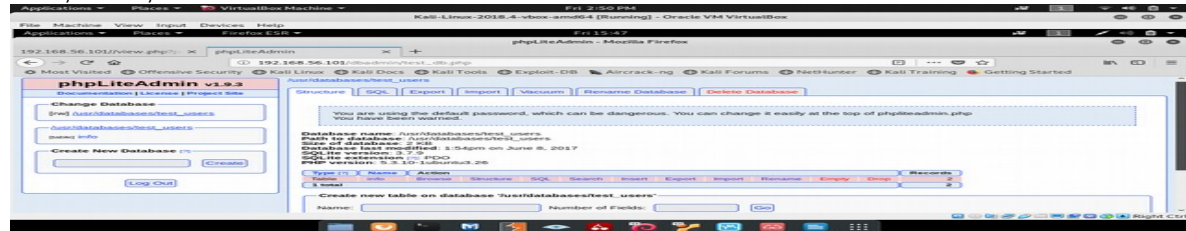
intenté con password, hola, y admin

Laboratorio N° 1 – Ethical Hacking

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

hola, holax, admin



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!**