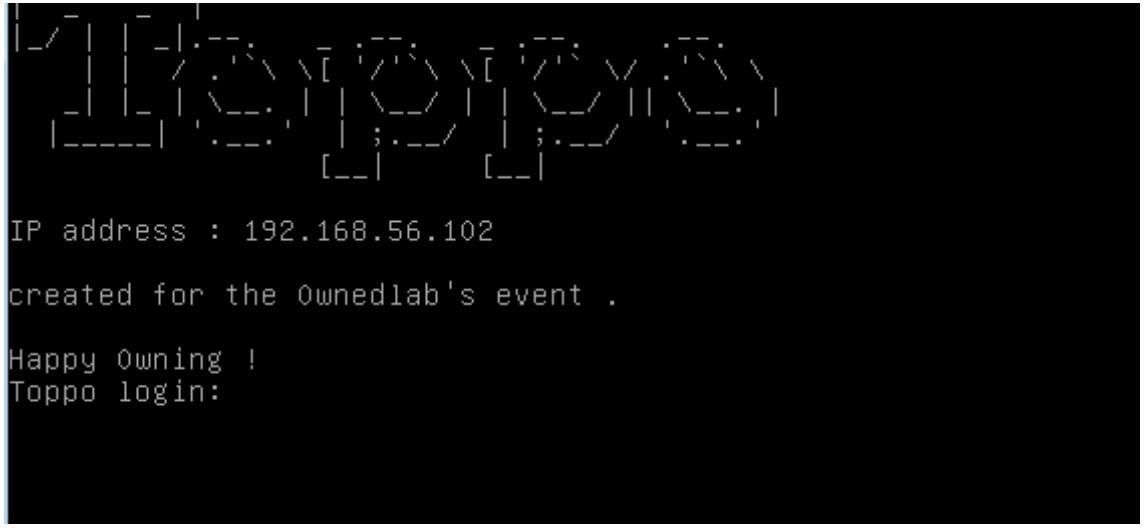
Toppo:1 | Vulnhub Walkthrough

Dot Dot Slash Follow
Aug 16, 2018 · 3 min read

Simple or tough, if the challenge has some takeaway lessons, I believe its worth my time. Toppo is a simple but great Vulnhub machine made by Hadi Mene. Toppo is one of the best challenges for one to start with Vulnhub machines.

> *Level:* Beginner

On bootup, Toppo displays its own IP address saving the trouble to use ***netdiscover*** or ***arp-scan.***



Enumeration and First Blood

Nmap scans identified a website running on port 80. Apparently there was a blog running on it.

```
root@kali:~# nmap -p- -Pn -n 192.168.56.102
Starting Nmap 7.70 ( https://nmap.org ) at 2018-08-13 12:17 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00016s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
60642/tcp open  unknown
MAC Address: 08:00:27:37:2F:A7 (Oracle VirtualBox virtual NIC)
```

```
Nmap done: 1 IP address (1 host up) scanned in 1.89 seconds
```

```
root@kali:~# nmap -p22,80,111,60642 -A  -Pn -n 192.168.56.102
Starting Nmap 7.70 ( https://nmap.org ) at 2018-08-13 12:17 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00073s latency).

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          49614/udp  status
|_  100024  1          60642/tcp  status
60642/tcp open  status  1 (RPC #100024)
MAC Address: 08:00:27:37:2F:A7 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and
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
```

Nmap detailed scan

Blog on port 80

Launching ***nikto*** or ***dirb*** was more than adequate to find the first hint. Inside the admin folder in notes.txt, was a password. But there was no username and this should be some SSH credentials. I had to do a bit of guesswork to find the username, I tried toppo, admin then finally ted to make my initial compromise.

SSH credentials for ted user stored in a file

ssh access

G0tmi1k's privilege escalation cheat sheet is one of best write-ups on basic Linux privilege escalation and it helped me to dig out the root. There is a section in his material that covers sticky bits, SUID and SGID.

SUID and SGID files

SUID (Set User ID) is a permission bit that can be set on an executable allowing any one to run the executable with the owner's permissions. That means if a user bob has set SUID bit on his executable, another user alice can run it with bob's privileges. Similarly SGID (Set Group ID) bit allows the executable to run with the groups privileges.On the first look , this might sound risky.

But SUID and SGID files are very important to the way Linux operates. Many legitimate Linux programs require these permissions. If SUID and SGID permissions are provided to many known binaries listed below, it could result in privilege escalation. You can find more details on pentestlab.blog.

- Nmap

- Vim
- find
- Bash
- More
- Less
- Nano
- cp

Path to root

We can use the below command to find SUID and SGID files.

```
find / -perm -g=s -o -perm -4000 ! -type l -maxdepth 3 -exec ls -ld
{} \; 2>/dev/null
```

There are two files in the binaries with SUID permissions, which are of special interest. Both of them can be exploited to gain root privileges.

1. /usr/bin/python2.7
2. /usr/bin/mawk

Privilege escalation using python

> *If you closely observed above screenshots, you can see that I was not able to invoke bash with SUID privileges. Bash ignores SUID/SGID bit and drops shell to current user privileges.We need to some other shell like sh or ksh for exploitation*

Overall a fun machine! If you are new to security or want to get started, Toppo is the challenge for you.

Hacking Ctf Walkthrough Vulnhub Beginner

60 claps

WRITTEN BY

Dot Dot Slash

Stay hungry. Stay foolish.

Follow

egghunter

Blog on security.

Follow

Write the first response

More From Medium

Related reads

Abusing autoresponders and email bounces

Related reads

What to Do if Your WordPress Website Was Hacked

Related reads

Redis Unauthorized Access Vulnerability Simulation |

Inti De Ceukelaire in...
Feb 21 · 6 min read

452

HostPapa
Oct 16, 2018 · 11 min read

42

Victor Zhu

Victor Zhu
Sep 11, 2018 · 6 min read

117