# Introduction To Hack the Box

Workshop 4 - 10/11/2022

# Kali Linux

To save time in future workshops, and to provide you with a suitable toolkit, we recommend installing a kali linux VM. Kali linux is a debian distribution designed for penetration testing. If you don't have a VM framework, we recommend either VMware or Virtualbox, this will be the program you use to launch the Virtual Machine. After you have your VM software installed

1. Head to https://www.kali.org/get-kali/ and select Virtual Machines
2. Select your VM software and press the download button
3. Once this download is complete, extract the file
4. Launch your VM software and press Add, then select the Machine image we just extracted
5. Adjust the settings to suit your system
6. Once installed, boot up the VM
7. Login to Kali using the Username & Password: kali / kali

Unlike Most VMs Kali is a very specialised tool, for this reason we recommend that you don't use tools that you are not familiar with, as many of them can be unsafe if used incorrectly. If you want to learn more about kali and it's tools feel free to message the society discord and we'll try to get back to you!

# Hack The Box

---

Run Kali Linux OS and go to https://www.hackthebox.com/

Create a new account and then verify

Navigate to Labs then Starting Point and find the Meow box

# Connecting

---

Download the VPN file

Open a terminal and navigate to Downloads

Run `sudo ovpn starting_point_username.ovpn`

# Connecting

---

Spawn the Machine and then check its connected by running `ping {ip_address}`

# Enumeration

---

Using NMap on the ip address will show what services it is running

A broad search such as nmap {ip_address} -p0-100 -T(5 or 4)

This should reveal the ports in use

# Service Detection

---

Using nmaps service detection will reveal the service its running

```
Nmap {ip_address} -pX -sV
```

Searching the service online should reveal information about how to interact with it

Eg `telnet {ip_address}`

# Foothold

---

Once you have access to the service you will be able to navigate the system and find the flag

This is done using `cd` and `ls` commands as you use in your own filesystem

# Payload

---

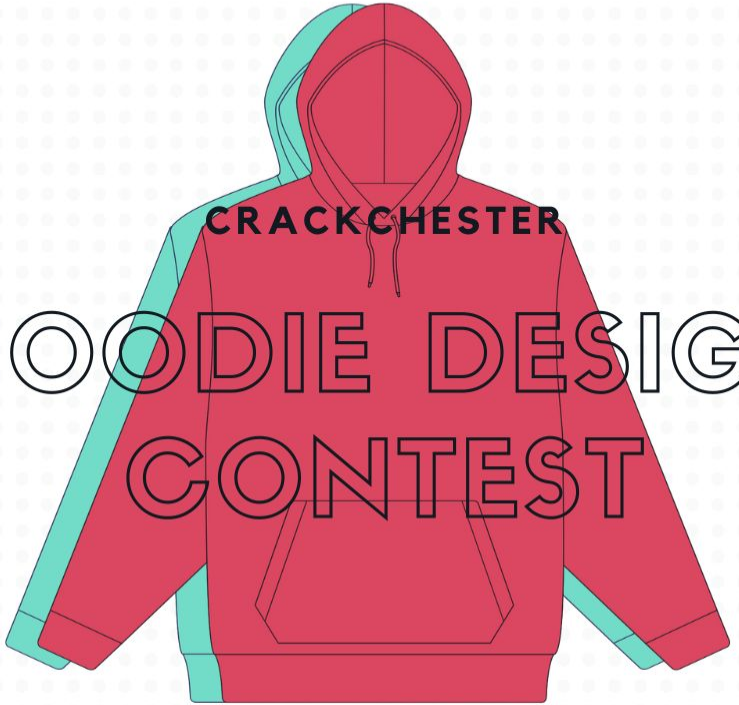
Finding the flag

This is something obvious in hack the box such as a file called `flag.txt`

Running `cat flag.txt` will show the key

CRACKCHESTER

# HOODIE DESIGN CONTEST



# Crackchester

Here’s a link to our link tree where you can find all our socials and our discord!


crackchester crackchester
chester
Demonstration