HTB Notetaking Tips

Pre-task: IP admin

Before we get started on the box, we have to get out IP admin and our note-taking housekeeping out of the way.

By IP admin, I mean two things: testing that the IP we've been given works; adding the IP to our /etc/hosts file.

Testing the IP

After you've connected to HTB via the vpn (click here if you aren't sure how to do this) AND you've started a particular machine on the HTB website, it's time to test if the machine is alive and ready to be communicated with

`Ping 10.10.10.X`

You'll need to replace the numbers here with whatever the IP is of machine you're hacking. You'll find this IP back on the HTB dashboard.

If you don't get anything back from your ping, something has gone wrong between your steps of the VPN, activating the machine, or inputting your IP.

- I would check in reverse, as it's most likely that the IP has been put in wrong, or that the machine hasn't been activated correclty.

/etc/hosts

There are some boxes where the putting the IP in the URL won't be enough, or won't unlock the page you need for exploitation. You do this via `sudo nano /etc/hosts.`

You'll be met with a page that looks like this, with the top two present. You'll want to add your boxes' IP and the box name with .htb at the end.

```
127.0.0.1 localhost
127.0.1.1 kali
10.10.10.x  [BoxName].htb
```

You'll now be able to go into your webrowser, or your scans in command line, and instead of the IP be able to use [BoxName].htb.

There are some boxes where you won't need to need to do this at all. However there are other boxes that will have you stumped in the first five minutes, all because the IP hasn't been added to your hostname.

This isn't just a Capture The Flag (CTF) thing. In real life, just using for the IP of websites means they may not render correctly compared to if you searched for their `XYZ.com`

Pre-task: House keeping

There have been countless times I have lost files, lost track of my enumeration, and misspelled passwords due to sloppy housekeeping. I wouldn't want this to happen to you!

So, for every box you do, I'd like to reccomend that you start with the following:

Make a directory of the box we will be working in and then move into it:

- `mkdir [BoxName]` and then `cd [BoxName]`

Create two .txt files. One for the Usernames we will find, and one for the Passwords we will find.

- `touch users.txt passwords.txt`

As we go through the box, you can add usernames and passwords via your preffered text editor (nano, Vim, gedit etc). I personally just echo the additional info in. So let's say we find out there's a user called 'Jimmy':

- `echo "jimmy" >> users.txt`
- It's very important we use the `>>`, as this ensures that we are merely appending Jimmy to the end of our username list that may have other usernames we have saved in there. Using a single `>` would wipe out every other username we have in that list.

With this out of the way, we have fufiled out housekeeping obligations! I know it seems tedious, but staying on top of your notetaking from the beginning will save you in the long run.

For basic enumeration scans, I tend to output them into a .txt file. So for example: `nmap 10.10.10.172 > nmap.txt.` I do this because I first am forgetful , and second because I don't need to clutter up my notes with the entire scan results. By saving a scan into a txt, I can access it as I need to throughout the box.

- Outputting a scan to a txt will not work if that scan requires user input throughout.
- For interactive scans, go through them normally. Then at the end copy and paste, or screenshot, the results and place them into a txt file or some other format

Nmap

I always run nmap and the IP without anything else from the beginning. This produces simplified results quickly, and I can think about these simplified results and try to enumerate them whilst subsequently more advanced scan runs in the background

Quick scan: `nmap 10.10.10.172 -Pn`

In depth scan:
`nmap 10.10.10.172 -A -O -T4  -Pn -p 1-1-65535  >nmap.txt`