

2023 Hackthebox CTF Training

This repo is best viewed in [Obsidian.md](#). Once installed, open this repo as an Obsidian Vault.

Goal

This training is meant to provide you a basic technical understanding of how to exploit common threats found in the [OWASP Top Ten](#) by providing you with 4 separate standalone vulnerable machines from Hackthebox. Each machine will have unique exploit killchains that you will need to carry out in order to fully compromise the box - this is determined by having root (linux) or system authority (windows) access to the machine. With this access, you will need to access the content of two 'flags' (text files containing a unique hash) found on the machines - one low privilege flag, and one requiring total compromise.

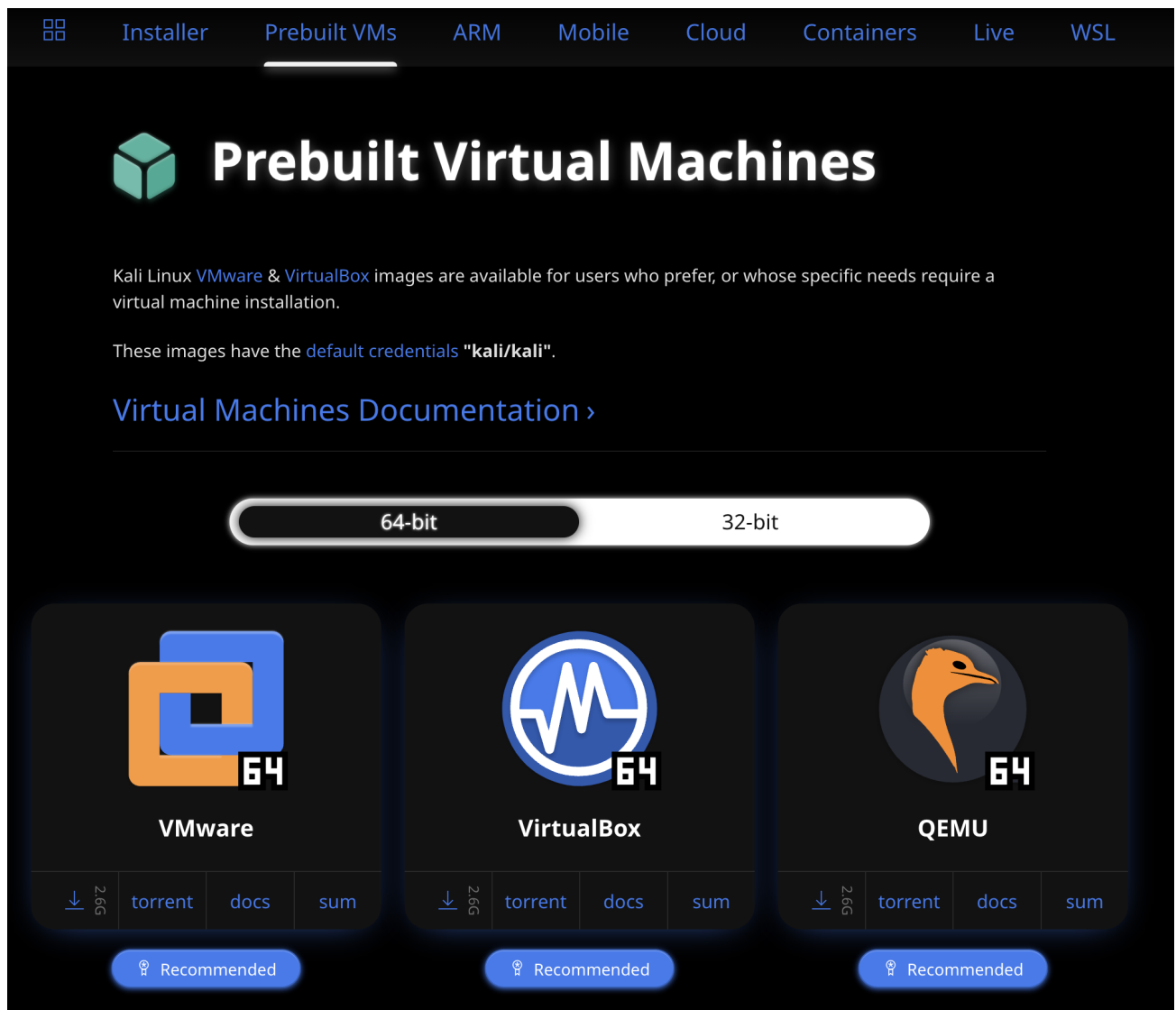
Note: This is a gamified environment where the end goal is to gain unrestricted access to the machines - this should be not be considered indicative of what an attack may look like in real life, as these labs do not take into consideration stealth, persistence, lateral movement, or other high-value vectors.

Getting Started

Setting up a kali vm

On your windows PC, perform the following:

- Download and install [VMWare Workstation Player](#)
- Download the [Kali VMWare image](#)









- To install, follow the instructions found in the docs linked at the [bottom of the download] ([Import Pre-Made Kali VMware VM | Kali Linux Documentation](#))
- Once installed, start the VM and connect as the user `kali` with a password of `kali` (default credentials)
 - You can change these if you want, but for the sake of the CTF this isn't required.
- Once connected, open the terminal in the top left corner of your screen and type `sudo apt update && sudo apt full-upgrade -y`
 - You may be prompted to allow install, or restart a service - in all cases, accept.
- With this done, your kali VM is fully up to date and ready to use.

Connecting to the Hackthebox Network

After receiving your login information for [Hackthebox](#), open firefox (orange icon on the top left of your desktop) on your **Kali VM** and navigate to the labs home page and click lab access at the top right. You'll need to download your VPN pack to gain access to the lab infrastructure.

- Select **Machines**
- For **VPN Access** choose **US-VIP+**
- For **VPN Server** choose **US VIP+ 1**
- For **Protocol** choose **UDP 1337**
- Download


 tylerptl 


 LAB ACCESS


<



Connect to Machines with OpenVPN


>

 ONLINE



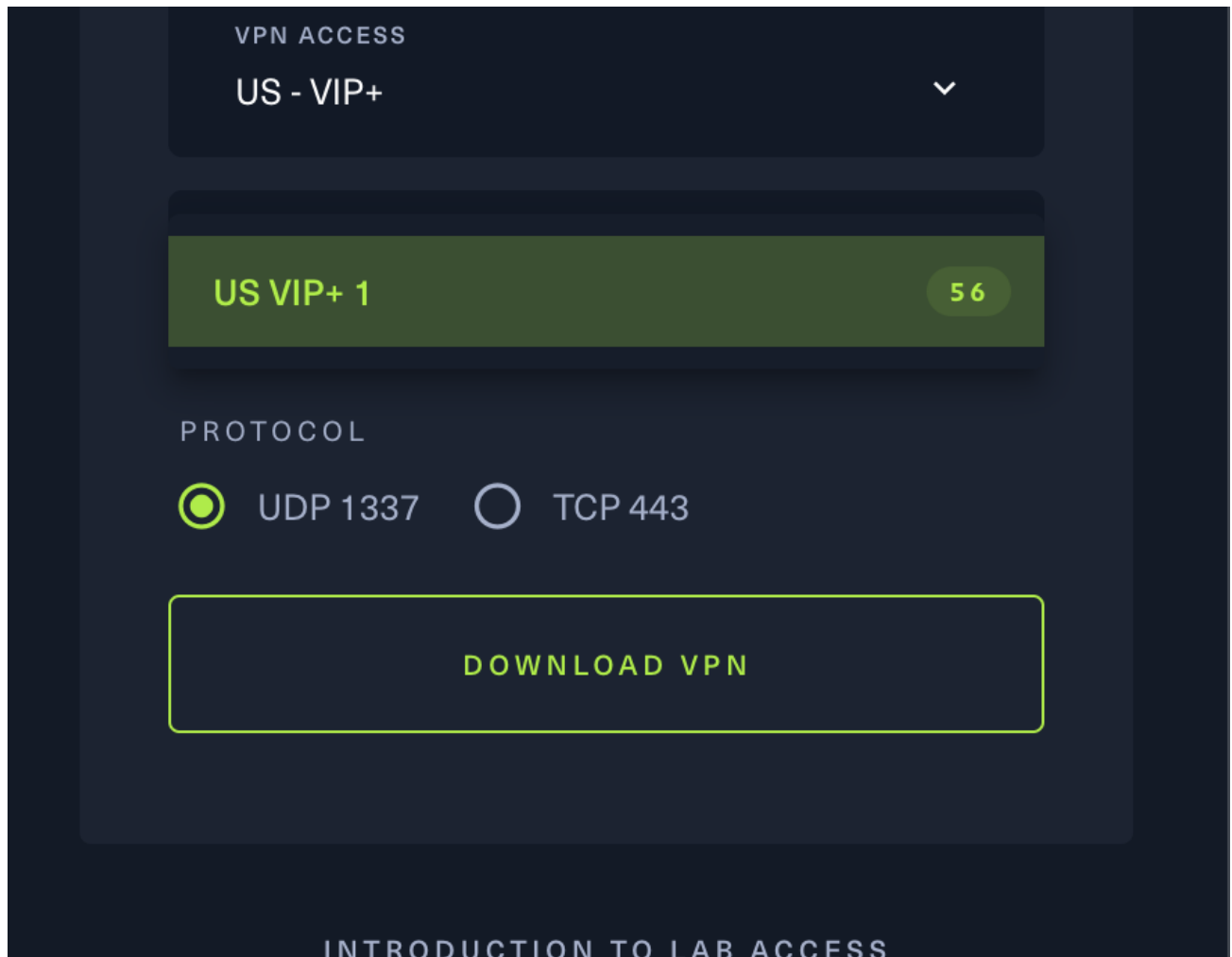
 56 PLAYERS

US ACCESS	US VIP+ 1 SERVER	10.10.14.89 IP ADDRESS
 DOWNLOAD VPN		 REGENERATE VPN



Connect to a **different** VPN server

If you switch your Access or your Server,
you will have to re-connect.



- Its recommended that you create a specific folder to store all CTF related artifacts including this `.ovpn` file.
 - Ex. In a kali terminal type `mkdir ~/Documents/ctf` and use that directory to store your scripts, findings, notes, etc.
- Once you have downloaded the `.ovpn` vpn pack, connect to the network by issuing `sudo openvpn NAME_OF_OVPN_FILE` in your terminal, and entering your kali password when prompted (default password is kali).
- Once connected you will see a new IP at the top right of your screen (something in the 10.10.x.x range) - this is the tunnel interface connecting you to the Hackthebox network. Whenever you need the IP of your box on the network, this is where you can quickly find it.

Connecting to a Hackthebox Lab Machine

Now that you are on the Hackthebox lab network, you'll need to instantiate a machine to exploit. For this CTF, labss have been selected based off the following factors:

- Relation to the [OWASP Top Ten](#)
- Relative difficulty

- Prevalence of vulnerability family in real world environments

The labs will be comprised of the following machines:

- [Shippy](#)
- [Postman](#)
- [Squashed](#)
- [Forest](#)