Starting Out

As a beginner in information security, it can be extremely daunting to know where to start. We have seen folks from all walks of life start from little to no knowledge and become successful on the HTB platform and consequently begin the journey down a technical career path. There are many great resources out there for beginners, including free and paid training, purposefully vulnerable machines and labs, tutorial websites, blogs, YouTube channels, etc.

Throughout our journey, we will continuously see the terms `guided` and `exploratory` learning.

HTB Academy follows a `guided` learning approach where students work through a module on a given subject, reading the material, and reproducing the examples to reinforce the topics presented. Most module sections have one or more hands-on exercises to test the students' knowledge of a given subject. Many modules culminate in a multi-step skills assessment to test the students' understanding of the material presented within the module sections when applied to a real-world scenario.

Guided learning has the benefit of providing students with structured methods to learn various techniques in a manner that correctly builds their knowledge, along with providing additional material, background knowledge, and real-world tie-ins to learn about a topic in-depth while forcing them to test their knowledge at various checkpoints throughout the learning process.

The main HTB platform follows an `exploratory` learning approach to put users in a wide variety of real-world scenarios in which they have to use their technical skills and processes such as enumeration to achieve an, often unknown, goal. The platform offers single challenges in categories such as reverse engineering, cryptography, steganography, pwn, web, forensics, OSINT, mobile, hardware, and more at various difficulty levels designed to test technical and critical thinking skills.

There are also single machines (boxes) of various operating system types, small (and challenging) mini-labs called Endgames, Fortresses that are single machines containing many challenges, and Pro Labs, which are large simulated enterprise networks where users can perform a mock penetration test at various difficulty levels.

There are always free "active" machines and challenges which users must attack from a "black box" approach or with little to no advance knowledge of the task at hand. Machines, challenges, and Endgames do "retire" and are available to VIP users along with official walkthroughs to assist in the learning process. When content is retired on the platform, the community is welcome to create blog and video walkthroughs. It is worth reading several blogs/watching several videos on the same retired machine to see different perspectives and styles that users take when approaching a task to begin building the approach that you are most comfortable with.

The `exploratory` learning approach's main benefit is to allow us to rely on our skills to break into machines and solve challenges, which helps us build our methodologies and techniques and help us shape our penetration testing style.

It is always good to mix between the two learning styles so that we build our skills with the proper structure of knowledge and challenge ourselves to deepen our understanding of the skills we learned.

Resources

When starting, the sheer amount of content available on the web can be overwhelming. Furthermore, it isn't easy to know where to start and the quality of materials available. What follows are some resources outside of HTB that we recommend to anyone starting on their journey or looking to enhance their skillset and pick up new tricks.

Vulnerable Machines/Applications

There are many resources available to practice common web and network vulnerabilities in a safe, controlled setting. The following are some examples of purposefully vulnerable web applications and vulnerable machines that we can set up in a lab environment for extra practice.

OWASP Juice Shop	Is a modern vulnerable web application written in Node.js, Express, and Angular which showcases the entire OWASP Top Ten along with many other real-world application security flaws.
Metasploitable 2	Is a purposefully vulnerable Ubuntu Linux VM that can be used to practice enumeration, automated, and manual exploitation.
Metasploitable 3	Is a template for building a vulnerable Windows VM configured with a wide range of vulnerabilities.
DVWA	This is a vulnerable PHP/MySQL web application showcasing many common web application vulnerabilities with varying degrees of difficulty.

It is worth learning how to set these up in your lab environment to gain extra practice setting up VMs and working with common configurations such as setting up a web server. Aside from these vulnerable machines/applications, we can also set up many machines and applications in a lab environment to practice configuration, enumeration/exploitation, and remediation.

YouTube Channels

There are many YouTube channels out there that showcase penetration testing/hacking techniques. A few worth bookmarking are:

IppSec	Provides an extremely in-depth walkthrough of every retired HTB box packed full of insight from his own experience, as well as videos on various techniques.
VbScrub	Provides HTB videos as well as videos on techniques, primarily focusing on Active Directory exploitation.
STOK	Provides videos on various infosec related topics, mainly focusing on bug bounties and web application penetration testing.
LiveOverflow	Provides videos on a wide variety of technical infosec topics.

Blogs

There are too many blogs out there to list them all. If you do a Google search for a walkthrough of most any retired HTB box, you will usually come across the same blogs time and time again. These can be great for seeing another person's perspective on the same topic, especially if their posts contain "extra" information about the target that other blogs do not cover.
One great blog worth checking out is 0xdf hacks stuff. This blog has fantastic walkthroughs of most retired HTB boxes, each with a "Beyond Root" section covering some unique aspect of the box that the author noticed. The blog also has posts on various techniques, malware analysis, and write-ups from past CTF events.

At any point in the learning process, it is worth reading as much material as possible to understand a subject better and gain different perspectives. Aside from blogs related to retired HTB boxes, it is also worth seeking out blog write-ups on recent exploits/attacks, Active Directory exploitation techniques, CTF event write-ups, and bug bounty report write-ups. These can all contain a wealth of information that may help connect some dots in our learning or even teach us something new that can come in handy on an assessment.

Tutorial Websites

There are many tutorial websites out there for practicing fundamental IT skills, such as scripting.
Two great tutorial websites are Under The Wire and Over The Wire. These websites are set up to help train users on using both Windows `PowerShell` and the Linux command line, respectively, through various scenarios in a "war games" format.
They take the user through various levels, consisting of tasks or challenges to training them on fundamental to advanced Windows and Linux command line usage and `Bash` and `PowerShell` scripting. These skills are paramount for anyone looking to succeed in this industry.

HTB Starting Point

Starting Point is an introduction to HTB labs and basic machines/challenges. After completing a tutorial covering connecting to VPN, enumeration, gaining a foothold, and privilege escalation against a single target, we are presented with several easy-rated machines that can be attacked before accessing the rest of the HTB platform.

HTB Tracks

On the main HTB platform Tracks, "selections of machines and challenges tied together for users to progress through, mastering a particular subject." Tracks cover a variety of topics and are continually being added to the platform. Their goal is to help students stay focused on a specific goal in a structured way while following an exploratory learning approach.

Beginner Friendly HTB Machines

There are many beginner-friendly machines on the main HTB platform. Some recommended ones are:

Lame	Blue	Nibbles	Shocker	Jerry

If you prefer to watch a video walkthrough while working on an easy machine, the below playlists from IppSec's channel have a walkthroughs for various Linux/Windows easy HTB boxes:

Easy Linux Boxes	Easy Windows Boxes

Beginner Friendly HTB Challenges

The HTB platform contains one-off challenges in a variety of categories. Some beginner-friendly challenges include:

Find The Easy Pass	Weak RSA	You know 0xDiablos

Dante Prolab

The HTB platform has various Pro Labs that are simulated enterprise networks with many interconnected hosts that players can use to practice their skills in a network containing multiple targets.
Successful exploitation of specific hosts will yield information that will help players when attacking hosts encountered later in the lab.

The Dante Pro Lab is the most beginner-friendly lab offered to date. This lab is geared towards players with some experience performing network and web application attacks and an understanding of networking concepts and the basics of penetration methodologies such as scanning/enumeration, lateral movement, privilege escalation, post-exploitation, etc.

Moving On

Now that we've covered basic terminology and techniques and scanning/enumeration let's put the pieces together by walking through an easy-rated HTB box step-by-step.

Cheat Sheet

Table of Contents

My Workstation

OFFLINE

Start Instance

1 / 1 spawns left