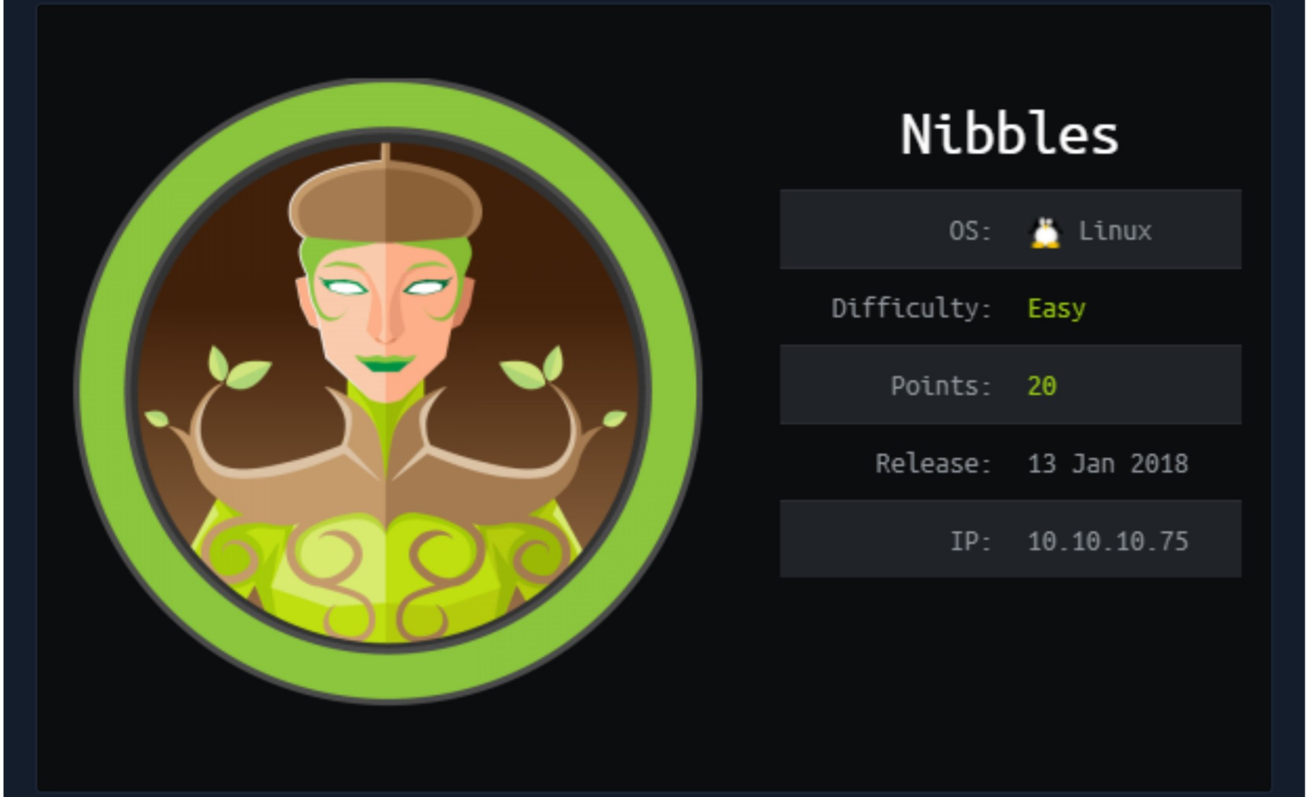
Nibbles - Enumeration

There are 201 standalone boxes of various operating systems and difficulty levels available to us on the HTB platform with VIP membership when writing this. This membership includes an official HTB created walkthrough for each retired machine. We can also find blog and video walkthroughs for most boxes with a quick Google search.

For our purposes, let us walk through the box `Nibbles`, an easy-rated Linux box that showcases common enumeration tactics, basic web application exploitation, and a file-related misconfiguration to escalate privileges.



Nibbles

OS:	🐧 Linux
Difficulty:	Easy
Points:	20
Release:	13 Jan 2018
IP:	10.10.10.75

Let us first look at some machine statistics:

Machine Name	Nibbles
Creator	mrb3n
Operating System	Linux
Difficulty	Easy
User Path	Web
Privilege Escalation	World-writable File / Sudoers Misconfiguration
Ippsec Video	https://www.youtube.com/watch?v=s_0GcRGv6Ds
Walkthrough	https://0xdf.gitlab.io/2018/06/30/htb-nibbles.html

Our first step when approaching any machine is to perform some basic enumeration. First, let us start with what do know about the target. We already know the target's IP address, that it is Linux, and has a web-related attack vector. We call this a grey-box approach because we have some information about the target. On the HTB platform, the 20 "active" weekly-release machines are all approached from a black-box perspective. Users are given the IP address and operating system type beforehand but no additional information about the target to formulate their attacks. This is why the thorough enumeration is critical and is often an iterative process.

Before we continue, let us take a quick step back and look at the various approaches to penetration testing actions. There are three main types, `black-box`, `grey-box`, and `white-box`, and each differs in the goal and approach.

Engagement	Description
`Black-Box`	Low level to no knowledge of a target. The penetration tester must perform in-depth reconnaissance to learn about the target. This may be an external penetration test where the tester is given only the company name and no further information such as target IP addresses, or an internal penetration test where the tester either has to bypass controls to gain initial access to the network or can connect to the internal network but has no information about internal networks/hosts. This type of penetration test most simulates an actual attack but is not as comprehensive as other assessment types and could leave misconfigurations/vulnerabilities undiscovered.
`Grey-Box`	In a grey-box test, the tester is given a certain amount of information in advance. This may be a list of in-scope IP addresses/ranges, low-level credentials to a web application or Active Directory, or some application/network diagrams. This type of penetration test can simulate a malicious insider or see what an attacker can do with a low level of access. In this scenario, the tester will typically spend less time on reconnaissance and more time looking for misconfigurations and attempting exploitation.
`White-Box`	In this type of test, the tester is given complete access. In a web application test, they may be provided with administrator-level credentials, access to the source code, build diagrams, etc., to look for logic vulnerabilities and other difficult-to-discover flaws. In a network test, they may be given administrator-level credentials to dig into Active Directory or other systems for misconfigurations that may otherwise be missed. This assessment type is highly comprehensive as the tester will have access to both sides of a target and perform a comprehensive analysis.

Nmap

Let us begin with a quick `nmap` scan to look for open ports using the command `nmap -sV --open -oA nibbles_initial_scan <ip address>`. This will run a service enumeration (`-sV`) scan against the default top 1,000 ports and only return open ports (`--open`). We can check which ports `nmap` scans for a given scan type by running a scan with no target specified, using the command `nmap -v -oG -`. Here we will output the greppable format to stdout with `-oG -` and `-v` for verbose output. Since no target is specified, the scan will fail but will show the ports scanned.

```
MichaelLuka@htb[/htb]$ nmap -v -oG -

# Nmap 7.80 scan initiated Wed Dec 16 23:22:26 2020 as: nmap -v -oG -

# Ports scanned: TCP(1000;1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,11

WARNING: No targets were specified, so 0 hosts scanned.

# Nmap done at Wed Dec 16 23:22:26 2020 -- 0 IP addresses (0 hosts up) scanned in 0.04 seconds
```

Finally, we will output all scan formats using `-oA`. This includes XML output, greppable output, and text output that may be useful to us later. It is essential to get in the habit of taking extensive notes and saving all console output early on. The better we get at this while practicing, the more second nature it will become when on real-world engagements. Proper notetaking is critical for us as penetration testers and will significantly speed up the reporting process and ensure no evidence is lost. It is also essential to keep detailed time-stamped logs of scanning and exploitation attempts in an outage or incident in which the client needs information about our activities.

```
MichaelLuka@htb[/htb]$ nmap -sV --open -oA nibbles_initial_scan 10.129.42.190
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-16 23:18 EST

Nmap scan report for 10.129.42.190
Host is up (0.11s latency).
Not shown: 991 closed ports, 7 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd <REDACTED> ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.82 seconds
```

From the initial scan output, we can see that the host is likely Ubuntu Linux and exposes an Apache web server on port 80 and an OpenSSH server on port 22. SSH, or Secure Shell, is a protocol typically used for remote access to Linux/Unix hosts. SSH can also be used to access Windows host and is now native to Windows 10 since version 1809. We can also see that all three types of scan output were created in our working directory.

```
MichaelLuka@htb[/htb]$ ls

nibbles_initial_scan.gnmap  nibbles_initial_scan.nmap  nibbles_initial_scan.xml
```

Before we start poking around at the open ports, we can run a full TCP port scan using the command `nmap -p- --open -oA nibbles_full_tcp_scan 10.129.42.190`. This will check for any services running on non-standard ports that our initial can may have missed. Since this scans all 65,535 TCP ports, it can take a long time to finish depending on the network. We can leave this running in the background and move on with our enumeration. Using `nc` to do some banner grabbing confirms what `nmap` told us; the target is running an Apache web server and an OpenSSH server.

```
MichaelLuka@htb[/htb]$ nc -nv 10.129.42.190 22

(UNKNOWN) [10.129.42.190] 22 (ssh) open
SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.8
```

`nc` tells us that port 80 runs an HTTP (web) server but does not show the banner.

```
MichaelLuka@htb[/htb]$ nc -nv 10.129.42.190 80

(UNKNOWN) [10.129.42.190] 80 (http) open
```

Checking our other terminal window, we can see that the full port scan (`-p-`) has finished and has not found any additional ports. Let's do perform an `nmap` script scan using the `-sC` flag. This flag uses the default scripts, which are listed here. These scripts can be intrusive, so it is always important to understand exactly how our tools work. We run the command `nmap -sC -p 22,80 -oA nibbles_script_scan 10.129.42.190`. Since we already know which ports are open, we can save time and limit unnecessary scanner traffic by specifying the target ports with `-p`.

```
MichaelLuka@htb[/htb]$ nmap -sC -p 22,80 -oA nibbles_script_scan 10.129.42.190
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-16 23:39 EST
Nmap scan report for 10.129.42.190
Host is up (0.11s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
80/tcp open  http
|_http-title: Site doesn't have a title (text/html).

Nmap done: 1 IP address (1 host up) scanned in 4.42 seconds
```

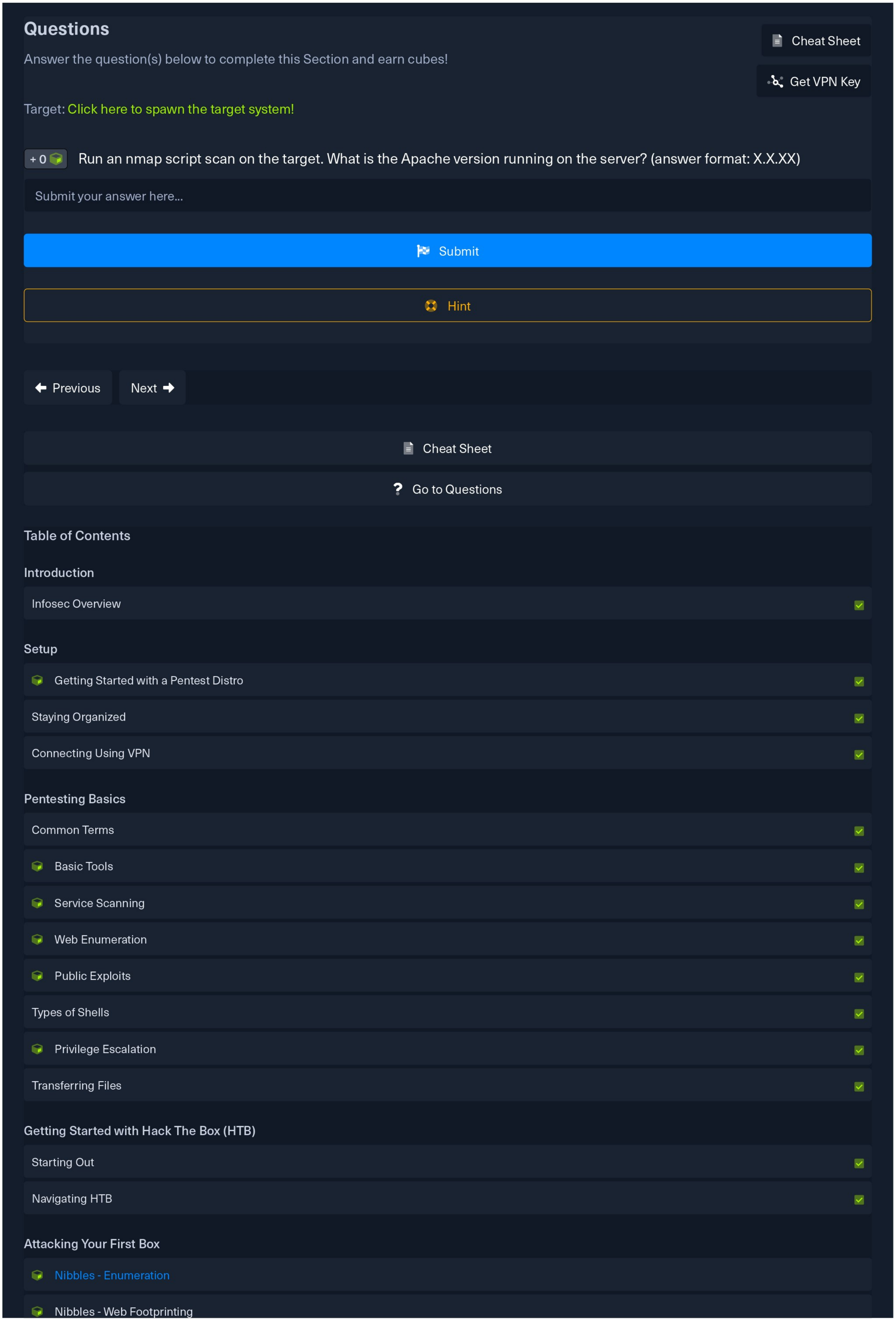
The script scan did not give us anything handy. Let us round out our `nmap` enumeration using the http-enum script, which can be used to enumerate common web application directories. This scan also did not uncover anything useful.

```
MichaelLuka@htb[/htb]$ nmap -sV --script=http-enum -oA nibbles_nmap_http_enum 10.129.42.190

Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-16 23:41 EST
Nmap scan report for 10.129.42.190
Host is up (0.11s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd <REDACTED> ((Ubuntu))
|_http-server-header: Apache/<REDACTED> (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.23 seconds
```

Start Instance

1 / 1 spawns left

Waiting to start...



Questions

Answer the question(s) below to complete this Section and earn cubes!

Target: Click here to spawn the target system!

+ 0 Run an nmap script scan on the target. What is the Apache version running on the server? (answer format: X.X.XX)

Table of Contents

Introduction

Setup

Pentesting Basics

Getting Started with Hack The Box (HTB)

Attacking Your First Box

Nibbles - Initial Foothold

Nibbles - Privilege Escalation

Nibbles - Alternate User Method - Metasploit

Problem Solving

Common Pitfalls

Getting Help

What's Next?

Next Steps

Knowledge Check

My Workstation

OFFLINE

▶ Start Instance

1 / 1 spawns left