TIMOTHY SEWE OGODE(CSSA0423076)

CYBER SHUJAA

WEEK 2

GETTING STARTED

Table of Contents

[1. INTRODUCTION 2](#_Toc136517975)

[2. SETUP 2](#_Toc136517976)

[3. PENTESTING BASICS 2](#_Toc136517977)

[Basic tools 2](#_Toc136517978)

[TASK 3](#_Toc136517979)

[Service Scanning 3](#_Toc136517980)

[Task 3](#_Toc136517981)

[Web Enumeration 4](#_Toc136517982)

[Task 4](#_Toc136517983)

[Public Exploits 4](#_Toc136517984)

[Task 4](#_Toc136517985)

[Privilege Escalation 5](#_Toc136517986)

[Tasks 5](#_Toc136517987)

[4. ATTACKING YOUR FIRST BOX 5](#_Toc136517988)

[Nibbles – Enumeration 5](#_Toc136517989)

[Nibbles - Web Footprinting 5](#_Toc136517990)

[Nibbles - Initial Foothold 6](#_Toc136517991)

[Nibbles - Privilege Escalation 7](#_Toc136517992)

[Task 7](#_Toc136517993)

[Knowledge Check 8](#_Toc136517994)

[Tasks 8](#_Toc136517995)

[5. CONCLUSION 9](#_Toc136517996)

# INTRODUCTION

The information security (infosec) field encompasses various specializations, including network security, application security, digital forensics, and incident response. Infosec professionals aim to protect data from unauthorized access, changes, and disruptions, focusing on the confidentiality, integrity, and availability of information. The risk management process plays a crucial role in implementing effective security measures without hindering business operations. This process involves identifying, analysing, evaluating, dealing with, and monitoring risks. In infosec, the red team simulates attackers, conducting penetration testing and offensive techniques, while the blue team focuses on defending the organization's systems, responding to threats, and implementing security tools. Penetration testers play a crucial role in identifying vulnerabilities and helping organizations mitigate risks. This report provides hands-on guidance for getting started in infosec and penetration testing, covering topics such as selecting a pentest distro, understanding common technologies and tools, performing penetration testing, navigating the Hack The Box platform, and seeking effective help.

# SETUP

This section provides an overview of getting started with a penetration testing distribution (distro) for individuals pursuing a career in information security. It highlights the importance of being familiar with different technologies and operating systems, particularly Linux and Windows, and the need to set up, maintain, and secure attack machines. The choice of a distro is discussed, with options ranging from pre-existing distros with preloaded tools to building a custom VM. Various methods of setting up a pentest distro, such as using virtualization software like Hyper-V, Proxmox, VMware ESXi, VirtualBox, or VMware Workstation, are explored. The concept of hypervisors is introduced, allowing the running of multiple isolated VMs on a single host system. The significance of using fresh VMs for each security assessment to protect client confidentiality is emphasized. Furthermore, the module emphasizes the value of setting up a home lab to practice and experiment with vulnerabilities, applications, and attack techniques.

A VPN allows secure connection to a private network over shared public networks, providing privacy and encryption. There are two types of remote access VPNs: client-based and SSL VPN. VPNs are used for security, privacy, bypassing restrictions, and accessing purposefully vulnerable networks like Hack The Box. Connecting to a VPN involves using client software or a web browser, and precautions should be taken to ensure a secure connection.

# PENTESTING BASICS

## Basic tools

SSH, Netcat, Tmux, and Vim are essential tools for information security professionals. SSH provides secure remote access to computers, while Netcat allows interaction with TCP/UDP ports and can be used for banner grabbing and file transfer. Tmux is a terminal multiplexer that enhances the features of a Linux terminal, allowing multiple windows and panes. Vim is a powerful text editor used for coding and editing files, often found on compromised Linux systems. Mastering these tools is crucial for penetration testing and daily use in the field of information security.

### TASK

Apply what you learned in this section to grab the banner of the above server and submit it as the answer. SSH-2.0-OpenSSH\_8.2p1 Ubuntu-4ubuntu0.1

A picture containing text, font, screenshot

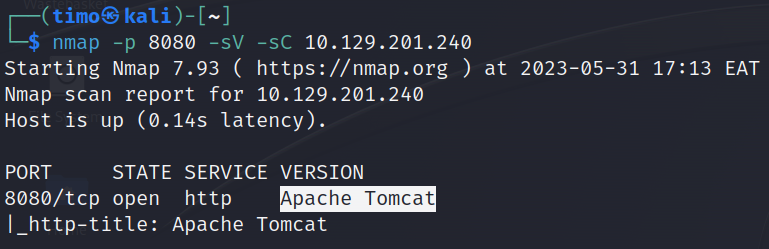
Description automatically generated

## Service Scanning

Service scanning involves identifying the operating system and available services on a machine or server. Nmap can scan the range of ports on a target system to identify open ports and the corresponding services running on them. By using options like -sC and -sV, Nmap can gather more detailed information about the services, including service versions and application names. Banner grabbing is another technique to quickly identify the service version by examining the banner displayed upon connection.

### Task

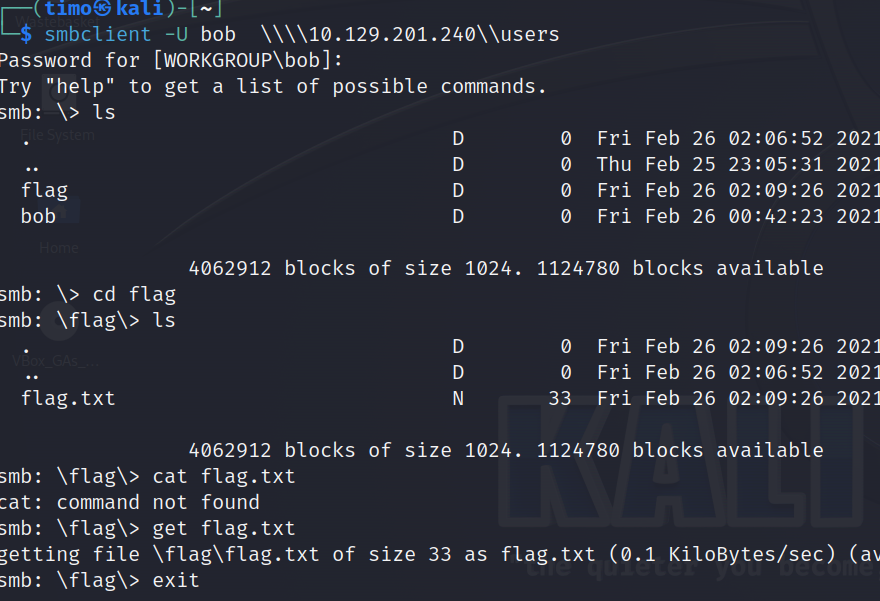
Perform a Nmap scan of the target. What is the version of the service from the Nmap scan running on port 8080? Apache Tomcat



Perform an Nmap scan of the target and identify the non-default port that the telnet service is running on. 2323

List the SMB shares available on the target host. Connect to the available share as the bob user. Once connected, access the folder called 'flag' and submit the contents of the flag.txt file.

dceece590f3284c3866305eb2473d099



## Web Enumeration

Web enumeration is an essential part of service scanning, particularly when targeting web servers on ports 80 and 443. It involves thoroughly examining the server to uncover hidden files, directories, and subdomains that may provide access or expose sensitive information. GoBuster is a useful tool for directory and DNS subdomain brute-forcing. HTTP status codes, such as 200 for success and 403 for forbidden access, provide valuable insights. Banner grabbing, SSL/TLS certificates, robots.txt files, and source code analysis are additional techniques for web enumeration. By utilizing these methods, one can effectively identify vulnerabilities and access points in web applications.

### Task

Try running some of the web enumeration techniques you learned in this section on the server above, and use the info you get to get the flag.

HTB{w3b\_3num3r4710n\_r3v34L5\_53cr375}

## Public Exploits

When identifying services running on scanned ports, we search for public exploits for those applications/services. Google and tools like searchsploit can be used to find public exploits by searching for the application name with "exploit." Online databases such as Exploit DB, Rapid7 DB, and Vulnerability Lab can also be helpful. The Metasploit Framework (MSF) is a powerful tool that includes built-in exploits and features like reconnaissance scripts, verification scripts, Meterpreter, and post-exploitation tools. By using the msfconsole command, we can search for exploits for the target application and configure them with the set command. We can then check if the server is vulnerable and run the exploit with the exploit command. Successful exploitation can lead to gaining admin access on the target system. It's important to have a well-rounded toolkit and not solely rely on Metasploit for penetration testing.

### Task

Try to identify the services running on the server above, and then try to search to find public exploits to exploit them. Once you do, try to get the content of the '/flag.txt' file. HTB{my\_f1r57\_h4ck}

A picture containing text, screenshot, font

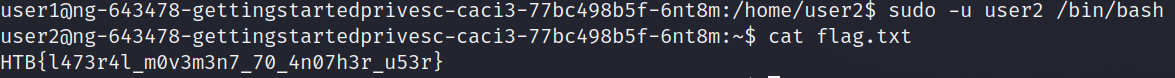
Description automatically generated

## Privilege Escalation

Privilege escalation is a critical step in gaining full control over a remote server. It involves identifying vulnerabilities to elevate our access from low-privileged user to root/administrator. We can use checklists, scripts, and tools like HackTricks, PayloadsAllTheThings, LinEnum, Seatbelt, JAWS, and PEASS to enumerate the server, search for kernel exploits, vulnerable software, user privileges, scheduled tasks, exposed credentials, and SSH keys. However, caution is necessary to avoid triggering alarms or compromising system stability. Proper authorization and a lab environment are recommended for testing before attempting these techniques on production systems.

### Tasks

SSH into the server above with the provided credentials and use the '-p xxxxxx' to specify the port shown above. Once you login, try to find a way to move to 'user2', to get the flag in '/home/user2/flag.txt'. HTB{l473r4l\_m0v3m3n7\_70\_4n07h3r\_u53r}



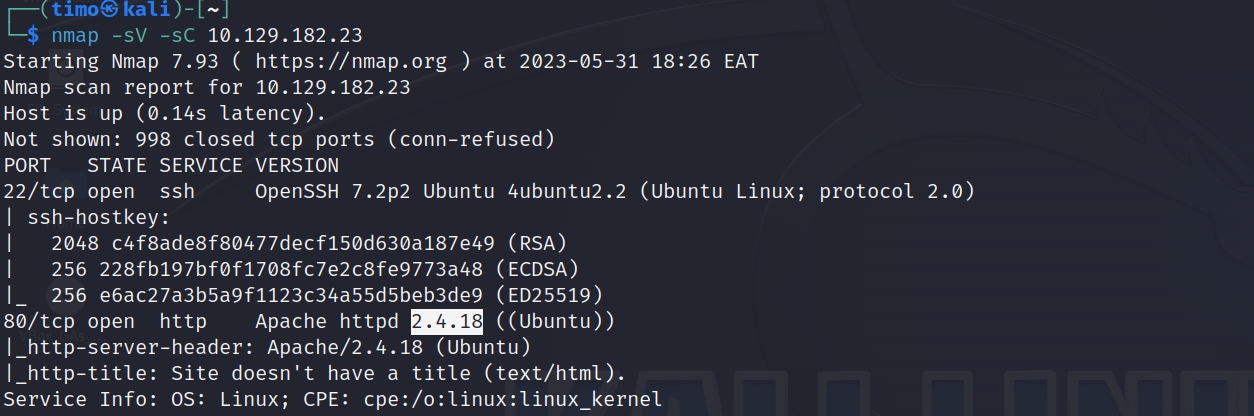
Once you gain access to 'user2', try to find a way to escalate your privileges to root, to get the flag in '/root/flag.txt'.

HTB{pr1v1l363\_35c4l4710n\_2\_r007}

# ATTACKING YOUR FIRST BOX

## Nibbles – Enumeration

Run an nmap script scan on the target. What is the Apache version running on the server? (answer format: X.X.XX) 2.4.18



## Nibbles - Web Footprinting

Refers to the process of gathering and analyzing data about a target system, network, or organization. It involves collecting information from publicly available sources to gain insight into the target's infrastructure, technology, personnel, and potential vulnerabilities. Footprinting techniques include examining websites, social media profiles, DNS records, WHOIS information, network scanning, and other methods to gather valuable intelligence. The goal of footprinting is to create a comprehensive profile of the target, which can be used for further analysis and planning in cybersecurity assessments or penetration testing.

## Nibbles - Initial Foothold

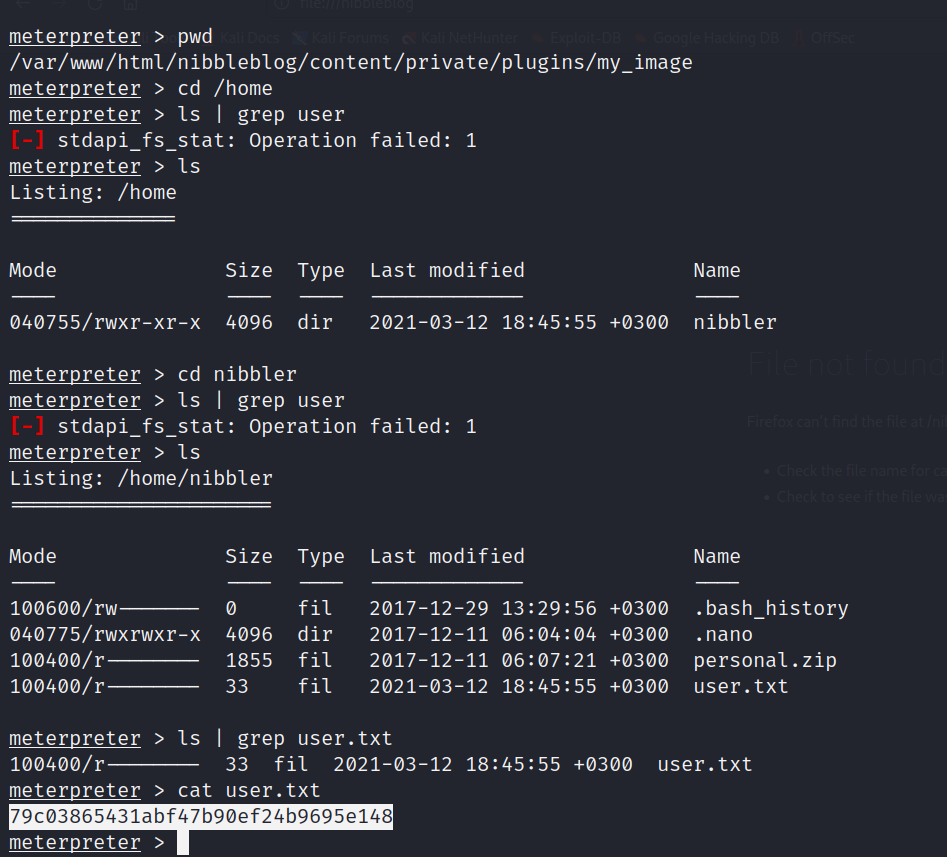
Now that we are logged in to the admin portal, we need to attempt to turn this access into code execution and ultimately gain reverse shell access to the webserver. We know a Metasploit module will likely work for this but let us enumerate the admin portal for other avenues of attack.

Gain a foothold on the target and submit the user.txt flag 79c03865431abf47b90ef24b9695e148

A screenshot of a computer

Description automatically generated with medium confidence

Exploit of choice = ‘Arbitrary File Upload(Metasploit)’ it will upload a php reverse shell in thye image upload.



## Nibbles - Privilege Escalation

Now that we have a reverse shell connection, it is time to escalate privileges.

### Task

Escalate privileges and submit the root.txt flag. de5e5d6619862a8aa5b9b212314e0cdd

A picture containing text, screenshot, font

Description automatically generated

A screenshot of a computer

Description automatically generated

I started a shell session with the shell command. Then, I attempted to spawn a more interactive shell using the Python pty module. Next, I checked the sudo privileges of the current user with sudo -l and found that the user "nibbler" can run the script monitor.sh as root without providing a password. I then overwrote the contents of monitor.sh with a new script that executes /bin/sh. Afterward, I ran the modified script as root using sudo -u root ./monitor.sh. When you run /bin/sh as root, it starts a new shell session running with root privileges. Any commands executed within that shell session will be executed with the privileges of the root user. That is how we escalated privileges to a root user.

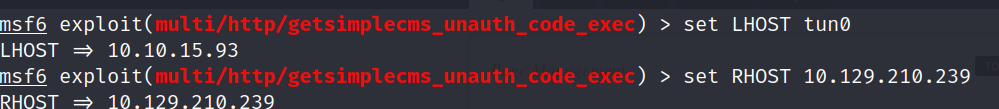
## Knowledge Check

### Tasks

Spawn the target, gain a foothold, and submit the contents of the user.txt flag. 7002d65b149b0a4d19132a66feed21d8

A screenshot of a computer

Description automatically generated with medium confidence



A screenshot of a computer

Description automatically generated with medium confidence

A screen shot of a computer

Description automatically generated with medium confidence

After obtaining a foothold on the target, escalate privileges to root and submit the contents of the root.txt flag. f1fba6e9f71efb2630e6e34da6387842

A quick search of GTFOBins shows several options for sudo PHP use, one of them is a way to get a root shell.

A screen shot of a computer

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated with medium confidence

# CONCLUSION

Throughout this module, we have learned essential concepts and skills related to penetration testing and ethical hacking. We have gained a comprehensive overview of information security and the significance of conducting penetration tests to uncover system vulnerabilities. We now possess knowledge about various penetration testing distributions, as well as the common terms and technologies used in this field. We have become proficient in scanning and enumeration techniques, utilizing public exploits, and executing commands to gain shells, escalate privileges, and transfer files. Moreover, we have navigated the Hack the Box platform and successfully completed a step-by-step walkthrough of a retired HTB box. We have also honed our problem-solving abilities and discovered how to ask questions effectively to overcome common pitfalls. Lastly, we have learned the importance of completing boxes without relying on walkthroughs and have gained insight into our next steps in the field. This module has equipped us with fundamental skills and knowledge in penetration testing, paving the way for further growth and exploration in this dynamic field. [**LINK**](https://academy.hackthebox.com/achievement/643478/77)

