

Knowledge Check

Let's put together everything we learned in this module and attack our first box without a guide.

Tips

Remember that enumeration is an iterative process. After performing our **Nmap** port scans, make sure to perform detailed enumeration against all open ports based on what is running on the discovered ports. Follow the same process as we did with **Nibbles**:

- Enumeration/Scanning with **Nmap** - perform a quick scan for open ports followed by a full port scan
- Web Footprinting - check any identified web ports for running web applications, and any hidden files/directories. Some useful tools for this phase include **whatweb** and **Gobuster**
- If you identify the website URL, you can add it to your '/etc/hosts' file with the IP you get in the question below to load it normally, though this is unnecessary.
- After identifying the technologies in use, use a tool such as **Searchsploit** to find public exploits or search on Google for manual exploitation techniques
- After gaining an initial foothold, use the **Python3 pty** trick to upgrade to a pseudo TTY
- Perform manual and automated enumeration of the file system, looking for misconfigurations, services with known vulnerabilities, and sensitive data in cleartext such as credentials
- Organize this data offline to determine the various ways to escalate privileges to root on this target

There are two ways to gain a foothold—one using **Metasploit** and one via a manual process. Challenge ourselves to work through and gain an understanding of both methods.

There are two ways to escalate privileges to root on the target after obtaining a foothold. Make use of helper scripts such as **LinEnum** and **LinPEAS** to assist you. Filter through the information searching for two well-known privilege escalation techniques.

Have fun, never stop learning, and do not forget to **think outside of the box!**

Start Instance

1 / 1 spawns left

Waiting to start...


Questions

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

 Cheat Sheet

 Get VPN Key


Target: [Click here to spawn the target system!](#)

+ 1  Spawn the target, gain a foothold and submit the contents of the user.txt flag.

Submit your answer here...

 Submit

 Hint

+ 1  After obtaining a foothold on the target, escalate privileges to root and submit the contents of the root.txt flag.

Submit your answer here...

 Submit

 Hint

 Previous

 Cheat Sheet




 Go to Questions


Table of Contents


Introduction

Infosec Overview 

Setup



 Getting Started with a Pentest Distro 











Staying Organized 

Connecting Using VPN 



Pentesting Basics

Common Terms 










 Basic Tools 

 Service Scanning	
 Web Enumeration	
 Public Exploits	
Types of Shells	
 Privilege Escalation	
Transferring Files	



Getting Started with Hack The Box (HTB)

Starting Out	
Navigating HTB	


Attacking Your First Box

 Nibbles - Enumeration	
 Nibbles - Web Footprinting	
 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