Lab Assignment

Cyber Security Professional Program

Ethical Hacking

Ethical Hacking Final Project

EH-13-L1
Ethical Hacking Final Project

Lab Mission

This project is a culmination of the lessons you studied in Ethical Hacking. It includes a challenge that combines different hacking methods and practices, and encourages thinking outside the box.

As the project progresses, it presents an infrastructure-based attack that requires working with different protocols to gain administrative rights and perform various actions.

Lab Duration

2.5-3.5 hours

Requirements

- Students should have knowledge of web applications and the ability to discover web page vulnerabilities. They must be aware of how and where to look for hints and backdoors.
- In addition, knowledge of protocols and how they operate will be necessary to perform infrastructure-based attacks.

Resources

- Environment & Tools
  - Kali Linux
  - Metasploitable
- Related Files

Textbook References

- Ethical Hacking: A Comprehensive Beginner’s Guide to Learn and Master Ethical Hacking

Project Scenario

You are working in a company called ‘Workaround’ as a penetration tester.
During work on a project that your manager assigned you to, you receive an email from Ian, the IT department manager.
Roger, your manager, asks you to review the message and help Ian.

From: Ian Tucker
To: Penetration Testing Team

Hello team,
Recently, our Web Development Manager, Jessica, was fired. In addition to the classified reason she was let go, we also suspect she was hiding information.
We managed to reset her password and accessed her computer, but didn’t find anything outwardly incriminating.
However, we do know that Jessica helped employees with web development (not as part of a company project and against company regulations) and suspect that somehow she managed to hide that fact via a web-based application.
The only thing we found is an encrypted compressed file called ‘Additional Files’ on her desktop.
The file seems out of place, but we cannot find any matching password for it. We even tried her birthday combination, and the names of both her husband and daughter, but nothing matches.
Can you please help obtain the password for the compressed file and find out what Jessica was hiding?

Thank you,
IT Department Manager,
Ian Tucker

Mission Steps

As a penetration tester, you are tasked with assisting Ian in the investigation.
Perform the following steps and solve them one-by-one to reach the final answer.
The file you have to work on is **CrackMeIfYouCan.rar**.

Step 1

1 Transfer the 'CrackMeIfYouCan.rar' file from the additional files provided to your Kali OS machine.

2 Crack the rar file's password.

Step 2

3 Extract the .rar file using the password you discovered.

4 Explore the extracted files to find any suspicious information.

5 Discover the credentials.

Step 3

6 Two of the files extracted may look familiar. Find out how you can use those files and implement the credentials.

7 Use the built-in service in the attacking machine to load the additional PHP file and try to log in.

Step 4

8 Search the webpage for another clue.

Step 5

9 Copy the encoded string to a decoder and transfer the decoded string to a PHP file that will act as a webpage. Name it 'page.php'.

10 Open page.php using the browser.

Step 6

11 Study the clue and find an additional machine in the network.

12 Find open ports on the machine, and a way to display the results in a web page.

Step 7

13 Find vulnerabilities in these protocols:

a) **vsftpd** - Find two ways to gain access to this protocol

b) **samba** - Find two ways to gain access to this protocol (**Hint**: Find out which protocol is responsible for port 3632)

Steps 8-9

14 Elevate your privileges to root user.

Step 10

15 Display the /etc/shadow file to reveal the hash, and compare it with the hash found by other classmates.