

Cyber Security Professional Program

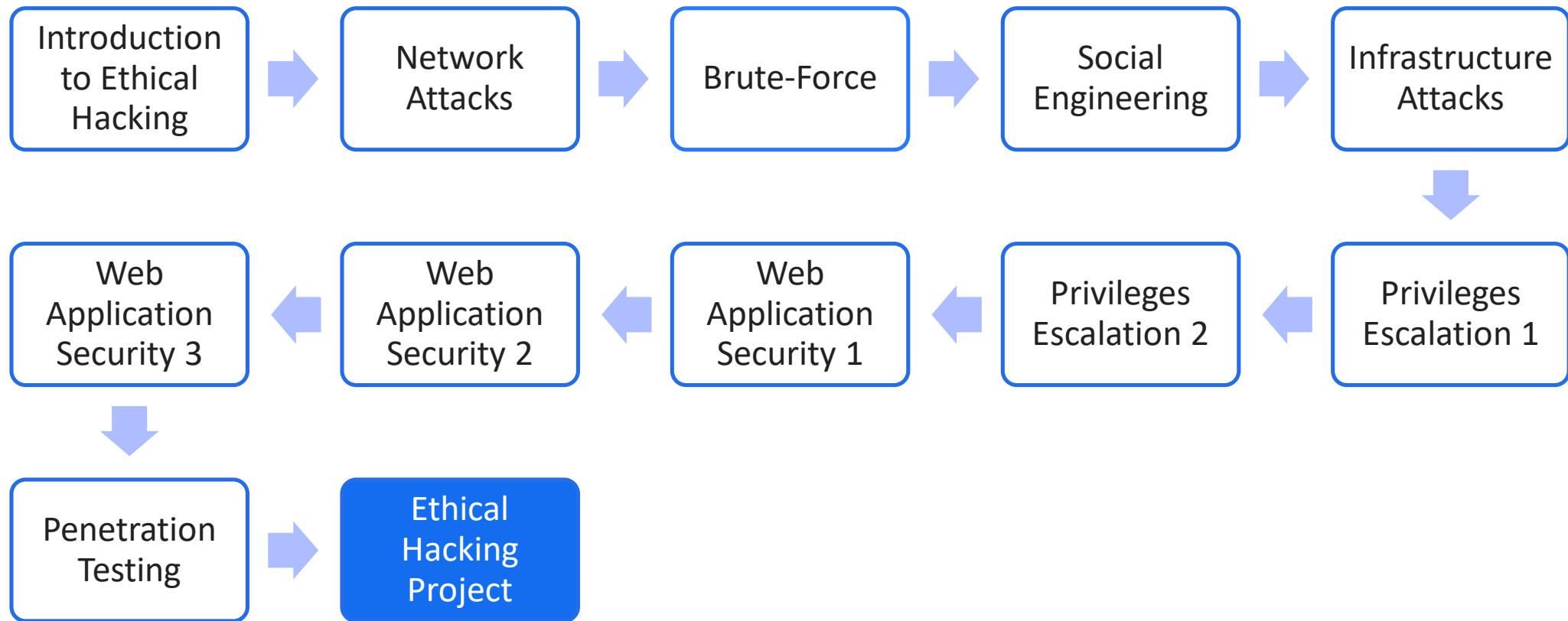
---

# Final Project

Ethical Hacking



# Ethical Hacking Course Path





# Final Project Objectives

This presentation will explain the scenario of the final project for the Ethical Hacking course, and its stages.

The challenge in the project is to obtain a root password.

- ◆ Compressed Folder Password
- ◆ Starting Web Service
- ◆ Gain Web Administrative Rights
- ◆ Import the Vmdk of Metasploitable
- ◆ Implement the Vsftpd Protocol
- ◆ Implement the Samba Protocol
- ◆ Find out the Root Password



Final Project

---

# Final Project Scenario

# Background – Who You Are



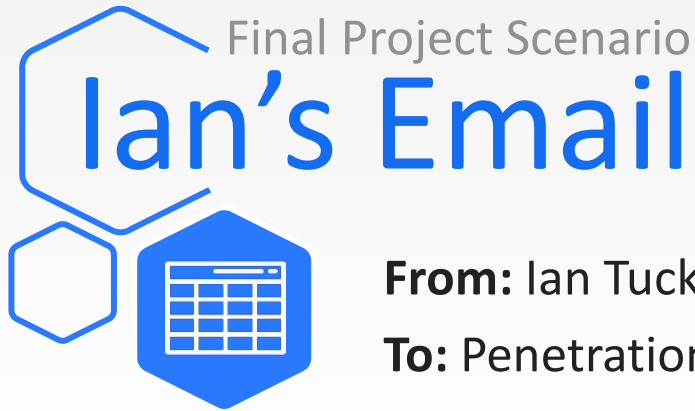
You are working in a company called 'Workaround' as a penetration tester.

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,

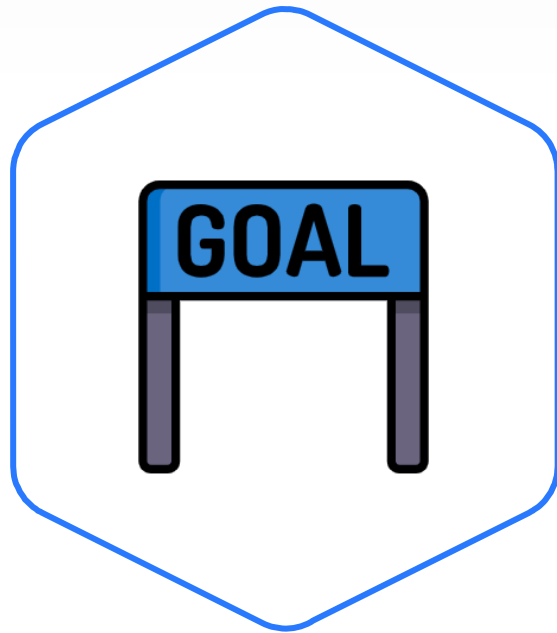

IT Department Manager,

Ian Tucker



# Final Project Scenario

# Your Mission



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 **CrackMelfYouCan.rar**.



# Mission Steps



## Step 1:

Find out the password for the compressed file.





# Mission Steps



## Step 2:

When you find the password, you notice that there are several files inside, and one of them seems suspicious. Investigate that file and find out its secrets.



# Final Project Scenario

# Mission Steps

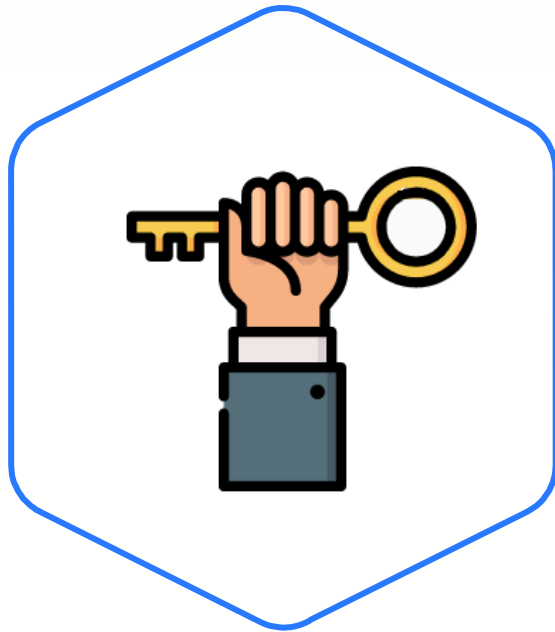


## Step 3:

You begin to understand that when linked together, the files comprise a customized website with a login page, but one of the files is not part of the website.

Investigate the website to obtain another clue that will lead you to the next stage.

# Mission Steps



## Step 4:

It appears that in the website's source code an encoded string was hidden.

The string is a clue for the next stage.

# Final Project Scenario

# Mission Steps



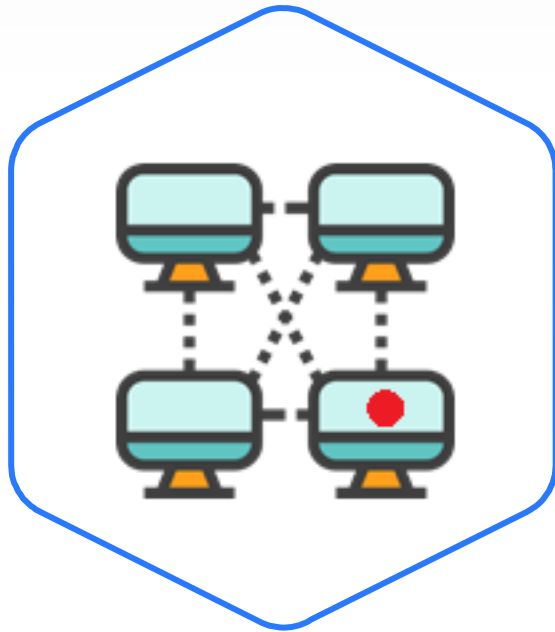
## Step 5:

The encoded string is decoded to a PHP code that can be used as a PHP file.

The file can guide you to the next step.

# Final Project Scenario

## Mission Steps



### Step 6:

When you scan the network, you discover a Linux machine that isn't part of the original workspace. Investigate that machine to find a way inside it and continue the investigation.

# Final Project Scenario

## Mission Steps



### Step 7:

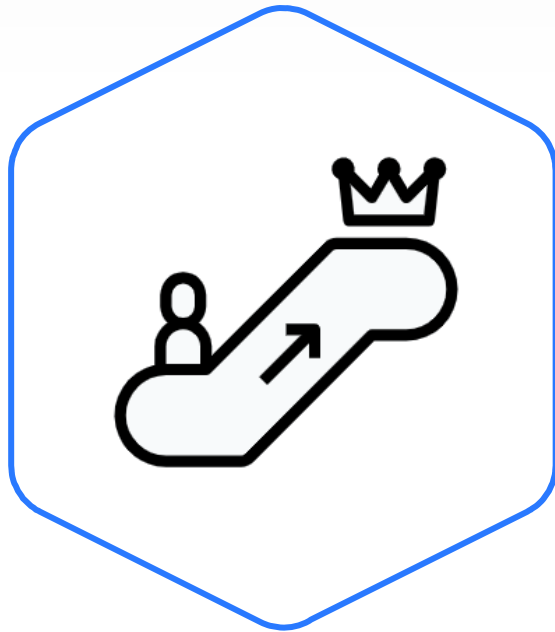
A scan of the machine reveals many open ports, and Ian asks you to export the results to an XML file, so he can review it. Ian requests that you to try to find vulnerabilities in Vsftpd and Samba, since he knows Jessica specializes in those services. Your task is to try to obtain access to the machine via each of those services.





# Final Project Scenario

# Mission Steps



## Step 8:

As a first step in your investigation of the services, you access the system using a regular user, and try to elevate your privileges to the level of root access.

# Final Project Scenario

# Mission Steps



## Step 9:

Navigating in the system you find that the udev process is running, enumerate its version, and notice that it can be used for privilege escalation.

# Mission Steps



## Step 10:

After obtaining root access to the machine, Ian asks you to find out the hash for the root user.





Questions?

---

**Good Luck!**