INFORMATION SECURITY PROJECT

Capture The Flag Project 2020

Project proposal

- **IT18136098 - P.A.U.T. De Alwis**
- **IT18133578 – R.P.R.D. Randunu**

CYBER HEIST

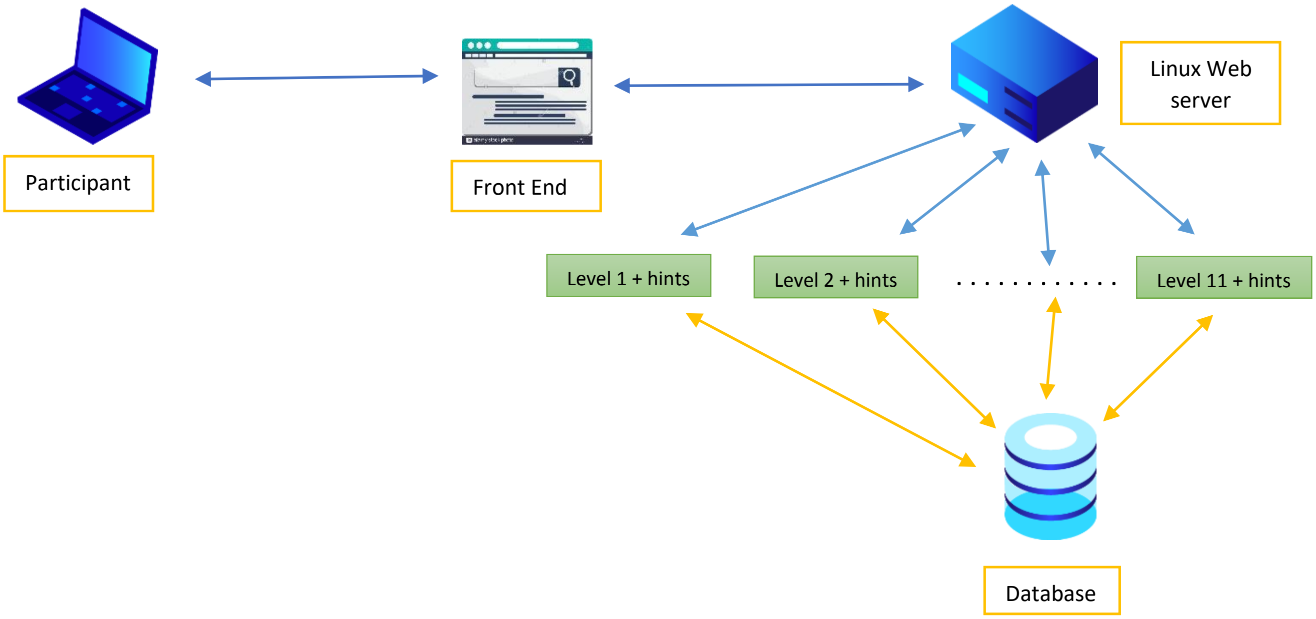
(La casa del ciber)

Table of Contents

Introduction

Capture the flag (CTF) challenges are designed to learn information security skills by solving a variety of tasks, in a range of categories (Jeopardy style) or performing a more advanced version which is attack and defense style. Cyber heist CTF challenge is a Jeopardy style web based challenge which will teach about specific cyber security skills and techniques such as Linux commands, SQL injection commands, brute force, XSS, cryptography, steganography, programming etc. Cyber Heist will be a challenge based on the popular Netflix Spanish drama series La Casa De Papel also known as Money heist which has an addictive storyline based on a bank robbery and a master mind character called “The Professor”. Cyber Heist will be consisted with eleven levels and each level is named after a plan name. When a contestant completes each task, they will be heading for more difficult tasks, which is considered as they are step by step heading towards a cyber heist which robs bitcoins from the internet. The beginning CTF levels are flowing based on how the professor plan the heist and assign tasks for the contestants in order to teach the plans. Ending levels would be much difficult so that those levels are considered as the actual heist. The minimum play duration is about 8 hours. The contestants will gain good knowledge about hacking tactics and they will improve their cyber security skills after they complete all the levels.

Architecture



Drill plan

We can perform the CTF box as a cyber drill for DevOps professionals if they have faced an attack. They can ensure that they have good cyber security practices. It is recommended that the participants should have knowledge in many areas including incident handling, information gathering, log analysis, packet analysis, familiarity of the Linux OS, programming, encryption methods and other attacks.

Theme/Audience

Theme

The theme is based on the popular Spanish Netflix drama series La Casa De Papel (Money heist). The professor is planning another heist, but this time it is a cyber heist.

Audience

The CTF challenge is mainly targeted for DevOps professionals that work in financial side of companies. The target audience can range between trainee DevOps professionals who have basic programming knowledge, have a basic understanding of how to use the command line and have understanding of system operations, to cyber security experts. The Cyber Heist challenge is based on the popular drama series Money Heist, so that the challenge could be interesting for money heist fans, but this time the heist is not a money or gold heist. It has the storyline for a cyber heist to steal bitcoins. The character “The professor” from the show will be the concept for guiding the contestants for this CTF challenge.

Note: Contestants do not need to know about the drama series to complete the levels.

Storyline

The professor who robbed money from the Royal Mint of Spain and gold from Bank of Spain is planning to rob bitcoins from a cyber heist. This time the heist will be performed by a chosen set of people from a CTF challenge. The professor will choose people for the heist based on the security skills. Specific levels in the cyber heist CTF challenge will choose the people for the heist while the hardest levels will be the actual cyber heist. The professor has a set of pre-determined plans for the cyber heist. The contestants should complete certain levels which indicates they have gained knowledge about each plan. The motive of the professor is to teach them the plans and, in the end, to perform the heist. Each level is named with a certain plan name. Some plan names are familiar because they have been used in the previous heists such as plan Valencia, plan Cameroon, plan Chernobyl, plan Alcatraz, plan Defcon 2.

Levels(plans) 1-6 will be the challenges which the professor intends to choose the contestants for the cyber heist. The contestants must find the flag and submit for each plan. In every plan the professor will give tips about the motive, so that the contestants could think like a hacker.

A contestant who completes first six levels(plans) will be eligible to the heist and the professor will reward them a city name as their name to feel anonymous. Each chosen contestant will not know each other who will perform the real heist. They will be completely anonymous. Each chosen contestant will be a part of the heist after completing the sixth level(plan), but they will not interact with each other. The master mind behind the heist will handle the plans and the tasks.

The 7-10 levels or plans will be harder because they will be the plans for the real cyber heist according to the storyline. The eleventh or the last level(plan) will be the hardest because according to the storyline, it is the plan to rob the bitcoins and leave without a trace. (Our task will not be to rob bitcoins; it will be a harder cyber security technique to learn.) If the contestant has completed the last plan it is considered as the conclusion of the CTF challenge and the storyline.

Budget

Projects	Prices
CTF designing	$20.00
Development	$100.00
Web hosting/1 year	$58.00
Domain name/1 year	$12.99
Testing environment	$5.00
	$195.99

Market plan/pricing

In order to introduce the CTF product to the industry and get the audience, our plan is to pitch the CTF box to the DevOps professionals. Then we can launch a blog dedicated to the CTF box, accounts on Facebook, Twitter, Reddit to join the conversation around the CTF subject and encourage more buyers to recommend this CTF to others. If we use these methods, we can attract an audience and convert the audience into participants.

Business value

The business perspective is to sell the product. We will give the CTF web application, server and domain for USD 399.00, but the domain is valid only for 5 years to estimate the business value.

Time line

Activity	Week											
	1	2	3	4	5	6	7	8	9	10	11	12
Group discussion	🟦											
Requirement gathering	🟦											
Prepare project proposal	🟦											
Levels implementation		🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦		
Prepare a report											🟦	🟦
Testing											🟦	🟦
Make a video												🟦
Final Submission												🟦

YouTube link: https://www.youtube.com/channel/UCLW6ivRWRL7iwDSsCQGVTjQ

GitHub link: https://github.com/PAUdara/Cyber-heist-ctf-project-ISP

END