INFORMATION SECURITY PROJECT

Capture The Flag Project 2020

Mid Review Report

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

SLIIT
Discover Your Future

BSc (Hons) Specializing in Cyber Security
Project - 2020

IE3092 – Information Security Project Year 3, Semester II, 2020

CYBER HEIST

(La casa del ciber)

Drill Plan

We can perform the CTF box as a cyber-drill for DevOps professionals to prepare them to face 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, and familiarity of the Linux OS, programming, encryption methods and other attacks. This CTF challenge will be useful to spread awareness about how not to take the bait in terms of basic cyber security attacks. Therefore, this can be settled as an awareness and training tool for DevOps and trainees.

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. Cyber Heist will be consisted with eleven levels and each level is named after a plan name. Money heist which has an addictive storyline based on a bank robbery and a master mind character called “The Professor”. 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.

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.

Environment

We are using a Linux web server to create this ctf. PHP, Nodejs are used to implement server side and we are implementing the web interface with html, css and java script. We will hide some hints and some awareness tips in the web interface to gain the flags of each level.

Techniques that planning to use in each level:

- Level 1 - Cryptography
- Level 2 - Linux commands
- Level 3 - Web challenge
- Level 4 - Linux commands
- Level 5 - Steganography
- Level 6 - Programming
- Level 7 - Web challenge
- Level 8 - Cryptography
- Level 9 - Forensics
- Level 10 - Database security
- Level 11 – Exploitation

How to be played

First, the contestant is provided with some hints in the home page to find the invite code. The contestant should find out the code and submit as the login password. Then they will be redirected to the instructions page where the main character who is the professor gives the contestants instructions about how to complete the challenge, rules and tips about the challenge. Then, they are redirected to the challenges page which includes all the 11 levels. The level 0 which is a cryptography challenge is unlocked for them to play, while other levels are locked. There will be a button which redirects to the hints of that level. When the contestant follows the hints and find the flag, he/she should submit the flag into the give form and then will be directed to a page which gives some sort of an awareness about the attacks which could happen for the specific topic. After that the next level will be unlocked. Likewise, all the first six levels will be played. When a contestant completes the six levels they will be rewarded with a special anonymous name. The contestant will be rewarded with a city name according to the storyline. Then they should complete the next levels which will be hard and consider more time.

Invite code

In this ctf we implement this to get an invite code before login to the ctf. After that the player can login using invite code and name. This invite code is an auto generated random number for each participant. To get this invite code, the first player must go to the view page source, and the player can see text with h3 tag but it does not appear in the page. And it has a class name called “find”. It says there is a file that colours up this website. It means, there is a main.css file in all pages in the website. Then contestant must go to it and he/she can see in the css part that is implemented to the "find' class. Contestant can see rot13 encoded message as a comment. Then they copy it and decode it. This says that cookie value will help to find invite code, this means invited code is stored as cookie content value. Now they can see it has base64 encrypted invite code, then we decrypt it and get it. Finally, player can login using it.

Level 1

The contestant is redirected to a page where there is a single picture, and we give the hint as “images will help you”, but in the source code there are two pictures in the source code to mislead the contestants, the encoded message is actually in the picture which is displayed in the page. Again the player will see the html code that used to display that image, but the player cannot see the exact image file. Hence contestant must remember the class name of that html code and go to the css file. When the contestant goes to the main css file and searches the corresponding image file using class name. The founded image file path should be pasted in the URL, then the image should be displayed. Then they should download and open the image using cat. There is a base 64 encoded message, and contestant can decode it using command or online decoders. After that player will get the hex value, and he/she wants to decode it again to the ASCII value. Finally, they can get their first flag message.

Level 2

This level is a Linux command based challenge. We give some hints to this level in the redirected page. First contestant must use dirb command to find directories that are in this site, then he/she will see the level directory. When the player goes to the level directory, he/she can see the level 2 folder. Then contestant must find the correct file using hint. If contestant found the file, he/she wants to download the file and find the unique flag in this file using Linux commands.