Sri Lanka Institute of Information Technology

Information Security Project

3rd Year 2nd Semester

CATCH ME IF YOU CAN

Walkthrough

AMARATHUNGA A.A.S.R.	IT15028938
RASHAN PASINDU K.A.	IT16006126
JAYAKODI S.M.P.V.	IT16522466

Contents

Introduction

- Main Operating System – Kali Linux
- There are 11 levels and 11 flags to be captured.
- Each level contains a clue about the flag.
- **No table of figures entries found.**submission will reduce the number of tries by 1.

Scenario

There is a server breach happened at SLIIT. The person who breach into the server room left a FLAG accidently, which can identify him. As a cyber expert it's your duty to find that FLAG and identify the anonymous person. To do that you have to go through a process.

Level 1

Method: Here focus is analyzing the source code and get the decode text.
Then the player must figure out what kind of encoding type it is and get the correct flag to login to the system.

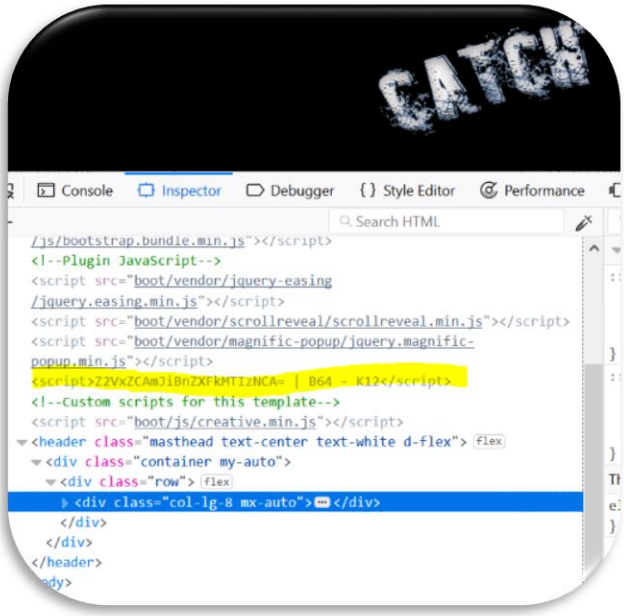


Figure 1.1 Source Code

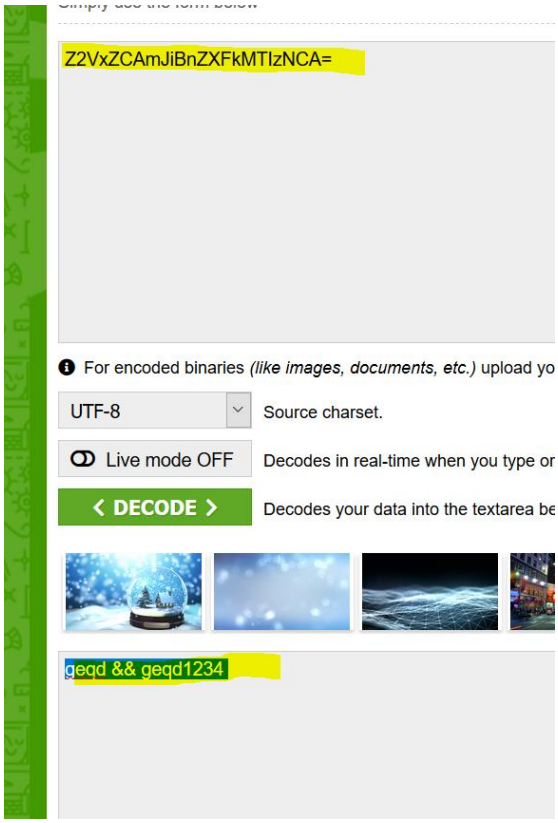


Figure 1.2 Base 64 Decode

Figure 1.3 Shift Cipher Decode

Tools Required: No tools required

Flags : Username = **user** Password = **user1234**

Level 2

Method: Steganography is the method used in this level. A text is hidden under the downloadable picture. Player must get the text and decode that text in order the get the correct flag.

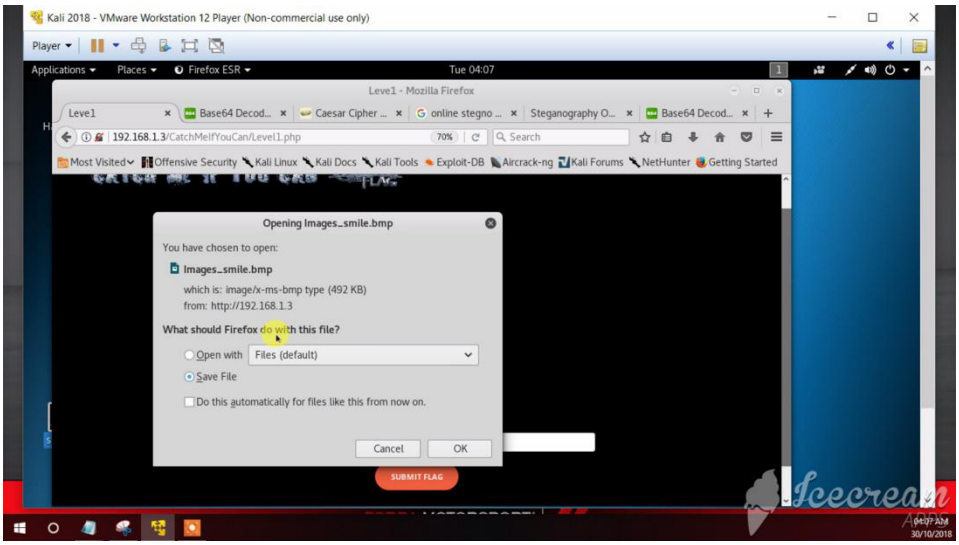


Figure 2.1 download the image

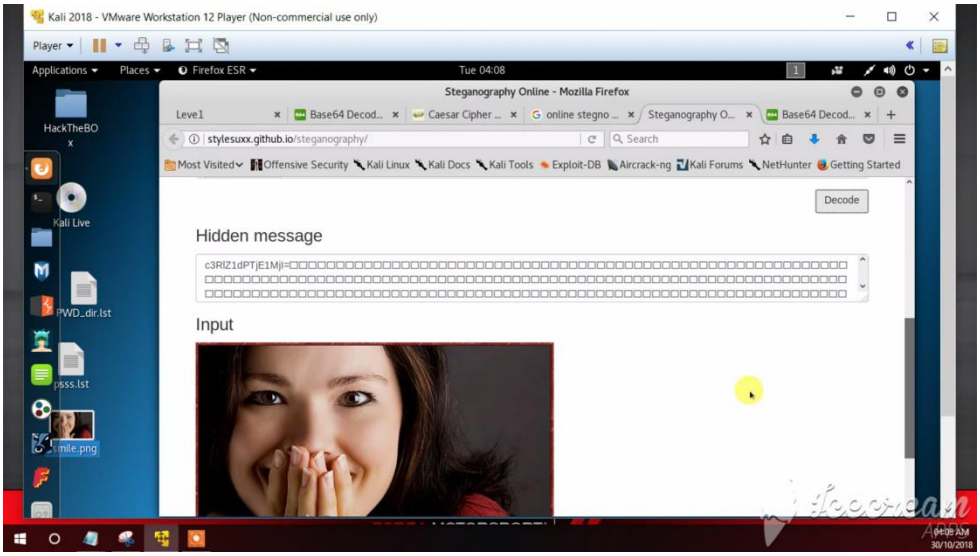


Figure 2.2 Decode using a tool

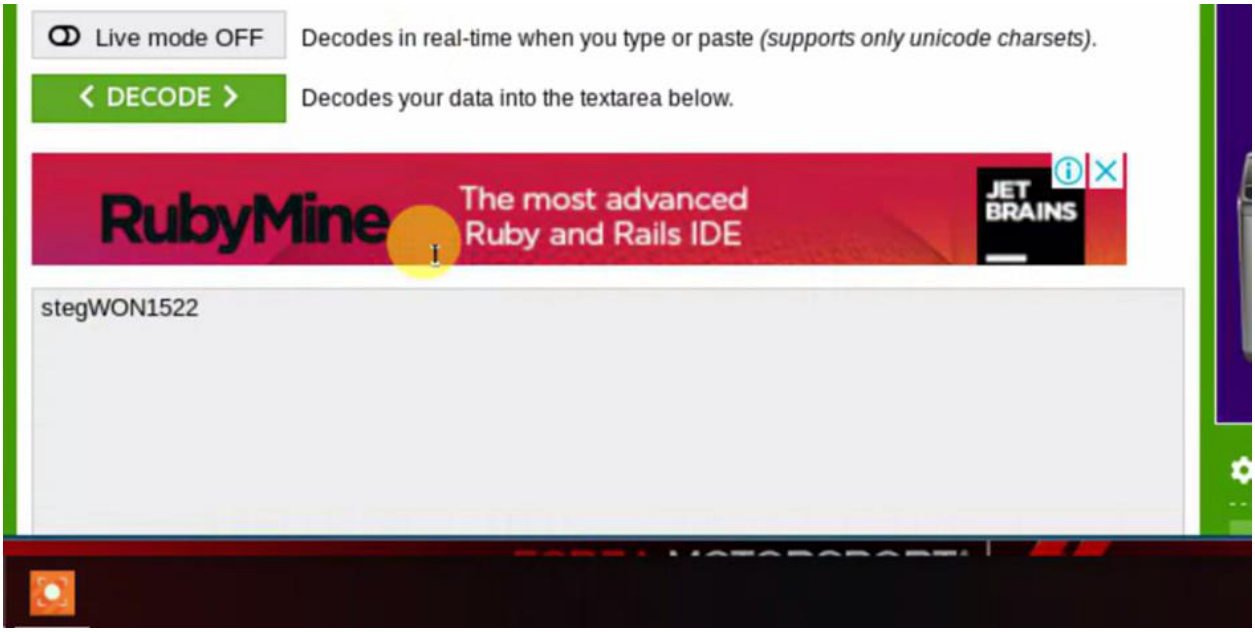


Figure 2.3 Get the flag by base 64 decoding

Tools required: S tool or any other tool which can decode steganographic files.

Flag: **stegWON1522**

Level 3

Method: Morse code is used here. Player has to download the attached text file and identify the pattern.

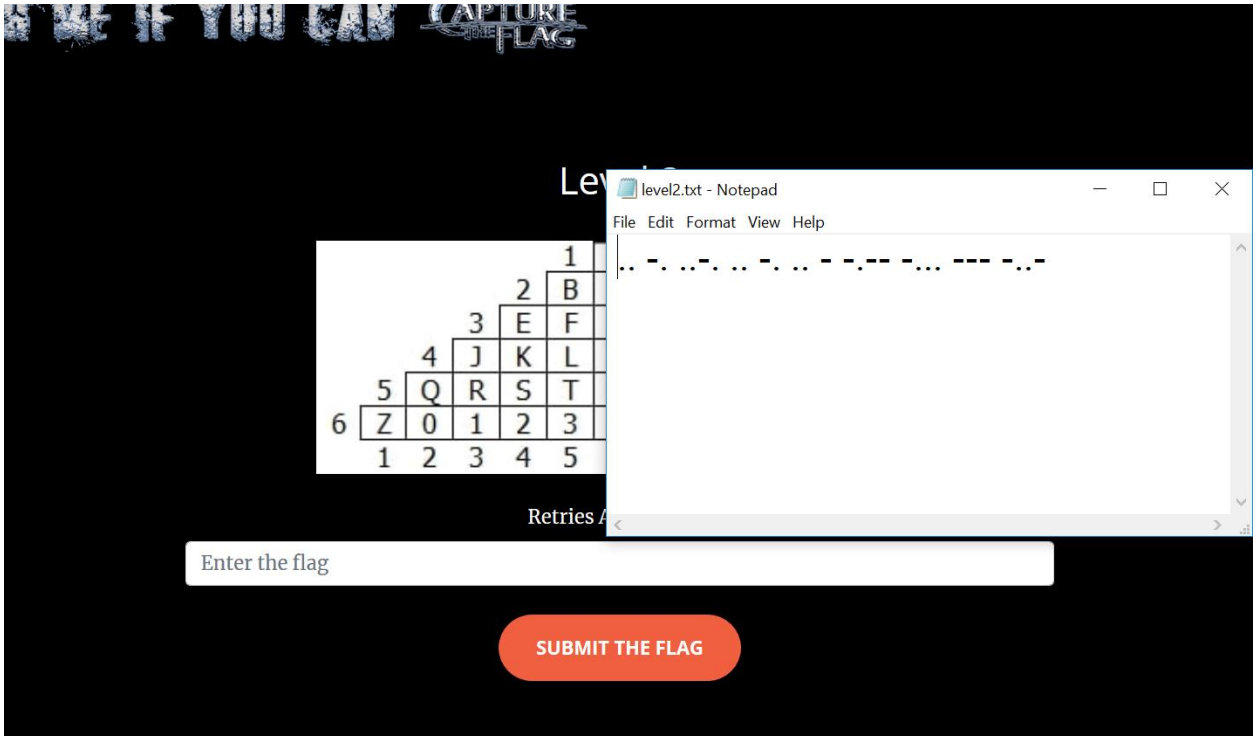


Figure 3.1 Download the Morse code file

Tools required: Any online tool which can use to decrypt Morse code.

Flag: **INFINITYBOX**

Level 4

Method: Linear Shift Feedback Cipher is used. In this level the player must have knowledge about how LFSR works. Player must draw and get the output of the LFSR.

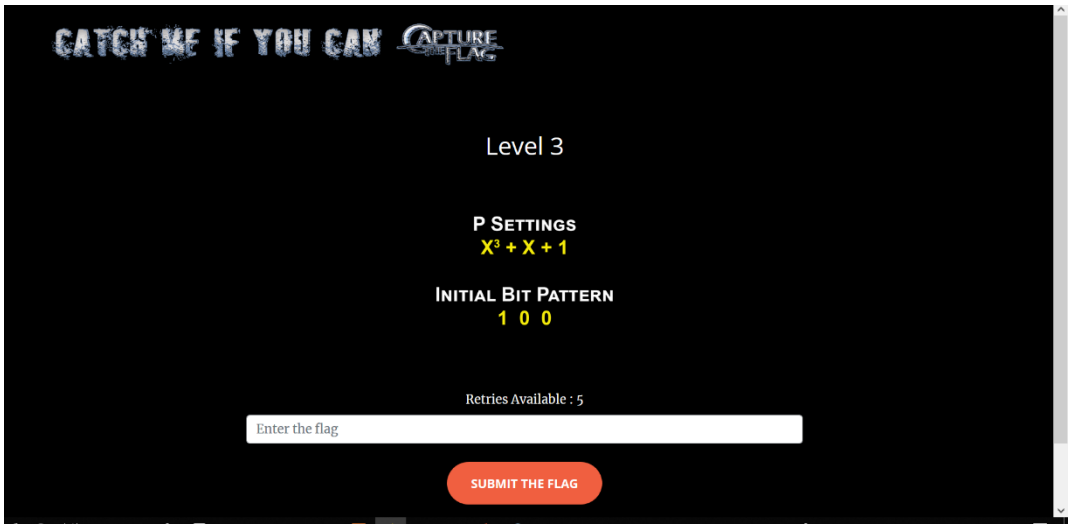
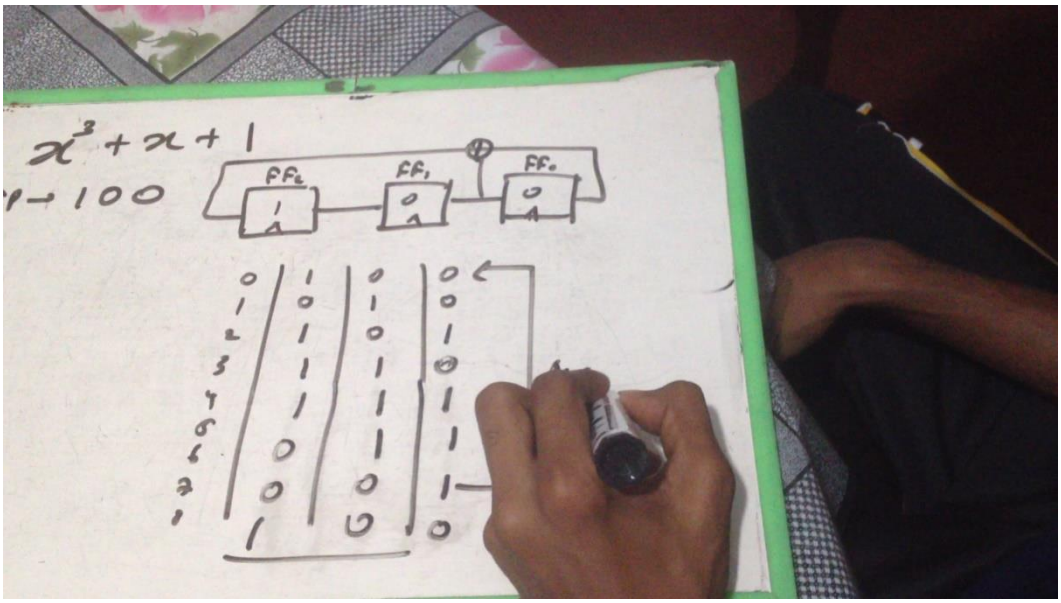


Figure 4.1 Linear Feedback Shift Cipher



4.2 Solve the LFSR and get the bit pattern

Tools Required: No tools required. But Player should have the basic knowledge about LFSR.

Flag: **00101110**

Level 5

Method: This level is about Dumpster diving. This level comes under digital forensics. Downloadable dump is given. Player must find the level key hidden in the dump using a tool.

Figure 5.1 Open Autopsy

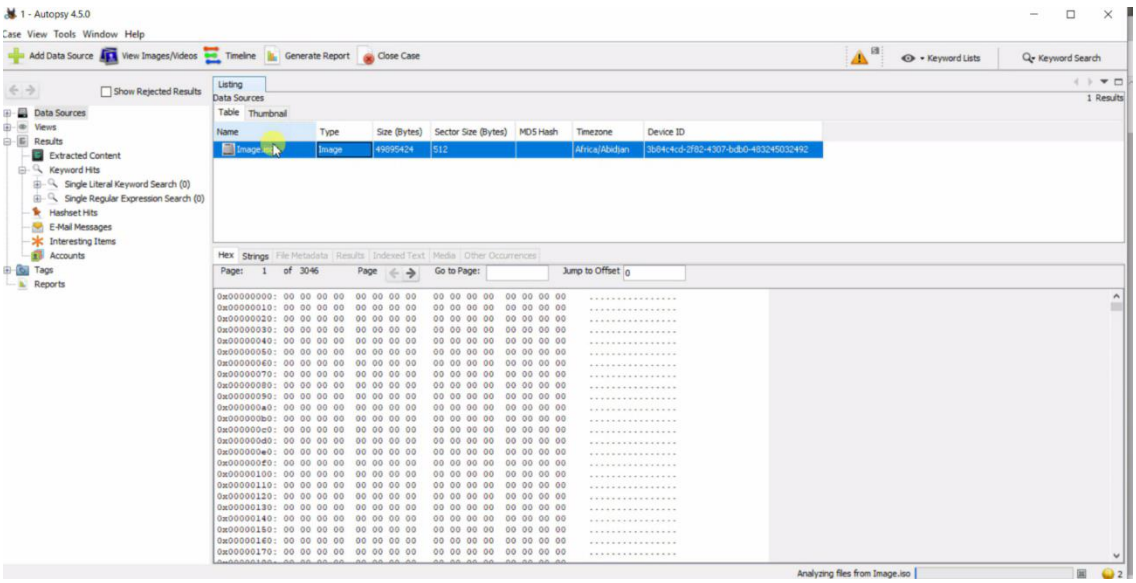
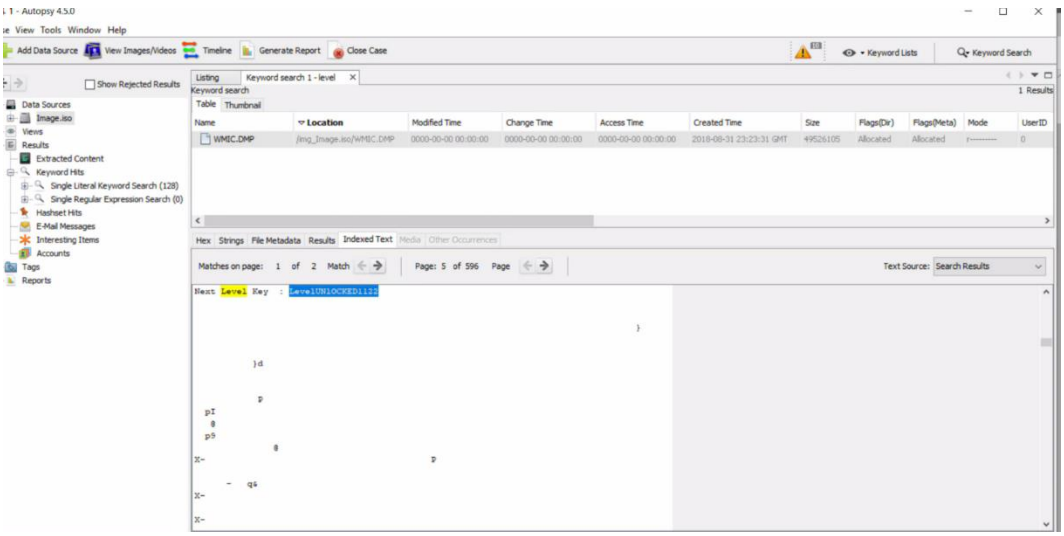


Figure 5.2 Load iso dump file to autopsy tool



5.3 Search for the flag

Tools required: Autopsy or any similar tool.

Flag: **LevelUNLOCKED1122**

Level 6

Method: To pass this level you must by pass it. That's the only way you can go to the next level.

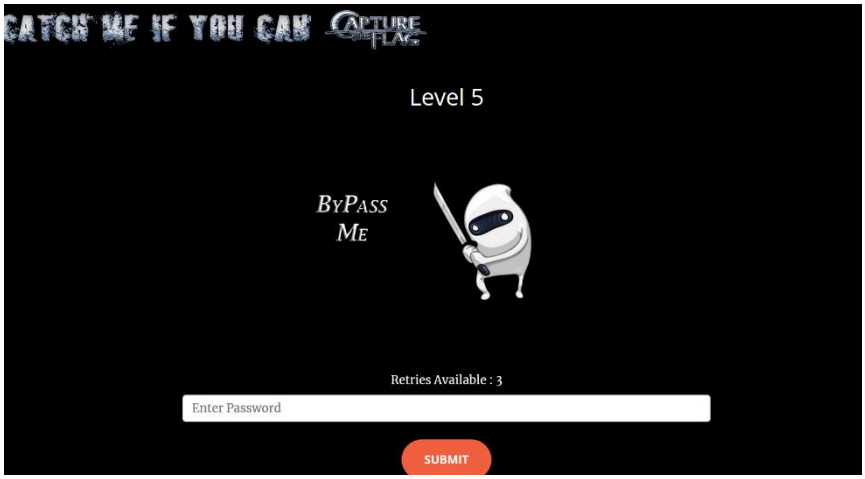


Figure 6.1 Page to bypass

Tools Required: No tools required. But player must have the basic knowledge about SQL Injection.

Flag: **' or 1=1-- - (or any other sql injection method)**

Level 7

Method: This level is on tiny Encryption. Player must first understand that this level must do using tiny algorithm. Clue is given.

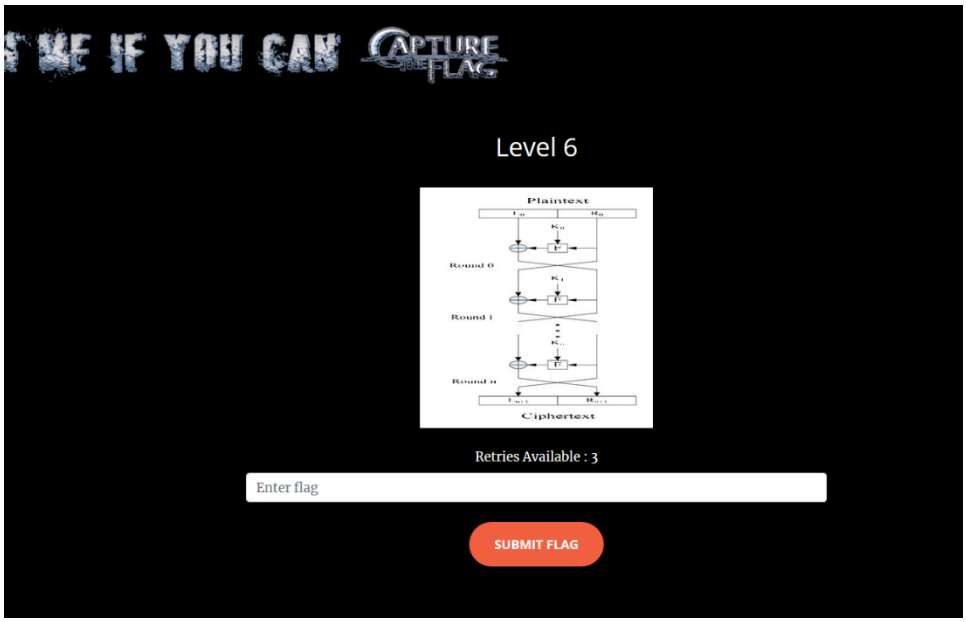


Figure 7.1 Tiny encryption

Tools required: Any online tool which can decrypt cipher text encrypted using tiny algorithm.
Flag: **congratsNextLevelUnlocked**

Level 8

Method: This is a cookie-based attack. A cookie is generated manually. The player has to find and submit the value of that cookie as the flag.

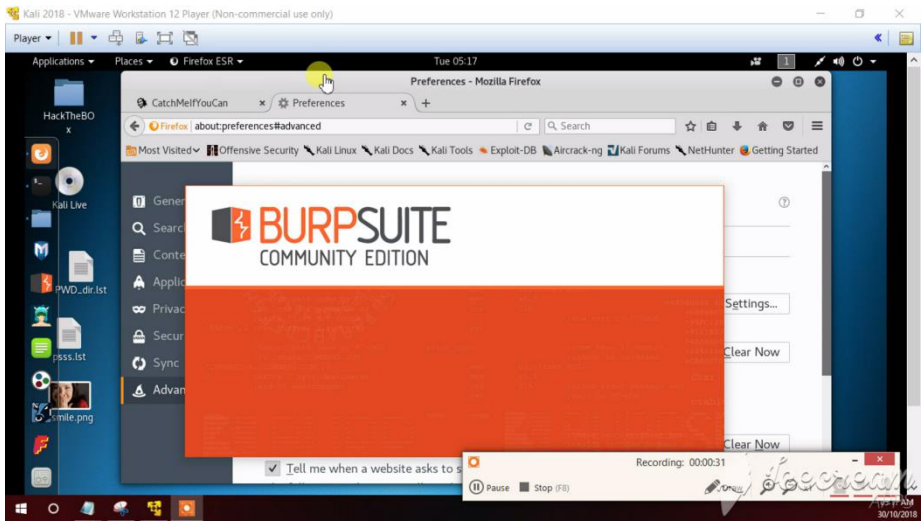


Figure 8.1 Open BurpSuite

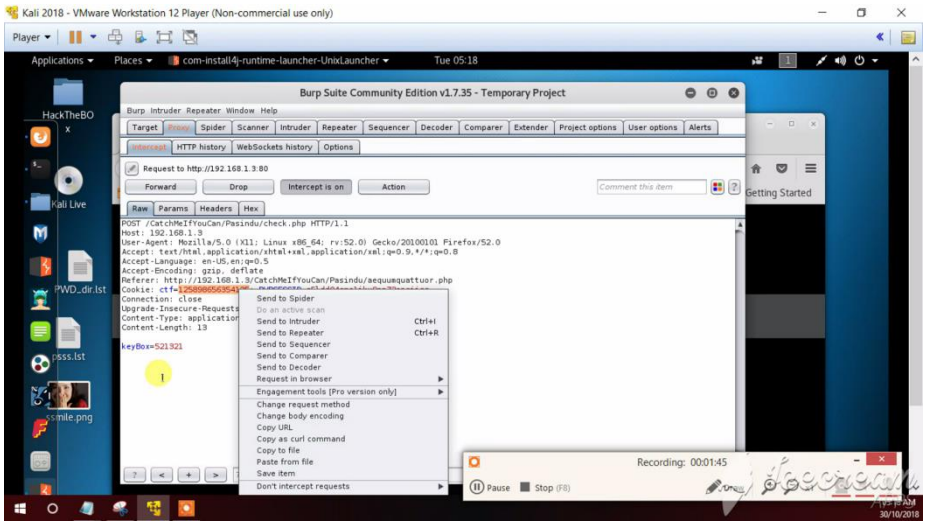


Figure 8.2 Make connection with burpsuite and check the cookie value

Tools Required: Burp Suite of any similar tool.

Flag: **125898656354125**

Level 9

- Method: AES Encryption is used in this level. Player should find the hidden encrypted cipher text and the key. Then use the hints to navigate through the 1GB of encrypted cipher text and find the flag by decrypting it.

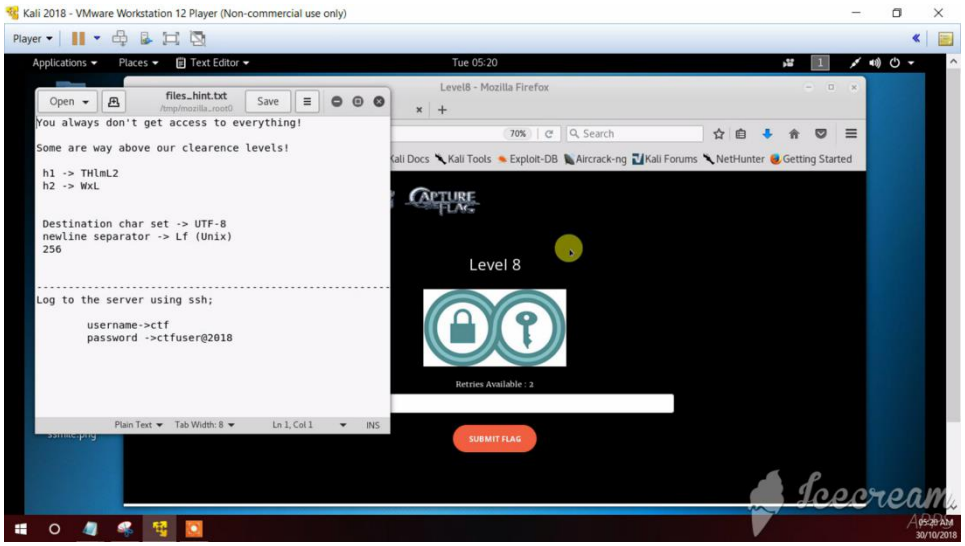


Figure 9.1 download the hint file

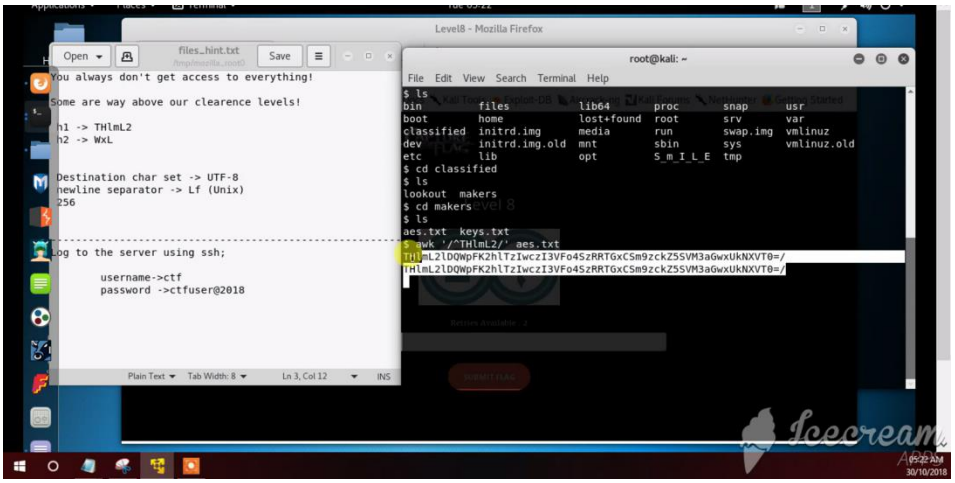


Figure 9.2 Find the hidden cipher text and the key

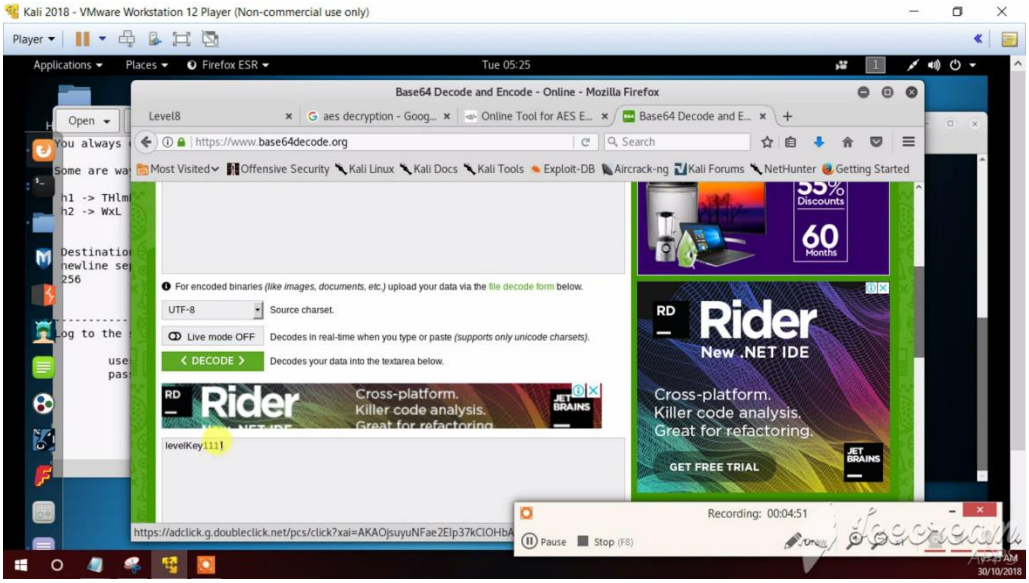


Figure 9.3 Decode the cipher text and get the flag

Tools Required: a Base 64 decoder and basic Linux command knowledge.

Flag: **levelKey1111**

Level 10

Method: Packet and Protocol analysis is used in this level. The player has to analyze the given ***pcap*** file and find out what kind of attack it is and submit the type of the attack as the flag.

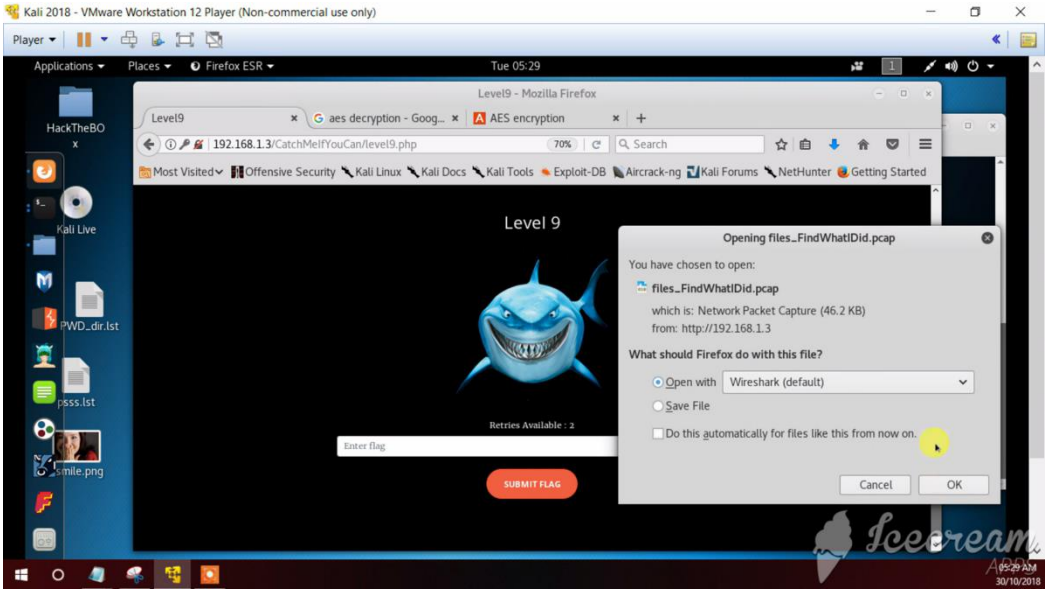


Figure 10.1 Downlaod the pcap file

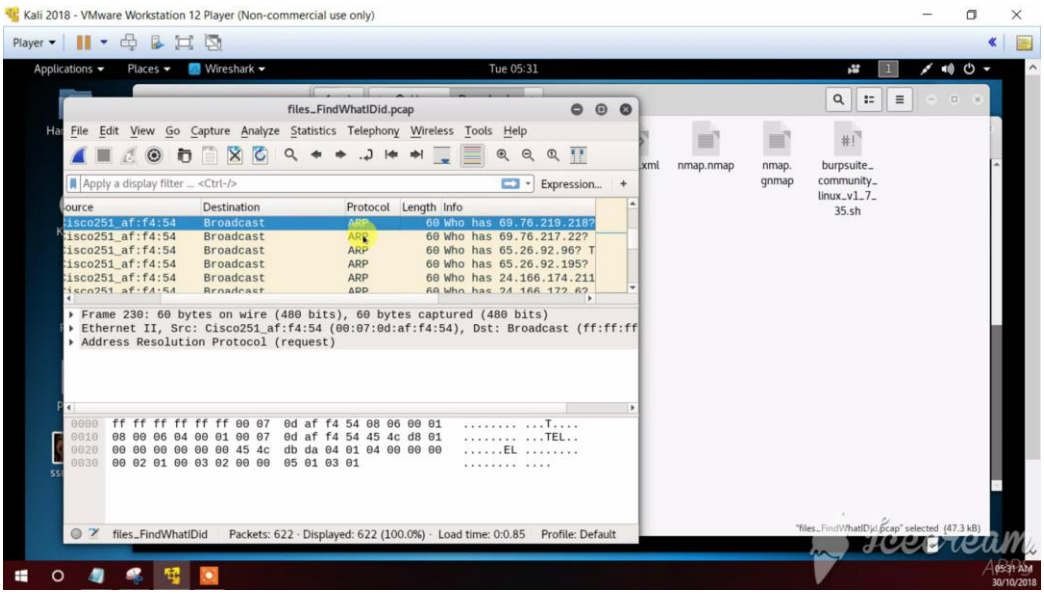


Figure 10.2 Load it to Wireshark

Tools required: Wireshark or any other packet analyzing software.

Flag: **arpstorm**

Level 11

Method: BruteForse attack is used in this level. This is the final level as well. To pass the final level player must make a bruteforse attack and find the correct flag. A password list is given.

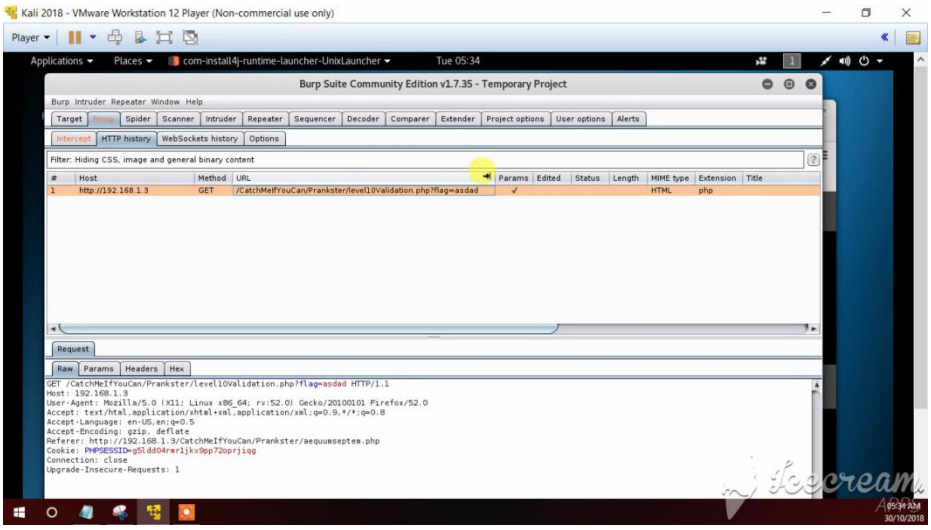


Figure 11.1 Send a get request after connecting to burp suite

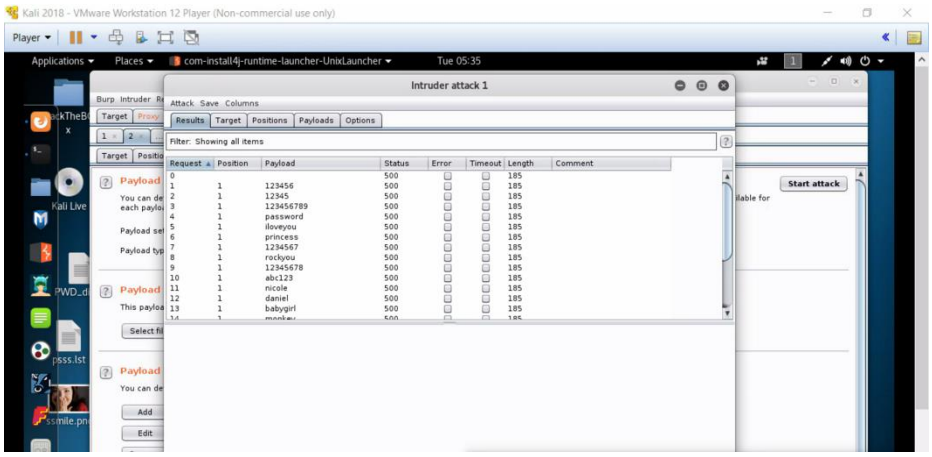


Figure 11.2 do the brute force using the given list

Tools required: BurpSuite or similar tool.

Flag: **zxcvbnm**

Conclusion

CATCH ME IF YOU CAN is a CTF box with a moderate difficulty level. This is best for the beginners in capture the flag challengers and anyone including people who doesn't open to cyber field. This is a good CTF box to welcome you for the CTF challenge world.