DARK WINDEN

CTF PROJECT PROPOSAL

Team Members

Student ID	Name
IT18118964	K.M.Samarasekara
IT18121148	H.M.G.V.Perera

Table of Contents

Introduction

Capture the flag, generally referred to as the CTF, is a popular outdoor game where two more teams each have a flag or other symbol and the goal is to catch the flag of the other side. In the information security context, the CTF case is an experiment that we set up to solve information security challenges and participate in innovative experimentation in a controlled atmosphere with minimized implications for the operation gene.

This CTF case focuses primarily on risk evaluation and penetration detection skills. Students who design applications must acquire expertise in the construction of stable networks, project management, teamwork, risk detection, and penetration testing skills. The main goal of this CTF is to promote security practices in the industry.

Dark is a German science fiction family drama series that focuses on Time Travelling. Dark was created by Baran bo Odar and Jantje Friese. Set in the fictional small town of Winden, it revolves around four interconnected families haunted by their secrets and contains elements of science fiction and fantasy. There is a complex family tree as well as connections among the characters in the storyline. This CTF is based on these connections along with the events that occurred. This CTF is made to make the users aware of Ransomware from the point of execution to recovery. The goal of this CTF is to get the decryption key once the Ransomware is executed, and finally decrypt the “pass.txt” file that has been encrypted by the Ransomware and that is stored in the root directory. Once the player starts playing the CTF, the first instruction will be given to make sure that the user runs an executable file named “start” which is in the home directory which will eventually act as the trigger to for the Ransomware program to be executed.

Architecture

The architecture of this CTF can be divided into five main sectors.

1. Front end

The web frontend for this CTF is built using HTML (Hypertext Markup Language) and Bootstrap User Interface Framework. HTML is the most basic building block of the Web. It defines the meaning and structure of web content. Other technologies besides HTML are generally used to describe a web page's appearance/presentation (CSS) or functionality/behavior (JavaScript). Bootstrap is a potent front-end framework used to create modern websites and web apps. It is open-source and free to use yet features numerous HTML and CSS templates for UI interface elements such as buttons and forms.

2. Hosting, Storage, and Technologies being used

The CTF is created and executed in an Ubuntu EC2 Instance of Amazon Web Services. This has a Nginx instance as well as the levels running at any moment. PHP is used as the server-side scripting language.

3. Levels

There are 10 levels in this CTF that should be solved to complete the CTF. Initially, the players will be getting an HTML page for each level to upload the captured flags of each level to proceed to the next level. Each level is based on a scenario or a complex character in the Dark Series. The technologies to solve each level is as follows:

Level 1 - A source code analysis

Level 2 - Web Exploitation (Finding and accessing a backdoor)

Level 3 - SQL Injection

Level 4 - Packet Analysis

Level 5 - Password Cracking

Level 6 - Debugging. ASCII

Level 7 - Cross-site scripting

Level 8 - Reverse engineering

Level 9 - Steganography

Level 10 – Cryptography

After solving the 10^{th} level, the player will get the decryption key which can be used to decrypt the encrypted “pass.txt” file. Once the file is decrypted, the player will find the final flag inside, which can be entered in to the web application where the flags must be entered in order to successfully complete the CTF.

Drill Plan

The CTF is based on a how to take action against a Ransomware attack. Ransomware attacks are typically carried out using a Trojan, entering a system through, for example, a malicious attachment, embedded link in a phishing email, or a vulnerability in a network service. Once the files are encrypted, the attackers will ask for a ransom to release the decryption key to decrypt the encrypted files. In this case, we can assume that the attackers had hidden the decryption key in the same instance with complex challenges to be solved, puzzles to be sorted to get the decryption key. The objective of this CTF is to make the players aware of how a decryption and recovery process of a Ransomware attack works.

Theme

Dark is a German science fiction thriller web television series co-created by Baran bo Odar and Jantje Friese. It ran for three seasons, from 2017 to 2020.this story start from Children vanishing from the German town of Winden, bringing to light the fractured relationships, double lives, and dark past of four families living there, and revealing a mystery that spans four generations.

The story begins in 2019 but spreads to include story-lines in 1986 and 1953 via time travel, as certain characters of the show's core families grow aware of the existence of a wormhole in the cave system beneath the local nuclear power plant, which is under the management of the influential Tiedemann family. During the first season, secrets begin to be revealed concerning the Kahnwald, Nielsen, Doppler, and Tiedemann families, and their lives start to crumble as the ties become evident between the missing children and the histories of the town and its citizens.

The second season continues the intertwining families' attempts to reunite with their missing loved ones, several months after the first-season finale, in 2020, 1987, and 1954, respectively. Additional story-lines set in 2053 and 1921 add new aspects to the mysteries, and the secret Sic Mundus fellowship, a major force in an underlying battle for the ultimate fate of the people of Winden, is explored, as the season counts down towards the apocalypse – the destruction of Winden and death of many of its citizens.

The third and final season follows the four families across time in the wake of the apocalypse in 2020, while also introducing a parallel world whose events are interconnected with those of the first world. The season is primarily set in 1888, 1954, 1987, 2020 and 2053 in the first world, and 2019 and 2052 in the second world, as the characters work to find a way out of the repeating cycle of events in Winden across both worlds

Budget

Task	Price
Developing Expenses	Approx. Rs. 5000.00/-
Hosting	Approx. Rs 5000.00/-
Marketing	Rs 2000.00/-
Total	**Rs. 12000.00/-**

Market Plan/Pricing

The main target audience of this CTF is who is focusing on cybersecurity at large corporates who may or may not have experienced a ransomware attack. This CTF can be used by anyone interested in solving challenges as well as who would like to have an exposure to addressing ransomware. The market plan would be to create a social media presence for this CTF once it's hosted and then promote it through advertising and sponsorships. Meanwhile, this CTF should be introduced to corporates as a paid package of Rs. 15000/-. This will include a free tutorial on how to solve it as well as a free guide on how to avoid ransomware.

Business Value

The objective of this CTF is to make the players aware of how a decryption and recovery process of a Ransomware attack works. This will make awareness for users about the criticality of Ransomware. The users will learn not to click on click on unverified links, not to open untrusted email attachments, only to download from trustable websites, keeping the software updated, etc. Not only this will protect an organization's data, but this will also save lots of money. Furthermore, they can be interested in trying to decrypt the encrypted data by searching for the encryption key in a case where ransomware has occurred.

Timeline

Activity	week											
	1	2	3	4	5	6	7	8	9	10	11	`12
Group discussion												
Requirement gathering												
Preparing project proposal												
Levels implementation												
Prepare a report												
Testing												
Making video and post												
Submission												

GitHub Repository - https://github.com/darkwinden33/ctf

YouTube Channel - https://www.youtube.com/channel/UC3apJ2xGGlz446-wa1oTOgA