SERVIZIO GRADED_LIST CTF 2019

-Jelly Hinge Team-

1 Introduzione

Graded_list è uno dei servizi della CTF dell'UNICT 2019, per ottenere la flag non bisogna eseguire un attacco classico ma, piuttosto, analizzare logicamente le funzionalità.

2 Il servizio

Il servizio presenta un'interfaccia a riga di comando accessibile via netcat. Il programma richiede l'inserimento di 5 parametri per calcolare un punteggio finale. Per ottenere la flag è necessario riuscire ad ottenere il primo posto nella classifica. I parametri richiesti per il calcolo del punteggio sono: due stringe alfabetiche, "**name**" e "**surname**" di massimo 10 caratteri per stringa, e tre valori numerici con range da 0 a 255: "**income**", "**credits**", "**sum of your votes**". Dopo aver inserito i 5 parametri il programma mostra un record con i valori appena aggiunti seguito dal punteggio ottenuto, la posizione in classifica, una serie di nomi non meglio identificati ed altri valori di poca importanza.

2.1 Indizi

Dalla sola interfaccia disponibile non risultano esserci evidenti indizi.

3 Analisi

Dalla descrizione del servizio si evince che l'obiettivo è di ottenere un punteggio più alto possibile per risultare primi in una, non meglio specificata, classifica, quindi risulta necessario capire in che modo le variabili inserite vengono utilizzate per il calcolo finale. Empiricamente risulta evidente che le tre variabili numeriche, che per comodità chiameremo in ordine di inserimento x, y e z, sono utilizzate nel seguente modo: **score = x - y + z**, ma il punteggio finale appare influenzato da altri fattori. Sperimentando si intuisce che gli unici altri valori

che possono influenzare lo score sono i primi due parametri alfabetici "**name**" e "**surname**". Sempre empiricamente si verifica che viene eseguito uno XOR carattere per carattere delle prime due stringhe inserite e che il risultato di questo viene sommato ad una costante di valore "12". Per dimostrare la costante basta inserire nei 5 parametri tutti valori nulli: quindi non inserendo nessun carattere nelle prime due variabili e tutti "0" nelle 3 successive, il risultato finale sarà "12", la costante ; mentre lo XOR si dimostra nel seguente modo: inserendo i caratteri "a" e "b" rispettivamente in "**name**" e "**surname**" , e "0" nei successivi valori, il servizio calcolerà uno punteggio di "**15**" ; lo XOR viene eseguito tra le rispettive forme binarie dei caratteri ASCII "a" e "b", ovvero "1100001" e "1100010" , il risultato binario "11" corrispondente a "3" in decimale; quindi sostituendo i valori nella formula: XOR(name,surname) + const –x + y + z = 3 +12 – 0 + 0 + 0 = **15**.

4 Risultati

Per ottenere un punteggio elevato è quindi necessario scegliere un "**name**" e un "**surname**" tali che la somma degli XOR dei singoli caratteri sia sufficientemente grande, ad esempio scegliendo una stringa di 10 caratteri "A" come "**name**" e una stringa di 10 caratteri "z" come "**surname**" con i valori **x** più basso possibile e **y**, **z** più alti possibile si ottiene un valore abbastanza grande da risultare primi nella classifica. Ma questo ancora non risulta sufficiente ad ottenere la flag dal servizio, un suggerimento dopo aver raggiuto un punteggio alto indica che siamo andati troppo oltre, questo porta ad una reinterpretazione del messaggio iniziale: non si deve ottenere semplicemente il punteggio più alto scavalcando tutti in classifica, ma ottenere esattamente il punteggio del primo classificato. Non essendo a conoscenza di quale sia questo punteggio non rimane altro che ricercarlo basandosi sulla posizione raggiunta indicata dal servizio, ovvero aumentare il punteggio quando si arriva ad una posizione inferiore alla prima e diminuirlo quando si riesce ad ottenerla senza ricevere la flag. Per fare ciò risulta ottimale variare i 3 valori numerici che si hanno a disposizione (eseguendo una ricerca dicotomica per velocizzare il processo), per ottenere il punteggio esatto corrispondente a: 1069.

5 Link

Alla pagina github ufficiale dell'evento è possibile trovare il codice sorgente del servizio, non disponibile durante la CTF, in quanto avrebbe reso evidente le operazioni che venivano eseguite con le variabili, di fatto rendendo la sfida inutile. Oltre al codice sorgente sono disponibili una serie di file per rendere il servizio utilizzabile, come la classifica dei punteggi, e uno script scritto in python in grado di eseguire automaticamente le operazioni necessarie per l'ottenimento della flag.

https://github.com/unictf/unictf-2019/tree/master/services/graded_list