EPICODE

Esercizio S7 – L4

TRACCIA

Abbiamo già parlato del buffer overflow, una vulnerabilità che è conseguenza di una mancanza di controllo dei limiti dei buffer che accettano input utente.  
Nelle prossime slide vedremo un esempio di codice in C volutamente vulnerabile ai BOF, e come scatenare una situazione di errore particolare chiamata «segmentation fault».

SOLUZIONE

Per prima cosa si scrive il codice vulnerabile al Buffer overflow in un file di testo.

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

Si salva il codice sul Desktop e lo si compila con il primo comando sotto riportato. Poi lo si esegue. In questo caso il codice funziona senza problemi perché l’utente ha inserito meno di 10 caratteri.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Se si eseguono più di 10 caratteri è possibile notare la situazione di errore particolare chiamata “segmentation fault”, ovvero un errore di memoria che si presenta quando un programma cerca inavvertitamente di scrivere su una posizione di memoria dove non gli è permesso scrivere

Immagine che contiene testo, schermata, Carattere, linea

Descrizione generata automaticamente

Per risolvere questo problema è possibile utilizzare “fgets” al posto di “scanf”. Così facendo il programma leggerà solamente i primi 9 caratteri inseriti in input dall’utente.

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

Sotto riportato l’effetto di “fgets” che risolve il problema del Buffer overflow.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente