W17D5

BUFFER OVERFLOW

La traccia

Traccia:

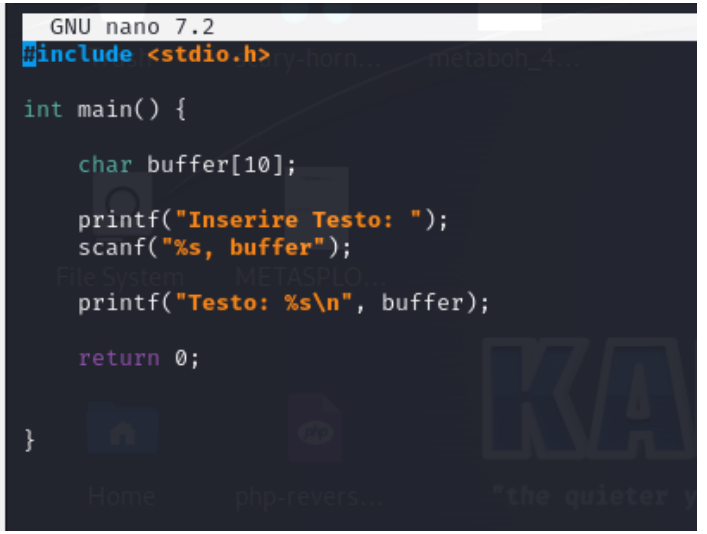
Nella lezione dedicata agli attacchi di sistema, abbiamo parlato dei buffer overflow, una vulnerabilità che è conseguenza di una mancanza di controllo dei limiti dei buffer che accettano input utente.

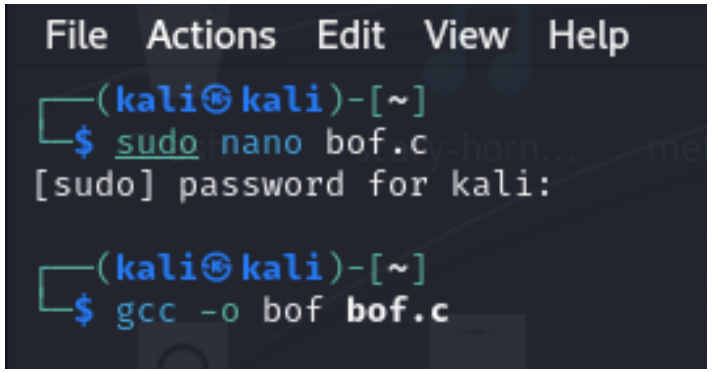
Nelle prossime slide vedremo un esempio di codice in C volutamente vulnerabile ai BOF, e come scatenare una situazione di errore particolare chiamata «segmentation fault», ovvero un errore di memoria che si presenta quando un programma cerca inavvertitamente di scrivere su una posizione di memoria dove non gli è permesso scrivere (come può essere ad esempio una posizione di memoria dedicata a funzioni del sistema operativo).

Avvio msfconsole e preparazione attacco.

Scrivo il file in ‘c’ che mi permetterà di verificare l’ipotesi di ‘segmentation default’.

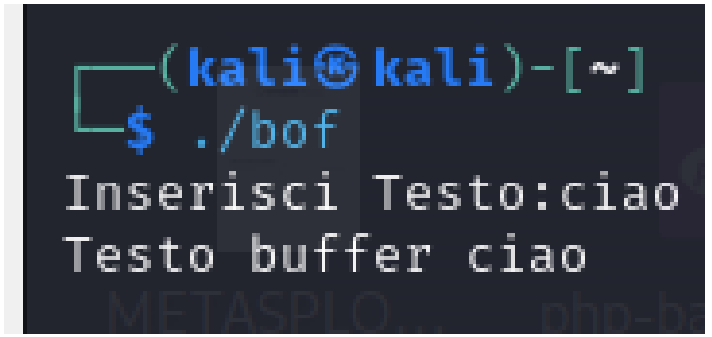
Analizzando velocemente il codice creo un array di caratteri e lo compilo con gcc.





Avvio msfconsole e preparazione attacco.

Se scrivo entro il buffer non succede nulla, mi fa il display di quanto scrivo in input.
Se vado oltre la dimensione dell'array il programma andrà in segmentation default.




```
(kali㉿kali)-[~]
$ ./bof
Inserisci Testo:kefwmkemkemvkewrmvklemvklermklwmelwmkeklwmewklvmeklmverklwmklwmvklwemvlkmerklmlemvlkwmlvkewmklmwklmlkwmvlwemke
mklwmklemklmewklvmweklemwkemwklmewklvkewlmlkwv
zsh: segmentation fault  ./bof
```