Cyber Security & Ethical Hacking

Buffer overflow

Compito S7-L4 Aguglia Andrea

Buffer overflow

File Actions Edit View Help

```c
#include <stdio.h>

int main ()  {

char buffer [10];

printf ("Si prega di inserire il nome utente:");
scanf ("%s", buffer);

printf ("Nome utente inserito: %s\n", buffer);

return 0;

}
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ./Buffer
Si prega di inserire il nome utente:qwertyuiop
Nome utente inserito: qwertyuiop

┌──(kali㉿kali)-[~/Desktop]
└─$ qwertyuioplkjhgfdsazxcvbnmqwert
qwertyuioplkjhgfdsazxcvbnmqwert: command not found
```

Il buffer overflow è una vulnerabilità di sicurezza che si verifica quando un programma, durante l'esecuzione, scrive più dati in un buffer di memoria di quelli che il buffer può gestire. Un buffer è una zona di memoria temporanea utilizzata per immagazzinare dati, come stringhe di caratteri o array. Se un programma non controlla accuratamente la quantità di dati che scrive in un buffer e supera i limiti di memoria assegnati al buffer, può verificarsi un overflow.

Buffer overflow

```c
#include <stdio.h>

int main ()  {

char buffer [40];

printf ("Si prega di inserire il nome utente:");
scanf ("%s", buffer);

printf ("Nome utente inserito: %s\n", buffer);

return 0;

}
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nano Boff.c

┌──(kali㉿kali)-[~/Desktop]
└─$ gcc -g Boff.c -o Boff

┌──(kali㉿kali)-[~/Desktop]
└─$ ./BOff
zsh: no such file or directory: ./BOff

┌──(kali㉿kali)-[~/Desktop]
└─$ ./Boff
Si prega di inserire il nome utente:qwertyuiopasdfghjklzxcvbnmqwert
Nome utente inserito: qwertyuiopasdfghjklzxcvbnmqwert
```