Gameshell guida e risoluzione

Mattia Carlesso 19/04/2025

Gameshell è un gioco open sourche trovabile su github,

insegna tramite un ambientazione fantasy su comand promp di Linux tramite una serie di missioni e task ad utilizzare i comandi Shell di Linux.

Ho scaricato il gioco quando consigliato dal professore di Teoria alla prima lezione del modulo 2 ho iniziato a comprenderlo piano piano nel tempo libero e il gioco mi ha intrigato nel tempo.

```
zsh: corrupt history file /home/kali/.zsh_history
$ gitclone https://github.com/phyver/GameShell.git
gitclone: command not found
   -(kali@kali)-[~]
$ git clone https://github.com/phyver/GameShell.git
Cloning into 'GameShell' ...
remote: Enumerating objects: 16031, done.
remote: Counting objects: 100% (1074/1074), done.
remote: Compressing objects: 100% (512/512), done.
remote: Total 16031 (delta 700), reused 611 (delta 556), pack-reused 14957 (f
Receiving objects: 100% (16031/16031), 5.50 MiB | 6.02 MiB/s, done.
Resolving deltas: 100% (10687/10687), done.
  -(kali⊕kali)-[~]
s cd gameshell
cd: no such file or directory: gameshell
   -(kali@kali)-[~]
$ cd GameShell
  -(kali⊗kali)-[~/GameShell]
$ ls mages
doc i18n lib Makefile README-fr.md README.md start.sh
Dockerfile Images LICENSE missions README-it.md scripts utils
___(kali⊛kali)-[~/GameShell]
```

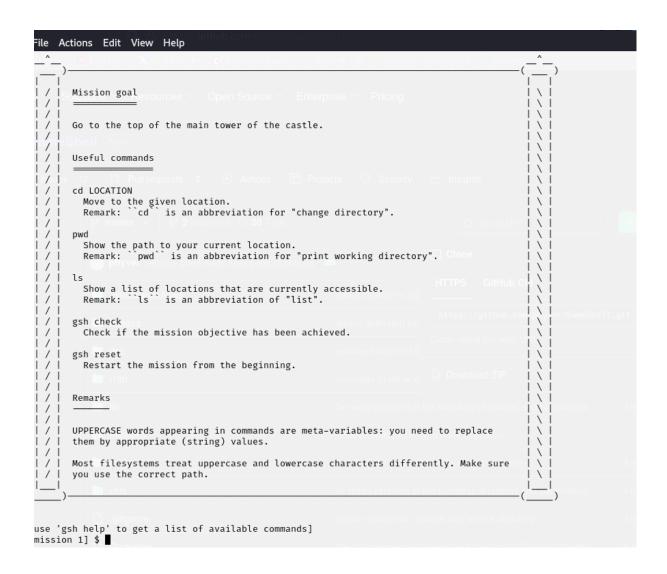
questi sono i comandi utilizzati per scaricare il file:

ho utilizzato git clone e il link https per ottimizzare e il download.

con cd GameShell sono entrato nella directory del "gioco"

con il comando ls ho visto la lista.

con il comando ./ start.sh ho avviato il gioco



il gioco si presenta così le missioni sono sono un totale di 44 missioni suddivise per varie categorie.

dall' 1 al 10 contengono la categoria di permessi e file system

gli obbiettivi sono di imparare a navigare attraverso le directory, leggere i file e gestire i permessi.

dai livelli 11 al 20 gli obbiettivi sono quelli di imparare le escalation di permessi e script

dal livello 21 al 30 gli obbiettivi sono interagire con i servizi di rete individuare le porte aperte e i socket

dal livello 31 al 38 gli obbiettivi sono di imparare a decifrare i file, rompere le password e effettuare qualcosa identificato da me come reverse engineering

dal livello 39 al livello 44 è una serie di combinazioni imparate sopra per exploit avanzati

ho constatato che: i livelli avanzando per le mie capacità diventano molto difficili, per risolverne alcuni ho impiegato anche più di 7\8 di lavoro.

i comandi principali comuni sono i seguenti

| Categoria | Comandi Utili |
|--------------|----------------------------------|
| File | cat, less, head, tail, strings |
| Permessi | chmod, chown, find / -perm -4000 |
| Rete | netstat -tuln, nc, curl, wget |
| Crittografia | openssl, base64, gpg, sha256sum |
| Debug | strace, ltrace, objdump, gdb |

le mie tips sul troubleshooting sono:

l controllare la grammatica, spesso gli errori di battitura portono ad errori che sono risolvibili con un filo di attenzione

2 mi è risultato difficile a volte ritrovare la linea di comandi corretta da digitare per risolvere alcuni livelli per esempio nella sezione di rete ed escalation permessi alcuni accantonamenti li ho avuti per trovare il codice corretto per tracciare i file.

3 il gioco è molto divertente e a suon di errori e battiture dai che ridai i comandi entrano in testa poi nel cassetto della memoria si ritrovano in qualche maniera.

fortuna che iniziai a giocarci per imparare da quando il prof ce lo consigliò per imparare i comandi shell.