Capture the Flag Manual

Alessio Gjergji
Author 2
Author 3
Author 4
Author 5

Indice

Capitolo 1

Comandi terminale

1.1 Introduzione

Durante una ctf potremmo trovarci di fronte ad alcune challenge in cui è necessario l'utilizzo di vari comandi della shell per recuperare la flag richiesta e quindi passare alla challenge successiva. Di seguito vedremo alcuni comandi della shell per sistemi UNIX o macOS che possono tornare utili.

1.2 Comandi di base

Se si conosce un comando ma non si sa come utilizzarlo è bene consultare il manuale scrivendo sul terminale **man** ⟨*command*⟩. Se non è presente la pagina del manuale provare a specificare il flag –**help**.

1.3 Operazioni sulle directory

1.3.1 cd

Per navigare attraverso il filesystem utilizziamo il comando **cd dir**.

- **cd esempio** (ci spostiamo nella cartella *esempio*)
- **cd Dekstop/esempio** (ci spostiamo nella cartella *esempio* identificata dal suo path)
- **cd ..** (ci permette di spostarci nella cartella superiore)
- **cd** ∼ (ci spostiamo nella home directory)
- **cd /** (ci spostiamo nella root directory)

Per creare una cartella utilizziamo il comando **mk dir**, se invece vogliamo vedere la cartella corrente utlizziamo il comando **pwd**.

1.3.2 ls

Se vogliamo vedere i file all'interno di una cartella utilizziamo il comando **ls**.

- **ls** (mostra i file nella cartella corrente)
- **ls Desktop/esempio** (mostra i file all'interno della cartella *esempio* identificata dal path)

Tra le opzioni del comando **ls** possiamo trovare:

- **-a** (mostra tutti i file, inclusi quelli nascosti)
- **-r** (inverte l'ordine della lista)
- **-t** (ordina in base all'ultimo modificato)
- **-S** (ordina per dimensione del file)

1.4 Operazioni sui file

1.4.1 touch

Per creare un file utilizzare il comando **touch file**.

1.4.2 cat

Il comando **cat** permette di concatenare file e stampare il loro contenuto sullo standard output.

- **cat file** (stampa il contenuto del file, se vengono specificati più file li concatena e stampa il contenuto, e.g. cat file file2)
- **cat < -file** (permette di stampare il contenuto di un file con il nome che inizia con un dash)
- **cat** "$nomefileconspazi$" (permette di stampare il contenuto di un file che contiene spazi nel nome)
- **cat .file** (stampa il contenuto del file nascosto)

1.4.3 cp, mv, rm, file

- **cp file file2** (copia file in file2)
- **mv file file2** (rinomino file in file2)
- **rm file** (elimino file)
  - **rm -r** (rimuovo le directory e i loro contenuti)
  - **rm -d** (rimuovo direcotry vuote)
- **file file1** (ritorna il tipo di file1)

1.4.4 head, tail

- **head file1** (ritorna le prime 10 linee di file1)
- **tail file1** (ritorna le ultime 10 linee di file1)

1.4.5 strings

Il comando **strings** stampa una sequenza di stringhe leggibili all'interno di un file.

- **strings file**
  - con il flag **-n number-of-lines** (specifichiamo la lunghezza minima delle stringhe)
  - con il flag **-e encoding** (specifichiamo la codifica)
  - con il flag **-w** (includiamo gli spazi bianchi)
  - con il flag **-s** (il separatore per l'output)

1.5 Ricerca

1.5.1 sort, unique

Il comando **sort file** permette di ordinare le linee all'interno di un file, il comando **unique -u** permette di mostrare le linee uniche non duplicate, questi due comandi possono essere comodi da usare in combinazione attraverso l'utilizzo di una pipe: **sort nomefile — unique -u**.

1.5.2 grep

Il comando **grep pattern files** permette di cercare un determinato pattern in ogni file, i pattern andrebbero specificati sempre compresi tra doppi apici.

- **grep -i** (ricerca case-insensitive)
- **grep -r** (ricerca ricorsiva)
- **grep -v** (ricerca invertita)
- **grep -o** (mostra solo la parte di file che ha matchato il pattern)

1.5.3 find

Il comando **find** permette di cercare dei file all'interno del filesystem.

- **find /percorso -name** "$filename$" (ricerca per nome)
- **find /percorso -name** "$*.txt$" (ricerca per estensione)
- **find /percorso -type f -size +1M** (ricerca per dimensione)
- **find /percorso -user utente -group gruppo** (ricerca per proprietario e gruppo)
- **find /percorso -mtime -7** (ricerca per data di modifica)

1.6 Connessioni ssh o tcp

Connessione ad una risorsa in ssh:

- **ssh -p numero-porta utente@indirizzo-del-server**

Connessione tramite tcp:

- **nc host port**

1.7 Gestione dei processi

- **ps** (mostra uno snapshot dei processi)
- **top** (mostra i processi real-time)
-
- **kill pid** (termina un processo con il pid=pid)
- **pkill name** (termina un processo col nome=name)
- **killall name** (termina tutti i processi con il nome che inizia per name)