



permessi kali



TRACCIA

Abbiamo visto come si gestiscono i permessi in Linux.

Obiettivo: Configurare e gestire i permessi di lettura, scrittura ed esecuzione per file o directory in un sistema Linux. La scelta dei file o delle directory da configurare spetta allo studente. Infine, lo studente dovrà creare degli screenshot che mostrino i passaggi effettuati e scrivere una relazione spiegando le scelte fatte riguardo ai permessi.



ESECUZIONE

The terminal window shows the following session:

```
kali㉿kali: ~
$ touch progetto.txt
$ mkdir documenti_privati
$ ls -l
total 17240
-rw-r--r-- 1 root root 244 Apr 30 09:10 192.168.50.101
-rw-rw-r-- 1 kali kali 2382030 May 21 04:44 29.gz
-rw-rw-r-- 1 kali kali 0 May 21 04:55 29_uncompressed
-rw-rw-r-- 1 kali kali 132340 May 21 04:44 29.zlib
-rw-r--r-- 1 root root 974 May 20 15:20 analyze.dumps.py
-rw-rw-r-- 1 kali kali 132381 Feb 13 2021 arsene_lupin.png
drwxrwxr-x 2 kali kali 4096 May 21 04:54 _arsene_lupin.png-0.extracted
drwxrwxr-x 2 kali kali 4096 May 21 04:55 _arsene_lupin.png.extracted
-rw-rw-r-- 1 kali kali 2986944 May 21 10:46 butterflyflyondesktop.exe
-rw-rw-r-- 1 kali kali 2963532 May 27 10:28 butterflyflyondesktop.exe.zip
-rw-rw-r-- 1 kali kali 2963532 May 27 10:29 butterflyflyondesktop.exe.zip.1
-rw-rw-r-- 1 kali kali 0 May 20 12:43 clean_dump.b64
-rw-rw-r-- 1 kali kali 0 May 7 08:30 code.deb
drwxrwxr-x 7 kali kali 4096 May 27 11:25 cuckoo
drwxrwxr-x 5 kali kali 4096 May 27 11:28 cuckoo_env
-rw-rw-r-- 1 kali kali 223 May 9 07:58 custom_pass.txt
-rw-rw-r-- 1 kali kali 120 May 9 07:58 custom_users.txt
-rw-rw-r-- 1 kali kali 0 May 20 12:43 decoded_dump.json
-rw-r----- 1 root root 3434 May 21 08:14 decoded_key.bin
-rw-r----- 1 root root 1 May 21 08:12 decoded_key.bin.save
drwxr-xr-x 5 kali kali 4096 May 30 11:16 Desktop
drwxrwxr-x 2 kali kali 4096 Jun 3 10:06 documenti_privati
-rwxrwxr-x 1 kali kali 113357 May 27 09:34 Documento_Sicuro.exe
drwxr-xr-x 2 kali kali 4096 Apr 24 06:38 Documents
drwxr-xr-x 3 kali kali 4096 May 30 04:04 Downloads
-rw-r--r-- 1 root root 635 May 20 15:46 dumpie.py
-rw-r--r-- 1 kali kali 4096 May 27 11:10 esc
-rw-rw-r-- 1 kali kali 90248 May 9 05:57 filtered_passwords.txt
-rw-rw-r-- 1 kali kali 3743405 May 9 05:57 filtered_users.txt
-rw-rw-r-- 1 kali kali 32 May 14 06:08 flag.txt
-rw-rw-r-- 1 kali kali 582 May 9 08:05 found_creds.txt
-rw-rw-r-- 1 kali kali 38 May 9 07:46 ftp_pass.txt
```

L'obiettivo di questa esercitazione è configurare e gestire i permessi di lettura, scrittura ed esecuzione su file e directory in un sistema Linux. In particolare, ho creato un file (progetto.txt) e una directory (documenti_privati) su cui ho applicato permessi personalizzati. Successivamente, ho testato i permessi con un utente differente (nobody) per verificare l'efficacia della configurazione. Ho usato il comando ls -l per visualizzare i permessi predefiniti assegnati a file e directory appena creati.



PERMESSI

Ho modificato i permessi in questo modo:

Al file `progetto.txt` ho assegnato permessi 600: solo il proprietario può leggere e scrivere.

Alla directory `documenti_privati` ho assegnato permessi 700: solo il proprietario può leggere, scrivere ed entrare nella directory.

```
(kali㉿kali)-[~]
$ chmod 600 progetto.txt
$ chmod 700 documenti_privati

(kali㉿kali)-[~]
$ ls -l
total 17240
-rw-r--r-- 1 root root 244 Apr 30 09:10 192.168.50.101
-rw-rw-r-- 1 kali kali 2382030 May 21 04:44 29.gz
-rw-rw-r-- 1 kali kali 0 May 21 04:55 29.uncompressed
-rw-rw-r-- 1 kali kali 132340 May 21 04:44 29.zlib
-rw-r--r-- 1 root root 974 May 20 15:20 analyze_dumps.py
-rw-rw-r-- 1 kali kali 132381 Feb 13 2021 arsenelupin.png
drwxrwxr-x 2 kali kali 4096 May 21 04:54 arsenelupin.png.extracted
drwxrwxr-x 2 kali kali 4096 May 21 04:55 arsenelupin.png.extracted
-rw-rw-r-- 1 kali kali 2986944 May 21 10:46 butterflyondesktop.exe
-rw-rw-r-- 1 kali kali 2963532 May 27 10:28 butterflyondesktop.exe.zip
-rw-rw-r-- 1 kali kali 2963532 May 27 10:29 butterflyondesktop.exe.zip.1
-rw-rw-r-- 1 kali kali 0 May 20 12:43 clean_dump.b64
-rw-rw-r-- 1 kali kali 0 May 7 08:30 code.deb
drwxrwxr-x 7 kali kali 4096 May 27 11:25 cuckoo
drwxrwxr-x 5 kali kali 4096 May 27 11:28 cuckoo_env
-rw-rw-r-- 1 kali kali 223 May 9 07:58 custom_pass.txt
-rw-rw-r-- 1 kali kali 120 May 9 07:58 custom_users.txt
-rw-rw-r-- 1 kali kali 0 May 20 12:43 decoded_dump.json
-rw----- 1 root root 3434 May 21 08:14 decoded_key.bin
-rw----- 1 root root 1 May 21 08:12 decoded_key.bin.save
drwxr-xr-x 5 kali kali 4096 May 30 11:16 Desktop
drwx----- 2 kali kali 4096 Jun 3 10:06 documenti_privati
-rwxrwxr-x 1 kali kali 113357 May 27 09:34 Documento_Sicuro.exe
drwxr-xr-x 2 kali kali 4096 Apr 24 06:38 Documents
drwxr-xr-x 3 kali kali 4096 May 30 04:04 Downloads
-rw-r--r-- 1 root root 635 May 20 15:46 dumpie.py
-rw-r--r-- 1 kali kali 4096 May 27 11:10 esc
-rw-rw-r-- 1 kali kali 90248 May 9 05:57 filtered_passwords.txt
-rw-rw-r-- 1 kali kali 3743405 May 9 05:57 filtered_users.txt
-rw-rw-r-- 1 kali kali 32 May 14 06:08 flag.txt
-rw-rw-r-- 1 kali kali 582 May 9 08:05 found_creds.txt
-rw-rw-r-- 1 kali kali 38 May 9 07:46 ftp_pass.txt
-rw-rw-r-- 1 kali kali 24 May 9 07:46 ftp_users.txt
-rw-rw-r-- 1 kali kali 3294 May 8 06:13 hashes
-rw-rw-r-- 1 kali kali 40 May 21 08:38 hash_johntheripper
-rw-r--r-- 1 root root 165 May 8 10:31 hash.txt
-rw-rw-r-- 1 kali kali 1696 Apr 21 06:03 kali-archive-key.asc
-rw-rw-r-- 1 root root 816 May 27 10:00 loader.c
-rw-rw-r-- 1 kali kali 73802 May 26 10:05 malware_nascosto.exe
-rw-rw-r-- 1 kali kali 73802 May 26 09:58 malware_offuscato.exe
drwxr-xr-x 2 kali kali 4096 Apr 24 06:38 Music
-rw-rw-r-- 1 kali kali 98 May 21 06:57 pass.txt
-rw-rw-r-- 1 kali kali 7 May 9 07:33 passwords.txt
-rw-rw-r-- 1 kali kali 43 May 8 04:56 password.txt
-rw-rw-r-- 1 kali kali 73802 May 15 09:51 payload.exe
-rw-rw-r-- 1 kali kali 354 May 26 10:07 payload.raw
drwxrwxr-x 5 kali kali 4096 May 30 11:27 pcapkit-env
drwxr-xr-x 2 kali kali 4096 Jun 3 10:07 Pictures
-rw-rw-r-- 1 kali kali 5724 May 27 08:09 polimorfico_definitivo.exe
-rw-rw-r-- 1 kali kali 7577 May 26 06:27 polimorficommm.exe
-rw----- 1 kali kali 0 Jun 3 10:05 progetto.txt
drwxr-xr-x 2 kali kali 4096 Apr 24 06:38 Public
```

TEST

Per testare l'efficacia dei permessi, ho usato il comando sudo -u nobody per eseguire operazioni come un utente non proprietario:

- Ho tentato di leggere progetto.txt con cat
- Ho tentato di scrivere nel file con echo >>
- Entrambe le operazioni sono fallite con "Permission denied", come previsto

progetto.txt: Ho scelto 600 perché voglio che sia un file privato accessibile solo da me. È utile per file sensibili o personali che non devono essere letti o modificati da altri utenti.

documenti_privati: Ho scelto 700 per assicurarmi che solo io possa accedere ai contenuti. Questo è utile per directory contenenti documenti riservati, impedendo l'accesso ad altri utenti anche solo per elencarne il contenuto.

The screenshot shows a Kali Linux desktop environment. In the top panel, there are icons for a terminal, file manager, browser, and other utilities. Below the panel, a file manager window lists files in a directory, including shellcode.c, shellcode_encoded.c, shellcode_xor.c, shell.php, shell.php.save, ssh_key, steghide_bruteforce.py, Templates, testo_meme.txt, theta-key.jpg, tortoise-tts, udp_flood.py, udp_flood.py.save, users.txt, venv-base58, Videos, wget-log, wget-log.1, xor_encoded.bin, xor_encoder.py, xss_server.py, and zeek. In the bottom left, a terminal window shows the user attempting to read and write to 'progetto.txt' using 'sudo -u nobody'. Both operations result in 'Permission denied' errors.

```
(kali㉿kali)-[~]
$ sudo -u nobody cat progetto.txt
sudo -u nobody echo "test" >> progetto.txt
[sudo] password for kali: 
cat: progetto.txt: Permission denied

(kali㉿kali)-[~]
$ sudo -u nobody cat progetto.txt
sudo -u nobody echo "test" >> progetto.txt
cat: progetto.txt: Permission denied

(kali㉿kali)-[~]
```