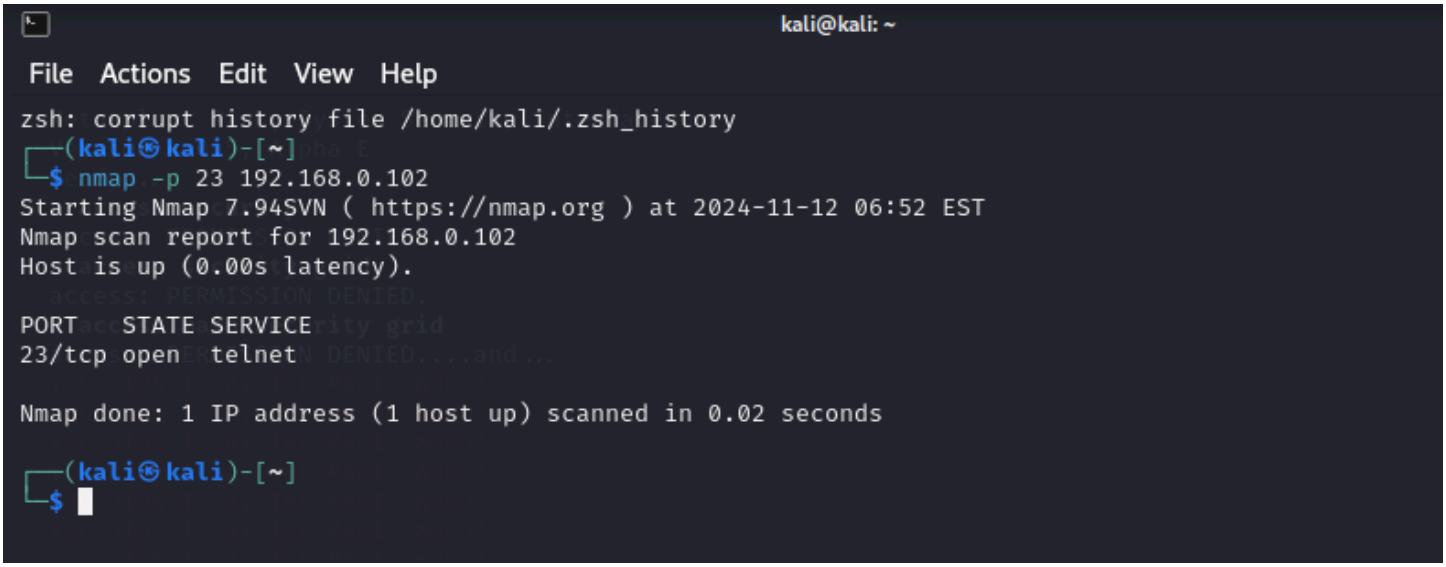
S7L2 Metasploit–Telnet

Introduzione:

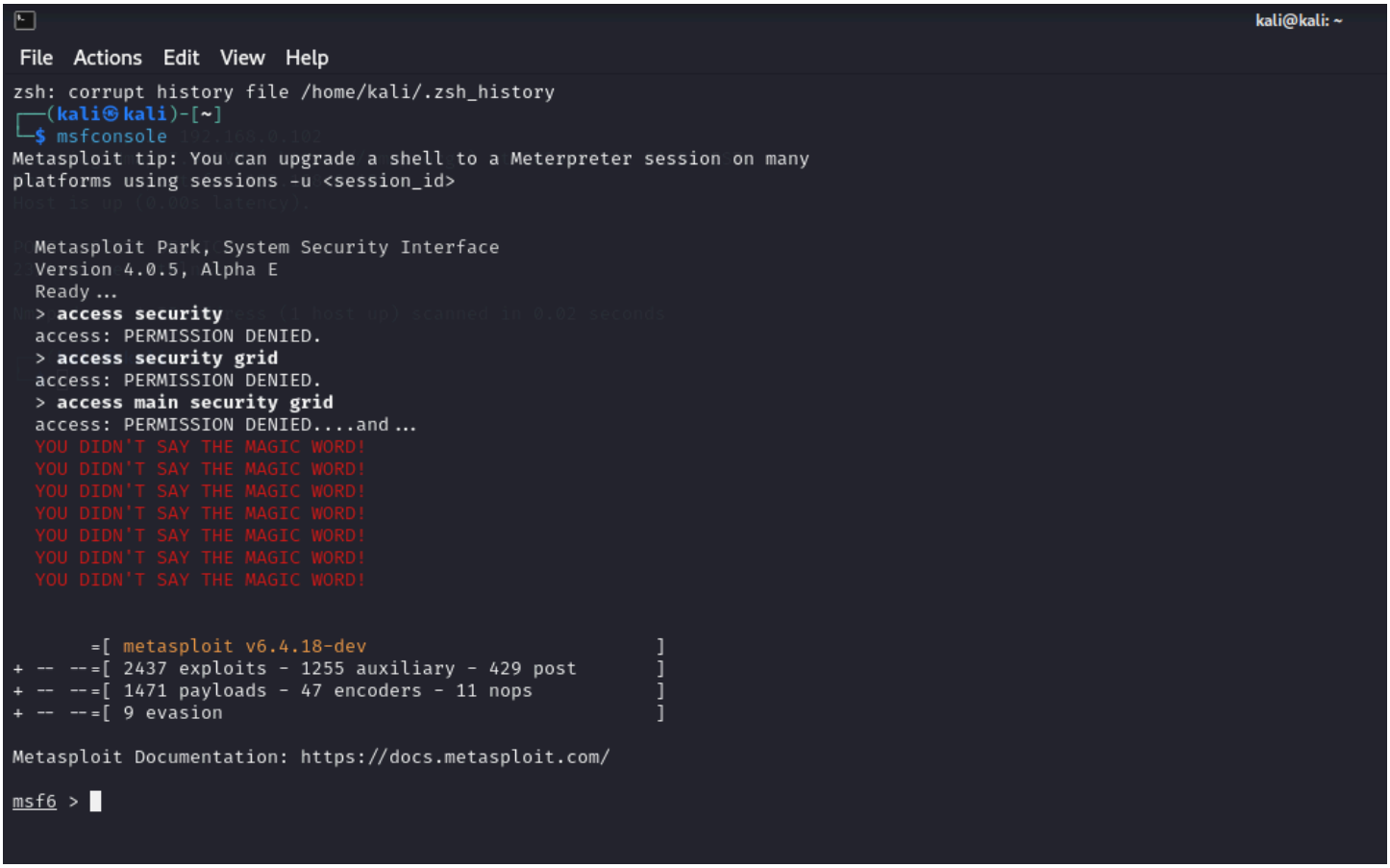
L'obiettivo del compito è quello di **exploitare** metasploitable attraverso alcune **vulnerabilità del protocollo telnet**. Attraverso sempre **Metasploit** installato sulla macchina Kali Linux.

Preparazione:

Vediamo subito se la porta del **servizio telnet 23** è aperta:



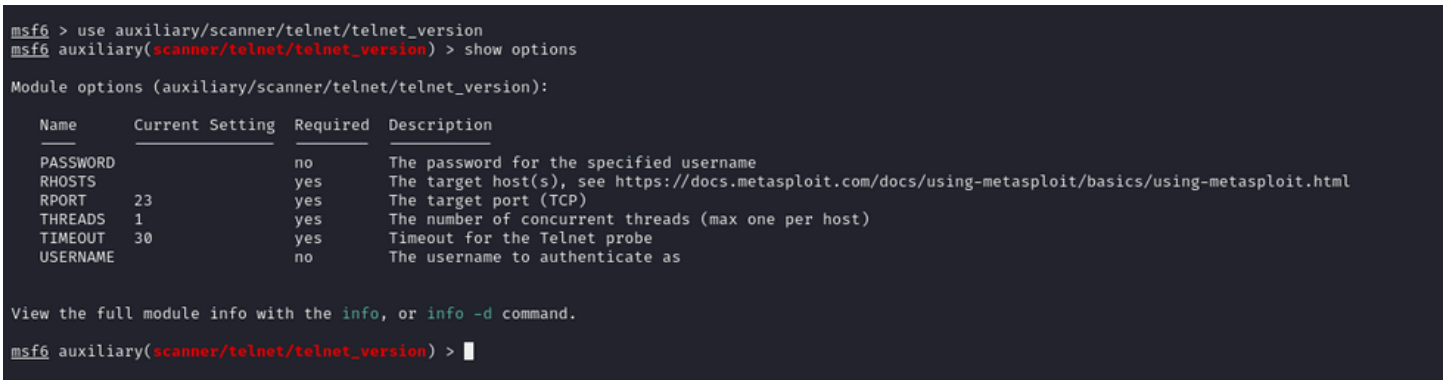
Dopo aver avuto conferma, avviamo Metasploit digitando **msfconsole** sul prompt di Kali:



Ed andiamo ad utilizzare un **exploit ausiliare**:

use auxiliary/scanner/telnet/telnet_version

E tramite *show options* vediamo che manca il RHOSTS, ovvero l'IP della macchina vittima.



Tramite il comando ***set*** vado ad impostare l'IP di metasploitable:

```
msf6 auxiliary(scanner/telnet/telnet_version) >
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.0.102
rhosts => 192.168.0.102
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS    192.168.0.102    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/telnet/telnet_version) >
```

Pratica:

Dopo aver digitando ***exploit*** e premuto invio, vengono raccolte informazioni sul servizio Telnet, come la versione e il banner. I **modelli ausiliari** come questo aiutano a identificare e raccogliere informazioni su potenziali vulnerabilità senza eseguire attacchi diretti.

Notiamo che questo exploit ci ha permesso di vedere informazioni che viaggiano in chiaro, come **username** e **password**, per accedere a metasploitable (evidenziate in giallo)

```
[+] 192.168.0.102:23      - 192.168.0.102:23 TELNET _                  _     _ _    _    _    ____  \x0a _ _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|
 __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____
                          \x0a\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get starte
[*] 192.168.0.102:23      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Ed ora avendo avuto accesso a quelle informazioni, posso accedere tranquillamente alla macchina, grazie alle credenziali viste:

Conclusione:

Esporre Telnet, soprattutto con credenziali di default, è un rischio grave in un contesto reale. Gli amministratori dovrebbero:

- **Disabilitare** Telnet se non necessario.
- **Usare SSH** al posto di Telnet per una connessione sicura.
- Cambiare le credenziali di default e adottare **password forti**.