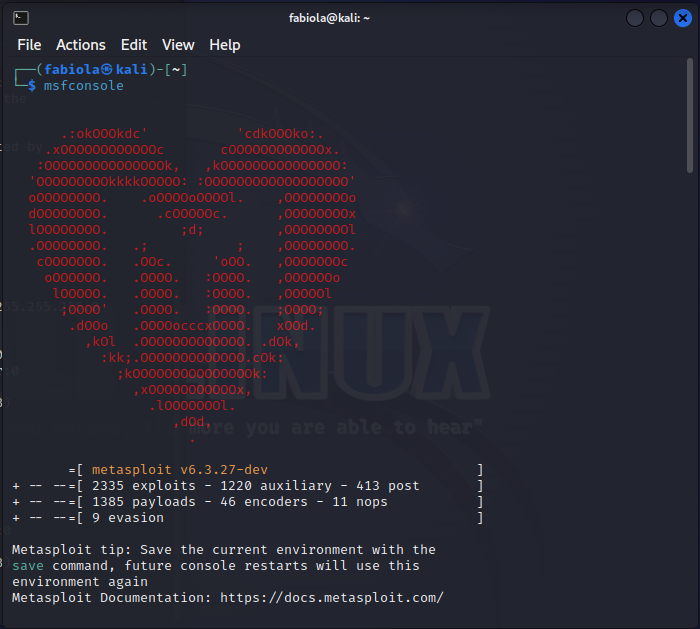
Traccia:

Utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo **auxiliary telnet\_version** sulla macchina Metasploitable.

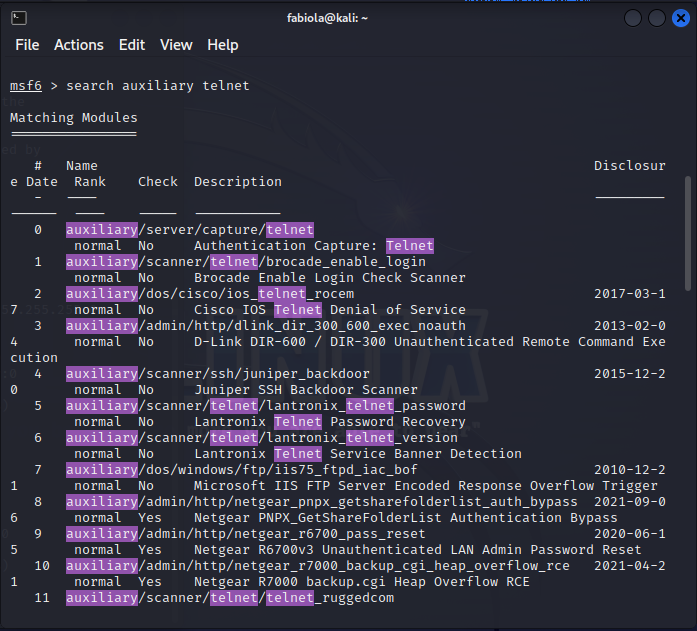
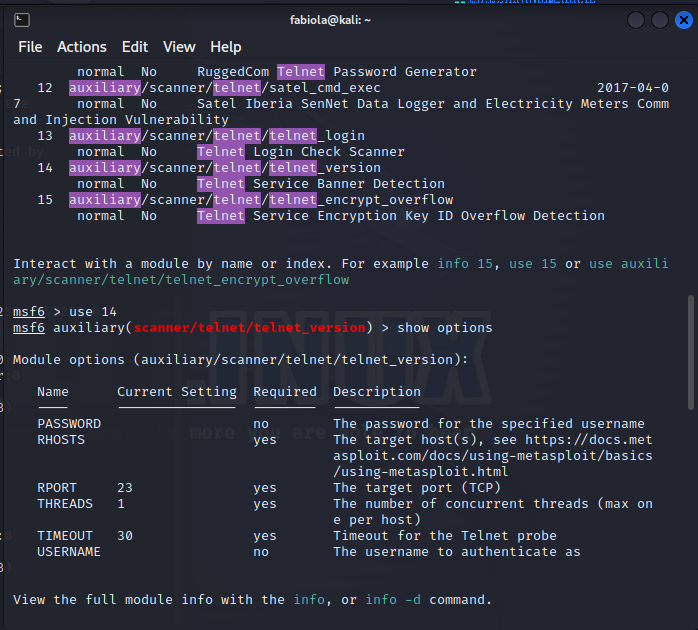
La macchina Metasploitable presenta un servizio Telnet in ascolto sulla porta 23, che trasferisce il traffico su canale non cifrato. Ciò significa che un potenziale attaccante potrebbe sniffare la comunicazione e rubare informazioni sensibili come username, password ed i comandi scambiati tra client e server.

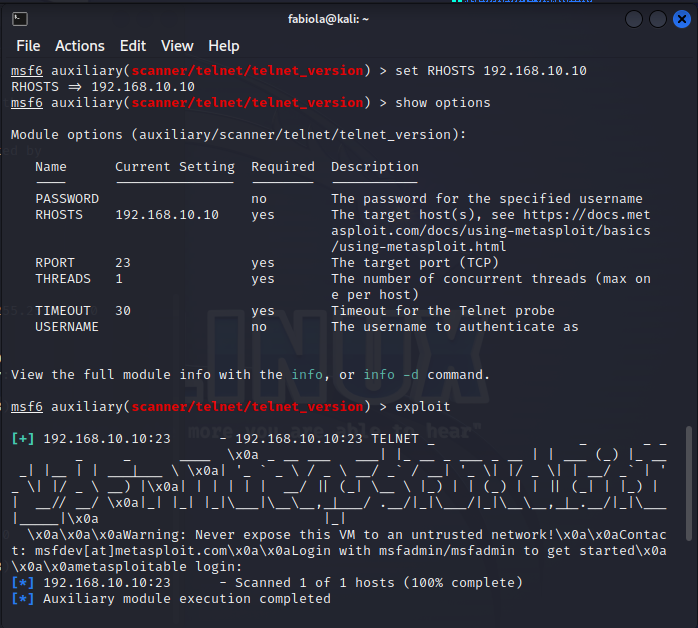
Vediamo come utilizzare Metasploit per sfruttare questa vulnerabilità. Come al solito, il primo step è eseguire il comando MSFConsole per avviare Metasploit:



Per sfruttare questa particolare vulnerabilità del servizio Telnet, utilizziamo un modulo ausiliario, che, contrariamente ai moduli normali, non eseguono necessariamente attacchi diretti ma forniscono informazioni e supporto aggiuntivi che possono essere utili per ottenere un quadro completo della sicurezza della rete o del sistema.

Quindi i comandi saranno **search auxiliary telnet, use 14, show options** (per controllare le opzioni necessarie per lanciare l’attacco, in questo caso l’unico da configurare è RHOSTS, ovvero l’indirizzo target dove è in esecuzione il servizio telnet), quindi **set RHOSTS+IP target** e infine **exploit** per lanciare l’attacco:

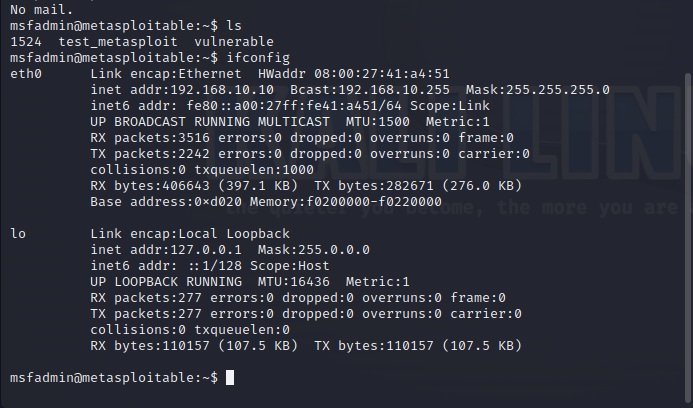
**** 



Il modulo ha recuperato i dati di login del servizio(msfadmin/msfadmin). Per verificare la correttezza delle informazioni, facciamo un test. Eseguiamo da terminale il comando «telnet» seguito dall’ip della macchina Metasploitable. Il servizio ci richiede delle credenziali.

Proviamo con le informazioni che ci ha restituito Metasploit, quindi username «msfadmin», password «msfadmin»:





L’attacco ha avuto effettivamente successo e la vulnerabilità del servizio Telnet è stata sfruttata correttamente, in quanto abbiamo ottenuto accesso non autorizzato alla macchina.