

Fare una ricerca dello scanning di telnet e fare una configurazione su msfconsole

Configurare rhosts con l'ip della macchina vittima (Meta): 192.168.50.101

Eseguire l'exploit di telnet e collegarci tramite telnet a metasploitable tramite il comando telnet 192.168.50.101

Exploit

Un exploit informatico è un insieme di istruzioni, software o sequenze di comandi che sfruttano un errore o una vulnerabilità presente in un software, hardware o in qualsiasi dispositivo elettronico. Tale manipolazione può indurre un comportamento inatteso o non desiderato. Gli exploit sono spesso impiegati a fini malevoli. La modalità di funzionamento di un exploit informatico inizia con l'individuazione di una vulnerabilità o di un difetto nel software o nell'hardware di destinazione. Una volta identificata questa debolezza, un attaccante può sviluppare un exploit con l'obiettivo specifico di sfruttarla. Molti attaccanti utilizzano gli exploit come strumento per la diffusione di malware, potenzialmente causando danni significativi al sistema bersaglio. La realizzazione e l'utilizzo di exploit sono componenti fondamentali nelle attività degli hacker, poiché consentono loro di approfittare delle debolezze nel codice o nella configurazione dei sistemi al fine di ottenere accesso non autorizzato o eseguire azioni dannose. La prevenzione e la gestione delle vulnerabilità sono cruciali per garantire la sicurezza informatica e limitare l'impatto degli exploit.

Protocollo Telnet

Il protocollo Telnet rappresenta un modello client-server che si fonda sulla comunicazione attraverso connessioni TCP, agevolando il trasferimento di informazioni. Telnet abilita il controllo remoto dei sistemi informatici mediante input e output basati su testo. La connessione client-server è instaurata di default mediante il protocollo di trasmissione TCP, utilizzando la porta TCP 23.