**Hacking con Metasploit**

**Track:**

completare una sessione di hacking sulla macchina Metasploitable, sul servizio «vsftpd», configurandola con il seguente IP: 192.168.1.149/24. Una volta ottenuta la sessione sulla Metasploitable, creare una cartella con il comando mkdir nella directory di root (/) chiamandola test\_metasploit.

**Step:**

1. Avviare Metasploit da Kali (la nostra macchina attaccante) tramite il comando **msfconsole**. Nel mentre, in un altro terminale possiamo fare un rapido scan delle porte con relativi servizi e versioni associate della macchina Metasploitable con il seguente comando di nmap:

**nmap -sV (IP Meta).**

La versione del servizio che a noi interessa è appunto vsftpd in ascolto sulla porta 21/tcp.

Con il comando **search**, troviamo l’exploit associato alla versione.

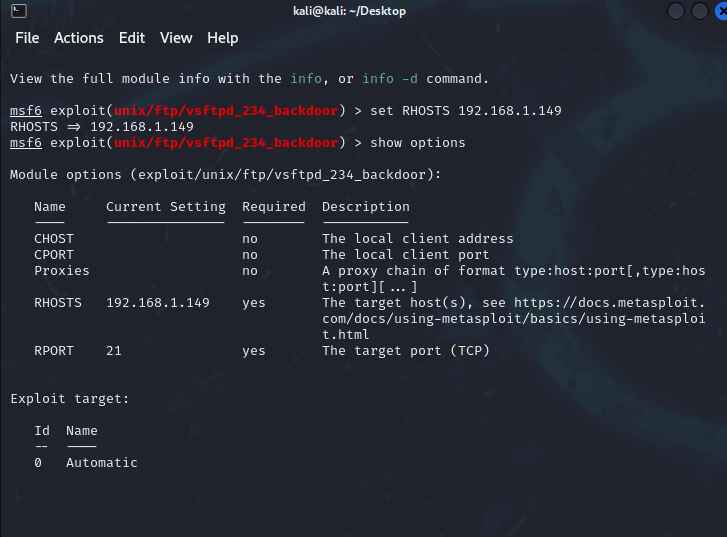
Immagine che contiene testo, schermata, software, Software multimediale

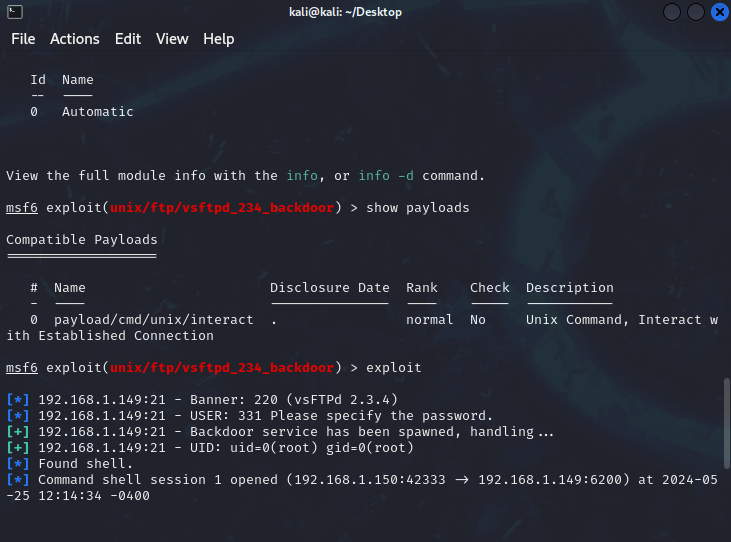
Descrizione generata automaticamente

1. Usiamo l’unico exploit disponibile tramite il comando **use**, anteponendolo al path dell’exploit stesso (come possiamo notare si tratta di una backdoor) e **show options** per vedere quali parametri debbano essere settati correttamente. RHOSTS, ovvero l’IP della macchina target, è l’unico che richieda ciò.

Immagine che contiene testo, schermata, software

Descrizione generata automaticamente

1. Usiamo dunque **set** per configurare l’IP della nostra macchina target e procedere alla scelta del payload. 
2. Scegliamo il nostro payload con il comando **show payloads**. Notiamo come ci sia solo un payload disponibile per questo exploit, dunque, non sarà necessario sceglierlo tramite il comando use, in quanto verrà preso di default. Siamo pronti quindi a lanciare il nostro **exploit**



1. Stabilita la connessione, saremo all’interno della macchina target ed in grado di creare la nostra cartella **test\_metasploit** con **mkdir**

