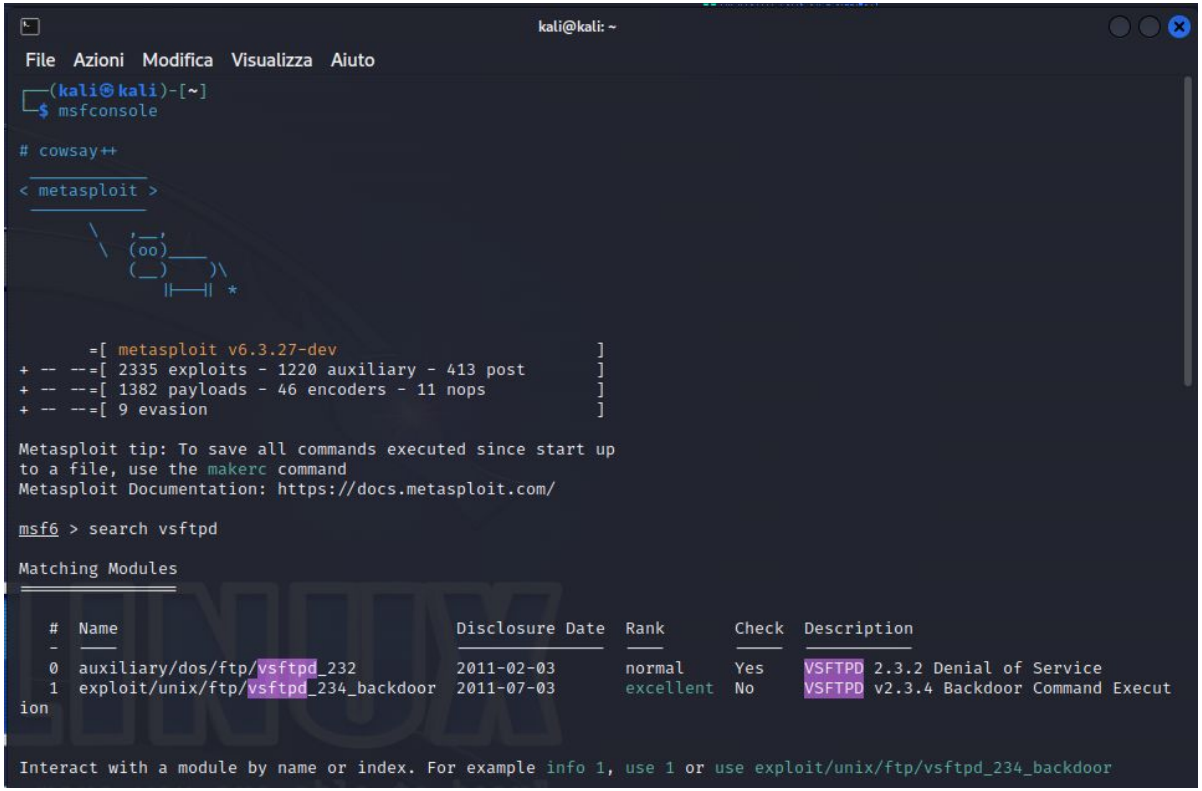
CONSEGNA S7L1

Metasploit e attacco a vsftpd

Come prima cosa andremo ad individuare la porta adatta al nostro caso scansionando la macchina di Metasploitable con Nmap e ci accorgeremo che la porta responsabile del File Tranfer Protocol (FTP) e che quindi andremo effettivamente ad utilizzare è la 21.

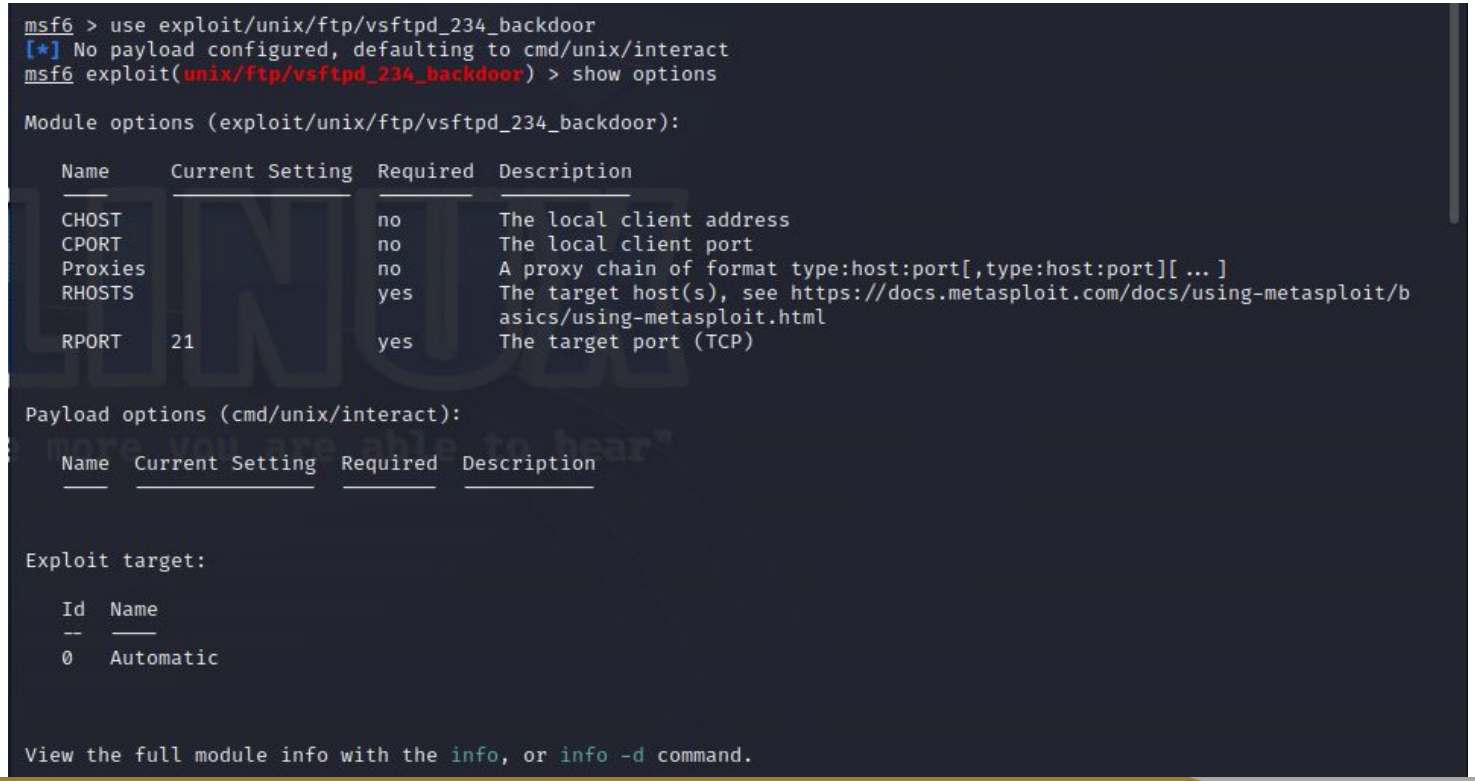
A questo punto avviamo metasploit con il comando *msfconsole* come in figura sotto.

Utilizzando il comando *search vsftpd* andremo a controllare se esiste un exploit per il servizio *vsftpd* e coma possiamo notare in figura esistono due exploit per questo servizio verso sistemi Linux ed è una backdoor.



Adesso possiamo far partire l'exploit caricando la backdoor usando il comando *use* seguito dal *path* dell'exploit stesso.

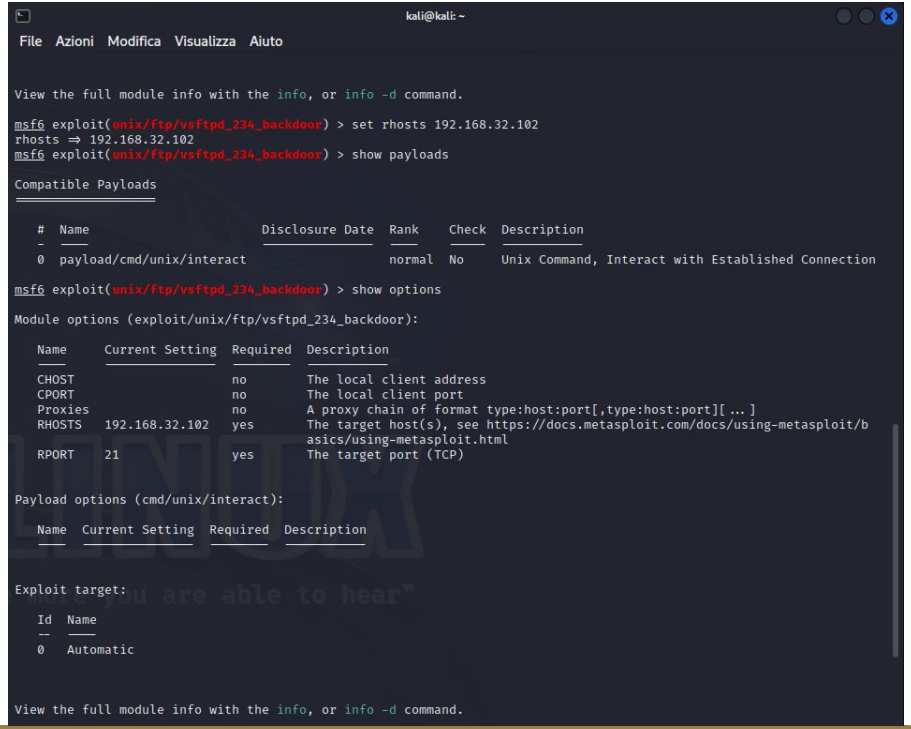
Usando successivamente il comando *show options* potremo capire quali parametri dovremo configurare per poter attaccare la macchina vittima, in questo caso *RPORT* è già impostata sulla 21 quindi andremo a configurare solo il parametro *RPORT* indicando l'ip di Metasploitable.



Per impostare correttamente l'ip della macchina vittima a questo punto useremo il comando *set rhosts* seguito dall'ip.

Successivamente andremo a capire ed a scegliere il payload che intendiamo utilizzare e per fare ciò useremo il comando *show payloads,* nella fattispecie vedremo che potremo utilizzare un unico payload, essendo l'unico presente non andrà configurato nulla poichè verrà utilizzato di default.

Riutilizzando il comando *show options* possiamo capire se ci sono parametri da impostare per lanciare il payload ed in questo caso non ci saranno quindi possiamo partire con l'attacco.



Lanciamo l'attacco con il comando *exploit* così facendo apriremo una sessione sulla macchina vittima avendo una shell da remoto, infatti come possiamo vedere in figura lanciando il comando *ifconfig* noteremo che l'ip è quello della macchina vittima, ora con il comando *mkdir* creeremo una cartella che chiameremo *test_metasploit* nella quale potremo navigare così da spostarci anche nell'intero sistema.