**Metasploit**

Nell’esercitazione odierna abbiamo visto come tramite il tool **Metasploit**, sia possibile sfruttare le vulnerabilità di determinati software attivi, tramite l’utilizzo di determinati exploit. Questo tipo di attacco, ha però successo solo se si utilizza un exploit *volto a mirare una specifica versione del software*, questo poiché se non si utilizza l’exploit della corretta versione l’attacco potrebbe risultare inefficace, per cui bisogna essere molto precisi quando riguardo ciò.

***Svolgimento dell’esercizio***

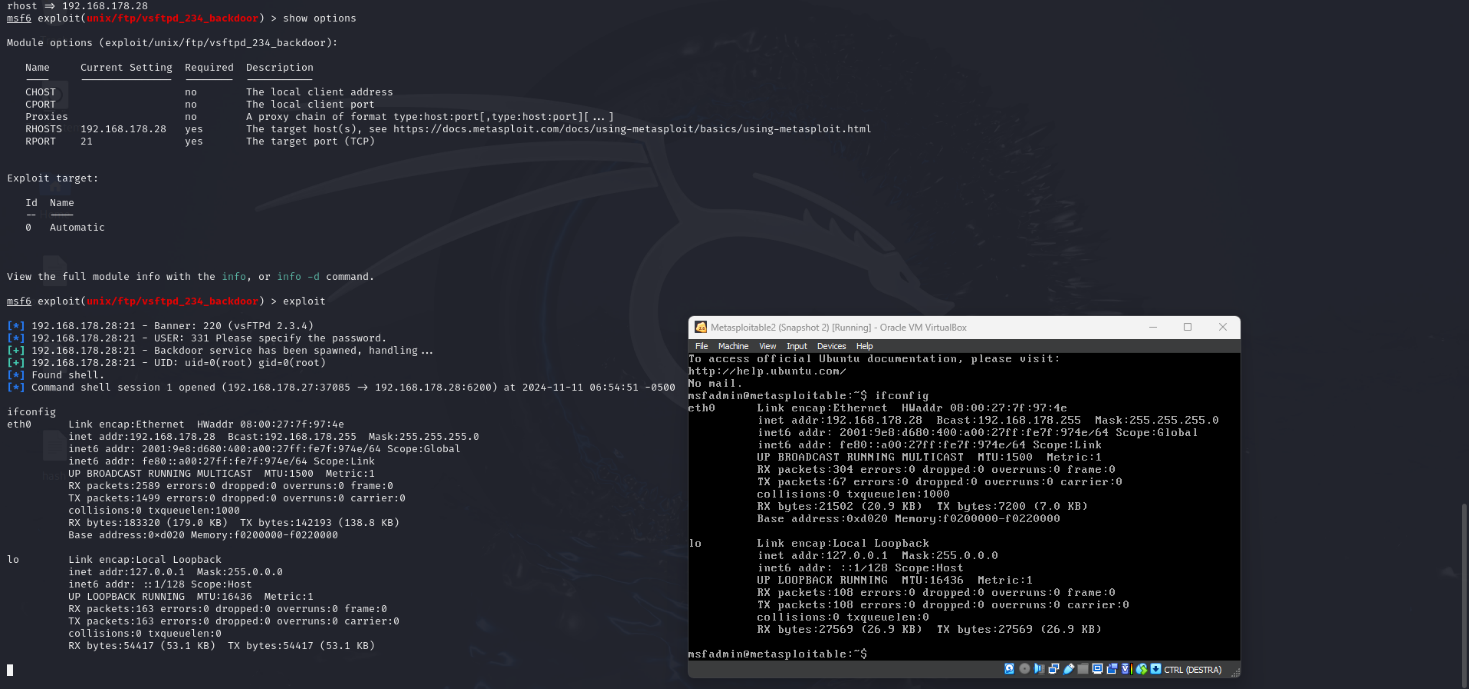
***1 parte***

Come bersaglio è stata utilizzata la macchina vulnerabile metasploitable 2, la quale una volta avviata è stata soggetto di una scansione tramite il tool **Nmap**, con il comando:

Nmap -sV <IP da scansionare>

In seguito a questa scansione sonno stati riportati tutti i protocolli attivi, cin relative porte e versioni.

Successivamente, tramite il comando **msfconsole** è stato avviato il tool **Metasploit**.



Sono stati impartiti due comando nello specifico, all’avvio del tool, il primo ***show exploit***, il quale ha mostrato tutti i 2000+ exploit disponibili, mentre il secondo comando, era diretto al protocollo ftp, per cui è stato scritto sulla riga di comando **search** **vsftpd**, in modo da filtrare tutti gli exploit relativi a quel determinato protocollo. Dopo aver scelto l’exploit è stata effettuata la scelta di un **payload**.

Di norma per trovare il payload più “corretto” è necessario effettuare una verifica per ognuno di essi, ma per l’esercizio odierno, ci siamo affidati al “suggerimento” del tool stesso, che ha fornito il payload corretto in base a questa specifica situazione.

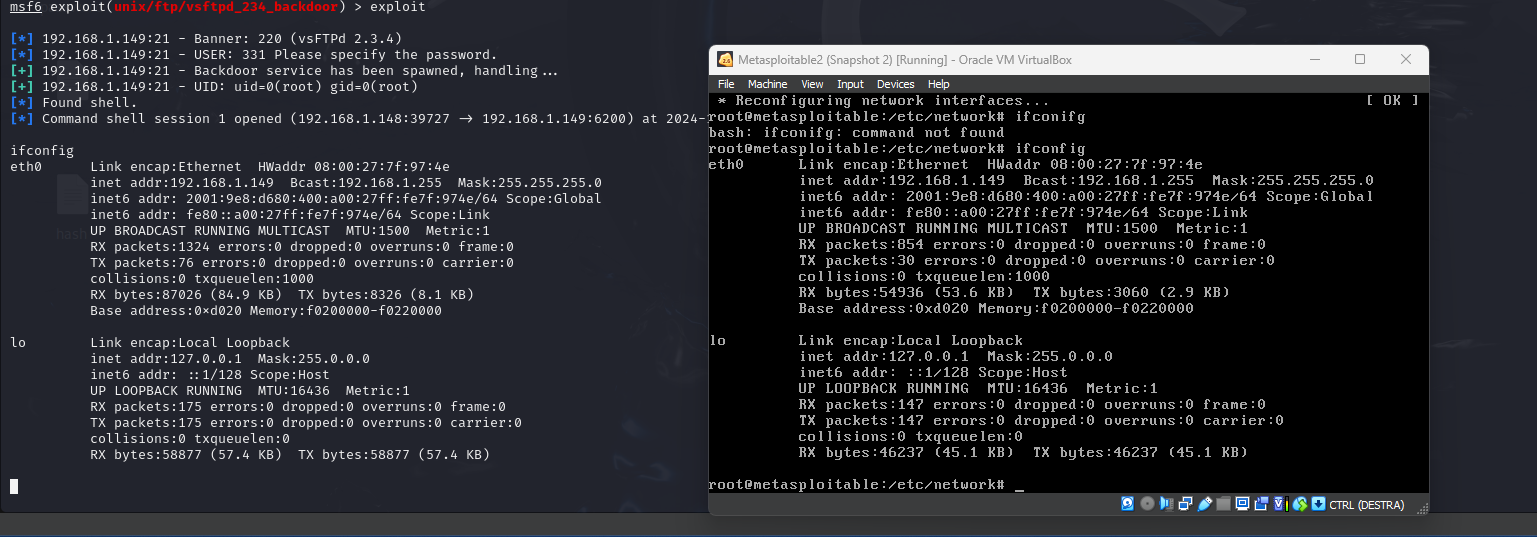
È stato poi modificato il parametro relativo al **rhosts**, specificando quello che era il nostro bersaglio, ed è stato successivamente fatto partire l’exploit.

Il risultato è stato quello riportato, ovvero, tramite l’attacco avvenuto con successo è stata creata una **shell** all’interno della macchina vulnerabile, consentendoci quindi di poter effettuare qualunque tipologia di comando, tra cui **l’ifconfig**, volto a dimostrare che l’attacco è avvenuto con successo.

***2 Parte dell’esercizio***

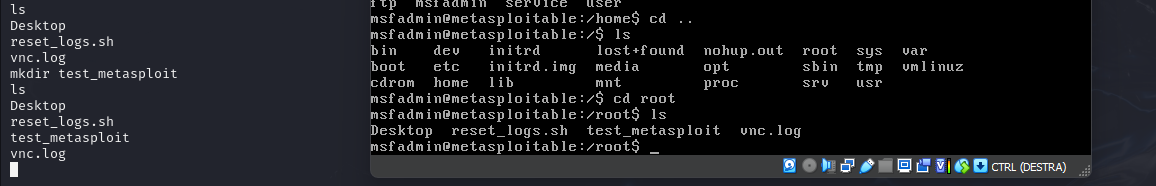
Dopo aver preso dimestichezza con il tool, è stato ripetuto nuovamente l’attacco, cambiando però come richiesto dalla traccia **gli indirizzi IP** delle due macchine.

Dopo aver settato manualmente i due indirizzi IP statici con relativi IP di **network**, **broadcast** e **gateway**, ed aver verificato che le macchine comunicassero, è stato quindi ripetuto l’attacco con la medesima procedura.



Il risultato è stato il medesimo, riuscendo nuovamente a creare una shell che ci consentisse di effettuare qualunque operazione sulla macchina bersaglio.

In seguito è stata creata una cartella all’interno del percorso **/root** dal nome **test\_metasploit**, tramite l’ausilio del comando **mkdir test\_metasploit** direttamente nella cartella /root.



Ciò è mirato a dimostrare non solo che l’attacco ha avuto successo, ma anche che l’attaccante potesse effettuare azioni sulla macchina vulnerabile.