Esercizio fine modulo 4 svolto con 2 target:

- 1)Metasploitable
- 2)Windows XP

Esercizio svolto su macchina Meta

Avvio del comando "MSFCONSOLE" dal terminale della macchina Kali e successiva ricerca attraverso il comando SEARCH della vulnerabilità che si vuole utilizzare.



In questo caso andremo ad utilizzare la vulnerabilità numero 1 con il tag della parola cercata " JAVA_RMI ".Una volta caricato il payload che si vuole utilizzare eseguiremo il comando " show options " o " show missing " per andare a settare i parametri richiesti per il lancio dell' exploit, quindi andremo a settare il RHOST " indirizzo IP macchina taget " e LHOST " indirizzo IP della macchina Kali dal quale parte l'attacco".



Una volta eseguito il comando "RUN", dopo aver settato i requisiti richiesti, potremo finalmente utilizzare il nostro terminale per ottenere informazioni di vario tipo relative alla macchina target. In questo caso mi sono preso la briga di vedere le informazioni relative alla configurazione della scheda di rete, informazioni relative al sistema operativo e un check sulle cartelle presenti sulla macchina.







Esercizio svolto su macchina XP

Questa volta abbiamo deciso di provare un attacco su una macchina Windows,utilizzando gli stessi procedimenti per prenderne il controllo,con la differenza che questa volta la nostra MSFconsole successivamente si tramuterà in un altro tool "METERPRETER ",questo ci permette di utilizzare dei comandi particolari che rendono meterpreter ancora più efficiente e potente nella fase degli esploit.



Al solito andiamo a settare gli indirizzi della macchina target e della macchina attaccante con la visualizzazione dei requisiti richiesti.



Una volta acquisito Meterpreter possiamo iniziare a mandare comandi per ottenere tutte le informazioni che vogliamo riguardo al sistema target.

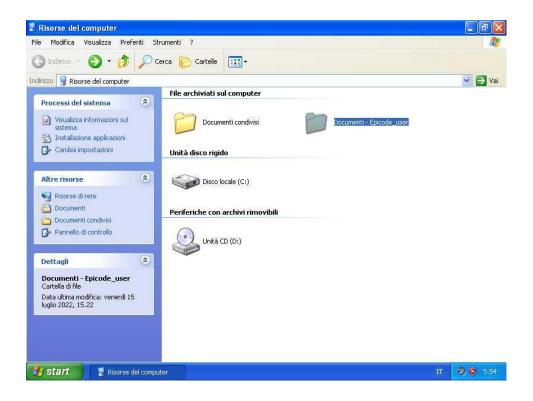






Con l'utilizzo del comando "screenshot" possiamo anche fare uno screen dell shcermata del computer target.





Hushdump: grazie a questo comando possiamo riuscire a ottenere i profili e le password in formato hash che poi dovremo andare a elaborare con John the ripper per avere le password in chiaro dei profili presenti sull macchina.







