

ES Lezione 1 Settimana 6

Durante l'esercizio di oggi andremo a effettuare una sessione di hacking, tramite metasploit verso la nostra macchina virtuale metasploitable. Attueremo un exploit dotandoti dei mezzi che disponiamo. Un exploit è un programma che, a differenza di un malware, sfrutta una vulnerabilità già presente all'interno del software o hardware, esso sfrutta questa vulnerabilità per infiltrarsi all'interno. Creando un varco da modo a l'host esterno di interagire direttamente con la macchina attaccata.

- Dopo aver avviato sia kali che metasploit, ho verificato che le macchine comunicassero. Subito dopo, tramite prompt di kali, ho effettuato una mappatura delle porte aperte e quindi potenzialmente attaccabili di metasploitable (comando `nmap -sV IPV4`).
- Trovata la porta vulnerabile (`n21 ftp`), ho avviato sempre tramite prompt, metasploitable. Ho ricercato una possibile vulnerabilità (comando `search svftpd`), ho scelto la vulnerabilità e ho settato solo i parametri necessari. In fine con il comando “exploit” ho fatto partire l'attacco.
- L'attacco è andato a buon fine, ho verificato di aver creato una connessione riscontando l'ipv4, che ora deve essere uguale a quello di metasploitable. In fine ho creato un cartella.