EPICODE

Esercizio S7 – L1

TRACCIA

Partendo dall’esercizio visto nella lezione di oggi, vi chiediamo di completare una sessione di hacking sulla macchina Metasploitable, sul servizio «vsftpd» (lo stesso visto in lezione teorica).  
Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando mkdir nella directory di root (/). Chiamate la cartella test\_metasploit.

SOLUZIONE

Exploit:  
Un exploit è un attacco ad una vulnerabilità di un software, di un hardware, o in generale in qualsiasi dispositivo elettronico. Un exploit può permettere all’attaccante di prendere il controllo del sistema vittima, accedere ai permessi da amministratore, inserire malware di vario tipo e addirittura spostarsi in altri dispositivi della stessa rete.

Metasploit:  
Metasploit è uno strumento che permette di effettuare exploit già noti e di abbinarci dei payload (insieme di istruzioni) già pronti. Contiene quasi 3.000 exploit e centinaia di payload. Con la versione a pagamento è anche possibile automatizzare il processo di test degli exploit e dei payload.

Per iniziare si scansionano, con Nmap, le porte per vedere i servizi attivi e le versioni.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

A questo punto, utilizzando Metasploit, si cercano gli exploit per il servizio ftp e per la specifica versione.

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

Si seleziona quindi l’exploit disponibile (use 0) e, in questo caso, viene messo il payload corretto di default.  
Con il comando “show options” si possono verificare i requisiti mancanti per effettuare l’exploit” (RHOSTS).

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

Si setta così l’ip dell’host vittima e si verifica il corretto settaggio con “show options”.

Immagine che contiene testo, schermata, Carattere, software

Descrizione generata automaticamente

A questo punto si utilizza il comando “exploit” per avviare l’attacco. Si prende così il controllo della macchina vittima (per verificare è sufficiente effettuare un “ifconfig” e visualizzare l’ip della vittima).

Immagine che contiene testo, schermata, Carattere, software

Descrizione generata automaticamente

A questo punto si verifica la propria posizione nella macchina con “pwd” e verifica la posizione “/” si crea la cartella “test\_metasploit” con il comando “mkdir”. Infine, con “ls” è possibile verificare la creazione della cartella “test\_metasploit” all’interno di “/”.

Immagine che contiene testo, schermata, Carattere, design

Descrizione generata automaticamente