EPICODE

Esercizio S7 – L2

TRACCIA

Sulla base dell’esercizio visto in lezione teorica, utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet\_version sulla macchina Metasploitable.

SOLUZIONE

Come prima operazione si è usato Nmap per rilevare il servizio Telnet sulla porta 23.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Segue

Si è poi aperto Metasploit e si è verificata la connessione.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Si è quindi cercato il modulo ausiliario corretto.

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

Segue

Una volta richiamato quello corretto (use 14) si utilizza “show options” per visualizzare le informazioni che mancano per effettuare l’exploit. In questo caso manca solamente l’indirizzo ip della vittima.

Immagine che contiene testo, schermata, software, Carattere

Descrizione generata automaticamente

Con “set rhosts 192.168.1.110” si setta l’ip destinatario mancante.

Immagine che contiene testo, schermata, software, Carattere

Descrizione generata automaticamente

A questo punto si effettua l’attacco con il comando “exploit”. L’attacco andato a buon fine ha restituito login e password da inserire per poter accedere alla macchina vittima.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente