EPICODE

Progetto S7 – L5

TRACCIA

La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI.  
Si richiede allo studente di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota.  
I requisiti dell’esercizio sono:  
● La macchina attaccante (KALI) deve avere il seguente indirizzo IP: 192.168.11.111 (opzionale)  
● La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: 192.168.11.112 (opzionale)  
● Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota:  
1) configurazione di rete.  
2) informazioni sulla tabella di routing della macchina vittima.

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 effettuare diverse operazioni. Tra cui: prendere il controllo del sistema vittima; accedere ai permessi da amministratore; inserire malware (codici dannosi) di vario tipo; spostarsi e attaccare altri dispositivi della stessa rete.

Metasploit:

Metasploit è uno strumento di pentesting che permette di utilizzare exploit già noti per vulnerabilità note e di abbinarci dei payload (insieme di istruzioni) già pronti. I payload possono svolgere diverse funzioni, tra cui prendere il controllo della macchina target e accedere ai privilegi di amministratore. 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.

Meterpreter:

Meterpreter è uno dei payload più utilizzati di Metasploit in quanto fornisce una shell potente che permette di utilizzare utility e comandi avanzati. È infatti possibile migrare su processi differenti, effettuare screenshot ed eseguire il pivoting (attaccare altri sistemi all’interno della stessa rete). La shell di Meterpreter può essere Bind Shell quando la connessione tra le macchine parte dall’attaccante e Reverse Shell quando la connessione viene stabilita da parte della macchina vittima. Idealmente è meglio ottenere una Reverse Shell in quanto più difficilmente il firewall bloccherà una connessione stabilita dall’interno.

IP Kali: 192.168.1.101 - IP Metasploitable: 192.168.1.110

Per iniziare si effettua una scansione con Nmap per identificare la porta ed il servizio vulnerabile java-rmi.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Si passa quindi su Metasploit e si utilizza l’exploit più adatto (use 1). Il payload inserito di default è ottimo perché crea una reverse shell di Meterpreter. Si verificano poi le opzioni.

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

Si settano le opzioni obbligatorie mancanti come l’ip target (rhosts) e quelle utili a far funzionare correttamente l’exploit (httpdelay).

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

A questo punto si può far partire l’attacco con il comando “exploit”. Una volta ottenuta la sessione remota è possibile verificare la configurazione di rete con il comando “ifconfig” e accertarsi così di essere effettivamente nella macchina target.

Immagine che contiene testo, schermata, Carattere, design

Descrizione generata automaticamente

Con il comando “route” si possono visualizzare informazioni sulla tabella di routing della macchina vittima.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente