Relazione

Java RMI

Sulla porta 1099 TCP della Metasploitable c'è un servizio Java-RMI che permette ai processi Java di comunicare tra loro. La vulnerabilità deriva da una configurazione di default errata che consente l'iniezione di codice per ottenere accesso amministrativo.
Per iniziare dovremmo utilizzare il comando MSFConsole per far partire Metasploit, dopo di che utilizziamo il keyword ”search java_rmi” per individuare l’exploit che ci possa servire.
Dopo aver individuato l’exploit che ci serve utilizziamo il commando “use” seguito poi dal path dell’exploit. Subito dopo vedremo che metasploit ci dare di default il playload. Dopo di che utilizziamo il commando “show options” dove potremmo configurare il parametro rhost and lhost.
Dopo aver configurato i parametri utilizziamo il comando “exploit” per lanciare l’attacco, se l’attacco va a buon fine allora riceveremo una shell di meterpret, subito dopo utilizziamo il comando “ifconfig” che ci restituisce la configurazione di rete della macchina.