BAB IV

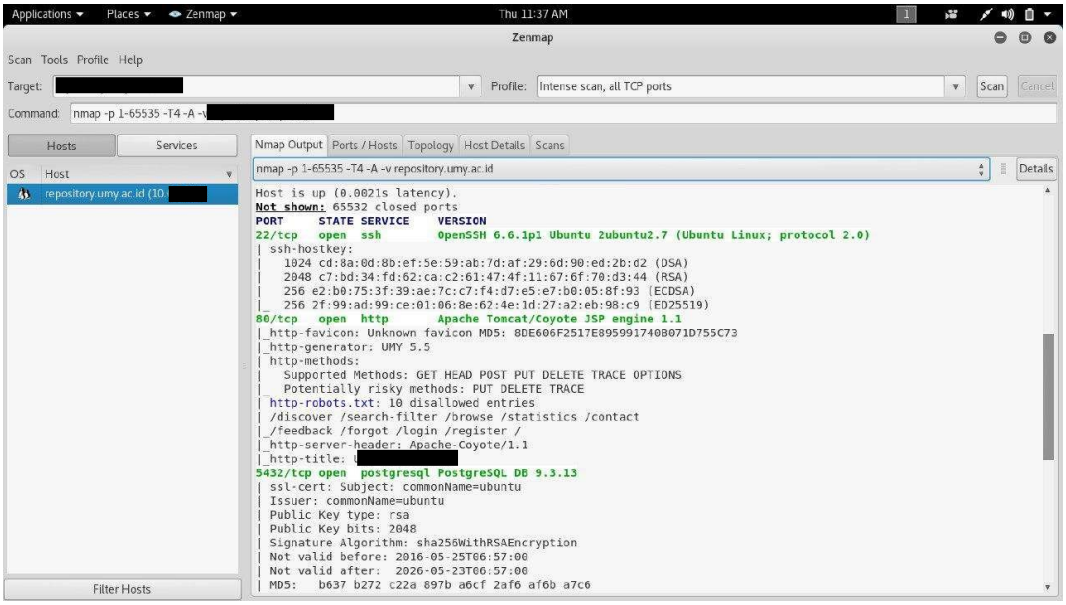
HASIL DAN PEMBAHASAN

4.1 *Scope*

Peneliti menetapkan cakupan pada web aplikasi repositori Institusi Pendidikan XYZ untuk menjadi target *penetration testing*. Alasan ditetapkannya aset tersebut adalah merujuk pada penelitian sebelumnya yang memebahas tentang daftar urutan aset penting milik Institusi Pendidikan XYZ (Yuhaz, 2018). Alasan lainnya adalah menurut pihak Institusi Pendidikan XYZ, web aplikasi repositori adalah aset yang sering terjadi serangan dari luar Institusi, serangan yang paling sering terjadi adalah percobaan masuk kedalam sistem. SQL Injection juga termasuk serangan yang pernah dialami oleh aset tersebut dan penanganan membutuhkan waktu beberapa hari. Cakupan untuk *penetration testing* terbatas pada pencarian hak akses pada web aplikasi tersebut.

4.2 *Reconnaisance*

Pemindaian informasi aset yang dalam hal ini adalah web aplikasi repositori. Hasil pemindaian ini berupa informasi sistem operasi yang digunakan, yaitu Linux Ubuntu. Alamat IP 10.X.X.X. Port yang terbuka adalah port 22, 80 dan 5432. **Gambar 4.1** menerangkan tentang hasil pemindaian menggunakan *tool* Zenmap.



Gambar 4. 1 Pemindaian Informasi Aset

4.3 *Vulnerability Detection*

Pada tahap ini dilakukan identifikasi celah keamanan pada web aplikasi repositori Institusi Pendidikan XYZ menggunakan *tool* Nessus. Celah keamanan pada repositori Institusi Pendidikan XYZ ditampilkan dalam **Tabel 4.1**.

Tabel 4. 1 Daftar Celah Keamanan

No	Tingkat	Nama	Deskripsi
1	*Medium*	*Apache Tomcat Default File*	Halaman kesalahan, beranda dan halaman contoh dari JSPs yang masih tersimpan di Apache Tomcat Server
2	*Medium*	*Web Application Potentially Vulnerable to Clickjacking*	Halaman web memungkinkan untuk dilakukan Clickjacking

No	Tingkat	Nama	Deskripsi
3	*Low*	*Web Server Transmits Cleartext Credentials*	Perjalanan data sensitif seperti username dan password yang bisa dibaca dengan jelas (Cleartext)
4	*Low*	*Web Server Uses Basic Autentication Without HTTPS*	Halaman web menggunakan autentikasi standar dan belum menggunakan HTTPS
5	*Info*	*Nessus SYN scanner*	Beberapa port setengah terbuka; Port 22, 80 dan 5432
6	*Info*	*Apache Tomcat Detection*	Web aplikasi ini menggunakan Apache Tomcat Web Server
7	*Info*	*CGI Generic Injectable Parameter*	Memungkinkan halaman web untuk membaca parameter yang tidak berbahaya pada url
9	*Info*	*CGE Generic Tests Load Estimation (all test)*	Skrip untuk menghitung jumlah maksimal permintaan yang akan dilakukan oleh generic web test
10	*Info*	*CGI Generic Tests Timeout*	Beberapa CGI generic test kehabisan waktu
11	*Info*	*External URLs*	Tool membaca link HREF yang mengarah ke situs luar
12	*Info*	*HTTP Methods Allowed (per directory)*	Metode HTTP yang memungkinkan untuk mengakses direktory
13	*Info*	*HTTP Server Type and Version*	Apache-Coyote/1.1
14	*Info*	*HTTP Information*	Informasi mengenai HTTP

No	Tingkat	Nama	Deskripsi
15	*Info*	*Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header*	Beberapa respon pada Web Server tidak menetapkan frame header CSP
16	*Info*	*Missing or Permissive X-Frame-Options HTTP Response Header*	Beberapa respon pada Web Server tidak menetapkan X-Frame-Options
17	*Info*	*Ping the remote host*	Remote host berstatus “up”
18	*Info*	*Protected Web Page Detection*	Beberapa halaman web diproteksi menggunakan autentikasi HTTP
19	*Info*	*Web Application Cookies Not Marked Secure*	Cookie yang berjalan pada web ini tidak terautentikasi dan terkonformasi oleh pengguna
20	*Info*	*Web Application Sitemap*	Web berisi konten yang bisa dikaitkan dengan penyerangan target
21	*Info*	*Web Mirroring*	Tool menggandakan web dan menjalankan CGI
24	*Info*	*Web Server Harvested Email Address*	Terdapat alamat email perorangan pada halaman web
25	*Info*	*Web Server Office File Inventory*	Beberapa file .pdf, .doc yang bisa diakses langsung dari url

4.4 *Information Analysis & Planning*

Hasil dari *vulnerability scanning* menampilkan informasi terkait celah keamanan pada web aplikasi repositori Institusi pendidikan XYZ. Peneliti mengambil dua celah yang digunakan untuk bahan *penetration testing*. Pemilihan celah ini didasari pada analisis kemungkinan untuk mendapatkan hasil dalam waktu yang relatif singkat. Dua celah yang digunakan oleh peneliti dijelaskan pada **Tabel 4.2**.

Tabel 4. 2 Daftar celah yang akan diuji

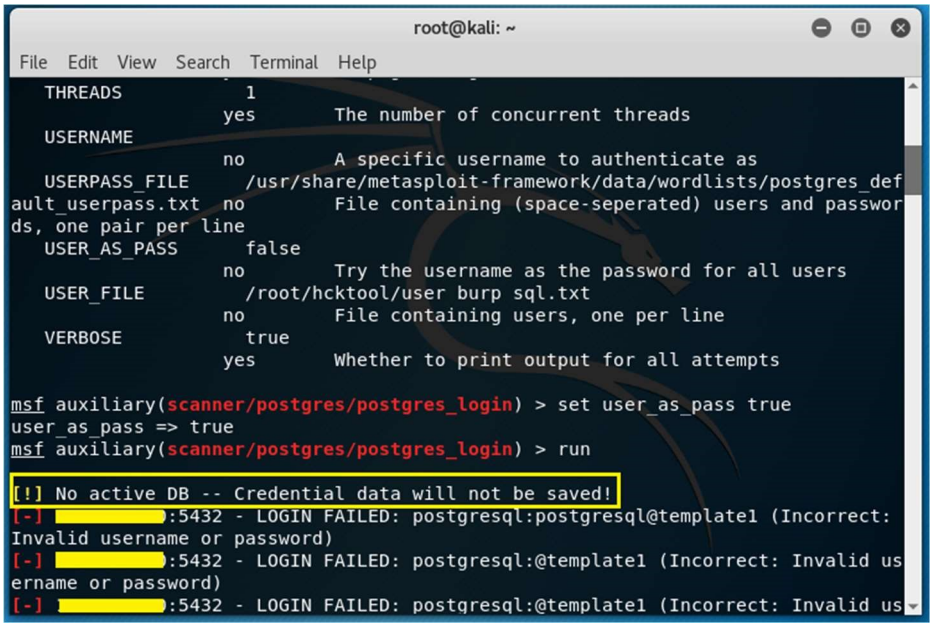
No	Tingkat	Nama	Alasan	*Tool*
1	*Info*	SYN *Scanner*	Untuk mengetahui port yang terbuka	Metasploit
2	*Low*	*Web Server Transmits Cleartext Credentials*	Untuk mengetahui *username* dan *password* dari pengguna	Arpspoof dan SSLStrip

4.5 *Penetration Testing*

Peneliti melakukan *penetration testing* pada web aplikasi repositori Institusi Pendidikan XYZ dengan memanfaatkan dua celah beserta *tool* yang digunakan pada **Tabel 4.2**. Hasil pengujiannya adalah sebagai berikut:

4.5.1 SYN *Scanner*

SYN Scanner adalah salah satu celah ini dimanfaatkan peneliti dengan teknik penyerangan *brute force* menggunakan *tool* Metasploit. Celah ini menjelaskan bahwa web server mempunyai tiga port yang terbuka, yaitu port 22, 80 dan 5432. Penyerangan dilakukan pada port 5432 yang merupakan port *database postgresql*. Hasil yang ingin dicapai oleh peneliti adalah masuk kedalam *database* melalui port tersebut. Berikut hasil pengujian yang ditampilkan pada **Gambar 4.2.**



Gambar 4. 2 Hasil Serangan *Brute Force*

Gambar 4.2 menjelaskan proses serangan menggunakan teknik serangan *brute force*. Cara kerja dari teknik serangan adalah peneliti mencoba masuk kedalam sistem *database postgresql* melalui port 5432. Percobaan masuk kedalam sistem ini adalah dengan cara mencoba satu per satu kombinasi dari baris *username* dan *password* menggunakan file berisi kumpulan *username* dan *password* yang dibuat oleh peneliti. Hasil dari penyerangan ini tidak berhasil, karena *firewall* lebih dahulu mencegah koneksi dengan *database*. Keterangan ini dijelaskan melalui pesan kesalahan **[!]** ***No active DB – Credential data will not be saved!*** yang ditampilkan pada tool metasploit.

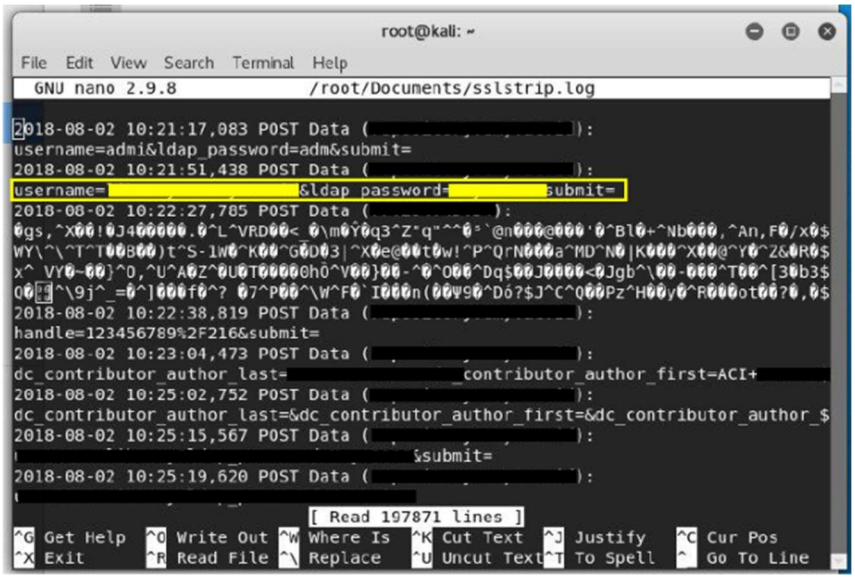
4.5.2 *Web Server Transmit Cleartext Credential*

Temuan celah ini mendefinisikan bahwa perjalanan data sesi dari dan menuju web aplikasi tidak terenkripsi, sehingga perjalanan data tersebut bisa dilihat secara jelas *Cleartext*. Celah ini dimanfaatkan peneliti untuk mengetahui akun yang digunakan untuk mengakses web aplikasi tersebut dengan cara membaca data sesi dari perangkat *client* menuju web aplikasi. Cara ini biasa disebut juga dengan teknik serangan *man in the middle*.

Untuk itu peneliti membuat skenario untuk mendapatkan akun tersebut. Penjelasan mengenai skenario adalah sebagai berikut:

1. Pertama, peneliti melakukan observasi untuk mengetahui staf yang memilki hak akses.
2. Mencari cara untuk terhubung dengan jaringan yang sama dengan perangkat yang digunakan oleh staf tersebut.
3. Melakukan *scanning* untuk mendapatkan seluruh alamat IP yang terhubung pada jaringan tersebut menggunakan *tool* Nmap.
4. Peneliti menjalankan *tool* arpspoof. *Tool* ini digunakan untuk memanipulasi tabel ARP untuk menjadikan laptop yang digunakan oleh peneliti dianggap sebagai gateway pada jaringan tersebut, sehingga paket yang akan berjalan dari dan menuju gateway akan melewati laptop peneliti terlebih dahulu.
5. Peneliti menjalankan *tool* sslstrip untuk menyadap paket data pada setiap transaksi yang terjadi pada jaringan tersebut.

Hasil dari menjalankan skenario tersebut adalah berupa file yang berisi informasi tentang transaksi yang terjadi pada jaringan tersebut. Diantara baris log tersebut terdapat *username* dan *password* yang ditujukan pada web aplikasi repositori yang terekam secara jelas (*cleartext*). **Gambar 4.3** menjelaskan tentang hasil log yang terekam pada kegiatan diatas.

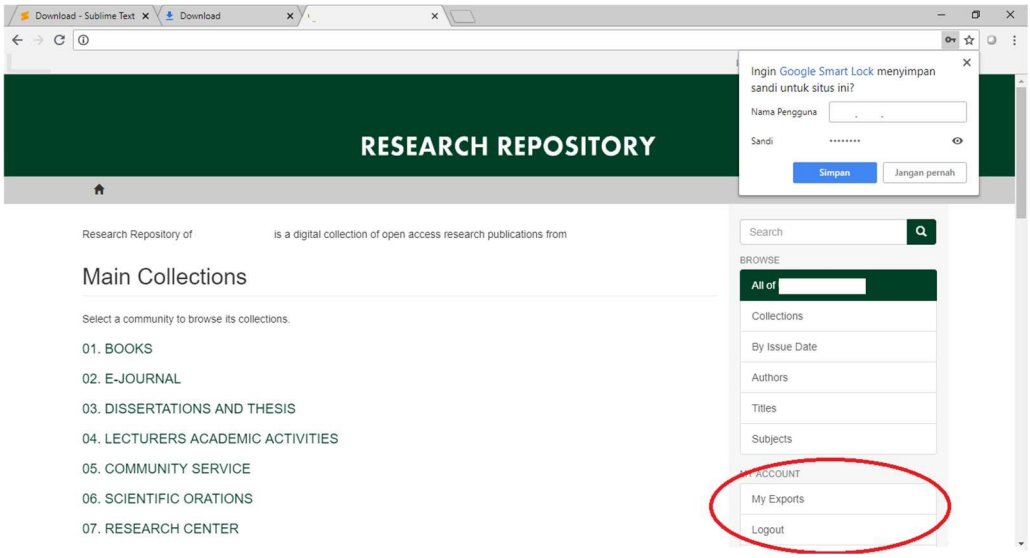


Gambar 4. 3 Log SSLStrip

Peneliti melakukan pencarian informasi lebih dalam dengan cara *social engineering*. Kegiatan *social engineering* dilakukan dengan bentuk wawancara kepada salah seorang staf. Wawancara dimaksudkan untuk mencari informasi tentang pengguna dari web aplikasi repositori ini. Dari hasil *social engineering* diketahui bahwa *username* dan *password* yang didapatkan pada kegiatan *penetration testing* adalah satu satunya akun admin yang digunakan oleh seluruh staf yang ada di ruangan tersebut. Akun tersebut digunakan untuk manajemen file pada web aplikasi tersebut.

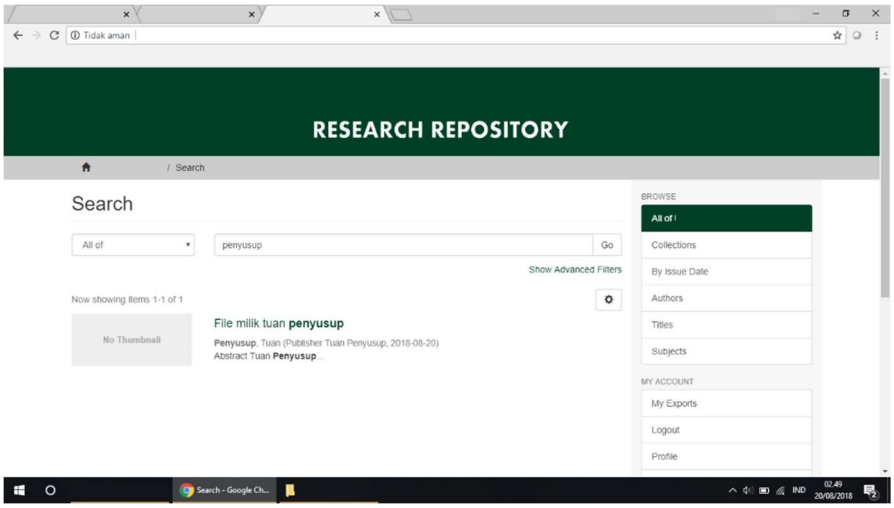
4.6 *Privilege Escalation*

Pemanfaatan celah keamanan yang dilakukan peneliti adalah melakukan login pada web aplikasi repositori Institusi Pendidikan XYZ yang ditunjukkan pada **Gambar 4.4**. Tidak ada perbedaan yang signifikan mengenai tampilan beranda pada web aplikasi ini, perbedaan hanya terdapat tombol *submission* yang digunakan untuk mengunggah dokumen dan tombol *logout* yang digunakan untuk keluar dari akun.



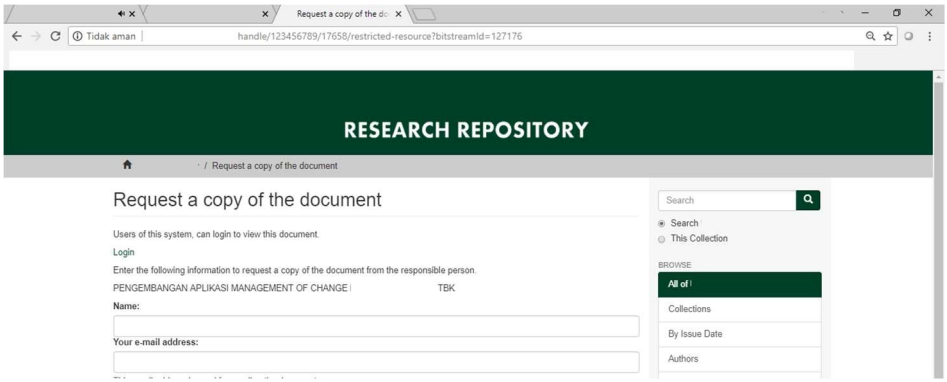
Gambar 4. 4 Tampilan Web Aplikasi Repositori Setelah *Login*

Peneliti juga memanfaatkan fitur berupa hak untuk mengunggah file berjenis .docx dengan cara mengikuti alur *submission* pada web aplikasi tersebut. Peneliti hanya perlu mengunggah file tersebut dan mengisi keterangan tentang dokumen tersebut seperti nama file, nama penulis dan lain-lain. File tersebut berhasil tersimpan pada web aplikasi tersebut dan diterangkan pada **Gambar 4.5**.



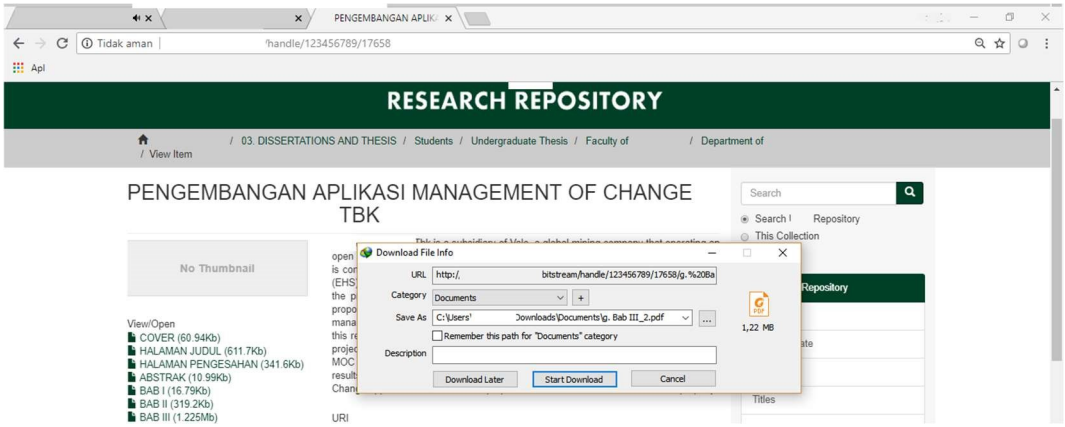
Gambar 4. 5 Berhasil Mengunggah File Setelah *Login*

Pada **Gambar 4.6** menjelaskan bahwa terdapat sebuah file yang tidak bisa diunduh secara langsung. File tersebut sengaja diatur untuk tidak bisa diunduh, atas permintaan dari *author* file tersebut yang tidak mengizinkan file tersebut untuk diakses secara publik dikarenakan alasan tertentu. Peneliti diharuskan melalui fase *request copy* jika ingin menyalin informasi dari file tersebut dan menunggu persetujuan dari *author* file tersebut untuk mendapatkan salinan file tersebut.



Gambar 4. 6 File tidak bisa diunduh

Perbedaan yang terlihat jika peneliti telah melakukan *login* adalah file tersebut bisa diunduh tanpa harus melewati fase *request copy* yang diterangkan pada **Gambar 4.6**. File tersebut berhasil diunduh secara langsung, seperti yang terlihat pada **Gambar 4.7**.



Gambar 4. 7 Berhasil Mengunduh File Setelah *Login*

4.7 Reporting

Pada tahap ini peneliti melakukan penulisan mengenai laporan hasil penelitian yang membahas tentang *security assessment* pada web aplikasi repositori Institusi Pendidikan XYZ. Hasil penulisan laporan akan ditujukan kepada Institusi Pendidikan XYZ sebagai dokumentasi dan bahan evaluasi untuk peningkatan keamanan pada web aplikasi repositori yang dimilikinya. Penulisan laporan akan disertakana dalam lampiran.