Keamanan Jaringan Komputer

Disusun Oleh

Nama : Kusuma Dwi Indriani

NIM : 09011181320017

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

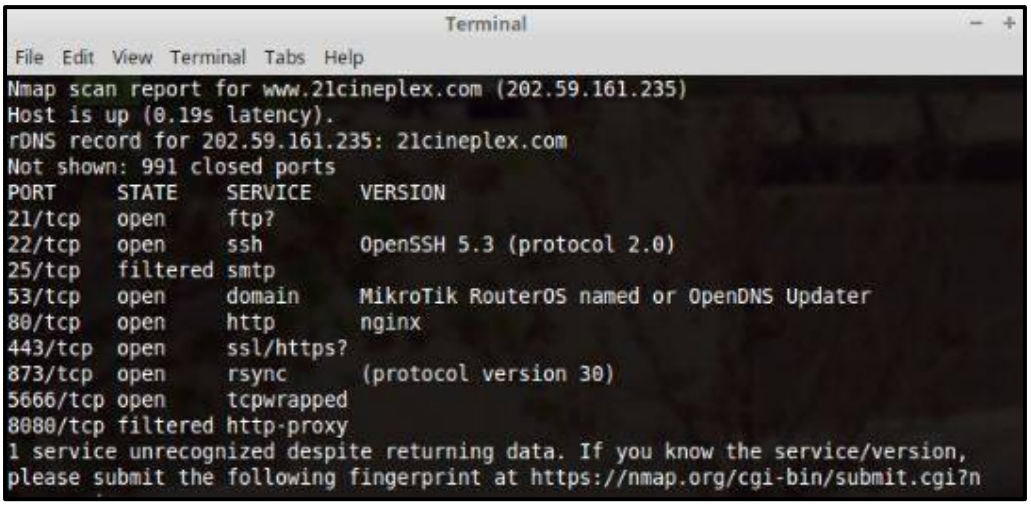
2017

TAHAP II. SCANNING

Scanning bertujuan untuk mencari port target yang terbuka. Aplikasi yang rentan terhadap kegiatan *hacking* dan celah lainnya. Pada tahapan scanning ini target dari web sama pada tahapan sebelumnya yaitu www.21cineplex.com. Adapun langkah-langkah yang dilakukan dalam proses scanning sebagai berikut :

1. Periksa port yang terbuka

   port scanning adalah suatu kegiatan atau aktifitas atau proses untuk mencari dan melihat serta meneliti port pada suatu komputer atau perlengkapan dan peralatannya. Tujuan dari kegiatan ini adalah meneliti kemungkinan-kemungkinan kelemahan dari suatu sistem yang terpasang pada suatu komputer atau perlengkapan dan peralatannya melalui port yang terbuka. Gambar 1 merupakan hasil dari pemindaan port yang terbuka pada target 21cineplex.com.

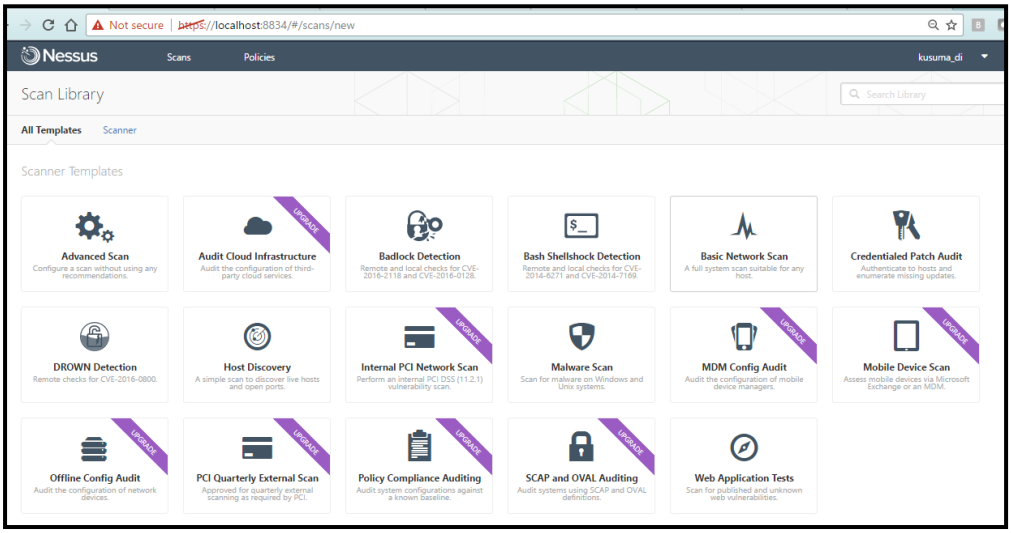


Gambar 1. Port scanning 21cineplex.com menggunakan nmap

2. Scan untuk mencari *Vulnerability*

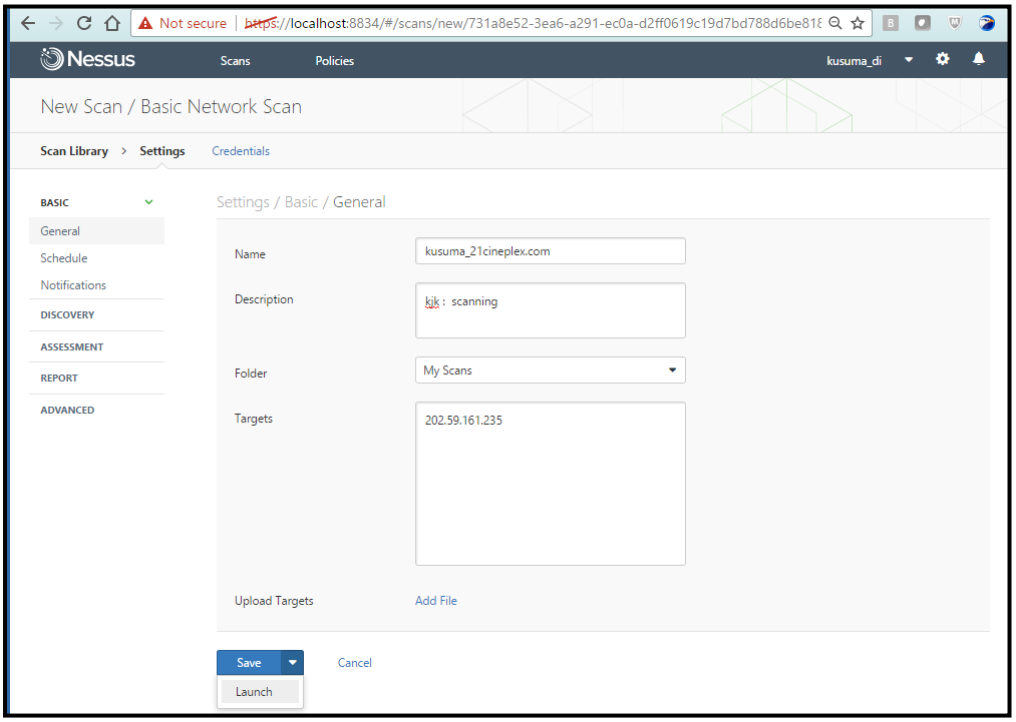
   Vulnerability scanner adalah sebuah program komputer yang di desain untuk mencari dan memetakan sistem untuk kelemahan pada aplikasi, computer atau jaringan. *Tools* yang digunakan untuk menganalisa kelemahan-kelemahan system salah satunya adalah Nessus. Nessus merupakan kelompok

free scanner. *Nessus* didistribusikan di bawah GNU *Public License* dari *Free Software Foundation*. Pada gambar 2 ditunjukkan tampilan *Nessus Scanner*.



Gambar 2. tampilan *Nessus Scanner*

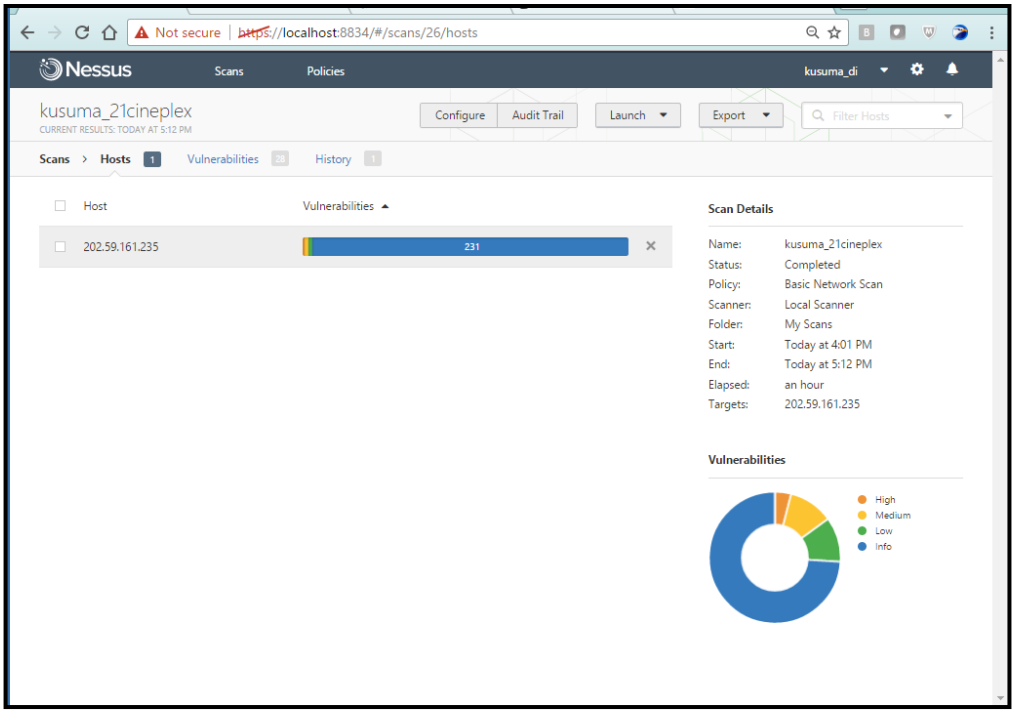
Jalankan nessus scanner dengan cara login terlebih dahulu kemudian masukkan IP target dan pada menu paling bawah pilih ‘Lauch’ seperti gambar 3. Tunggu hingga proses scan *completed.*



Gambar 3. Masukkan ip target saat ingin melakukan scanning

3. Analisa *Vulnerability* yang dihasilkan dari *Nessus Scanner* untuk mengetahui celah yang didapat

Setelah proses scanning telah selesai dilakukan pada *nessus scanner* hasil dari analisa *Vulnerability* terhadap target dapat diketahui beberapa kelemahan-kelemahan yang bisa menjadi pintu masuk. Hasil yang ditunjukkan Nessus Scanner dapat diketahui terdapat 7 jenis kelemahan terdiri dari berbagai kategori yakni *high*, *medium*, dan *low*. Sedangkan info hanya menampilkan informasi yang menyangkut informasi target. Pada gambar 4 menunjukkan hasil dari *Nessus scanner*.

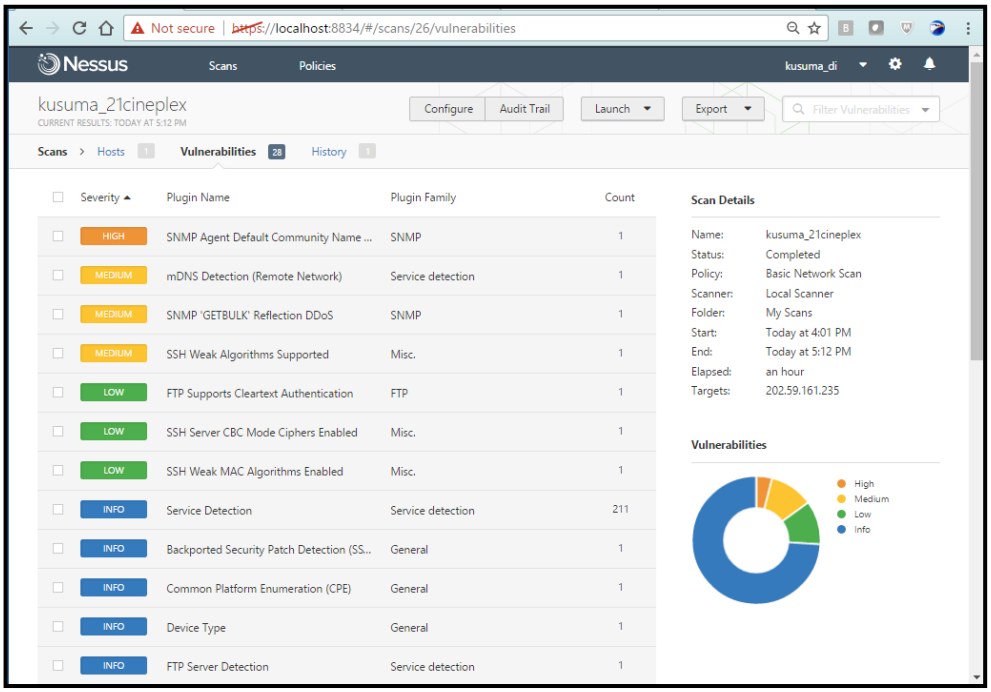


Gambar 4. Hasil Nessus Scanner

Dari gambar 3 dapat diketahui jenis kelemahan dengan rincian sebagai berikut:

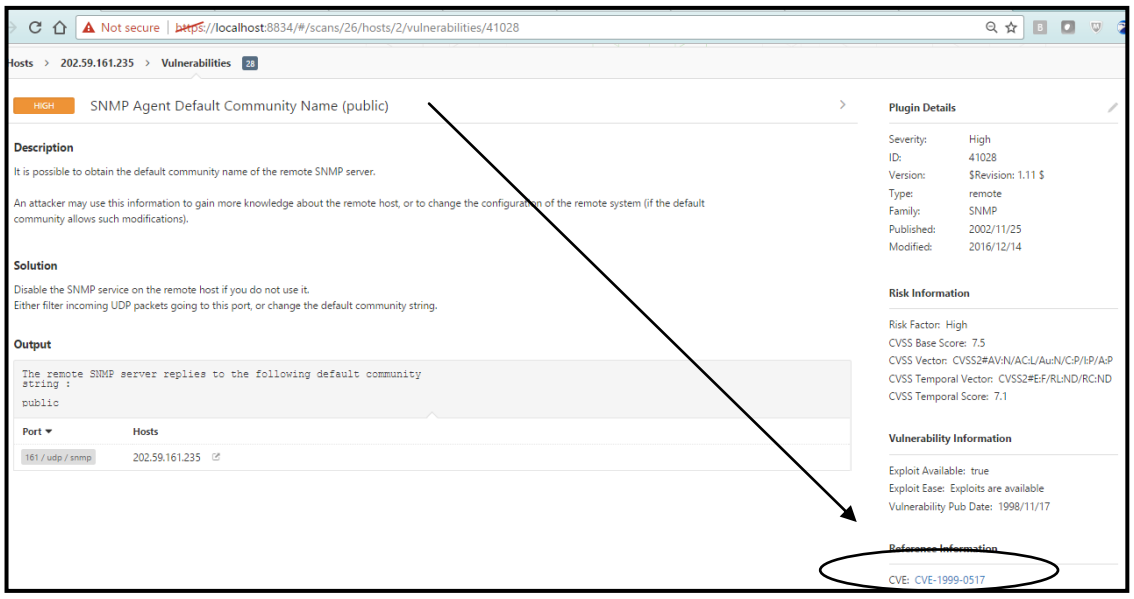
a. Kategori High 1 kelemahan
b. Kategori Medium 3 kelemahan
c. Kategori Low 3 kelemahan

Tidak hanya menampilkan kelemahan dari suatu target, hasil scan menggunakan Nessus juga dapat menampilkan secara detail apa yang menjadi penyebab kelemahan serta solusi dari kelemahan tersebut. Kelemahan-kelemahan tersebut secara rinci ditampilkan pada gambar 5



Gambar 5. Detail hasil scan menggunakan nessus pada target 21cineplex.com

Semua kategori kelemahan hasil dari scan menggunakan Nessus ditampilkan penjelasan tentang kelemahan yang ada. Saat klik pada bagian kelemahan tersebut maka akan muncul detail informasi kelemahan tersebut. *Reference information* juga didapatkan pada *Nessus Scanner* ini. Seperti yang ditampilkan pada gambar 6.



Gambar 6. Informasi Detail Kategori High

Berikut hasil penjabaran *Vulnerability* pada web 21cineplex besert pada web 21cineplex solusi dalam mengatasi kelemahan-kelemahan tersebut :

Tabel 1. Deskripsi *Vulnerability* pada web 21cineplex

no	*Vulnerability*	deskripsi	solusi	referensi
1	SNMP Agent Default Community Name (public)	Hal ini dimungkinkan untuk mendapatkan nama komunitas default server SNMP terpencil. Seorang penyerang dapat menggunakan informasi ini untuk mendapatkan lebih banyak pengetahuan tentang remote host, atau untuk mengubah konfigurasi sistem remote	-Menonaktifkan layanan SNMP dari host remote jika tidak menggunakannya. -Menyaring masuk paket UDP akan port ini, atau mengubah string komunitas default.	CVE-1999-0517 OSVDB: 209 BID: 2112
2	Mendeteksi mDNS (Remote Jaringan)	Layanan remote memahami Bonjour (juga dikenal sebagai Zeroconf atau mDNS) protokol, yang memungkinkan setiap orang untuk mengungkap informasi dari remote host	Filter traffic masuk ke port UDP 5353, jika memungkinkan.	-

		seperti jenisnya sistem operasi dan versi yang tepat, nama host, dan daftar layanan sedang berjalan. Nessus menemukan mDNS digunakan oleh host yang tidak pada segmen jaringan		
3	DDoS Refleksi SNMP 'GETBULK'	Remote SNMP daemon merespons dengan sejumlah besar data permintaan 'GETBULK' dengan lebih besar dari normal nilai 'max-pengulangan'. Seorang penyerang jarak jauh dapat menggunakan server SNMP ini untuk melakukan penolakan didistribusikan tercermin dari serangan layanan pada host remote yang sewenang-wenang.	-Menonaktifkan layanan SNMP dari host remote jika tidak menggunakannya. -Jika tidak, membatasi dan memonitor akses ke layanan ini, dan mempertimbangkan mengubah default 'publik' string public.	OSVDB: 125796
4	Didukung oleh Algoritma SSH yang Lemah	Nessus telah mendeteksi bahwa server SSH remote dikonfigurasi untuk menggunakan arcfour stream cipher atau tanpa cipher sama sekali. RFC 4253 menyarankan untuk tidak menggunakan arcfour karena ada masalah dengan pada kelemahan kunci.	Hubungi vendor atau berkonsultasi dengan dokumentasi produk untuk menghapus cipher lemah.	-
5	FTP Mendukung autentikasi cleartext	Remote FTP server memungkinkan nama pengguna dan kata sandi untuk ditransmisikan dalam format teks, yang dapat disadap oleh sniffer jaringan atau serangan man-in-the-middle.	Beralih ke SFTP (bagian dari SSH suite) atau FTPS (FTP over SSL / TLS). Dalam kasus terakhir, mengkonfigurasi server sehingga koneksi kontrol akan dienkripsi.	CWE: 522, 523, 928, 930
6	SSH Server CBC mode Cipher Diaktifkan	Server SSH dikonfigurasi untuk mendukung Cipher Block Chaining (CBC) enkripsi. Hal ini dapat memungkinkan	Hubungi vendor atau berkonsultasi dengan dokumentasi produk untuk menonaktifkan	CVE: CVE-2008-5161 OSVDB: 50035, 50036

		seorang penyerang untuk memulihkan pesan plaintext dari ciphertext. Perhatikan bahwa plugin ini hanya memeriksa opsi dari server SSH dan tidak memeriksa versi software rentan.	CBC enkripsi modus cipher, dan memungkinkan RKT atau enkripsi modus GCM cipher.	BID: 32319 CERT: 958563 CWE: 200
7	Lemahny SSH Algoritma MAC yng aktif	remote Server SSH dikonfigurasi untuk memungkinkan baik MD5 atau 96-bit MAC algoritma, yang keduanya dianggap lemah. Perhatikan bahwa plugin ini hanya memeriksa opsi dari server SSH, dan tidak memeriksa versi software rentan	Hubungi vendor atau berkonsultasi dengan dokumentasi produk untuk menonaktifkan MD5 dan 96-bit MAC algoritma.	-