NETWORK SECURITY MID:
SCANNING AND VULNERABILITY PADA WEBSITE RESMI PALEMBANG

BY

NAME	: DENI DANUARTA
NIM	: 09121001045
CLASS	: SK 8 PILIHAN
STUDY	: NETWORK SECURITY

COMPUTER ENGINEERING
DEPARTMENT OF COMPUTER SCIENCE
SRIWIJAYA UNIVERSITY

I. LATAR BELAKANG

Pada situs pemerintahan sering terjadi bug-bug yang tidak di inginkan. Hal tersebut menjadi rentan untuk kebocoran informasi dan di susupi kode-kode yang tidak diinginkan. Selain itu banyak sekali bug-bug yang tidak kita inginkan. Ini menjadi senjata para hacker bahwa kebocoran dan rahasia sebuah informasi dapat mereka retas. Kurang upgrade dari sebuah situs pemerintahan daerah adalah penyebab masalah ini.

Pada penulisan ini saya melakukan scanning di palembang.go.id. Ini terjadi karena kepedulian saya terhadap website daerah yang punya banyak sekali masalah pada servernya. Dengan hal ini mungkin sebagai solusi dari permasalahan yang di hadapi saat ini

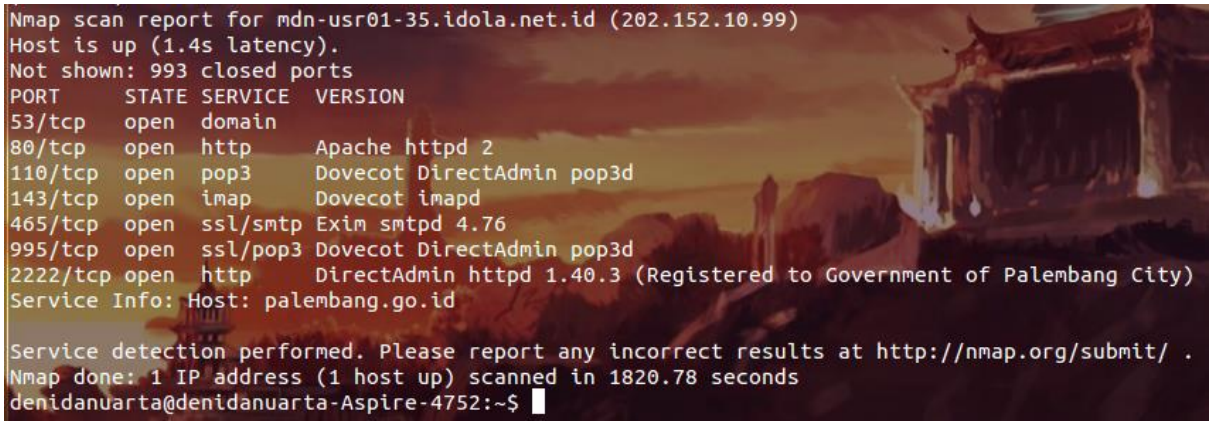
A. OPEN PORT

Dalam protokol jaringan TCP/IP, Port dapat mengidentifikasikan aplikasi dan layanan yang menggunakan koneksi di dalam jaringan TCP/IP. Sehingga, port juga mengidentifikasikan sebuah proses tertentu di mana sebuah server dapat memberikan sebuah layanan kepada klien atau bagaimana sebuah klien dapat mengakses sebuah layanan yang ada dalam server.

Pada penulisan ini, kita dapat mencari informasi open port dengan melakukan port scanning pada port target yang dituju. ***Port Scanning*** adalah a*ktivitas yang dilakukan untuk memeriksa status port TCP dan UDP pada sebuah mesin.* Jadi kita memeriksa open port target yang dituju apakah statusnya open, closed, bahkan filtered. Target yang kita tuju kali ini adalah www.palembang.go.id dengan menggunakan NMAP.

1. NMAP

Nmap (Network Mapper) merupakan sebuah tool open source untuk eksplorasi dan audit keamanan jaringan. Ia dirancang untuk memeriksa jaringan besar secara cepat, meskipun ia dapat pula bekerja terhadap host tunggal. Nmap menggunakan paket IP raw dalam cara yang canggih untuk menentukan host mana saja yang tersedia pada jaringan, layanan (nama aplikasi dan versi) apa yang diberikan, sistem operasi (dan versinya) apa yang digunakan, apa jenis firewall/filter paket yang digunakan, dan sejumlah karakteristik lainnya. NMAP sangat berguna untuk tugas rutin seperti inventori jaringan, mengelola jadwal upgrade layanan, dan melakukan monitoring uptime host atau layanan dan lain-lain. Pada tulisan ini, kita akan melihat openport dari www.palembang.go.id dengan menggunakan NMAP.

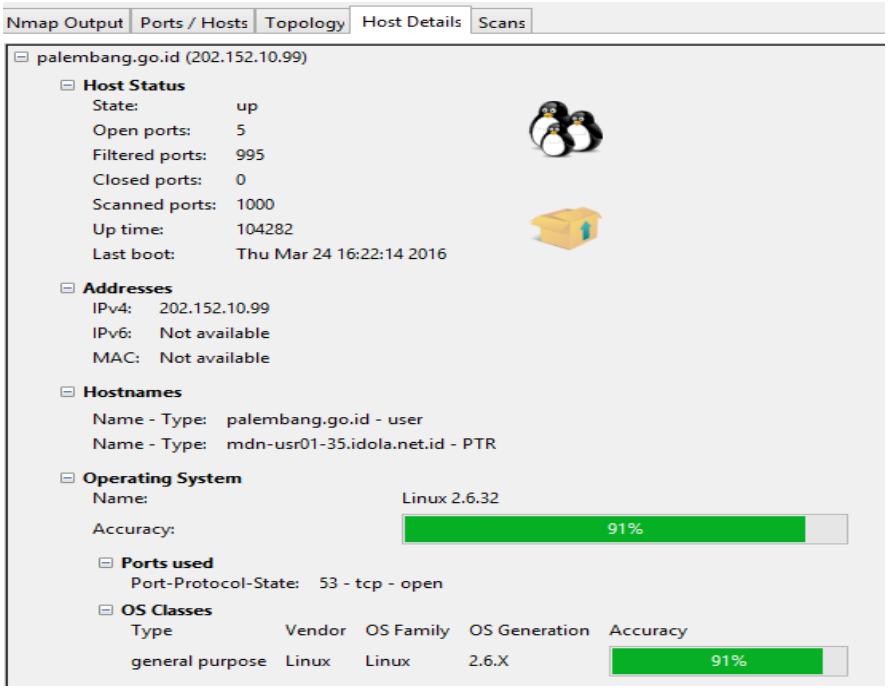


Gambar 1 Scanning Open Port Menggunakan NMAP

Pada gambar diatas adalah sebuah scanning Open Port dengan menggunakan NMAP pada Operating System Linux Ubuntu. Terdapat 7 openport yang ada pada sistem www.palembang.go.id yang terdiri dari port 53, 80, 110, 143, 465, 995, dan 2222. Tugas dari port port tersebut adalah sebagai berikut:

- port 53 adalah port domain name service
- port 80 merupakan webserver
- port 143 adalah port imap dan ssl
- port 465 adalah port ssl dan smtp
- port 995 adalah ssl dan pop3
- port 2222 adalah port http

Selain itu pada gambar tersebut terdapat rDNS yang merupakan mapping alamat ke suatu nama domain. rDNS biasanya digunakan untuk tracking visitor atau darimana sebuah email berasal dan lain-lain. rDNS tidak bersifat 'critical' seperti DNS. Pada Gambar 1 rDNS yang digunakan oleh www.palembang.go.id adalah **mdn-usr01-35.idola.net.id** yang vendornya adalah PT. Aplikanusa Lintasarta.



Gambar 2 Host Detail pada www.palembang.ac.id

Pada Host Detail seperti yang ada di atas, www.palembang.go.id memiliki 5 openport yang statusnya up dari 1000 port. 995 port yang ada hanya berstatus filtered. Selain itu pada Operating System www.palembang.go.id menggunakan Operating System Linux versi 2.6.X.

B. DAEMON

Gambar 3 Daemon pada www.palembang.go.id

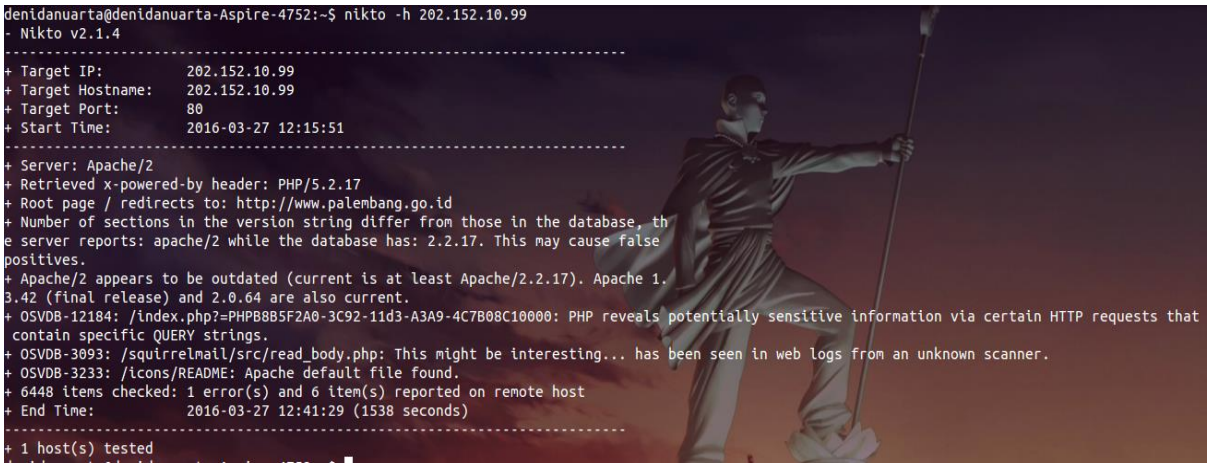
Gambar diatas merupakan contoh dari daemon. Daemon merupakan sebuah nama vendor/merk yang digunakan dalam sebuah port. Pada hasil scanning menggunakan NMAP pada **Gambar 1** terdapat vendor-vendor yang mendukung situs www.palembang.go.id. Berikut merupakan port dan vendor dari hasil scanning tersebut:

- Port 80 : Apache httpd 2
- Port 110 : Dovecot DirectAdmin pop3d
- Port 143 : Dovecot imapd
- Port 465 : Exim smtpd 4.76
- Port 995 : Dovecot DirectAdmin pop3d
- Port 2222 : DirectAdmin httpd 1.40.3 (Registered to Goverment of Palembang City)

C. VULNERABILITY

Vulnerability adalah mencari kelemahan dari suatu target atau situs website yang dituju. Pada percobaan kali ini, kita akan menganalisis vulnerability dari situs website www.palembag.go.id dengan menggunakan Nikto dan Nessus.

1. NIKTO



Gambar 4 Scanning Vulnerability Web dengan Menggunakan Nikto

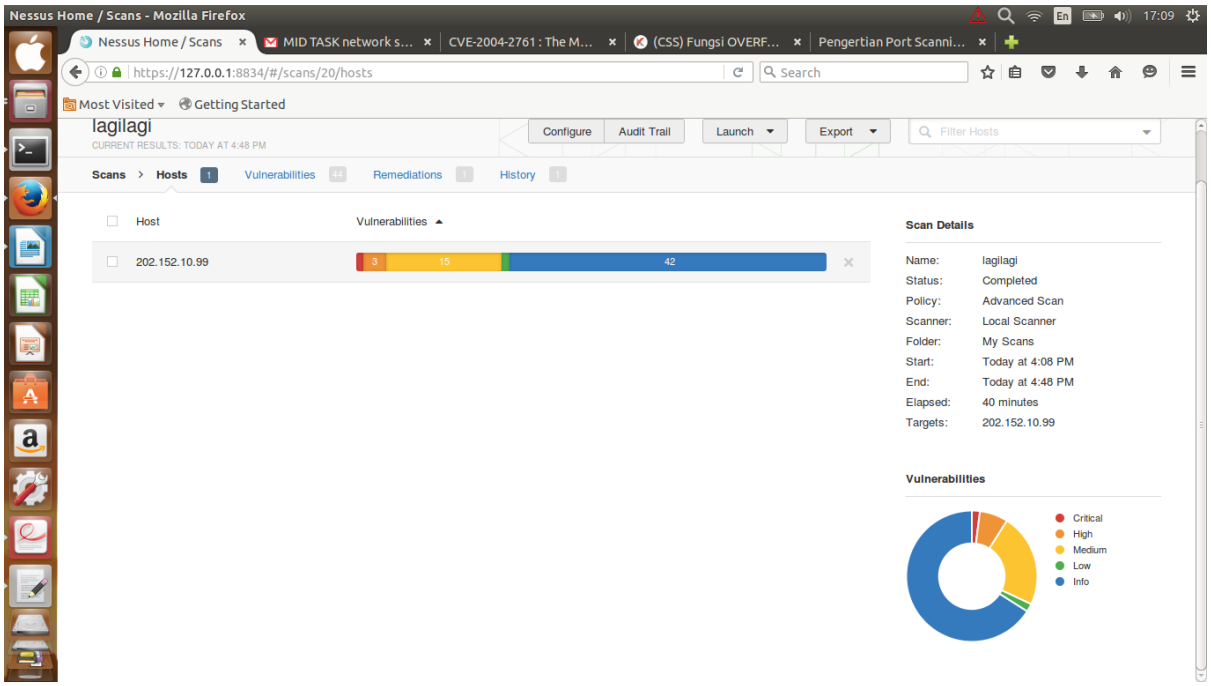
Pada percobaan kali ini, kita menggunakan software Nikto. Nikto merupakan sebuah software dimana kita bisa mencari lalulintas dari kelemahan webserver secara detail. Nikto hanya melakukan scanning port 80. Dari **Gambar 4,** kita dapat menganalisiskan bahwa www.palembang.ac.id memiliki beberapa kelemahan di webserver.

Pertama adalah penggunaan webserver dengan vendor Apache 2. Penggunaan ini sangat rentan karena dari situs tersebut kurang upgradenya vendor Apache 2 sehingga vendor tersebut sudah ketinggalan zaman. Resiko yang dihadapi adanya teknologi baru yang tidak mendukung Apache 2 tersebut.

Kedua adalah pada PHP CGI. PHP mengungkapkan informasi sensitif melalui HTTP request tertentu yang mengandung string QUERY tertentu. Adanya string query tersebut menjadikan kodingan pada web tersebut sedikit terganggu dan terjadi bug-bug yang tidak diinginkan.

Ketiga adalah log pada web. Adanya web log dari situs tersebut sudah terlihat dari scanner yang tidak diketahui oleh webserver tersebut. Dan kelemahan website yang terakhir yaitu file-file yang ada pada Apache default sudah ditemukan.

2. NESSUS



Gambar 5 Scanning Vulnerability pada NESSUS

Nessus merupakan scanning yang paling lengkap dalam mendapatkan informasi dari target yang dituju. Ini sangat bermanfaat karena informasinya jelas dan bisa menyelidiki CVE yang kita dapatkan. Dalam scanning menggunakan Nessus kita mendapatkan kelemahan target secara lengkap dan komplex. Berikut adalah gambar Vulnerability pada scanning website www.palembang.go.id:

CRITICAL	PHP Unsupported Version Detection	CGI abuses	1
HIGH	PHP < 5.3.11 Multiple Vulnerabilities	CGI abuses	1
HIGH	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution Plugin ID: 57537	CGI abuses	1
HIGH	PHP < 5.3.9 Multiple Vulnerabilities	CGI abuses	1
MEDIUM	SSL Certificate Cannot Be Trusted	General	2
MEDIUM	SSL Certificate with Wrong Hostname	General	2
MEDIUM	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	General	2
MEDIUM	SSL Self-Signed Certificate	General	2
MEDIUM	SSL Version 2 and 3 Protocol Detection	Service detection	2
MEDIUM	DNS Server Zone Transfer Information Disclosure (AXFR)	DNS	1
MEDIUM	PHP PHP_RSHUTDOWN_FUNCTION Security Bypass	CGI abuses	1
MEDIUM	SSL Certificate Expiry	General	1
MEDIUM	SSL Certificate Signed Using Weak Hashing Algorithm	General	1
MEDIUM	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	General	1
LOW	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	General	1

Gambar 6 Vulnerability pada www.palembang.go.id dengan menggunakan NESSUS

Pada hasil Scanning tersebut, kita telah mendapatkan vulnerability www.palembang.go.id. Berpacu pada hasil Nikto di **Gambar 4,** bahwa kelemahan target pada port 80 tersebut persis dengan yang kita lakukan pada Nessus. Kurang Upgradenya webserver dan juga pada CGI dalam kodingan PHP menyebabkan terjadi banyak tipe serangan pada web tersebut. Selain itu adanya Execute Code yang menyebabkan banyak sekali bug-bug yang tidak diinginkan. Untuk tipe serangan kita akan jelaskan pada bagian CVE Map. Untuk bagian DNS Server IMAP dan SSL kita akan jelaskan dibawah ini:

- SSL RC4 Cipher Suites didukung (Bar Mitzvah)
  Deskripsi
  Host remote mendukung penggunaan RC4 dalam satu atau lebih suite cipher. RC4 cipher adalah cacat dalam generasi dari aliran pseudo-random byte sehingga berbagai bias kecil yang diperkenalkan ke sungai, penurunan keacakan.
  Jika plaintext berulang kali dienkripsi (misalnya, cookies HTTP), dan penyerang dapat memperoleh banyak (yaitu, puluhan juta) cipherteks, penyerang mungkin dapat memperoleh plaintext.
  Solusi
  Mengkonfigurasi ulang aplikasi yang terpengaruh, jika mungkin, untuk menghindari penggunaan cipher RC4. Pertimbangkan untuk menggunakan TLS 1.2 dengan AES-GCM suite subjek ke browser dan dukungan web server.

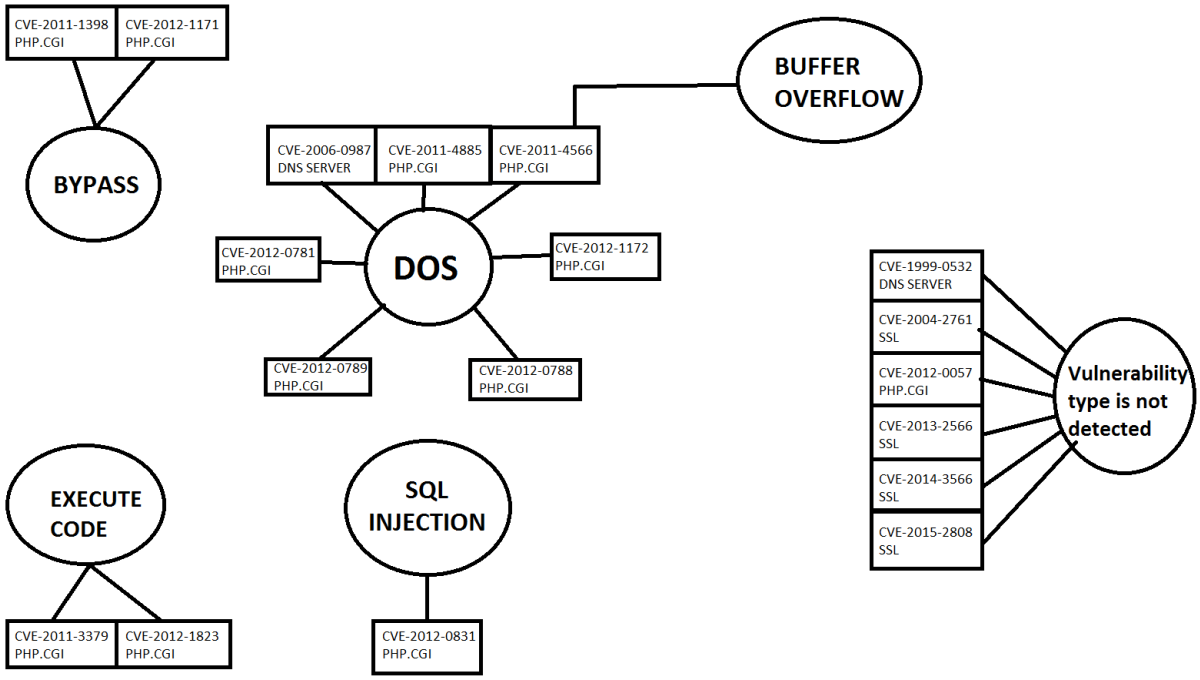
- SSLv3 Padding Oracle Pada Downgraded Legacy Encryption Kerentanan (POODLE)
  Deskripsi
  Remote host dipengaruhi oleh kerentanan (MITM) keterbukaan informasi man-in-the-middle dikenal sebagai POODLE. Kerentanan ini disebabkan oleh SSL cara 3.0 menangani padding byte ketika mendekripsi pesan dienkripsi menggunakan block cipher dalam mode cipher block chaining (CBC).
  - MITM penyerang dapat mendekripsi byte yang dipilih dari teks cipher dalam sedikitnya 256 mencoba jika mereka mampu memaksa aplikasi korban berulang kali mengirim data yang sama lebih dari yang baru dibuat SSL 3.0 koneksi.
  - Selama klien dan layanan baik dukungan SSLv3, sambungan dapat 'digulung kembali' ke SSLv3, bahkan jika TLSv1 atau lebih baru didukung oleh klien dan layanan.
  - TLS menggantikan SCSV mekanisme mencegah 'versi rollback' serangan tanpa mempengaruhi klien warisan; Namun, hal itu hanya bisa melindungi koneksi ketika klien dan layanan mendukung mekanisme. Situs yang tidak dapat menonaktifkanSSLv3 segera harus mengaktifkan mekanisme ini.
  - Ini adalah kerentanan dalam spesifikasi SSLv3, tidak dalam implementasi SSL tertentu. Menonaktifkan SSLv3 adalah satu-satunya cara untuk benar-benar mengurangi kerentanan.

  Solusi
  Nonaktifkan SSLv3.
  - Layanan yang harus mendukung SSLv3 harus mengaktifkan mekanisme TLS penggantian SCSV sampai SSLv3 dapat dinonaktifkan.

- DNS Server Zona Informasi transfer Pengungkapan (AXFR)
  Deskripsi
  Nama server jauh memungkinkan transfer zona DNS yang akan dilakukan.
  - Sebuah transfer zona memungkinkan penyerang remote langsung mengisi daftar target potensial. Selain itu, perusahaan sering menggunakan konvensi penamaan yang dapat memberikan petunjuk untuk sebuah server aplikasi utama (misalnya, proxy.example.com, payroll.example.com, b2b.example.com, dll).
  - Dengan demikian, informasi ini adalah penggunaan besar untuk seorang penyerang, yang mungkin menggunakannya untuk memperoleh informasi tentang topologi jaringan dan tempat target baru.

  Solusi
  Membatasi transfer zona DNS hanya server yang membutuhkan informasi.

II. CVE Mapping



Gambar 7 CVE Mapping www.palembang.go.id

Pada **Gambar 7** merupakan CVE mapping yang ada pada situs www.palembang.go.id. Pada CVE tersebut terdapat tipe serangan yang ada pada web tersebut. Serangan itu adalaah Denial Of Service, SQL Injection, Bypass, Buffer Overflow, Code yang tereksekusi, dan serangan yang tidak ada vulnerabilitynya yang menuju SSL, PHP.cgi dan DNS server melalui kriptografi.

II. KESIMPULAN & SARAN

A. Kesimpulan

Pada analisa dan hasil tersebut dapat kita simpulkan bahwa:

- Target tersebut memiliki 7 port.
- Target tersebut menggunakan OS Linux 2.6.x
- Target tersebut memiliki rDNS
- Kelemahan target tersebut terdapat kurang updatenya webserver, dan cgi
- Adanya web log
- Adanya string tertentu yang tidak di ketahui oleh pengguna webserver tersebut

B. Saran

- Lakukan Upgrade webserver dan CGI
- Nonaktifkan SSLv3 dan menggantikan dengan TLS
- Batasi zona transfer DNS server

Referensi

- **cvedetails.com**
- **id.wikipedia.org**
- **nmap.org**
- **tenable.com**