UNIVERSITAS AMIKOM YOGYAKARTA

LAPORAN
FINAL PROJECT

SISTEM ADMINISTRATOR & LAYANAN JARINGAN

DNS SECURITY (DNSEC)

Nama Kelompok :

- Vicky Geral Dino (17.83.0111)
- Nurhalis Jusman (17.83.0079)
- Garda Pramudya (17.83.0078)

Kelas : 17-S1TK-02

A. TUJUAN

1. Mengamankan DNS Server
2. Protecting Data
3. Mengetahui Cara Menggunakan DNSec

B. PERALATAN

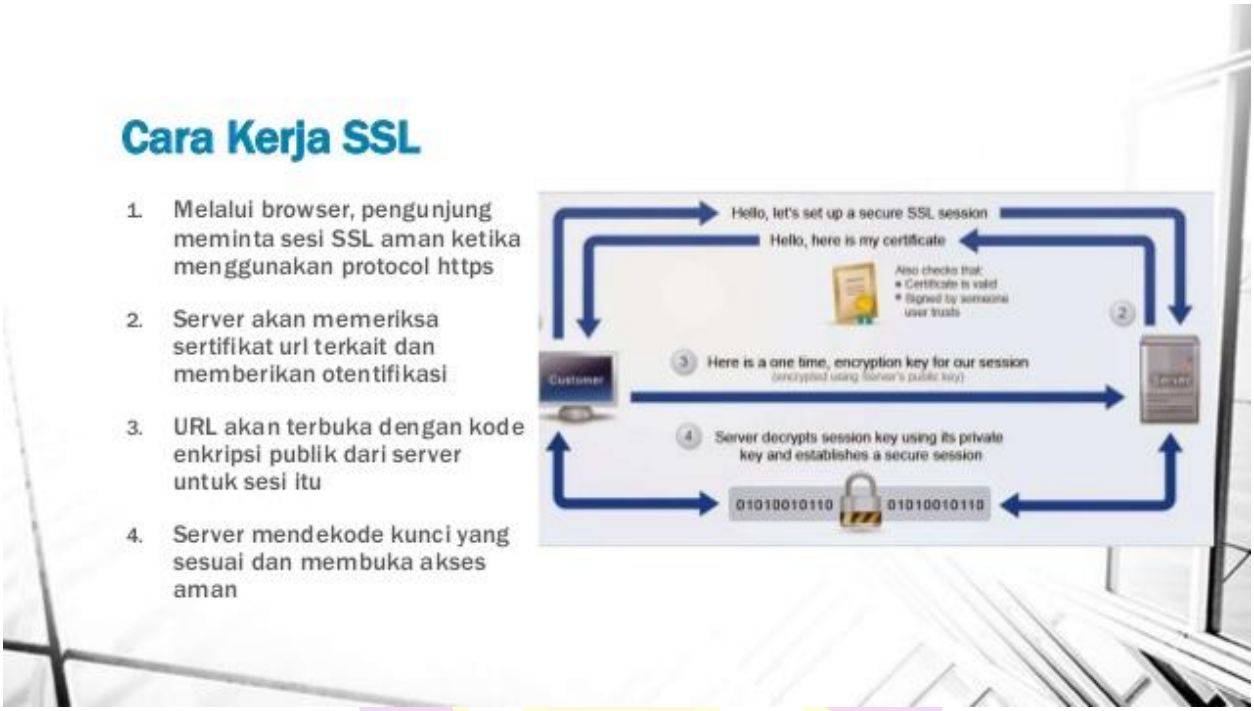
1. PC / Laptop
2. DNS Server
3. LAMP
4. SSL
5. Python
6. C++/GCC
7. Internet

C. TEORI SINGKAT

Seperti banyak protokol internet, sistem DNS tidak dirancang dengan keamanan dalam pikiran dan mengandung beberapa keterbatasan desain. Keterbatasan ini, dikombinasikan dengan kemajuan teknologi, telah mempermudah penyerang untuk membajak pencarian DNS untuk tujuan jahat, seperti mengirim pengguna ke situs web palsu yang dapat menyebarkan malware atau mengumpulkan informasi pribadi. Ekstensi Keamanan DNS (DNSec) adalah protokol keamanan yang dibuat untuk mengurangi masalah ini. DNSEC melindungi terhadap serangan dengan menandatangani data secara digital untuk membantu memastikan keabsahannya. Untuk memastikan pencarian yang aman, penandatanganan harus dilakukan di setiap tingkat dalam proses pencarian DNS.

Meskipun keamanan yang ditingkatkan selalu lebih disukai, DNSec dirancang agar kompatibel ke belakang untuk memastikan bahwa pencarian DNS tradisional masih diselesaikan dengan benar, meskipun tanpa keamanan tambahan. DNSec dimaksudkan untuk bekerja dengan tindakan keamanan lainnya seperti SSL / TLS sebagai bagian dari strategi keamanan Internet holistik.

Cara Kerja SSL/TLS:



TUJUAN

Proses pembuatan project yang bertujuan untuk sekuriti (security) pada DNS dengan cara memanipulasi sertifikasi awal dengan mengubah length bit dan menutup akses SSL pada zone DNS serta mengandakan kunci palsu pada sertifikat dengan length sesuai kebutuhan

KONFIGURASI

Download Source kode DNSec di https://github.com/GenoiSec/DNSec

1. openssl genrsa 1024 > privkey.pem
2. openssl rsa -pubout -in privkey.pem > pubkey.pem
3. python ./gentlsa.py pubkey.pem
4. Result Show -> _443._tcp.EXAMPLE.COM. 60 IN TYPE52 \# 35 020461757468303e3039060a2b06010401d67902
   (Taruh ini di zona DNS Anda, tetapi jangan lupa untuk mengubah "EXAMPLE.COM." Agar cocok dengan nama domain yang sebenarnya. Setelah ini selesai, dan catatan bersifat publik, Anda dapat melakukan langkah berikutnya. Anda dapat memeriksa rekam dengan dig -t type52 example.com.)
5. python ./chain.py example.com chain
6. (Jangan lupa untuk mengubah example.com ke nama domain yang sebenarnya di server Anda.)
7. gcc -o gencert gencert.c -Wall -lcrypto
8. ./gencert privkey.pem chain > cert.pem
9. openssl x509 -text < cert.pem | less

CARA KERJA

1. Cara kerja DNSec sendiri adalah memanipulasi data utama DNS serta SSL yang memiliki lenght bit awal ke lenght bit berikutnya sesuai kebutuhan. lenght bit sendiri terdiri dari length default 1024 atau 2048 yang mana selanjutnya menggunakan length sesuai kebutuhan.
2. Pada "Zone DNS" akses DNSec memanipulasi akses ke Sertifikasi HTTPS dengan lenght yang telah dirubah tadi.

3. --ATTACK & DEFENSE
4. Dari ini adanya Primary Data dan Foreign Data. mengamankan keseluruhan data Primary dan tetap mengamankan Foreign Data jika ada penyerangan harus melewati Foreign Data terlebih dahulu.
5. Jika adanya penyerangan langsung mengincar primary data, maka akses akan mengalihkanya ke foreign data, yang mana di primary terdapat Log atas Ilegal Administration access.

Skenario jika terjadi penyerangan