BAB 8 – NIDS (Network Intrusion Detection System) Snort

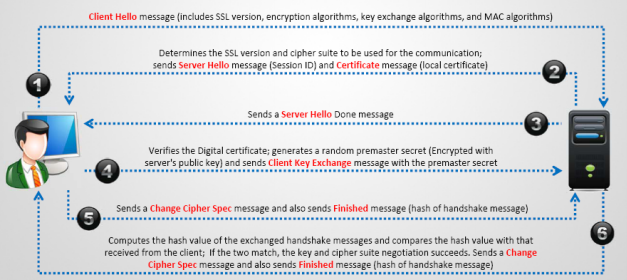
* Intrusion detection adalah aktivitas untuk mendeteksi penyusupan(intrusi) secara cepat dengan menggunakan program khusus yang otomatis. Program yang digunakan disebut dengan Intrusion Detection System
* Tipe Dari IDS antara lain,
  + Rule-based System, adalah berdasarkan atas database dari tanda2 intrusi atau serangan yang telah dikenal (didefinisikan sebelumnya). Jika IDS mencatat traffic yang sesuai dengan database yang ada, maka akan langsung dikategorikan sebagai intrusi
  + Adaptive System, menggunaan metode yang lebih canggih, tidak hanya berdasarkan database yang ada namun juga membuka kemungkinan untuk mendeteksi bentuk intrusi yang baru
* Bentuk yang secara umum digunakan adalah **rule-based system**
* **Rule-based System,** memiliki dua pendekatan, yaitu
  + Pencegahan (preemptory), pada pendekatan ini, program IDS akan memperhatikan semua traffic yang ada. Jika ditemukan paket yang mencurigakan, maka program akan melakukan suatu tindakan
  + Reaksi (reactionary), pada pendekatan ini, program IDS hanya mengamati file log yang telah dibuat. Jika ditemukan paket yang mencurigakan, maka program akan segera melakukan tindakan
* **Snort**, merupakan rule-based IDS opensource yang berbasis komunitas, sehingga rule-rule yang ada adalah rule yang dibuat dan dikembangkan oleh komunitas. Snort memiliki tiga buah mode yang dapat dijalankan, yaitu
  + **Sniffer mode,** untuk melihat paket yang lewat di jaringan
    - Untuk menjalankannya dapat menggunakan perintah
      * #snort [-v] [-vd] [-vde] [-v –d –e]
    - Operator –v, -d, dan –e, memiliki keluaran yang berbeda
      * -v, untuk melihat header TCP/IP paket yang lewat
      * -d, untuk melihat isi paket
      * -e, untuk melihat header link layer paket serperti header ethernet
  + **Packet logger mode**, untuk mencatat semua paket yang lewat di jaringan untuk dianalisa di kemudian hari
    - Mode ini dapat membantu jika paket yang dicatat berjumlah besar, sehingga dengna mode ini, paket tersebut dapat disimpan ke sebuah file tersendiri. Beberapa perintah yang dapat digunakan adalah
      * #snort [–dev –l ./log] [-dev –l ./log –h 192.168.0.0/24] [-dev –l ./log –b]
        + Opsi –l ./log mendefinisikan dimana log paket akan disimpan
        + Opsi –h 192.168.0.0/24 menunjukan hanya paket dari host mana yang akan disimpan
        + Opsi –b memberitahukan agar file log berformat binary, bukan ASCII
      * Untuk membaca file log dapat dilakukan dengan menjalankan snort dan ditambahkan opsi –r [nama file log]
  + **Intrusion Detection mode,** pada mode ini, snort berfungsi untuk mendeteksi serangan yang dilakukan. Untuk menggunakan mode IDS diperlukan untuk melakukan setup rules yang dapat membedakan antara paket normal dengan paket yang merupakan serangan
    - Ciri dari penggunaan mode ini iadalah dengan menambahkan perintah ke snort untuk membaca file konfigurasi. File konfigurasi ini berisi rule-set yang telah atau baru dibuat. Perintahnya adalah
      * #snort –dev –l ./log –h 192.168.0.0/24 –c snort.conf
    - Untuk melakukan mode IDS, secara prinsipnya harus melakukan mode logging paket, lalu hasil log file yang ada dapat dianalisa.
    - Ada beberapa tambahan perintah yang akan membuat proses deteksi menjadi lebih efisien, yaitu dengan menggunakan mekanisme alert di Linux dengan perintah –A
      * -A fast, model alert yang berisi waktu, berita, IP dan port tujuan
      * -A full, mode alert dengan informasi lengkap
      * -A unsock, mode alert ke unix socket
      * -A nonde, mematikan mode alert
    - Untuk mengirimkan alert ke syslog UNIX kita bisa menambahkan switch –s, seperti berikut
      * #snort –c snort.conf –l ./log –s –h 192.168.0.0/24
    - Untuk mengirimkan alert binary ke workstation windows, dapat digunakan perintah di bawah ini
      * #snort –c snort.conf –b –M WORKSTATIONS
    - Agar Snort beroperasi secara langsung setiap kali workstation/server booting, dapat ditambahkan baris di bawa ini pada file **/etc/rc.d/rc.local**
      * /usr/local/bin/snort –d –c /root/snort/snort.conf –A full –s –D
      * -D adalah opsi untuk set snort beekrja sebagai daemon
  + Membuat basic rule snort
    - [aksi] [protocol] [source ip] [source port] -> [destination ip] [destination port] (msg : “blablabla”; sid:1000001; rev:1; classtype:[kategori egent])
    - Alert icmp any any -> any any (msg:”ICMP test”; sid:1000001; rev:1; classtype:icmp-event;)
  + Ada beberapa aplikasi yang digunakan untuk membaca data log snort, yaitu snorby, dan acidbase

BAB 9 – Computer Virus, Malware, Ransomware (Wannacry)

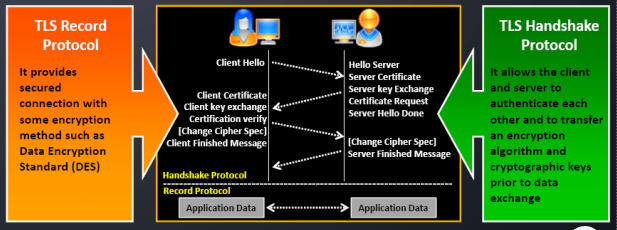
* Malware merupakan set instruksi yang berjalan di komputer dan membuat sistem komputer melakukan apa yang diinginkan attacker
* Tujuannya adalah untuk mencuri informasi, menghapus file, click fraud (klik tipu-tipu), mencuri serial number, menjadikan komputer sebagai relay
* Malware memiliki jenis yang bermacam-macam
  + Virus, program yang dapat menginfeksi program lain dengan cara memodifikasinya agar program tersebut memiliki sebagian atau keseluruhan fungsionalitas virus, beberapa tipe virus,
    - Polymorphic, menggunakan polymorphic engine untuk mengubah dirinya, namun algoritmanya bersifat tetap
    - Metamorfic, akan mengubah keseluruhan bentuk virus setelah melakukan infeksi
  + Backdoor
  + Trojan, merupakan malware yang tampil dan memiliki fungsionalitas yang sesuai dengan yang diharapkan, namun terdapat fungsi tersembunyi yang memungkinkan unauthorized access ke komputer tersebut
  + Rootkit, rootkit merupakan komponen yang bersifat stealth(sembunyi2) untuk me-maintain access attacker ke komputer korban
  + Scareware
  + Adware
  + Worm, merupakan program komputer yang dapat menggandakan dirinya sendiri melalui jaringan tanpa harus menggunakan bantuan dari user
* Metode penyebaran malware bermacam macam, yang paling banyak adalah dengan cara menginfeksi, berikut adalah komponen komputer yang dapat diinfeksi oleh virus
  + Executable (.exe)
    - Overwiriting, sepenuhnya melakukan overwrite pada executable target
    - Prepending, menginfeksi dengan cara menempelkan dirinya ke bagian awal dari executable
    - Appending, menginfeksi dengan cara menambahkan dirinya ke bagian akhir executable
    - Cavity, menginfeksi dengan cara menyisipkan dirinya di bagian tengah executable
    - Multi-cavity, menginfeksi dengan cara memecah dirinya lalu menyisipkan pecahan tersebut pada random bagian suatu executable
  + Interpreted file (.dll), akan menyisipkan program malware ke suatu packer, sehingga suatu payload akan dipack bersamaan dengan malware
  + Kernel, dengan melakukan subverting pada kernel, tekniknya antara lain
    - Kernel patch
    - Loadable kernel module
    - Kernel memory patching
  + Service
  + MBR, disebut juga bootkit, menginfeksi bootkit akan menjadikan suatu malware menjadi tidak terdeteksi karena bootkit dapat digunakan untuk menghindari proteksi suatu OS. Bootkit merupakan bagian dari OS ketika OS melakukan boot, dan karena OS dikategorikan sebagai system yang trusted pada saat boot loader muncul
  + Hypervisor
* Malware dapat menyebar melalui
  + Email
  + Codec
  + Fake antivirus
  + Fake page
  + P2P file
* Contoh malware
  + Adware
  + Backorifice
  + Netbus
  + Browser toolbar
  + Ransomware
* Wanna Cry Ransomware
  + Merupakan ransomware yang melakukan enkripsi file lalu meminta dana tebusan agar file tersebut di dekripsi
  + Wannacry menyebar menggunakan EternalBlue, sebuah exploit dari windows SMB protocol.
  + Cara kerjanya adalah sebagai berikut
    - Mencari file lalu mengenkripsinya
    - Lalu menampilkan “ransom note” yang menginformasikan user agar membayar sejumlah bitcoin ke address tertentu
    - Lalu menyebarkan dirinya melalui jaringan yang ada
    - Kode transport nya akan melakukan scan ke sistem yang memiliki celah, lalu menggunakan EternalBlue exploit untuk mendapatkan akses
    - Lalu menggunakan tool DoublePulsar untuk menginstall dan mengeksekusi salinannya
  + Kill switch, tak lama setelah serangan global dari virus wanna cry, ada seseorang yang menemukan “kill switch” untuk wannacry. Kill switch tersebut dibuat dengan cara mendaftarkan URL domain yang ada pada source code program.
    - Software wanacry memiliki URL yang digunakan oleh attacker sebagai mekanisme untuk mencegah software berjalan di mesin yang quarantided oleh anti-virus
    - Software akan berusaha untuk mengontak URL tersebut untuk mendeteksi apakah software tersebut berjalan di evironment sandbox ataukah tidak.
  + EternalBlue merupakan *network infection vector*, yang di rilis oleh hacker group bernama The Shadow Brokers.
    - EternalBlue memanfaatkan celah keamanan protokol SMB milik microsoft. EternalBlue digunakan oleh wanna cry untuk menyebarkan dirinya melalui jaringan komputer
  + Proses eksekusi virus ini dapat dibagi menjadi tiga tahap, yaitu
    - Program utama (main program) menggunakan exploit (EternalBlue) untuk menyebarkan dirinya sendiri, lalu program ransom “WannaCry” dijalankan
    - Program “WannaCry” akan mengenkripsi file yang ada
      * Sample yang ada menunjukan adanya RSA public-key, dan menunjukan bahwa attacker memiliki decrypted RSA private-key
      * Sebelum mengenkripsi file, **CryptoAPI** akan men-generate pair of RSA key (sub-public key, dan sub-private key).
      * Lalu sample akan mengenkripsi sub-private key dengan RSA public key dan menyimpannya dengan nama “0000000000.eky” lalu sub-public key disimpan sebagai “0000000000.pky”
      * Sample mengenerate AES key untuk mengenkripsi file, file yang telah dienkripsi disebut **M2,** kemudian AES key akan dienkripsi menggunakan sub-public key “0000000000.pky”, AES key yang dienkripsi disebut **M1,** lalu M1 dan M2 digabung lalu ditambahkan header “WANACRY!” untuk menyimpan file yang telah dienkripsi
      * Setiap encrypted-file, dienkripsi menggunakan AES key yang berbeda beda. Jika ingin mendekripsi file, perlu diketahui RSA-sub-private key terlebih dahulu, setelah itu mendekripsi AES key-nya, lalu menggunakan AES key untuk mendekripsi file. Jika tidak ada RSA sub-private key maka file tidak dapat didekripsi
    - Ransom inteface (@ WanaDecryptor @.exe) menampilkan informasi dan sample decrypt
      * Interface tersebut akan menampilkan wallet address bitcoin dan menampilkan pesan untuk dekripsi file. Jika ingin mendekripsi seluruh file, maka harus membayar sejumlah bitcoin

BAB 10 – Enkripsi (kriptografi)

* Kriptografi adalah konversi data menjadi kode acak yang dapat di decrypt dan dikirimkan melalui private atau public network
* Kriptografi digunakan untuk melindungi pesan email, informasi kartu kredit dan corporate data
* Tujuan dari kriptografi
  + Confidentiality
  + Integrity
  + Authentication
  + Non-repudiation
* Tipe kriptografi
  + Symmetric encryption (secret key, shared key, private key)
    - Menggunakan key yang sama untuk enkripsi dan dekripsi
  + Asymmetric encryption (public key)
    - Menggunakan key yang berbeda untuk enkripsi dan dekripsinya. Dikenal sebagai public dan private keys
  + Hash function
    - Tidak menggunakan key untuk dekripsi, melainkan menggunakan algoritma hash untuk melakukan enkripsi satu arah
    - Tidak dapat di dekripsi
* Cipher
  + Classical Cipher
    - Substitution cipher, me-replace bit, char, block of char, dengan bit, char atau block lain
    - Transposition cipher, huruf pada plaintext dilakukan operasi shift untuk membuat cryptogram
  + Modern Cipher
    - Based on type of key
      * Private key, key yang sama digunakan untuk enkripsi dan dekripsi
      * Public Key, dua key yang berbeda digunakan untuk enkripsi dan dekripsi
    - Based on type of input data
      * Block Cipher, enkripsi data secara blok sekaligus
      * Stream Cipher, enkripsi data secara stream
* Contoh contoh enkripsi
  + AES (Advance Encryption Standard)
    - Merupakan symmetric-key encryption
    - Merupakan block chipher
  + DES (Data Encryption Standard)
    - Merupakan symmetric encryption yang didesain untuk hardware
  + RC4, RC5 & RC6
    - Merupakan stream cipher
  + DSA (Digital signature algorithm)
  + RSA (Rivest Shamir Adleman)
    - Merupakan internet encryption and authentication system
    - Menggunakan aritmatika modular dan elementary number theories untuk melakukan komputasi menggunakan dua bilangan prima yang besar
  + MD5
    - Merupakan hash function cipher
  + SHA (Secure Hasing Algorithm)
    - Merupakan algoritma untuk men-generate one-way hash cryptography
* Public Key Infrastructure (PKI)
  + Merupakan kumpulan hardware, software, seorangan, kebijakan dan prosedur untuk membuat, memanage, mendistribusikan, menggunakan, menyimpan dan mencabut digital certificates
  + Komponennya antara lain
    - Certificate management system, untuk generate, distribusi, penyimpanan dan verfikasi certificate
    - Satu atau lebih direktori dimana certificate disimpan
    - Certificate Authority (CA) yang mengeluarkan dan memverifikasi digital certificates
    - Registration Authority (RA) yang bertindak sebagai pelaku verifikasi certificate authority
  + Langkah kerja
    - (1) User meminta untuk pembuatan certificate dan public key ke Registration Authority (RA)
    - (2) RA melakukan verifikasi terhadap applicant, setelah diverifikasi, RA akan melakukan request untuk pengadaan certificate ke Certification Authority (CA)
    - (3) CA akan mengisukan public key certificate ke user
    - (4) CA melakukan update informasi ke Validation Authority (VA) terkait certificate yang telah dibuat tadi
    - (5) User menggunakan public key certificate yang sudah signed dengan ditigal signature ke sebuah situs marketplace
    - (6) Situs marketplace tersebut akan memvalidasi public key certificate milik user ke VA
    - (7) VA akan mengirimkan hasil dari validasi certificate tersebut (valid atau tidak)
* SSL



* TLS



BAB 11 – Securing Web & SSL/TLS

* File .htaccess merupakan file yang dapat digunakan untuk melakukan overriding konfigurasi default dari sebuah web server
  + File .htaccess berupa file ascii yang ditempatkan pada direktori hosting.
  + Akses file yang harus di setting adalah 644.
  + Fungsinya adalah memungkinkan server untuk mengakses file, namun mencegah pengunjung untuk mengakses file lewat browser dengan alasan keamanan
  + Fitur .htaccess
    - Memberikan pesan error, jika ingin melakukan overriding pesan error dari server, file .htaccess dapat digunakan, berikut adalah contoh konfigurasinya



* + - Overiding setting SSI, hanya halaman web yang memiliki ekstensi .shtml yang dapat melakukan SSI, namun dengan .htaccess hal ini dapat dioverride agar SSI bekerja dengan file .html ataupun .htm, contoh konfigurasinya



* + - Mengganti file index.\* pada homepage
    - Memungkinkan broswing direktori, untuk mengijinkan pengaksesan
    - browsing direktori web dapat dikonfigurasikan seperti berikut



* + - Blocking user untuk mengakses website, jika ingin mencegah website diakses oleh user tertentu, .htaccess dapat dikonfigurasikan seperti berikut

<Limit GET>

order deny,allow

deny from 10.252.44.210

deny from 10.252.32.

deny from .domainku.com

allow from all

</Limit>

* + - Redireksi ke halaman web atau direktori tertentu, dengan cara



Atau



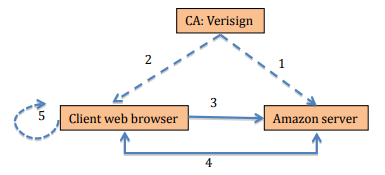
* + - Terdapat beberapa tipe redireksi yaitu
      * Permanent – halaman web dipindahkan secara permanen (status : 301)
      * Temp – halaman web dipindah secara temporer (status : 302)
      * Seeother – halamawn web diganti (status : 303)
      * Gone – halaman web telah dihapus permanen (status : 410)
    - Mencegah hot linking dan bandwith leeching, dilakukan untuk mencegah hot linking atau mencuri bandwith dengan cara melink-kan image file yang dimiliki oleh suatu web server dengan web server lain secara ilegal. Hal ini dapat diblok dengan .htacces dengan cara



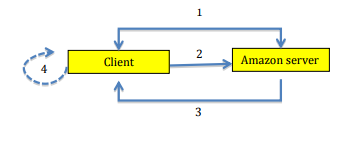
* + - Mencegah pengunjung melihat file .htaccess atau file lain, untuk mencegahnya dapat dilakukan dengan cara



* SSL/TLS
  + TLS (Transport Layer Security) merupakan protocol untuk mengamankan komunikasi antar aplikasi melalui internet. TLS mengamankan konten pada layer aplikasi.
  + Untuk menjamin keamanan, data yang dikirim dienkripsi dan diotentifikasi pada sisi server dan client.
  + SSL adalah protocol yang diciptakan sebelum TLS.
  + SSL/TLS biasanya dioperasikan secara bersama-sama dengan HTTP, sehingga membentuk protocol baru yang disebut HTTPS.
* HTTPS
  + HTTPS menggabungkan protocol HTTP dan SSL/TLS untuk menjamin keamanan komunikasi antara web server dan web browser.
  + HTTPS beroperasi pada port 443
  + HTTPS bekerja dengan menyediakan enkripsi untuk konten web dan otentikasi web server
  + HTTPS tidak melakukan otentikasi client sehingga website tidak dapat melakukan otentikasi user selama koneksi
  + Komunikasi SSL/TLS meliputi dua tahap, yaitu handhaksing dan data sending.
    - Sebelum berkomunikasi, website harus meminta *certificate authority* (CA) agar dapat digunakan untuk menandatangani (signing) digital certificate-nya yang berisi public key dari site.
    - User yang menerima digital sertificate CA, segera memanggil sertifikat root yang sudah dimiliki ketika menginstall web browser
  + Jalannya SSL/TLS adalah sebagai berikut
    - (1) Verisign menandatangani sertifikat amazon dengan public key-nya
    - (2) Install CA sertifikat dengan public key-nya pada browser client
    - (3) Koneksi lewat https
    - (4) Saling bertikat digital sertificate, termasuk public key
    - (5) Client melakukan verifikasi sertifikat amazon menggunakan public key dari CA



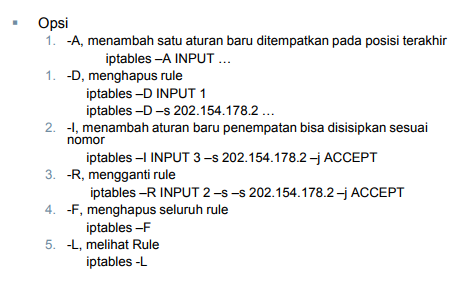
* + - Pada gambar tersebut, ketika user hendak mengkoneksikan diri dengan website melalui koneksi https, web server mengirimkan sertifikatnya yang mengandung public key dari web site tersebut. User akan memverifikasi sertifika ini dengan nmemakai pre-installed sertifikat root dari website CA
  + Tahap kedua dari SSL/TLS adalah tahapan enkripsi antara server dan client berdasarkan protocol kriptografi yang dinegosiasikan antara kedua belah pihak



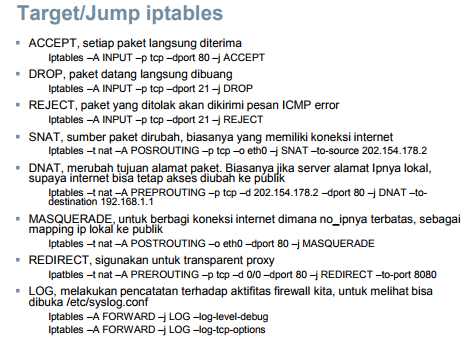
* + - Pada gambar tersebut, ketika sertifikat digital milik server berhasil diverifikasi, maka browser dan server mulai saling bernegosiasi cipher (metode enkripsi) yang digunakan untuk pengkodean data dan verifikasi digital signature. Jika public key enkripsi sudah dipilih, kedua belah pihak mengenkripsikan data dengan public key masing-masing dan mendrkripsi dengan private keynya
    - (1) mengasosiasikan cipher (metode kriptografinya)
    - (2) mengirim data yang telah terenkripsi dengan Amazon public key
    - (3) mengirim data yang telah terenkripsi dengan client public key
    - (4) Dekripsi/decoding data dari Amazon dengan public key client

BAB 12 – Firewall

* SYNTAX



* IPTABLES



* Parameter

