PERTEMUAN 12
MAIL SERVER SECURITY

A. TUJUAN PEMBELAJARAN

Pada Pertemuan ini akan dijelaskan mengenai *Mail Server Security*. Setelah mempelajari materi ini mahasiswa diharapkan mampu untuk:

1. Memahami mail server security
2. Memproteksi mail server security
3. Mendeteksi aktvitas berbahaya pada mail server security

B. URAIAN MATERI

1. Memahami Cara Kerja Mail Server

Email elektronik adalah salah satu aplikasi Internet yang paling banyak digunakan. Memang, kemampuan untuk mengirim pesan dan file ke kelompok atau individu tertentu melalui Internet adalah alat yang ampuh sehingga telah mengubah cara orang berkomunikasi secara umum.

Sistem email saat ini menggunakan beberapa protokol untuk mengirimkan pesan. Untuk menangani pengiriman pesan dari mesin klien ke server email penerima, *Simple Mail Transfer Protocol (SMTP)* digunakan. SMTP adalah protokol lapisan aplikasi berbasis teks sederhana yang menggunakan TCP untuk memfasilitasi "percakapan" antara klien yang ingin mengirim email dan server penerima yang sesuai. Dalam model SMTP, klien disebut sebagai *Mail User Agent (MUA)*. MUA mengirimkan pesan SMTP ke *Mail Sending Agent (MSA)*, yang kemudian mengirimkan pesan ke *Mail Transfer Agent (MTA)* yang bertanggung jawab untuk mengirimkan pesan ke pihak penerima. MSA dan MTA sering kali berada di server fisik yang sama. Pesan dikirim dari MTA pengirim ke MTA penerima, di mana pesan tersebut dikirimkan ke *Mail Delivery Agent (MDA)* yang bertanggung jawab untuk memastikan pesan mencapai MUA penerima.

Klien memulai percakapan SMTP melalui Port 25 dengan MSA, seperti percakapan yang dikelola oleh ISP pengguna. Setelah membuat koneksi TCP dan menerima spanduk server, klien mengidentifikasi dirinya sendiri dengan perintah HELO. Setelah menerima pengakuan dari server, klien mengidentifikasi

pengirim pesan dengan bidang MAIL FROM. Selanjutnya, klien menentukan penerima menggunakan bidang RCPT TO. Terakhir, klien memberikan pesan dan lampiran apa pun di bagian DATA, setelah itu pesan dikirim dan klien mengakhiri koneksi dengan perintah QUIT. Contoh percakapan SMTP mungkin muncul sebagai berikut, di mana klien diberi notasi sebagai "C" dan server sebagai "S":

S: 220 mail.example.com ESMTP Postfix

C: HELO relay.example.com

S: 250 mail.example.com Halo relay.example.com, senang bertemu dengan Anda

C: MAIL FROM:<joe@example.com>

S: 250 <joe@example.com> pengirim ok

C: RCPT TO:<alice@othersite.com>

S: 250 <alice@othersite.com> penerima ok

C: DATA

S: 354 masukan mail, diakhiri "." di baris selanjutnya

C: Dari: "Joe Smith" <joe@example.com>

C: Kepada: "Alice" <alice@othersite.com>

C: Subject: Contoh percakapan SMTP

C: Ini adalah contoh percakapan SMTP. Harap Anda menyukainya.

C: .

S: 250 Mail diterima untuk pengiriman

C: QUIT

S: 221 mail.example.com menutup koneksi

Selanjutnya, MSA mengirimkan pesan ini ke MTA, yang kemudian menanyakan sistem nama domain (DNS) untuk menyelesaikan alamat IP dari MTA penerima. Misalnya, penerima tertentu, MTA pengirim akan mendapatkan alamat IP untuk MTA domain. MTA pengirim kemudian meneruskan pesan ke MTA penerima dengan percakapan yang sama seperti di atas, dan MTA mentransfer pesan ke MDA.

Protokol SMTP menangani pengiriman email ke server yang dirancang untuk menangani antrian pesan, tetapi tidak digunakan untuk mengirim email ke klien. Sebagai gantinya, dua protokol lain yang paling banyak digunakan, Post Office Protocol (POP) dan *Internet Message Access Protocol (IMAP)*.

POP adalah yang lebih tua dari keduanya dan dirancang untuk mendukung klien dengan koneksi Internet dial-up. Dengan demikian, percakapan POP biasa melibatkan klien yang menyambung ke MDA mereka, mengunduh pesan baru apa pun, menghapus pesan tersebut dari server, dan memutuskan sambungan.

IMAP adalah protokol baru yang menyediakan operasi online dan offline. Dalam mode online, klien menyambung ke server email dan mempertahankan sambungan tetap yang memungkinkannya mengunduh pesan sesuai kebutuhan. IMAP juga memungkinkan klien untuk mencari pesan di server email berdasarkan beberapa kriteria, sebelum benar-benar mendownload pesan tersebut. Terakhir, sebagian besar sesi IMAP secara default membiarkan pesan email tetap utuh di server email daripada menghapusnya saat diunduh.

a. Melindungi privasi email

Teknik paling umum untuk melindungi privasi email adalah dengan mengenkripsi pengiriman pesan yang sebenarnya daripada isinya. Sebagian besar server email mendukung penggunaan SSL / TLS, protokol yang mengenkripsi lalu lintas TCP dengan aman. Protokol ini sering kali digunakan di setiap tingkat komunikasi antara klien dan server email lokal, antara server email lokal dan tujuan, dan antara server email tujuan dan penerima.

Mengandalkan hanya pada enkripsi lapisan transportasi melindungi pesan dari penyadapan dalam penerbangan, tetapi menyiratkan tingkat kepercayaan pada server email yang menangani pesan ini. Misalnya, karyawan ISP yang memiliki akses ke server email ISP tersebut mungkin dapat membaca konten dari semua pesan email yang disimpan di server tersebut.

b. Pretty Good Privacy (PGP)

Untuk memberikan tingkat kerahasiaan yang lebih kuat, yang melindungi pesan dari klien ke klien, konten sebenarnya dari pesan email harus dienkripsi. Ada beberapa pendekatan yang telah diusulkan untuk tujuan ini. Salah satu sistem yang terkenal adalah *Pretty Good Privacy (PGP)*, yang menggunakan kriptografi kunci publik untuk mengenkripsi dan / atau menandatangani pesan email secara digital. Saat mengirim pesan ke penerima yang dituju menggunakan PGP, pengirim mengenkripsi pesan menggunakan kunci publik penerima, sehingga hanya penerima yang dapat mendekripsi pesan menggunakan kunci pribadinya yang sesuai.

c. Otentikasi

Dua pendekatan utama yang saat ini digunakan untuk mengautentikasi asal pesan email meliputi:

1) *Authentication of the sending user*. Pendekatan ini memungkinkan server email penerima untuk mengidentifikasi penulis pesan email. Agar efektif, bagaimanapun, ini membutuhkan penyebaran yang luas dari pasangan kunci publik-pribadi untuk pengguna email. Untuk alasan ini, ini jarang digunakan dalam praktik.
2) *Authentication of the sending mail transfer agent*. Pendekatan ini biasanya mengidentifikasi organisasi penulis, tetapi bukan penulis individu. Ini lebih mudah untuk diterapkan daripada mengirim otentikasi pengguna dan memiliki adopsi yang berkembang.

Kerumitan muncul dengan semua jenis pesan email yang ditandatangani, tentu saja, karena bahkan modifikasi yang tidak penting saat dalam perjalanan, seperti perubahan enkode, akan menyebabkan verifikasi tanda tangan gagal. Karenanya, isi pesan email yang ditandatangani harus diformat sedemikian rupa sehingga mengurangi risiko modifikasi selama pengiriman. Proses pemformatan ini disebut *canonicalization*.

2. Memproteksi Mail Server Security

Email telah menjadi layanan penting untuk hampir setiap perusahaan. Sayangnya, sebagian besar email yang diterima adalah email yang tidak diminta

yang disebut *spam* atau email sampah, beberapa di antaranya dapat membawa malware dan dapat menyebabkan penipuan (*fraud)* atau penipuan (*scams*).

a. Kelola Spam

Untuk menjaga agar sistem Anda berjalan dengan lancar, penting bagi administrator jaringan untuk berusaha memblokir spam. Tempat terbaik untuk membuat sistem penyaringan antispam adalah di server atau alat khusus atau sebagai bagian dari perangkat atau layanan firewall. Semua email akan diarahkan ke filter antispam dengan mengubah data *DNS Mail Exchanger (MX)* Anda agar mengarah ke server atau perangkat antispam. Setiap email yang tidak dianggap spam akan diteruskan ke server email internal Anda.

Sistem pemfilteran spam tidak akan menangkap setiap pesan spam. Seperti paket antivirus, solusi pemfilteran spam harus selalu diperbarui dan perlu terus ditingkatkan. Selain itu, pertimbangkan untuk menambahkan alamat email, domain email, rentang alamat IP, atau kata kunci yang mengancam ke dalam daftar hitam. Setiap email yang terdaftar dalam daftar hitam akan secara otomatis diblokir. Pastikan untuk berhati-hati saat menggunakan daftar hitam, jadi kriteria untuk memblokir email tidak terlalu luas sehingga mulai memblokir email yang sah.

Banyak solusi antispam juga akan menggunakan *Real-time Blackhole Lists* (RBL) atau *DNS-based Blackhole List* (DNSBL), yang dapat diakses dengan bebas. RBL dan DNSBL adalah daftar pengirim spam yang dikenal yang sering diperbarui. Sebagian besar perangkat lunak server email dapat dikonfigurasi untuk menolak atau menandai pesan yang telah dikirim dari situs yang terdaftar pada satu atau lebih daftar tersebut. Tentu saja, saat pelaku spam mencari cara untuk menyiasatinya, ini hanyalah salah satu alat yang dapat membantu mengurangi jumlah spam yang masuk.

Setiap email yang diidentifikasi sebagai spam biasanya dikarantina atau disimpan sementara, jika email yang sah teridentifikasi sebagai spam. Meskipun jumlah ini seharusnya relatif rendah, latih personel pusat bantuan Anda dan mungkin pengguna Anda untuk mengakses email yang dikarantina untuk merilis email yang sah ke tujuannya. Selain itu, tambahkan alamat email atau domain pengirim ke daftar putih sehingga tidak akan teridentifikasi sebagai spam di masa mendatang.

Mendeteksi spam bisa menjadi tugas yang menakutkan jika harus dilakukan secara manual. Selain iklan dan kata kunci yang jelas, sistem antispam juga akan melihat header email untuk menganalisis informasi tentang email dan asalnya.

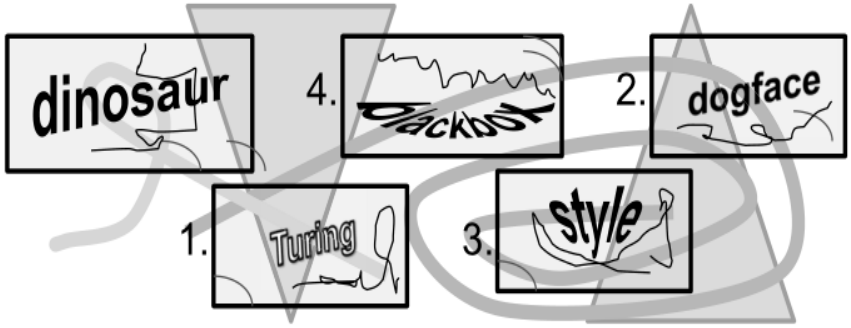
Terkadang, pelaku spam akan mencoba memalsukan alamat email atau alamat IP yang sah jika pesan tersebut benar-benar berasal dari alamat email atau alamat IP yang kemungkinan besar akan diidentifikasi sebagai spam. Salah satu cara untuk mendeteksinya adalah melalui pencarian terbalik.

Saat ini, paket antispam menggunakan algoritme khusus, seperti *Bayesian filters*, untuk menentukan apakah email dianggap sebagai spam. Algoritma ini biasanya menganalisis email yang diterima sebelumnya dan membuat database pada beberapa atribut berdasarkan email yang dianalisis sebelumnya. Saat menerima email, ia akan membandingkan email tersebut dengan atribut yang telah dikumpulkannya untuk menentukan apakah itu spam.

b. CAPTCHAs

Semakin populernya webmail telah memberikan strategi baru bagi para spammer. Pelaku *spam* dapat dengan mudah mendaftarkan akun dengan layanan email web gratis dan menggunakan akun tersebut untuk mengirim spam hingga penyedia email web mendeteksi aktivitas ini. Banyak pelaku spam telah mengotomatiskan proses ini dengan membuat program yang mendaftarkan akun email web, mengirim email sebanyak mungkin, dan mengulangi proses tersebut saat akun dibatalkan.

Untuk memerangi taktik pembuatan akun email otomatis, sebagian besar layanan email web mengharuskan pengguna menyelesaikan CAPTCHA (*Completely Automated Public Turing test to tell Computers and Humans Apart*). Tugas semacam itu adalah segala sesuatu yang mudah diselesaikan oleh manusia tetapi sulit diselesaikan secara terprogram oleh komputer. Kebanyakan CAPTCHA adalah masalah pengenalan gambar, di mana gambar terdistorsi yang berisi garis teks disajikan, dan pengguna harus menafsirkan teks yang disematkan.



Gambar 17. CAPTHA

Sayangnya, beberapa pelaku spam menghindari CAPTCHA ini menggunakan situs web yang mengharuskan pengunjung memecahkan CAPTCHA untuk mendapatkan akses. Tanpa sepengetahuan pengunjung, CAPTCHA ini sebenarnya disalin dari halaman registrasi webmail. Solusi yang diberikan pengguna kemudian diteruskan ke robot spam otomatis untuk mendaftarkan akun email web untuk mengirim spam. Selain itu, beberapa pelaku spam bahkan mempekerjakan pekerja bergaji rendah dari negara berkembang untuk menyelesaikan CAPTCHA bagi mereka. Bagaimanapun, dalam kedua kasus, penggunaan CAPTCHA meningkatkan biaya operasional pengirim spam; karenanya, teknik-teknik ini memiliki efek positif.

c. Spam dan Malware

Seringkali, komputer yang terinfeksi malware digunakan untuk mengirim spam, yang memungkinkan peretas mengubah mesin korbannya menjadi alat untuk menghasilkan uang. Faktanya, diperkirakan lebih dari 80% dari semua spam berasal dari botnet, yang merupakan jaringan komputer yang disusupi yang dikendalikan oleh satu penyerang Keamanan Aplikasi Terdistribusi. Bahkan ketika botnet tidak terlibat, banyak virus mengubah host mereka menjadi robot spam yang menghasilkan jutaan email setiap hari. Virus lain mengubah host mereka menjadi proxy terbuka yang digunakan pelaku spam untuk membuat email mereka anonim. Email spam semacam itu tentu saja lebih sulit dideteksi karena berasal dari bot yang meniru pengguna yang sah.

d. Email Spoofing

Spoofing email adalah pembuatan header email palsu di mana penyerang menipu penerima agar mengira bahwa email tersebut berasal dari sumber tepercaya. Penyerang mengubah bagian email agar terlihat seolah-olah ditulis oleh orang lain. Karena protokol email tidak memiliki metode autentikasi internal, biasanya email *spam* dan phishing digunakan untuk mencoba mengelabui penerima agar mempercayai asal pesan.

Tujuan akhir dari *spoofing* email adalah membuat penerima terbuka dan berpotensi menanggapi permintaan. Bahkan mungkin mengeklik tautan ke situs web palsu yang dimaksudkan untuk mengumpulkan informasi pribadi (proses yang dikenal sebagai *phishing*).

Alasan penyerang mengubah informasi email adalah untuk membuat orang memercayai mereka. Email biasanya tidak aman dan rentan terhadap berbagai teknik *spoofing* alamat. Pastikan untuk tidak pernah mengungkapkan informasi pribadi atau keuangan Anda dalam email. Jangan pernah menanggapi permintaan email yang meminta informasi sensitif dan berhati-hatilah saat memberikan informasi setelah mengikuti tautan web yang disematkan di email.

Metode yang populer adalah memasukkan tautan survei dalam email yang mungkin menawarkan hadiah dan kemudian mengajukan pertanyaan. Beberapa pertanyaan mungkin terkait dengan lingkungan komputasi mereka seperti, "Berapa banyak firewall yang Anda miliki?" atau "Vendor firewall apa yang Anda gunakan?" Kadang-kadang karyawan sangat terbiasa melihat jenis survei email ini di kotak masuk mereka sehingga mereka hampir tidak berpikir dua kali untuk menanggapinya.

e. Relaying Email

Salah satu protokol email utama adalah SMTP. Simple Mail Transfer Protocol (SMTP) digunakan untuk mentransfer email dari satu server ke server lain, dan bertanggung jawab untuk pengangkutan email keluar. SMTP menggunakan port TCP 25.

Server email tidak hanya digunakan oleh pengguna kita untuk mengirim dan mengambil email: mereka juga digunakan untuk menyampaikan email. Misalnya, server web dan aplikasi mungkin merelay email melalui server email

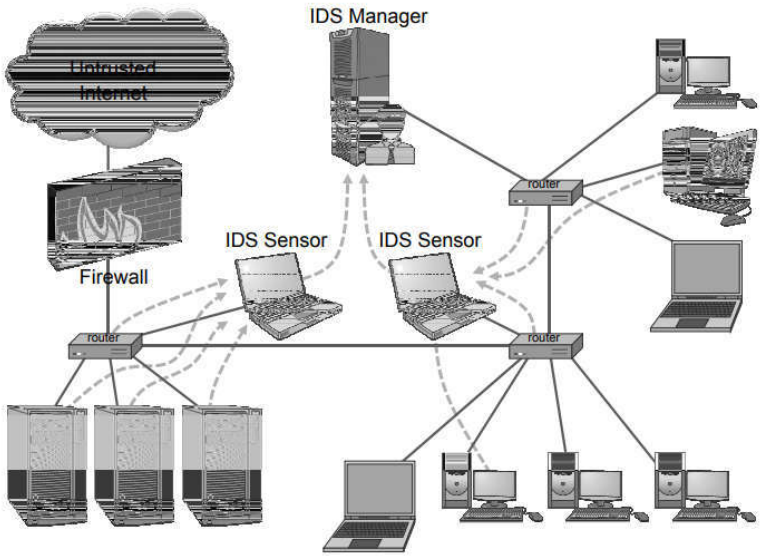
mereka ketika kita memesan sesuatu melalui Internet dan email konfirmasi dikirimkan kepada kita.

3. Mendeteksi Aktivitas Berbahaya pada Mail Server Security

a. Intrusion Detection System (IDS)

Intrusion detection system (IDS) adalah sistem perangkat lunak atau perangkat keras yang digunakan untuk mendeteksi tanda-tanda aktivitas berbahaya di jaringan atau komputer individual. Fungsi-fungsi IDS dibagi antara sensor-sensor ID, yang mengumpulkan data waktu-nyata tentang fungsi komponen jaringan dan komputer, dan manajer IDS, yang menerima laporan dari sensor.

Manajer IDS mengumpulkan data dari sensor IDS untuk menentukan apakah telah terjadi intrusi. Penentuan ini biasanya didasarkan pada sekumpulan kebijakan situs, yang merupakan kumpulan aturan dan kondisi statistik yang menentukan kemungkinan intrusi. Jika seorang manajer IDS mendeteksi intrusi, maka itu akan membunyikan alarm sehingga administrator sistem dapat bereaksi terhadap kemungkinan serangan. Lihat gambar 17 dibawah ini ;



Gambar 18. Jaringan area lokal yang dipantau oleh sistem deteksi intrusi (IDS).

Garis padat menggambarkan koneksi jaringan dan garis putus-putus abu-abu menggambarkan tanggung jawab pelaporan data. Router dan komputer yang dipilih melapor ke sensor IDS, yang pada gilirannya melaporkan ke manajer IDS. Intrusi IDS dirancang untuk mendeteksi sejumlah ancaman, termasuk yang berikut ini:

1) masquerader: penyerang yang secara tidak benar menggunakan identitas dan / atau kredensial pengguna yang sah untuk mendapatkan akses ke sistem atau jaringan komputer
2) Misfeasor: pengguna yang sah yang melakukan tindakan yang tidak diizinkan untuk dilakukannya
3) Pengguna rahasia: pengguna yang mencoba memblokir atau menutupi tindakannya dengan menghapus file audit dan / atau log sistem

Selain itu, IDS dirancang untuk mendeteksi serangan dan ancaman otomatis, termasuk yang berikut ini :

1) portscans: pengumpulan informasi yang dimaksudkan untuk menentukan yangport pada host terbuka untuk koneksi TCP
2) Serangan Denial-of-service: serangan jaringan yang dimaksudkan untuk membanjiri host dan menutup akses yang sah
3) Serangan malware: mereplikasi serangan perangkat lunak berbahaya, seperti Trojan horse, worm komputer, virus, dll.
4) ARPspoofing: sebuah jaringan server lokal yang dicoba untuk diarahkan
5) DNScachepoisoning: apharmingattackdirectedmencocokkan cache DNS host untuk membuat asosiasi nama-domain / alamat-IP yang salah

b. Intrusion Detection Event

Peristiwa Deteksi Intrusi Deteksi intrusi bukanlah ilmu pasti. Dua jenis kesalahan dapat terjadi:

1) Salah-positif: ketika analarmissoundedonbenignactivity, yang bukan merupakan gangguan
2) Negatif palsu: ketika alarm tidak berbunyi pada peristiwa berbahaya, yang merupakan gangguan dari keduanya, negatif palsu umumnya dianggap lebih bermasalah karena kerusakan sistem dapat akan luput dari perhatian. Positif palsu, di sisi lain, lebih menjengkelkan, karena mereka cenderung menghabiskan waktu dan sumber daya pada ancaman yang

dirasakan yang bukan merupakan serangan sebenarnya. Maka, kondisi ideal adalah sebagai berikut.

3) Benar-benar positif: bila ada suara yang mengganggu, yang merupakan gangguan
4) Benar negatif: ketika alarm tidak dibunyikan pada aktivitas jinak, yang bukan merupakan gangguan

c. Rule-Based Intrusion Detection

Sebuah teknik yang digunakan oleh sistem deteksi intrusi untuk mengidentifikasi kejadian yang harus memicu kesalahan saraf. Aturan tersebut dapat mengidentifikasi jenis tindakan yang cocok dengan profil tertentu yang diketahui untuk serangan intrusi, dalam hal ini aturan akan menyandikan tanda tangan untuk serangan tersebut. Jadi, jika manajer IDS melihat peristiwa yang cocok dengan tanda tangan untuk aturan tersebut, itu akan segera membunyikan alarm, bahkan mungkin menunjukkan jenis serangan tertentu yang dicurigai. Aturan IDS juga dapat menyandikan kebijakan yang telah disiapkan oleh administrator sistem untuk pengguna dan / atau host. Jika aturan seperti itu dipicu, menurut kebijakan, itu berarti bahwa pengguna bertindak dengan cara yang mencurigakan atau bahwa host sedang diakses dengan cara yang mencurigakan. Contoh kebijakan tersebut dapat mencakup berikut ini:

1) Komputer desktop tidak boleh digunakan sebagai server HTTP.
2) Server HTTP mungkin tidak menerima sesi telnet atau FTP (tidak terenkripsi).
3) Pengguna tidak boleh membaca direktori pribadi pengguna lain.
4) Pengguna tidak boleh menulis ke file yang dimiliki oleh pengguna lain.
5) Pengguna hanya dapat menggunakan perangkat lunak berlisensi pada satu mesin dalam satu waktu.
6) Pengguna harus menggunakan perangkat lunak VPN resmi untuk mengakses komputer desktop mereka dari jarak jauh.
7) Pengguna tidak boleh menggunakan server komputer administratif antara tengah malam dan 4:00 pagi.

d. Statistical Intrusion Detection

Salah satu pendekatan utama untuk deteksi intrusi didasarkan pada statistik. Prosesnya dimulai dengan mengumpulkan data audit tentang

pengguna atau host tertentu, untuk menentukan nilai numerik dasar tentang tindakan yang dilakukan oleh orang atau mesin tersebut. Tindakan dapat dikelompokkan berdasarkan objek (yaitu, semua tindakan yang memiliki bidang objek yang sama), tindakan, atau kondisi pengecualian. Tindakan juga dapat digabungkan dalam berbagai rentang waktu atau dalam hal rentang atau persentase penggunaan sumber. Nilai numerik yang dapat diperoleh termasuk: • Hitung: jumlah kemunculan jenis tindakan tertentu dalam rentang waktu tertentu • Rata-rata: jumlah kejadian yang lebih sedikit dari jenis tindakan tertentu dalam rentang waktu tertentu • Persentase: persentase dari sumber daya bahwa jenis tindakan tertentu diambil selama rentang waktu tertentu • Pengukuran: agregat atau rata-rata-dari-rata-rata selama periode waktu yang relatif lama • Panjang interval waktu: jumlah waktu yang berlalu di antara contoh tindakan dari jenis tertentu.

C. SOAL LATIHAN/ TUGAS

1. Apa yang dimaksud dengan Simple Mail Transfer Protocol (SMTP) ?
2. Apa yang anda ketahui tentang Spam Email ?
3. Sebutkan jenis-jenis serangan pada Email ?
4. Buatkan proteksi dengan Intrusion detection system (IDS) !

D. REFERENSI

Vacca, J. R. (2017). *Computer and Information Security Handbook*. 3rd Edition. Elsevier, Inc.

Bosworth, S., Kabay, M. E., & Whyne, E. (2014). Computer Security Handbook. 6th Edition. Canada: John Wiley & Sons, Inc.

Goodrich, M., & Tamassia, R. (2014). Introduction to Computer Security. Harlow: Pearson Education Ltd.

Panek, C. (2020). Security Fundamental. Canada: Sybex A Wiley Brand.

Furnell, S., & Dowland, P. (2010). E-mail Security A Pocket Guide. IT Governance Publishing.

Paulsen, C., & Byers, R. D. *Glossary of Key Information Security Terms* [Internet]. Juli 2019. NIST Pubs. Tersedia pada: https://www.nist.gov/publications/glossary-key-information-security-terms-2, https://csrc.nist.gov/glossary