LAMPIRAN

1. Lampiran detail analisa studi kasus PT. Simpli Mobile Indonesia
2. Lampiran hasil framework
3. Kode Pemprograman

DETAIL ANALISA STUDI KASUS PT. SIMPLI MOBILE INDONESIA

Pada landasan teori telah disebutkan 6 tahap untuk melakukan laporan penelitian masalah yang dihadapi oleh PT. SMI. Hasilnya berupa sebuah laporan yang akan menjadi masukan untuk menjawab kasus yang dihadapi.

= **Memutuskan dan menentukan pertanyaan penelitian**

Untuk menentukan pertanyaan penelitian studi kasus sistem keamanan PT. SMI, penulis akan lihat dari lingkup masalah yang ingin diteliti. Berikut ini merupakan pertanyaan yang akan dijawab sesuai dengan pemaparan masalah pada I.1.2 :

Firewall* yang diandalkan sebagai pelindung keamanan data bekerja di lapisan *network*, sehingga sulit menganalisa gangguan keamanan yang menggunakan lapisan *application* dari *Open System Interconnection

Pertanyaan penelitian yang bisa dibuat dari pernyataan ini ialah :

1. Pada aplikasi-aplikasi apa perangkat keamanan mampu menganalisanya?
2. Untuk aplikasi yang menggunakan enkripsi, apakah perlu diteliti juga, mengingat membuka sebuah enkripsi tidaklah mudah?
3. Apakah perlu dilakukan otomatis pemblokiran penyerangan, lalu bagaimana bila yang diblokir itu merupakan *traffic legitimate*?

Setiap aplikasi berbasis *client-server* memiliki pencatatan fasilitas aktifitas penggunaan yang berbeda-beda dan terpisah-pisah secara logis ataupun fisik sehingga mempersulit dalam mendapatkan gambaran yang utuh tentang aktifitas layanan

Pertanyaan penelitian yang bisa dibuat dari pernyataan ini ialah :

1. Apakah bisa pencatatan aktifitas ini dikonsolidasi disebuah *server* pencatatan aktifitas?

2. Bila bisa dikonsolidasi, bagaimana dengan keamaan dari *server* ini, dikarenakan bila tersebar, keuntungannya, belum tentu sebuah *server* yang tersusupi akan berhasil masuk ke *server* lain, sedangkan bila telah terkonsolidasi, maka bila penyusup berhasil masuk kedalam *server* konsolidasi, seluruh aktifitas *server* dapat dibaca dengan mudah?

Terjadi peningkatan aktifitas yang tiba-tiba diluar waktu yang telah ditentukan menyebabkan lambatnya akses ke layanan tertentu karena *bandwidth* yang dimiliki oleh PT. SMI telah penuh oleh aktifitas pengguna yang tidak diketahui apakah ada penambahan pengguna layanan atau telah terjadi penyerangan.

Pertanyaan penelitian yang bisa dibuat dari pernyataan ini ialah :

1. Melalui aplikasi-aplikasi apa terjadi peningkatan *traffic*?
2. Apakah tidak ada perbedaan *traffic* yang baik atau yang jahat yang bisa dilihat, misalkan dari *payload* yang dikirimkan?

Pengembangan layanan konten yang dibutuhkan oleh pelanggan tidak diimbangi oleh perangkat layanan yang dimiliki oleh PT. SMI dan perancangan layanan konten tidak memperhatikan masalah-masalah keamanan.

Pertanyaan yang bisa dibuat dari pernyataan ini adalah :

1. Apakah mungkin dilakukan perubahan proses bisnis tentang bagaimana layanan konten itu dibuat?

= Memilih kasus dan memutuskan pengumpulan data dan teknis analisa

Dari empat pernyataan terhadap masalah yang dihadapi oleh PT. SMI, penulis mengambil dua pernyataan kasus yang akan menjadi objek penelitian penulis, kasus yang penulis ambil :

1. *Firewall* yang diandalkan sebagai pelindung keamanan data bekerja di lapisan *network*, sehingga sulit menganalisa gangguan kemanan yang menggunakan lapisan *application* dari *Open System Interconnection.*
2. Terjadi peningkatan aktifitas yang tiba-tiba diluar waktu yang telah ditentukan menyebabkan lambatnya akses ke layanan tertentu karena *bandwidth* yang dimiliki oleh PT. SMI telah penuh oleh aktifitas pengguna yang tidak diketahui apakah ada penambahan pengguna layanan atau telah terjadi penyerangan.

Melihat kasus-kasus yang dihadapkan kita bisa mengambil keputusan data-data apakah yang perlu dikumpulkan untuk pengumpulan data ini. Berdasarkan informasi dari kasus ini, maka penulis akan memerlukan kumpulan data berupa :

1. *Traffic* dari IP *address* yang bersifat serangan
2. *Traffic* dari IP *address* yang bersifat bukan serangan

Semua informasi itu akan dianalisa dengan sebuah perhitungan kemungkinan sebuah ip ini melakukan serangan atau tidak. Informasi yang ada diproses, lalu sistem akan menentukan tindakan selanjutnya. Tindakan yang dimaksud bisa berupa peringatan ataupun langsung tindakan pencegahan usaha intrusi.

= **Mempersiapkan pengumpulan data**

Untuk mendapatkan data-data ini, penulis akan melakukan perekaman data transaksi setiap IP yang masuk dalam 1 waktu untuk melihat kebiasaan IP tersebut. Perekaman data ini akan dilakukan dengan cara *sniffing* pada sebuah jaringan komputer dalam satu waktu tertentu. Selama perekaman akan juga dilihat berapa banyak *traffic* dari sebuah IP yang normal sebagai *traffic* baik, ataupun yang kurang normal yang bisa diasumsikan *traffic* jahat.

Selain analisa dari *traffic*, penulis juga akan meng*interview* sistem administrator untuk mendapatkan informasi yang terkait dengan pertanyaan penelitian yang terkait dengan kasus yang dihadapi oleh PT. SMI

= **Mengumpulkan data di lapangan**

Setelah diperoleh cara-cara untuk mengumpulkan informasi sebuah IP itu apakah baik atau tidak, maka penulis akan melakukan berbagai mencoba menimbulkan pertanyaan *interview* yang akan diberikan kepada sistem administrator PT. SMI.

Pertanyaan Penelitian : Pada aplikasi-aplikasi apa perangkat keamanan mampu menganalisanya?

Pertanyaan *Interview* : Aplikasi-aplikasi yang aktif di *server* menggunakan protokol apa saja?

Pertanyaan Penelitian : Apakah perlu diteliti juga *traffic* enkripsi, mengingat membuka sebuah enkripsi tidaklah mudah?

Pertanyaan *Interview* : Aplikasi seperti VPN, SSL sangat sulit untuk diteliti, apa perlu dianalisa, apa keperluan analisa *traffic* ini?

Pertanyaan Penelitian : Apakah tidak ada perbedaan *traffic* yang baik atau yang jahat yang bisa dilihat, misalkan dari *payload* yang dikirimkan?

Pertanyaan *Interview* : Pernah melihat rekaman-rekaman transaksi masuk dan keluar saat sebuah transaksi konten meningkat?

Pertanyaan Penelitian : Apakah perlu dilakukan otomatis pemblokiran penerobosan, lalu bagaimana bisa yang diblok itu merupakan *traffic* legitimate?

Pertanyaan *Interview* : Bila ingin dibuat mampu melakukan blokir IP *address* bila mentrigger suatu masalah, apakah bisa? Bagaimana bila dibuat semi otomatis, dimana sistem administrator bisa memutuskan juga?

Pertanyaan Penelitian : Melalui aplikasi-aplikasi apa terjadi peningkatan *traffic*?

Pertanyaan *Interview* : Apakah ada protokol tertentu yang mengalami peningkatan *traffic* yang diluar aktifitas?

= **Mengevaluasi dan menganalisa data**

Selama pemprosesan kasus yang dihadapi, semua hasil survey, *interview*, dan pengumpulan data *traffic* dikumpulkan untuk dianalisa, kemudian dicari pattern yang sesuai bisa digunakan sebagai kunci. Pattern ini bisa didapatkan dari persamaan atau perbedaan dari masing-masing kasus. Ini disebut dengan Analisa Antara Kasus.

Analisa Antara Kasus berupa memeriksa pasangan kasus, melakukan kategori persamaan dan perbedaan setiap pasangan kasus. Kemudian juga diperiksa kesamaan pasangan yang serupa untuk perbedaannya, maupun yang berbeda untuk persamaannya. Seiring dengan itu, beberapa bukti yang berlawanan dengan *pattern* bisa dikeluarkan. Bila ini terjadi bisa dianalisa kembali proses *interview*, pengumpulan data, dan kaitan antara hasil dan pertanyaan penelitian.

= **Mempersiapkan laporan**

Seluruh informasi pattern akan dikumpulkan untuk dibuatkan solusi yang menyangkut masalah pattern tersebut. Solusi ini berupa perangkat lunak yang bisa menghubungkan berbagai macam kasus yang dihadapi oleh PT.SMI dalam satu waktu.

= **Analisa & Pembahasan Pertanyaan Penelitian**

Pertanyaan penelitian yang dijadikan dasar peneltian ini menjadi acuan untuk menentukan pattern yang bisa muncul untuk pengembangan solusi atas permasalahan PT. SMI, berikut merupakan pertanyaan penelitian, pertanyaan *interview*, dan hasil *interview* dari sistem administrator perusahaan.

Pertanyaan Penelitian : Pada aplikasi-aplikasi apa perangkat keamanan mampu menganalisanya?

Pertanyaan *Interview* : Aplikasi-aplikasi yang aktif di *server* menggunakan protokol apa saja?

Berdasarkan hasil *interview* yang dilakukan ke sistem administrator ada beberapa jenis protokol aplikasi yang umum digunakan di PT. SMI, protokol tersebut ialah :

1. Protokol HTTP, protokol ini digunakan untuk mengirimkan/menerima SMS dari operator untuk diproses oleh PT. SMI. Selain untuk SMS, protokol ini juga digunakan di PT. SMI untuk layanan memasukkan konten ke pihak-pihak penyedia konten, memberikan layanan laporan *traffic* sms ke pihak internal atau penyedia konten, layanan website informasi perusahaan.
2. Protokol Database, protokol ini digunakan untuk mengakses database langsung dari kantor/remote saat administrator perusahaan harus melakukan pengisian data, peng-*input*-an data dan pemprosesan data.
3. Protokol SSH, protokol ini digunakan untuk mengakses *server-server* di data center untuk *maintenance*, ataupun untuk mengakses perangkat jaringan.
4. Protokol SMPP, protokol ini digunakan untuk mengirimkan/menerima SMS dari operator. Ada beberapa operator yang menggunakan protokol SMPP dikarenakan protokol ini lebih efesien daripada protokol HTTP.
5. Protokol FTP, protokol ini digunakan untuk mengirimkan file ke *server*, ataupun untuk menerima file dari beberapa penyedia konten untuk diproses oleh PT. SMI.

Berdasarkan informasi diatas, protokol HTTP merupakan protokol yang lebih banyak memberikan informasi terhadap apa yang mungkin bisa disimpan di data center PT. SMI. Dengan intrusi di protokol HTTP memungkinkan terjadinya "*information leak*" yang mungkin bisa disalahgunakan oleh pihak-pihak yang tidak bertanggungjawab. Intrusi pada protokol HTTP bisa memberikan informasi sebagai berikut :

1. Pengaksesan langsung pada *server*, sehingga bisa melakukan perubahan-perubahan konfigurasi pada aplikasi yang terkena pada intrusi yang bisa menganggu aktifitas. Intrusi pada pengaksesan langsung pada *server* bisa digunakan misalkan untuk penyimpanan file, melakukan proses pengiriman SMS secara manual yang bisa berakibat dimasukkannya PT. SMI ke *blacklist* operator selular.

2. Pengaksesan langsung ke *database*, sehingga bisa melakukan pengambilan, perubahan data yang bisa berdampak buruk terhadap pelanggan PT. SMI.

Melihat informasi diatas, protokol HTTP harus diberikan perlindungan ekstra terhadap usaha-usaha intrusi karena bisa menjadi pintu akses ke protokol lainnya di PT. SMI, seperti protokol *database*, protokol FTP dan protokol SSH. Protokol HTTP umumnya tidak dienkripsi sehingga besar kemungkinan bisa disadap juga ditengah jalan untuk mendapatkan informasi yang lebih jelas tentang apa yang dilakukan sebuah aplikasi berbasis protokol HTTP. Hal ini bisa berbahaya bagi PT. SMI.

Pertanyaan Penelitian : Apakah perlu diteliti juga *traffic* enkripsi, mengingat membuka sebuah enkripsi tidaklah mudah?

Pertanyaan *Interview* : Aplikasi seperti VPN, SSL sangat sulit untuk diteliti, apa perlu dianalisa, apa keperluan analisa *traffic* ini?

Berdasarkan hasil *interview*, aplikasi seperti VPN ataupun SSL hanya digunakan di administrator tertentu yang memiliki akses lebih tinggi ke *server-server* perusahaan di data center. Untuk VPN sendiri, PT. SMI menggunakan sebuah perangkat lunak OpenVPN yang berbasis pada SSL. OpenVPN menggunakan protokol UDP pada port 1194, sehingga koneksi-koneksi yang terhubung menjadi seperti tidak terkait seperti TCP. Sedangkan SSL sendiri tidaklah digunakan di PT. SMI dalam bentuk HTTPS, dikarenakan belum ada layanan PT. SMI yang membutuhkan HTTPS untuk mengakses informasinya.

Pertanyaan Penelitian : Apakah tidak ada perbedaan *traffic* yang baik atau yang jahat yang bisa dilihat, misalkan dari *payload* yang dikirimkan?

Pertanyaan *Interview* : Pernah melihat rekaman-rekaman transaksi masuk dan keluar saat sebuah transaksi konten meningkat?

Berdasarkan hasil *interview*, rekaman aplikasi-aplikasi transaksi masuk dan keluar di aplikasi SMS berupa :

1. URL masuk yang berisi informasi MSISDN, TRXDATE, SMS. MSISDN merupakan nomor pelanggan, TRXDATE merupakan tanggal transaksi dari SMS tersebut dan SMS merupakan isi dari SMS.
2. URL keluar yang berisi informasi MSISDN, TRXDATE, SMS, STATUS. MSISDN merupakan nomor pelanggan, TRXDATE merupakan tanggal transaksi dari SMS tersebut, SMS merupakan isi dari SMS, dan STATUS merupakan status informasi dari sebuah SMS di sisi operator.

Rekaman transaksi lain seperti layanan untuk pengisian konten, melihat report, melihat informasi website, PT. SMI tidak memiliki fasilitas transaksi yang lengkap, yang ada pada misalkan pada pengisian konten, saat melakukan pengisian konten, akan dimasukan ke sebuah *history* layanan tersebut.

Berdasarkan hasil *interview* diatas penulis menganalisa beberapa hal yang bisa menjadi sumber masalah bila terjadi sistem PT. SMI ini :

1. URL transaksi yang masuk terekam dalam bentuk tidak dienkripsi, maka akan terlihat bagaimana sebuah operator mengirimkan transaksi ke PT. SMI, dengan transaksi ini, dimungkinkan untuk mengirimkan transaksi seolah-olah dari operator selular.
2. URL transaksi yang keluar juga terekam dalam bentuk tidak terenkripsi, apalagi transaksi ini bisa dibedakan dengan jelas, antara jenis PUSH atau PULL. PUSH merupakan transaksi sms yang tidak perlu dipicu oleh transaksi SMS dari operator, sedangkan PULL harus dipicu oleh transaksi SMS dari operator.

Berdasarkan hal ini, maka sebuah intrusi yang berhasil masuk ke dalam sistem SMS, bisa mengirimkan SMS dalam jumlah besar dengan metoda PUSH ke nomor pelanggan manapun, bahkan tanpa pelanggan harus melakukan registrasi terhadap layanan tertentu. Hal ini sangat berbahaya, karena nomor pelanggan bisa mendapatkan SMS sampah, yang berakibat akan mengurangi jumlah kredit dari nomor pelanggan tersebut. Untuk itu perlu dilakukan usaha untuk membatasi akses ke *server* SMS ini secara langsung.

Berdasarkan hasil *interview*, sistem administrator menginginkan sistem yang bisa memberikan peringatan lebih jelas akan usaha intrusi terhadap data center PT. SMI. Peringatan intrusi ini haruslah dikirimkan secepat mungkin, namun sebisa mungkin tidak memberikan peringatan yang salah kepada sistem administrator. Peringatan salah pada sistem administrator akan membuat bingung akan keamanan data di PT. SMI.

Analisa yang penulis dapat dari pertanyaan ini ialah sistem diharuskan dapat memperkirakan sebuah IP sedang melakukan serangan atau tidak. Sistem yang dikembangkan haruslah memiliki kemampuan untuk mengumpulkan seluruh data yang terkait dengan transaksi sebuah IP terhadap sistem. Dengan adanya data transaksi ini bisa ditarik persentase berapa besar kemungkinan sebuah IP melakukan serangan intrusi. Besarnya jumlah transaksi yang bersifat serangan akan berbanding lurus dengan total jumlah transaksi yang dilakukan oleh sebuah IP. Informasi ini kemudian harus digabungkan dengan informasi lain untuk mendapatkan sebuah nilai yang akan dibandingkan dengan sebuah batas yang telah ditentukan oleh sistem administrator.

Pertanyaan Penelitian : Apakah perlu dilakukan otomatis pemblokiran penerobosan, lalu bagaimana bisa yang diblok itu merupakan *traffic* l*egitimate*?

Pertanyaan *Interview* : Bila ingin dibuat mampu melakukan blokir ip address bila mentrigger suatu masalah, apakah bisa? Bagaimana bila dibuat semi otomatis, dimana sistem administrator bisa memutuskan juga?

Berdasarkan hasil *interview*, sistem administrator bisa menerima cara blokir IP address secara otomatis. Namun juga tetap sistem administrator memiliki kontrol terhadap keputusan akan diblokir atau tidaknya sebuah IP. Sistem administrator menginginkan informasi misalkan berupa IP address dan berapa persen IP ini kemungkinan melakukan intrusi terhadap sistem PT. SMI.

Berdasarkan analisa diperoleh sistem ini harus mampu memberikan informasi berapa persen sebuah IP ini melakukan aktifitas intrusi, bila dibandingkan dengan total *traffic* yang ada. Dengan adanya informasi ini diputuskan apakah ini merupakan intrusi atau tidak. Bila dalam jangka waktu

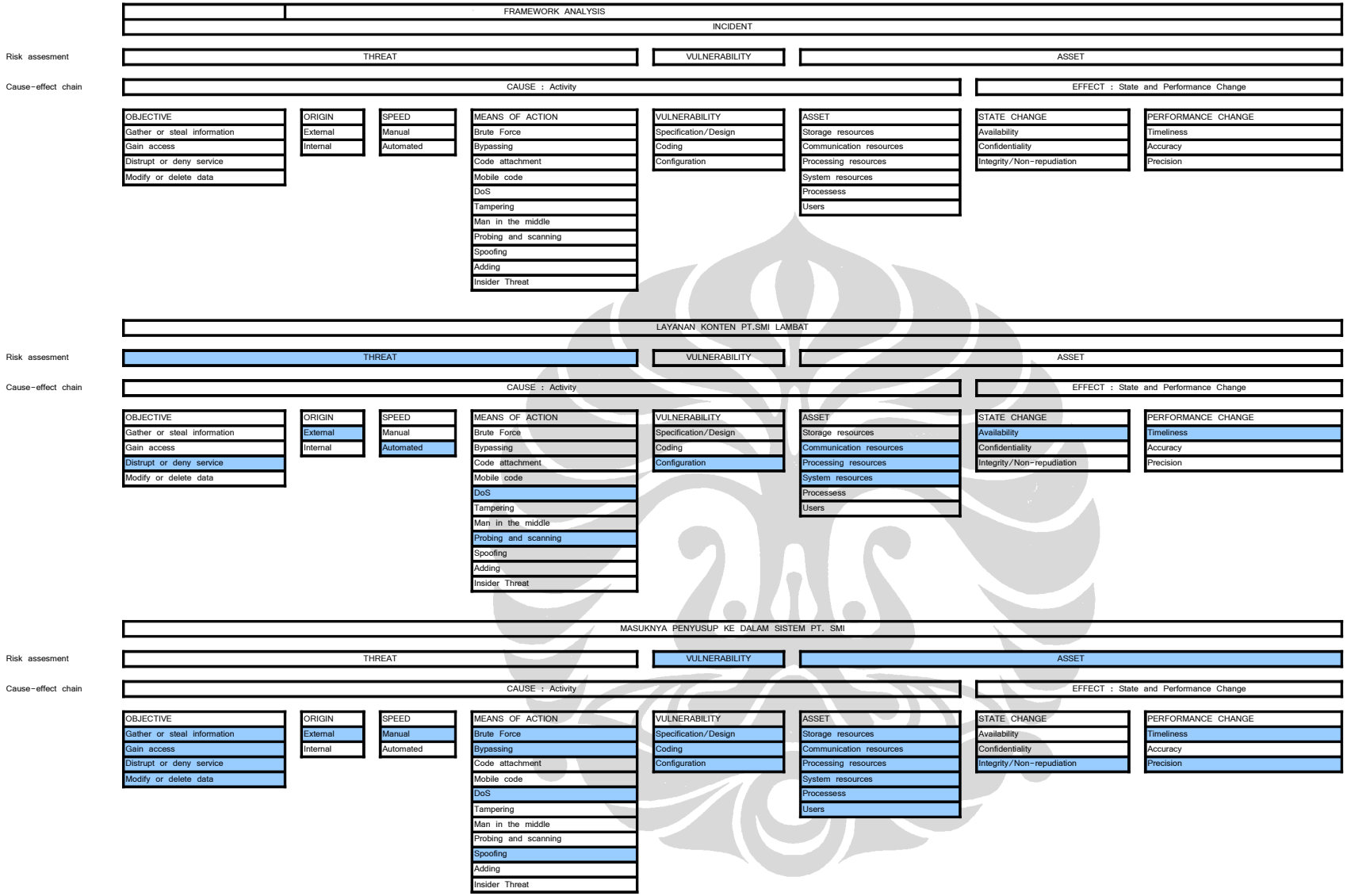
tertentu sistem administrator tidak bisa memutuskan, sistem secara otomatis bisa ditentukan apakah harus diblok atau tidak.

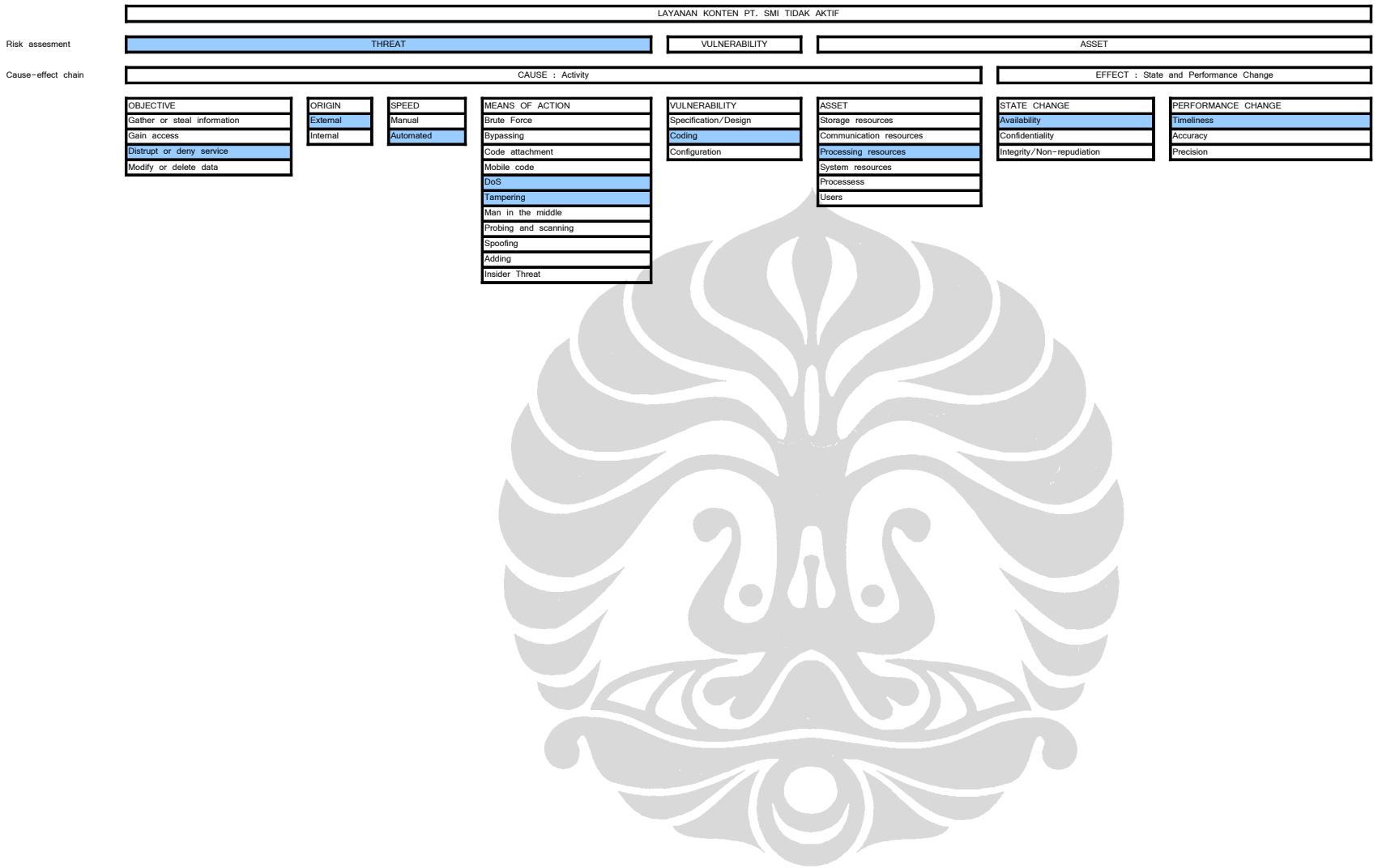
Pertanyaan Penelitian : Melalui aplikasi-aplikasi apa terjadi peningkatan *traffic*?

Pertanyaan *Interview* : Apakah ada protokol tertentu yang mengalami peningkatan *traffic* yang diluar aktifitas?

Berdasarkan hasil *interview,* aplikasi-aplikasi HTTP sering mengalami peningkatan akses dalam jangka waktu tertentu. Padahal tidak ada promosi akan layanan konten tersebut dalam kurun waktu peningkatan *traffic.* Hal ini mencurigakan bagi sistem administrator PT. SMI.

Berdasarkan analisa diperoleh sistem ini harus mampu memberikan rekaman transaksi sebuah IP baik yang bersifat serangan atau bukan, agar bisa melihat lebih lanjut tentang aktifitas dalam sehari yang mungkin bisa merupakan sebuah serangan jenis baru yang tidak terdeteksi oleh sistem keamanan.


FRAMEWORK ANALYSIS
INCIDENT
Risk assesment
THREAT
VULNERABILITY
ASSET
Cause-effect chain
CAUSE : Activity
EFFECT : State and Performance Change
OBJECTIVE
Gather or steal information
Gain access
Distrupt or deny service
Modify or delete data
ORIGIN
External
Internal
SPEED
Manual
Automated
MEANS OF ACTION
Brute Force
Bypassing
Code attachment
Mobile code
DoS
Tampering
Man in the middle
Probing and scanning
Spoofing
Adding
Insider Threat
VULNERABILITY
Specification/Design
Coding
Configuration
ASSET
Storage resources
Communication resources
Processing resources
System resources
Processess
Users
STATE CHANGE
Availability
Confidentiality
Integrity/Non-repudiation
PERFORMANCE CHANGE
Timeliness
Accuracy
Precision
LAYANAN KONTEN PT.SMI LAMBAT
Risk assesment
THREAT
VULNERABILITY
ASSET
Cause-effect chain
CAUSE : Activity
EFFECT : State and Performance Change
OBJECTIVE
Gather or steal information
Gain access
Distrupt or deny service
Modify or delete data
ORIGIN
External
Internal
SPEED
Manual
Automated
MEANS OF ACTION
Brute Force
Bypassing
Code attachment
Mobile code
DoS
Tampering
Man in the middle
Probing and scanning
Spoofing
Adding
Insider Threat
VULNERABILITY
Specification/Design
Coding
Configuration
ASSET
Storage resources
Communication resources
Processing resources
System resources
Processess
Users
STATE CHANGE
Availability
Confidentiality
Integrity/Non-repudiation
PERFORMANCE CHANGE
Timeliness
Accuracy
Precision
MASUKNYA PENYUSUP KE DALAM SISTEM PT. SMI
Risk assesment
THREAT
VULNERABILITY
ASSET
Cause-effect chain
CAUSE : Activity
EFFECT : State and Performance Change
OBJECTIVE
Gather or steal information
Gain access
Distrupt or deny service
Modify or delete data
ORIGIN
External
Internal
SPEED
Manual
Automated
MEANS OF ACTION
Brute Force
Bypassing
Code attachment
Mobile code
DoS
Tampering
Man in the middle
Probing and scanning
Spoofing
Adding
Insider Threat
VULNERABILITY
Specification/Design
Coding
Configuration
ASSET
Storage resources
Communication resources
Processing resources
System resources
Processess
Users
STATE CHANGE
Availability
Confidentiality
Integrity/Non-repudiation
PERFORMANCE CHANGE
Timeliness
Accuracy
Precision


LAYANAN KONTEN PT. SMI TIDAK AKTIF
Risk assesment
THREAT
VULNERABILITY
ASSET
Cause-effect chain
CAUSE : Activity
EFFECT : State and Performance Change
OBJECTIVE
Gather or steal information
Gain access
Distrupt or deny service
Modify or delete data
ORIGIN
External
Internal
SPEED
Manual
Automated
MEANS OF ACTION
Brute Force
Bypassing
Code attachment
Mobile code
DoS
Tampering
Man in the middle
Probing and scanning
Spoofing
Adding
Insider Threat
VULNERABILITY
Specification/Design
Coding
Configuration
ASSET
Storage resources
Communication resources
Processing resources
System resources
Processess
Users
STATE CHANGE
Availability
Confidentiality
Integrity/Non-repudiation
PERFORMANCE CHANGE
Timeliness
Accuracy
Precision