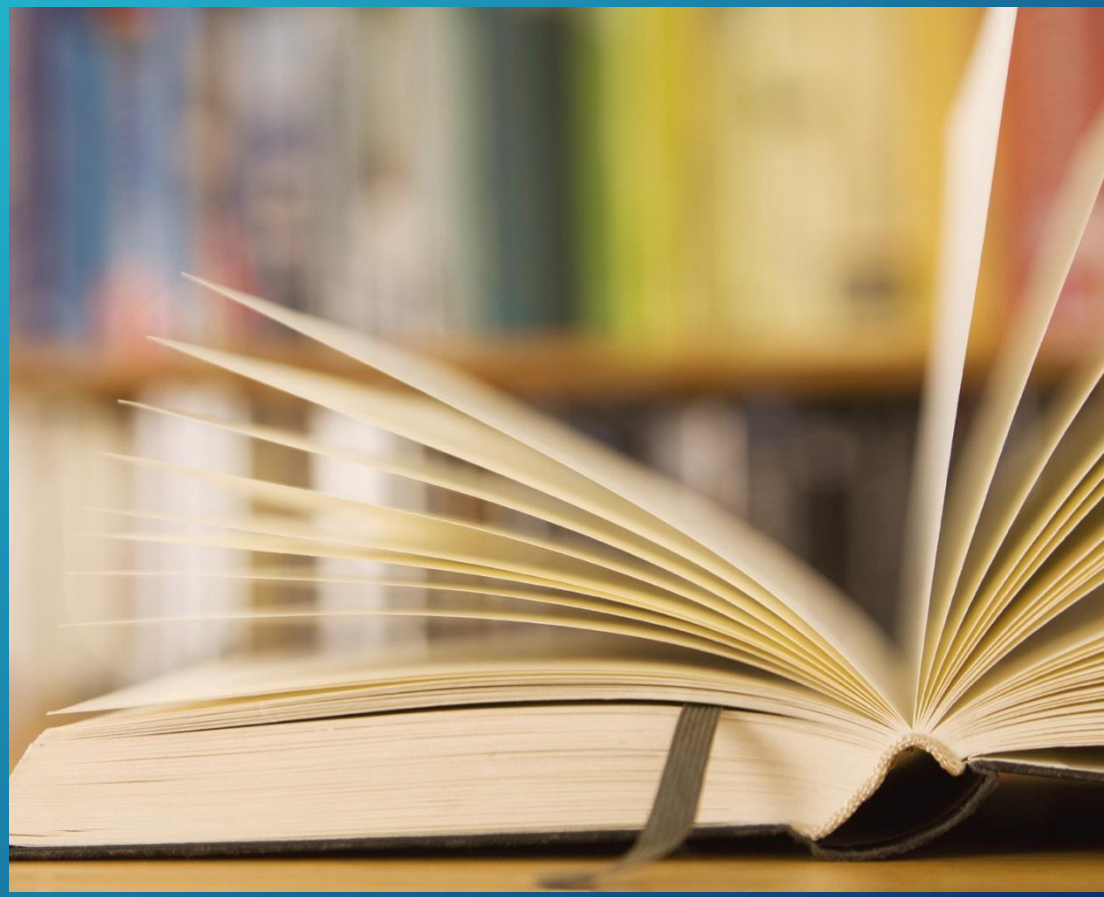
SEKOLAH TINGGI TEKNOLOGI
TERPADU NURUL FIKRI
CHARACTER BUILDING CAMPUS
STT - NF

KEAMANAN SERVER DAN JARINGAN



Keamanan Sistem Informasi – Aditya Putra, ST., MT.

Agenda

- Hardening Operating System
- Menutup Servis yang tidak digunakan
- Memasang Proteksi Jaringan: Firewall
- Memasang Proteksi Jaringan: IDS/IPS
  - Tentang Akurasi Sensor
- File Integrity Monitoring
- Audit Log
- Backup Rutin
- Enkripsi :
  - Data
  - Secure Shell (SSH)

Hardening Operating System

Checklist Standar untuk hardening OS

- Disable service yang tidak digunakan
- Update patch secara rutin
- Gunakan password yang kuat
- Disable akun yang tidak digunakan
- Install software antivirus
- Gunakan enkripsi pada file/direktori penting
- Aktifkan logging
- Disable file sharing yang tidak digunakan

Menutup Service yang tidak Digunakan

- OS Ketika pertama kali diinstall secara default membuka beberapa servis dasar. Sebagai contoh, Telnet, FTP, SMTP, POP, dll. Servis ini tidak semuanya dibutuhkan. Untuk mengamankan system, servis yang tidak dibutuhkan tersebut akan lebih aman jika ditutup.
- Beberapa command di Linux yang bisa digunakan dalam proses menutup/stop service

No	Command	Arti
1	`ps ax`	Mengetahui tipe service yang sedang berjalan
2	`netstat -a`	Mengetahui proses apa yang portnya terbuka dan sedang melakukan transaksi data ke/dari internet
3	`service [service_name] stop`	Disable service
4	`update-rc.d -f [service name] remove`	Disable service sejak boot up

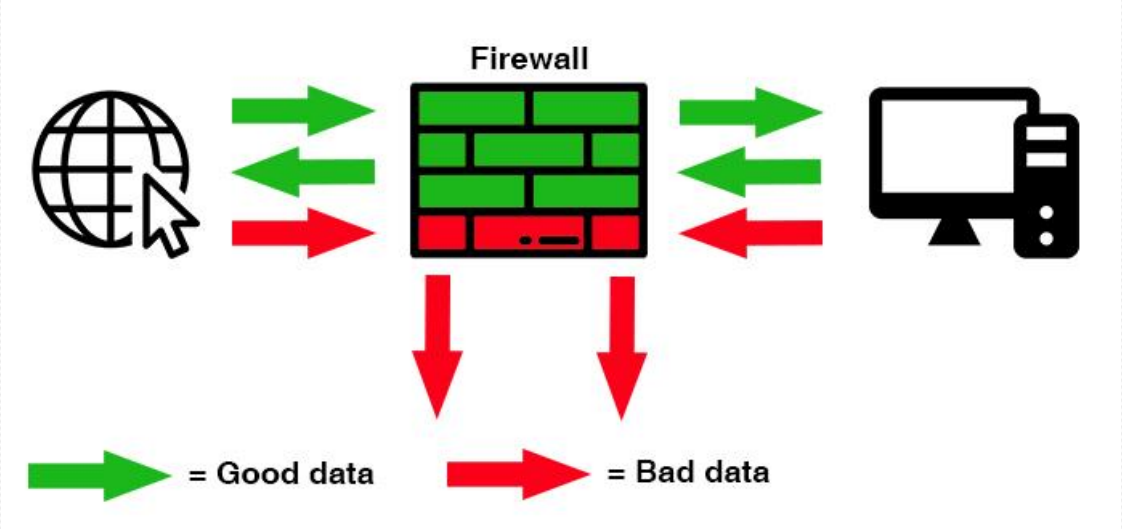
Memasang Proteksi Jaringan: FIREWALL

Jaringan dapat diproteksi menggunakan beberapa macam perangkat yang memiliki cara kerja dan tujuan yang berbeda. Proteksi pada Jaringan adalah salah satu cara untuk mengimplementasikan Defense-in-Depth pada jaringan kita.

Berikut contoh Perangkat/Middleware yang dapat memproteksi jaringan

FIREWALL

- Firewall dapat berupa software jika ia diinstall sebagai Host Firewall atau Hardware jika diinstall sebagai Network Firewall. Pada dasarnya Firewall adalah Router yang memiliki kemampuan untuk melakukan Filtering Trafik berdasarkan IP, Port, dan Protocol
- Perkembangan Firewall menjadikannya memiliki kemampuan lain dengan mengintegrasikannya dengan berbagai perangkat lain



Memasang Proteksi Jaringan: IDS/IPS

Intrusion Detection/Prevention System (IDS/IPS)

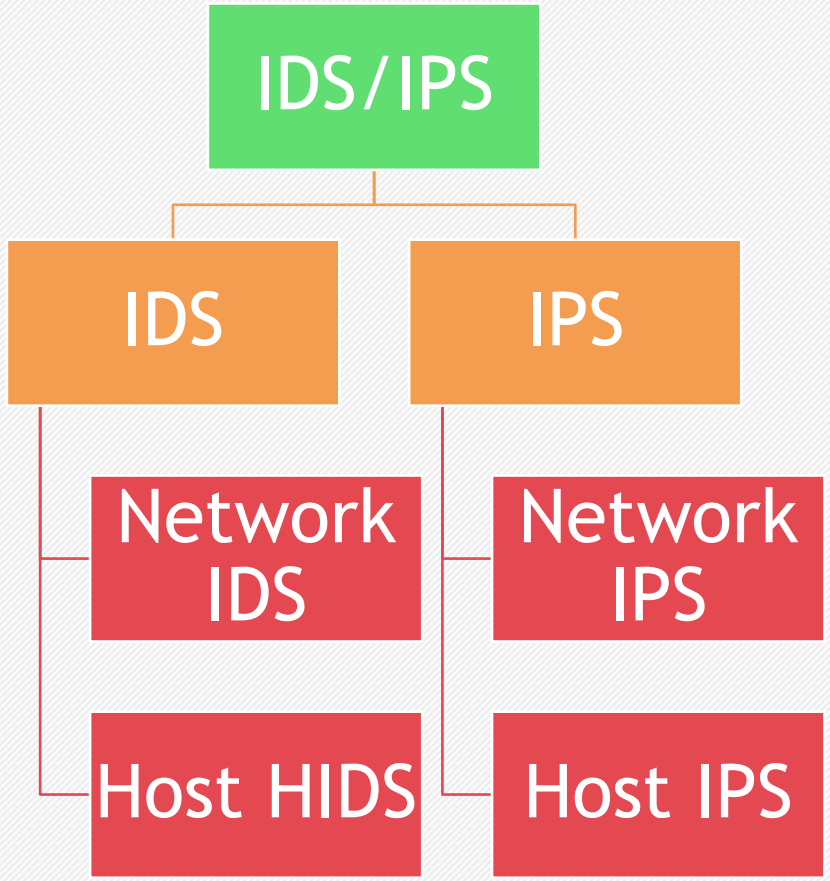
Intrusi adalah upaya illegal untuk merusak nilai CIA dan membahayakan keamanan asset yang dilindungi

Tipe Intrusi pada Jaringan

- Koneksi dari Lokasi (IP) yang tidak biasa
- Percobaan login yang berulang secara remote
- Upaya DDoS/premintaan service berulang dalam jumlah besar

IDS/IPS digunakan untuk mengedalikan intrusi pada jaringan. IDS berperan mendeteksi intrusi sedangkan IPS selain deteksi, memiliki kemampuan untuk mencegah intrusi pada Jaringan

Perbedaan Firewall dengan IDS/IPS adalah kemampuan IDS/IPS yang bisa mengenali sampai behaviour atau pola aktivitas suatu trafik



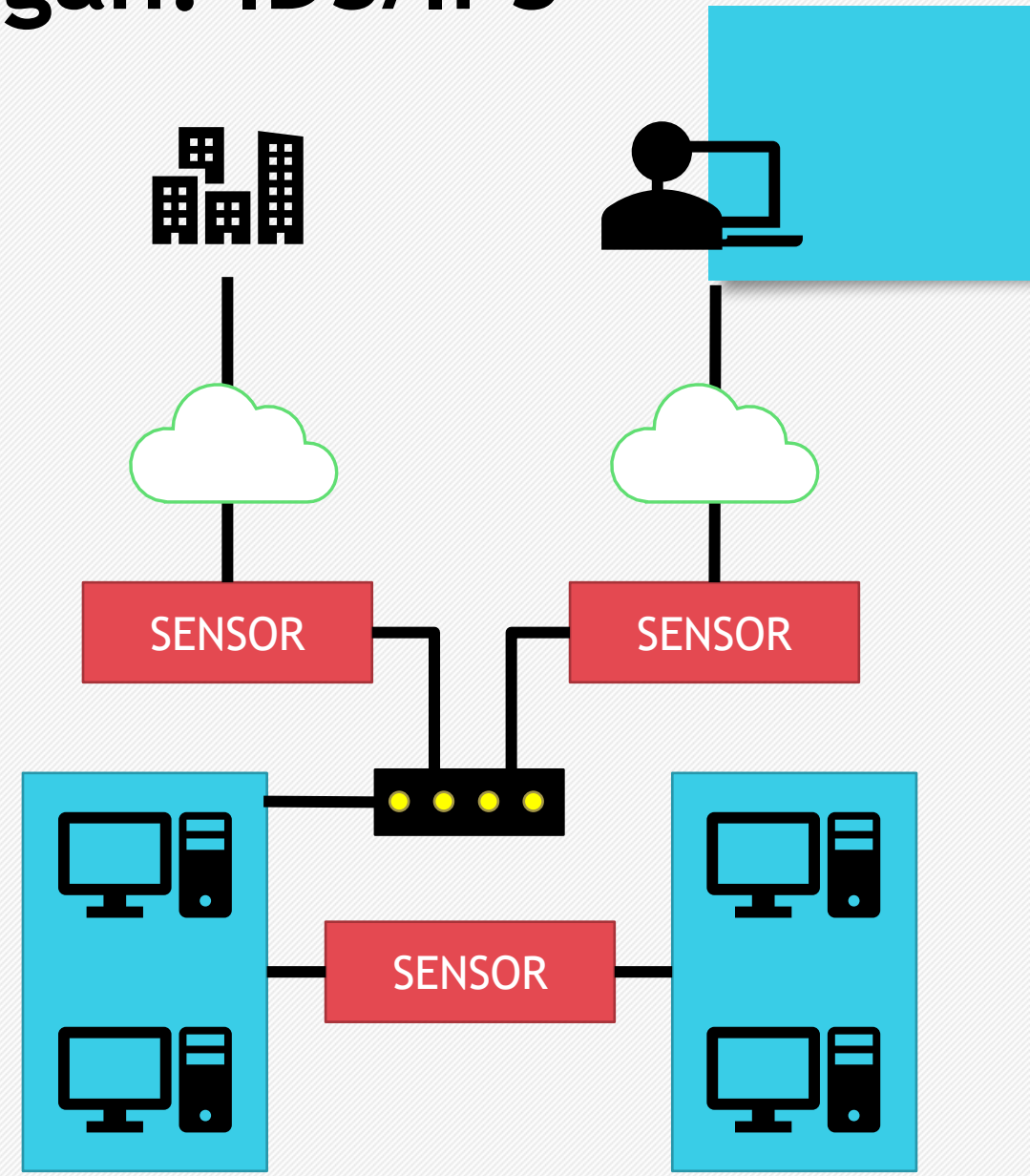
Memasang Proteksi Jaringan: IDS/IPS

Tidak seperti Firewall, IDS/IPS memiliki beberapa komponen:

1. Network Sensor

   Perangkat ini adalah komponen yang melakukan monitoring trafik dan menginisiasi alert jika ada aktivitas abnormal yang terdeteksi. Biasanya diletakkan pada

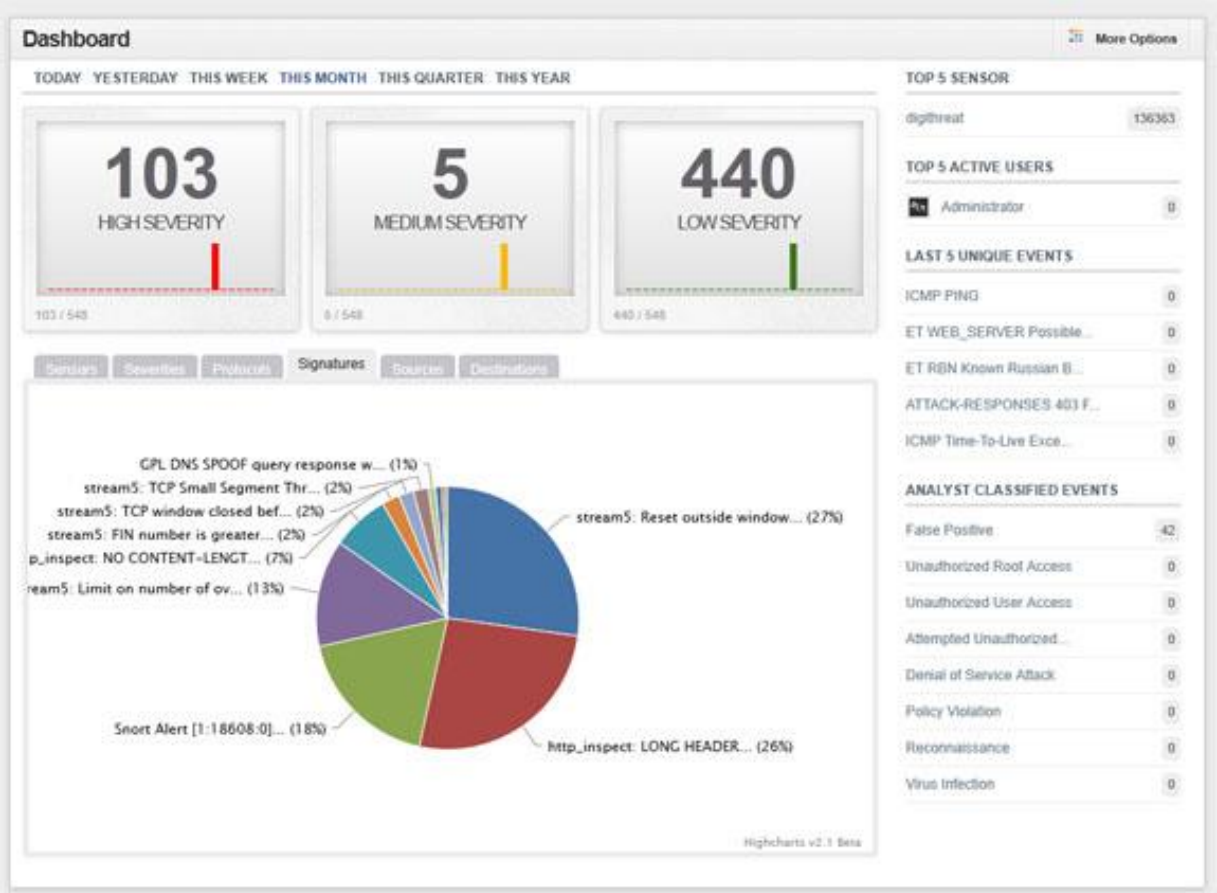
   - Antara remote user dengan jaringan
   - Antara kantor cabang dengan jaringan
   - Antar subnet di jaringan kantor



Memasang Proteksi Jaringan: IDS/IPS

2. Command Console

- Perangkat ini adalah komponen yang terpisah dari Sensor dan diinstall software untuk menampilkan User Interface
- User Interface ini juga membantu administrator untuk menganalisa security event, pesan alert dan log file
- Security event, pesan alert, dan log file didapatkan dari berbagai sensor yang telah dideploy



Command Console karena membutuhkan resource yang besar sehingga perlu diinstall pada dedicated server. Kurangnya resource dapat mengurangi performanya untuk memproses data yang dikirimkan oleh Sensor

Memasang Proteksi Jaringan: IDS/IPS

3. Response System

- Response System berperan dalam melakukan penindakan
- Response system bukan pengganti administrator karena Response system harus memiliki kemampuan dalam menentukan keputusan apa yang diambil dan meresponnya secara otomatis
- Administrator akan membuat keputusan saat menemukan kasus False Positif atau respon lain yang memerlukan eskalasi

4. Attack Signature Database

- Komponen inilah yang membuat IDS memiliki kemampuan untuk membuat keputusan
- Database ini memuat daftar attack signature yaitu karakteristik trafik yang abnormal. Dengan mencocokkan trafik real dengan database ini, IDS dapat mengetahui apakah suatu trafik dapat dikatakan intrusi atau bukan. Lalu memberikan respon yang tepat untuk trafik tersebut

Administrator yang baik tidak bergantung sepenuhnya pada IDS Response Systems untuk merespon intrusi

Akurasi Sensor

Masih ingat dengan ilustrasi di samping?

Setiap sensor memiliki akurasinya masing-masing dan Sensor yang Baik adalah yang memiliki Nilai TP dan TN tinggi serta FP dan FN yang rendah

- FP Rate (FPR) ➔ Tingkat kesalahan Ketika serangan benar-benar terjadi

$$FPR = \frac{FP}{FP + TN} = 1 - TNR$$

*FP + TN adalah 2 kondisi dimana serangan **BENAR** terjadi*

- FN Rate (FNR) ➔ Tingkat kesalahan Ketika serangan tidak terjadi

$$FNR = \frac{FN}{FN + TP} = 1 - TPR$$

*FN + TP adalah 2 kondisi dimana serangan **TIDAK** terjadi*

An Aesop's Fable: The Boy Who Cried Wolf (*compressed*)

A shepherd boy gets bored tending the town's flock. To have some fun, he cries out, "Wolf!" even though no wolf is in sight. The villagers run to protect the flock, but then get really mad when they realize the boy was playing a joke on them.

[Iterate previous paragraph *N* times.]

One night, the shepherd boy sees a real wolf approaching the flock and calls out, "Wolf!" The villagers refuse to be fooled again and stay in their houses. The hungry wolf turns the flock into lamb chops. The town goes hungry. Panic ensues.

Let's make the following definitions:

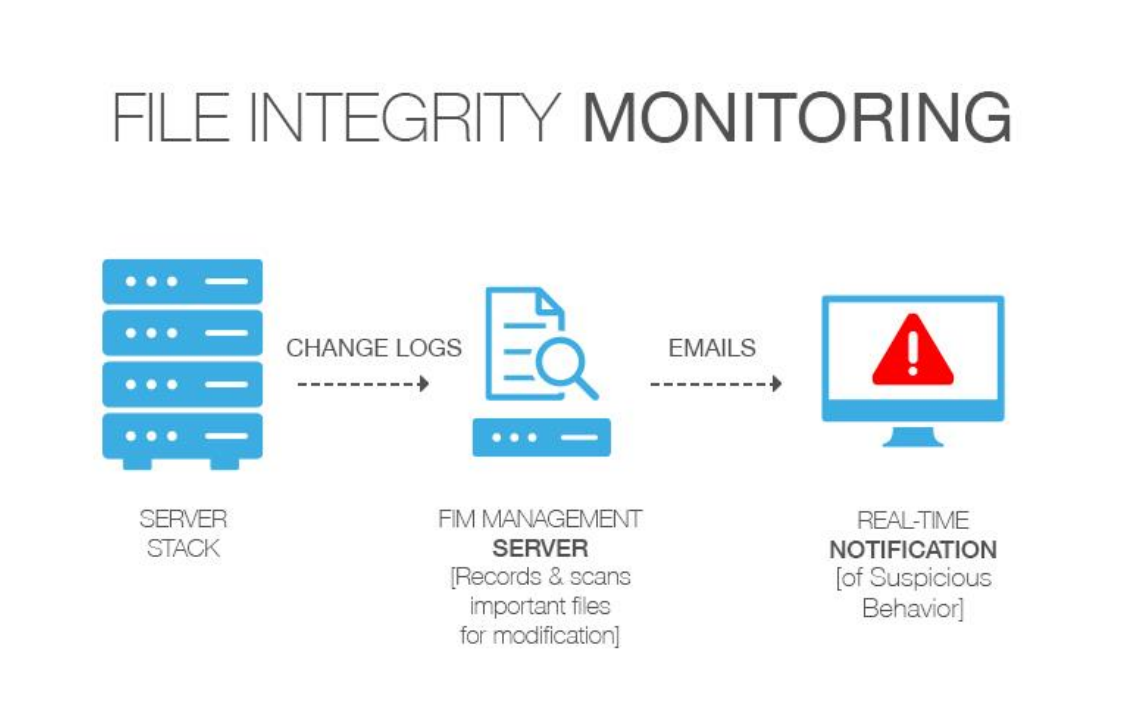
- "Wolf" is a **positive class**.
- "No wolf" is a **negative class**.

We can summarize our "wolf-prediction" model using a 2x2 confusion matrix that depicts all four possible outcomes:

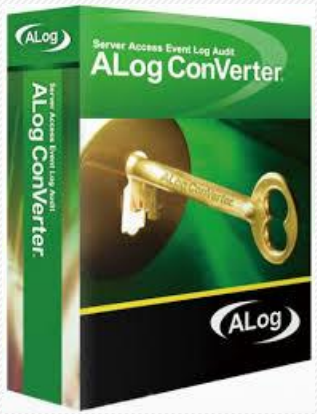
True Positive (TP): • Reality: A wolf threatened. • Shepherd said: "Wolf." • Outcome: Shepherd is a hero.	**False Positive (FP):** • Reality: No wolf threatened. • Shepherd said: "Wolf." • Outcome: Villagers are angry at shepherd for waking them up.
False Negative (FN): • Reality: A wolf threatened. • Shepherd said: "No wolf." • Outcome: The wolf ate all the sheep.	**True Negative (TN):** • Reality: No wolf threatened. • Shepherd said: "No wolf." • Outcome: Everyone is fine.

System/File Integrity Monitoring

- File Integrity Monitoring adalah tools untuk memantau integritas sistem.
- Tools ini berjalan dengan membuat database mengenai file atau direktori yang ingin diamati beserta signaturenya
- Signature berisi informasi mengenai size, waktu dibuat/modified, pemilik, hasil checksum atau hash dan informasi meta data lain dari file/direktori tersebut. Jika ada file yang berubah maka akan menghasilkan checksum yang berbeda dan ini akan memicu alert / pencatatan log
- Contoh dari Tools ini adalah Tripwire pada UNIX dan ALog Converter



tripwire



Audit Log

- Log menyimpan dan mencatat aktivitas yang terjadi pada server. Log ini sangat berguna untuk mengamati adanya penyimpangan yang terjadi
- Failed attempt saat login misalnya tercatat pula di log file. Anomali seperti failed attempt yang terjadi pada waktu yang singkat dapat menunjukkan bahwa ini adalah serangan brute force attack
- Pada sistem UNIX/Linux/Debian, file log disimpan pada direktori: `/var/adm` atau `/var/log`
- Berikut macam-macam log file

Log File	Keterangan
`/var/log/auth.log`	Berisi informasi otentikasi seperti gagal login
`/var/log/daemon.log`	Berisi informasi program-program daemon/yang running di background
`/var/log/mail.log`	Berisi informasi tentang email yang dikirimkan dan diterima MTA serta akses ke sistem melalui POP3 dan IMAP
`/var/log/syslog`	Berisi informasi pesan yang dihasilkan oleh program syslog

Audit Log

CONTOH AUTH LOG

- Auth.log 1

```
Apr 8 08:47:12 xact passwd[8518]: password for `inet' changed by root
```

Log di atas mencatat bahwa password untuk user “inet” telah diganti oleh user “root” pada waktu tsb

- Auth.log 2

```
Apr 5 17:20:10 alliance wu-ftpd[12037]: failed login from ws170.library.msstate.edu
[130.18.249.170], m1
```

Log di atas mencatat bahwa ada upaya login pada service FTP

Backup Rutin

- Backup rutin diperlukan untuk menghindari kehilangan data baik secara sengaja maupun tidak
- Intruder suatu saat mungkin masuk ke dalam sistem dan merusak sistem dengan menghapus data-data yang dapat ia temui. Jika intruder berhasil melakukan privilege escalation menjadi super user (administrator/root) maka dia memiliki akses penuh terhadap suatu sistem
- Sistem yang esensial perlu membuat backup yang secara fisik jauh dengan sistem asli untuk menghindari hilangnya data karena bencana alam seperti kebakaran, banjir, gempa, dll.
- Jika bencana terjadi merusak Sistem asli sedangkan backup diletakkan pada lokasi yang sama, maka tujuan backup akan menjadi sia-sia

Enkripsi

Enkripsi wajib dilakukan untuk melindungi data dan informasi

- Perlindungan data menggunakan enkripsi tidak hanya dilakukan pada storage/penyimpanannya namun juga saat data tersebut ditransmisikan/dikirimkan. Media pengiriman juga perlu mengimplementasikan enkripsi
- Contoh Perlindungan pada transmisi SSH
- Secure Shell (SSH) adalah protokol secure remote login dari klien ke server menggunakan default port 22. SSH menjadi solusi alternatif yang aman dibandingkan dengan protocol login lain seperti telnet dan rlogin
- SSH juga diimplementasikan ke dalam service lain seperti SFTP