

# **UAS KEAMANAN INFORMASI**

**Operasi  
keamanan**



**Dosen pengampu :**  
Triawan adi cahyanto MK.

**Disusun oleh:**  
Habi aburrohman  
1310651055

**JURUSAN TEKNIK INFORMATIKA  
FAKULTAS TEKNIK  
UNIVERSITAS MUHAMMADIYAH JEMBER  
2014**

Operasi keamanan berkaitan dengan ancaman terhadap lingkungan operasi produksi. Agen ancaman bisa menjadi aktor internal atau eksternal, dan keamanan operasi harus memperhitungkan untuk kedua sumber ancaman tersebut agar efektif. Operasi keamanan adalah tentang orang, data, media, perangkat keras, dan ancaman yang terkait dengan masing-masing di produksi lingkungan Hidup.

## KEAMANAN ADMINISTRASI

Sebuah aspek fundamental dari keamanan operasi adalah memastikan bahwa kontrol berada di tempat untuk menghambat orang baik sengaja atau tidak sengaja mengorbankan kerahasiaan, integritas, atau ketersediaan data atau sistem dan media memegang data. administratif keamanan menyediakan sarana untuk mengontrol akses operasional masyarakat untuk data.

## Penyimpanan

Ketika menyimpan informasi sensitif, adalah lebih baik untuk mengenkripsi data.

### Enkripsi

Data pada saat istirahat sangat mengurangi kemungkinan data yang diungkapkan dalam sebuah sah

mode karena masalah keamanan Media. Penyimpanan fisik dari media yang mengandung

informasi sensitif tidak boleh dilakukan secara sembarangan, apakah data dienkripsi atau tidak.

Penyimpanan Media dan informasi memiliki masa manfaat yang terbatas. Penyimpanan informasi sensitif tidak harus bertahan di luar periode kegunaan atau persyaratan hukum (mana yang lebih besar), karena sia-sia memperlihatkan data ancaman pengungkapan ketika data tersebut tidak lagi diperlukan oleh organisasi. Perlu diingat mungkin ada peraturan atau lainnya alasan hukum yang dapat memaksa organisasi untuk mempertahankan data tersebut untuk menjaga Data melampaui waktu dari utilitas.

Media sanitasi atau kerusakan data Sementara beberapa data mungkin tidak sensitif dan tidak menjamin kerusakan data menyeluruh langkah-langkah, sebuah organisasi akan memiliki data yang harus diverifikasi dihancurkan atau diberikan nonusable dalam kasus media di mana ia ditempatkan dipulihkan oleh pihak ketiga. Proses untuk sanitasi media atau kerusakan data bervariasi secara langsung dengan jenis media dan sensitivitas data.

## Data remanence

Data remanen adalah data yang berlangsung di luar kemampuan noninvasif untuk menghapusnya. Meskipun

Data remanen kadang-kadang digunakan secara khusus untuk mengacu pada data residual yang berlangsung

pada penyimpanan magnetik, kekhawatiran remanence melampaui hanya itu penyimpanan magnetic Media. Menyeka, Timpa, atau merobek-robek

Dalam kebanyakan sistem file, jika pengguna menghapus file, sistem file hanya menghapus meta data pointer atau referensi ke file. Tabel alokasi file referensi dihapus, tapi file data itu sendiri tetap. Jumlah signifikan "data yang dihapus" dapat pulih (Terhapus); alat forensik yang tersedia untuk melakukannya. Memformat sistem file juga dapat meninggalkan data utuh.

Meskipun penghapusan sederhana dari file atau memformat hard disk tidak cukup untuk membuat data unrecoverable, file dapat dengan aman dihapus atau ditimpa. Menyeka, juga disebut Timpa atau merobek-robek, menulis data baru atas setiap bit atau blok file data. Salah satu kekurangan dari menyeka adalah ketika hard disk menjadi rusak secara fisik, mencegah Timpa sukses dari semua data.

### Degaussing

Dengan memperkenalkan medan magnet eksternal melalui penggunaan degausser, data pada media penyimpanan magnetik dapat dibuat tidak terpulihkan. Sebuah degausser menghancurkan integritas dari magnetisasi dari media penyimpanan itu sendiri, membuat data dipulihkan.

### Kerusakan fisik

Kerusakan fisik, bila dilakukan dengan benar, dianggap cara yang paling aman media sanitasi. Salah satu alasan untuk tingkat yang lebih tinggi dari jaminan adalah karena kemungkinan besar kesalahan yang mengakibatkan data yang remanence dengan menyeka atau degaussing. Kerusakan fisik dibenarkan untuk paling sensitif data. Umumnya kehancuran termasuk pembakaran dan penumbukan.

### Shredding

Bentuk sederhana media sanitasi yang merobek-robek, jenis kerusakan fisik. Meskipun istilah ini kadang-kadang digunakan dalam kaitannya dengan Timpa data, di sini merobek-robek mengacu pada proses pembuatan data yang dicetak pada hard copy, atau benda-benda kecil seperti sebagai disk floppy atau optik, dipulihkan. Informasi sensitif seperti informasi dicetak kebutuhan untuk robek sebelum dibuang untuk menggagalkan menyelam tempat sampah serangan. Dumpster diving adalah serangan fisik di mana seseorang pulih sampah dengan harapan menemukan informasi sensitif yang belum aman terhapus atau hancur.

## MANAJEMEN ASET

Pendekatan holistik untuk keamanan informasi operasional mengharuskan organisasi untuk fokus pada sistem serta orang, data, dan media. Sistem keamanan lain komponen penting untuk keamanan operasi, dan ada kontrol khusus yang sangat bisa membantu sistem keamanan di seluruh siklus hidup sistem. manajemen konfigurasi

Praktek manajemen konfigurasi dasar yang terkait dengan sistem keamanan akan melibatkan tugas-tugas seperti menonaktifkan layanan yang tidak perlu; menghapus program asing;

memungkinkan kemampuan keamanan seperti firewall, antivirus, dan deteksi intrusi atau sistem pencegahan; dan keamanan dan pemeriksaan log configuring.

baselining

Keamanan baselining adalah proses menangkap titik dalam pemahaman saat konfigurasi sistem keamanan saat ini. Membangun sarana mudah untuk menangkap konfigurasi sistem keamanan saat ini bisa sangat membantu dalam menanggapi potensi insiden keamanan.

Manajemen kerentanan

Kerentanan pemindaian adalah cara untuk menemukan konfigurasi miskin dan hilang patch dalam lingkungan. Manajemen kerentanan istilah digunakan agak hanya kerentanan pemindaian untuk menekankan perlunya pengelolaan kerentananInformasi. Remediasi atau mitigasi kerentanan harusdiprioritaskan berdasarkan pada kedua risiko untuk organisasi dan kemudahan remediasi prosedur.

Kerentanan zero-day dan zero-day eksploitasi

Sebuah kerentanan zero-day adalah kerentanan yang dikenal sebelum adanya Patch. Kerentanan zero-day, juga biasa ditulis 0-hari, menjadi semakin penting sebagai penyerang menjadi lebih terampil dalam penemuan, dan pengungkapan kerentanan zero-day sedang menghasilkan uang. Sebuah nol-hari memanfaatkan, daripada kerentanan, mengacu pada keberadaan mengeksploitasi kode untuk kerentanan yang belum menjadi ditambal.

Perubahan manajemen

Dalam rangka menjaga keamanan operasi yang konsisten dan dikenal, perubahan teratur manajemen atau proses pengendalian perubahan harus diikuti. Tujuan dari Proses pengendalian perubahan adalah untuk memahami, berkomunikasi, dan dokumen perubahan dengan tujuan utama untuk bisa memahami, kontrol, dan menghindari secara langsung atau tidak langsung dampak negatif perubahan mungkin memaksakan.

KONTINUITAS OPERASIONAL

Kelangsungan operasional adalah prinsipnya berhubungan dengan porsi ketersediaan kerahasiaan, integritas, dan ketersediaan triad.

Agar sistem dan solusi dalam sebuah organisasi untuk dapat terus menyediakan ketersediaan operasional, mereka harus dilaksanakan dengan toleransi kesalahan dalam pikiran. Ketersediaan tidak hanya semata-mata terfokus pada persyaratan sistem uptime tetapi juga mensyaratkan bahwa data yang dapat diakses secara tepat waktu.

## Backup

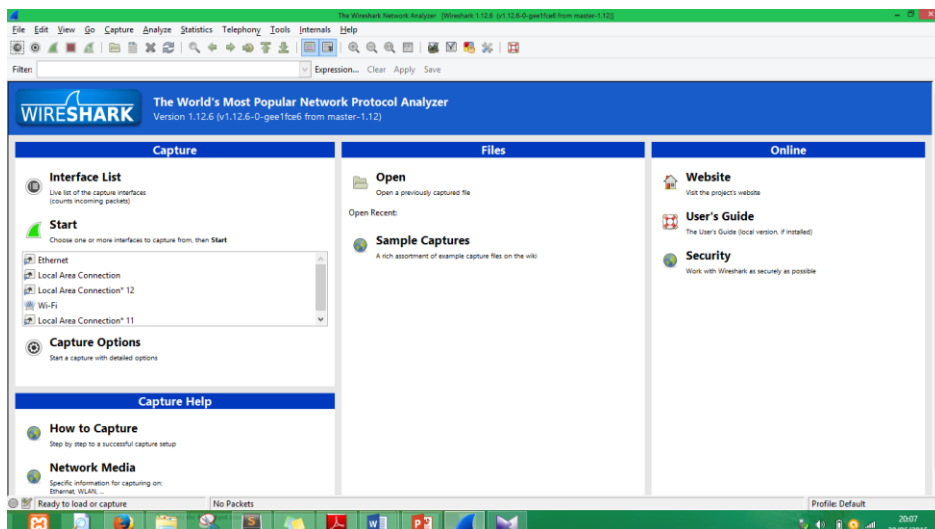
Agar data dapat dipulihkan dalam kasus kesalahan, beberapa bentuk cadangan atau redundansi harus disediakan. Meskipun media tape magnetik cukup teknologi lama, masih repositori paling umum data cadangan. Tiga tipe dasar backup: backup penuh, incremental backup, dan backup diferensial.

Penuh

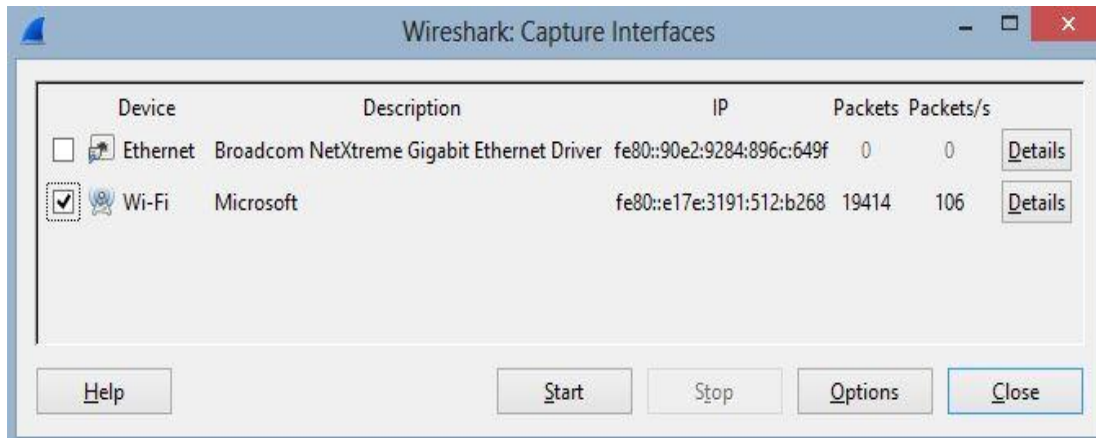
Penuh backup merupakan replika dari semua data yang dialokasikan pada hard disk. Karena lebih besar jumlah media, dan karena itu biaya media, dan jendela lagi cadangan persyaratan, backup penuh sering digabungkan dengan baik tambahan atau diferensial backup untuk menyeimbangkan waktu dan pertimbangan media yang. Incremental dan diferensial Incremental backup hanya file arsip yang telah berubah sejak terakhir cadangan dari setiap jenis dilakukan. Backup diferensial akan arsip file yang telah diubah sejak full backup terakhir.

N0 2. Login [sia.unmuhjember.ac.id](http://sia.unmuhjember.ac.id)

Pertama buka dulu wireshark



Centang yang ada wi-fi kemudian start



Keluar dan kunjungi website seperti di bawah

The screenshot shows the website 'sia.unmuhjember.ac.id'. The header features the university's logo and the text 'SISTEM INFORMASI AKADEMIK Universitas Muhammadiyah Jember'. The main content area is divided into two sections:

### Login

Id User :

Password :

☐ Case Sensitif

[Login](#) [Reset](#)

### Informasi Akademik Universitas Muhammadiyah Jember

#### Tahun Akademik 2014/2015 Genap

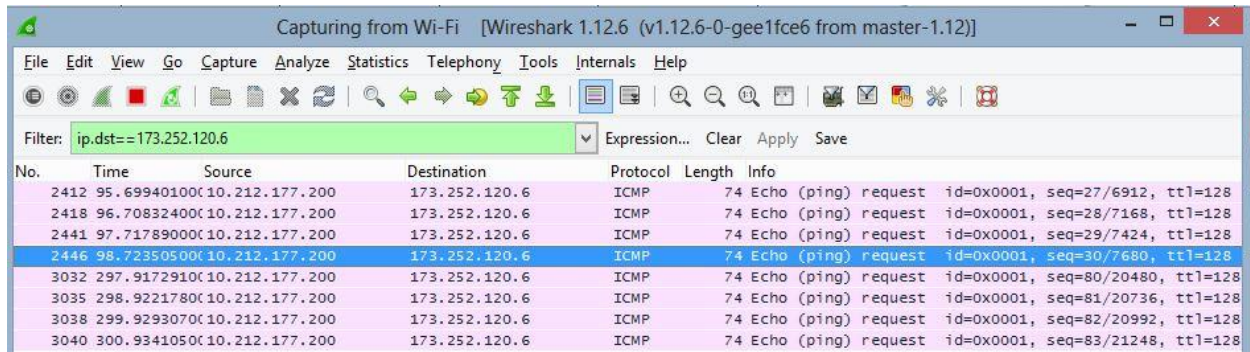
Pembayaran	Masa Akademik	Periode
Angsuran 3	Kartu Rencana Studi (KRS)	2015-01-29 s/d 2015-02-07
	Masa Kuliah	2015-02-16 s/d 2015-07-04
Angsuran 4	Ujian Tengah Semester (UTS)	2015-04-13 s/d 2015-04-27
	Ujian Akhir Semester (UAS)	2015-06-23 s/d 2015-07-04
Penilaian Terakhir		2015-07-08

**Panduan:**

1. Untuk Dosen dan Mahasiswa, Panduan dapat di download Setelah Login pada Menu **Panduan**
2. Jika Mengalami Masalah dalam menggunakan Sistem Informasi Akademik, silahkan konsultasi ke  
- Ruang Pelayanan Mahasiswa, Gedung A lantai 1
3. Kritik dan Saran yang bersifat membangun, email ke : [davidheriawanto@unmuhjember.ac.id](mailto:davidheriawanto@unmuhjember.ac.id)

Masukkan username dan kata sandi lalu login seperti biasa...

Ketika Selesai LOGIN, STOP Wreshark

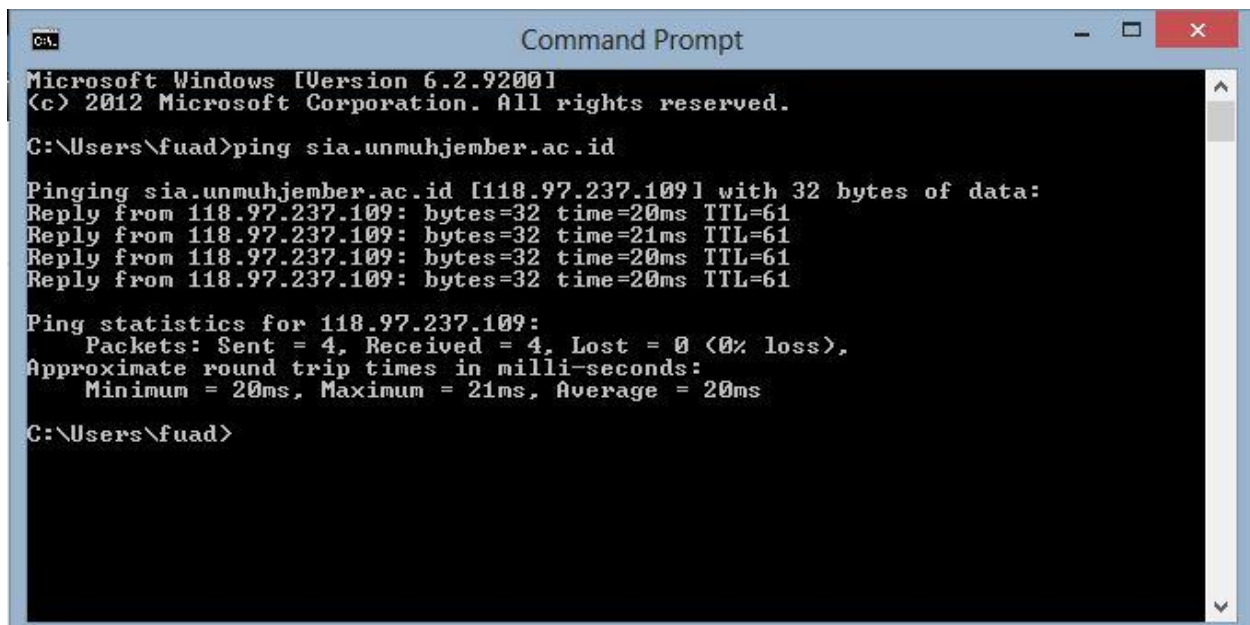


Capturing from Wi-Fi [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]

Filter: `ip.dst==173.252.120.6`

No.	Time	Source	Destination	Protocol	Length	Info
2412	95.699401000	10.212.177.200	173.252.120.6	ICMP	74	Echo (ping) request id=0x0001, seq=27/6912, ttl=128
2418	96.708324000	10.212.177.200	173.252.120.6	ICMP	74	Echo (ping) request id=0x0001, seq=28/7168, ttl=128
2441	97.717890000	10.212.177.200	173.252.120.6	ICMP	74	Echo (ping) request id=0x0001, seq=29/7424, ttl=128
2446	98.723505000	10.212.177.200	173.252.120.6	ICMP	74	Echo (ping) request id=0x0001, seq=30/7680, ttl=128
3032	297.917291000	10.212.177.200	173.252.120.6	ICMP	74	Echo (ping) request id=0x0001, seq=80/20480, ttl=128
3035	298.922178000	10.212.177.200	173.252.120.6	ICMP	74	Echo (ping) request id=0x0001, seq=81/20736, ttl=128
3038	299.929307000	10.212.177.200	173.252.120.6	ICMP	74	Echo (ping) request id=0x0001, seq=82/20992, ttl=128
3040	300.934105000	10.212.177.200	173.252.120.6	ICMP	74	Echo (ping) request id=0x0001, seq=83/21248, ttl=128

Kemudian lihat di cmd



```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\fuad>ping sia.unmuhjember.ac.id

Pinging sia.unmuhjember.ac.id [118.97.237.109] with 32 bytes of data:
Reply from 118.97.237.109: bytes=32 time=20ms TTL=61
Reply from 118.97.237.109: bytes=32 time=21ms TTL=61
Reply from 118.97.237.109: bytes=32 time=20ms TTL=61
Reply from 118.97.237.109: bytes=32 time=20ms TTL=61

Ping statistics for 118.97.237.109:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 21ms, Average = 20ms

C:\Users\fuad>
```

Filter ip nya dengan kode “ip.dst==118.97.237.109

Cari di info yg ada login.phpnya

Lihat di HTML Form URL Decoded

Capturing from Wi-Fi [Wireshark 1.12.0 (Wireshark 1.12.0-0-gce9f0c0 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `ip.dst==118.97.237.109` Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
4511	39.268867000	10.212.177.200	118.97.237.109	TCP	74	61019-80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256
4513	39.298012000	10.212.177.200	118.97.237.109	TCP	66	61019-80 [ACK] Seq=1 Ack=1 Win=16384 Len=0 TSval=15
4514	39.298448000	10.212.177.200	118.97.237.109	HTTP	599	POST /?act=login HTTP/1.1 (application/x-www-form-
4518	39.350092000	10.212.177.200	118.97.237.109	TCP	66	61019-80 [ACK] Seq=534 Ack=1462 Win=16384 Len=0 TSv
4521	39.351021000	10.212.177.200	118.97.237.109	TCP	66	61019-80 [ACK] Seq=534 Ack=2915 Win=16384 Len=0 TSv
4524	39.351288000	10.212.177.200	118.97.237.109	TCP	66	61019-80 [ACK] Seq=534 Ack=2922 Win=16384 Len=0 TSv
4527	39.352169000	10.212.177.200	118.97.237.109	TCP	66	61019-80 [ACK] Seq=534 Ack=4377 Win=16384 Len=0 TSv
4530	39.376376000	10.212.177.200	118.97.237.109	TCP	66	61019-80 [ACK] Seq=534 Ack=5832 Win=16384 Len=0 TSv

< >

Frame 4511: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

Ethernet II, Src: IntelCor\_45:56:90 (00:1c:bf:45:56:90), Dst: HuaweiTe\_9a:6b:08 (dc:d2:fc:9a:6b:08)

Internet Protocol Version 4, Src: 10.212.177.200 (10.212.177.200), Dst: 118.97.237.109 (118.97.237.109)

Transmission Control Protocol, Src Port: 61019 (61019), Dst Port: 80 (80), Seq: 0, Len: 0

```
0000  dc d2 fc 9a 6b 08 00 1c bf 45 56 90 08 00 45 00  ....k... .EV...E.
0010  00 3c 5f 1f 40 00 80 06 7b 31 0a d4 b1 c8 76 61  .<_@... {1....va
0020  ed 6d ee 5b 00 50 48 a7 c8 62 00 00 00 00 a0 02  .m.[.PH. .b.....
0030  20 00 81 a8 00 00 02 04 05 b4 01 03 03 08 04 02  .....
0040  08 0a 09 48 7c ed 00 00 00 00  ....H|... ..
```