KEAMANAN INFORMASI

Disusun oleh:

(IKA PURWATININGSIH)

(1310651023)

(E)

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH JEMBER

2015

JAWABAN!

1. Operations Security

Operations security is concerned with threats to a production operating environment. Threatagents canbeinternal orexternalactors,andoperations security mustaccount for both of these threat sources in order to be effective. Operations security is about people, data, media, hardware, and the threats associated with each of these in a pro-duction environment.

ADMINISTRATIVE SECURITY

A fundamental aspect of operations security is ensuring that controls are in place to inhibitpeople either inadvertentlyor intentionally compromising the confidentiality, integrity, or availability of data or the systems and media holding that data. Admin-istrative security provides the means to control people's operational access to data.

- Labels
- Clearance
- Separation of duties
- Rotation of duties
- Mandatory leave/forced vacation
- Nondisclosure agreement
- Background checks

SENSITIVE INFORMATION/MEDIA SECURITY

Though security and controls related to the people within an enterprise are vitally important, so is having a regimented process for handling sensitive information, including media security. This section discusses concepts that are an important com-ponent of a strong overall information security posture.

- Sensitive information
- Labeling/marking
- Handling
- Storage
- Retention
- Media sanitization or destruction of data

A holistic approach to operational information security requires organizations to focus on systems as well as the people, data, and media. Systems security is another vital component to operations security,and there are specific controls that can greatly help system security throughout the system's life cycle.

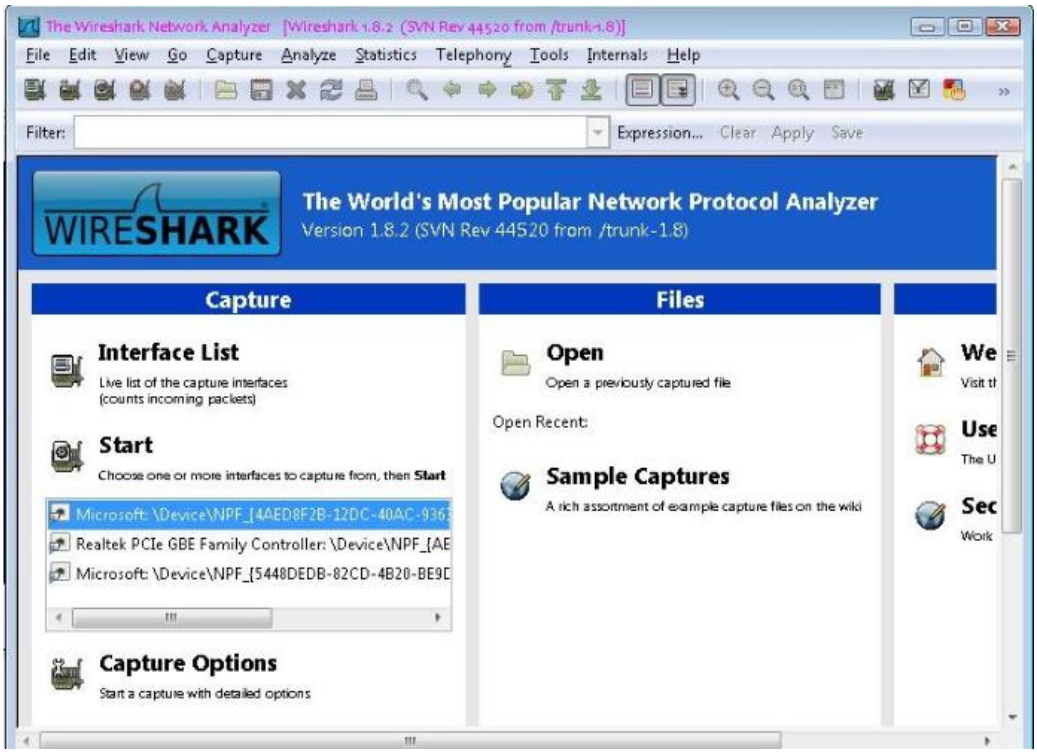
Continuity of operations is principally concerned with the availability portion of the confidentiality, integrity, and availability triad.

Asecurity incident is a harmful occurrence on a system or network. Allorganizations will experience security incidents. Incident response management is a regimented and tested methodology for identifying and responding to these incidents. A Computer Security Incident Response Team (CSIRT) is the group tasked with monitoring, identifying, and responding to security incidents. The goal of the inci-dent response plan is to allow the organization to control the cost and damage asso-ciated with incidents and to make the recovery of impacted systems quicker.

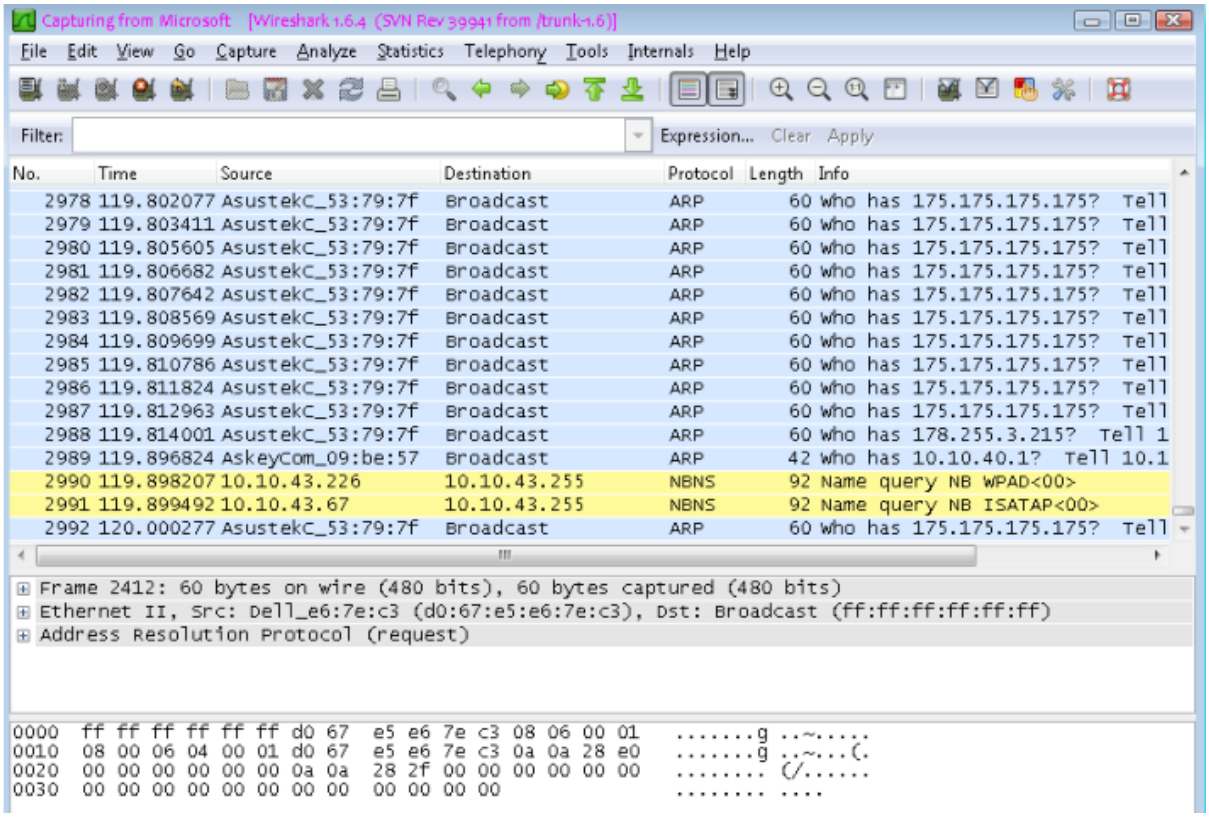
In this chapter, we have discussed operations security. Operations security concerns the security of systems and data while being actively used in a production environ-ment. Ultimately, operations security is about people, data, media, and hardware; all of which are elements that need to be considered from a security perspective. The best technical security infrastructure in the world will be rendered moot if an indi-vidual with privileged access decides to turn against the organization and there are no preventive or detective controls in place within the organization.

2. Sniffing Dengan Wireshark

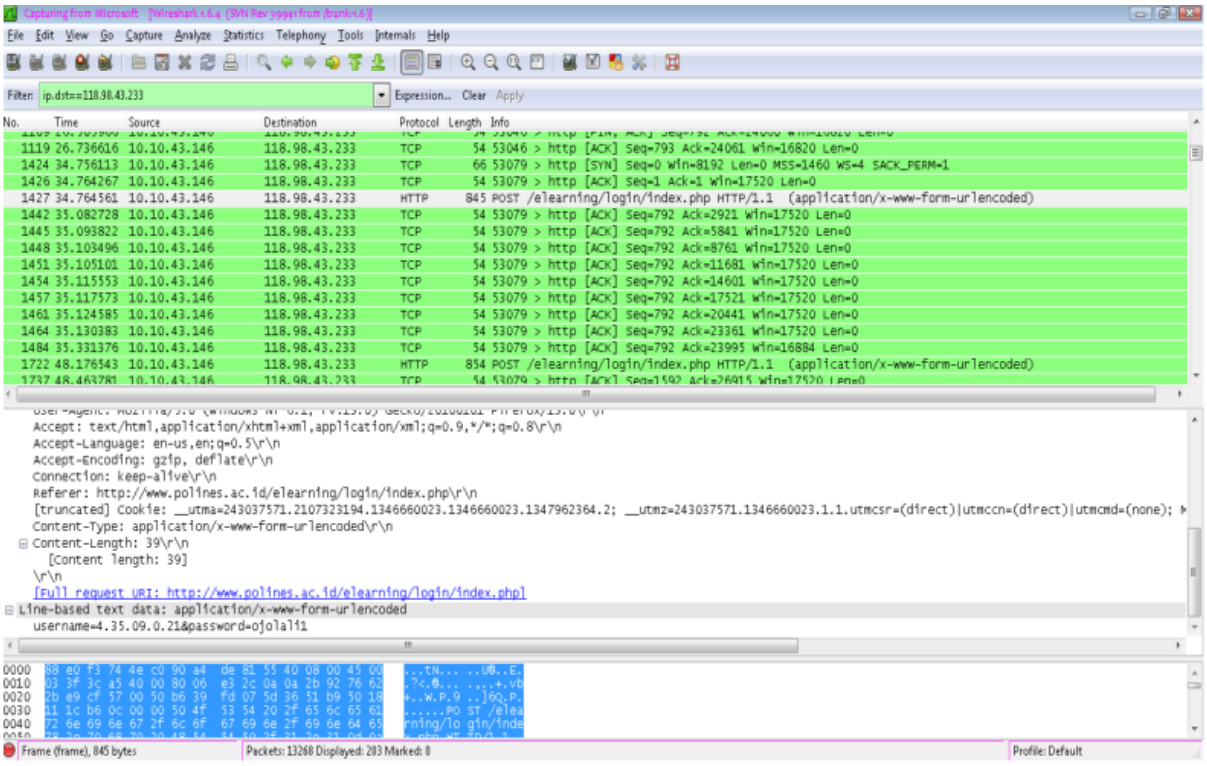
Tampilan awal wireshark adalah sebagai berikut.



Pilih salah satu interface yang akan ditampilkan, misalnya pilih interface bawaan microsoft yang paling atas. Maka akan muncul tampilan seperti ini.



Untuk melakukan sniffing caranya adalah login ke sebuah situs yang membutuhkan username dan password sambil menjalankan wireshark. Lalu ping ke alamat tersebut melalui command prompt, misal saya masuk ke situs **elearning polines** maka saya tulis di command prompt **"ping www.polines.ac.id/elearning"**. Akan muncul ip address dari alamat tersebut. Ip address itulah yang dimasukkan ke filter. Dan lalu lintas paket yang menyangkutpautkan ip address tersebut akan langsung terlihat seperti ini.



Lalu cari paket yang jenisnya HTTP dengan tipe POST. Klik dan akan muncul informasi di bawah berupa username dan password yang telah dimasukkan tadi.