UJIAN AKHIR SEMESTER GANJIL TA 2020/2021

IT FORENSIK

Disusun Oleh:

Rizky Yamanashi Pradana

311610032

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS PELITA BANGSA

BEKASI

2020

1. Video tentang : Tutorial metasploit dan wireshark 2020

   Link : https://youtu.be/Oonf5riFF2Y

   Penjelasan : Metasploit merupakan *software security* yang sering digunakan untuk menguji coba ketahanan suatu sistem dengan cara mengeksploitasi kelemahan *software* suatu sistem. Pada video tersebut adalah metasploit payload. Payload adalah bagian dari perangkat lunak yang memungkinkan pelaku mengendalikan sistem komputer setelah sudah dieksploitasi. Contohnya pada video tersebut pelaku mengirim file atau folder apapun, karena korban tersebut berada dijaringan yang sama. Jadi hati – hati ketika kalian memasuki jaringan bersifat publik. Wireshark merupakan salah satu tools atau aplikasi "Network Analyzer" atau Penganalisa Jaringan. Penganalisaan Kinerja Jaringan itu dapat melingkupi berbagai hal, mulai dari proses menangkap paket-paket data atau informasi yang berlalu-lalang dalam jaringan, sampai pada digunakan pula untuk sniffing (memperoleh informasi penting seperti password email, dll). Wireshark sendiri merupakan free tools untuk Network Analyzer yang ada saat ini. Dan tampilan dari wireshark ini sendiri terbilang sangat bersahabat dengan user karena menggunakan tampilan grafis atau GUI (Graphical User Interface).

2. Video tentang : Sniffing dengan Wireshark

   Link : https://youtu.be/9Dj-CRrVGqM

   Penjelasan : Sniffing adalah tindak kejahatan penyadapan yang dilakukan menggunakan jaringan internet dengan tujuan utama untuk mengambil data dan informasi sensitive secara *illegal*. Cara kerja sniffing adalah ketika Anda terhubung ke jaringan yang bersifat publik, saat Anda melakukan proses transfer data dari client server dan sebaliknya. Karena data yang mengalir pada *client* dan *server* yang bersifat bolak-balik, sniffing ini akan menangkap paket-paket yang dikirimkan dengan cara illegal menggunakan tools pembantu.

3. Video tentang : Mengubah Tampilan Kolom Wireshark

   Link : https://youtu.be/9Xa_mD7MCz4

   Penjelasan :

   Wireshark default column adalah berikut ini :

   a. No. Frame number from the beginning of the pcap. The first frame is always
   b. Time - econds broken down to the nanosecond from the first frame of the pcap. The first frame is always 0.000000.

c. Source - Source address, commonly an IPv4, IPv6, or Ethernet address.
d. Destination - Destination address, commonly an IPv4, IPv6, or Ethernet address.
e. Protocol - P rotocol used in the Ethernet frame, IP packet, or TCP segment (ARP, DNS, TCP, HTTP, etc.).
f. Length - Length of the frame in bytes.

Diubah menjadi berikut ini

a. Date & time in UTC
b. Source IP and source port
c. Destination IP and destination port
d. HTTP host
e. HTTPS server
f. Info