# Forensik Jaringan (Network Forensic)

## Server, Email, Log

Pengantar Komputer Forensik Teknologi Informasi

UNIVERSITAS GUNADARMA
Fakultas Teknologi Industri
Jurusan Teknik Informatika

# Pendahuluan

* Ketika suatu mekanisme keamanan gagal menangani dan mengidentifikasi adanya serangan secara cepat,
* Diperlukan suatu pelengkap pada sistem keamanan yang dapat memonitor
* Menangkap dan menyimpan bukti digital
* Diperlukan mekanisme forensik pada jaringan sehingga bukti-bukti yang dibutuhkan untuk analisa lebih lanjut tidak hilang atau berubah

# Pendekatan Keamanan Sistem

* Avoidance :
  * menggunakan mekanisme proteksi seperti firewall, VPN, enkripsi dan mekanisme autentikasi
* Intrusion Detection
  * mendeteksi percobaan intrusi menggunakan audit file log dan IDS.
* Security Investigation
  * mengumpulkan informasi yang diperlukan untuk melakukan investigasi dari kerusakan ketika pelanggaran keamanan terjadi

# Forensik Jaringan (Network Forensic)

* Sistematis pelacakan lalu lintas masuk dan keluar
* Memastikan bagaimana serangan dilakukan
* Bagaimana suatu peristiwa terjadi pada jaringan
* Menentukan penyebab dari lalu lintas normal
  * Internal bug
  * Attackers

# Forensik Jaringan (Network Forensic)

* Metode menangkap
* Metode menyimpan dan analisis data penggunaan jaringan (log analisis)
* Untuk menemukan sumber dari pelanggaran keamanan sistem atau masalah keamanan informasi (tracking)

# Fokus utama Forensik Jaringan

* Mengidentifikasi semua kemungkinan yang dapat menyebabkan pelanggaran keamanan sistem
* Membuat mekanisme pendeteksian
* Pencegahan yang dapat meminimalisir kerugian yang lebih banyak

# Proses Forensik Jaringan

* Monitoring dan koleksi data
  * pada dasarnya adalah audit terhadap penggunaan jaringan, seperti traffik, bandwidth dan isi data
* Analisa isi data
  * mendeteksi data mana saja yang menggangu keamanan sistem
* Source traceback
  * metode untuk mengetahui sumber dari serangan

# Hal-hal yang dicurigai pada jaringan




# Paket Yang Dicurigai

* Diperlukan kemampuan untuk mengidentifikasi jenis paket yang berbeda sesuai dengan beragamnya Internet Protocol
* Misalnya :
  * Email (POP3, SMTP and IMAP)
  * Web Mail (Yahoo Mail, Gmail, Hotmail)
  * Instant Messaging (Windows Live Messenger, Yahoo, ICQ )
  * FTP
  * Telnet
  * HTTP
  * VOIP

# Mendeteksi Penyusupan

* Dilakukan dengan menggunakan Intrution Detection System (IDS)
* Jenis IDS
  * Network-based IDS
  * Host-based IDS
* Sensor dipasang di titik tertentu
* Aturan (rules) dibuat sesuai dengan definisi dari jenis penyusupan yang dapat terjadi
  * Misal, definisikan anomali di jaringan

# Output IDS

* Menunjukkan adanya penyusupan atau pelanggaran aturan (rules)
* Memilah informasi yang masuk
* Menjadi jejak untuk melakukan investigasi lebih lanjut

# Memahami Paket

```
root# tcpdump -n -i lo0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo0, link-type NULL (BSD loopback), capture size 96 bytes
03:46:22.758381 IP 127.0.0.1 > 127.0.0.1: ICMP echo request, id 204, seq 0, length 64
03:46:22.758450 IP 127.0.0.1 > 127.0.0.1: ICMP echo reply, id 204, seq 0, length 64
03:46:23.758607 IP 127.0.0.1 > 127.0.0.1: ICMP echo request, id 204, seq 1, length 64
03:46:23.758674 IP 127.0.0.1 > 127.0.0.1: ICMP echo reply, id 204, seq 1, length 64
```

# Packet Capture / Dump

*Beberapa contoh aplikasi 'PaketCapture' antara lain:*

* *tcpdump, wireshark, tshark*
  * Tangkap paket dan simpan dalam file
  * Ada koleksi *packet dump* (dari berbagai kegiatan, seminar, kumpulan hacker)
* *tcpreplay*
  * Memainkan ulang paket di jaringan

# TCPdump

* Tools untuk menganalisa packet
* Tersedia source code (untuk sistem UNIX)
  * http://www.tcpdump.org
* Ada *WinDump* untuk MS Windows
  * http://windump.polito.it/
  * Harus pasang *WinPcap* yang dapat diperoleh dari situs yang sama

# *TCP flags* di tcpdump

Berikut istilah yang dipakai dalam TCPdump:

* SYN “S”
* ACK “ack”
* FIN “F”
* RESET “R”
* PUSH “P”
* URGENT “urg”
* Placeholder “.”

# Contoh TCPdump Output

```
09:32:43:910000 nmap.edu.1173 > dns.net.21: S
  62697789:62697789(0) win 512
```

* `09:32:43:910000`: Time stamp
* `nmap.edu`: Source host name
* `1173`: Source port number
* `>` tanda arah paket
* `dns.net`: Destination host name
* `21`: Destination port number
* `S`: TCP flag
* `62697789:62697789(0)`: TCP sequence number begin:end (data bytes)
* `win 512`: Receiving TCP buffer size (in bytes) of nmap.edu

# Sumber Data Lain

* Data dari IDS belum cukup untuk menarik kesimpulan mengenai terjadinya penyusupan
* Dibutuhkan sumber data lainnya
  * Log dari perangkat jaringan lainnya (router)
  * Log dari server yang menjadi sasaran, misal data syslog, log web server
  * Catatan di komputer penyusup (bila bisa diperoleh)
  * Catatan daftar kehadiran

# Analisis

* Melakukan korelasi terhadap berbagai data
* Membuat *time line* beserta fakta
  * Kadang sulit sinkronisasi waktu
* Membuat beberapa skenario
* Melakukan analisis
* Mengambil beberapa kesimpulan

# Langkah Berikutnya

* Penyusup masuk menuju atau melalui jaringan untuk terhadap sebuah server (komputer)
* Penyusup menggunakan komputer untuk melakukan kegiatannya
* Ada banyak data dari komputer yang dapat dimanfaatkan untuk membangun kasus penyidikan

# Contoh Analysis Intrusion

* IOS Vulnerabilities
  * Menganalisa kelemahan pada sistem operasi
* Running v/s Startup configurations
  * Menganalisa konfigurasi
* Logging
  * Menganalisa log aktifitas sudah terjadi pada sistem
* Timestamps
  * Menganalisa waktu dimana sebuah event tertercatat oleh sistem atau komputer

# Logging

* Console Logging
  * Akan melakukan capture dengan cara merekam session
* Buffer Logging
  * Jika buffer logging dalam kondisi ON, maka dengan menggunakan perintah untuk menampilkan log di router,
  * akan memunculkan level logging yang sedang berjalan, dan kepada host logging mana akan dikirimkan

# Logging

* Terminal Logging
  * Mengijinkan non console sessions untuk menampilkan pesan
* Syslog Logging
  * Jika dalam kondisi ON, maka mengirimkan pesan kepada syslog server
* SNMP logging
  * Jika dalam kondisi ON, maka SNMP traps dapat dikirimkan kepada sebuah logging server

# Forensik Email

* *Store-and-forward Architectures* memungkinkan pesan yang akan shuttled melalui serangkaian sistem intermediate
* *Human-readable Message Headers* menunjukkan jalur antara pengirim dan penerima
* Investigasi memerlukan informasi logging  yang ditransmisikan setiap host pesan
* *Client-based E-mail* (program yang diinstal pada client) vs *Web-based E-mail* (online email menggunakan browser)

# Internet Standards (RFCs)

RFC – (Request for Comment)

- Standards for Internet Protocols

RFC 2821

- Simple Mail Transfer Protocol (SMTP)
- Berfungsi untuk mentransfer email dengan efisien dan handal.
- Sebuah email mungkin saja melewati beberapa gateway sepanjang perjalanan dari pengirim hingga sampai ke penerima

# Tracking e-mail

* Microsoft Outlook, Eudora, dan Mozilla Thunderbird adalah perangkat lunak berbasis jaringan yang ditujukan untuk berinteraksi dengan server untuk e-mail
* Biasanya untuk berinteraksi dengan dua server yang berbeda
  * satu untuk surat masuk
  * surat keluar satu untuk

# Tracking e-mail

* Email komersial sistem menggunakan format proprietary untuk menyimpan e-mail
* Misalnya, Outlook menggunakan file dengan extention *.pst,
* Outlook Express dbx.,. atau  MDX dan. idx
* Penampil teks sederhana tidak akan bekerja

# Implikasi Forensik

* Pengguna POP mail selalu menggunakan mesin lokal untuk arsipe-mail
* Email dengan protokol mail user lain, mungkin menyimpan email mereka di server
* Pada lingkungan perusahaan, lebih memilih untuk memiliki mail server sendiri dari pada server email internet umum untuk memudahkan investigasi

# Implikasi Forensik

* Commercial tools termasuk membungkus seperti Guidance's EnCase, AccessData's FTK, and Paraben's e-mail Examiner
* Akan banyak sekali data email untuk diselidiki, sehingga alat bantu (tools) pengindeksan dan pencarian menjadi sangat penting

# Pengiriman Email

* Menggunakan SMTP RFCs 821 and 1869
  * Pembacaan email memerlukan otentikasi (username & password)
  * Mengirimkan email terkadang tidak membutuhkan otentikasi
  * Pengiriman email dari sumber A ke penerima B, umumnya menggunakan MTA (Mail Transfer Agent), server lain yang merelay pesan dan dimana informasi Log disimpan

# Hacking Pengiriman Email

* Secara manual mengirim email dengan cara mengkoneksikan port 25 SMTP dengan menggunakan telnet
* Pesan tertulis pada mail header

# Contoh Telnet

```
[frodo]# telnet localhost 25
Trying 127.0.0.1 …
Connected to frodo.com. 220 frodo.com ESMTP Sendmail <version> <date>
helo
250 OK
mail from: witch@forensics.com
250 witch@forensics.com… Sender ok
rcpt to: yourself@yoursystem.com
250 yourself@yoursystem.com.. Recipient ok
data
354
This is a spoofed message
.
250 RAA<numbers> Message accepted for delivery
quit
221 frodo.com closing connection
Connection closed by foreign host
```

# RFC Identification Fields

* Meskipun bersifat opsional, setiap pesan pasti memiliki sebuah field “Message-ID”
* Message-ID menyediakan sebuah “message identifier” yang mengacu pada versi tertentu dari suatu pesan
* “message identifier” ditujukan untuk dibaca oleh mesin dan tidak ditujukan untuk manusia
- Bentuk formula Message-ID

  *<date/time integer.unique_id.domain>*

# Authentic Message-ID String

* Berbentuk hexadesimal sehingga harus dikonfersi menjadi desimal agar dapat terbaca manusia
* Contoh:
* 3989F5A3.87BDEEE2@tech.com
* 3989F5A3 = hexadecimal
* 965342627 = decimal
* Aug 3, 2000 18:43 = Date & Time (+1 hour logs)

# Kesimpulan

* Forensik Jaringan Server
* Mengenali Tipe Paket dan Protokol
* Menangkap Paket Data
* Investigasi terhadap Log
* Inversitasi terhadap Email

# Terima Kasih

Universitas Gunadarma