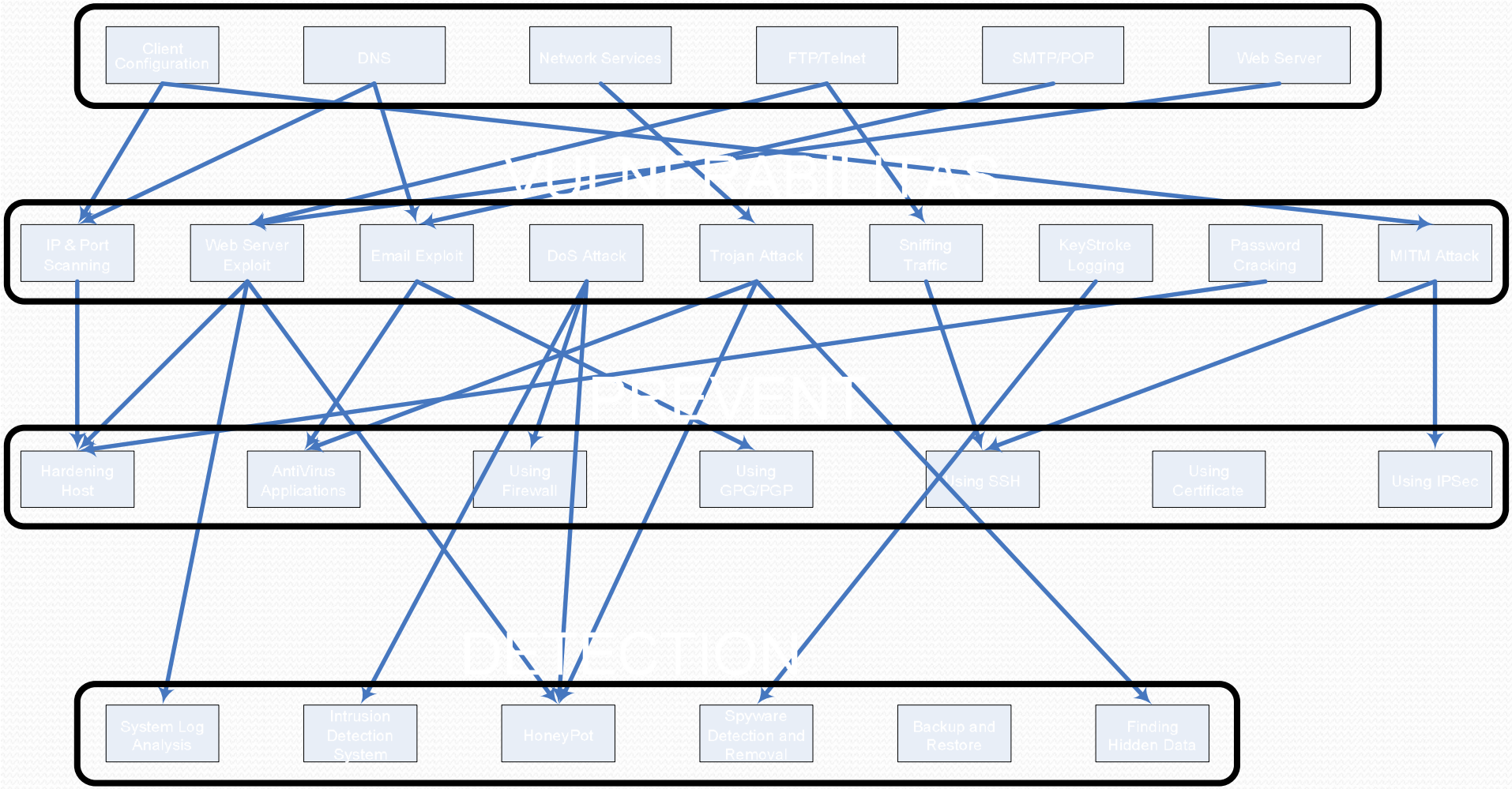
SILABUS

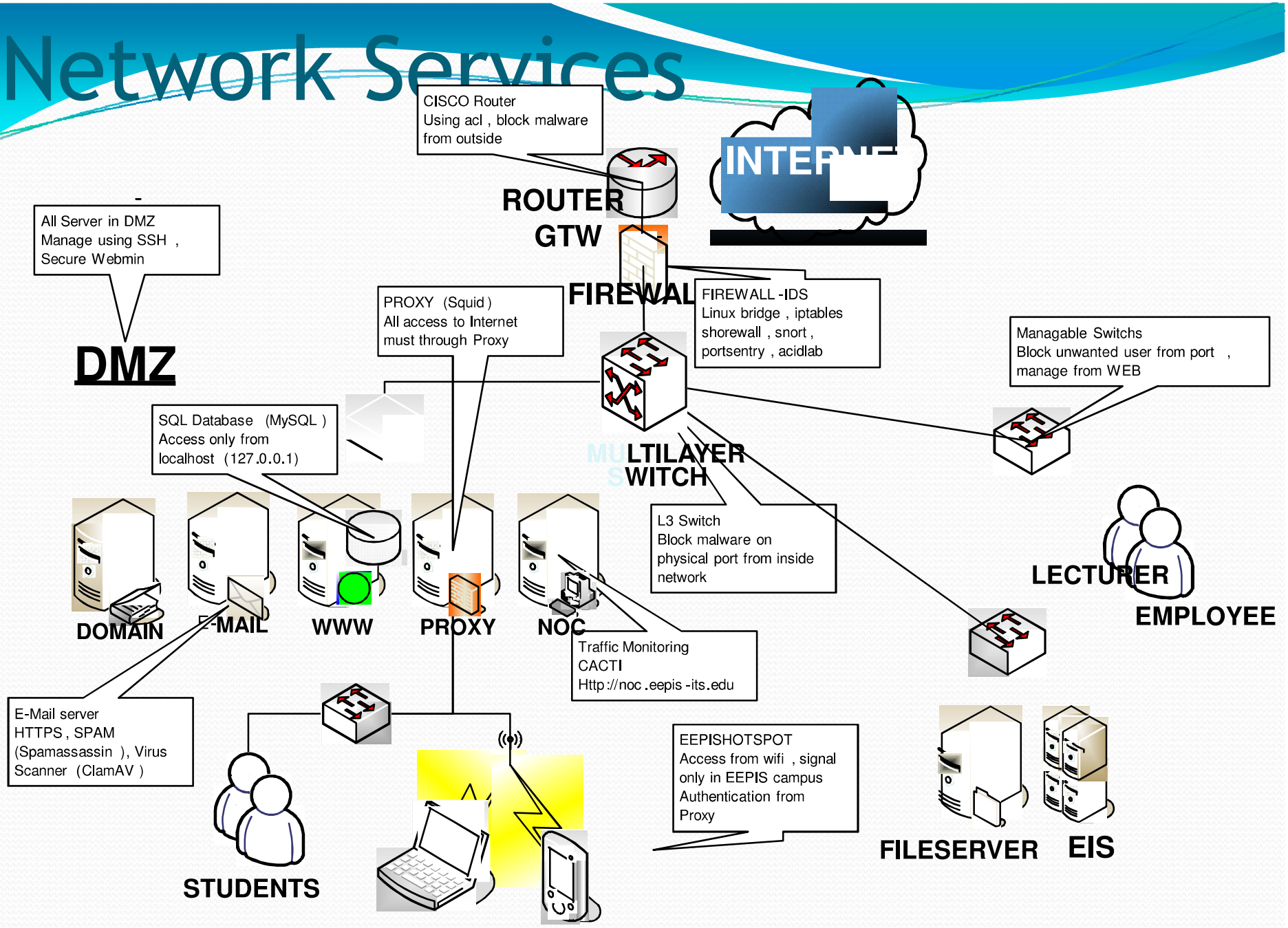
PERTEMUAN

1. Introduksi
2. Pendekatan Analisis Sistem untuk Teknologi Informasi
3. Sekuriti sebagai sebuah Proses
4. Memahami Cara Sistem Network Berkomunikasi
5. Sekuriti Topologi
6. Firewall
7. TTS
8. Intrusion Detection System (IDS)
9. Otentikasi dan Enkripsi
10. Digital Signature
11. Virtual Private Networking
12. E-Mail Server Security
13. Wireless Security
14. TAS

NETWORK SECURITY IN ACTION

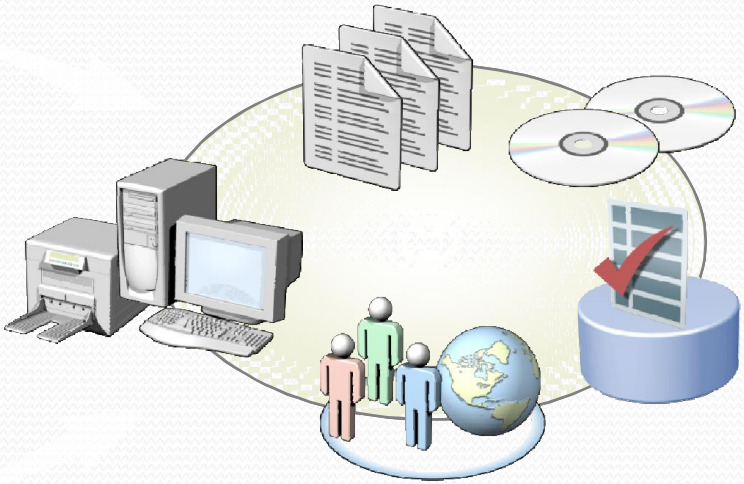


Network Services



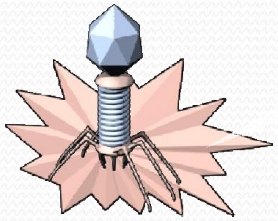
WHY SECURE NETWORK ?

Internal attacker

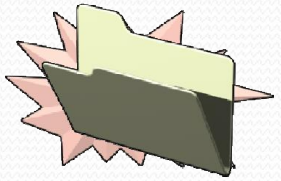


Corporate Assets

External attacker



Virus



Incorrect permissions

- A network security design protects assets from threats and vulnerabilities in an organized manner
- To design security, analyze risks to your assets and create responses

SANS SECURITY THREATS

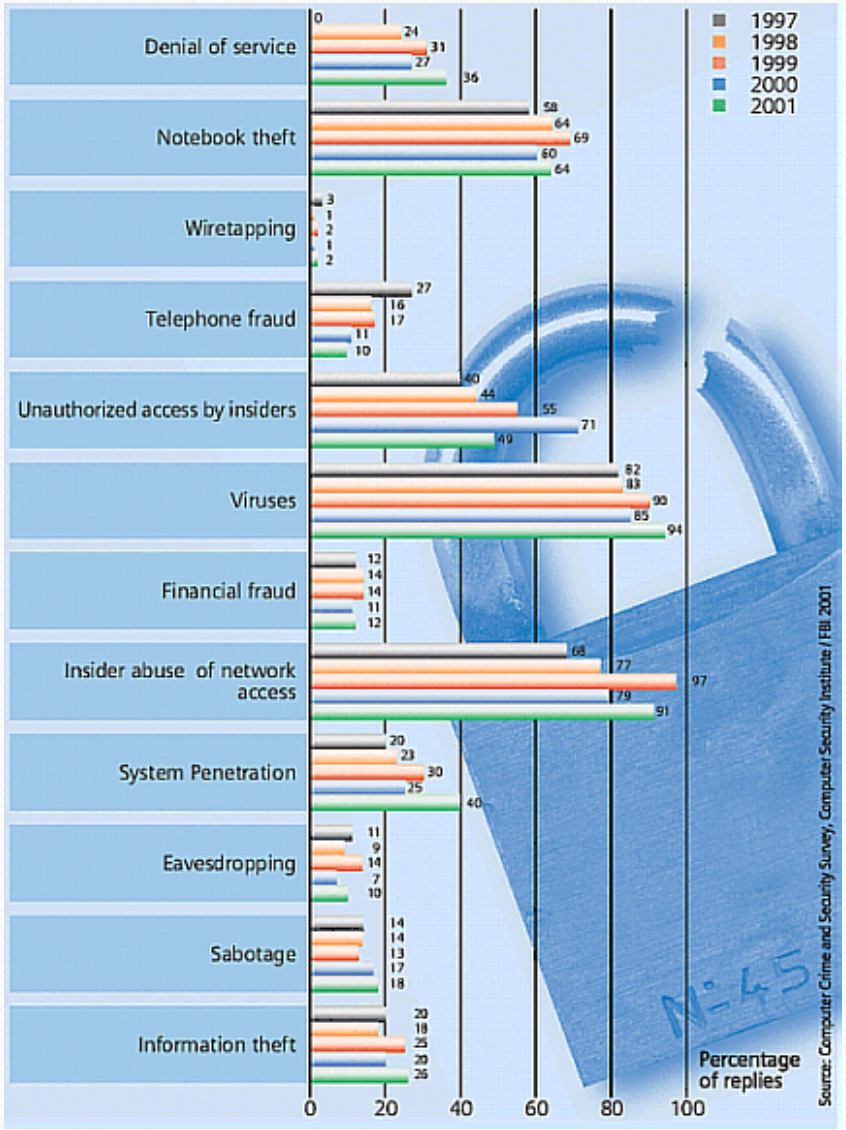
- SANS/FBI top 20 security threats
  - http://www.sans.org/top20/
- Goals attackers try to achieve
  - Gain unauthorized access
  - Obtain administrative or root level
  - Destroy vital data
  - Deny legitimate users service
  - Individual selfish goals
  - Criminal intent

SECURITY STATISTICS: ATTACK TRENDS

- Computer Security Institute (http://www.gocsi.com)
- Growing Incident Frequency
  - Incidents reported to the Computer Emergency Response Team/Coordination Center
  - 1997: 2,134
  - 1998: 3,474 (75% growth from previous year)
  - 1999: 9,859 (164% growth)
  - 2000: 21,756 (121% growth)
  - 2001: 52,658 (142% growth)
  - Tomorrow?

NETWORK ATTACKS – TRENDS

TYPES OF ATTACKS



ATTACK TARGETS

- SecurityFocus
  - 31 million Windows-specific attacks
  - 22 million UNIX/LINUX attacks
  - 7 million Cisco IOS attacks
  - All operating systems are attacked!

HACKERS VS CRACKERS

- Ethical Hackers vs. Crackers
  - Hacker usually is a programmer constantly seeks further knowledge, freely share what they have discovered, and never intentionally damage data.
  - Cracker breaks into or otherwise violates system integrity with malicious intent. They destroy vital data or cause problems for their targets.

PRINSIP KEAMANAN JARINGAN

- Confidentiality

  Protecting information from exposure and disclosure

- Integrity

  Decrease possible problems caused by corruption of data

- Availability

  Make information always available

EXPLOIT

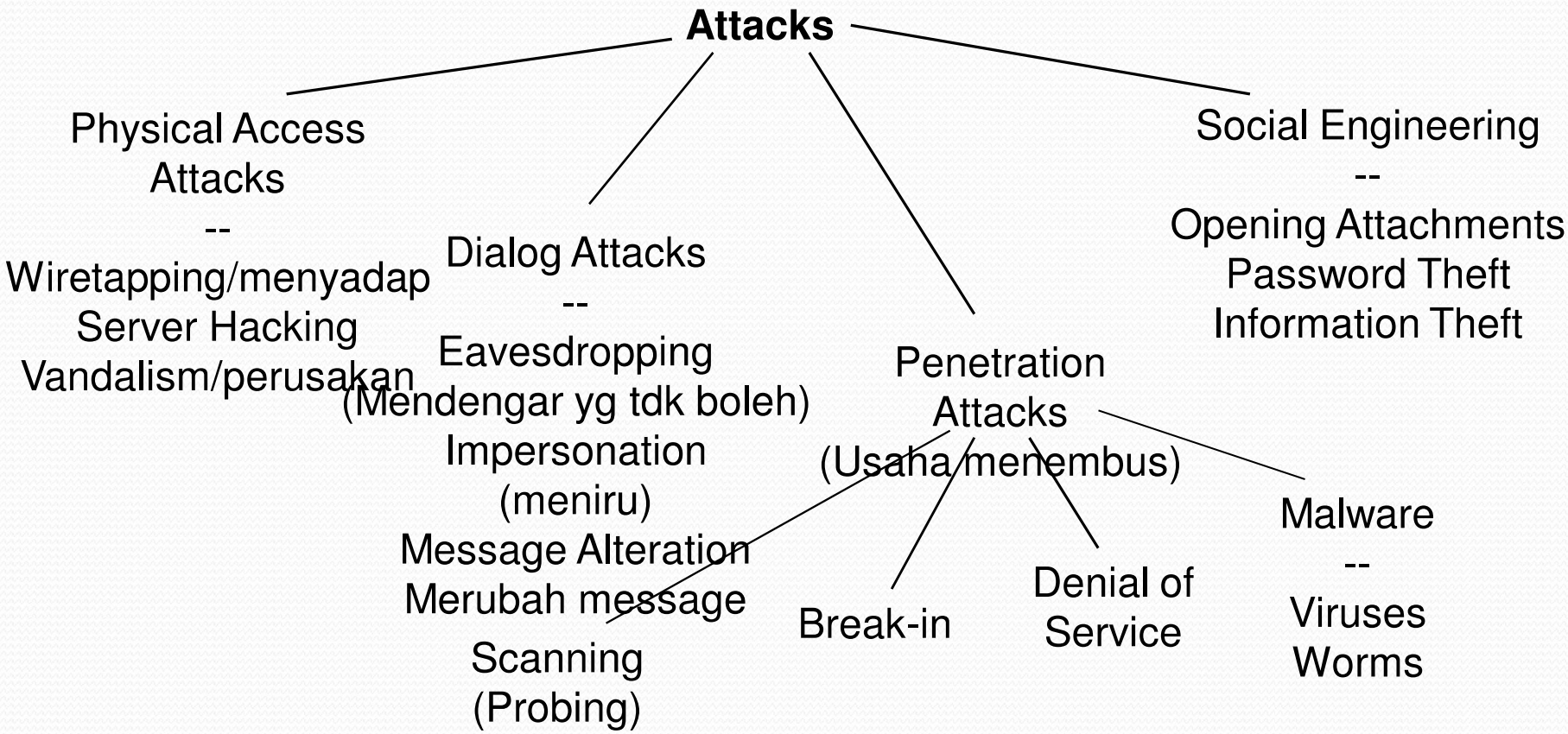
- What is an Exploit?
  - Crackers break into a computer network by exploiting weaknesses in operating system services.
- Types of attacks
  - Local
  - Remote
- Categories of exploits
  - 0-day (new unpublished)
  - Account cracking
  - Buffer overflow
  - Denial of service
  - Impersonation

EXPLOIT

- Categories of exploits (cont.)
  - Man in the middle
  - Misconfiguration
  - Network sniffing
  - Session hijacking
  - System/application design errors

TIPE SERANGAN

MACAM - MACAM SERANGAN



SOCIAL ENGINEERING

- Definisi Social enginering
  - seni dan ilmu memaksa orang untuk memenuhi harapan anda (Bernz),
  - Suatu pemanfaatan trik-trik psikologis hacker luar pada seorang user legitimate dari sebuah sistem komputer (Palumbo)
  - Mendapatkan informasi yang diperlukan (misalnya sebuah password) dari seseorang daripada merusak sebuah sistem (Berg).
- Tujuan dasar social engineering sama seperti umumnya hacking: mendapatkan akses tidak resmi pada sistem atau informasi untuk melakukan penipuan, intrusi jaringan, mata-mata industrial, pencurian identitas, atau secara sederhana untuk mengganggu sistem atau jaringan.
- Target-target tipikal termasuk perusahaan telepon dan jasa-jasa pemberian jawaban, perusahaan dan lembaga keuangan dengan nama besar, badan-badan militer dan pemerintah dan rumah sakit.

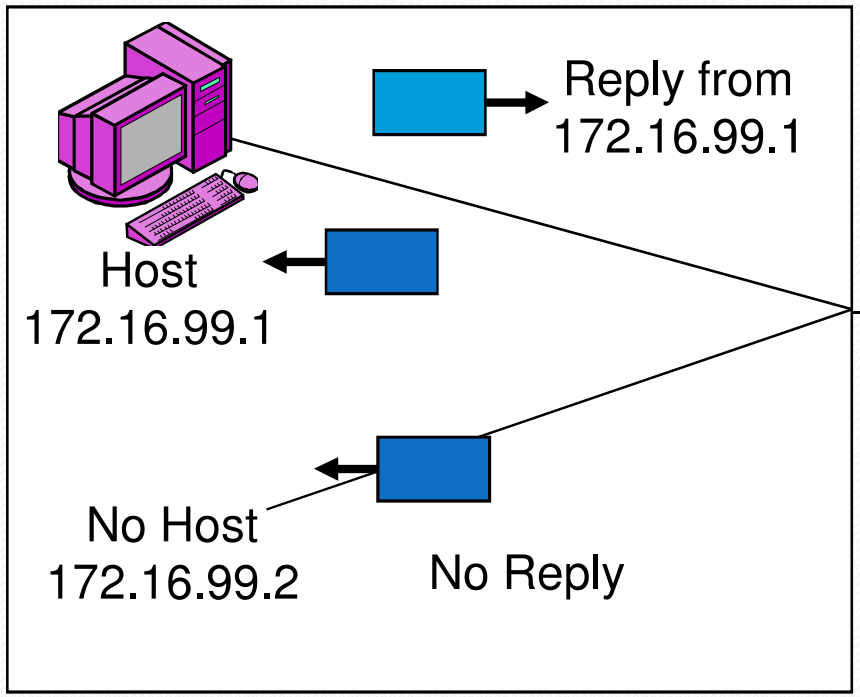
BENTUK SOCIAL ENGINEERING

- Social Engineering dengan telepon
  - Seorang hacker akan menelpon dan meniru seseorang dalam suatu kedudukan berwenang atau yang relevan dan secara gradual menarik informasi dari user.
- Diving Dumpster
  - Sejumlah informasi yang sangat besar bisa dikumpulkan melalui company Dumpster.
- Social engineering on-line :
  - Internet adalah lahan subur bagi para teknisi sosiaal yang ingin mendapatkan password
  - Berpura-pura menjadi administrator jaringan, mengirimkan e-mail melalui jaringan dan meminta password seorang user.
- Persuasi
  - Sasaran utamanya adalah untuk meyakinkan orang untuk memberikan informasi yang sensitif
- Reverse social engineering
  - sabotase, iklan, dan assisting

PENETRATION ATTACKS STEPS

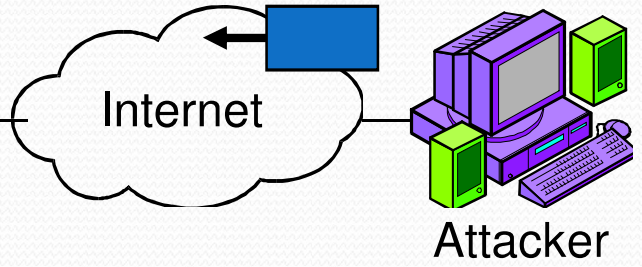
- Port scanner
- Network enumeration
- Gaining & keeping root / administrator access
- Using access and/or information gained
- Leaving backdoor
- Attack
  - Denial of Services (DoS) :Network flooding
  - Buffer overflows : Software error
  - Malware :Virus, worm, trojan horse
  - Brute force
- Covering his tracks

SCANNING (PROBING) ATTACKS



Corporate Network

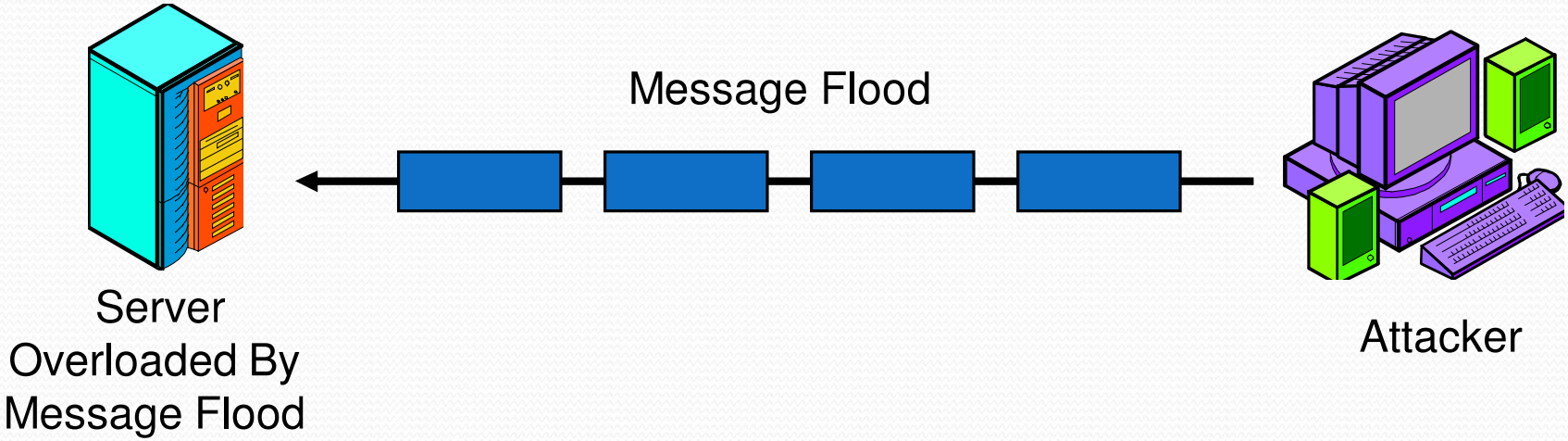
Probe Packets to
172.16.99.1, 172.16.99.2, etc.



Attacker

Results
172.16.99.1 is reachable
172.16.99.2 is not reachable
…

DENIAL-OF-SERVICE (DOS) FLOODING ATTACK

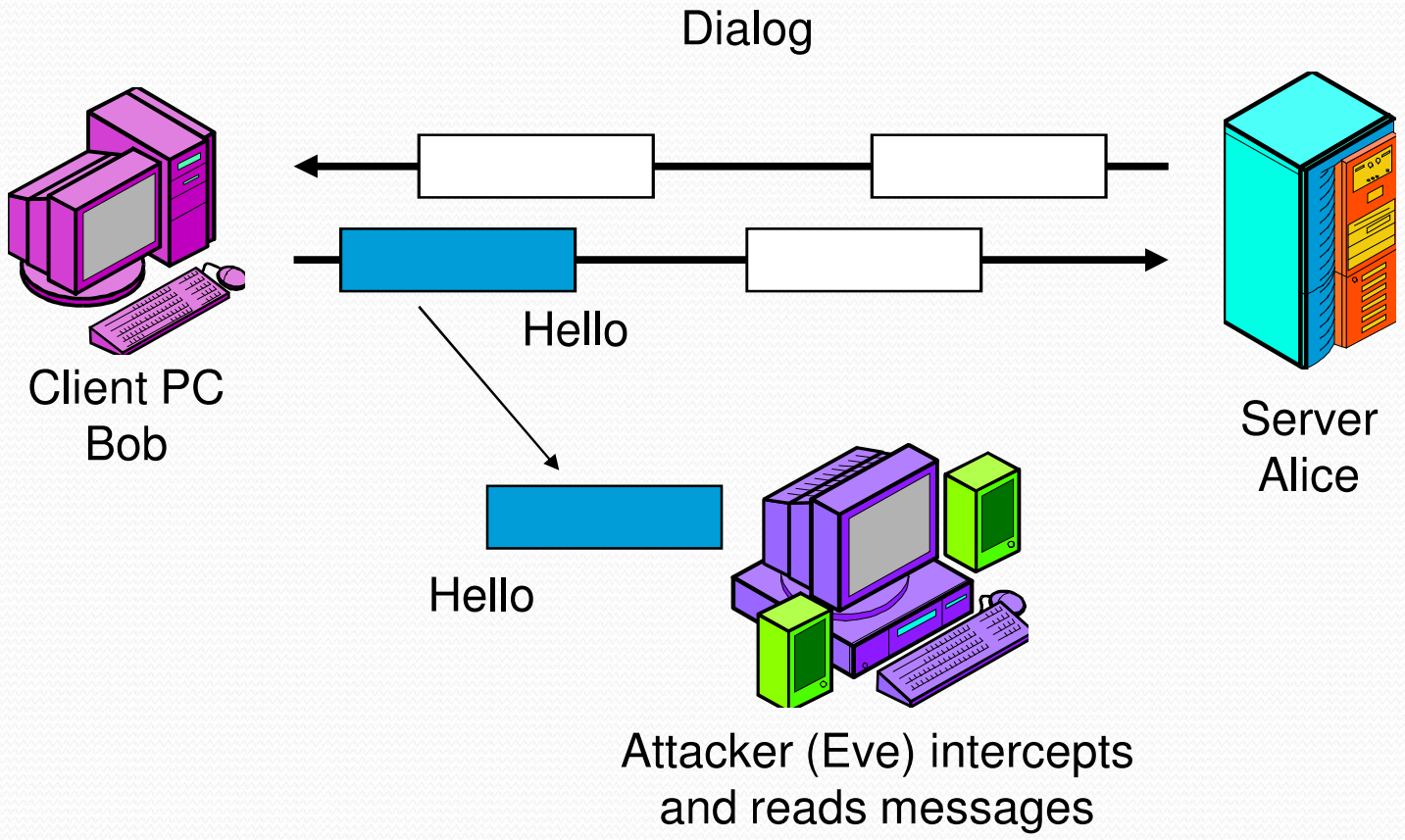


CONTOH D O S

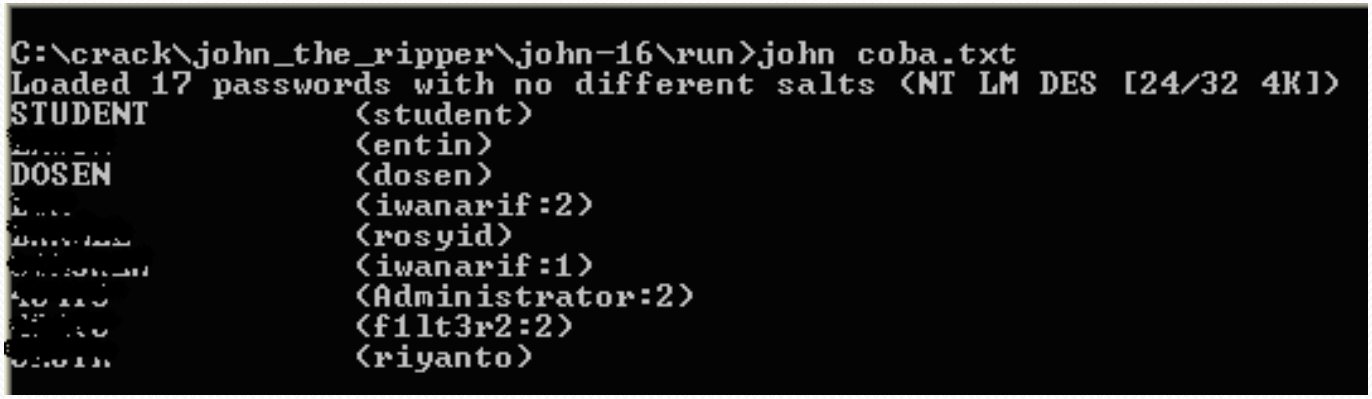
DIALOG ATTACK

- Eavesdropping, biasa disebut dengan spoofing, cara penanganan dengan Enkripsi
- Impersonation dan message alteration ditangani dengan gabungan Enkripsi dan autentikasi

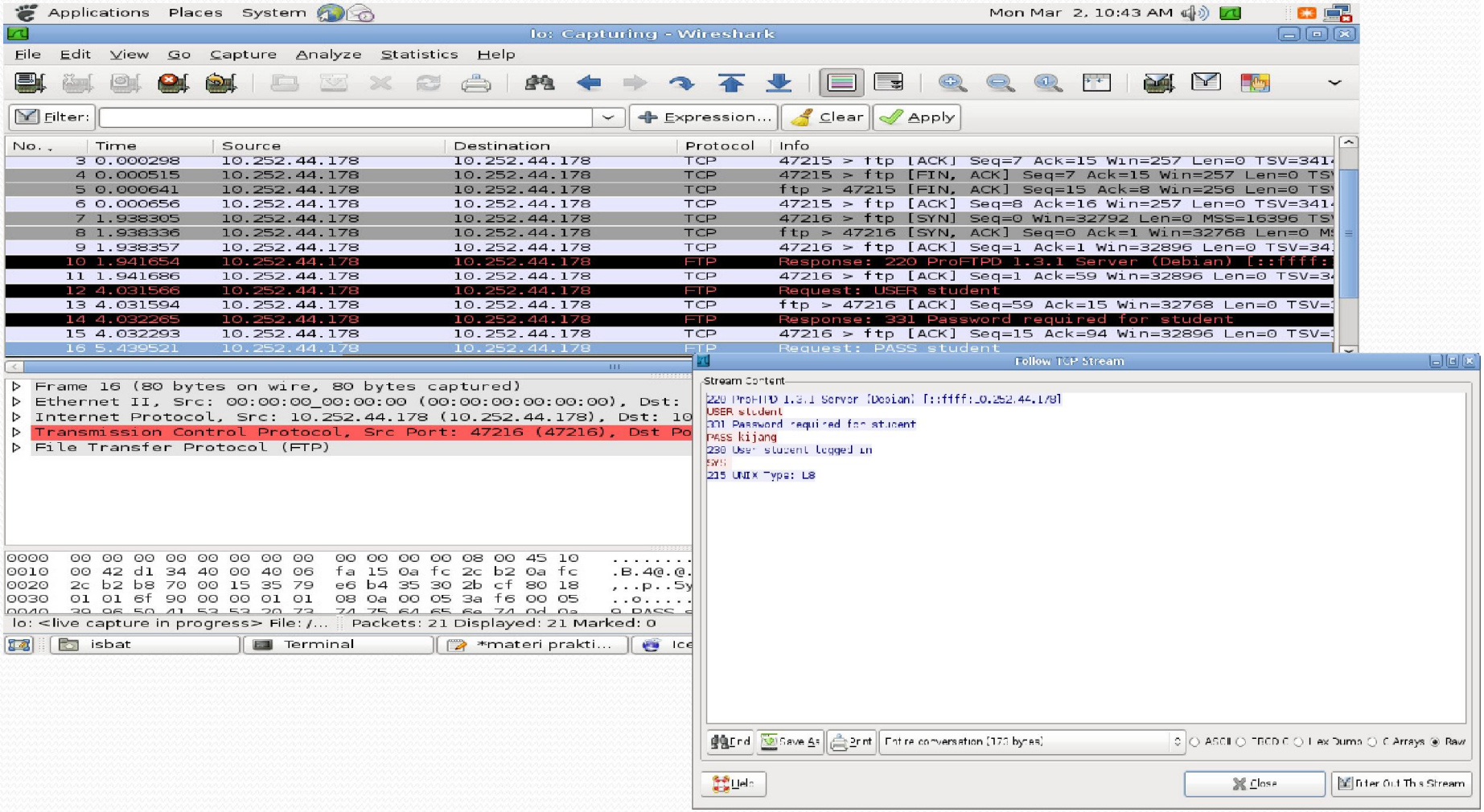
EAVESDROPPING ON A DIALOG



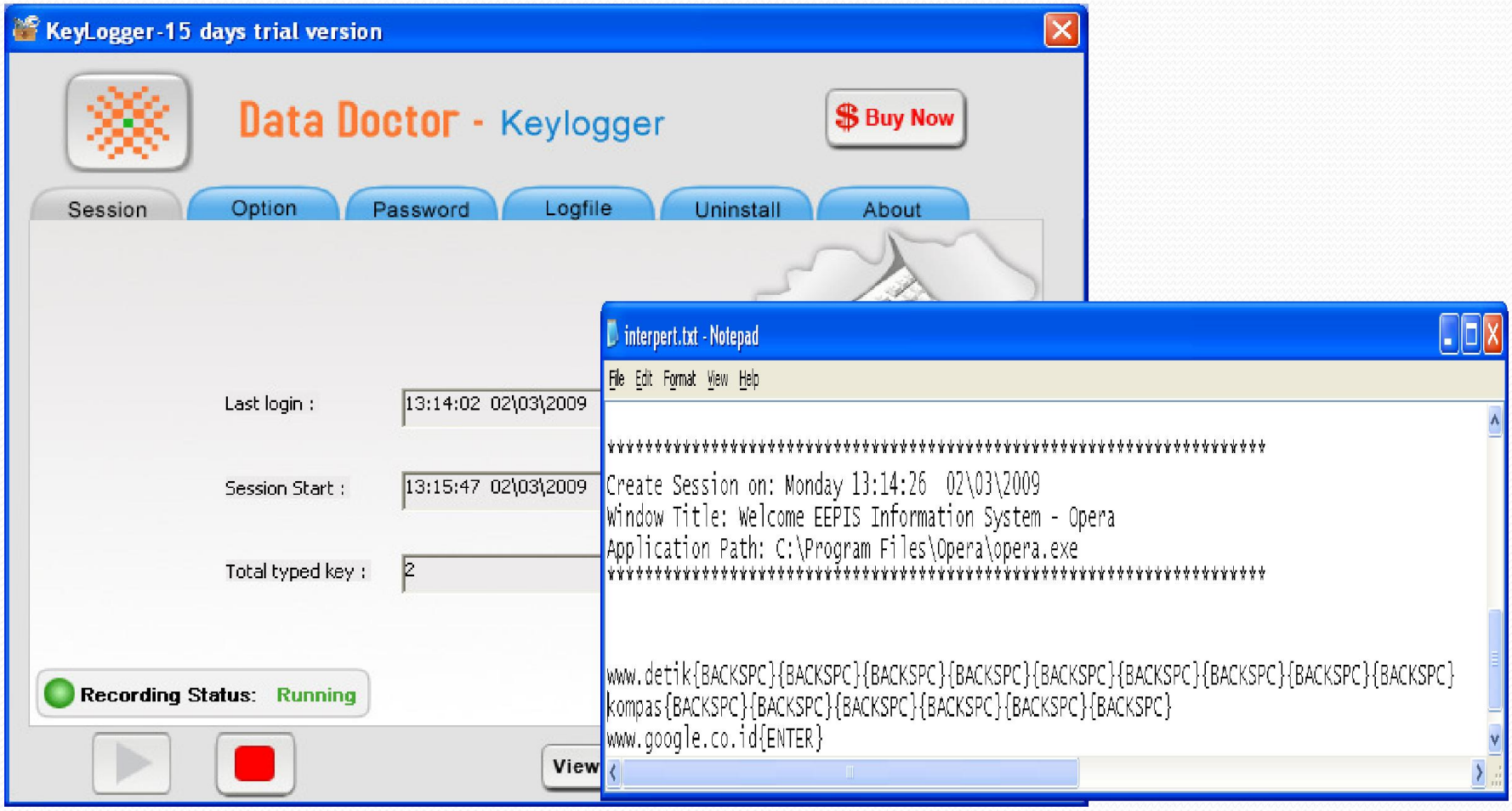
PASSWORD ATTACK BY EXAMPLE



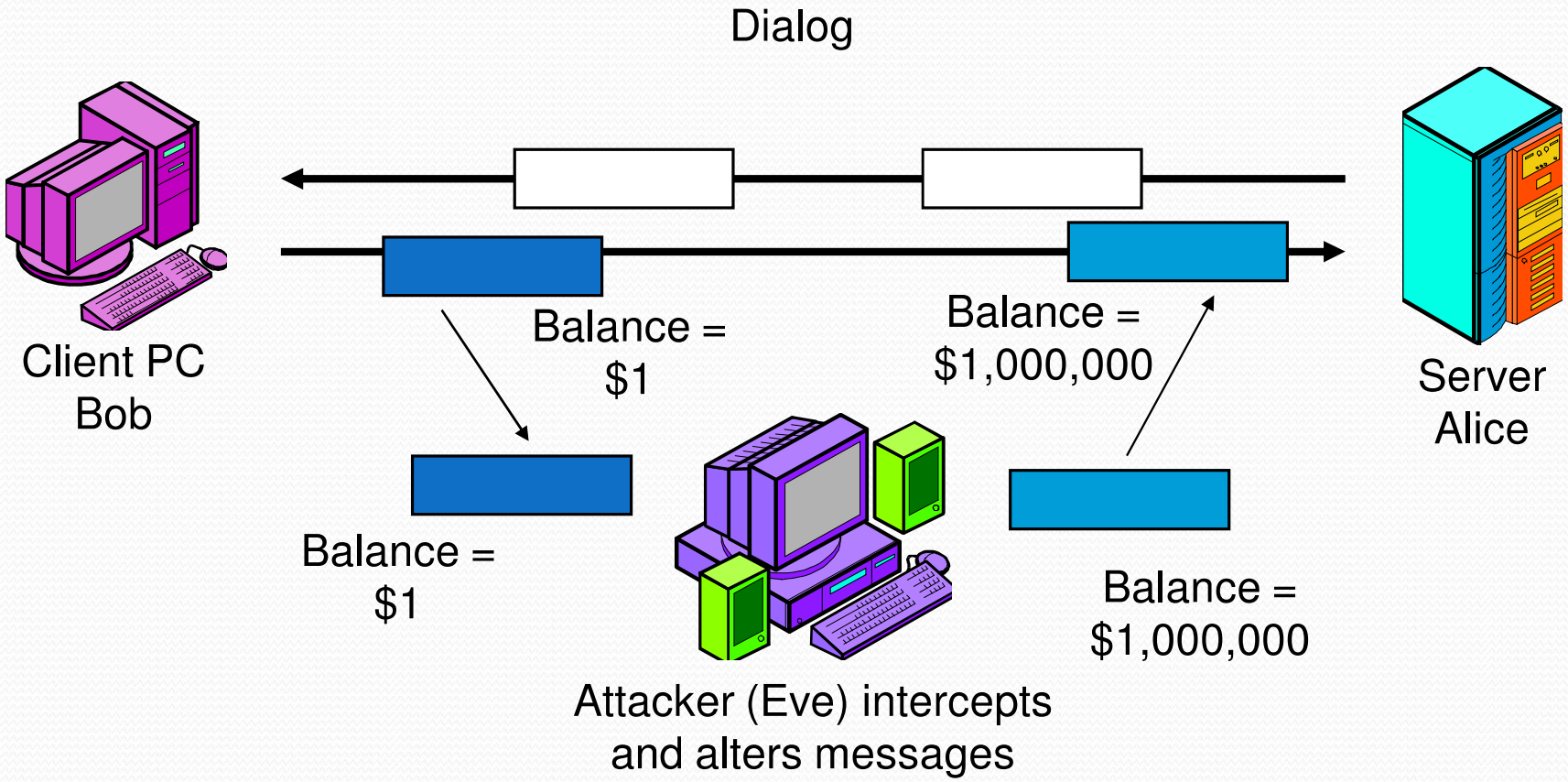
SNIFFING BY EXAMPLE



KEYLOGGER

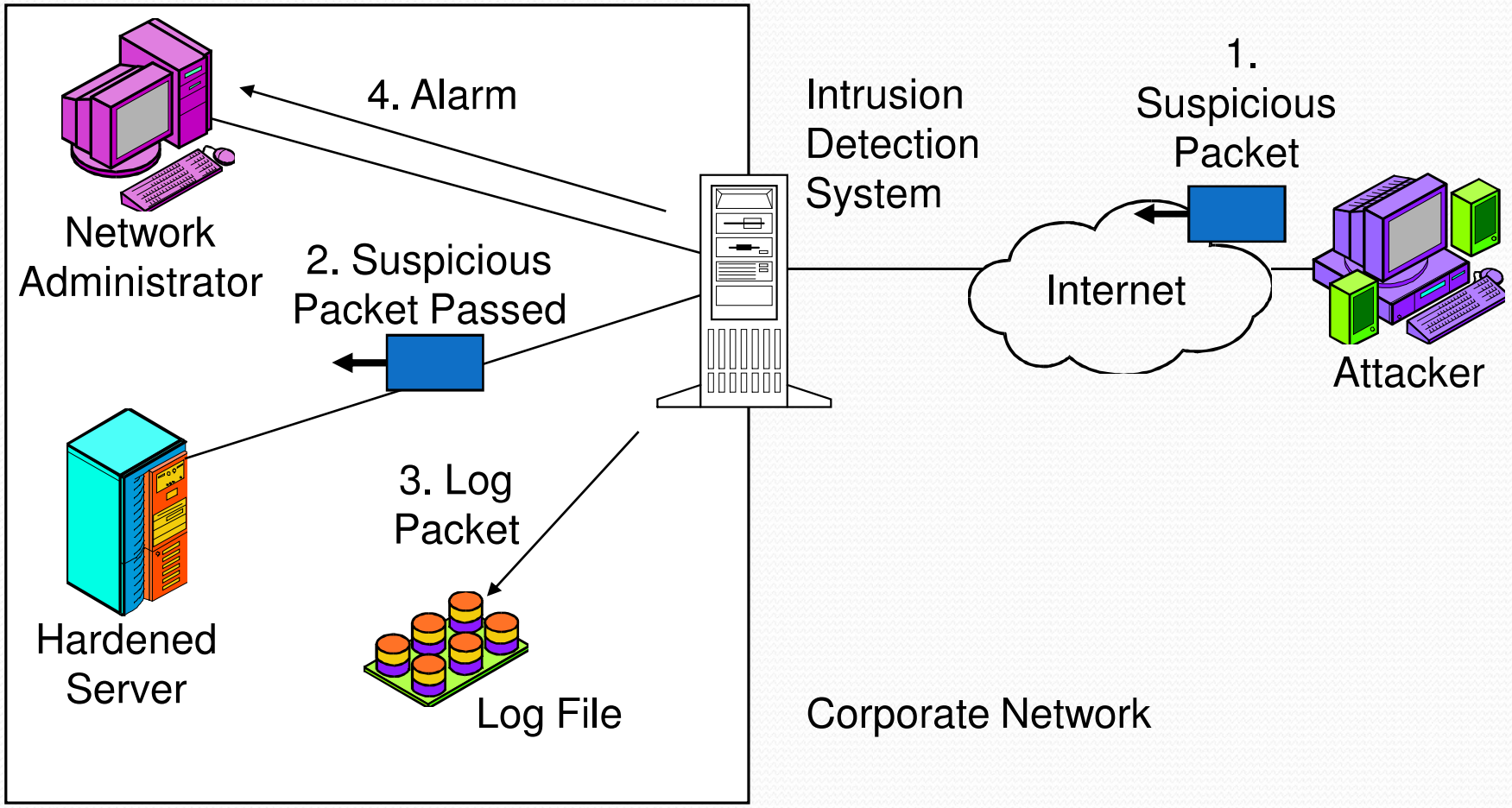

KeyLogger-15 days trial version
Data Doctor - Keylogger
$ Buy Now
Session
Option
Password
Logfile
Uninstall
About
Last login :
13:14:02 02\03\2009
Session Start :
13:15:47 02\03\2009
Total typed key :
2
Recording Status: Running
View
interpert.txt - Notepad
File Edit Format View Help
Create Session on: Monday 13:14:26 02\03\2009
Window Title: Welcome EEPIS Information System - Opera
Application Path: C:\Program Files\Opera\opera.exe
www.detik{BACKSPC}{BACKSPC}{BACKSPC}{BACKSPC}{BACKSPC}{BACKSPC}{BACKSPC}{BACKSPC}{BACKSPC}
kompas{BACKSPC}{BACKSPC}{BACKSPC}{BACKSPC}{BACKSPC}{BACKSPC}
www.google.co.id{ENTER}

MESSAGE ALTERATION

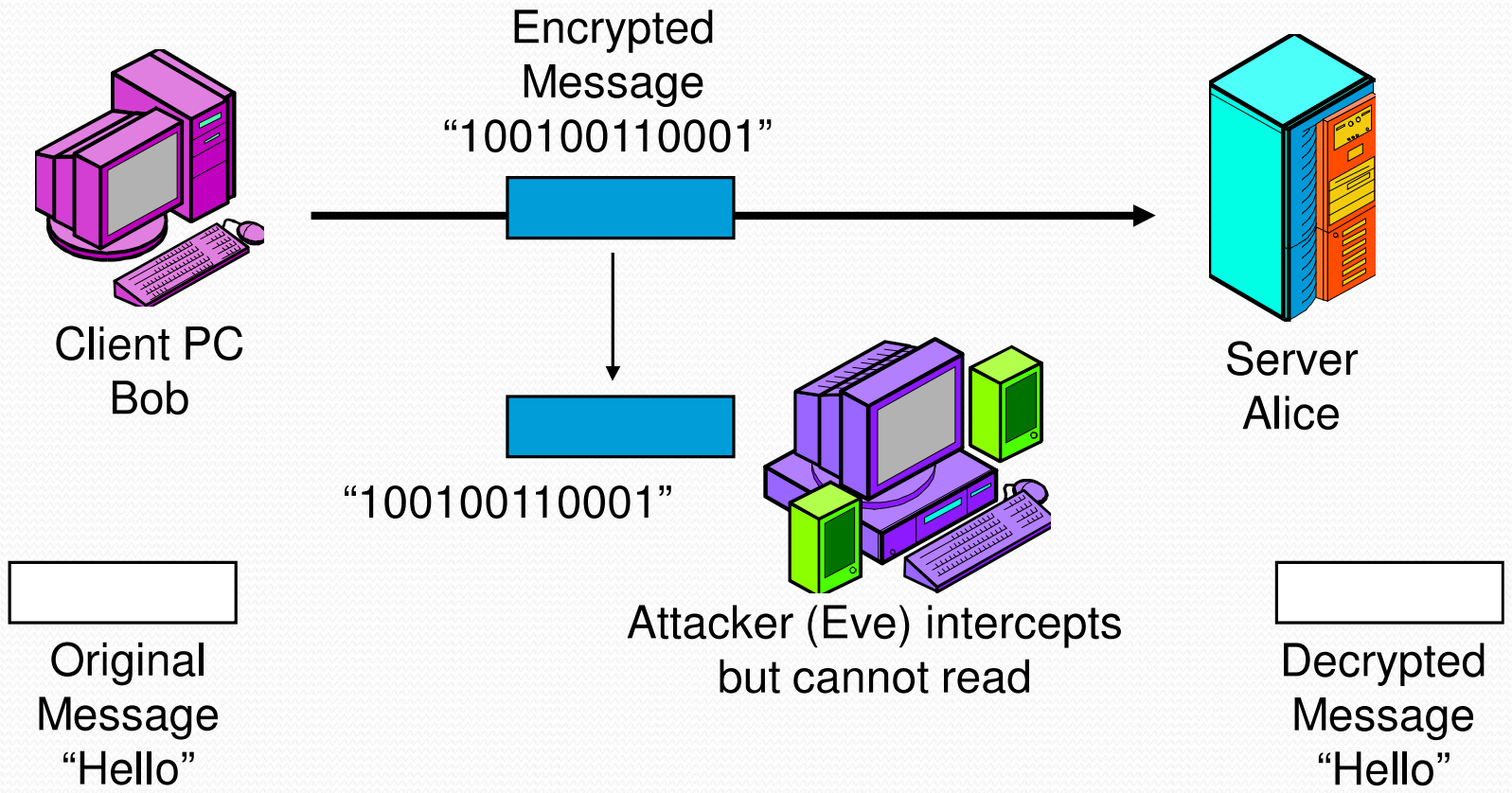


MENGAMANKAN TIPE SERANGAN

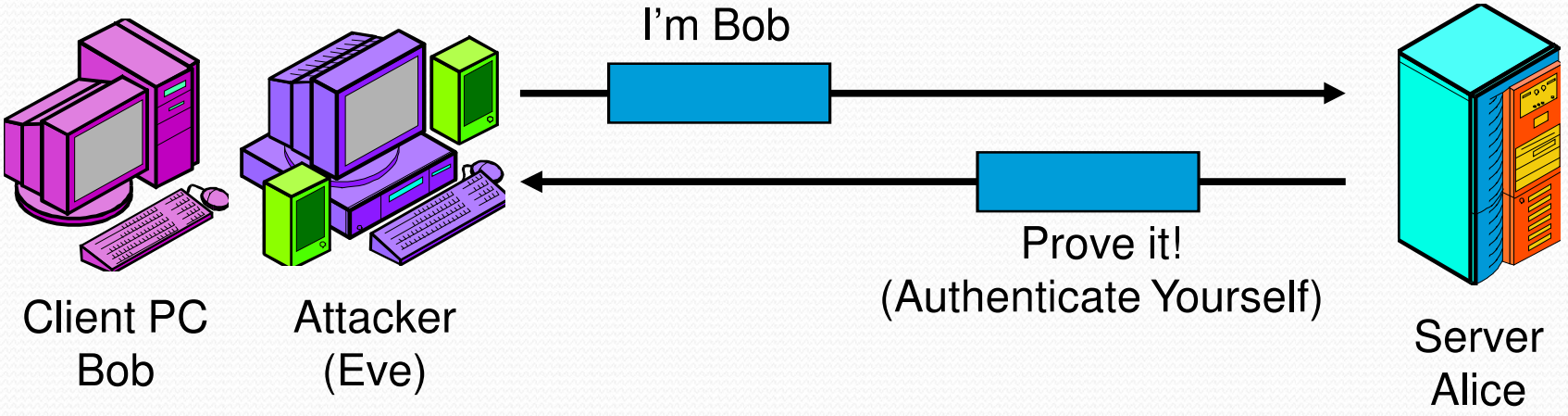
INTRUSION DETECTION SYSTEM



ENKRIPSI UNTUK KERAHASIAAN



AUTENTIKASI MENCEGAH SPOOFING



HARDENING HOST COMPUTER

- The Problem
  - Computers installed out of the box have known vulnerabilities
    - Not just Windows computers
  - Hackers can take them over easily
  - They must be hardened—a complex process that involves many actions

HARDENING HOST COMPUTER

- Elements of Hardening
  - Physical security
  - Secure installation and configuration
  - Fix known vulnerabilities
  - Turn off unnecessary services (applications)
  - Harden all remaining applications
  - (more on next page)

HARDENING HOST COMPUTER

- Elements of Hardening (continued)
  - Manage users and groups
  - Manage access permissions
    - For individual files and directories, assign access permissions specific users and groups
  - Back up the server regularly
  - Advanced protections

- Security Baselines Guide the Hardening Effort
  - Specifications for how hardening should be done
  - Different for different operating systems
  - Different for different types of servers (webservers, mail servers, etc.)
  - Needed because it is easy to forget a step

INSTALLATION AND PATCHING

- Installation Offers Many Options, Some of Which Affect Security
  - For example, in Windows, the NTFS file system is better for security than FAT32
  - Need a security baseline to guide option choices during installation

- Known Vulnerabilities
  - Most programs have known vulnerabilities
  - Exploits are programs that take advantage of known vulnerabilities

- Fixes
  - Work-around: A series of actions to be taken; no new software
  - Patches: New software to be added to the operating system
  - Upgrades: Newer versions of programs usually fix older vulnerabilities.

- Upgrades
  - Often, security vulnerabilities are fixed in new versions
  - If a version is too old, the vendor might stop offering fixes
  - It might be good to wait to upgrade until after the first round of bug and security fixes

TURNING OFF UNNECESSARY SERVICES

- Unnecessary Services
  - Operating system vendors used to install many services by default
  - This made them easier to use. When use changes, services do not have to be turned on.
  - Attackers have found flaws in many of these rare services

- Unnecessary Services
  - Vendors now install fewer services by default—lock down mode
  - Turn to security baseline to see what services to turn on and off
  - Easier to install too few and add than to install too many and remove unwanted services

MANAGING USERS AND GROUPS

- Introduction
  - Every user must have an account
  - There can also be groups
    - Can assign security measures to groups
    - These measures apply to the individual group members automatically
    - Faster and easier than assigning security measures to individuals

MANAGING PERMISSIONS

- Principle of Least Permissions: Give Users the Minimum Permissions Needed for Their Job
  - More feasible to add permissions selectively than to start with many, reduce for security

ADVANCED SERVER HARDENING TECHNIQUES

- Reading Event Logs
  - The importance of logging to diagnose problems
    - Failed logins, changing permissions, starting programs, kernel messages, etc.
- Backup
- File Encryption
- File Integrity Checker