DENNIS GUNAWAN


# IF470 COMPUTER SECURITY

## 08 INTERNAL NETWORK SECURITY

# COURSE SUB LEARNING OUTCOMES (SUB-CLO)

- Sub-CLO 8
  - Students are able to relate internal network security to real case in their daily life (C3)

# OUTLINE

- Threat
  - Port Scan
- Harm
  - Knowledge and Exposure
- Vulnerability
  - Revealing Too Much
  - Allowing Internet Access
- Countermeasure
  - System Architecture
  - Firewall
  - Network Address Translation (NAT)
  - Security Perimeter

# INTRODUCTION

- What kid can resist picking up, looking at, feeling, or playing with the delights in a grocery, hardware, stationery or, most enticing, toy store?
- Children learn by encountering new things and cataloging their size, shape, color, texture, weight, and smell
- As long as they don't damage things, surely children aren't doing any harm by just exploring

# INTRODUCTION

- Can the same thing be said for a computing system?
- Is there any harm in an outsider's probing a system?
  - Perhaps not, but some exploring outsiders are not as innocent as children
- Network scanning is a way to determine characteristics and vulnerabilities of a network

# PORT SCAN

- Vulnerabilities in different versions of software products are well known
- Hackers circulate copies of attack code and scripts
- The problem for the attacker is to know which attacks to address to which machines

Sending an attack against a machine that is not vulnerable

- Time consuming
- May even make the attacker stand out or become visible and identifiable

# PORT SCAN

## Port Scanner

A program that, for a particular Internet (IP) address,
reports which ports respond to queries and
which of several known vulnerabilities seem to be present

- An easy way to gather network information is to use a port scanner
- A port scan is much like a routine physical examination from a doctor, particularly the initial questions used to determine a medical history

# PORT SCAN

- Many common services are bound to agreed-upon ports
- The destination port number is given in the header of each packet or data unit
- Ports 0 – 1023 are called well-known ports and are informally associated with specific services

**Ports**

Numbers to identify different services

# PORT SCAN

- A scanner such as nmap probes a range of ports, testing to see what services respond
- Notice that the entire scan took only 34 seconds

```
Nmap scan report
192.168.1.1 / somehost.com (online) ping results
address: 192.168.1.1 (ipv4)
hostnames: somehost.com (user)
The 83 ports scanned but not shown below are in state: closed
Port       State     Service  Reason      Product   Version  Extra info
21   tcp   open      ftp      syn-ack     ProFTPD   1.3.1
22   tcp   filtered  ssh      no-response
25   tcp   filtered  smtp     no-response
80   tcp   open      http     syn-ack     Apache    2.2.3    (CentOS)
106  tcp   open      pop3pw   -ack        poppassd
110  tcp   open      pop3     syn-ack     Courier pop3d
111  tcp   filtered  rpcbind  no-response
113  tcp   filtered  auth     no-response
143  tcp   open      imap     syn-ack     Courier   Imapd    rel'd 2004
443  tcp   open      http     syn-ack     Apache    2.2.3    (CentOS)
465  tcp   open      unknown  syn-ack
646  tcp   filtered  ldp      no-response
993  tcp   open      imap     syn-ack     Courier   Imapd    rel'd 2004
995  tcp   open               syn-ack
2049 tcp   filtered  nfs      no-response
3306 tcp   open      mysql    syn-ack     MySQL     5.0.45
8443 tcp   open      unknown  syn-ack
34 sec. scanned
1 host(s) scanned
1 host(s) online
0 host(s) offline
```

# PORT SCAN

- Port scanning tells an attacker 3 things
  - Which standard ports or services are running and responding on the target system
  - What operating system is installed on the target system
  - What applications and versions of applications are present

- This information is readily available for the asking from a networked system
  - It can be obtained quietly, anonymously, without identification or authentication, drawing little or no attention to the scan

# PORT SCAN

- Knowing that a particular host runs a given version – that may contain a known or even undisclosed flaw – of a service, an attacker can devise an attack to exploit precisely that vulnerability

- A port scan can be a first step in a more serious attack

# PORT SCAN

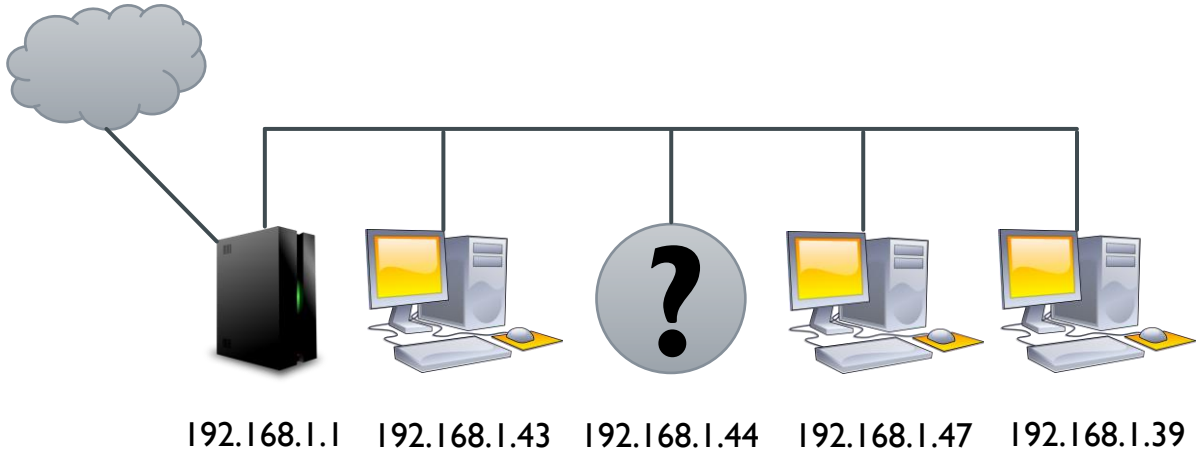
- Another thing an attacker can learn is connectivity
  - We have expanded the search to an entire subnetwork
  - The network consists of a router, 3 computers, and 1 unidentified device
  - Because the latency time (the time between when a packet is sent to the device and the device responds) for all device is similar, it is likely they are on the same network segment

```
Starting Nmap 5.21 (http://nmap.org) at 2010-00-00 12:32 Eastern
Daylight Time

Nmap scan report for router (192.168.1.1)
Host is up (0.00s latency).
MAC Address: 00:11:22:33:44:55 (Brand 1)

Nmap scan report for computer (192.168.1.39)
Host is up (0.78s latency).
MAC Address: 00:22:33:44:55:66 (Brand 2)

Nmap scan report computer (192.168.1.43)
Host is up (0.010s latency).
MAC Address: 00:11:33:55:77:99 (Brand 3)

Nmap scan report for unknown device 192.168.1.44
Host is up (0.010s latency).
MAC Address: 00:12:34:56:78:9A (Brand 4)

Nmap scan report for computer (192.168.1.47)
Host is up.
```

# PORT SCAN

- You could sketch a connectivity diagram of the network

```
Starting Nmap 5.21 (http://nmap.org) at 2010-00-00 12:32 Eastern
Daylight Time

Nmap scan report for router (192.168.1.1)
Host is up (0.00s latency).
MAC Address: 00:11:22:33:44:55 (Brand 1)

Nmap scan report for computer (192.168.1.39)
Host is up (0.78s latency).
MAC Address: 00:22:33:44:55:66 (Brand 2)

Nmap scan report computer (192.168.1.43)
Host is up (0.010s latency).
MAC Address: 00:11:33:55:77:99 (Brand 3)

Nmap scan report for unknown device 192.168.1.44
Host is up (0.010s latency).
MAC Address: 00:12:34:56:78:9A (Brand 4)

Nmap scan report for computer (192.168.1.47)
Host is up.
```



# HARM: KNOWLEDGE & EXPOSURE

Think of 2 houses in a neighborhood a burglar is casing. He knows nothing about the first house. As to the second house, he knows it is occupied by 2 people, whose bedroom is on the upper floor. The couple have a dog, which sleeps in the basement behind a closed door. They always leave a back window open slightly so the cat can get in and out. And one of the occupants recently sprained her ankle, so she moves slowly and with some pain.

- What is the harm of someone knowing machines and services?
- The second house is more attractive to the burglar
  - He can plan an attack that capitalizes on the known vulnerabilities in that house
- Unnecessarily exposing characteristics of a computing system can be harmful

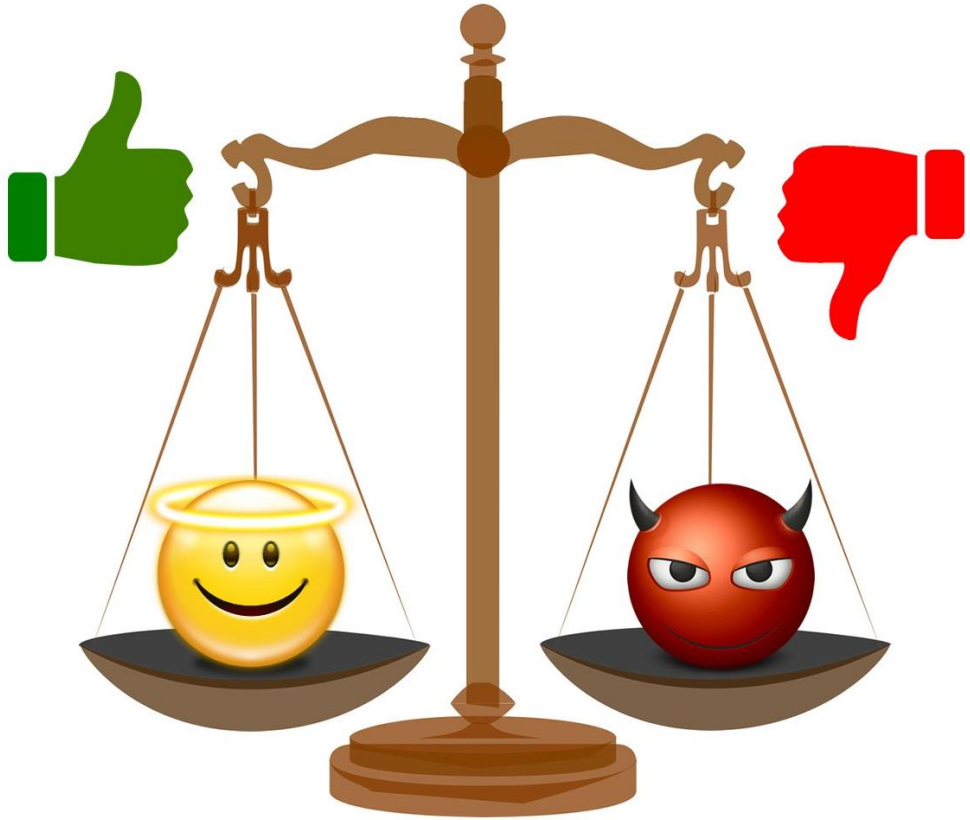
# THE GOOD & BAD OF NETWORK & VULNERABILITY SCANNERS

- Good use
  - By network administrators or system owners who will explore their networks with the tool
  - The tool will report
    - Which devices may be running out-of-date and vulnerable versions of software that should be upgraded
    - Which ports are unnecessarily exposed and should be closed
  - To document and review all the devices connected to the network

- Bad use
  - Allow an attacker to learn about a system

# THE GOOD & BAD OF NETWORK & VULNERABILITY SCANNERS

Because of the importance of the good use,
sound commercial software companies continue
to improve the uses and usability of network scanners
which, unfortunately, also supports the bad use



# REVEALING TOO MUCH

- A computer, device or network can introduce a vulnerability by giving away too much information

- 2 examples of the login prompt

```
Enter user ID       : MyID
Enter password      : PASS1
** Error: Incorrect password **
```

  - The attacker has learned that MyID is a valid system ID
  - Reduces the attacker's work significantly
  - The attacker need only find a password that matches MyID

```
Enter user ID       : MyID
Enter password      : PASS1
** Error: Unacceptable user ID or password **
```

  - Only that one or the other or both are invalid

# REVEALING TOO MUCH

- Systems can be configured to divulge the minimum amount of information
- Some service applications respond immediately with their make, model, and version number

```
443   tcp   open   http   syn-ack   Apache   2.2.3   (CentOS)
```

- It may be possible to defer revealing that information until a connection has been established
- System administrators may not have full control over how much detail of their network is revealed

# REVEALING TOO MUCH

- System administrators do have control over open ports
- A service application should be running only if it is needed
- System administrators should regularly scan their network to ensure that only necessary ports are active

# ALLOWING INTERNAL ACCESS

- Achieving some degree of control of a target machine may let the attacker access other machines not accessible from outside the network

- The attacker will appear to other network components as an insider
  - Presumably more trustworthy and often with greater privileges than an outsider

A router, specifically, is a connection between 2 subnetworks. Although a port scan may reveal only one side of a router's connectivity, that of the visible subnetwork, once the attacker has compromised the router, the attacker can continue, through the router, to explore and attack machines on the router's internal network side.

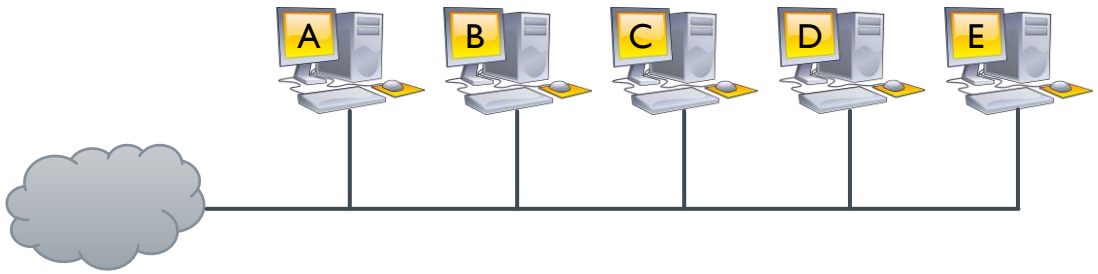
# SYSTEM ARCHITECTURE

- If you are trying to limit the information a port scan reveals about a network and its hosts and services, the natural approach is to segment the network, with many hosts on segments that are not immediately visible to the outside

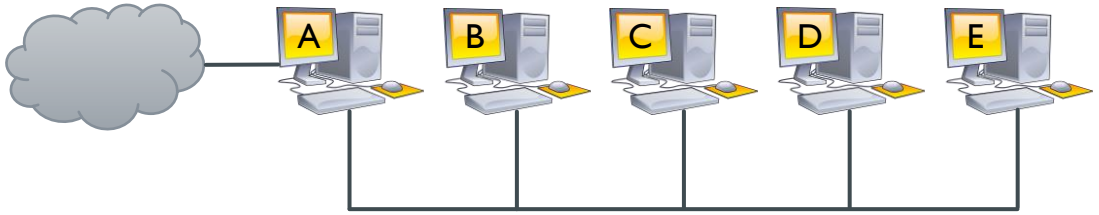
## A Typical Hospital Telephone System

Some functions, such as human resources or patient services, need to accept calls directly from outsiders, and those telephone numbers could be published in a directory. But you do not want the telephone number of the operating room or the diagnostics laboratory or even housekeeping or maintenance to be readily available to outsiders. The hospital would publish a general operator's number; if an outsider has a convincing reason to need to be connected with the operating room, the operator can determine that and forward the call or perhaps redirect it to someone else who can be of better assistance.

# SYSTEM ARCHITECTURE

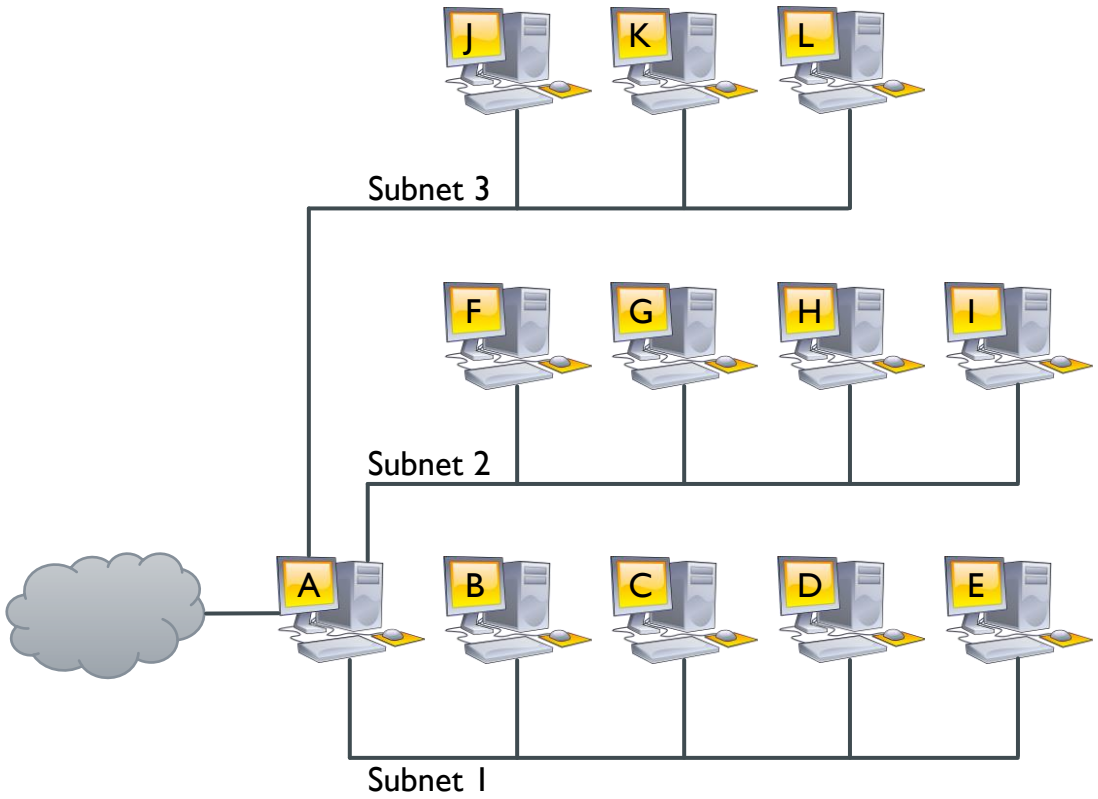



- All 5 computers A – E are visible to the outside network




- Only computer A is visible
- The network of devices B – E is known as a protected subnet
- Device A is called a dual-homed gateway
- Host A becomes a single point of failure
- The gateway device A becomes a potential bottleneck

# SYSTEM ARCHITECTURE




- The 3 subnets could be for separate departments or user groups, or they could be allocated geographically
- The more subnets gateway A supports, the more risk if device A fails

# FIREWALL

- In buildings
  - Walls intended to inhibit the spread of fire from one part of a building to another
- As computer security devices
  - Protecting one subnet from harm from another subnet

A device that filters all traffic

between a protected or “inside” network

and a less trustworthy or “outside” network

# FIREWALL

## PURPOSE

Keep "bad" things
outside a protected environment

- Usually runs on a dedicated device
  - Performance is important
    - A single point through which traffic is channeled
  - Only firewall functions should run on the firewall machine
    - The fewer pieces of code on the device, the fewer tools the attacker would win by compromising the firewall
    - The firewall system typically does not have tools an attacker might use to extend an attack from the firewall computer

# FIREWALL'S DEFAULT BEHAVIOR

## Default Permit

- "that which is not expressly forbidden is permitted"
- Users, always interested in new features, prefer this approach

## Default Deny

- "that which is not expressly permitted is forbidden"
- Security experts, relying on several decades of experience, strongly counsel this approach

# DESIGN OF FIREWALLS

A well-understood traffic flow policy

A trustworthy design and implementation

# DESIGN OF FIREWALLS: POLICY

**A firewall implements a security policy**

A set of rules that determine what traffic can or cannot pass through the firewall

- The table is processed from the top down
  - The first matching rule determines the firewall's action

| Type | Source Addr. | Destination Addr. | Destination Port | Action |
|---|---|---|---|---|
| TCP | * | 192.168.1.* | 25 | Permit |
| UDP | * | 192.168.1.* | 69 | Permit |
| TCP | 192.168.1.* | * | 80 | Permit |
| TCP | * | 192.168.1.18 | 80 | Permit |
| TCP | * | 192.168.1.* | * | Deny |
| UDP | * | 192.168.1.* | * | Deny |

# DESIGN OF FIREWALLS: TRUST

## UNBYPASSABLE

- All network accesses that we want to control must pass through the firewall
- A firewall is positioned as the single physical connection between a protected (internal) network and an uncontrolled (external) one

## TAMPERPROOF

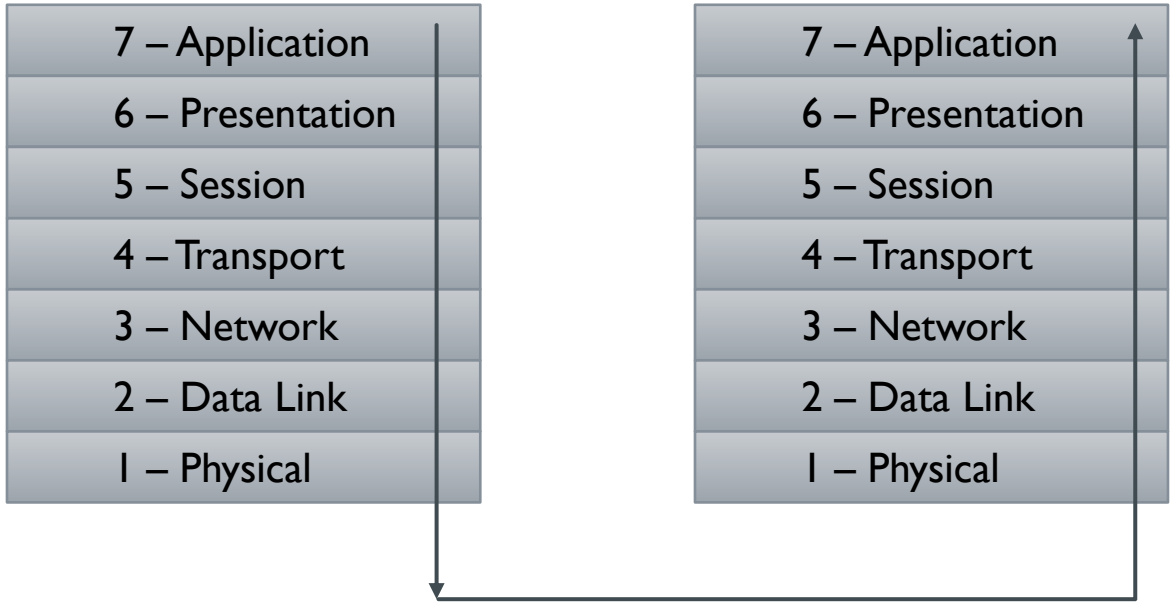
- A firewall is typically well isolated, making it highly immune to modification
- Usually a firewall is implemented on a separate computer
- The firewall platform runs a stripped-down operating system running minimal services

## ANALYZABLE

- Keeping the functionality of the firewall simple

# NETWORK TECHNOLOGY BACKGROUND

- ISO Open Systems Interconnect (OSI) model of networking



# TYPES OF FIREWALLS

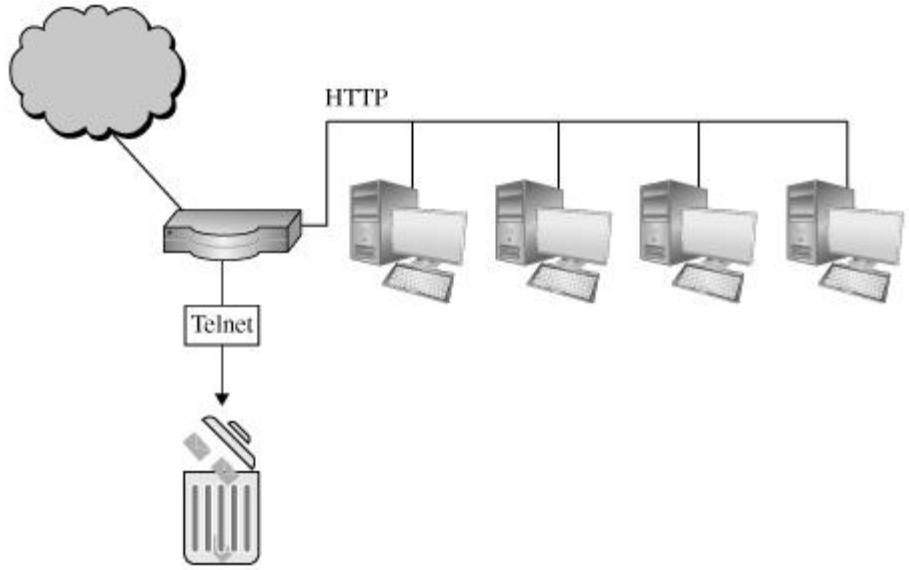
- Different kinds of attack and different ways to detect them lead to several kinds of firewalls
  - Packet filtering gateways or screening routers
  - Stateful inspection firewalls
  - Application-level gateways, also known as proxies
  - Circuit-level gateways
  - Guards
  - Personal firewalls

# PACKET FILTERING GATEWAY / SCREENING ROUTER

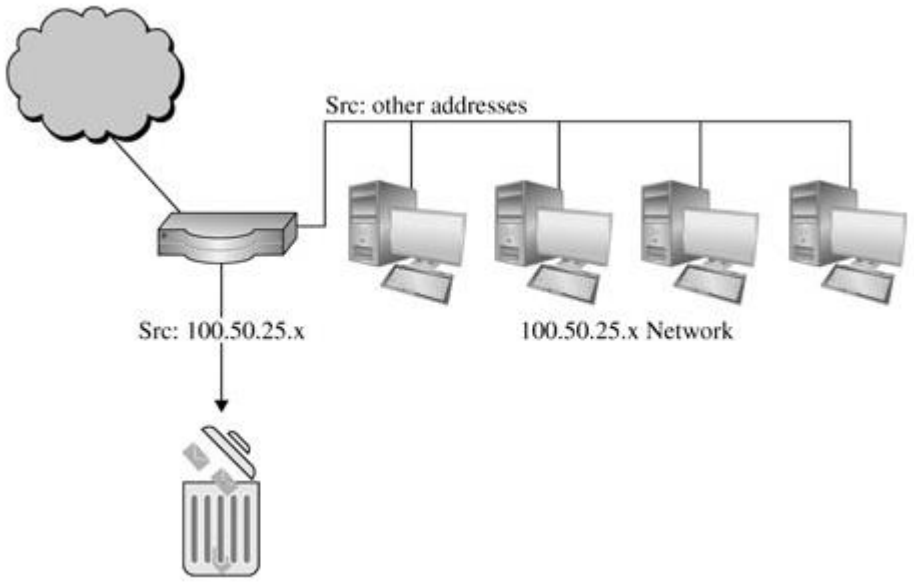
- The simplest

- A packet filter accepts or rejects packets solely according to the header information of each packet
  - IP address (source or destination)
  - Size
  - Protocol type / port

- Packet filters do not "see inside" a packet
  - Any details in the packet's data field is beyond the capability of a packet filter



# PACKET FILTERING GATEWAY / SCREENING ROUTER




- Source addresses in packets can be forged
- A screening packet filter might be configured to block all packets from the outside that claimed their source address was an inside address

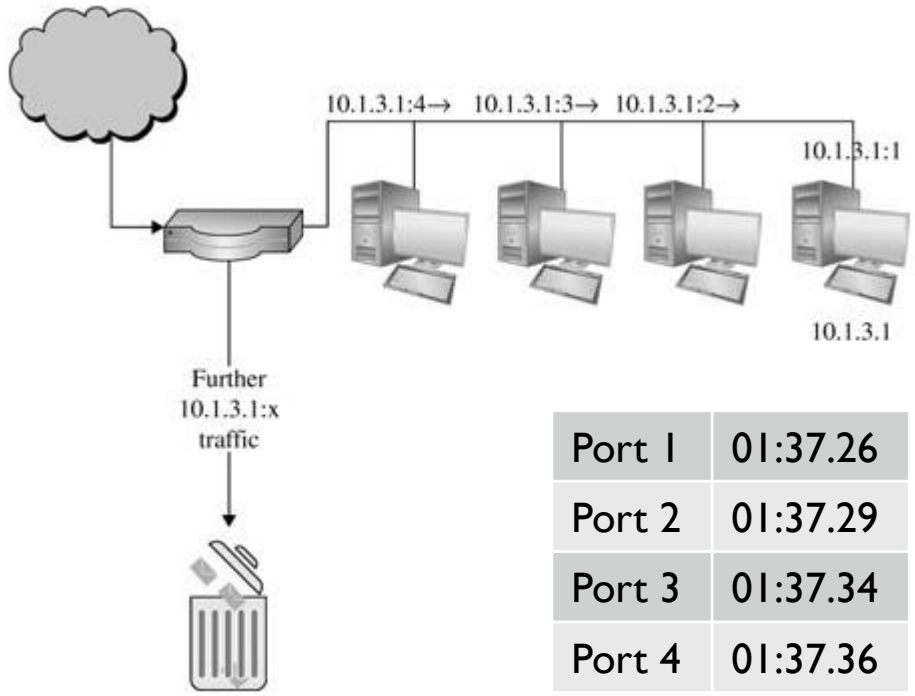
# PACKET FILTERING GATEWAY / SCREENING ROUTER

- The primary disadvantage of packet filtering routers is a combination of simplicity and complexity
  - The router's inspection is simplistic
  - To perform sophisticated filtering, the filtering rules set needs to be very detailed
    - A detailed rules set will be complex and therefore prone to error

Blocking all port 23 traffic (Telnet) is simple and straightforward. But if some Telnet traffic is to be allowed, each IP address from which it is allowed must be specified in the rules. In this way, the rule set can become very long.

# STATEFUL INSPECTION FIREWALL

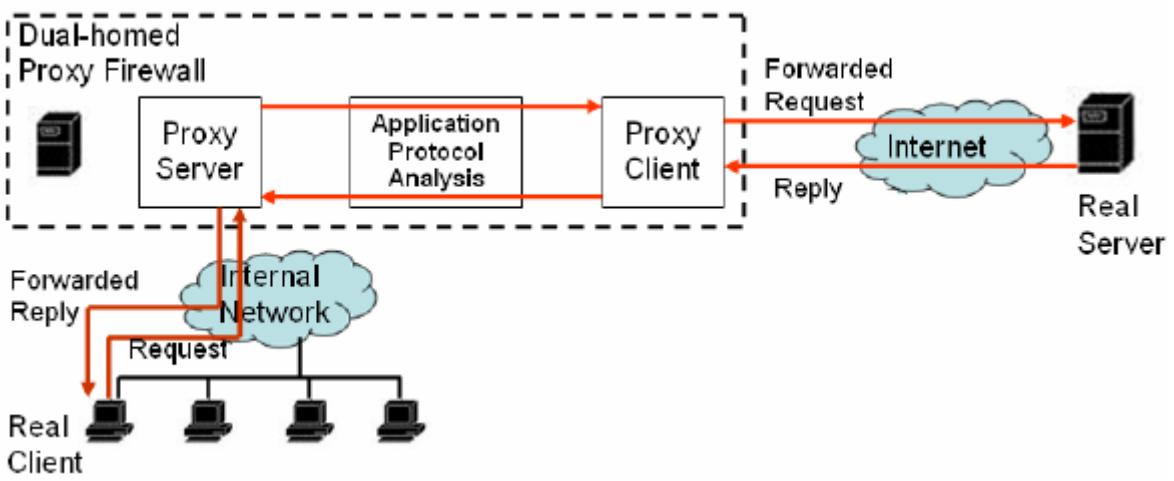
- A stateful inspection firewall maintains state information from one packet to another in the input stream
- The name stateful inspection refers to accumulating threat evidence across multiple packets




| | |
|---|---|
| Port 1 | 01:37.26 |
| Port 2 | 01:37.29 |
| Port 3 | 01:37.34 |
| Port 4 | 01:37.36 |

# APPLICATION PROXY

- An application proxy gateway is also called a bastion host
- A firewall that simulates the (proper) effects of an application
  - The application receives only requests to act properly
- The proxy interprets the protocol stream to an application, to control actions through the firewall on the basis of things visible within the protocol, not just on external header data



# APPLICATION PROXY

**Consider the FTP (File Transfer Protocol)**

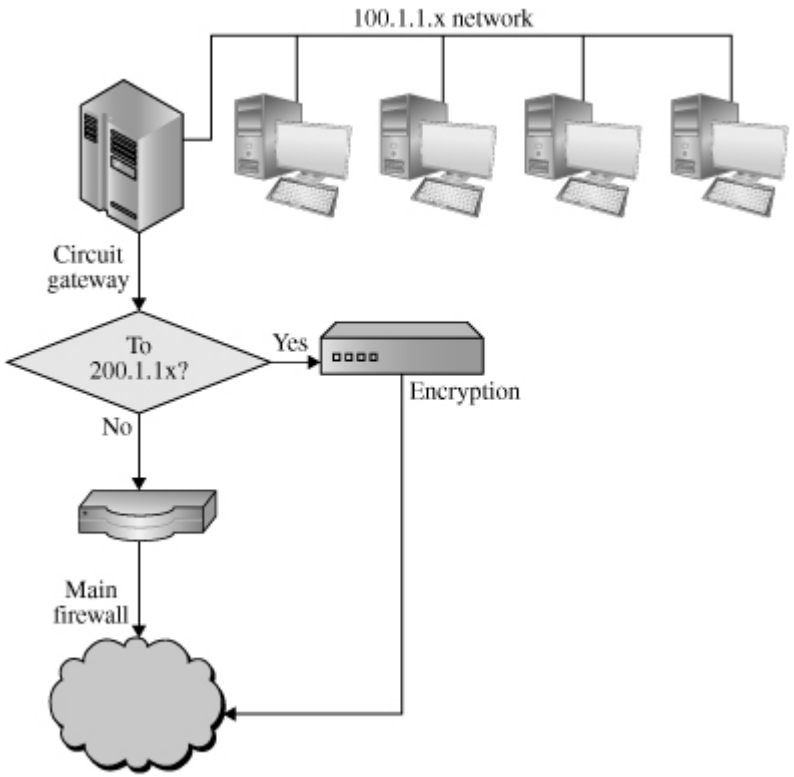
An outsider could retrieve only files from a prespecified directory

- Some administrators might want to permit gets but block puts, and to list only certain files or prohibit changing out of a particular directory
- The proxy would simulate both sides of this protocol exchange
- The proxy might accept get commands, reject put commands, and filter the local response to a request to list files

# CIRCUIT–LEVEL GATEWAY

- A firewall that essentially allows one network to be an extension of another
- It operates at level 5, the session level
- It functions as a virtual gateway between 2 networks

# CIRCUIT–LEVEL GATEWAY




- One use for a circuit-level gateway is to implement a virtual private network
- Suppose a company has 2 offices, each with its own network, at addresses 100.1.1.x and 200.1.1.x
- It wants to ensure that communication between these 2 addresses is private
  - It installs a pair of encryption devices

# GUARD

- A sophisticated firewall
- Like a proxy firewall, it receives protocol data units, interprets them, and emits the same or different protocol data units that achieve either the same result or a modified result
- A guard aims to control the information exchange that the network communication is supporting at the business level
- The degree of control a guard can provide is limited only by what is computable

# GUARD

A university wants to allow its students to use email up to a limit of so many messages or so many characters of email in the last so many days. Although this result could be achieved by modifying email handlers, it is more easily done by monitoring the common point through which all email flows, the mail transfer protocol.

A school wants its students to be able to access the World Wide Web but, because of the capacity of its connection to the web, it will allow only so many bytes per second (that is, allowing text mode and simple graphics but disallowing complex graphics, video, music, or the like).

# GUARD

A library wants to make available certain documents but, to support fair use of copyrighted matter, it will allow a user to retrieve only the first so many characters of a document. After that amount, the library will require the user to pay a fee that will be forwarded to the author.

A company is developing a new product based on petroleum and helium gas, code-named “light oil”. In any outbound data flows, as file transfers, email, web pages, or other data stream, it will replace the words “petroleum”, “helium”, or “light oil” with “magic”. A firewall is thought of primarily as an inbound filter: letting in only appropriate traffic (that which conforms to the firewall’s security policy). A firewall or guard can easily screen outbound traffic in this instance.

# GUARD

- Guards and proxy firewalls are similar enough that the distinction between them is sometimes fuzzy
  - We can add functionality to a proxy firewall until it starts to look a lot like a guard
- The security policy implemented by the guard is somewhat more complex than the action of most proxies
  - The guard's code is also more complex and therefore more exposed to error
- Simpler firewalls have fewer possible ways to fail or be subverted

# PERSONAL FIREWALLS

- An application program that runs on a workstation to block unwanted traffic, usually from the network
- A personal firewall screens traffic on a single workstation
- A personal firewall can provide reasonable protection to clients that are not behind a network firewall

**Commercial Implementations of Personal Firewalls**

- SaaS Endpoint Protection from McAfee
- F-Secure Internet Security
- Microsoft Windows Firewall
- ZoneAlarm from CheckPoint

# COMPARISON OF FIREWALL TYPES

| Packet Filter | Stateful Inspection | Application Proxy | Circuit Gateway | Guard | Personal Firewall |
|---|---|---|---|---|---|
| Simplest decision-making rules | More complex | Even more complex | Between packet filter and stateful inspection | Most complex | Similar to packet filter, but getting more complex |
| Sees only addresses and service protocol type | Can see addresses and data | Sees and analyzes full data portion of pack | Sees addresses and data | Sees and analyzes full content of data | Can see full data portion |
| Auditing limited because of speed limitations | Auditing possible | Auditing likely | Auditing likely | Auditing likely | Auditing likely |
| Screens based on connection rules | Screens based on information across multiple packets – in either headers or data | Screens based on behavior of application | Screens based on address | Screens based on interpretation of content | Typically screens based on content of each packet individually, based on address or content |
| Complex addressing rules can make configuration tricky | Usually preconfigured to detect certain attack signatures | Simple proxies can substitute for complex decision rules, but proxies must be aware of application's behavior | Relatively simple addressing rules make configuration straightforward | Complex guard functionality; can be difficult to define accurately | Usually starts in mode to deny all inbound traffic; adds addresses and functions to trust as they arise |

# FIREWALL

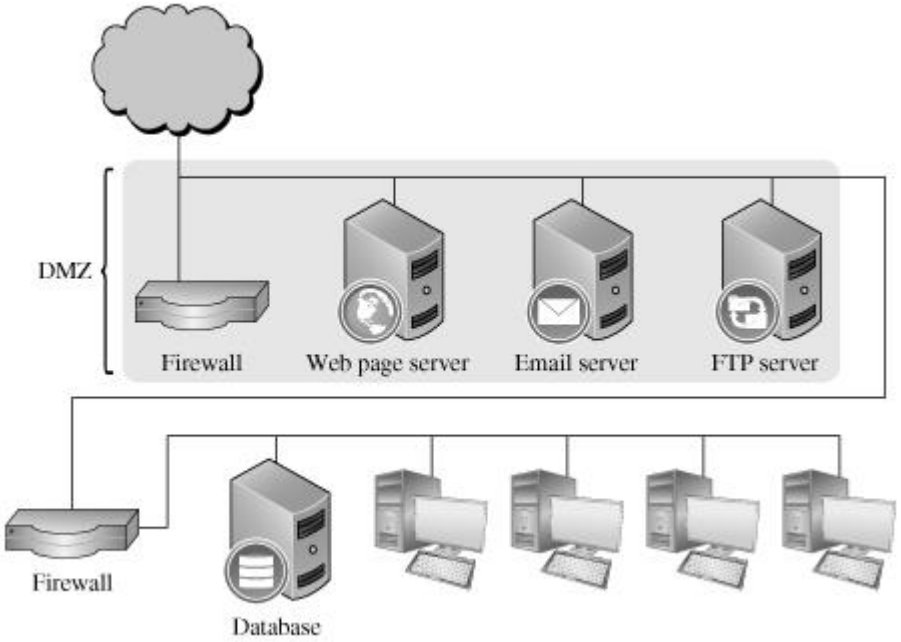
Do not interpret least sophisticated as meaning weakest or least desirable

- In fact, packet filtering firewalls are the workhorses of enterprise networks, quickly and efficiently blocking much undesirable traffic

Firewalls, like many other commercial products, are caught in marketing wars

- Products that started as simple packet filters soon began to appear with functions more normally found in stateful inspection and application-level firewalls

# EXAMPLE FIREWALL CONFIGURATIONS

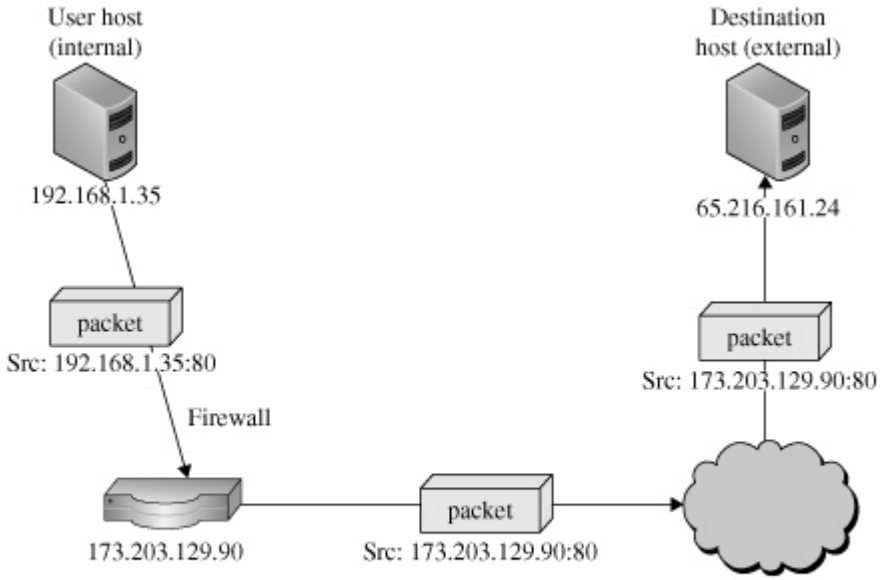



The externally accessible services, such as web pages, email, and file transfer, are on servers in the demilitarized zone or DMZ, named after the military buffer space, sometimes called the "no man's land", between the territories held by 2 competing armies

# KEEP IN MIND THESE POINTS ABOUT FIREWALLS

- Firewalls can protect an environment only if the firewalls control the entire perimeter
- Firewalls do not protect data outside the perimeter
- Firewalls are the most visible part of an installation to the outside, so they are the most attractive target for attack
- Firewalls must be correctly configured
- Firewalls are targets for penetrators
- Firewalls exercise only minor control over the content admitted to the inside

# NETWORK ADDRESS TRANSLATION (NAT)




| Table of translations performed | |
|---|---|
| Source | Dest |
| 192.168.1.35:80 | 65.216.161.24:80 |

- Internal host 192.168.1.35 port 80 is sending a packet to external host 65.216.161.24 port 80
- The source firewall converts source address 192.168.1.35:80 in the packet to the firewall's own address, 173.203.129.90
- To be able to forward any replies to the original source address, the firewall makes an entry in a table showing the destination address, the source port, and the original source address

# NETWORK ADDRESS TRANSLATION (NAT)

- The outside world sees only 1 external address for the whole secured internal network
  - Outsiders cannot infer the design of the internal network
- Outsiders do not know if one communication at one time is from the same internal host as a later communication
  - Shielding individual internal users
- Although primarily used because of another problem (limited public address numbers), network address translation performs a significant security role

# SECURITY PERIMETER

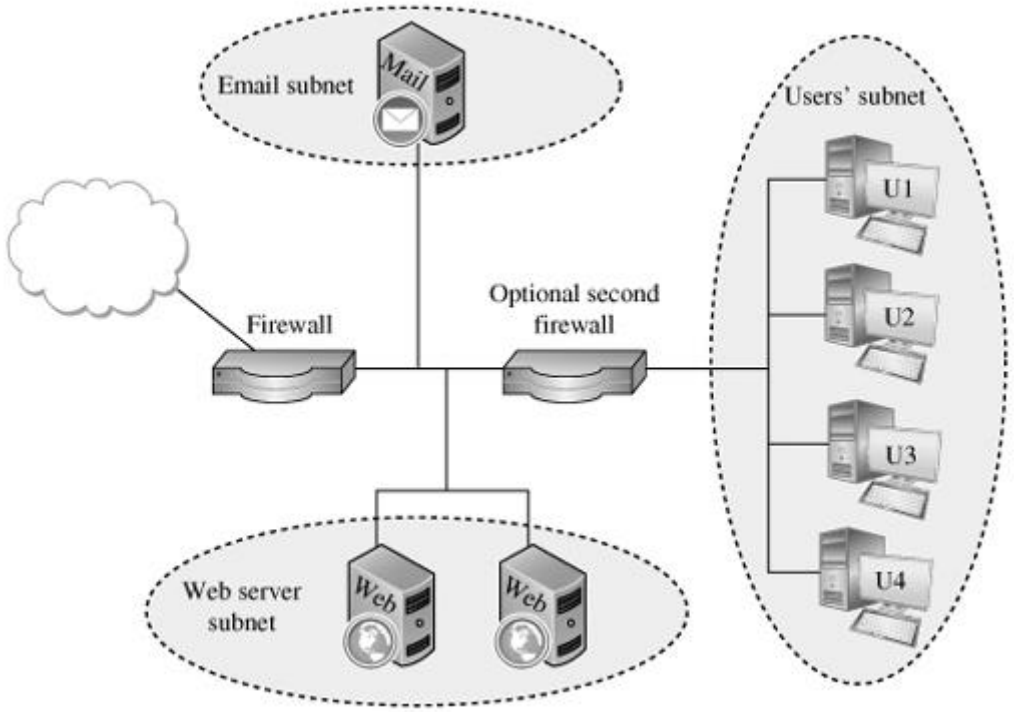
A network that is surrounded by security

–

A design in which an identifiable set of devices is protected together

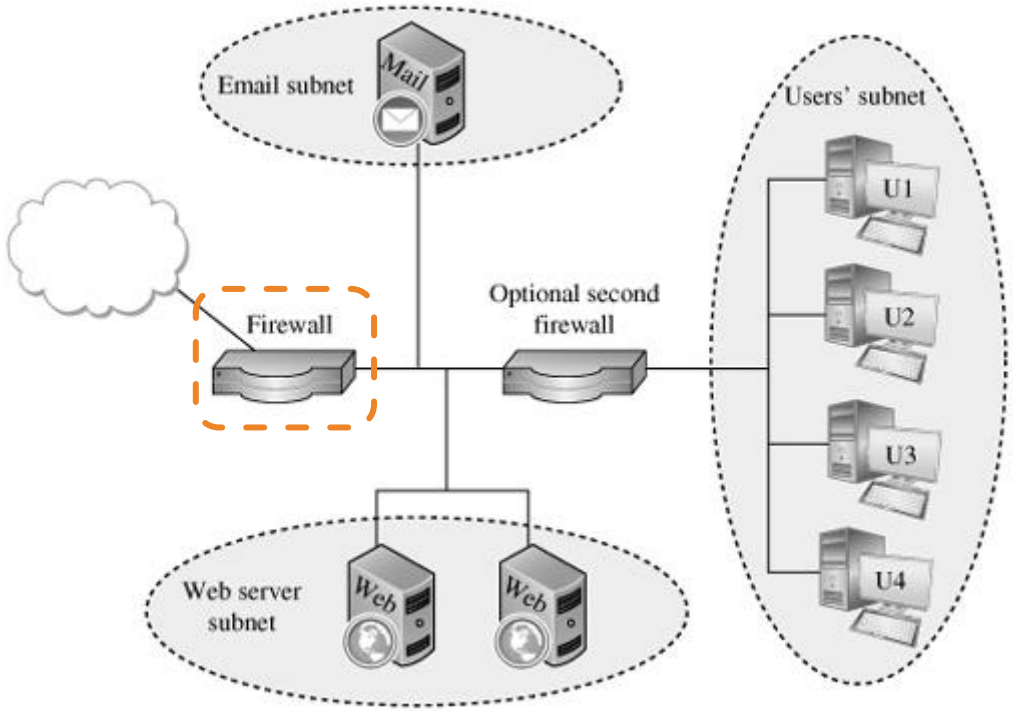
- A security perimeter is both a physical and logical concept
  - The design of one entry point, protected with a firewall
  - Different subnetworks
    - Less sensitive activities in the outer rings
    - Most sensitive data and processes embedded more deeply in inner rings

# SECURITY PERIMETER




- These 2 firewalls implement 2 layers of protection
  - The first (outer) firewall handles only the web and email subnets
  - The second firewall protects the users and data on the internal subnet

# SECURITY PERIMETER




- The front firewall performs 3 functions
  - It directs incoming web searches and email deliveries to the web and email servers, respectively
  - Network address translation
  - It drops any other requests, thus protecting all internal subnetworks from potentially harmful traffic

# REFERENCES


- Pfleeger, Charles P. and Shari Lawrence Pfleeger (2012), *Analyzing Computer Security*, 1st Edition, Prentice Hall.

# NEXT WEEK: SECURITY IN EXTERNAL NETWORK COMMUNICATION

- Wireless or WiFi Network Communications
- Interception
- Peer-to-Peer Networks

# AS THE WORLD IS INCREASINGLY INTERCONNECTED, EVERYONE SHARES THE RESPONSIBILITY OF SECURING CYBERSPACE

# Vision

To become an **outstanding** undergraduate Computer Science program that produces **international-minded** graduates who are **competent** in software engineering and have **entrepreneurial spirit** and **noble character**.

INFORMATIKA
UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA

# Mission

1. To conduct studies with the best technology and curriculum, supported by professional lecturer
2. To conduct research in Informatics to promote science and technology
3. To deliver science-and-technology-based society services to implement science and technology