Security Countermeasures

Lecture (1) - Overview

Information Security Department

2nd Class- Second Course

29 January /2024

By

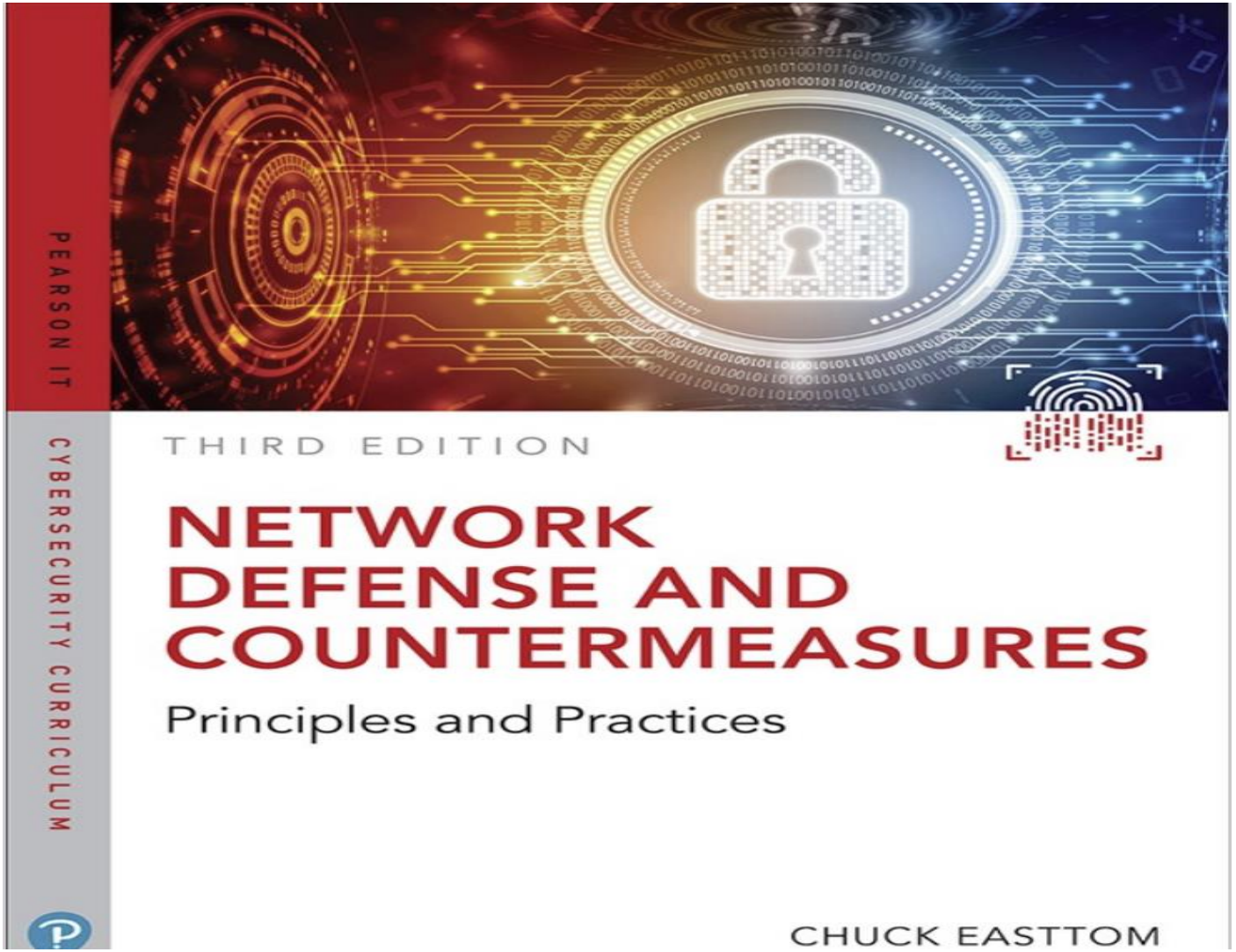
Assist. Lecturer : Nuha Kareem Hameed

Email : NuhaKareem@uobabylon.edu.iq

Outline

- The Basics of a Network
  - Data Packets
  - IP Addresses and Network Classes
    - Public and Private IP
    - NAT
    - MAC Addresses
  - Protocols
    - FTP

THE MAIN TEXT BOOK



The Basics of a Network

- A network is simply a way for machines/computers to communicate.
- At the physical level, it consists of all the machines you want to connect and the devices you use to connect them.
  - Individual machines are connected either with a physical connection (a category 5 cable going into a network interface card, or **NIC**) or wirelessly.
  - To connect multiple machines together, each machine must connect to a hub or switch, and then those hubs/switches must connect together.
- In larger networks, each sub network is connected to the others by a router.
  - "Types of Attacks" that focus on the devices that connect machines together on a network (that is, routers, hubs, and switches).

Basic Network Structure

- Some connection point(s) must exist between your network and the outside world.
  - A barrier is set up between that network and the Internet, usually in the form of a firewall.
    - Many attacks will be covered in this course. They are working to overcome the resistance of the firewall.
    - However, every avenue of communication is also an avenue of attack .
- The first step in understanding how to **defend a network** is having a detailed understanding of how computers communicate over a network.
- The fundamental physical pieces of a network are :
  - Network interface cards,
  - switches,
  - routers,
  - hubs,
  - and firewalls.

Q / Switch vs. Hub ?

Data Packets

- The standard size of a TCP packet has a minimum size of 20 bytes, and a maximum of 65535 bytes. The UDP packets can have any size from 8 to 65535 bytes for each packet.
- A packet can have multiple headers. In fact, most packets will have at least three headers.
  - information such as IP addresses for the source and The IP header has a destination and the protocol of the packet.
  - The TCP header has information such as a port number.
  - The Ethernet header has information such as the MAC address for the source and destination.
  - If a packet is encrypted with Transport Layer Security (TLS), it will also have a TLS header.

Q/ What is the difference between the Size and Length of the packet?

Q/ Why are TCP packets larger than UDP packets?

IP Addresses and Network Classes

Class	IP Range for the First Byte	Use
A	0–126	Extremely large networks. No Class A network IP addresses are left. All have been used.
B	128–191	Large corporate and government networks. All Class B IP addresses have been used.
C	192–223	The most common group of IP addresses. Your ISP probably has a Class C address.
D	224–247	These are reserved for multicasting (transmitting different data on the same channel).
E	248–255	Reserved for experimental use.

IP Addresses and Network Classes

- The IP range of 127 was not listed. This omission is because that range is reserved for testing. The IP address of 127.0.0.1 designates the machine you are on, regardless of that machine's assigned IP address. This address is often referred to as the *loopback address*. That address will be used often in testing your machine and your NIC.

Public and Private IP

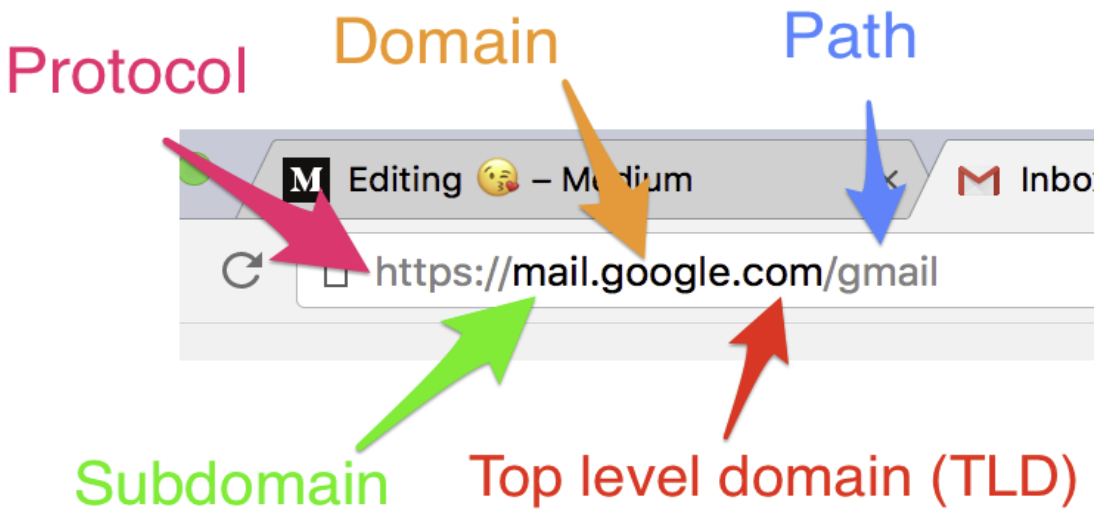
- Private IP addresses are another issue to be aware of. Certain ranges of IP addresses have been designated for use within networks. These cannot be used as public IP addresses but can be used for internal workstations and servers. Those IP addresses are
- 10.0.0.10 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255

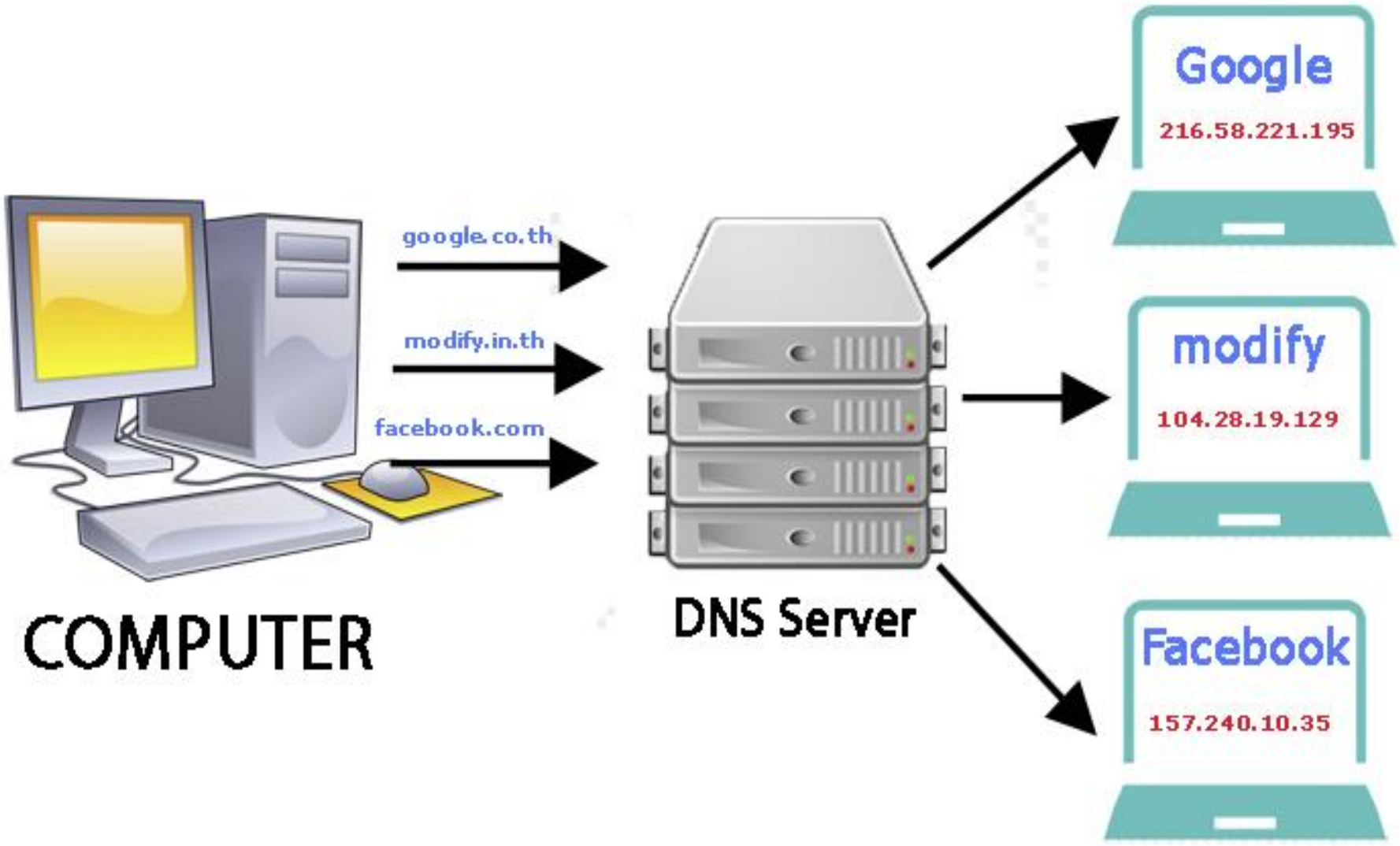
NAT

- One of the roles of a gateway router is to perform what is called network address translation (NAT). Using NAT, a router takes the private IP address on outgoing packets and replaces it with the public IP address of the gateway router so that the packet can be routed through the Internet.

Uniform Resource Locators

- You might type in mail.google.com to go to Gmail dashboard. Your computer, or your ISP, must translate the name you typed in (called a Uniform Resource Locator, or URL) into an IP address.
- URL components:
  1. Protocol
  2. Domain
  3. Path
  4. Subdomain
  5. TLD




google.co.th
modify.in.th
facebook.com
COMPUTER
DNS Server
Google
216.58.221.195
modify
104.28.19.129
Facebook
157.240.10.35

MAC Addresses

- A MAC address is a unique address for an NIC. Every NIC in the world has a unique address that is represented by a six-byte hexadecimal number. The Address Resolution Protocol (ARP) is used to convert IP addresses to MAC addresses.
- **So, when you type in a web address,**
  - the DNS protocol is used to translate that into an IP address.
  - The ARP protocol then translates that IP address into a specific MAC address of an individual NIC.

Protocols

Protocol name	Purpose	Port numb
FTP (File Transfer Protocol)	For transferring files between computers.	20 & 21
SSH	Secure Shell. A secure/encrypted way to transfer files.	22
Telnet	Used to remotely log on to a system. You can then use a command prompt or shell to execute commands on that system. Popular with network administrators.	23
SMTP (Simple Mail Transfer Protocol)	Sends e-mail.	25
WhoIS	A command that queries a target IP address for information.	43
DNS (Domain Name Service)	Translates URLs into web addresses.	53
tFTP (Trivial File Transfer Protocol)	A quicker, but less reliable form of FTP.	69
HTTP (Hypertext Transfer Protocol)	Displays web pages.	80

POP3 (Post Office Protocol Version 3)	Retrieves e-mail.	110
NNTP (Network News Transfer Protocol)	Used for network news groups (Usenet newsgroups). You can access these groups over the web via www.google.com.	119
NetBIOS	An older Microsoft protocol for naming systems on a local	137,
	network.	138, 139
IRC (Internet Relay Chat)	Chat rooms.	194
HTTPS (Hypertext Transfer Protocol Secure)	HTTP encrypted with SSL or TLS.	443
SMB (Server Message Block)	Used by Microsoft Active Directory.	445
ICMP (Internet Control Message Protocol)	These are simply packets that contain error messages, informational messages, and control messages.	No spec port

FTP

- FTP uses two TCP connections for communication. One to pass control information and is not used to send files on port 21, only control information. And the other, a data connection on port 20 to send the data files between the client and the server.