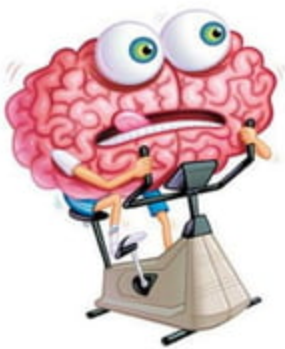
Domain Overview

- Deals with digital communication mechanism by concentrating on the security aspect!

Mind Exercises

- Divide 30 by half and add ten. What do you get?
- A farmer had 17 sheep. All but 9 died. How many alive sheep were left?
- Some months have 30 days, some months have 31 days. How many months have 28 days?



Network Concepts

Data Network Types

- Local Area Network (LAN)
- Wide Area Network (WAN)

- What is intranet?
- What is extranet?

OSI Reference Model

- Adopted by ISO in 1984
- Defines standard protocols for communication and interoperability by using a **layered approach**
- Follows Divide and Conquer Rule?

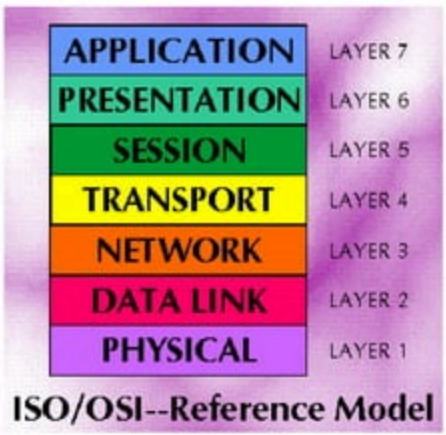
OPEN SYSTEMS INTERCONNECTION

OSI Reference Model

- Advantages
  - Clarifies the functions of a communication process
  - Reduces complex networking processes
  - Promotes interoperability by defining standard interfaces
  - Aids development
  - Facilitates easier and more logical troubleshooting

OSI Layers

- Application Layer
- Presentation Layer
- Session Layer
- Transport Layer
- Network Layer
- Data Link Layer
- Physical Layer



Application Layer

- Serves as the interface between user and the communication technologies
  - SMTP, FTP, HTTP

Message format, Human-Machine interfaces

Presentation Layer

- Ensures communication between different data representations
  - ASCII, EBCDIC, JPEG, MPEG, GIF

Formatting, Encryption, Compression

Session Layer

- Establishes, maintains and terminates sessions between applications
  - SQL, RPC

Authentication, Permissions, Session restoration

Transport Layer

- Provides reliable, transparent transfer of data between end points
  - TCP, UDP

End to end error control

Network Layer

- Provides routing and forwarding functionalities
  - IP, DHCP

Addressing, Routing, Switching

Data Link Layer

- Provides reliable transfer of information across the physical link
  - Ethernet, Token Ring

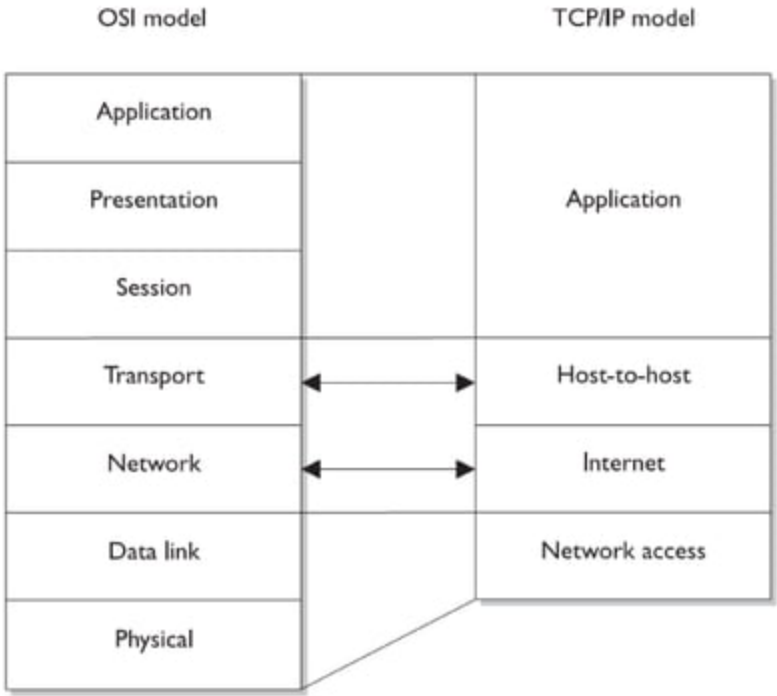
Error detection, Flow control on physical link

Physical Layer

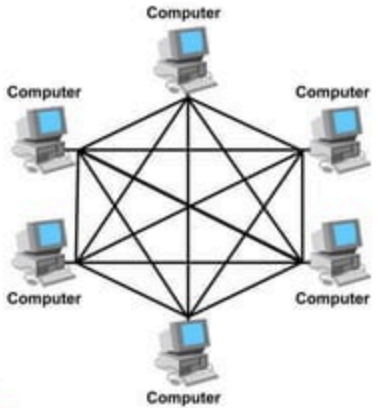
- Concerned with transmission of unstructured bit streams over physical medium
  - E1, T1

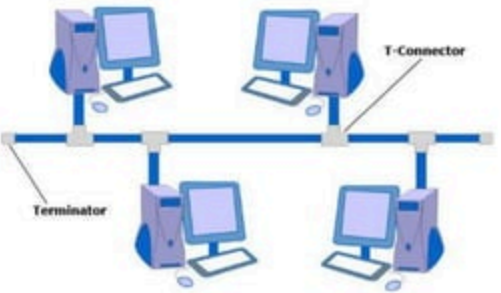
Bit streams, Physical medium, Method of representing bits

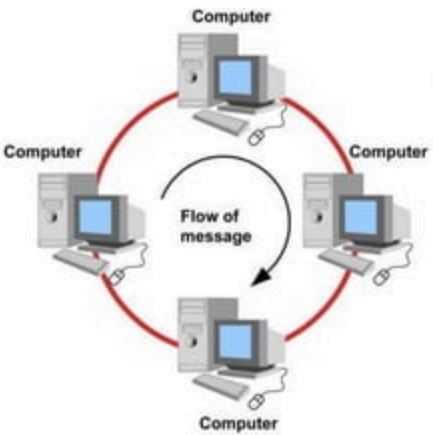
TCP/IP Model

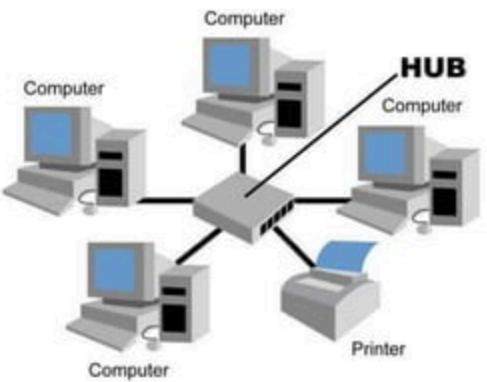

OSI model
TCP/IP model
Application
Presentation
Session
Transport
Network
Data link
Physical
Application
Host-to-host
Internet
Network access

Topologies


Computer
Computer
Computer
Computer
Computer
Computer
Computer


T-Connector
Terminator

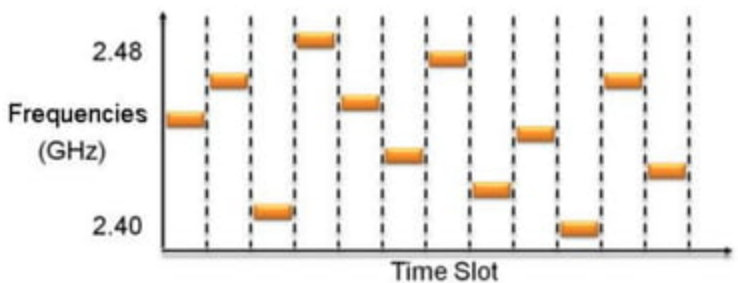

Computer
Computer
Computer
Flow of
message
Computer


Computer
HUB
Computer
Computer
Computer
Printer

Wireless Networks

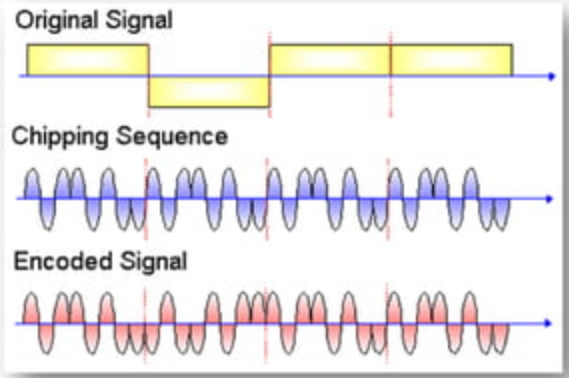
FHSS

- **F**requency **H**oping **S**pread **S**pectrum
  - Takes the total bandwidth and splits it into smaller sub-channels



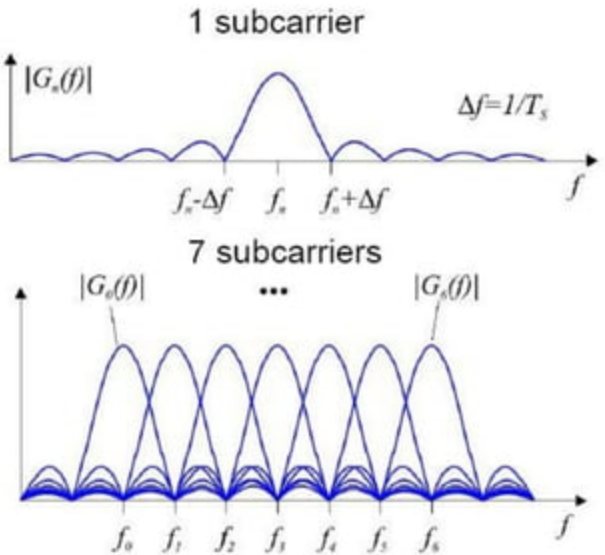
DSSS

- **D**irect **S**equence **S**pread **S**pectrum
  - Applies sub-bits to a message
    - The sub-bits are used to generate a different format of the data before the data are transmitted
    - The receiving end uses these sub-bits to reassemble the signal into the original data format



OFDM

- Orthogonal Frequency Division Multiplexing



Data Link Layer

- WLAN technologies and protocols

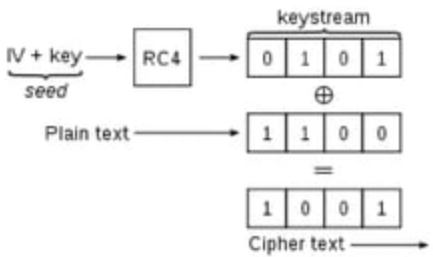
Type	Speed	Frequency	Modulation	Description
802.11	1 Mbps	2.4 Ghz	DSSS	Legacy Protocol
802.11b	11 Mbps	2.4 Ghz	DSSS	First widely used protocol
802.11a	54 Mbps	5.0 Ghz	OFDM	Operated in 5 Ghz band
802.11g	54 Mbps	2.4 Ghz	OFDM/DSSS	
802.11n	150 Mbps	2.4 Ghz	OFDM	

Security Flaws

- No user authentication
- No mutual authentication
- Flawed encryption protocol
  - Allows specific bits to be modified
- Solution?
  - 802.11i
    - Incorporates security measures for the 802.11 standards!

WEP

- Wired Equivalent Privacy
  - Used to provide confidentiality
  - Uses stream cipher RC4
  - Versions
    - WEP-64 and WEP-128
      - 24 bit IV
  - Authentication Methods
    - Open System Authentication
    - Shared Key Authentication



WEP

- Open System Authentication
  - Any client, regardless of its WEP keys, can associate itself with the Access Point
  - No authentication (in the true sense of the term) occurs
  - After the association, WEP key needed for encrypting the data frames
    - At this point, the client needs to have the right key!

WEP

- Shared Key Authentication
  - A four-way challenge-response handshake is used
    - Client sends an authentication request to the Access Point
    - Access Point replies with a clear-text challenge
    - Client encrypts the challenge text using configured WEP key, and sends it back to Access Point
    - Access Point decrypts the material, and compares it with the sent clear-text
      - Depending on the success of this comparison, the Access Point sends back a positive or negative response!

WPA

- WiFi Protected Access
  - Uses Temporal Key Integrity Protocol (TKIP)
    - Adds 48 bit IV value
    - Implements a frame counter to discourage replay attacks!
  - Uses EAP via RADIUS Server
    - For authentication

WPA

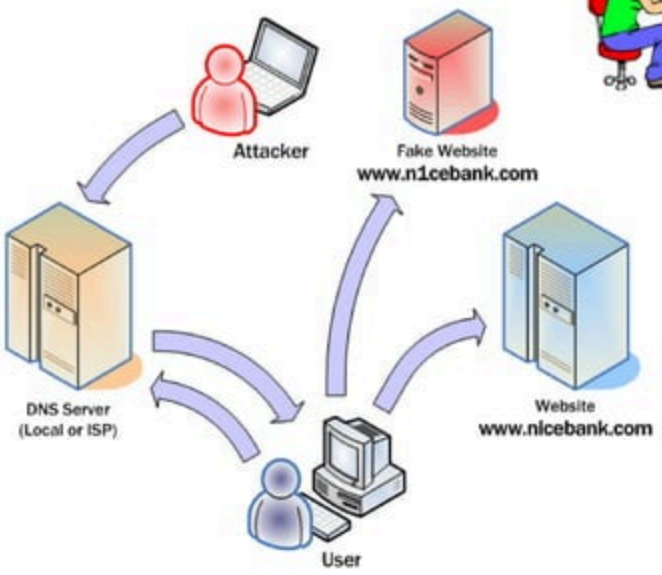
- WPA Modes
  - Enterprise Mode
    - Requires an authentication server
    - Uses RADIUS protocols for authentication and key distribution
    - Centralizes management of user credentials
  - Pre-Shared Key Mode
    - Does not require an authentication server
    - Shared secret is used for authentication
    - Device-oriented management

WPA2

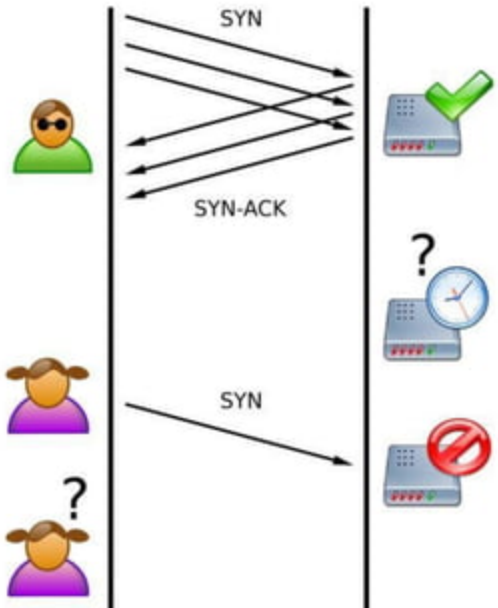
- WiFi Protected Access 2
  - Replaces TKIP with CCMP
    - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
    - Uses AES
    - Provides more robust security

Network Attacks

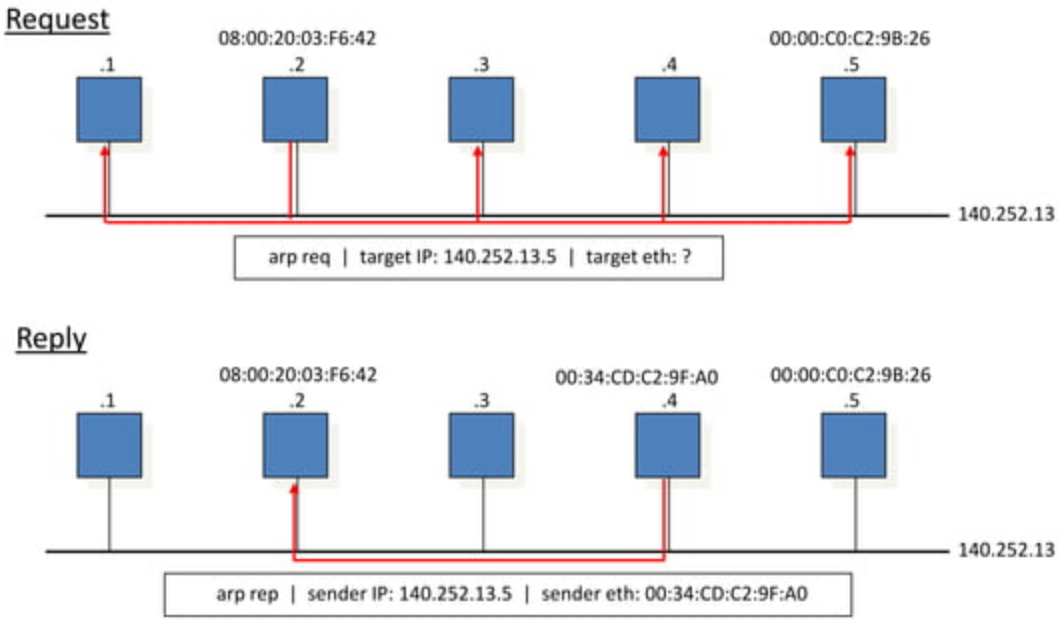
DNS Poisoning



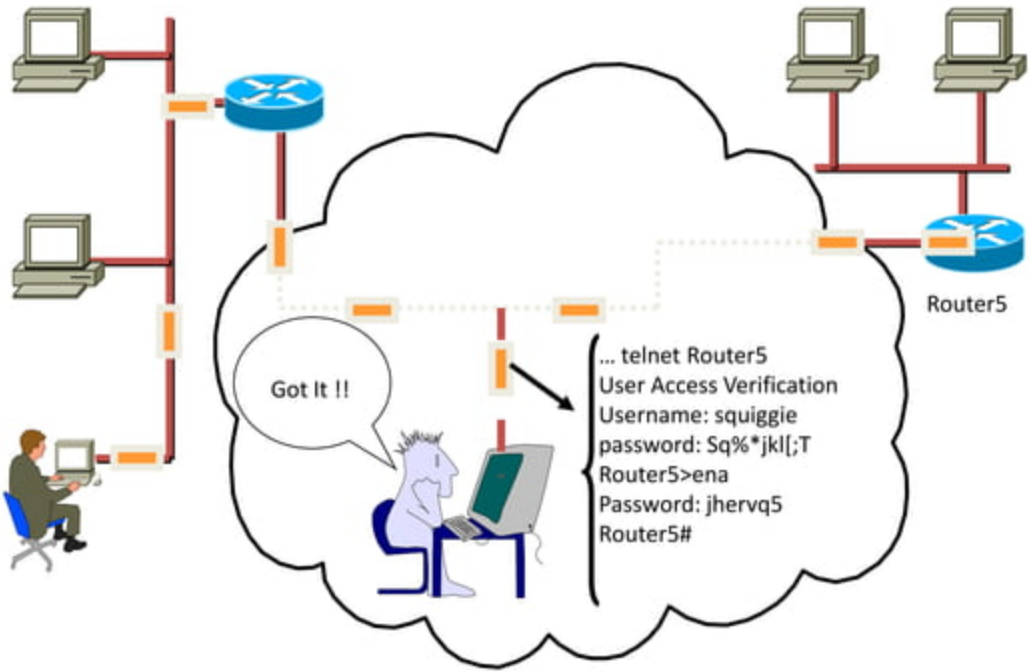
SYN Flood



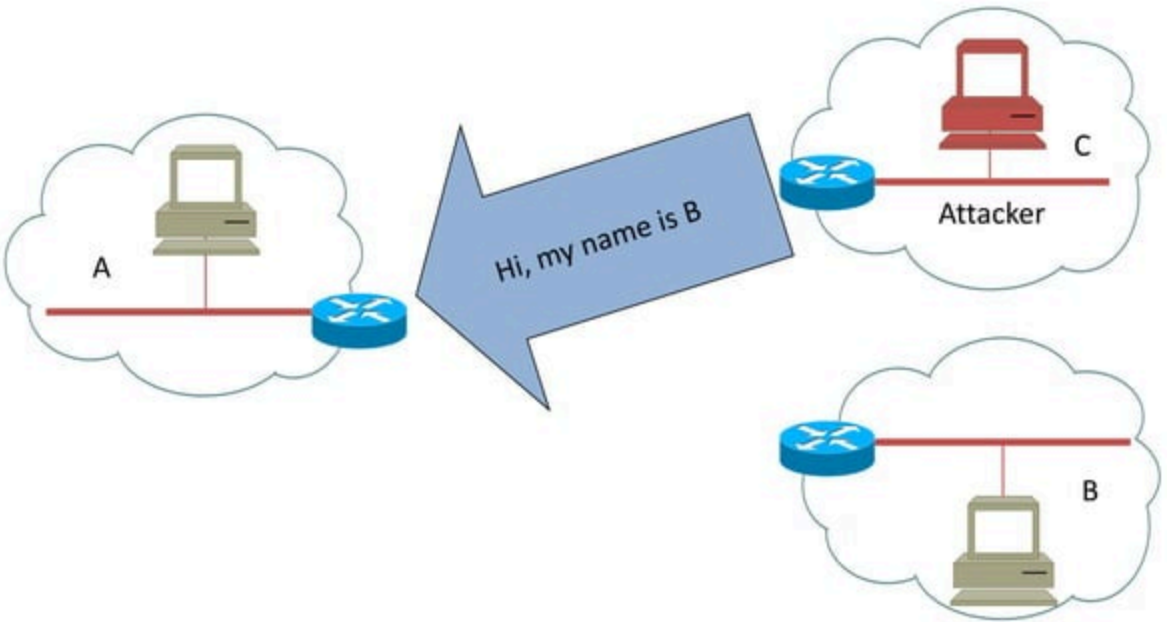
ARP Poisoning



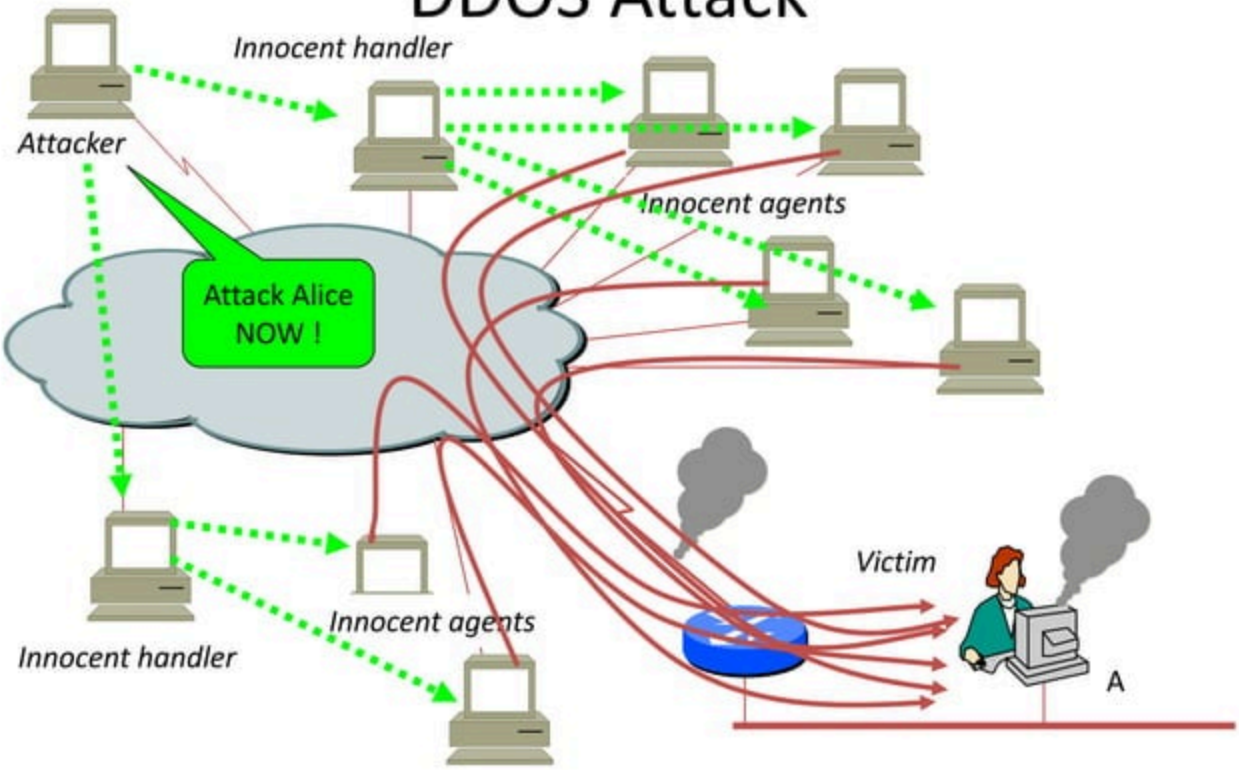
Network Sniffing



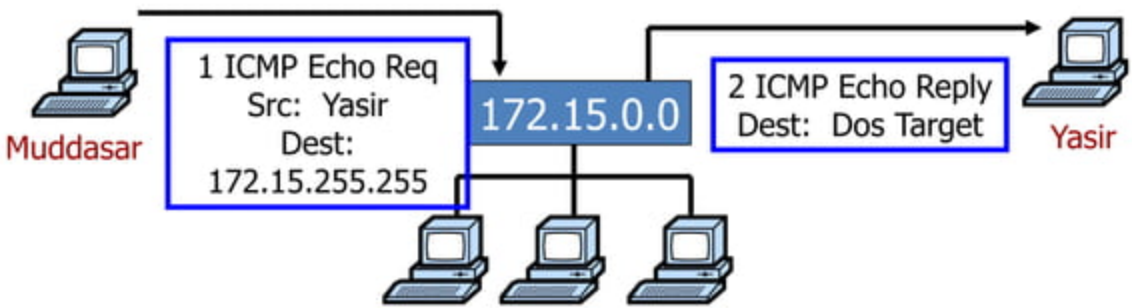
IP Spoofing



DDOS Attack


Innocent handler
Attacker
Innocent agents
Attack Alice
NOW !
Victim
Innocent agents
Innocent handler
A

Smurf Attack

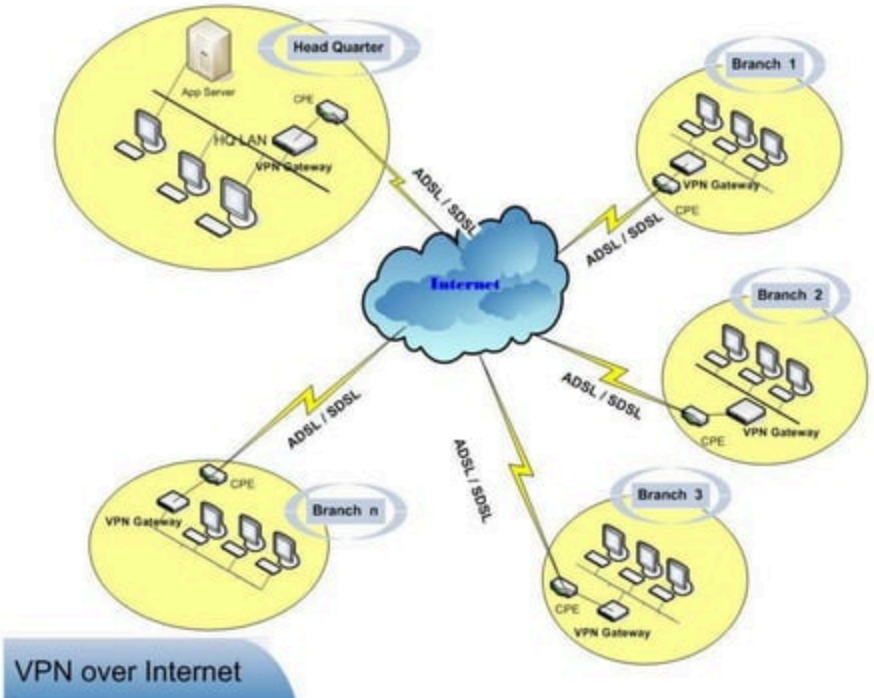


Virtual Private Networks

Introduction

- A private network that uses a public network to connect remote sites or users together!

Concept


Head Quarter
App Server
CPE
HQ LAN
VPN Gateway
ADSL / SDSL
Internet
Branch 1
VPN Gateway
CPE
ADSL / SDSL
Branch 2
ADSL / SDSL
VPN Gateway
CPE
ADSL / SDSL
Branch 3
CPE
VPN Gateway
ADSL / SDSL
CPE
VPN Gateway
Branch n
VPN over Internet

Features of VPN

- Security
- Reliability
- Scalability
- Network management
- Policy management

VPN Concepts

- Encapsulation
  - Inclusion of one data structure within another structure
- Encryption
  - Hiding of real information
- Tunneling
  - Virtual path that delivers a packet

Tunneling Protocols

- PPTP
- L2F
- L2TP
- IPSec

PPTP

- Point to Point Tunneling Protocol
  - Designed for client/server connectivity
  - Sets up a single point-to-point connection between two computers
  - Works at the data link layer
  - Transmits over IP networks only

L2F

- Layer 2 Forwarding
  - Created before L2TP by Cisco
  - Merged with PPTP, which resulted in L2TP
  - Provides mutual authentication
  - No encryption

L2TP

- Layer 2 Tunneling Protocol
  - Hybrid of L2F and PPTP
  - Sets up a single point-to-point connection between two computers
  - Works at the data link layer
  - Transmits over multiple types of networks, not just IP
  - Combined with IPSec for security

IPSec

- Internet Protocol Security
  - Handles multiple connections at the same time
  - Provides secure authentication and encryption
  - Supports only IP networks
  - Focuses on LAN-to-LAN communication rather than user-to-user
  - Works at the network layer, and provides security on top of IP
  - Can work in tunnel mode, meaning the payload and the header are protected, or transport mode, meaning only the payload is protected

Benefits of VPN

- Extend geographic connectivity
- Improve security
- Improve productivity
- Simplify network topology
- Provide global networking opportunities
- Provide broadband networking compatibility
- Provide faster ROI (return on investment) than traditional WAN

Intrusion Detection Systems

Introduction

- A system that detects and logs
  - Inappropriate, Incorrect, or Anomalous activity

Types

- Network based IDS
- Host based IDS

Methods

- Pattern matching
  - Signature based
- Anomaly detection
  - Checks any abnormality
- Protocol behavior
  - Checks correct usage of protocol

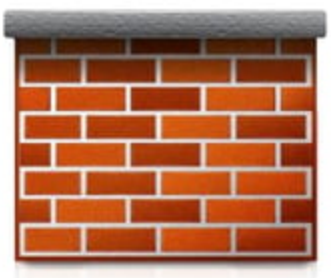
Events

- True positive
  - When the IDS sets off an alert and it is a real attack
- True negative
  - When the IDS does not set off an alert and it is normal traffic
- False positive
  - When the IDS sets off an alert and it is normal traffic
- False negative
  - When the IDS does not set off an alert and it is attack traffic

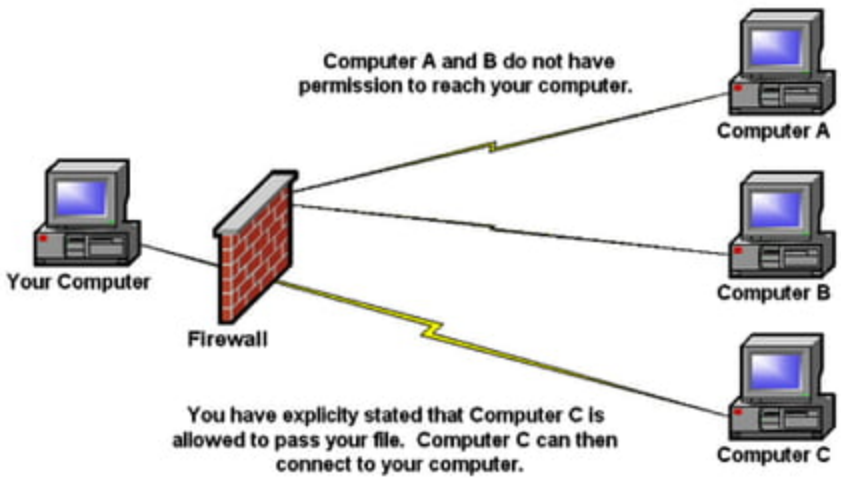
Firewalls

Introduction

- A system that prevents unauthorized access
  - To or from a network
- Controls the flow of traffic



Concept


Computer A and B do not have permission to reach your computer.
Computer A
Computer B
Your Computer
Firewall
You have explicity stated that Computer C is allowed to pass your file. Computer C can then connect to your computer.
Computer C

Firewall Types

- Packet filtering firewall
- Proxy firewall
  - Application level proxy
  - Circuit level proxy
- Stateful inspection firewall
- Dynamic packet filtering firewall
- Kernel proxy firewall

Packet Filtering Firewall

- Governed by set of directives
- Works at network layer
- Makes decisions on
  - Packet's source IP Address
  - Packet's destination IP Address
  - Network and transport protocol being used
  - Source and destination ports
  - The interface being traversed

Packet Filtering Firewall

- Ingress Filtering
  - Blocking inbound traffic
- Egress Filtering
  - Blocking outbound traffic

Application Level Proxy

- Contains a proxy agent
- Does not allow a direct communication
- Operates at the application level
- Inspects the content, payload and header!
- Can require authentication from the user

Circuit Level Proxy

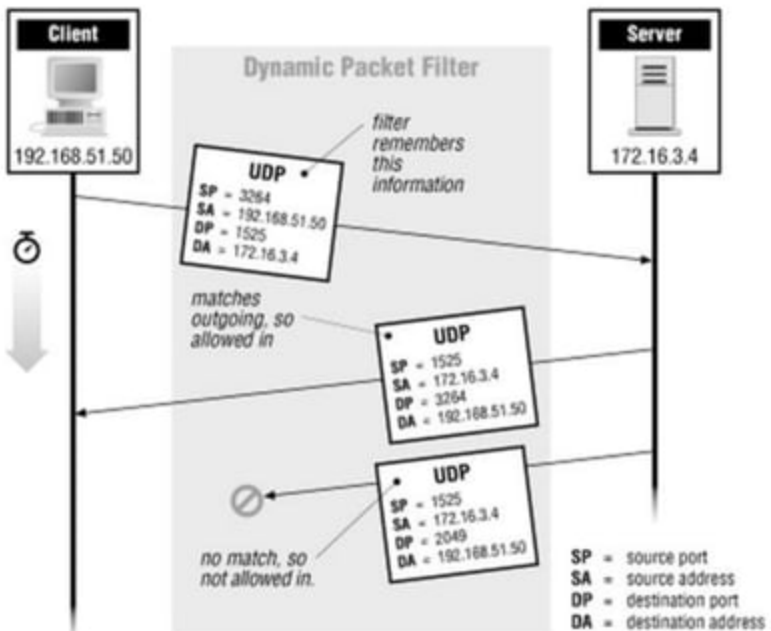
- Creates a circuit between client and the server
- Works at session layer
- Knows the source and destination addresses and makes access decisions based on the header information
- Faster than application level proxy

Stateful Inspection Firewall

- Tracks the state of connections
- Blocks packets deviating from expected state
- Works same as packet filtering firewall but keeps a state table as well!
- Works at network and transport layer

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	192.0.2.71	80	Initiated
192.168.1.102	1031	10.12.18.74	80	Established
192.168.1.101	1033	10.66.32.122	25	Established
192.168.1.106	1035	10.231.32.12	79	Established

Dynamic Packet Filtering



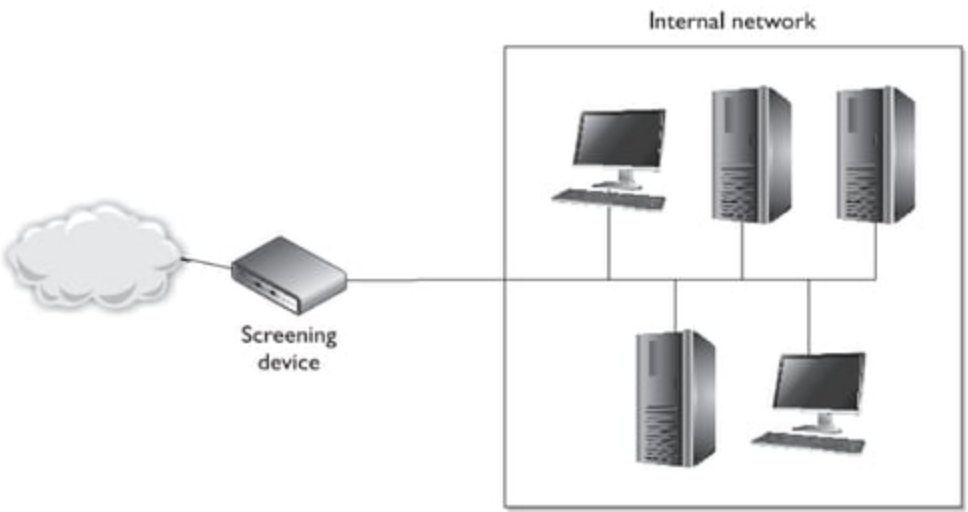
Kernel Proxy Firewalls

- Fifth generation firewall!
- Creates dynamic, customized TCP/IP stacks for packet evaluation
- When a packet arrives, a new virtual network stack is created, which is made up of only the protocol proxies necessary to examine this specific packet properly
- Speed of Packet filtering firewalls

Firewall Architectures

- Screening Router
- Dual Homed Gateways
- Screened Host Gateways
- Screened Subnet

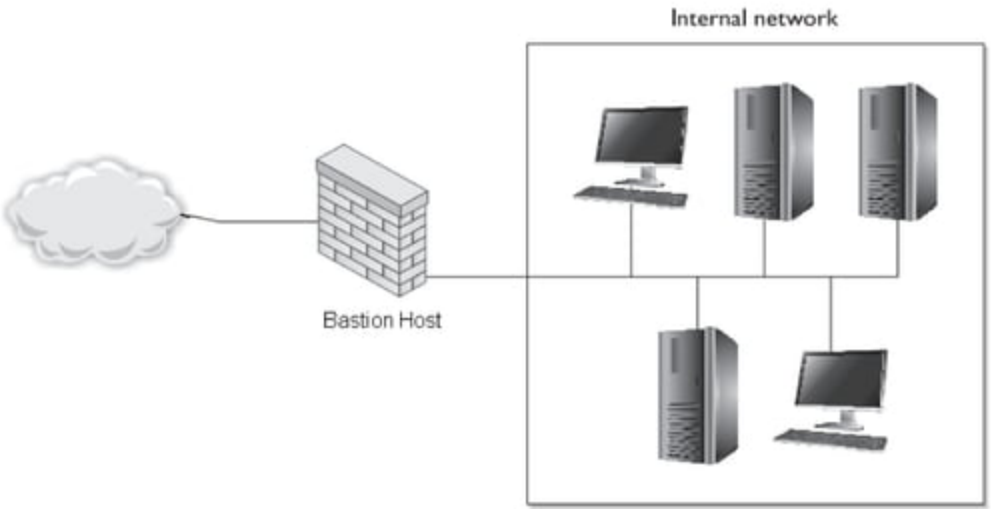
Screening Router



Screening Router

- Screening Router
  - A router placed between trusted and public networks
  - Security policy implemented using ACLs
  - Advantages:
    - Inexpensive
    - Simple and completely transparent
  - Disadvantages
    - Limited logging functionality
    - Single point of failure
    - Uses no user authentication

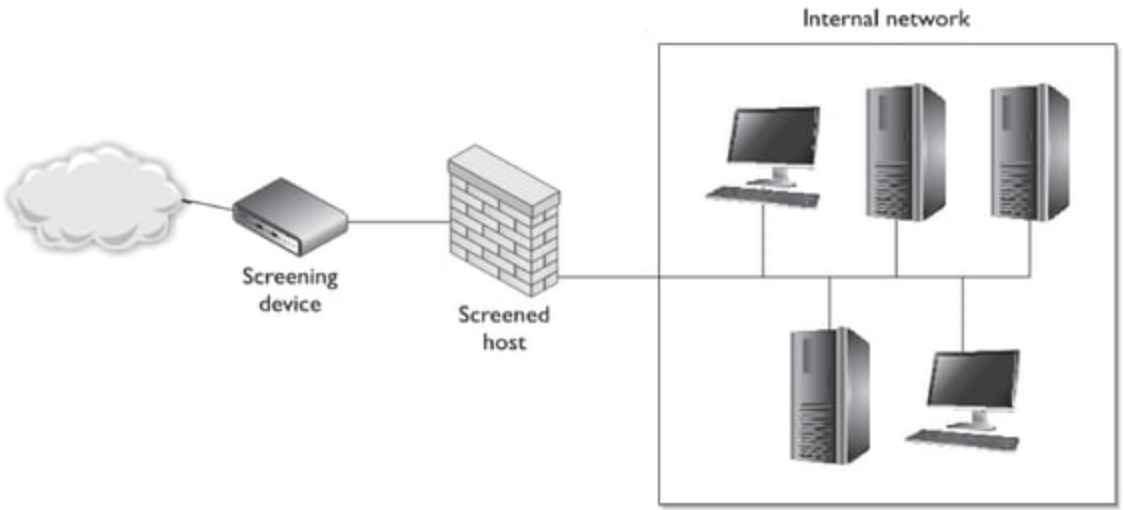
Dual Homed Gateway



Dual Homed Gateways

- A single computer with separate NICs connected to each network
- Used to divide internal trusted network from external networks
- Advantages:
  - Operates in a Fail Secure mode
  - Logging functionality
- Disadvantages:
  - Inconvenience to users
  - Slower network performance

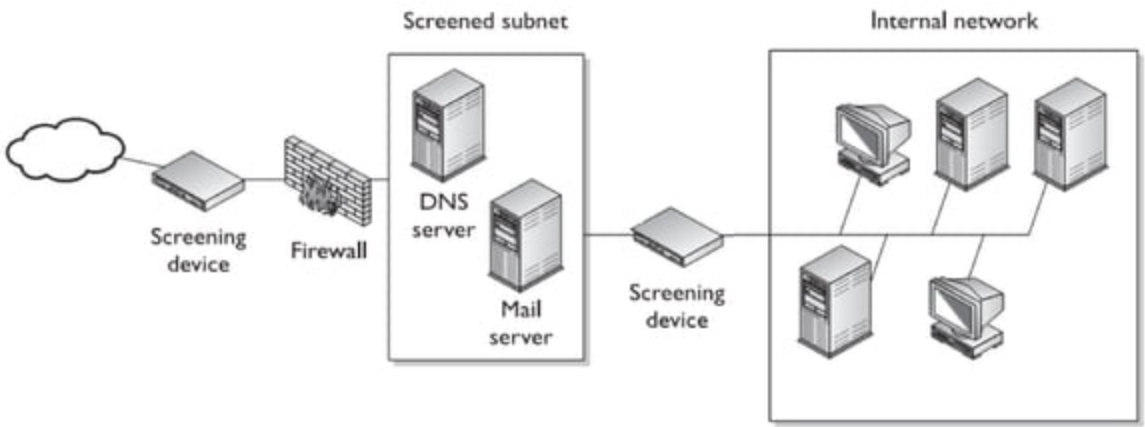
Screened Host Gateways



Screened Host Gateways

- Employs external screening router and internal bastion host
- Advantages:
  - Provides distributed security between two devices
  - Restricted inbound/outbound access
- Disadvantages:
  - Multiple single point of failures

Screened Subnet



Screened Subnet

- Deploys external screening router, internal bastion host and internal screening router
- Concept of DMZ
- Advantages:
  - Provides defense in depth
- Disadvantages:
  - Difficult to configure and maintain
  - Difficult to troubleshoot

Unified Threat Management

- Single system with all the solutions
- Contains firewall, malware detection and eradication, sensing and blocking of suspicious network probes, and so on…
- Requires lot of resources
- Reduces network complexity

Why Firewall Security

- Remote login
- Application backdoors
- Operating system bugs
- Denial of service
- Spam
- Source routing

Best Practices

- Change the default configurations
- ACLs should be simple and direct
- Disallow source routing
- Close unnecessary ports with dangerous services
- Disable unused interfaces
- Block directed IP broadcasts
- Block incoming packets with internal address (they are spoofed)
- Enable logging
- Daily checks to ensure security

Thank You! ☺

- Any Questions?

Questions

Question 1

- Which of the following is not a security goal for remote access?
  A. Reliable authentication of users and systems
  B. Protection of confidential data
  C. Easy to manage access control to systems and network resources
  D. Automated login for remote users

Question 1

- Which of the following is not a security goal for remote access?
  A. Reliable authentication of users and systems
  B. Protection of confidential data
  C. Easy to manage access control to systems and network resources
  D. Automated login for remote users

Question 2

- Which of the following is the biggest concern with firewall security?
  A. Internal hackers
  B. Complex configuration rules leading to misconfiguration
  C. Buffer overflows
  D. Distributed denial of service (DDOS) attacks

Question 2

- Which of the following is the biggest concern with firewall security?
  A. Internal hackers
  B. Complex configuration rules leading to misconfiguration
  C. Buffer overflows
  D. Distributed denial of service (DDOS) attacks

Question 3

- Which of the following should NOT normally be allowed through a firewall?
  A. SNMP
  B. SMTP
  C. HTTP
  D. SSH

Question 3

- Which of the following should NOT normally be allowed through a firewall?
  - **A. SNMP**
  - B. SMTP
  - C. HTTP
  - D. SSH

Question 4

- Which type of attack involves the alteration of a packet at the IP level to convince a system that it is communicating with a known entity in order to gain access to a system?
  A. TCP sequence number attack
  B. IP spoofing attack
  C. Piggybacking attack
  D. Teardrop attack

Question 4

- Which type of attack involves the alteration of a packet at the IP level to convince a system that it is communicating with a known entity in order to gain access to a system?
  A. TCP sequence number attack
  B. IP spoofing attack
  C. Piggybacking attack
  D. Teardrop attack

Question 5

- Which of the following statements pertaining to packet filtering is incorrect?
  A. It is based on ACLs
  B. It is not application dependant
  C. It operates at the network layer
  D. It keeps track of the state of a connection

Question 5

- Which of the following statements pertaining to packet filtering is incorrect?
  A. It is based on ACLs
  B. It is not application dependant
  C. It operates at the network layer
  D. It keeps track of the state of a connection

Question 6

- What is the main characteristic of a multi-homed host?
  A. It is placed between two routers or firewalls
  B. It allows IP routing
  C. It has multiple network interfaces, each connected to separate networks
  D. It operates at multiple layers

Question 6

- What is the main characteristic of a multi-homed host?
  A. It is placed between two routers or firewalls
  B. It allows IP routing
  C. It has multiple network interfaces, each connected to separate networks
  D. It operates at multiple layers

Question 7

- One drawback of Application Level Firewall is that it reduces network performance due to the fact that it must analyze every packet and:
  A. Decide what to do with each application
  B. Decide what to do with each user
  C. Decide what to do with each port
  D. Decide what to do with each packet

Question 7

- One drawback of Application Level Firewall is that it reduces network performance due to the fact that it must analyze every packet and:
  A. Decide what to do with each application
  B. Decide what to do with each user
  C. Decide what to do with each port
  D. Decide what to do with each packet

Question 8

- Address Resolution Protocol (ARP) interrogates the network by sending out a?
  A. Broadcast
  B. Multicast
  C. Unicast
  D. Semicast

Question 8

- Address Resolution Protocol (ARP) interrogates the network by sending out a?
  - **A. Broadcast**
  - B. Multicast
  - C. Unicast
  - D. Semicast

Question 9

- As a result of a risk assessment, your security manager has determined that your organization needs to implement an intrusion detection system that can detect unknown attacks and can watch for unusual traffic behavior, such as a new service appearing on the network. What type of intrusion detection system would you select?

A. Protocol anomaly based
B. Pattern matching
C. Stateful matching
D. Traffic anomaly-based

Question 9

- As a result of a risk assessment, your security manager has determined that your organization needs to implement an intrusion detection system that can detect unknown attacks and can watch for unusual traffic behavior, such as a new service appearing on the network. What type of intrusion detection system would you select?

A. Protocol anomaly based
B. Pattern matching
C. Stateful matching
D. Traffic anomaly-based

Question 10

- What refers to legitimate users accessing networked services that would normally be restricted to them?
  A. Spoofing
  B. Piggybacking
  C. Eavesdropping
  D. Logon abuse

Question 10

- What refers to legitimate users accessing networked services that would normally be restricted to them?
  A. Spoofing
  B. Piggybacking
  C. Eavesdropping
  D. Logon abuse

Thank You! ☺