Introduction to Network Security:
Network basics and threats

CIS377

Dr. Atul Rawal

References:

Know the background

How the internet works (overview)

- https://www.youtube.com/watch?v=7_LPdttKXPc

How the Internet Works (several great focused videos) – watch after #1

https://www.youtube.com/playlist?list=PLzdnOPI1iJNfMRZm5DDxco3UdsFegvuB7

Network basics and threats

TOWSON UNIVERSITY

- Topics:
  - Basics of network (OSI model, DoD TCP/IP model)
  - Network attacks
  - Denial-of-Service attacks
  - Distributed Denial-of-Service attacks
  - Zombies and Botnets
- Learning Outcomes:

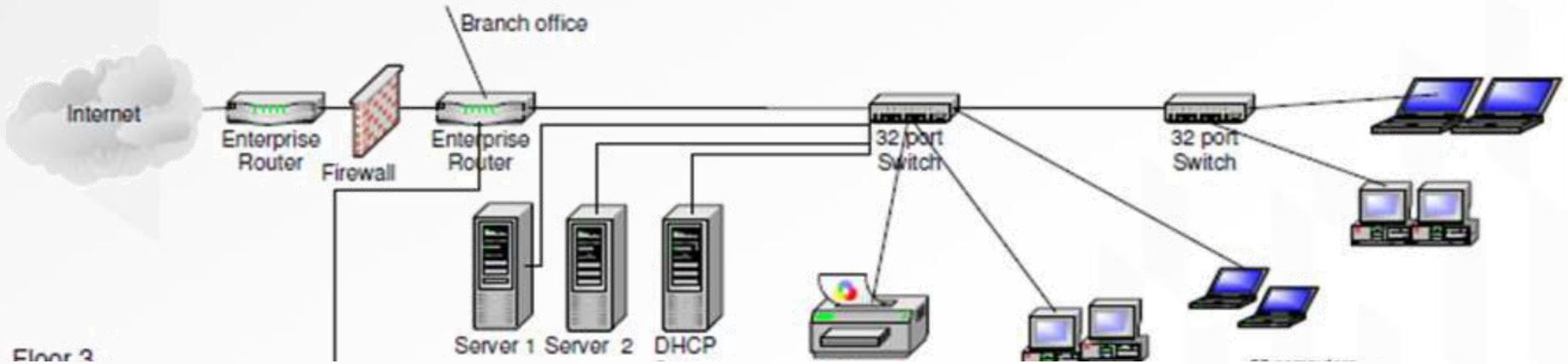
  Upon completion of this lesson:
  - Students will be able to understand network basics.
  - Students will be able to describe Denial-of-Service attacks.
  - Students will be able to explain Distributed DoS attacks.
  - Students will be able to define Zombies and Botnets.

Network basics

TOWSON UNIVERSITY

Network – System(s) implemented with a collection of interconnected components.

- A component (or host) can be a computer, printer, or any device capable of sending and/or receiving data generated by other components on the network.
- Interconnect link: can be a cable, air, optical fiber, or any medium which can transport a signal carrying information.



Background

TOWSON UNIVERSITY

How do data networks work?

- Systems communicate over a shared communication medium according to an agreed upon convention (standard).
- Several sets of standards currently exist:
  - DoD: TCP/IP
  - ISO: OSI model
  - Commercial: SNA, IPX, X.25, ...
  - Proprietary

TCP/IP Protocol suite

TOWSON UNIVERSITY

Transmission Control Protocol/Internet Protocol, is a suite of communication protocols used to interconnect network devices on the internet.

- Application layer: SMTP, HTTP, FTP, etc
- Transport layer: TCP, UDP
- Network layer: IP, ICMP, IGMP
- Data link layer: Device drivers (Ethernet, WiFi), ARP
- Physical Layer: Network Adapters

Network Transmission Media

TOWSON UNIVERSITY

Data travels either on wire or wirelessly, both of which are vulnerable.

- Cable
- Optical fiber
- Microwave
- Radio (WiFi, Satellite)

When data leave the protected environment, others along the way can view or intercept the data:

- Eavesdrop
- Wiretap
- Sniff

Transmission Control Protocol (TCP)

TOWSON UNIVERSITY

Connection oriented.

- Explicit set-up and tear-down of TCP session.

Reliable, in-order delivery.

- Checksums to detect corrupted data.
- Acknowledgments & retransmissions for reliable delivery.
- Sequence numbers to detect losses and reorder data.

Flow control.

- Prevent overflow of the receiver’s buffer space.

User Datagram Protocol (UDP)

TOWSON UNIVERSITY

User Datagram Protocol (UDP).

- IP plus port numbers to support (de)multiplexing.
- Optional error checking on the packet contents.

No delay for connection establishment.

- UDP just blasts away without any formal preliminaries.

Unreliable Message Delivery service.

Good for multimedia streaming.

OSI Reference Model

TOWSON UNIVERSITY

The Open Systems Interconnection (OSI).

Introduced in 1983 & adopted by ISO as an international standard in 1984.

Seven layers that computer systems use to communicate over a network.

- First standard model for network communications, adopted in the early 1980s.

OSI 7-layer model is still widely used, as it helps visualize and communicate how networks operate, and helps isolate and troubleshoot networking problems.

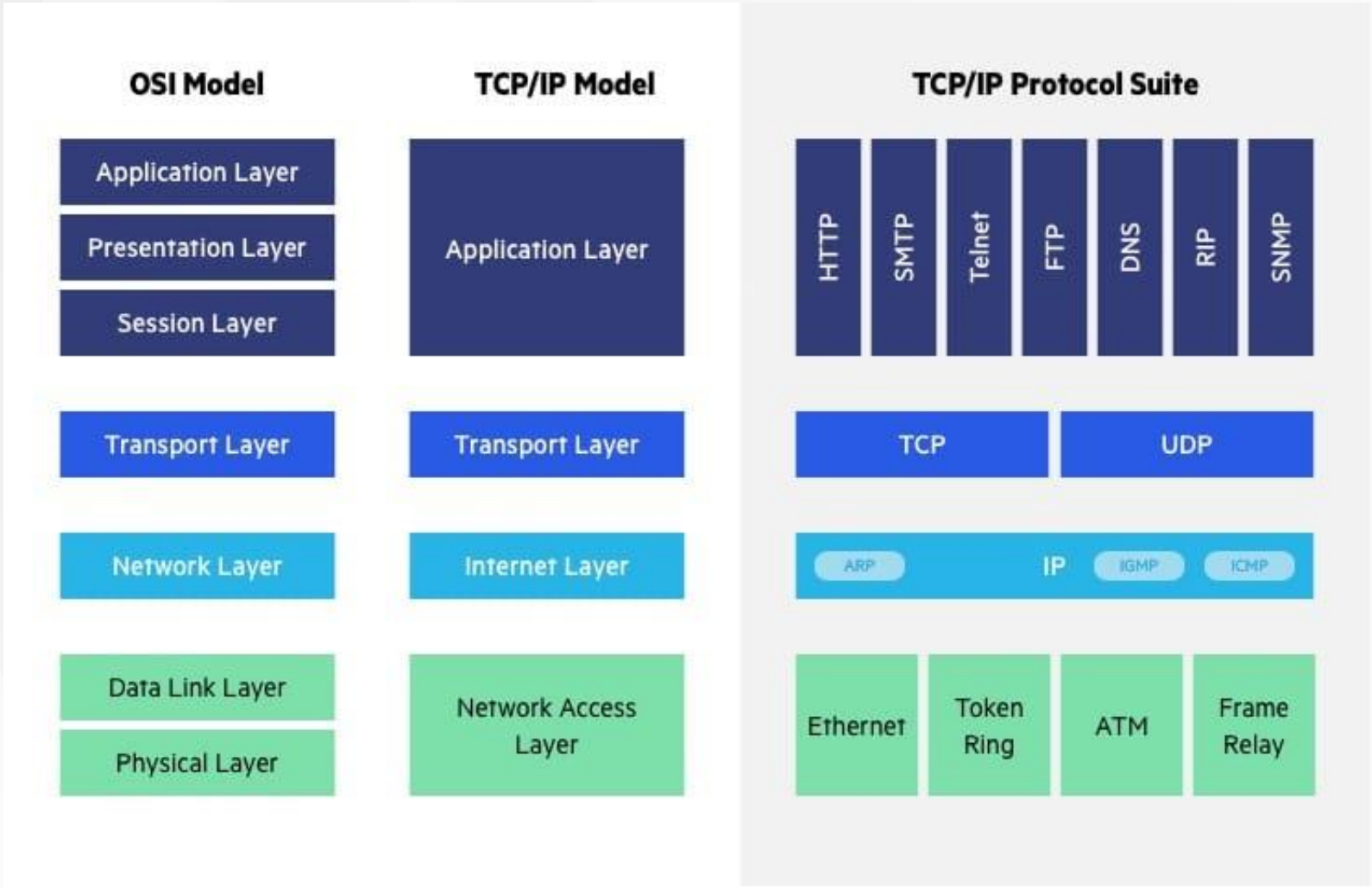
OSI Reference Model

TOWSON UNIVERSITY

7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

TCP/IP vs OSI Reference Model

TOWSON UNIVERSITY



Internet Control Message Protocol (ICMP)

TOWSON UNIVERSITY

Used by network devices, such as routers, to send error messages and operational information.

Ping is a computer network administration software utility used to test the reachability of a host on the network.

- Ping sends ICMP Echo Request packets to the target host and waiting for an ICMP Echo Reply.
- The program reports errors, packet loss, and a statistical summary of the results.

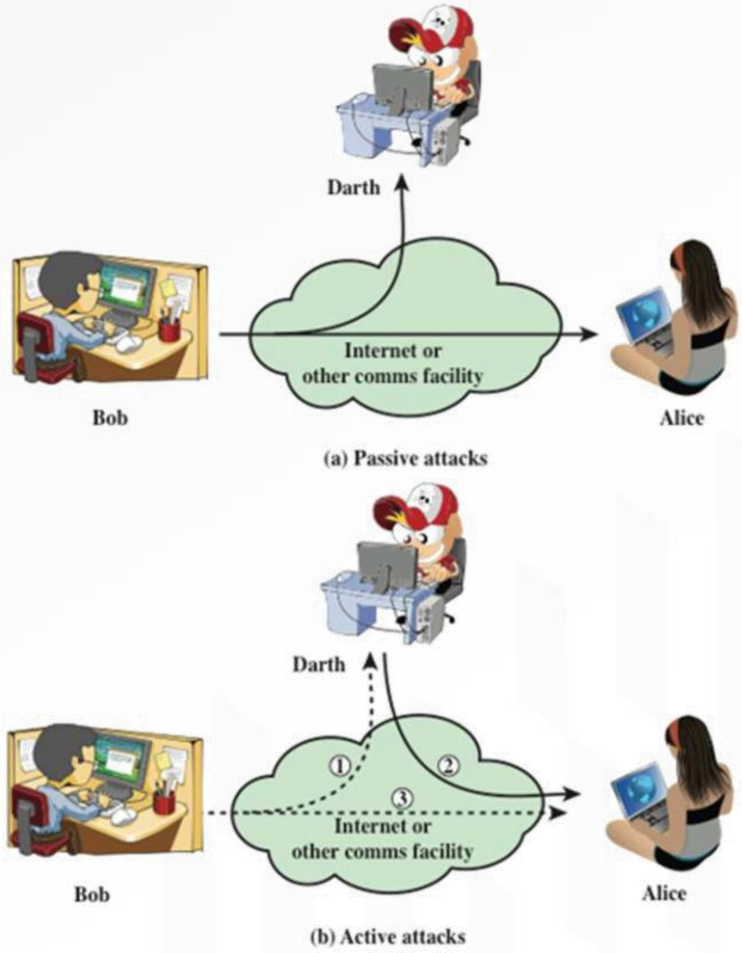
Security Attacks

A passive attack attempts to learn or make use of information from the system but does not affect system resources.

- e.g., eavesdropping on, or monitoring of, transmissions to obtain information that is being transmitted.
- Two types of passive attacks are:
  - The release of message contents.
  - Traffic analysis.

An active attack attempts to alter system resources or affect their operations.

- Involve some modification of the data stream or the creation of a false stream.



Denial of Service (DoS)

TOWSON UNIVERSITY

DoS - The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)

Denial of service ranges from complete loss of access to unacceptable slowing of service.

The source of a denial-of-service attack is typically difficult to determine.

Know the background

TOWSON UNIVERSITY

Routing and Packets

https://www.youtube.com/watch?v=AYdF7b3nMto

DoS attack: Ping of Death

TOWSON UNIVERSITY

In ping of death attack, a flood of ping commands will be sent to the victim.

Ping required the recipient to respond to the packet.

If the victim has smaller bandwidth, the response to the flood of ping commands may exhaust the victim's bandwidth.

DoS attack: SYN flood

TOWSON UNIVERSITY

In SYN flood attack, TCP packets with a spoofed source IP address request a connection to the victim's network.

The victim's network responds, but there will be no response from the source address.

However, the victim will wait with an open connection. This will eventually overwhelm it.

Know the background

TOWSON UNIVERSITY

- DNS and IP addresses
- https://www.youtube.com/watch?v=5o8CwafCxnU&t=336s

DoS Attack: DNS Spoofing

TOWSON UNIVERSITY

A domain name server (DNS) is a table that converts domain names like website.com into network addresses like 211.217.74.130; this process is called resolving the domain name.

In DNS spoofing attack, the attacker acts as the DNS server and quickly respond to a DNS lookup request with a attacker's network address. Therefore redirect the user to malicious sites.

Distributed Denial of Service (DDoS)

TOWSON UNIVERSITY

Distributed Denial of Service (DDoS) - A Denial of Service technique that uses numerous hosts to perform the attack.

To perform a distributed denial-of-service (or DDoS) attack, an attacker needs to do:

- Plant a Trojan horse on a target machine, and repeat this process with many targets. These targets are called zombies.
- If a victim is chosen, the attacker sends a signal to all the zombies, and the zombies will launch the attack to the victim.

Bots & Botnets

TOWSON UNIVERSITY

- Zombie/bot - A compromised computer under the control of an attacker.
- Bot code, a malware installed on the compromised computer to communicates with the attacker's server and perform the malicious activities.
- Botnets, a networks of bots controlled by an attacker to perform malicious activities.
- Botnets are often used to execute DDoS attacks.

Botnets command-and-control

TOWSON UNIVERSITY

People who infect machines to turn them into bots are called botmasters.

The botmaster is called a command-and-control center. It control the individual bots, sends commands to the bots, such as when to start/stop and attack against which victim.

Network encryption and protocols

TOWSON UNIVERSITY

Topics:

- Network encryption concepts and tools.
- Network protocols (IPv4, IPv6, SSH, SSL/TLS, IPSec, HTTPS).

Learning Outcomes:

Upon completion of this lesson:

- Students will be able to understand some of the network protocols which have security features built in (such as SSL/TLS, HTTPS).
- Students will be able to describe network data encryption.

Warm up

TOWSON UNIVERSITY

How to protect the data while it's transferring over the network?

Encryption for network

TOWSON UNIVERSITY

Link Encryption

- Data are encrypted right before the transfer over the physical communications link and are decrypted when they arrive at the destination system.
- Encryption occurs at lower levels in the network.
- Link encryption protects the message in transit between two computers, but the message is in plaintext inside the hosts.

Encryption for network (cont.)

TOWSON UNIVERSITY

End-to-End Encryption

- End-to-end encryption provides security from one end of a transmission to the other.
- The encryption is performed at the highest levels (usually at the application layer).
- The encryption can be done by software running on the host computer.
- Decryption will be done by the software on the other end.

Link vs. End-to-End Encryption

TOWSON UNIVERSITY

Which is better?

Link encryption:

- Faster.
- Easier for the user.
- Uses fewer keys.
- Encrypts all traffic.

End-to-end encryption:

- More flexible.
- Can be used selectively.
- Done at the user level.
- Can be integrated with the application.

Browser Encryption

TOWSON UNIVERSITY

Browsers can encrypt data for protection during transmission.

The browser and the server negotiate a common encryption key, so even if an attacker does hijack a session at the TCP or IP protocol level, the attacker cannot exchange data because of not having the proper key.

- SSH encryption.
- SSL and TLS encryption.

Secure Shell (SSH)

TOWSON UNIVERSITY

- Originally developed for UNIX but now available on most operating systems.
- SSH provides an authenticated, encrypted path to the shell over the network.
- The SSH protocol involves negotiation between local and remote sites to agree on encryption algorithm and authentication.
- SSH protects against spoofing attacks and modification of data in communication.

SSL and TLS

TOWSON UNIVERSITY

- Secure Sockets Layer (SSL) was designed in the 1990s to protect communication between a web browser and server.
- In 1999, it was renamed to Transport Layer Security (TLS).
- TLS is designed use TCP to provide a reliable end-to-end secure service.
- SSL is implemented in transport layer in the network stack.

HTTPS (HTTP over SSL)

TOWSON UNIVERSITY

- HTTPS - Combination of HTTP (HyperText Transfer Protocol) and SSL to implement secure communication between a web browser and a web server.
- Built into all modern Web browsers

  URL addresses begin with https://

BRIAN BARRETT SECURITY 07.24.18 01:00 PM

GOOGLE CHROME NOW LABELS HTTP SITES AS 'NOT SECURE'

Onion Routing

TOWSON UNIVERSITY

- Both link encryption and end-to-end encryption, the transferred data was secured by encryption. However, the addressing data were exposed.
- Onion routing prevents an eavesdropper from learning source, destination, or content of data in transit in a network.
  - The intermediate host that sends the message to the final destination cannot determine the original sender, and.
  - The host that received the message from the original sender cannot determine the ultimate destination.

IP Address (version 4)

TOWSON UNIVERSITY

32-bit (4-byte) addressing.

- The total number of IPv4 addresses is 4 294 967 296

The text form of the IPv4 address is nnn.nnn.nnn.nnn, where each n is a decimal digit.

IP address version 6

TOWSON UNIVERSITY

128 bits long (16 bytes) addressing

The text form of the IPv6 address is xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, where each x is a hexadecimal digit, representing 4 bits.

IPSec

TOWSON UNIVERSITY

- As a part of the IPv6 suite, the IETF (Internet Engineering Task Force) adopted IPSec, or the IP Security Protocol Suite.
- IPSec was designed to address some drawbacks of IPv4, such as being subject to spoofing, eavesdropping, and session hijacking.
- IPSec is implemented at the IP layer, so it affects all layers above it, in particular TCP and UDP. And it does not require any change to the existing TCP and UDP protocols.

Goals of IPSec

TOWSON UNIVERSITY

- Prevent from IP spoofing.
- Protect integrity and/or confidentiality of packets.
- Prevent replay attack.
  - Relay attack - An attack that involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access.
- Provide security for upper layer protocols and applications.

IPSec modes

TOWSON UNIVERSITY

- There are two operation modes in IPSec: transport mode and tunnel mode.
- In transport mode, security protection is provided to traffic from one host to another (end-to-end).
- In tunnel mode, security protection is provided to traffic from one gateway of a network to the gateway of another network (virtual private network, VPN).

Virtual Private Network

TOWSON UNIVERSITY

- A virtual network, built on top of existing physical networks, that provides a secure communications tunnel for data and other information transmitted between networks.
- VPN reduces the overall telecommunication infrastructure, and the cost of management, maintenance of equipment.

Summary

TOWSON UNIVERSITY

Network encryption concepts and tools.

- Network protocols:
  - IPv4
  - IPv6
  - SSH
  - SSL/TLS
  - IPSec
  - HTTPS

Introduction to Network Security:
Network defense technologies.

CIS377

Dr. Atul Rawal

References:

Network defense technologies

TOWSON UNIVERSITY

Topics:

- Different types of firewalls and their advantages.
- Intrusion detection and prevention systems.
- Honeypot.

Learning Outcomes:

Upon completion of this lesson:

- Students will be able to understand different types of firewalls and what are the advantages of each type.
- Students will be able to understand intrusion detection and prevention systems.
- Students will be able to describe honeypots and what is the purpose of setting up a honeypot.

Discussion

TOWSON UNIVERSITY

Do you have firewall installed on your computers?

What are the purpose of having a firewall?

Firewalls

TOWSON UNIVERSITY

Firewall - A device or program that controls the flow of network traffic between networks or hosts that employ differing security postures.

Firewalls implement security policies, or set of rules that determine what traffic can or cannot pass through it.

Firewall Security Policy

TOWSON UNIVERSITY

Lists the types of traffic authorized to pass through the firewall.

Usually include address ranges, protocols, actions.

Rule	Type	Source Address	Destination Address	Destination Port	Action
1	TCP	*	192.168.1.*	25	Permit
2	UDP	*	192.168.1.*	69	Permit
3	TCP	192.168.1.*	*	80	Permit
4	TCP	*	192.168.1.18	80	Permit
5	TCP	*	192.168.1.*	*	Deny
6	UDP	*	192.168.1.*	*	Deny

Firewall security policy example

TOWSON UNIVERSITY

In this example firewall configuration,

- External traffic can reach the entire internal network on TCP port 25 and UDP port 69.
- Internal traffic can go out to external network on port 80.
- External traffic can reach TCP/80 on one internal server (192.168.1.18).
- All other traffic from external to internal is denied.

Rule	Type	Source Address	Destination Address	Destination Port	Action
1	TCP	*	192.168.1.*	25	Permit
2	UDP	*	192.168.1.*	69	Permit
3	TCP	192.168.1.*	*	80	Permit
4	TCP	*	192.168.1.18	80	Permit
5	TCP	*	192.168.1.*	*	Deny
6	UDP	*	192.168.1.*	*	Deny

Firewall capabilities

TOWSON UNIVERSITY

- Defines a single point to check network traffic
- Provides a location for monitoring security events
- Logs can be used to examine the traffic
- It can provide network address translation.

Firewall limitations

TOWSON UNIVERSITY

- If the traffic bypass the firewall, then the firewall cannot protect it.
- If the firewall is misconfigured, it may not provide enough protection.
- Cannot protect internal attacks.

Types of Firewalls

TOWSON UNIVERSITY

Packet filtering gateways:

- Applies rules to each incoming and outgoing IP packet.
- Decisions made on per-packet basis.
- No state information saved.

Stateful inspection firewalls:

- Specific rules for TCP traffic by using a directory of TCP connections.
- It reviews packet information and also records TCP connection information, such as TCP sequence numbers.

Types of Firewalls (cont.)

TOWSON UNIVERSITY

Application-level gateways(proxies)

- Acts as a relay of application-level traffic.
- It tends to be more secure than packet filters, because it only scrutinize a few allowable applications.
- It is easy to log and audit all incoming traffic at the application level.

Personal or host-based firewalls

- Controls traffic between a personal computer and the internet.
- Available in OS or can be provided as an add-on program.
- Less complex.

Intrusion

TOWSON UNIVERSITY

Intrusion - Unauthorized act of bypassing the security mechanisms of a system.

Classes of intruders:

- Cyber Criminals (financial reward).
- Motivated by social or political causes.
- National states.
- Hackers with other motivations.

Examples of Intrusion

TOWSON UNIVERSITY

- Web server defacement.
- Guessing passwords.
- Man-in-the-middle attack.
- Copying databases containing personal identities.
- Viewing sensitive data without authorization.
- Remote root compromise.
- Distributing malware.
- Impersonating an executive to get information.
- …

Intrusion Detection Systems (IDS)

TOWSON UNIVERSITY

Hardware or software product that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches.

IDS components

TOWSON UNIVERSITY

- Sensors - collect data (network packets, system call traces, log files…)
- Analyzers – get input from sensors and determine if intrusion has occurred or not.
- User interface - view output or control system behavior.
- IDSs can be effective against known, less sophisticated attacks. They are less likely to be effective against the more sophisticated, targeted attacks, or zero-day exploits.

Types of IDS

TOWSON UNIVERSITY

Detection method:

- Signature-based.
- Heuristic.

Scope:

- Host-based IDS (HIDS).
- Network-based IDS (NIDS).

Capability:

- Passive.
- Active, also known as intrusion prevention systems (IPS).

Signature-based vs Heuristic IDSs

TOWSON UNIVERSITY

Signature-based IDSs:

- Perform simple pattern-matching and report situations that match a pattern (signature) of a known attack type.
- Can only detect known patterns.

Heuristic IDSs:

- Looks for patterns of behavior that are out of the ordinary.
- Build a model of acceptable behavior and flag exceptions to that model.
- Learn characteristics of unacceptable behavior over time.

HIDS vs NIDS

TOWSON UNIVERSITY

Host-based IDS (HIDS):

- Monitors the characteristics of a single host for suspicious activity.
- Goal: protect one machine and its data.

Network-based IDS (NIDS):

- Monitors network traffic and analyzes network, transport, and application protocols to identify suspicious activity.
- Goal: protect the entire network.

Distributed or hybrid IDS:

- Combines information from both host and network based IDSs, therefore better identify any intrusion activity.

Intrusion Prevention systems (IPS)

TOWSON UNIVERSITY

- Intrusion prevention systems (IPS) - System(s) which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.
- IPS is an extension of an IDS that includes the capability to attempt to block or prevent detected malicious activity.
- As response to an detected attack, it may block access, reject traffic.

Honeypots

TOWSON UNIVERSITY

Honeypot - A system (e.g., a Web server) or system resource (e.g., a file on a server) that is designed to be attractive to potential crackers and intruders and has no authorized users other than its administrators.

Honeypots (cont.)

TOWSON UNIVERSITY

Honeypots are designed to:

- Lure a potential attacker away from critical systems.
- Collect information about the attacker's activity.
- Encourage the attacker to stay on the system long enough for administrators to respond.
- Resources that have no production value.
- Trigger monitors and event loggers when malicious activity detected.

Summary

TOWSON UNIVERSITY

Topics:

- Different types of firewalls and their advantages.
- Intrusion detection and prevention systems.
- Honeypot.