AUTOMATIC CYBER THREAT DETECTION AND ANALYSIS

➢ Plan

- ❖Basic Network Security
- ❖Firewalls
- ❖System Auditing
- ❖AI & ML

What is Threat Detection?

- Practice of analyzing the entirety of a security ecosystem to identify any malicious activity that could compromise the network.
- If a threat is detected, then mitigation efforts must be enacted to properly neutralize the threat before it can exploit any present vulnerabilities.
- When it comes to detecting and mitigating threats, speed is crucial.
- Security programs must be able to detect threats quickly and efficiently so attackers don't have enough time to root around in sensitive data.

➢ Several methods available in the defender's arsenal:

1. **Leveraging Threat Intelligence:**
   - ❖ way of looking at signature data from previously seen attacks and comparing it to enterprise data to identify threats.

2. **Analyzing User and Attacker Behavior Analytics**

   - ❖ With user behavior analytics, an organization is able to gain a baseline understanding of what normal behavior for an employee

   - ❖ what kind of data they access, what times they log on, and where they are physically located

   - ❖ With attacker behavior analytics, there's no "baseline" of activity to compare information to; instead, small, seemingly unrelated activities detected on the network over time

3. Setting Intruder Traps

- ❖ Some targets are just too tempting for an attacker to pass up.

4.Conducting Threat Hunts

- ➢ **Threat Detection Requires a Two-Pronged Approach:**
  - ❖ Security event threat detection technology
  - ❖ Network threat detection technology
  - ❖ Endpoint threat detection technology

Security Through Obscurity

- Security through obscurity (STO) is a process of implementing security within a system by enforcing secrecy and confidentiality of the system's internal design architecture.
- STO is based on the idea that any information system is secure as long as security vulnerabilities remain hidden.
- create systems which attempt to be algorithmically secure.

➢ TCP/IP Evolution and Security

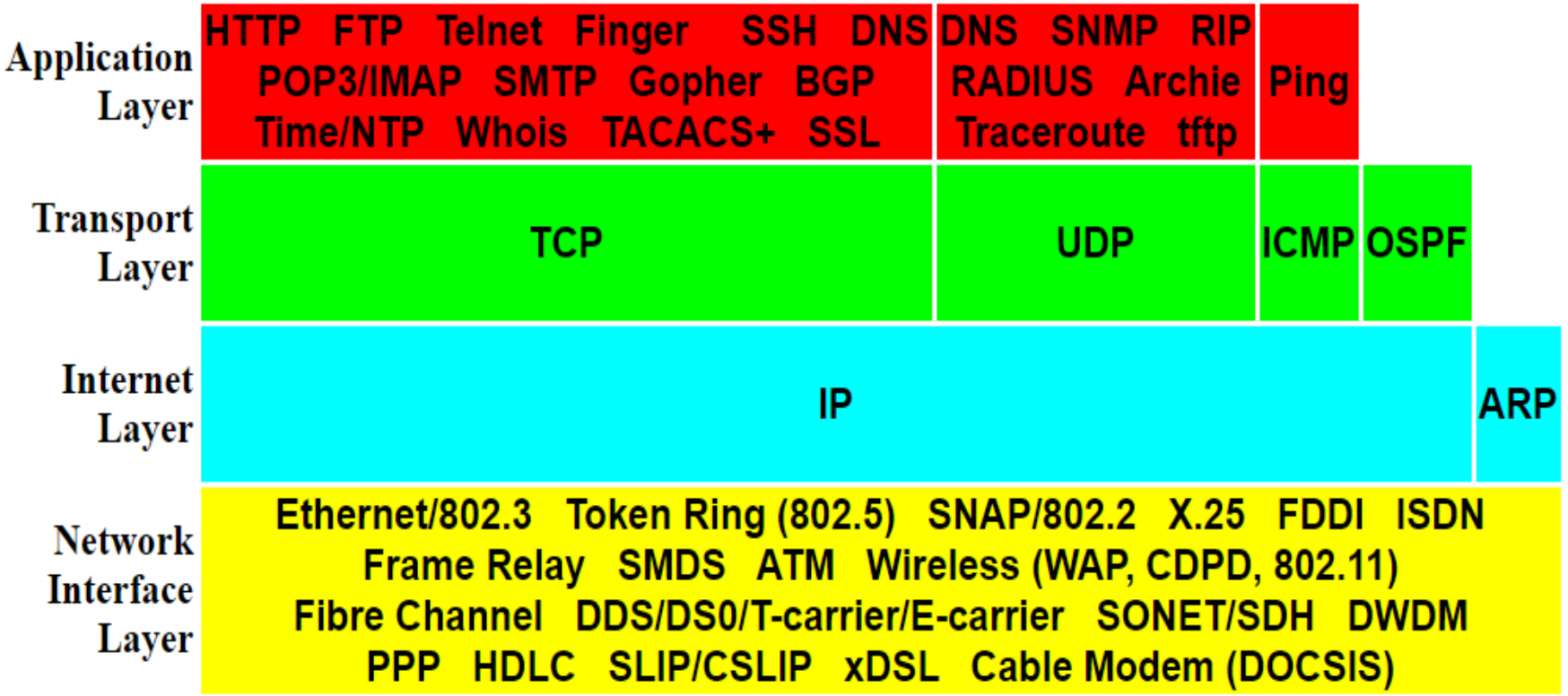
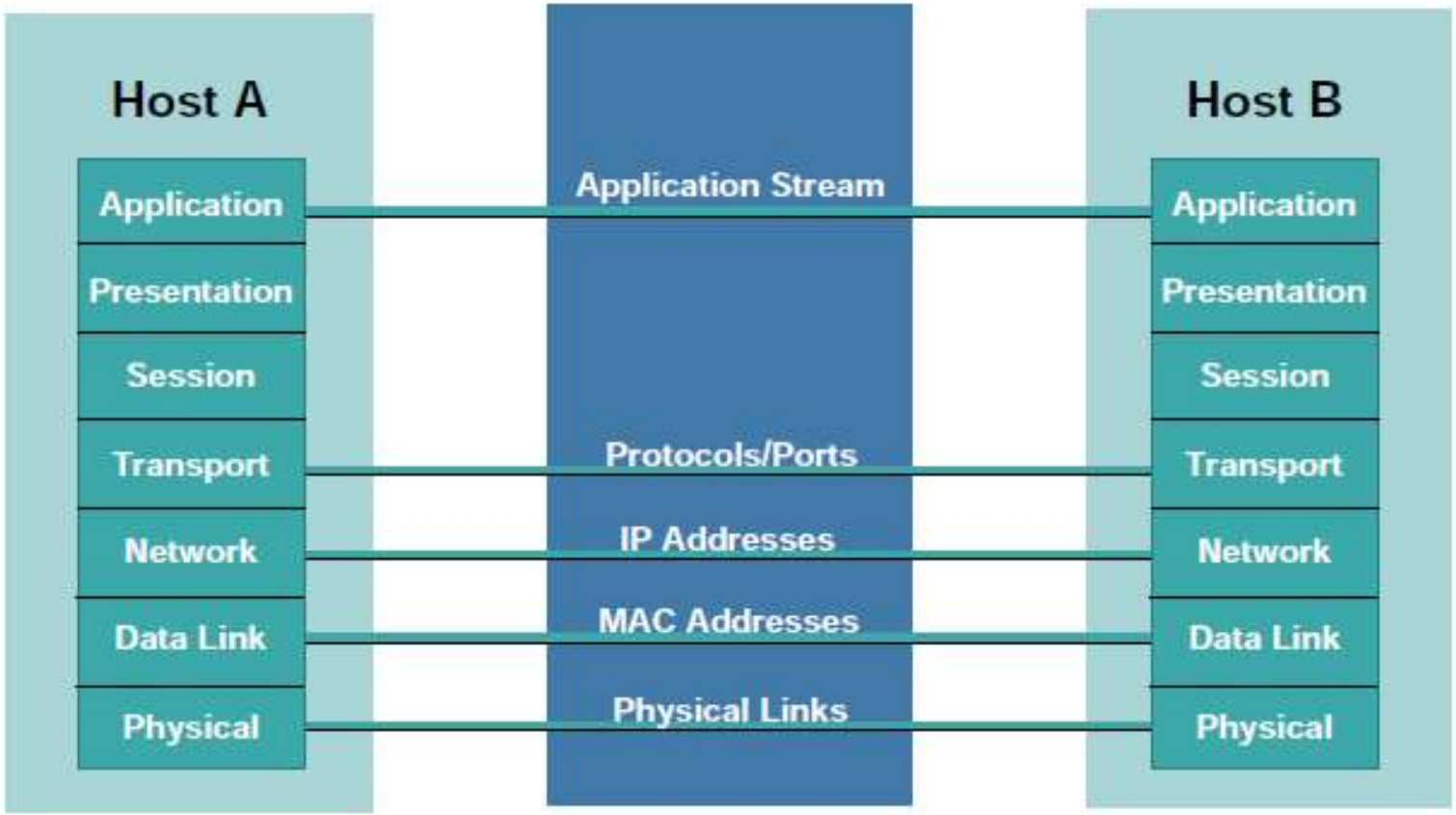
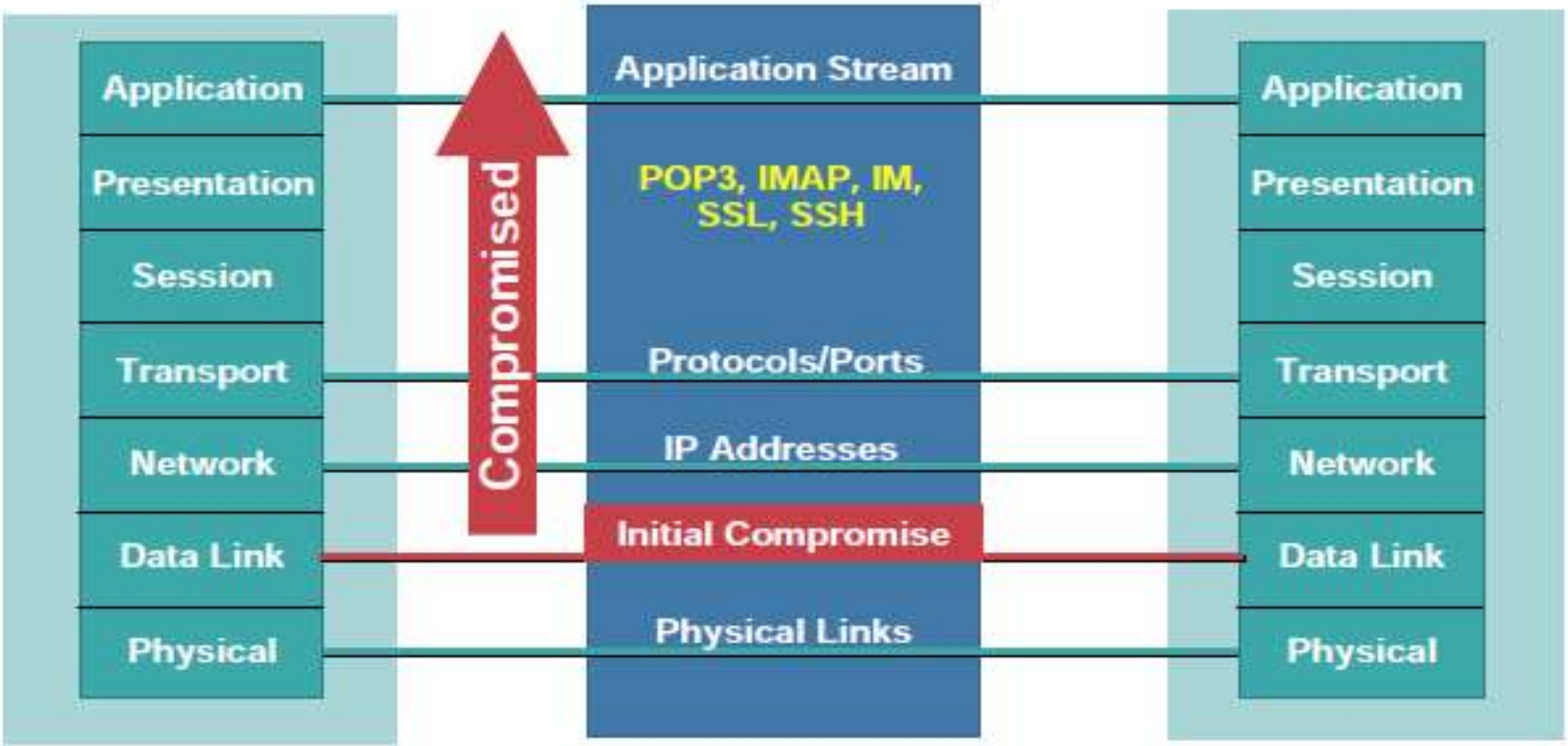


FIGURE 2. Abbreviated TCP/IP protocol stack.

OSI Was Built to Allow Different Layers to Work Without the Knowledge of Each Other



- Unfortunately this means if one layer is hacked, communications are compromised without the other layers being aware of the problem
- Security is only as strong as the weakest link
- When it comes to networking, layer 2 can be a VERY weak link



➢ IP Spoofing

- Spoofing is an impersonation of a user, device or client on the Internet. It's often used during a cyber attack to disguise the source of attack traffic.

- The most common forms of spoofing are:
  - **DNS server spoofing** – Modifies a DNS server in order to redirect a domain name to a different IP address. It's typically used to spread viruses.
  - **ARP spoofing** – Links a perpetrator's MAC address to a legitimate IP address through spoofed ARP messages. It's typically used in denial of service (DoS) and man-in-the-middle assaults.
  - **IP address spoofing** – Disguises an attacker's origin IP. It's typically used in DoS assaults.

IPv4 Network Packet Headers

Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time To Live		Protocol	Header Checksum	
Source IP Address				
Destination IP Address				
Options				
Data				

❖ IP address spoofing is used for two reasons in DDoS attacks:

- To mask botnet device locations
- To stage a reflected assault.

❖ IP address spoofing in application layer attacks

- For application layer connections to be established, the host and visitor are required to engage in a process of mutual verification, known as a TCP three-way handshake.

- The process consists of the following exchange
  - Visitor sends a SYN packet to a host.
  - Host replies with a SYN-ACK.
  - Visitor acknowledges receipt of the SYN-ACK by replying with an ACK packet.

Source IP spoofing makes the third step of this process impossible, as it prohibits the visitor from ever receiving the SYN-ACK reply, which is sent to the spoofed IP address.

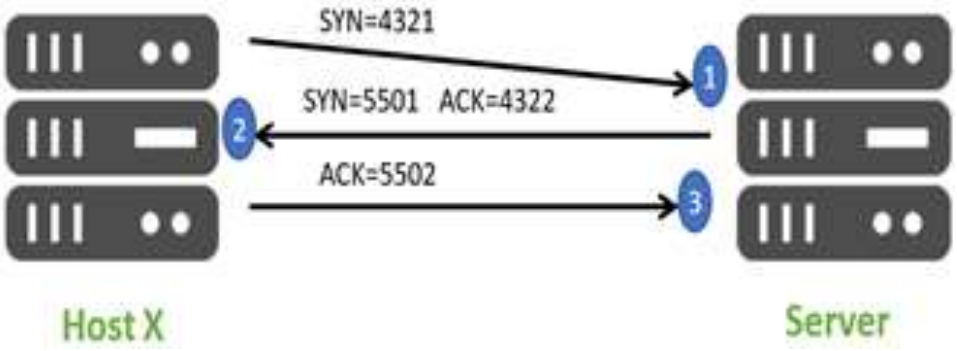
❖ Anti-spoofing in DDoS protection

- ❖ To overcome this, modern mitigation solutions rely on deep packet inspection (DPI), which uses granular analysis of all packet headers rather than just source IP address.

- ❖ With DPI, mitigation solutions are able to cross-examine the content of different packet headers to uncover other metrics to identify and filter out malicious traffic.

DPI is likely to cause performance degradation—sometimes even making the protected network almost completely unresponsive.

➢ TCP Sequence Number Attack



- ❖ sequence numbers play a big part in TCP communications.
- ❖ TCP uses the sequence number field to take responsibility for ensuring that data packets are delivered to higher layers in the protocol stack in their correct order.
- ❖ An attacker listening into a TCP exchange could in principle determine the flow of sequence numbers.

❖ Anatomy of a TCP Sequence Prediction Attack

- An attacker would spend some time monitoring the data flow.
- The attacker would then cut off the other system (which is trusted by the target) from the communication, perhaps via a Denial of Service (DoS) attack.
- Attacker prepares a packet with the source IP address of the trusted system, and the expected sequence number.

❖ Measures to Prevent a TCP Sequence Prediction Attack

- Internet Engineering Task Force (IETF) issued a renewed standard (RFC 6528) in 2012, setting out an improved algorithm for generating Initial Sequence Numbers.
- Operating system manufacturers responded to the threat by introducing new and more unpredictable methods of sequence number generation

➢ Packet Flooding

- ❖ A UDP flood is a form of volumetric Denial-of-Service (DoS) attack where the attacker targets and overwhelms random ports on the host.
- ❖ In this type of attack, the host looks for applications associated with these datagrams.
- ❖ When none are found, the host issues a “Destination Unreachable” packet back to the sender.
- ❖ System becomes inundated and therefore unresponsive to legitimate traffic.

❖ How to Mitigate and Prevent a UDP Flood Attack?

- Most operating systems attempt to limit the response rate of ICMP packets with the goal of stopping DDoS attacks.
- Using deep packet inspection, can be used to balance the attack load across a network of scrubbing servers.
- Scrubbing software that is designed to look at IP reputation, abnormal attributes and suspicious behavior, can uncover and filter out malicious DDoS packets.

➢ Packet Sniffing

- Packet sniffing is the practice of gathering, collecting, and logging some or all packets that pass through a computer network, regardless of how the packet is addressed.

- When you install packet sniffing software, the **network interface card (NIC)**—the interface between your computer and the network—must be set to **promiscuous mode.**

- **Two main types of packet sniffers**
  - **Hardware Packet Sniffers**
    - Plugged directly into the physical network at the appropriate location.
  - **Software Packet Sniffers**

➢ Packet Filtering

- ❖ Packet filtering is a network security mechanism that works by controlling what data can flow to and from a network.
- ❖ The basic device that interconnects IP networks is called a *router*.
- ❖ A router may be a dedicated piece of hardware that has no other purpose, or it may be a piece of software that runs on a general-purpose PC.
- ❖ Packet filtering lets you control (allow or disallow) data transfer based on:
  - The address the data is (supposedly) coming from
  - The address the data is going to
  - The session and application protocols being used to transfer the data

Ex: **Don't let anybody use Telnet (an application protocol) to log in from the outside.**
or:
Let everybody send us email via SMTP (another application protocol).

❖ Advantages of Packet Filtering

- One screening router can help protect an entire network
- Packet filtering doesn't require user knowledge or cooperation
- Packet filtering is widely available in many routers

❖ Disadvantages of Packet Filtering

- Current filtering tools are not perfect
- Some protocols are not well suited to packet filtering
- Some policies can't readily be enforced by normal packet filtering routers

Firewalls

➢ Types of Firewall Architectures

- ❖ A firewall is a network security system designed to prevent unauthorized access to or from a private network.
- ❖ All messages entering or leaving the intranet pass through the firewall.
- ❖ It examines each message and blocks those that do not meet the specified security criteria.
- ❖ *Firewall types*
  - *Hardware*
  - *Software*

- There are several types of firewall techniques that will prevent potentially harmful information from getting through:

  - **Packet Filter:** Looks at each packet entering or leaving the network.

  - **Application Gateway:** Applies security mechanisms to specific applications, such as FTP and Telnet servers.

  - **Circuit-level Gateway:** Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

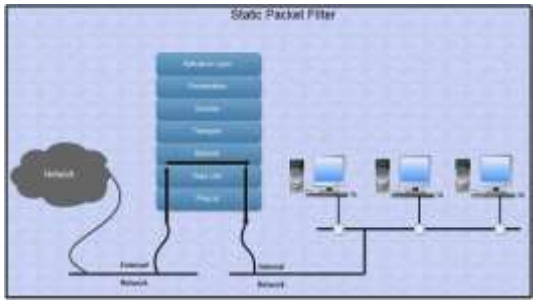
  - **Proxy Server:** Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

❖ **Firewalls utilize following technologies for firewall architectures:**

1. Static packet filter
2. Dynamic (state aware) packet filter
3. Circuit level gateway
4. Application level gateway (proxy)
5. Stateful inspection
6. Cutoff proxy
7. Air gap.

1. Static Packet Filter

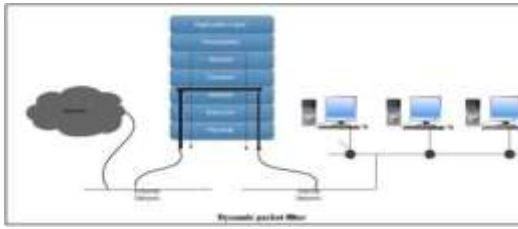
- Packet filtering policies may be based upon any of the following:
  - Allowing or disallowing packets on the basis of the source IP address (sender)
  - Allowing or disallowing packets on the basis of their destination port (service port)
  - Allowing or disallowing packets according to protocol.



- **Advantages**
  - Low impact on network performance
  - Low cost.
- **Disadvantages**
  - Operates only at network layer therefore it only examines IP and TCP headers
  - Unaware of packet payload-offers low level of security.
  - Lacks state awareness-may require numerous ports be left open to facilitate services that use dynamically allocated ports.
  - Susceptible to IP spoofing
  - Difficult to create rules (order of precedence).

2. Dynamic (State Aware) Packet filter

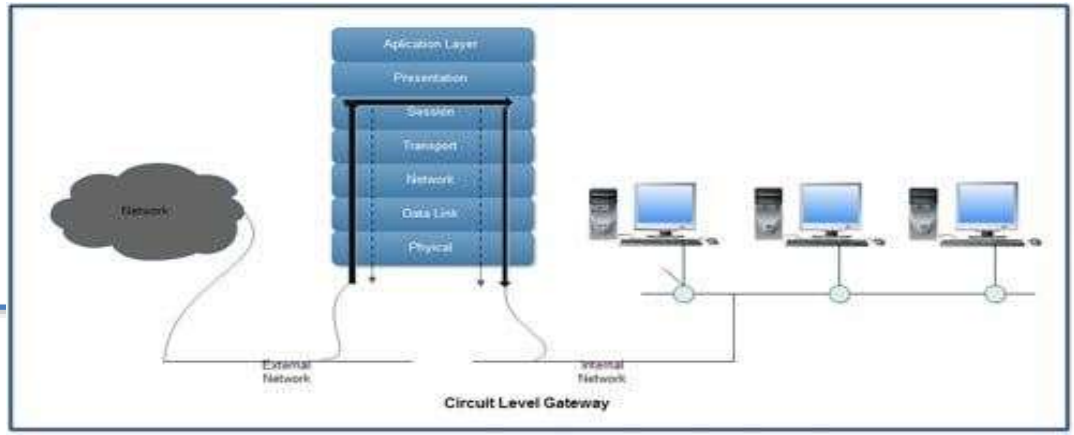
- A dynamic packet filter can monitor the state of active connections and use the information obtained to determine which network packets to allow through the firewall.



- **Advantages**
  - Low cost
  - State awareness provides measurable .performance benefit, scalability and extensibility.
- **Disadvantages**
  - Operates only at network layer therefore, it only examines IP and TCP headers.
  - Unaware of packet payload-offers low level of security
  - Susceptible to IP spoofing
  - Difficult to create rules (order of precedence)
  - Can introduce additional risk if connections
    Can be established without following the RFC-recommended 3 way-handshake.

3. Circuit level Gateway

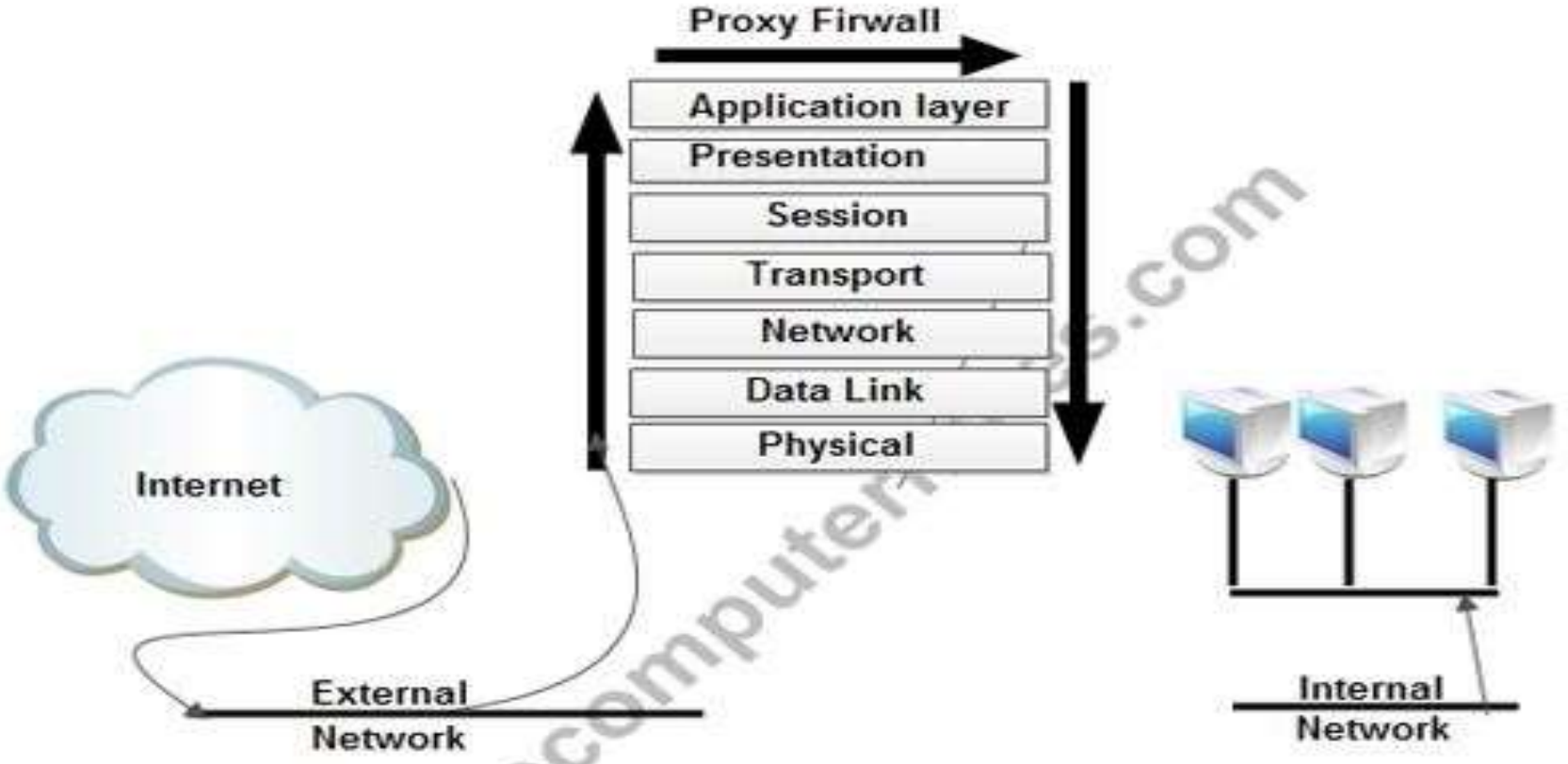
- The circuit level gateway operates at the session layer-OSI layer 5.
- **Advantages**
  - Low to moderate impact on network performance
  - Breaks direct connection to server behind firewall
  - Higher level of security than a static or dynamic (state aware) packet filter
  - Provides services for a wide range of protocols.
- **Disadvantages**
  - Shares many of the same negative issues associated with packet filters
  - Allows any data to simply pass through the connection
  - Only provides for a low to moderate level of security.



4. Application level Gateway

- A firewall that filters information at the application level blocks all IP traffic between the private network and the Internet.
- The proxies are application specific
- The proxies examine the entire packet and can filter packets at the application layer of the OSI model.

- **Advantages**
  - Better logging handling of traffic
  - State aware of services (FTP etc.)
  - Strong application proxy that inspects protocol header lengths can eliminate an entire class of buffer overrun attacks
  - Highest level of security.
- **Disadvantages**
  - Complex setup of application firewall needs more and detailed attentions to the applications that use the gateway.



Application Level Gateway Firewall

5. Stateful Inspection

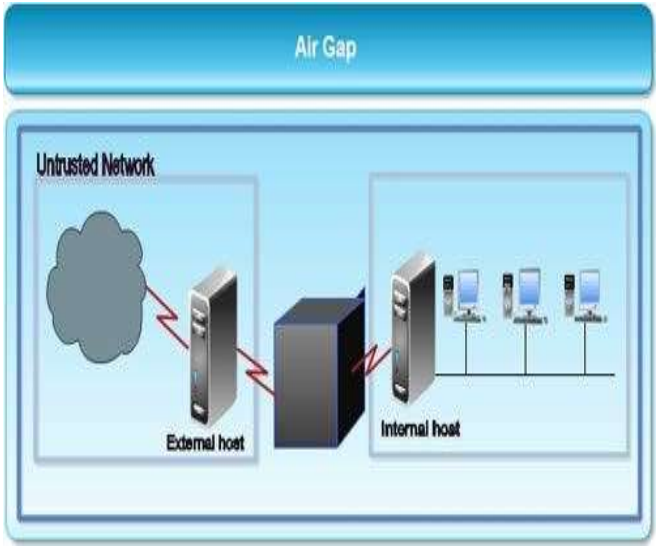
- Stateful inspection combines the many aspects of dynamic packet filtering, circuit *level* and application level gateways.
- Stateful firewalls remember information about previously passed packets and are considered much more secure.
- A unique limitation of one popular stateful inspection implementation is that it does not provide the ability to inspect sequence numbers on outbound packets from users behind the firewall.

- **Advantages**
  - Offers the ability to inspect all seven layers of the OSI model and is user configurable to customize specific filter constructs
  - Does not break the client server model
- **Disadvantages**
  - The single-threaded process of the stateful inspection engine has a dramatic impact on performance.

5. Air Gap

- This is an extreme kind of firewall where there is no direct or automated connection between two devices.
- Air gap technology provides a physical gap between trusted and untrusted networks
- In air gap technology, the external client connection "causes the connection data to be written to an SCSI e-Disk.
- The internal connection then reads this data from the SCSI e-Disk.

- **Advantages**
  - Inside is insulated from outside
  - Packets are not "automatically" passed through
  - Only explicitly launched services work
  - No unexpected traffic via other sockets.



System Auditing

➢ What Is an IT Security Audit?

❖ A network security audit is a technical assessment of an organization's IT infrastructure—their operating systems, applications, and more.

❖ Who can conduct an audit in the first place

1. Internal Auditors
2. External Auditors
3. Manual Audits
4. Automated Audits

IT security standards in existence today

- **ISO Compliance**
  - The ISO/IEC 27000 family of standards are some of the most relevant to system administrators, as these standards focus on keeping information assets secure.
- **HIPAA Security Rule:**
  - The HIPAA Security Rule outlines specific guidelines pertaining to exactly how organizations should protect patients' electronic personal health information.
- **PCI DSS Compliance:**
  - The PCI DSS compliance standard applies directly to companies dealing with any sort of customer payment.

- **Automated Audit Assessment Tools:**
  - SolarWinds Access Rights Manager
  - ManageEngine EventLog Manager

➢ Common Web App Vulnerabilities

According to OWASP, the top 10 most common application vulnerabilities include:

1. **Injection.** An injection happens when a bad actor sends invalid data to the web app to make it operate differently from the intended purpose of the application.

2. **Broken Authentication.** A broken authentication vulnerability allows a bad actor to gain control over an account within a system or the entire system.

3. **Sensitive Data Exposure.** Sensitive data exposure means data is vulnerable to being exploited by a bad actor when it should have been protected.

4. **XML External Entities (XXE).** A type of attack against an application that parses XML input and occurs when XML input containing a reference to an external entity is processed by a weakly configured XML parser.

5. **Broken Access Control.** When components of a web application are accessible instead of being protected like they should be, leaving them vulnerable to data breaches.

6. Security Misconfigurations. Incorrectly misconfiguring a web application provides bad actors with an easy way in to exploit sensitive information.

7. Cross Site Scripting (XSS). An XSS attack means a bad actor injects malicious client-side scripts into a web application.

8. Insecure Deserialization. Bad actors will exploit anything that interacts with a web application—from URLs to serialized objects—to gain access.

9. Using Components with Known Vulnerabilities. Instances such as missed software and update change logs can serve as big tip-offs for bad actors looking for ins into a web application. Disregarding updates can allow a known vulnerability to survive within a system.

10. Insufficient Logging and Monitoring. Lack of efficient logging and monitoring processes increases the chances of a web app being compromised.

➢ Practical Solutions for Protecting Web Apps:

- ❖ **Passive Protection:**
- ❖ **Active Protection:** to protect against browser data exfiltration
- ❖ **Real-Time Threat Notification:** to alert the business if code, page tampering or analysis is attempted that can initiate an immediate operational response — such as shutting down attacker accounts or updating web code protection to counter an attack.

How an IDS Works

- An IDS deploys sensors that monitor designated key points throughout an IT network.
- Administrators develop detection content that they distribute throughout the IDS platform.
- An IDS captures small amounts of security-critical data and transmits it back to the administrator for analysis.
- When a cyber attack occurs, the IDS detects the attack in real-time.
- IDS administrators can address and disrupt cyber attacks as they occur.
- Afterward, the IDS can perform an assessment of the attack to determine weaknesses in the network.

➢ Types of Intrusion Detection Systems

- ***Host-Based IDS:*** operate on individual desktop or remote devices within a network.
- ***Network-Based IDS:*** monitor activity across strategic points over an entire network.
- ***Stack IDS:*** monitor network packets in transit through the network stack (TCP/IP).
- ***Signature-Based IDS:*** searches a string of malicious bytes or sequences.
- ***Anomaly-Based IDS:*** works on the concept of a baseline for network behavior.

Virus Name	*String Pattern (Signature)*
Accom.1280	89C3 B440 8A2E 2004 8A0E 2104 BA00 05CD 21E8 D500 BF50 04CD
Die.448	B440 B9E8 0133 D2CD 2172 1126 8955 15B4 40B9 0500 BA5A 01CD
Xany.979	8B96 0906 B000 E85C FF8B D5B9 D303 E864 FFC6 8602 0401 F8C3

Design of SIEM

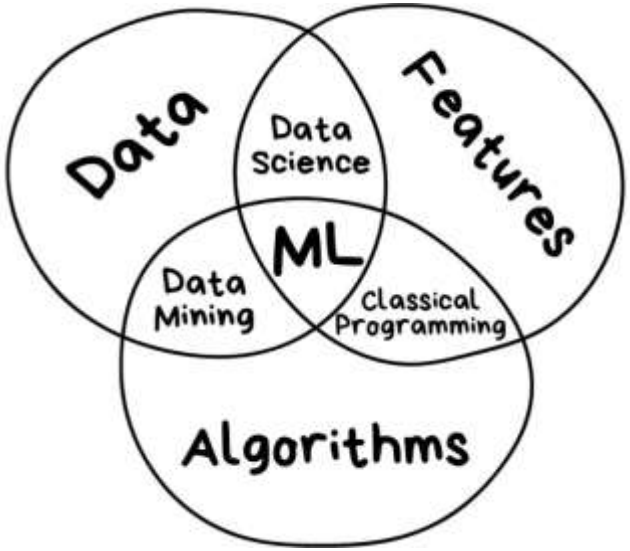
- **Security Information and Event Management** (SIEM) can be an extraordinary benefit to an organization's security posture.

- **Tools:**
  - Cloud SIEM
  - Elasticsearch
    - Elasticsearch is a real-time, distributed storage, search, and analytics engine.
    - **Kibana :** for Visualization

- ML has the power to comprehend threats in real time, to understand the infrastructure of a company.
- From a threat-detection perspective, ML is a game-changer
- **Reducing false positives**

Machine Learning for Cybersecurity

- **AI (Artificial Intelligence)** — a broad concept.A *Science* of making things smart or, in other words, human tasks performed by machines.
- **ML (Machine Learning)** — an *Approach*(just one of many approaches) to AI that uses a system that is capable of learning from experience.
- **DL (Deep Learning)** — a set of *Techniques* for implementing machine learning that recognize patterns of patterns -like image recognition.



- Most of tasks are subclasses of the most common ones, which are described below.

  - **Regression (or prediction)** — a task of predicting the next value based on the previous values.
  - **Classification** — a task of separating things into different categories.
  - **Clustering** — similar to classification but the classes are unknown, grouping things by their similarity.
  - **Association rule learning (or recommendation)** — a task of recommending something based on the previous experience.
  - **Dimensionality reduction** — or generalization, a task of searching common and most important features in multiple examples.
  - **Generative models** — a task of creating something based on the previous knowledge of the distribution.

➢ Machine Learning tasks and Cyber security:

- **Regression:**
  - ❖ It can be applied to fraud detection. The features (e.g., the total amount of suspicious transaction, location, etc.) determine a probability of fraudulent actions.

- **Classification:**
  - ❖ a spam filter separating spams from other messages can serve as an example. Spam filters are probably the first ML approach applied to Cyber security tasks.

- **Association Rule Learning**:
  - ❖ For incident response

- There are three dimensions (Why, What, and How).

- Security tasks can be divided into five categories:

  - prediction
  - prevention
  - detection
  - response
  - monitoring

- The second dimension is a technical layer and an answer to the “What” question:
  - Network (network traffic analysis and intrusion detection);
  - Endpoint (anti-malware);
  - Application (WAF or database firewalls);
  - User
  - Process (anti-fraud).

- The third dimension is a question of “How” (e.g., how to check security of a particular area):
  - in transit in real time;
  - at rest;
  - historically;

- **Machine learning for Network Protection**
  - regression to predict the network packet parameters and compare them with the normal ones;
  - classification to identify different classes of network attacks such as scanning and spoofing;
  - clustering for forensic analysis.

- **Machine learning for Endpoint Protection**
  - regression to predict the next system call for executable process and compare it with real ones;
  - classification to divide programs into such categories as malware, spyware and ransomware;
  - clustering for malware protection on secure email gateways (e.g., to separate legal file attachments from outliers).

➢ Machine learning for Application Security:

- ❖ To remind you, Application security can differ. There are web applications, databases, ERP systems, SaaS applications, micro services, etc.
- ❖ It's almost impossible to build a universal ML model to deal with all threats effectively in near future.

➢ ML can be applied as below

- ❖ regression to detect anomalies in HTTP requests (for example, XXE and SSRF attacks and auth bypass);
- ❖ classification to detect known types of attacks like injections (SQLi, XSS, RCE, etc.);
- ❖ clustering user activity to detect DDOS attacks and mass exploitation.

➢ Machine learning for Process Behavior:

- ❖ regression to predict the next user action and detect outliers such as credit card fraud;
- ❖ classification to detect known types of fraud;
- ❖ clustering to compare business processes and detect outliers.

➢ Deep Learning in Cybersecurity:

1. Intrusion Detection and Prevention Systems (IDS/IPS)

Deep learning, convolutional neural networks and Recurrent Neural Networks (RNNs) can be applied to create smarter ID/IP systems

2. Dealing with Malware

- ❖ Traditional malware solutions such as regular firewalls detect malware by using a signature-based detection system.
- ❖ Deep learning algorithms are capable of detecting more advanced threats and are not reliant on remembering known signatures and common attack patterns.
- ❖ They learn the system and can recognize suspicious activities

3. Spam and Social Engineering Detection

Natural Language Processing (NLP), a deep learning technique, can help you to easily detect and deal with spam

4. Network Traffic Analysis:

Deep learning ANNs are showing promising results in analyzing HTTPS network traffic to look for malicious activities. This is very useful to deal with many cyber threats such as SQL injections and DOS attacks.

5. User Behavior Analytics

THANK YOU

jayaram@cdac.in