BCSE353E
Information Security Analysis and Audit

Module 2

System Security

- System Vulnerabilities – Network Security Systems – System Security – Web Security – Intrusion Detection Systems

System Vulnerabilities

- Vulnerabilities are **weaknesses in a system** that gives threats the opportunity to compromise assets.
- It is a **flaw** or weakness in a system or network that could be **exploited to cause damage**, or allow an attacker to manipulate the system in some way.
- The way that a computer vulnerability is exploited depends on the **nature of the vulnerability and the motives of the attacker**.

What Causes Vulnerabilities?

- Human error
- Software bugs
- System complexity
- Increased connectivity
- Poor access control

Types of Security Vulnerabilities

- **Hardware Vulnerability**
  - Attack the system hardware physically or remotely
    - Old version of systems or devices
    - Unprotected storage
    - Unencrypted devices, etc.
- **Software Vulnerability**
  - Weakness due to poor design or implementation of any software
    - Lack of input validation
- **Network Vulnerabilities**
  - Weaknesses in the hardware or software of a network
    - Unprotected communication
    - Malware or malicious software (e.g.:Viruses, Keyloggers, Worms, etc)
    - Social engineering attacks
    - Misconfigured firewalls
- **Operating System Vulnerabilities**
  - Flaws within an OS
    - Default Superuser account
- **Human Vulnerabilities**
  - User errors can easily expose sensitive data, create exploitable access points for attackers, or disrupt systems.
- **Process/Procedural Vulnerability**
  - Weakness in an organization operational methods.
    - Password procedure
    - Training procedure

OS vulnerabilities

- **Remote code execution**
  - Allows attackers to remotely run arbitrary code on vulnerable servers and workstations.
- **Denial-of-service**
- **Elevation of privilege**
  - Elevation of privilege, also known as privilege escalation or EoP, gives an attacker **authorization permissions beyond those initially granted**.
  - In an EoP attack, a remote user executes commands to give an unauthorized user the rights of an administrator.
- **Information disclosure**
  - Software **bugs are exploited to obtain personal data** stored in a computer's memory
- **Spoofing**
  - Spoofing is the process of **impersonating** someone by tampering with the authentication process using a username and password.

Examples of security vulnerabilities

- Hidden Backdoor Programs
- Superuser or Admin Account Privileges
- Automated Running of Scripts without Malware/Virus Checks
- Unknown Security Bugs in Software or Programming Interfaces
- Unencrypted Data on the Network

Common System Vulnerabilities

- Missing data encryption
- OS command injection
- SQL injection
- Buffer overflow
- Missing authentication for critical function
- Missing authorization
- Unrestricted upload of dangerous file types
- Reliance on untrusted inputs in a security decision
- Cross-site scripting and forgery
- Download of codes without integrity checks
- Use of broken algorithms
- URL redirection to untrusted sites
- Path traversal
- Bugs
- Weak passwords
- Software that is already infected with virus

Network Security

- Security management in any network, whether public or private, is a set of **policies and routine procedures implemented by the networking system** to shield the network from unauthorized access.
- **Need for Network Security**
  - To **protect the information against any unwanted access**.
  - To safeguard the data from any inappropriate delay in the route followed to deliver it to the destination at the desired period of time.
  - To guard the data from any undesired amendment.
  - To **prohibit a particular user in the network from sending any mail, or message in such a way in which it appears to the receiving party that it has been sent by some third party**. (Protection from hiding the identity of the original sender of the resource message).
  - To **guard our hardware like hard disks, PC's, and laptops** from the attack of malware, viruses, etc., which can damage our system by corrupting or deleting all the content stored within it.
  - To protect our PC's from the software which if installed can harm our system as hackers do.
  - To **safeguard our system from Trojan horses, worms**, etc. which can completely destroy our system.

Network Security Controls

- **Physical Network Security**
  - Physical security controls are designed to **prevent unauthorized personnel from gaining physical access to network components such as routers, cabling cupboards** and so on.
  - Controlled access, such as locks, biometric authentication and other devices, is essential in any organization.
- **Technical Network Security**
  - **Protects data that is stored on the network** or which is in transit across, into or out of the network.
  - Protection is twofold;
    - It needs to protect data and systems from **unauthorized personnel**
    - It also needs to protect against **malicious activities** from employees.
- **Administrative Network Security**
  - **Security policies and processes that control user behavior**, including how users are authenticated, their level of access and also how IT staff members implement changes to the infrastructure.

Network Security Types

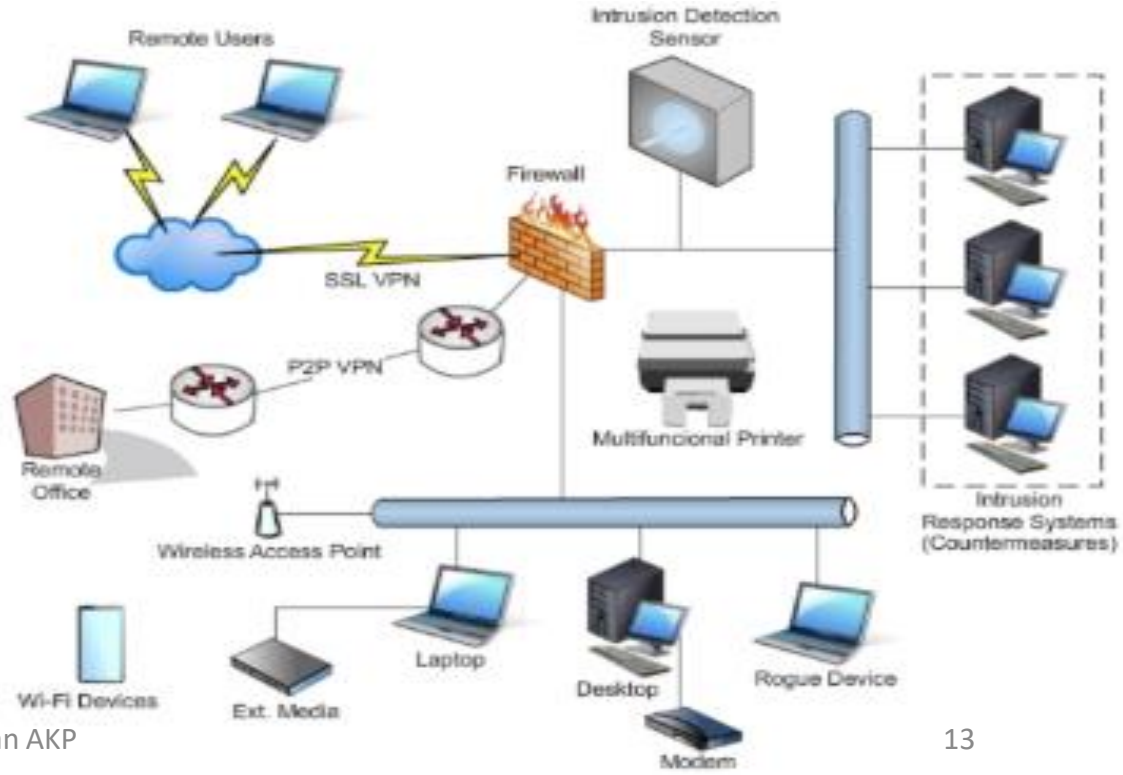
- **Antivirus and Anti-malware Software**
- Data Loss Prevention (DLP)
- Email Security
- **Firewalls**
- Mobile Security
- Network Segmentation
- Web Security
- Endpoint Security
- **Access Control**
- **Virtual Private Network**

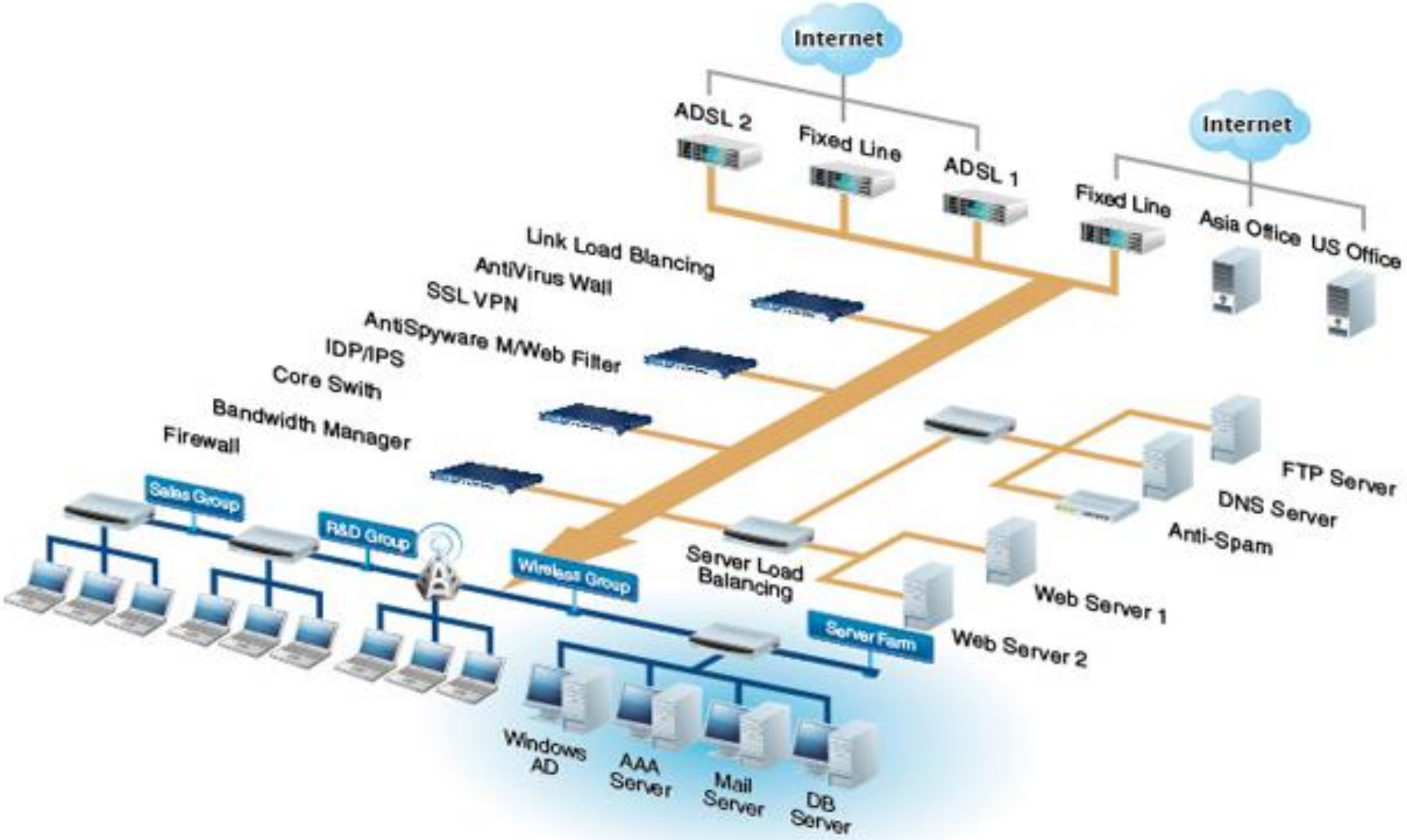
How To Make Your System And Network Safe?

- Set up Strong Passwords
- Establish a Firewall
- Antivirus Protection
- Continuous Updation
- Guard Laptops and Mobile Phones
- On-Time backups
- Smart Surfing on websites
- Secure Configuration
- Removable media control

Network Security Systems

- The devices used to establish network security
  - Firewall
  - Intrusion Detection/ Prevention Systems
  - Advanced Malware protection systems
  - Web Security Applications




Internet
ADSL 2
Fixed Line
ADSL 1
Internet
Fixed Line
Asia Office
US Office
Link Load Blancing
AntiVirus Wall
SSL VPN
AntiSpyware M/Web Filter
IDP/IPS
Core Swith
Bandwidth Manager
Firewall
FTP Server
DNS Server
Anti-Spam
Sales Group
R&D Group
Wireless Group
Server Load Balancing
Server Farm
Web Server 1
Web Server 2
Windows AD
AAA Server
Mail Server
DB Server

Types of Network Security Devices

- **Active Devices**
  - These security devices **block the surplus traffic**.
  - **Firewalls, antivirus scanning devices, and content filtering devices** are the examples of such devices.
- **Passive Devices**
  - These devices **identify and report on unwanted traffic**, for example, **intrusion detection appliances.**
- **Preventative Devices**
  - These devices **scan the networks and identify potential security problems**.
  - For example, **penetration testing devices and vulnerability assessment appliances**.
- **Unified Threat Management (UTM)**
  - These devices serve as **all-in-one security devices**.
  - Examples include **firewalls, content filtering, web caching**, etc.

System Security

- The objective of system security is the **protection of information and property from theft, corruption and other types of damage**, while allowing the information and property to remain accessible and productive.
- System security includes the **development and implementation of security countermeasures**.
- The **security of a system can be threatened** via two violations:
  - **Threat**
    - Accidental Threat
    - Malicious Threat
  - **Attack**

Compromising System Security

- Security can be **compromised** via any of the breaches mentioned:
  - **Breach of confidentiality**
    - This type of violation involves the **unauthorized reading/access of data**.
  - **Breach of integrity**
    - This violation involves **unauthorized modification of data**.
  - **Breach of availability**
    - It involves **unauthorized destruction of data**.
  - **Theft of service**
    - It involves **unauthorized use of resources**.
  - **Denial of service**
    - It involves **preventing legitimate use of the system**.

Security System Goal

- **Integrity**
  - The objects in the system **should not be accessed by any unauthorized user** & any user not having sufficient rights should not be allowed to modify the important system files and resources.
- **Secrecy**
  - The **objects of the system must be accessible only to a limited number of authorized users**. Not everyone should be able to view the system files.
- **Availability**
  - All the resources of the system **must be accessible to all the authorized users**

Classification of Threat

Program Threats

- If a user program is altered to perform some malicious unwanted tasks, then it is known as Program Threats.
  - Virus
  - Trojan Horse
  - Trap Door
  - Logic Bomb
  - Worm

System Threats

- These threats involve the abuse of system services.
  - Worm
  - Port Scanning
  - Denial of Service

Security Measures

- To protect the system, Security measures can be taken at the following levels:
  - **Physical Security**
    - The sites containing **computer systems must be physically secured against armed and malicious intruders.** The workstations must be carefully protected.
  - **Human Security**
    - Only **appropriate users must have the authorization to access the system**.
    - Phishing(collecting confidential information) and Dumpster Diving(collecting basic information so as to gain unauthorized access) must be avoided.
  - **Operating system Security**
    - The system must protect itself from **accidental or purposeful security breaches**.
  - **Networking System Security**
    - Almost all of the information is shared between different systems via a network.
    - Intercepting these data could be just as harmful as breaking into a computer.
    - Henceforth, Network should be properly secured against such attacks.

Various Approaches for System Security

- **Firewall**
  - To Improve the efficiency of filtering and increase the level of security in its network, every organization should apply the following recommendations:
  - 1. **Traffic-filtering rules**
    - That will determine the manner in which the incoming and outgoing traffic flows in the network will be regulated.
    - A set of traffic-filtering rules can be adopted as an independent packet filtering policy or as a part of the information security policy.
  - 2. **Select a traffic-filtering technology**
    - That will be implemented depending on the requirements and needs
  - 3. **Implement defined rules**
    - On the selected technology and optimize the performance of devices accordingly.
  - 4. **Maintain all the components of the solution**
    - Including not only devices, but also the policy.
- **Data encryption**
  - Encryption is widely used in systems like **e-commerce and Internet banking**, where the databases contain very sensitive information.
- **Passwords and biometrics**
  - A password is a string of characters used to authenticate a user to access a system.
  - Use Strong Passwords for enhanced security
    - **Long Password**
    - **Combination of various symbols**
    - **Avoid the obvious passwords**

Web Security

- Web security refers to the **protective measures and protocols that organizations adopt to protect the organization from, cyber criminals and threats that use the web channel**.
- Web security is critical to business continuity and to protecting data, users and companies from risk.
- Web security is also known as "**Cybersecurity**".
  - It basically means **protecting a website or web application by detecting, preventing and responding to cyber threats.**
- **Formal Definition**
  - Web Security is the act/practice of protecting websites from unauthorized access, use, modification, destruction, or disruption.

Need of Web Security

- Websites and web applications are just as **prone to security breaches**.
- Unfortunately, **cybercrime happens every day**, and great web security measures are needed to protect websites and web applications from becoming compromised.
  - **Websites becoming unavailable due to denial of service attacks**
  - **High-profile cases** - millions of passwords, email addresses, and credit card details have been leaked into the public domain, exposing website users to both personal embarrassment and financial risk.
- The purpose of website security is to **prevent these (or any) sorts of attacks.**

Benefits of Web Security

- For a modern enterprise, effective web security has broad technical and human benefits:
  - **Protect your business and stay compliant** by preventing loss of sensitive data
  - **Protect customers and employees by securing their private information**
  - **Avoid costly service interruptions** by preventing infections and exploits
  - Offer a **better user experience by helping your users stay safe and productive**
  - Maintain **customer loyalty and trust** by staying secure and out of the news
- **Effective website security requires design effort across the whole of the website.**

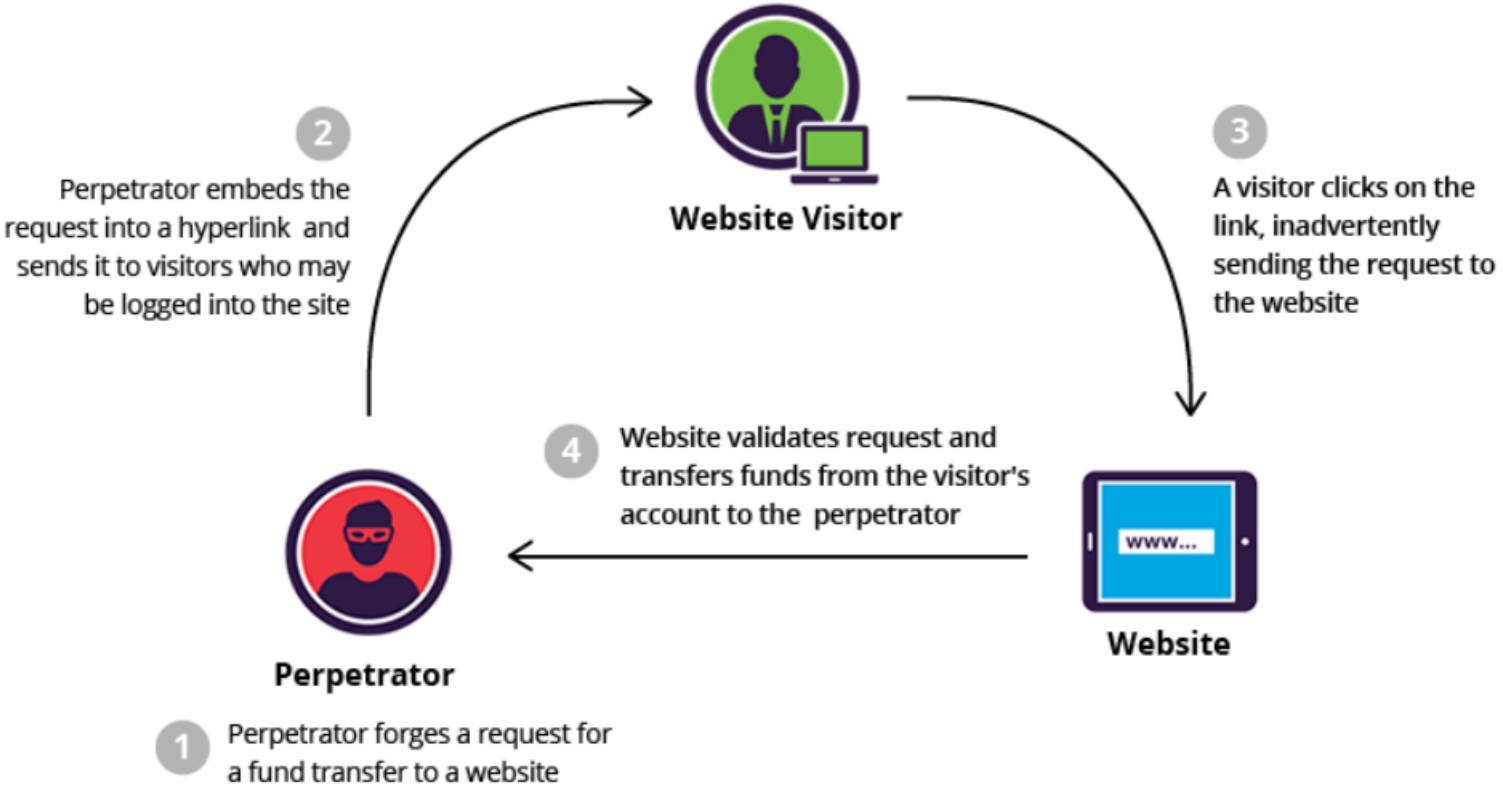
Factors related to Web Security

- There are a lot of factors that go into web security and web protection.
- Any website or application that is secure is surely backed by different types of checkpoints and techniques for keeping it safe.
- There are a variety of security standards that must be followed at all times, and these standards are implemented and highlighted by the **Open Web Application Security Project (OWASP)**.
  - Most experienced web developers from top cybersecurity companies will follow the standards of the OWASP as well as keep a close eye on the Web Hacking Incident Database to see when, how, and why different people are hacking different websites and services.
- **Essential steps in protecting web apps from attacks include**
  - Applying up-to-date **encryption**,
  - Setting proper **authentication**,
  - Continuously **patching discovered vulnerabilities**,
  - Avoiding data theft by having **secure software development practices**.

Technologies for Web Security

- **Black box testing tools**
  - Black box testing refers to checking a system without any knowledge regarding how it works.
- **Fuzzing tools**
  - Used to check software, networks, or operating systems for coding errors that may result in security weaknesses.
- **White box testing tools**
  - With white box testing, the design, coding, and internal structure of software is tested to enhance its design, as well as ensure the smooth flow of data into and out of the application.
- **Web application firewalls (WAF)**
  - A web application firewall (WAF) protects web applications by monitoring and filtering internet traffic that flows between an application and the internet.
  - In this way, a WAF works as a secure web gateway (SWG).
  - It provides protection for web applications against attacks, including cross-site scripting, file inclusion, cross-site forgery, Structured Query Language (SQL) injection, and other threats.
- **Security or vulnerability scanners**
  - Vulnerability scanners refer to tools that organizations use to automatically examine their systems, networks, and applications to check for weaknesses in their security.
- **Password cracking tools**
  - First, if you need to reset your password but cannot remember the original one, a password-cracking tool allows you to gain access.
  - Second, if someone has penetrated your system and changed the password, you can use a password-cracking tool to get back in and change the password to something harder to figure out, thereby regaining control.

Threats to Web Security



- SQL Injection
- Cross-site Scripting
- Remote File Inclusion
- Password Breach
- Data Breach
- Code Injection
- Denial of Service
- Directory Traversal
- Cross-Site Request Forgery (CSRF)
  - Tricks a web browser into executing an unwanted action in an application to which a user is logged in.
- Click jacking
  - Clickjacking could also be used to get the user to click a button on a visible site, but in doing so actually unwittingly click a completely different button.

Web Security Strategies

- **Resource assignment**
  - By assigning all necessary resources to causes that are dedicated to alerting the developer about new web security issues and threats, the developer can receive a constant and updated alert system that will help them detect and eradicate any threats before security is officially breached.
- **Web scanning**
  - There are several web scanning solutions already in existence that are available for purchase or download.
  - These solutions, however, are only good for known vulnerability threats – seeking unknown threats can be much more complicated.
  - This method can protect against many breaches, however, and is proven to keep websites safe in the long run.

Web Security Vs Clients

- Web Security also protects the visitors from the below-mentioned points -
  - Stolen Data
  - Phishing schemes
  - Session hijacking
  - Malicious redirects
  - Search Engine Optimization (SEO) Spam
    - Unusual links, pages, and comments can be displayed on a site by the hackers to distract your visitors and drive traffic to malicious websites.

Intrusion Detection System (IDS)

- An Intrusion Detection System (IDS) is a system that **monitors network traffic for suspicious activity and issues alerts** when such activity is discovered.
- It is a **software application that scans a network or a system for the harmful activity** or policy breaching.
- Any malicious venture or violation is normally reported either to an **administrator** or collected centrally using a **security information and event management (SIEM) system**.
  - A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from **false alarms**.
  - **Organizations need to fine-tune their IDS products when they first install them.**

Classification of Intrusion Detection System

- **Network Intrusion Detection System (NIDS)**
  - Planned **point within the network to examine traffic from all devices on the network.**
  - Observes the passing traffic – compares it with known attacks to identify abnormal behavior.
- **Host Intrusion Detection System (HIDS)**
  - Run on **independent hosts or devices on the network**
  - Monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected.
  - Snapshot of existing system files and compares it with the previous snapshot
- **Protocol-based Intrusion Detection System (PIDS)**
  - A system or agent that would consistently **resides at the front end of a server, controlling and interpreting the protocol** between a user/device and the server.
- **Application Protocol-based Intrusion Detection System (APIDS)**
  - A system or agent that generally **resides within a group of servers**. It identifies the intrusions by monitoring and interpreting the communication on **application-specific protocols**.
- **Hybrid Intrusion Detection System**
  - **Combination of two or more approaches** of the intrusion detection system.
  - In the hybrid intrusion detection system, host agent or system data is combined with network information to develop a complete view of the network system.

Detection Methods of IDS

- **Signature-based Method**
  - Detects the attacks on the basis of the **specific patterns such as number of bytes or number of 1's or number of 0's in the network traffic**.
  - It also detects on the basis of the **already known malicious instruction sequence** that is used by the malware.
  - The detected patterns in the IDS are known as **signatures**.
  - Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system but it is quite difficult to detect the new malware attacks as their pattern (signature) is not known.
- **Anomaly-based Method**
  - Anomaly-based IDS was introduced to **detect unknown malware attacks as new malware are developed rapidly**.
  - In anomaly-based IDS there is use of **machine learning to create a trustful activity model** and anything coming is compared with that model and it is declared suspicious if it is not found in model. (General Profiles are used)
  - Machine learning-based method has a better-generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

Detection Methods of IDS (Contd…)

- **Hybrid Detection**
  - A hybrid IDS uses both **signature-based and anomaly-based detection**.
  - This enables it to detect more potential attacks with a lower error rate than using either system in isolation.
- **Detection based on stateful protocol analysis**
  - Stateful protocol analysis is a process of **comparing predefined operation profiles with the specific data flow of that protocol on the network**.
  - Predefined profiles of operation of a protocol are defined by the **manufacturers of IDP devices** and they identify everything that is acceptable or not acceptable in the exchange of messages in a protocol.

Intrusion Prevention Systems (IPS)

- Intrusion Prevention System is also known as **Intrusion Detection and Prevention System**.
- It is a network security application that **monitors network or system activities for malicious activity**.
- Major functions of intrusion prevention systems are to **identify malicious activity, collect information about this activity, report it and attempt to block or stop it.**
- Intrusion prevention systems are contemplated as augmentation of Intrusion Detection Systems (IDS) because both IPS and IDS operate network traffic and system activities for malicious activity.
- IPS typically record information related to observed events, notify security administrators of important observed events and produce reports.
- IPS can also respond to a detected threat by attempting to prevent it from succeeding.

IPS (Contd…)

- One important distinction to make is the difference between intrusion prevention and active response.
- An **active response device dynamically reconfigures or alters network or system access controls**, session streams or individual packets based on triggers from packet inspection and other detection devices.
- **Active response happens after the event has occurred; thus, a single packet attack will be successful on the first attempt but will be blocked in future attempts**; for example, a DDoS attack will be successful on the first packets but will be blocked afterwards.
- While active response devices are beneficial, this one aspect makes them unsuitable as an overall solution.
- Network intrusion prevention devices, on the other hand, are typically inline devices on the network that inspect packets and make decisions before forwarding them on to the destination.

Classification of Intrusion Prevention System (IPS)

- **Network-based intrusion prevention system (NIPS)**
  - It monitors the **entire network for suspicious traffic** by analyzing protocol activity.
- **Wireless intrusion prevention system (WIPS)**
  - It monitors a **wireless network for suspicious traffic** by analyzing wireless networking protocols.
- **Network behavior analysis (NBA)**
  - It **examines network traffic to identify threats** that generate unusual traffic flows, such as distributed denial of service attacks, specific forms of malware and policy violations.
- **Host-based intrusion prevention system (HIPS)**
  - It is an **inbuilt software package which operates a single host** for doubtful activity by scanning events that occur within that host.

Comparison of IPS Technologies

IPS Technology Type	Types of Malicious Activity Detected	Scope per Sensor	Strengths
Network-Based	Network, transport, and application TCP/IP layer activity	Multiple network subnets and groups of hosts	Only IDPS which can analyze the widest range of application protocols;
Wireless	Wireless protocol activity; unauthorized wireless local area networks (WLAN) in use	Multiple WLANs and groups of wireless clients	Only IDPS able to predict wireless protocol activity
NBA	Network, transport, and application TCP/IP layer activity that causes anomalous network flows	Multiple network subnets and groups of hosts	Typically more effective than the others at identifying reconnaissance scanning and DoS attacks, and at reconstructing major malware infections
Host-Based	Host application and operating system (OS) activity; network, transport, and application TCP/IP layer activity	Individual host	Can analyze activity that was transferred in end-to-end encrypted communications

Detection Method of Intrusion Prevention System (IPS)

- **Signature-based detection**
  - Signature-based IDS operates packets in the network and compares with pre-built and preordained attack patterns known as signatures.
- **Statistical anomaly-based detection**
  - Anomaly based IDS monitors network traffic and compares it against an established baseline. The baseline will identify what is normal for that network and what protocols are used. However, It may raise a false alarm if the baselines are not intelligently configured.
- **Stateful protocol analysis detection**
  - This IDS method recognizes divergence of protocols stated by comparing observed events with pre-built profiles of generally accepted definitions of not harmful activity.

Intrusion Prevention Technologies/ Strategies

- **System memory and process protection**
  - This type of intrusion prevention strategy **resides at the system level.**
  - Memory protection consists of a mechanism to **prevent a process from corrupting the memory** of another process running on the same system.
  - Process protection consists of a **mechanism for monitoring process execution**, with the ability to kill processes that are suspected of being attacks.
- **Inline network devices**
  - This type of intrusion prevention strategy **places a network device directly in the path of network communications with the capability to modify and block attack packets** as they traverse the device's interfaces.
  - The detection and response happens in real time before the packet is passed on to the destination network.
- **Session sniping**
  - This type of intrusion prevention strategy **terminates a TCP session by sending a TCP RST packet** to both ends of the connection.
  - When an **attempted attack is detected, the TCP RST is sent and the attempted exploit is flushed from the buffers** and thus prevented.
- **Gateway interaction devices**
  - This type of intrusion prevention strategy allows a **detection device to dynamically interact with network gateway devices such as routers or firewalls**. When an attempted attack is detected, the detection device can direct the router or firewall to block the attack.

Risks Related to IPS

- False Positives
- Gateway interaction timing and race conditions
  - Detection device directs a router or firewall to block the attempted attack.
  - However, because of network latency, the attack has already passed the gateway device before it receives this direction from the detection device.

PARAMETER	FIREWALL	IPS	IDS
Abbreviation for	-	Intrusion Prevention System	Intrusion Detection System
Philosophy	Firewall is a network security device that filters incoming and outgoing network traffic based on predetermined rules	IPS is a device that inspects traffic, detects it, classifies and then proactively stops malicious traffic from attack.	An intrusion detection system (IDS) is a device or software application that monitors a traffic for malicious activity or policy violations and sends alert on detection.
Principle of working	Filters traffic based on IP address and port numbers	inspects real time traffic and looks for traffic patterns or signatures of attack and then prevents the attacks on detection	Detects real time traffic and looks for traffic patterns or signatures of attack and them generates alerts
Configuration mode	Layer 3 mode or transparent mode	Inline mode , generally being in layer 2	Inline or as end host (via span) for monitoring and detection
Placement	Inline at the Perimeter of Network	Inline generally after Firewall	Non-Inline through port span (or via tap)
Traffic patterns	Not analyzed	Analyzed	Analyzed
Placement wrt each other	Should be 1st Line of defense	Should be placed after the Firewall device in network	Should be placed after firewall
Action on unauthorized traffic detection	Block the traffic	Preventing the traffic on Detection of anomaly	Alerts/alarms on detection of anomaly
Related terminologies	> Stateful packet filtering > permits and blocks traffic by port/protocol rules	> Anomaly based detection > Signature detection > Zero day attacks > Blocking the attack	> Anomaly based detection > Signature detection > Zero day attacks > Monitoring > Alarm