

Prepared by Dr. Mohammed Anbar

CYB 630
Network Security Mechanisms

Lecture 5



- Understand the attack vectors, surfaces, and data breaches,
- Explain monitoring techniques and their types,
- Explain the Intrusion detection system (IDS) and its types,
- Understand types of IDS detection mechanisms,
- Explain Intrusion Prevention System (IPS) ,
- Differentiate between IPS and IDS,
- Explain Honeypot.

What is the difference between attack vectors, attack surfaces, and data breach?

In computer security, an attack vector is a specific path, method, or scenario that can be exploited to break into an IT system, thus compromising its security

An attack surface is the total number of attack vectors an attacker can use to manipulate a network or computer system or extract data.

A data breach is any security incident where sensitive, protected, or confidential data is accessed or stolen by an unauthorized party.



Passive Attacks

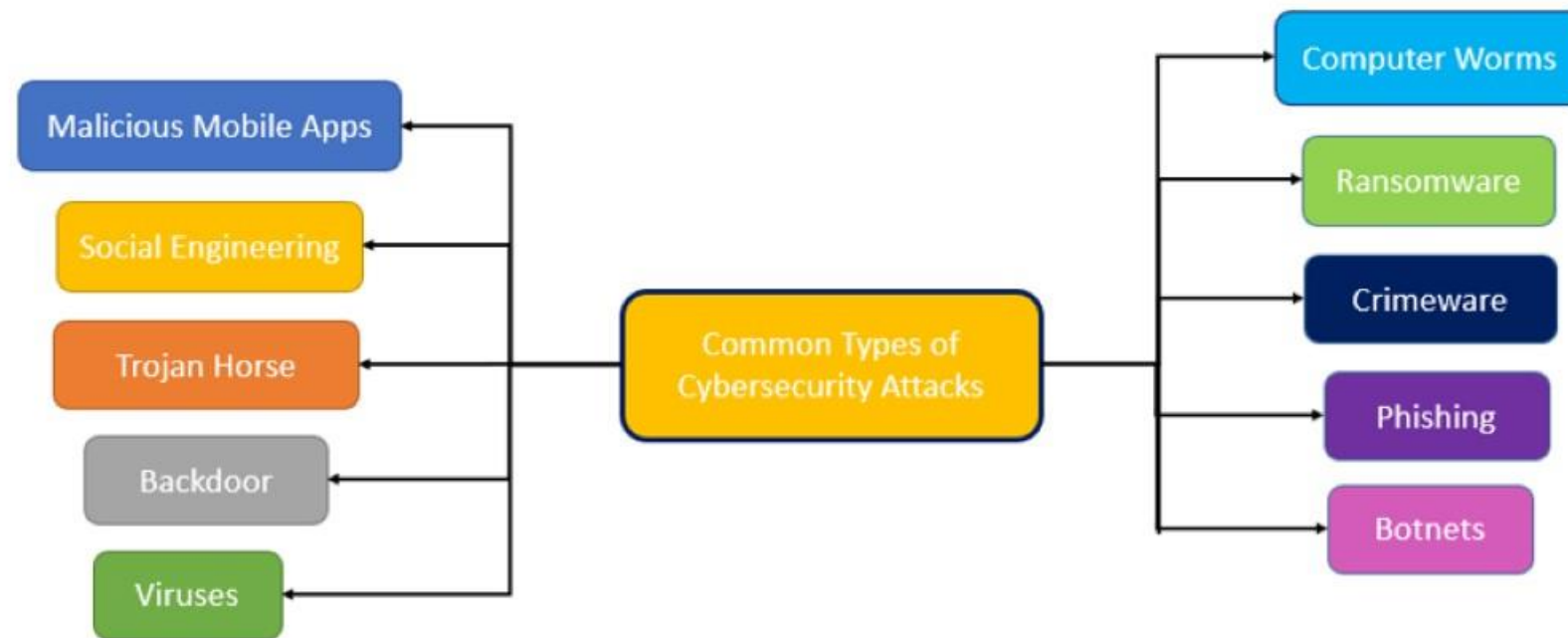
Active Attacks

- In passive attacks, the attacker attempt to silently sniff the network traffic to learn or make use of information from the system but does not affect system resources.
- This attack is difficult to detect because they do not involve any alteration of the data and do disturb the network communication.



- In an active attack, an attacker attempt to alter system resources or affect their operation.
- Compared to passive attacks, active attacks are easier to detect due to the anomalies they cause in the system.
- The damage that is done by these attacks can be very harmful to the system and its resources.





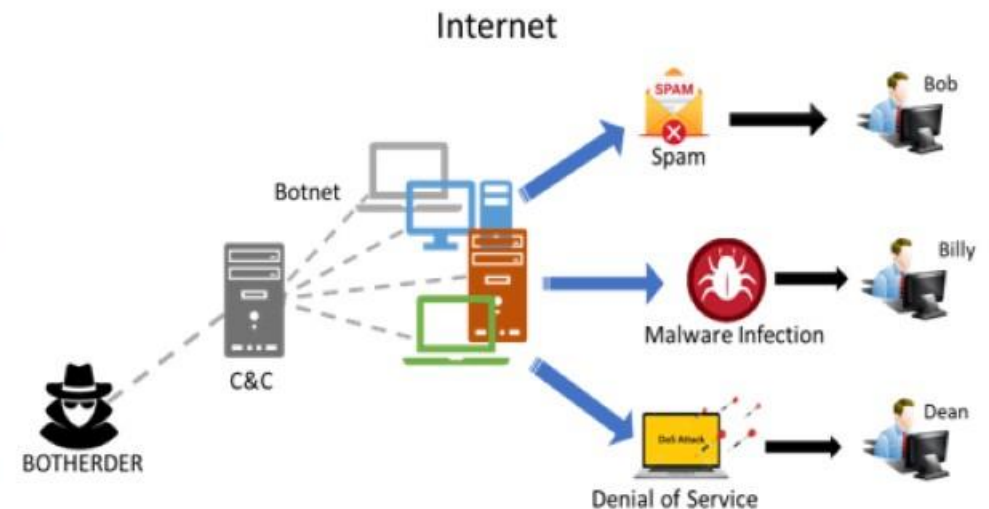
What is a computer worm?

A computer worm is a self-replicating malware program whose primary purpose is to infect other computers by duplicating itself without human intervention while remaining active on infected systems.



What are bots and botnets?

- A bot is a computer that is infected with malware that allows it to be remotely controlled by an attacker.
- The bot (or zombie computer) can then be used to launch more cyber attacks or become part of a botnet (a collection of bots).
- Botnets are a popular method for distributed denial of service (DDoS) attacks, spreading ransomware, keylogging, and spreading other types of malware.



What are bugs and vulnerabilities?

- All the attacks are taken place due to bugs and vulnerabilities in systems, resources, services, and applications.
- A bug is when the system isn't behaving as it's supposed to, whereas a vulnerability is a bug that manifests itself as an opportunity for exploitation.



Bug



Vulnerability

Chapter 04

Common Vulnerabilities and Exposures (CVE)

The Common Vulnerabilities and Exposures (CVE) system provides a reference method for publicly known information-security vulnerabilities and exposures. CVE can be accessed via this link "<https://cve.mitre.org/>"

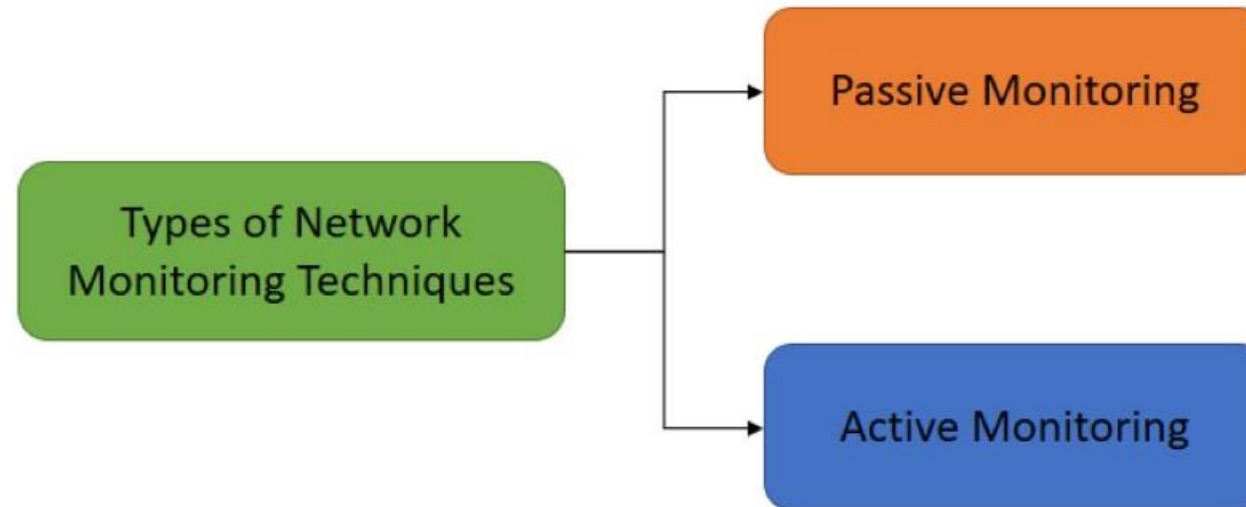


The screenshot shows the CVE Mitre website interface. At the top, there's a navigation bar with links like 'CVE List', 'CVEs', 'FAQs', 'About', and 'News & Blog'. Below this is a search bar and a 'TOTAL CVE Records: 156463' indicator. The main section is titled 'Search Results' and shows 'There are 8829 CVE Records that match your search.' Below this is a table with columns 'Name' and 'Description'. The first row is for CVE-2021-3694, which describes a security issue in Secure 8 (ZVolo) where user input data is not validated correctly, allowing a remote attacker to perform a blind SQL injection. The table continues with several other CVE entries, each with a brief description of the vulnerability or exposure.

Name	Description
CVE-2021-3694	Secure 8 (ZVolo) does not validate user input data correctly, allowing a remote attacker to perform a blind SQL injection. An attacker could exploit this vulnerability in order to extract information of users and administrator accounts stored in the database.
CVE-2021-36436	Online Pet Shop Web App 1.0 is vulnerable to remote SQL injection and shell upload vulnerability in Fidele Network and Deception CommandPost enables unauthenticated SQL injection through the web interface. The vulnerability could lead to exposure of authentication tokens in some versions of Fidele software. The vulnerability is present in Fidele Network and Deception versions prior to 9.3.7 and in version 9.4. Patches and updates are available to address this vulnerability.
CVE-2021-36848	Opango 3.1.x before 3.1.13 and 3.2.x before 3.2.5 allows QuerySet.order_by SQL injection if order_by is untrusted input from a client of a web application.
CVE-2021-36945	main/inc/ajax/model_ajax.php in Chamilo through 1.11.14 allows SQL injection via the searchfield_filters, or filters2 parameter.
CVE-2021-34187	In Progress MOVEit Transfer before 2019-0-6 (11.0.6), 2019.1.x before 2019.1.5 (11.1.5), 2019.1.x before 2019.2.2 (11.2.2), 2020.x before 2020.0.5 (12.0.5), 2020.1.x before 2020.1.4 (12.1.4), and 2020.1.x before 2021.0.1 (13.0.1), a SQL injection vulnerability exists in SQLUtility.vb in MOVEit.SM2 WebApp in the MOVEit Transfer web app. This could allow an authenticated attacker to gain unauthorized access to the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database and/or execute arbitrary SQL statements or delete database elements.
CVE-2021-32479	COVINT9 Testing Management System 1.0 is vulnerable to SQL injection via the admin panel.
CVE-2021-32186	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in csp component in Synology Media Server before 1.8.1 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.
CVE-2021-32528	The affected product is vulnerable to a SQL injection, which may allow an unauthorized attacker to disclose information on the filev (versions prior to 1.4.9) and filev2 (versions 1.4.9 and later) components.
CVE-2021-32186	SQL injection exists in Spotweb 1.4.9 because the notAllowedCommands protection mechanism is inadequate, e.g., a variation of the payload may be used to bypass this protection. This issue exists because of an incomplete fix for CVE-2020-25545.
CVE-2021-32178	Local Service Search Engine Management System 1.0 has a vulnerability through authentication bypass using SQL injection. Using the vulnerability, an attacker can bypass the login page.
CVE-2021-32206	DHS 2 is an information system for data capture, management, validation, analytics and visualization. A SQL injection security vulnerability has been found in specific versions of DHS2. This vulnerability affects the /api/trackedentityinstances API endpoint in DHS2 versions 2.34.4, 2.35.2, 2.35.3, 2.35.4, and 2.36.0. Earlier versions, 2.34.0, 2.34.1, 2.34.2, 2.34.3, 2.34.4, 2.34.5, 2.34.6, 2.34.7, 2.34.8, 2.34.9, 2.35.0, 2.35.1 and all versions 2.33 and older are unaffected. The system is vulnerable to attack only from users that are logged in to DHS2, and there is no known way of exploiting the vulnerability without first being logged in as a DHS2 user. A successful exploit of this vulnerability could allow the malicious user to read, edit and delete data in the DHS2 instance. There are no known exploits of the security vulnerabilities addressed by this advisory. However, we strongly recommend that all DHS2 implementations using versions 2.34, 2.35 and 2.36 install these patches as soon as possible. There is no straightforward known workaround for DHS2 instances using Tracker functionality other than upgrading the affected DHS2 server to one of the patches in which this vulnerability has been fixed. For implementations which do NOT use Tracker functionality, it may be possible to disable network access to POST to the /api/trackedentityinstances endpoint as a temporary workaround while waiting to upgrade.
CVE-2021-32615	Phiggo 11.4.0 allows admin/user_bot_backend.php order[0][dr] SQL injection.
CVE-2021-32582	An issue was discovered in ConnectWise Automate before 2021.5. A blind SQL injection vulnerability exists in core agent inventory communication that can enable an attacker to extract database information or administrative credentials from an instance via crafted monitor status responses.
CVE-2021-32239	E-Learning System 1.0 suffers from an unauthenticated SQL injection vulnerability, which allows remote attackers to execute arbitrary code on the hosting web server and gain a reverse shell.
CVE-2021-32108	A SQL injection vulnerability exists (with user privileges) in interface/admin/eye_img/save.php in OpenDMR 5.0.2.1.
CVE-2021-32102	A SQL injection vulnerability exists (with user privileges) in library/custom_template/eye_code.php in OpenDMR 5.0.2.1.
CVE-2021-32095	A SQL injection vulnerability in the pandora_console component of Artica Pandora FMS 742 allows an unauthenticated attacker to upgrade his unprivileged session via the include/chart_generator.php session_id parameter, leading to a login bypass.
CVE-2021-32051	Hexagon Givisi Aukuntportal before 5.0.0.0 allows SQL injection via the Gifworkflow/Service/DownloadPublicFile id parameter.

- The term network monitoring describes the use of a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator in case of outages via email, pager, or other alarms.
- Network monitoring monitors all the traffic that goes through the network (inbound and outbound traffic)
- It is a subset of the functions involved in network management.

- **Who is accessing your network?**
 - students, academics, staff, visitors or others
- **What are they accessing your network for?**
 - academic study, social use, business use, illegal use
- **Where are they accessing your network from?**
 - internal, external
- **How are they accessing your network?**
 - remote user, local Ethernet, WAN, dial-up, Wi-Fi, VPN
- **When did they access your network?**
 - today, yesterday, last week, last month...



Network Monitoring Techniques (cont.)

Passive monitoring

- Passive monitoring uses devices to watch the traffic as it passes by.
- The passive monitoring devices are polled periodically, and information is collected to assess network performance and status.
- The passive approach does not increase the traffic on the network for the measurements. It also measures real traffic.
- The passive technique is extremely valuable in network troubleshooting; however, they are limited in their ability to emulate error scenarios or isolate the exact fault location.
- Since the passive approach may require viewing all packets on the network, there can be privacy or security issues about how to access/protect the data gathered.

- Active monitoring relies on the capability to inject test packets into the network or send packets to servers and applications, following them and measuring the service obtained from the network.
- As such, it does create extra traffic, and the traffic or its parameters are artificial. However, the volume and other parameters of the introduced traffic are fully adjustable, and small traffic volumes are enough to obtain meaningful measurements.
- On the other hand, the active technique provides precise control of the generation of packets for measurement scenarios. This includes control of the nature of traffic generation, the sampling techniques, the timing, frequency, scheduling, packet sizes and types (to emulate various applications), statistical quality, and the path.

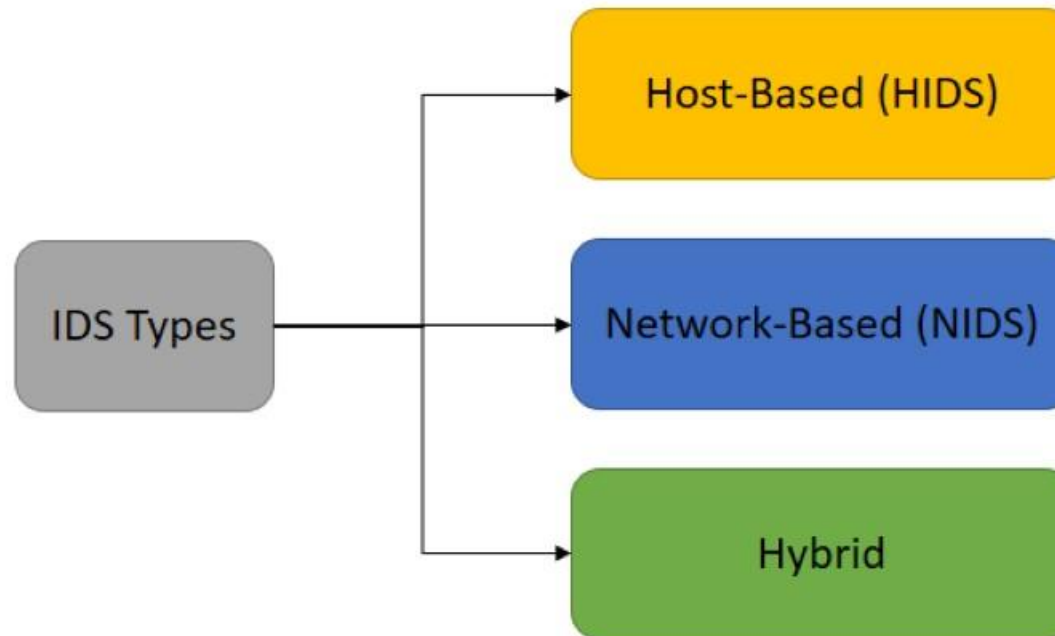
- Defined as the instruments, techniques, and sources that support the detection, evaluation, and reporting of illicit or forbidden network activity.
- IDSs are frequently highly helpful in identifying breaches of corporate security policy and other internal risks.
- IDSs can detect and respond to both insider and external attacks.

- Monitoring, detecting, and responding to illegal activity are the three key security functions performed by IDSs.
- IDS can also react to a security breach event automatically (in real-time) by activating some scripts, disabling user accounts, and logging off users.
- At the main gateway, IDS is installed to keep track of all network traffic and to compare traffic packets to predefined rules.
- These rules were developed to detect suspicious packets (such as worm packets) or anomalous traffic

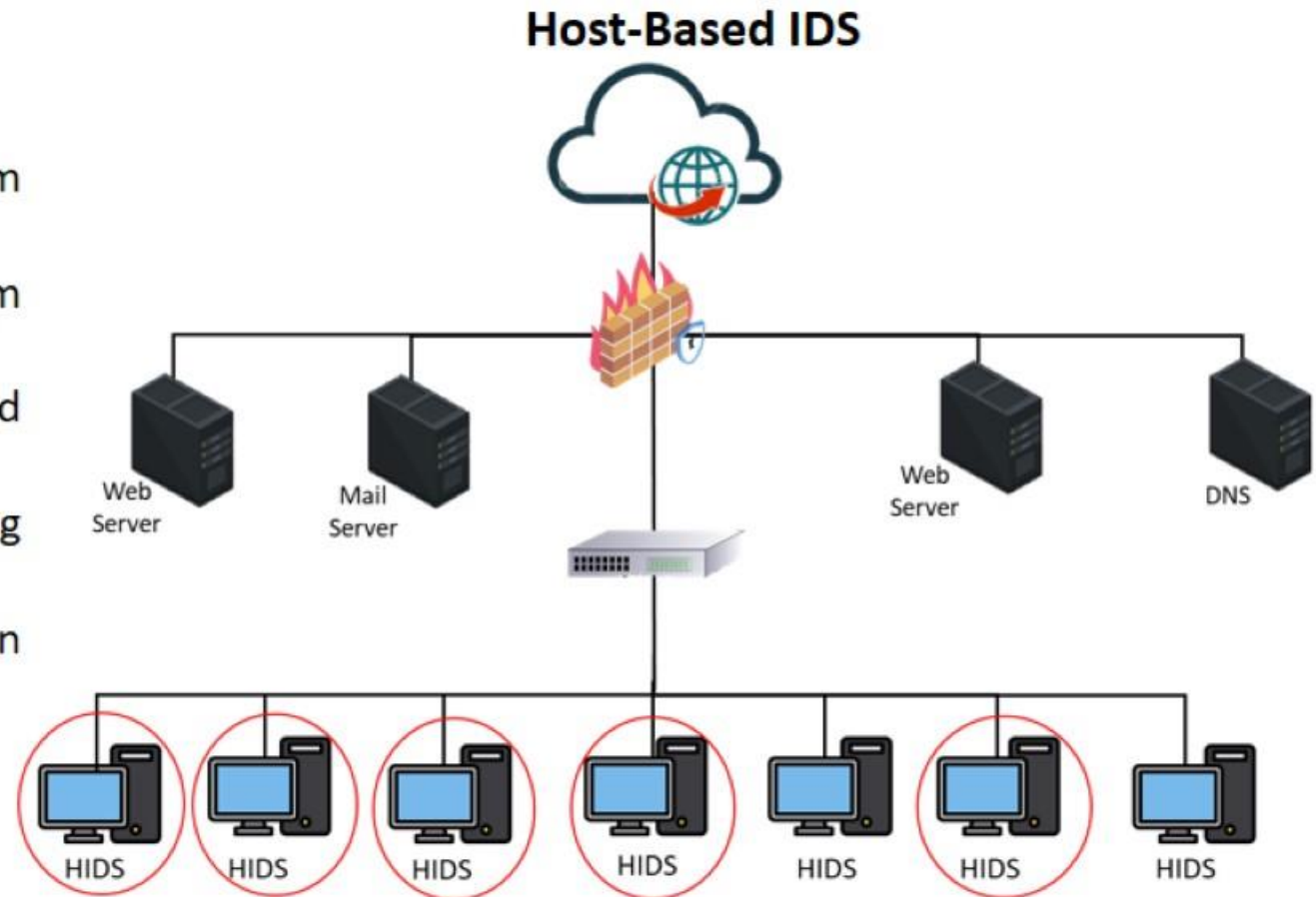
- Attack and intrusion can be viewed from a number of perspectives; the intruder and the victim.
- An intrusion has taken place if the attack is considered successful from the victims' point of view (the victim has experienced some loss or consequences)
- Vulnerability in the victim's system that is exploited by the intruder with the objective enables a successful attack
- The intrusion process ends when some or all objectives of the intruder are realized or the intruder gives up

- IDS keeps track of the entire system or just certain areas.
- Intrusion detection takes place either during or after an intrusion.
- IDS can be stealthy or openly advertised.
- It generates an alarm and retains logs that can be utilized for reports on long-term development if suspicious behavior is detected.
- IDS systems can generate an alarm and/or an automatic reaction.

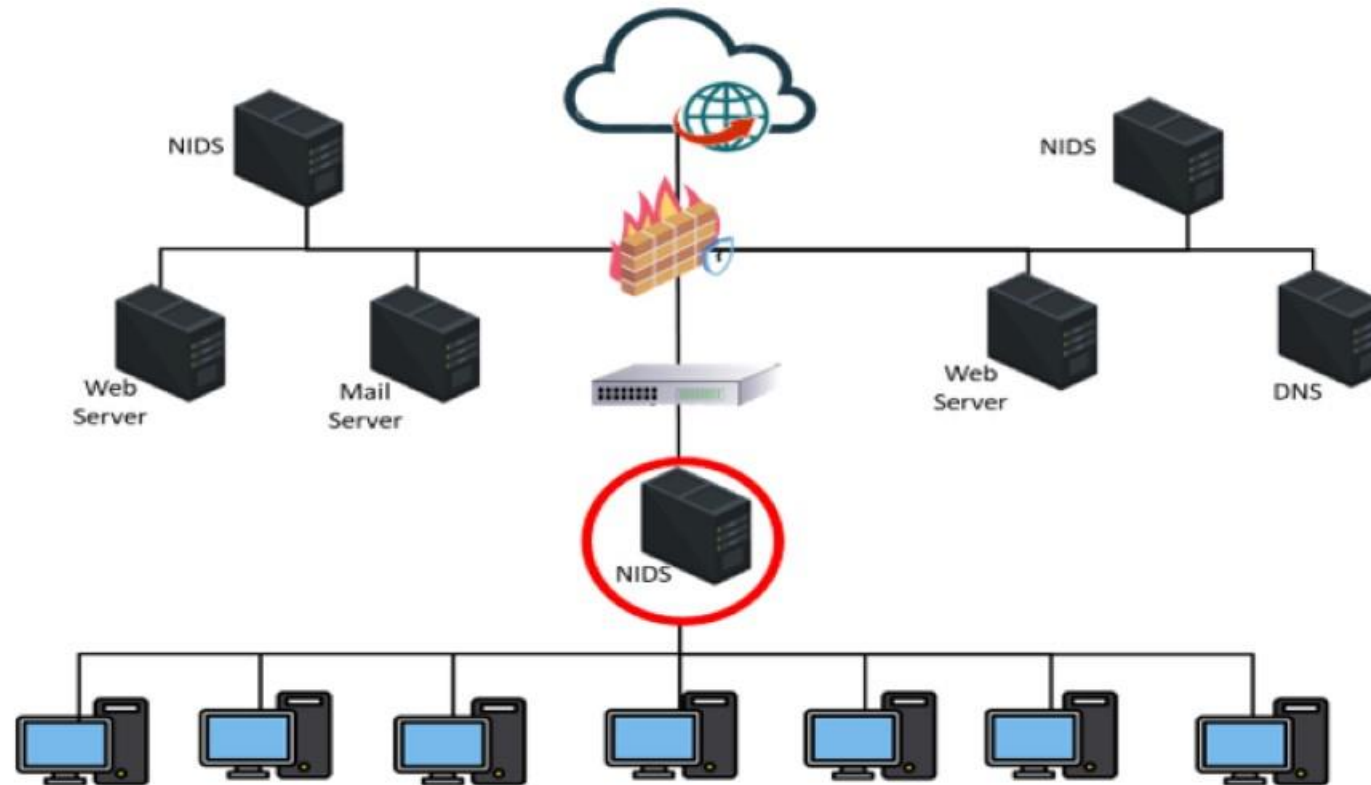
- Monitors the operation of firewalls, routers, key management servers and files critical to other security mechanisms
- Allows the administrator to adjust, arrange, and comprehend the operating system audit trails and other logs, which are frequently incomprehensible.
- Can make the security management of systems by non-expert staff possible by providing a nice user-friendly interface
- Comes with an extensive attack signature database.
- Can recognize and report alterations to data files



A host-based intrusion detection system (HIDS) is an intrusion detection system that is capable of monitoring and analyzing the internals of a computing system as well as the network packets on its network interfaces.



- Dedicated network devices known as NIDS are dispersed throughout networks and are used to track and examine network activity.
- NIDS uses packet sniffing techniques to extract data from TCP/IP packets or other protocols that are moving through the network, as opposed to analyzing data that originates and resides on a host.
- The majority of NIDS record their actions and alert or report suspicious incidents.
- Network-based IDS work best when located on the DMZ, on any subnets containing mission-critical servers, and just inside the firewall.



- A hybrid intrusion detection system is created by combining two or more intrusion detection system approaches.
- In the hybrid intrusion detection system, network data is merged with the host agent or system data to create a comprehensive picture of the network system.
- In comparison to other intrusion detection systems, the hybrid system is more effective.

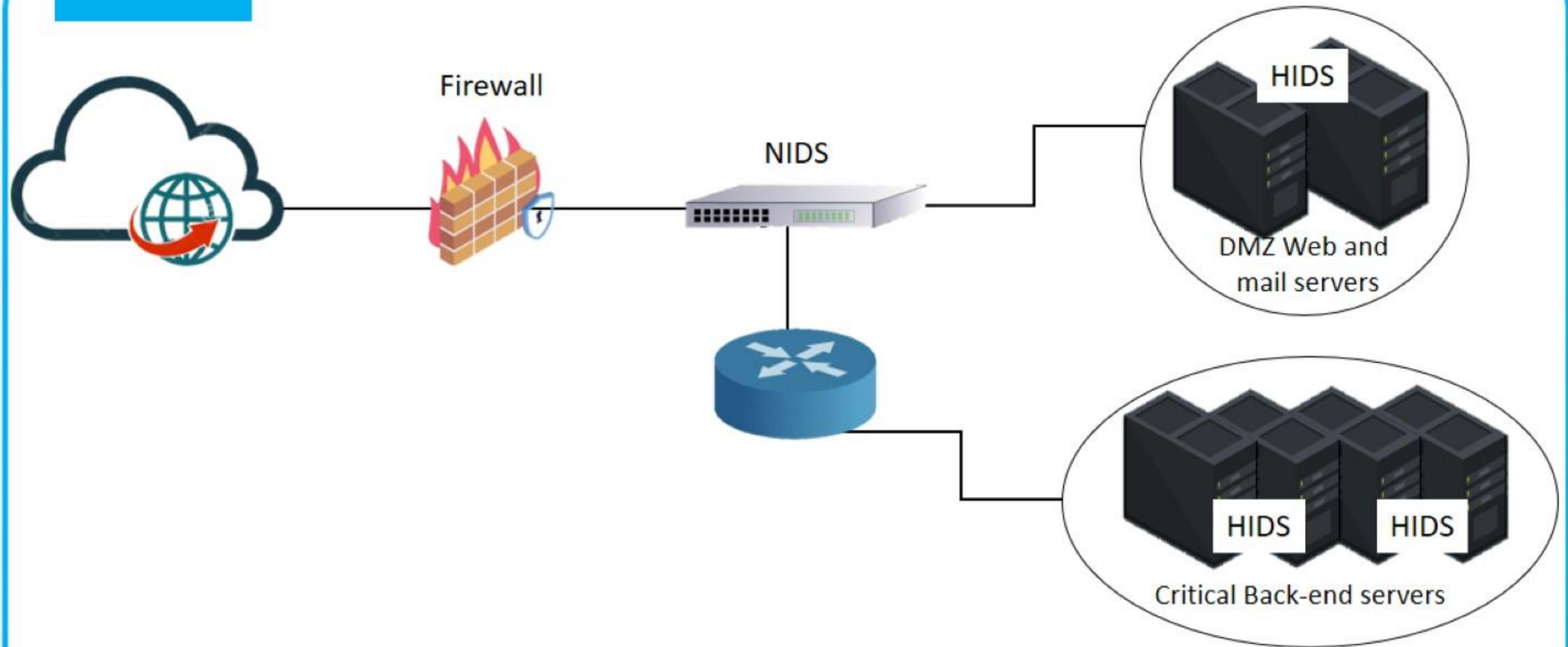
Host-Based

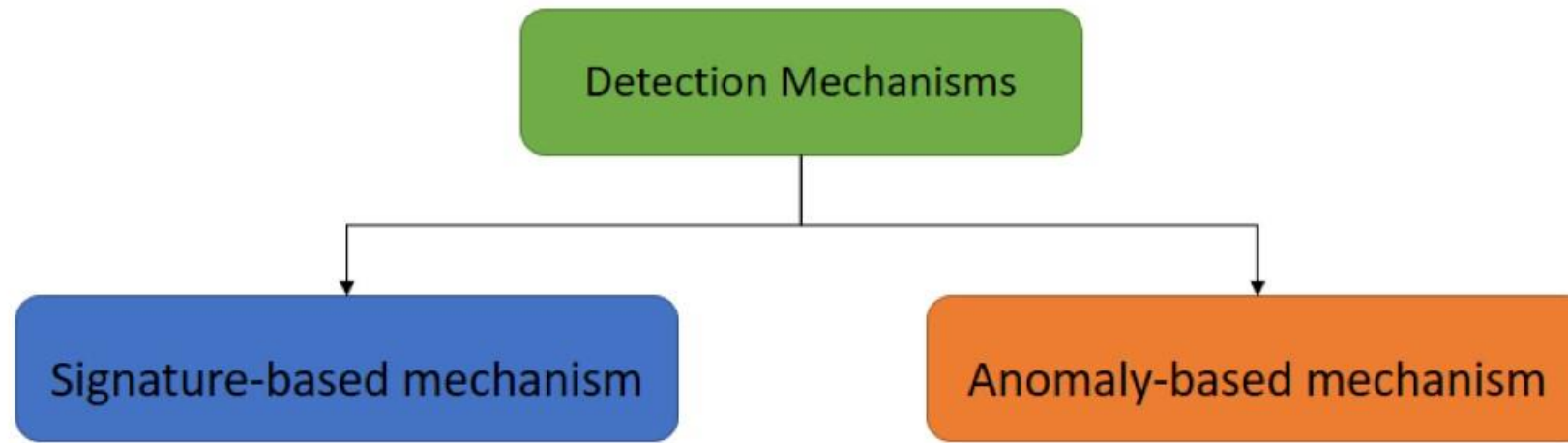
- Narrow in scope (watches only specific host activities)
- More complex setup
- Better for detecting attacks from the **inside**
- **More expensive** to implement
- Detection is based on what any **single host** can record
- Does not see packet headers
- Usually only responds **after** a suspicious log entry has been made
- OS-specific
- Detects local attacks before they hit the network

Network-Based

- Broad in scope (watches all network activities)
- Easier setup
- Better for detecting attacks from the **outside**
- **Less expensive** to implement
- Detection is based on what can be recorded on the **entire network**.
- Examines packet headers
- Near **real-time** response
- OS-independent
- Detects network attacks as the payload is analyzed

- Between your network and Extranet
- In the DMZ before the Firewall to identify the attacks on your servers in DMZ.
- Between the firewall and your network, to identify a threat in case of firewall penetration.
- If possible, between your servers and user community, to identify the attacks from the inside on the intranet, FTP, and database environment





- Signature-based IDS match the current behaviors of the network against predefined attack patterns.
- Signatures are pre-configured and stored on the device and each signature matches a certain attack.
- They need a signature of each attack and must also store it. This requires specific knowledge of each attack and storage costs grow with the number of attacks.
- Signatures are easy to develop and understand if you know what network behavior you're trying to identify.

However, because they only detect known attacks, a signature must be created for every attack.

- In this type of detection, IDS checks the incoming packet payload and system log files against the network attacks' signatures that are already stored in the IDS database. An alert will be triggered when a match is found.
- One advantage of signature-based detection is its ability to detect known attacks with a high accuracy rate. However, signature-based detection systems cannot detect zero-day or newly released attacks.

- The anomaly-based mechanism is a profiling program that will be created for the normal behavior of the network, which will be used by the anomaly-based detection system as a baseline. Deviation from this baseline will be treated as an anomaly or a possible intrusion.
- One advantage of this detection mechanism is that able to detect zero-day attacks.
- The drawback of this detection mechanism is that the duration spent on profiling the normal traffic behavior of the network.
- In addition, the profiling process must be repeated if changes occur in the target environment. This situation is known as the drift problem, which complicates the creation of a normal traffic profile.

- Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity.
- The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it

Both systems can:

- **Monitor**
After setup, these programs can look over the traffic within the parameters you specify, and they will work until you turn them off.
- **Alert.**
Both programs will send a notification to those you specify when a problem has been spotted.
- **Learn**
Both can use machine learning to understand patterns and emerging threats.
- **Log**
Both will keep records of attacks and responses, so you can adjust your protections accordingly.

But they differ due to:

- **Response**

An IDS is passive, while an IPS is an active control system. You must take action after an IDS alerts you, as your system is still under attack.

- **Protection**

Arguably, an IDS offers less help when you're under threat. You must figure out what to do when to do it, and how to clean up the mess. An IPS does all of this for you.

- **False positives**

If an IDS gives you an alert about something that isn't troublesome at all, you're the only one inconvenienced. If an IPS shuts down traffic, many people could be impacted.

- The honeypot fools hackers into thinking it's a legitimate target by having the appearance of a real computer system, complete with apps and data. For instance, a honeypot could be designed to look like a company's customer billing system, which is frequently targeted by thieves looking for credit card details.
- Once the hackers are inside, it is possible to trace them and analyse their activity to find out how to safeguard the real network.
- Honeypots are made attractive to attackers by building deliberate security vulnerabilities. For instance, a honeypot might have ports that respond to a port scan or weak passwords

- In addition, vulnerable ports might be left open to entice attackers into the honeypot environment rather than the more secure live network.
- A honeypot isn't set up to address a specific problem, like a firewall or anti-virus. Instead, it's an information tool that can help you understand existing threats to your business and spot the emergence of new threats.
- As a result, security efforts can be ranked and focused on the intelligence obtained from a honeypot.

By monitoring traffic coming into the honeypot system, you can assess:

1

Where the cybercriminals are coming from

2

The level of threat

3

What data or applications they are interested

4

How well your security measures are working to stop cyberattacks

- Stallings, W. (2006). Cryptography and network security principles and practices 4th edition
- Vincent Nestler, Gregory White, wm. Arthur Conklin, Principles of Computer Security: CompTIA Security+ and Beyond – Lab Manual, ISBN: 978-0-07-174856-8, MHID: 0-07-174856-3, McGraw Hill, 2011



Thank You