Co-funded by
the European Union

Course: Real time Cyber Threat Detection and Mitigation

Project: Cyber Security 4 ALL(CS4ALL)

Co-funded by
the European Union

Chapter 4: Intrusion Detection and Prevention Systems

Index

4.1 Components and Architecture

4.2 Common Detection Methodologies

4.3 Anomaly and Stateful Protocol Analysis

4.4 Network and Hardware Layer attacks

4.5 Honeypots

4.6 Working with SNORT IDS

4.7 Need for multiple IDPS Technologies

4.8 IPS using IP Trace back - Probabilistic and Deterministic Packet Marking

4.9 Threats against WLANs

4.10 Behavioural Analytics

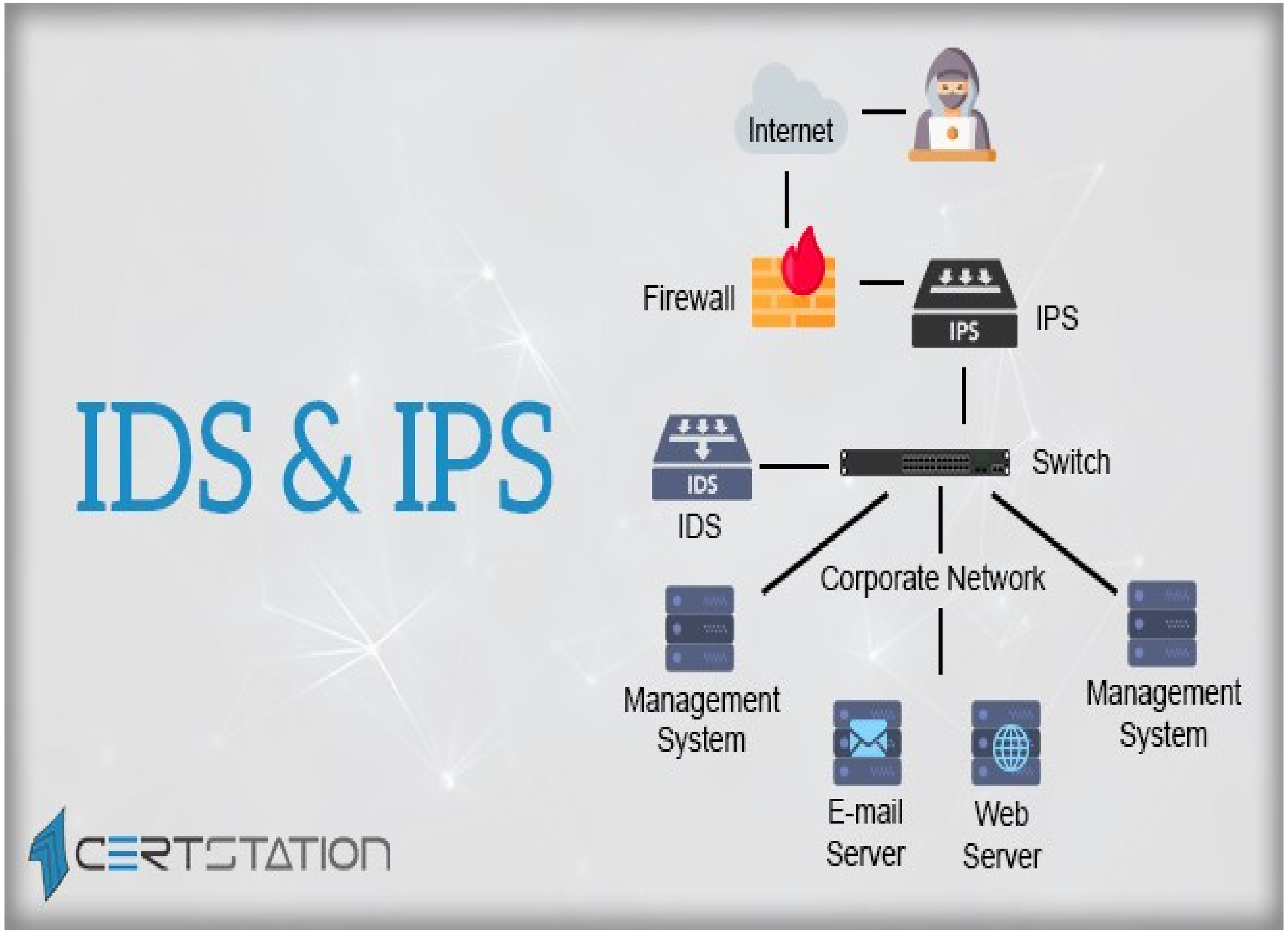
4.11 Vulnerability Management

Co-funded by
the European Union

4.1 Intrusion Detection and Prevention Systems

- cybersecurity tools designed to detect and prevent unauthorized access, misuse, or malicious activities within a network or system
- work by monitoring network traffic and system activities, identifying suspicious behavior, and taking action to block or mitigate potential threats
- combines both Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) functionalities to provide a comprehensive defense mechanism.

Co-funded by
the European Union



Co-funded by the European Union

4.1 Components and Architecture

Intrusion Detection System (IDS):

- monitoring system that analyzes traffic to identify abnormal or malicious activities
- When a threat is detected, the IDS generates alerts but does not take action to stop the threat itself.
- **Types:**
- **Network-based IDS (NIDS):** Monitors entire network traffic for potential threats.
- **Host-based IDS (HIDS):** Monitors activities on individual devices (hosts), such as file system changes or application behavior.

4.1 Components and Architecture

Detection Methods:

Signature-based Detection: Compares incoming data to a known database of threat signatures

Anomaly-based Detection: Uses machine learning or statistical models to detect deviations from normal network behavior

CS4ALL CYBERSECURITY FOR ALL

Co-funded by the European Union

4.1 Components and Architecture

- **Intrusion Prevention System (IPS):**

extends IDS functionality by not only detecting threats but also actively preventing or blocking them

When malicious activity is identified, the IPS can drop malicious packets, block traffic, or terminate connections in real-time.

4.1 Components and Architecture

- **Types**
- **Network-based IPS (NIPS):** Sits inline with network traffic to detect and block threats before they reach their destination.
- **Host-based IPS (HIPS):** Installed on individual devices and takes action to stop malicious activity at the host level.

CS4ALL CYBERSECURITY FOR ALL
Co-funded by the European Union

4.1 Components and Architecture

Prevention Actions:

Packet Dropping: Discarding malicious packets

Connection Termination: Breaking connections associated with malicious activities.

Rate Limiting: Slowing down traffic flows that seem to overwhelm the network

4.1 Components and Architecture

Monitoring and Analysis:

- involves continuous monitoring of network traffic, system logs, and endpoint behaviors
- Advanced systems incorporate machine learning to improve accuracy in identifying potential threats.
- Data is collected and analyzed in real-time to detect attack patterns, unauthorized access attempts, and other malicious activity.

CS4ALL CYBERSECURITY FOR ALL

Co-funded by the European Union

4.1 Components and Architecture

Logging and Alerting:

- When a suspicious activity is detected, IDPS systems log the event details, including timestamps, IP addresses, and nature of the threat

- Alerts are generated and sent to security teams or SIEM (Security Information and Event Management) systems for further analysis and response.

Co-funded by
the European Union

4.1 Components and Architecture

Response Mechanisms:

- **Automatic Responses:** take automatic actions such as blocking malicious traffic, terminating sessions, or applying firewall rules.
- **Manual Responses:** alerts are sent to administrators who can manually intervene by investigating and stopping the threat.

Co-funded by the European Union

4.2 Common Detection Methodologies

Signature-Based Detection:

- Detects known threats by comparing traffic against a database of known attack patterns or malware signatures
- Advantage: Effective for identifying known threats.
- Limitation: Cannot detect new or unknown threats

CS4ALL CYBERSECURITY FOR ALL
Co-funded by the European Union

4.2 Common Detection Methodologies

Anomaly-Based Detection:

- Detects potential threats by identifying deviations from normal behavior or baseline traffic patterns.
- Advantage: Can detect new or previously unknown threats.
- Limitation: Can produce false positives, as normal behavior may change over time.

Co-funded by the European Union

4.2 Common Detection Methodologies

Hybrid Detection:

- Combines both signature-based and anomaly-based detection methods to increase accuracy and reduce false positives.
- Most modern IDPS systems use hybrid models to balance effectiveness and efficiency.

Co-funded by the European Union

4.3 Anomaly and Stateful Protocol Analysis

Anomaly Detection:

- focuses on identifying deviations from normal or expected behavior within a network or system
- approach compares current activities to a predefined baseline of normal behavior and flags any significant deviations as potential threats.

Co-funded by
the European Union

Key Concepts of Anomaly Detection:

- **Baseline Creation:** establishing a baseline of normal behavior.
- monitoring network traffic, system activities, or user behavior over time to understand what "normal" looks like in the environment.
- **Deviation Detection:** system monitors current activities and compares them to the baseline.
- If an activity or event deviates significantly from the norm, it is flagged as an anomaly.
- **Machine Learning and Statistical Models:** identify deviations. For example, a machine learning algorithm might learn typical user login times, network traffic patterns, or data access behaviors, and flag anomalies based on these insights.

CS4ALL CYBERSECURITY FOR ALL

Co-funded by the European Union

Stateful Protocol Analysis

- structured and protocol-specific approach to detecting malicious activity
- It involves monitoring network traffic and comparing it to expected patterns based on established protocols (like HTTP, FTP, DNS, etc.)
- keep track of the state of network connections.

CS4ALL CYBERSECURITY FOR ALL

Co-funded by the European Union

Key Concepts of Stateful Protocol Analysis

- **Protocol Specification:** uses predefined models of how network protocols should behave
- For example, the HTTP protocol has well-defined request and response structures
- any deviation from this expected behavior could signal malicious activity.

- **State Tracking:** analysis tracks the state of network connections over time.
- it remembers the sequence of packet exchanges in a connection, ensuring that each step in the process conforms to the protocol's expected behavior.

CS4ALL CYBERSECURITY FOR ALL

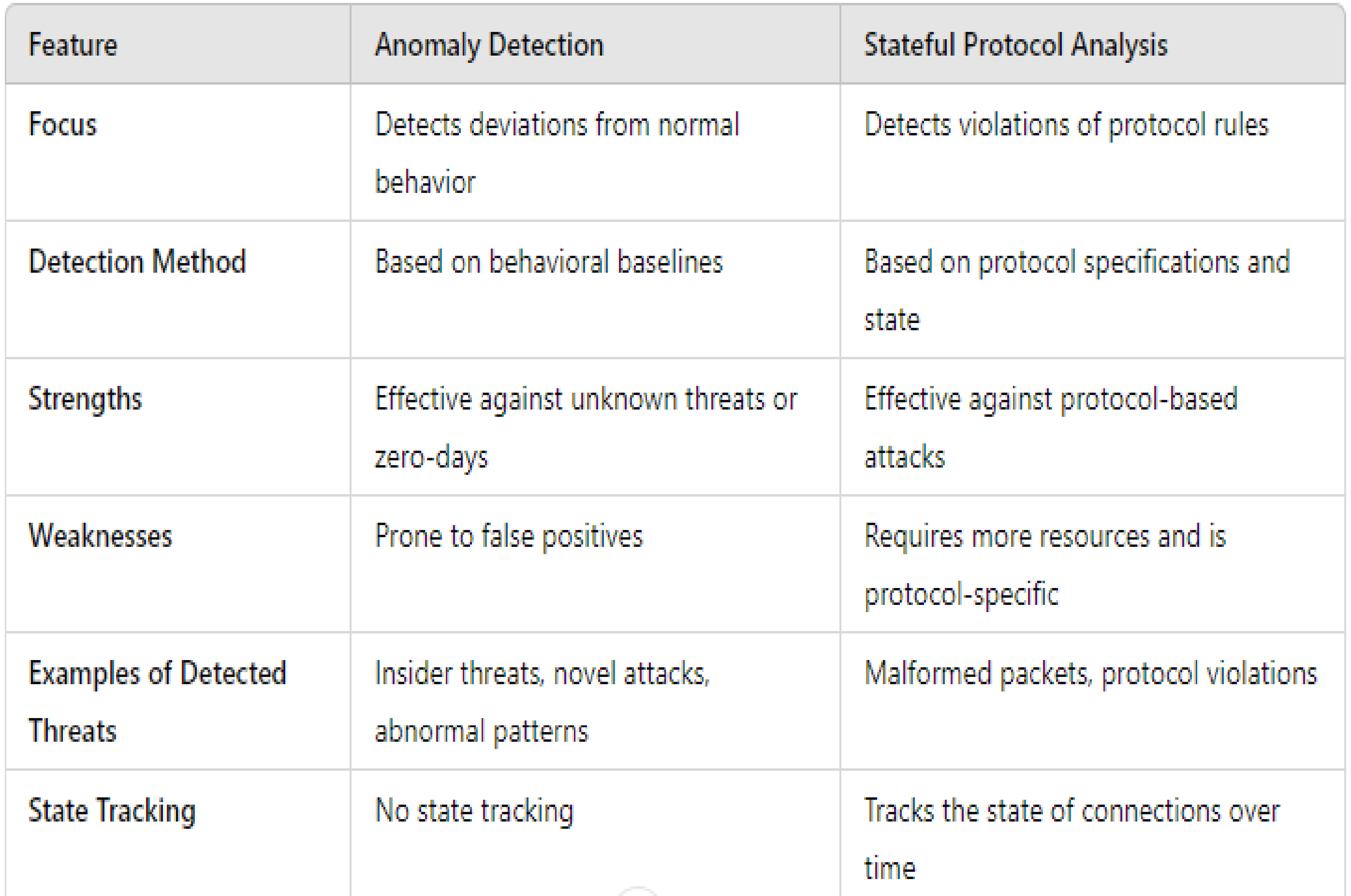
Co-funded by the European Union

Key Concepts of Stateful Protocol Analysis

- **Behavior Comparison:** compares the actual behavior of traffic to the expected behavior defined by the protocol.
- If the traffic deviates from the expected behavior it is flagged as suspicious.

Co-funded by the European Union

Comparison of Anomaly Detection and Stateful Protocol Analysis



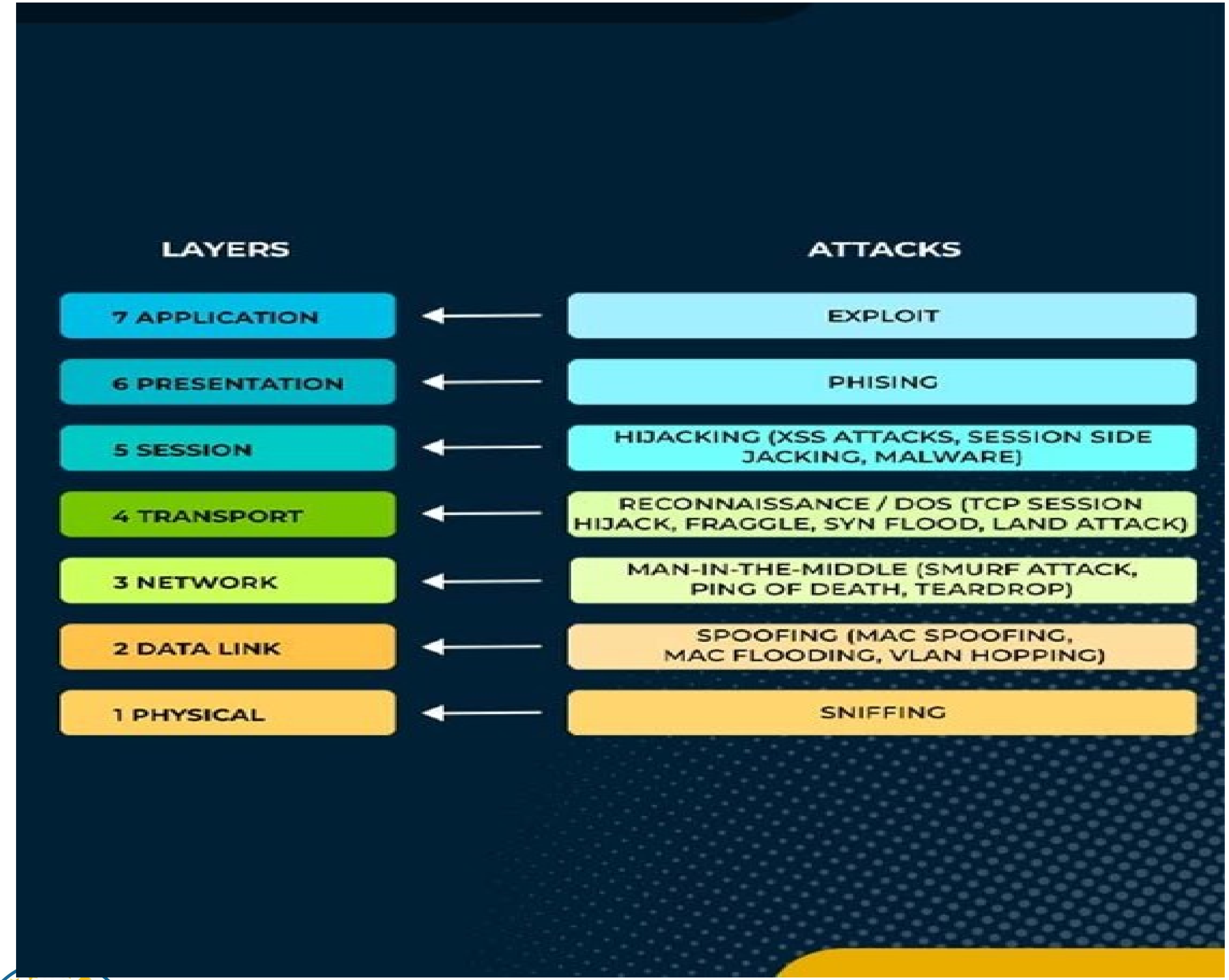
Feature	Anomaly Detection	Stateful Protocol Analysis
Focus	Detects deviations from normal behavior	Detects violations of protocol rules
Detection Method	Based on behavioral baselines	Based on protocol specifications and state
Strengths	Effective against unknown threats or zero-days	Effective against protocol-based attacks
Weaknesses	Prone to false positives	Requires more resources and is protocol-specific
Examples of Detected Threats	Insider threats, novel attacks, abnormal patterns	Malformed packets, protocol violations
State Tracking	No state tracking	Tracks the state of connections over time

Co-funded by
the European Union

4.4 Network and Hardware Layer attacks

- attacks target the foundational levels of the OSI model, specifically focusing on the network layer (Layer 3) and the data link or physical layers (Layer 2 and Layer 1).
- attacks exploit vulnerabilities in the underlying network infrastructure, hardware components, or communication protocols to disrupt services, gain unauthorized access, or compromise data integrity.

Co-funded by
the European Union



LAYERS	ATTACKS
7 APPLICATION	EXPLOIT
6 PRESENTATION	PHISING
5 SESSION	HIJACKING (XSS ATTACKS, SESSION SIDE JACKING, MALWARE)
4 TRANSPORT	RECONNAISSANCE / DOS (TCP SESSION HIJACK, FRAGGLE, SYN FLOOD, LAND ATTACK)
3 NETWORK	MAN-IN-THE-MIDDLE (SMURF ATTACK, PING OF DEATH, TEARDROP)
2 DATA LINK	SPOOFING (MAC SPOOFING, MAC FLOODING, VLAN HOPPING)
1 PHYSICAL	SNIFFING

CS4ALL
CYBERSECURITY FOR ALL

Co-funded by
the European Union

Network Layer (Layer 3) Attacks

- The network layer is responsible for routing data packets across networks, managing IP addresses, and ensuring that data reaches its intended destination.

- attacks typically target the protocols, devices, or mechanisms used for packet delivery and routing.

Co-funded by
the European Union

Common Network Layer Attacks

- IP Spoofing
- Man-in-the-Middle (MitM) Attack
- Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks
- Packet Sniffing
- Routing Table Poisoning
- Fragmentation Attacks

CS4ALL CYBERSECURITY FOR ALL

Co-funded by the European Union

Hardware Layer and Data Link Layer (Layers 1 and 2) Attacks

- involves the physical infrastructure of the network, including routers, switches, network interface cards (NICs), and communication cables
- The data link layer manages how data is formatted for transmission over physical media and includes MAC addresses for local network communications
- Attacks at these layers focus on exploiting vulnerabilities in hardware devices, network interfaces, or communication protocols.

Hardware and Data Link Layer Attacks

- MAC Address Spoofing
- ARP Spoofing
- Switch Spoofing
- Physical Layer Attacks
- Firmware Attacks

CS4ALL CYBERSECURITY FOR ALL

Co-funded by the European Union

Countermeasures for Network and Hardware Layer Attacks

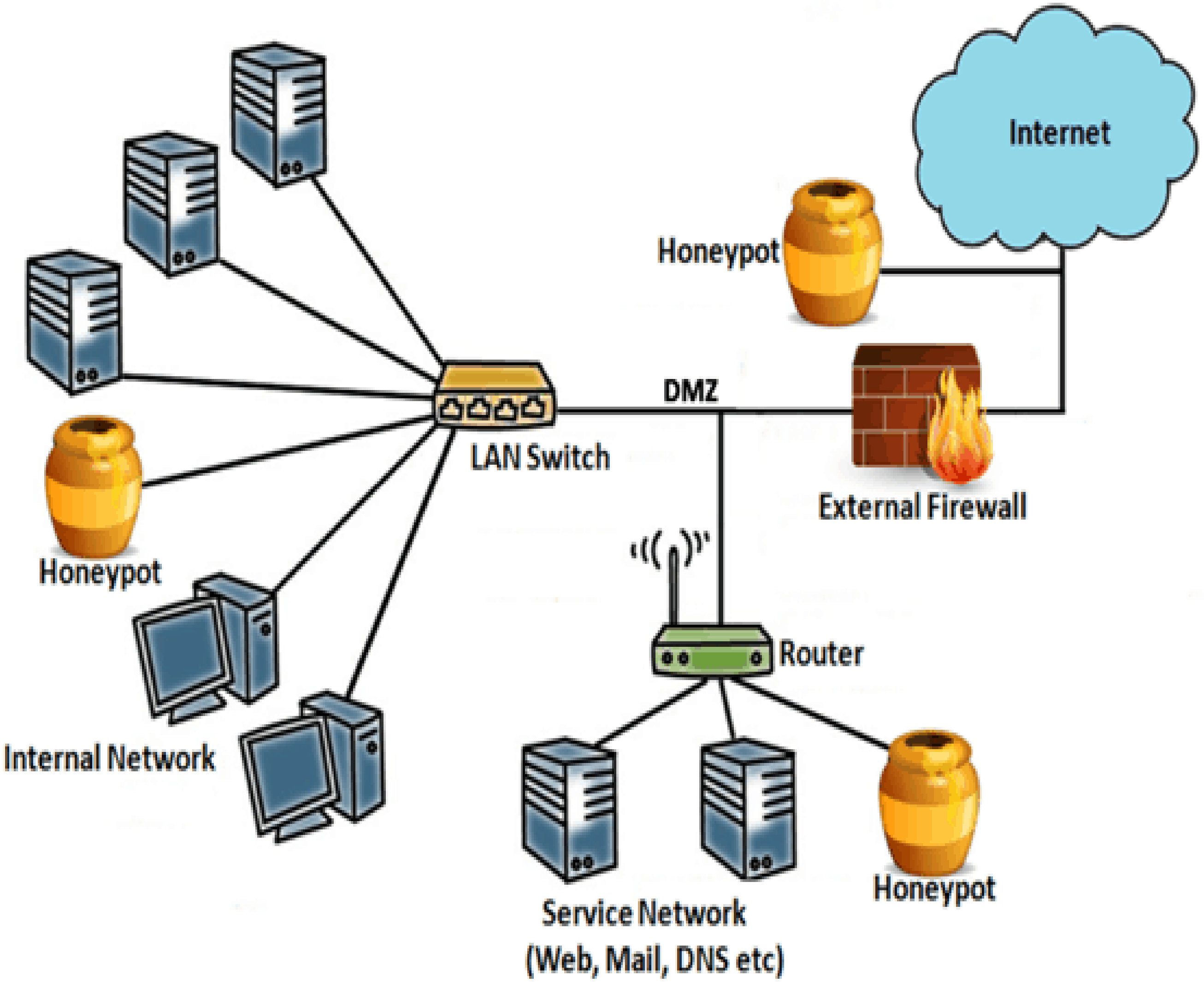
- Strong Network Segmentation
- Firewalls and Access Control Lists (ACLs)
- Encryption
- Intrusion Detection and Prevention Systems (IDPS)
- Port Security
- Physical Security

CS4ALL
CYBERSECURITY FOR ALL
Co-funded by the European Union

4.5 Honeypots

- networks set up to attract, detect, and analyze cyber attackers by simulating vulnerabilities that seem appealing to them
- act as bait, luring attackers into interacting with them
- while allowing defenders to monitor and study the attack techniques used,
- without putting the real network or systems at risk.

Co-funded by
the European Union



Co-funded by
the European Union

Types of Honeypots

- **Low-Interaction Honeypots**
- simulate basic services or operating systems but offer limited interaction.
- designed to emulate a system or service (e.g., a web server or database) with minimal functionality,
- allowing defenders to capture information about the attacker’s tools and methods without letting them perform complex operations.
- Primarily used to collect basic information about attack patterns, detect automated attacks, or identify scanning activities.

Co-funded by
the European Union

Types of Honeypots

High-Interaction Honeypots:

- simulate a full, real environment where attackers are free to interact.
- sophisticated and allow attackers to perform complex actions, giving security teams more detailed insights into their behavior, tactics, and tools.
- Used for in-depth analysis of attackers' strategies, especially for identifying sophisticated threats

CS4ALL CYBERSECURITY FOR ALL
Co-funded by the European Union

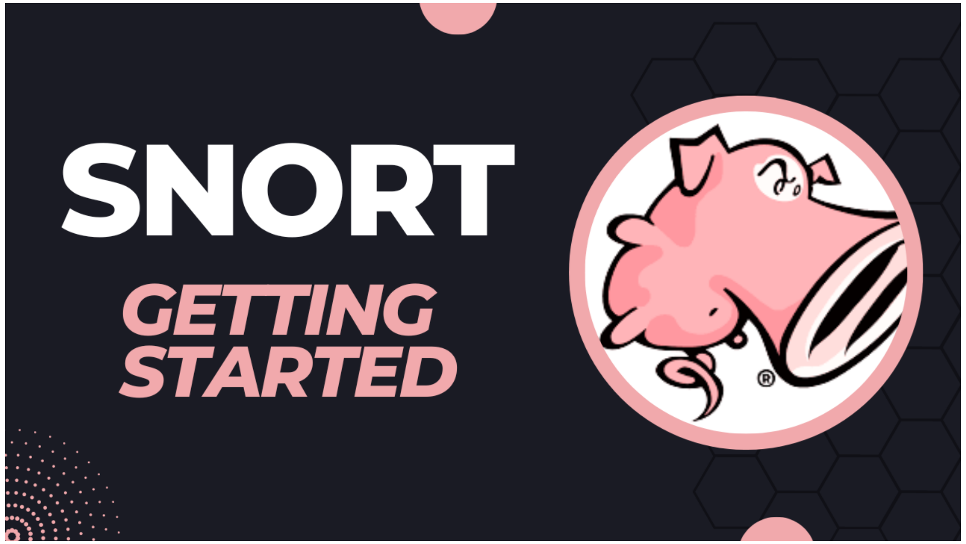
Benefits of Honeypots

- Early Detection of Threats
- Gathering Threat Intelligence
- Identifying New Vulnerabilities
- Understanding Attack Trends
- Diverting Attackers

Co-funded by
the European Union

4.6 Working with SNORT IDS

- open-source Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).
- used to monitor network traffic and detect malicious activities or policy violations.



Co-funded by the European Union

Installation and Configuration

- **Installation:** installation usually involves downloading the software from the SNORT website or using package managers.
- **Configuration:**involves setting up the SNORT configuration file (snort.conf)
- define various parameters such as network interfaces to monitor, log file locations, and rule sets.

Co-funded by the European Union

Rules and Signatures

- **Rules:** SNORT rules are written in a specific format
- include conditions that specify what constitutes malicious activity.
- Rules can be customized to suit your environment.
- **Rule Sets:** SNORT has default rule sets,
- Rules can be specific to different types of attacks, such as SQL injection, buffer overflows, or port scans.

Co-funded by
the European Union

Modes of Operation

- **IDS Mode:** SNORT passively monitors network traffic
- generates alerts based on the rules configured.
- It doesn’t block any traffic
- provides logs and alerts that can use for analysis.
- **IPS Mode:** SNORT can actively block or reject malicious traffic.
- requires more configuration to ensure that legitimate traffic is not mistakenly blocked.

CS4ALL CYBERSECURITY FOR ALL

Co-funded by the European Union

Analysis and Logs

- **Alerts:** detects suspicious activity based on the rules, it generates alerts.
- alerts can be logged to a file,
- sent to a remote server,
- integrated with other monitoring systems.
- **Logs:** maintains detailed logs of network traffic and alerts.
- logs are crucial for forensic analysis and troubleshooting.

Co-funded by
the European Union

Integration and Tools

- **Snort Reporters:** Tools like BASE (Basic Analysis and Security Engine) or Snorby can be used to visualize and analyze SNORT alerts.
- **Integration:** can be integrated with other security tools like SIEM (Security Information and Event Management) systems to provide a comprehensive view of network security.

Co-funded by
the European Union

Updates and Maintenance

- **Rules Updates:** frequently updates the rule sets to address new threats.
- **System Maintenance:** Periodically check and maintain the SNORT installation and configuration to ensure it operates efficiently and effectively.

- **Overall, working with SNORT involves setting it up, configuring rules, monitoring alerts, and integrating it with other tools to enhance network security posture.**

CS4ALL CYBERSECURITY FOR ALL

Co-funded by
the European Union

4.7 Need for multiple IDPS Technologies?

- Using multiple Intrusion Detection and Prevention Systems (IDPS) technologies helps strengthen overall security.

Co-funded by
the European Union

Covering Different Areas

- **Network-Based IDPS:** helps catch threats trying to enter or leave network, like hackers or malicious software.
- **Host-Based IDPS:** helps catch problems that the outside might miss, such as suspicious activity on a specific computer.
- **Signature-Based Detection:** spotting familiar threats but might miss new ones.

Co-funded by
the European Union

Using Different Detection Methods

- **Anomaly-Based Detection:** helps catch new or strange behavior but might sometimes flag harmless activities as suspicious.
- **Behavioral Analysis:** focuses on watching patterns of activity to spot anything out of the ordinary.

Filling in the Gaps

Different IDPS technologies can spot different types of threats:

- **Network Sensors:** Watch the overall network to catch threats from external sources.
- **Endpoint Sensors:** Watch individual computers or servers to spot threats that might get past the network sensors.

Reducing Mistakes

- **Fewer False Alarms:** Using various systems together helps reduce mistakes

- **Better Accuracy:** Combining different detection methods helps improve accuracy, catching genuine threats while avoiding false alarms.

CS4ALL CYBERSECURITY FOR ALL
Co-funded by the European Union

Adapting to New Threats

- **Staying Updated:** Cyber threats keep changing, so using different systems means are better prepared to deal with new kinds of attacks.
- **Flexible Response:** Different systems can adapt to different types of threats, making overall security more flexible.

Co-funded by
the European Union

4.8 IPS using IP Trace back - Probabilistic and Deterministic Packet Marking

Co-funded by
the European Union

IP Traceback

- technique used to identify the source of malicious network traffic
- particularly useful in mitigating attacks like Distributed Denial of Service (DDoS).
- When combined with Intrusion Prevention Systems (IPS), it helps in tracing and potentially blocking the source of attacks
- There are two main methods for IP traceback:
- Probabilistic Packet Marking
- Deterministic Packet Marking.

Co-funded by
the European Union

Deterministic Packet Marking

- Routers mark packets in a fixed and predetermined way
- packet is marked with specific information that helps trace back to its origin.
- marking is consistent and does not rely on randomness.

CS4ALL CYBERSECURITY FOR ALL
Co-funded by the European Union

How It Works

- **Marking Process:**router adds a specific mark or identifier to the packet header.
- mark indicates the router's identity and its position in the path taken by the packet.
- **Traceback Process:** When an attack occurs, the IPS collects packets and their marks.
- By analyzing these marks, it can reconstruct the path the packets took,
- helping to trace back to the source of the attack.

Co-funded by
the European Union

Probabilistic Packet Marking

- uses a random approach to add traceback information to packets.
- Routers mark packets with some probability rather than consistently marking every packet.

Co-funded by
the European Union

How It Works

- **Marking Process:** router decides whether to mark a packet based on a certain probability.
- If a packet is marked, it contains a mark that helps identify the router.
- not every packet carries traceback information, only a subset.
- **Traceback Process:** The IPS collects marked packets and uses statistical methods to infer the path taken by the packets.
- By analyzing the probability and distribution of marks, it can reconstruct the attack path.

CS4ALL CYBERSECURITY FOR ALL
Co-funded by the European Union

Example Scenario

1. **Attack Traffic:**

o An attacker sends malicious packets to your network.

2. **Packet Marking:**

o Routers along the path add traceback marks to some of these packets.

3. **Malicious Packet Detection:**

o The IPS detects that some packets are malicious based on their content or behavior.

4. **Path Reconstruction:**

o Using the traceback marks, the IPS reconstructs the route taken by the malicious packets and identifies that they passed through certain routers.

5. **Identifying the Origin:**

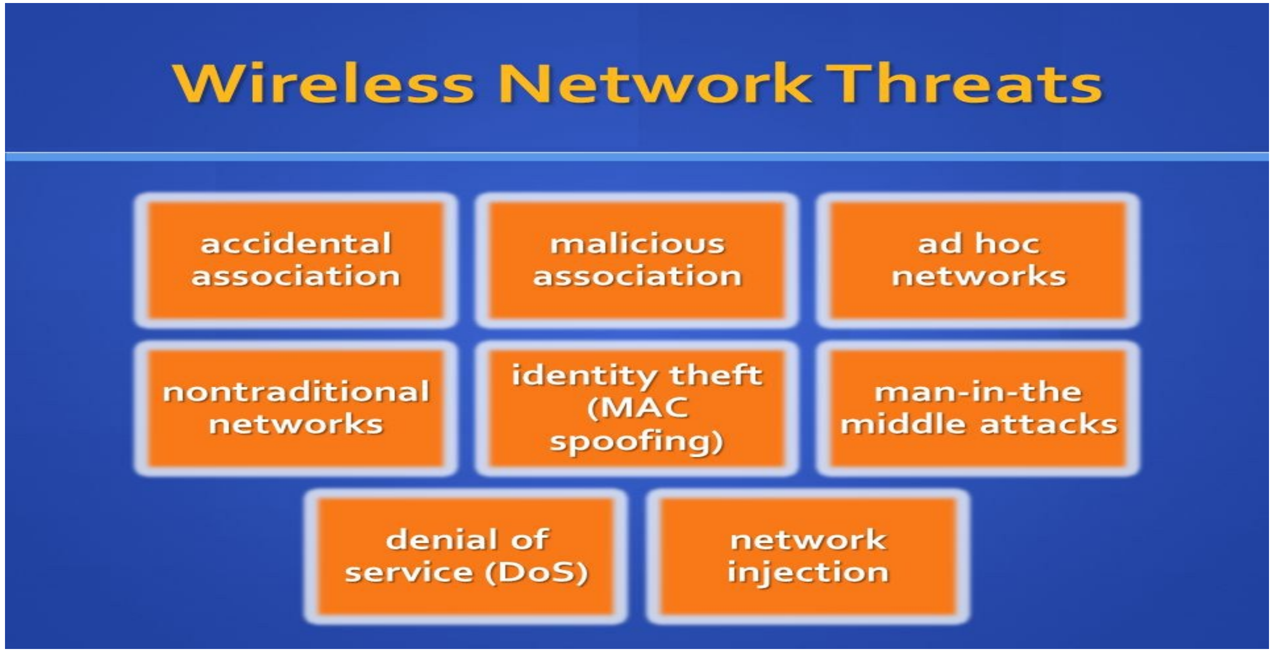
o By tracing the path and analyzing the traceback information, you can determine the source network or IP address of the attack.

CS4ALL CYBERSECURITY FOR ALL

Co-funded by
the European Union

4.9 Threats against WLANs

- WLANs are popular for their convenience and flexibility,
- face various threats that can compromise their security.



Wireless Network Threats

accidental association

malicious association

ad hoc networks

nontraditional networks

identity theft (MAC spoofing)

man-in-the middle attacks

denial of service (DoS)

network injection

Co-funded by the European Union

Eavesdropping

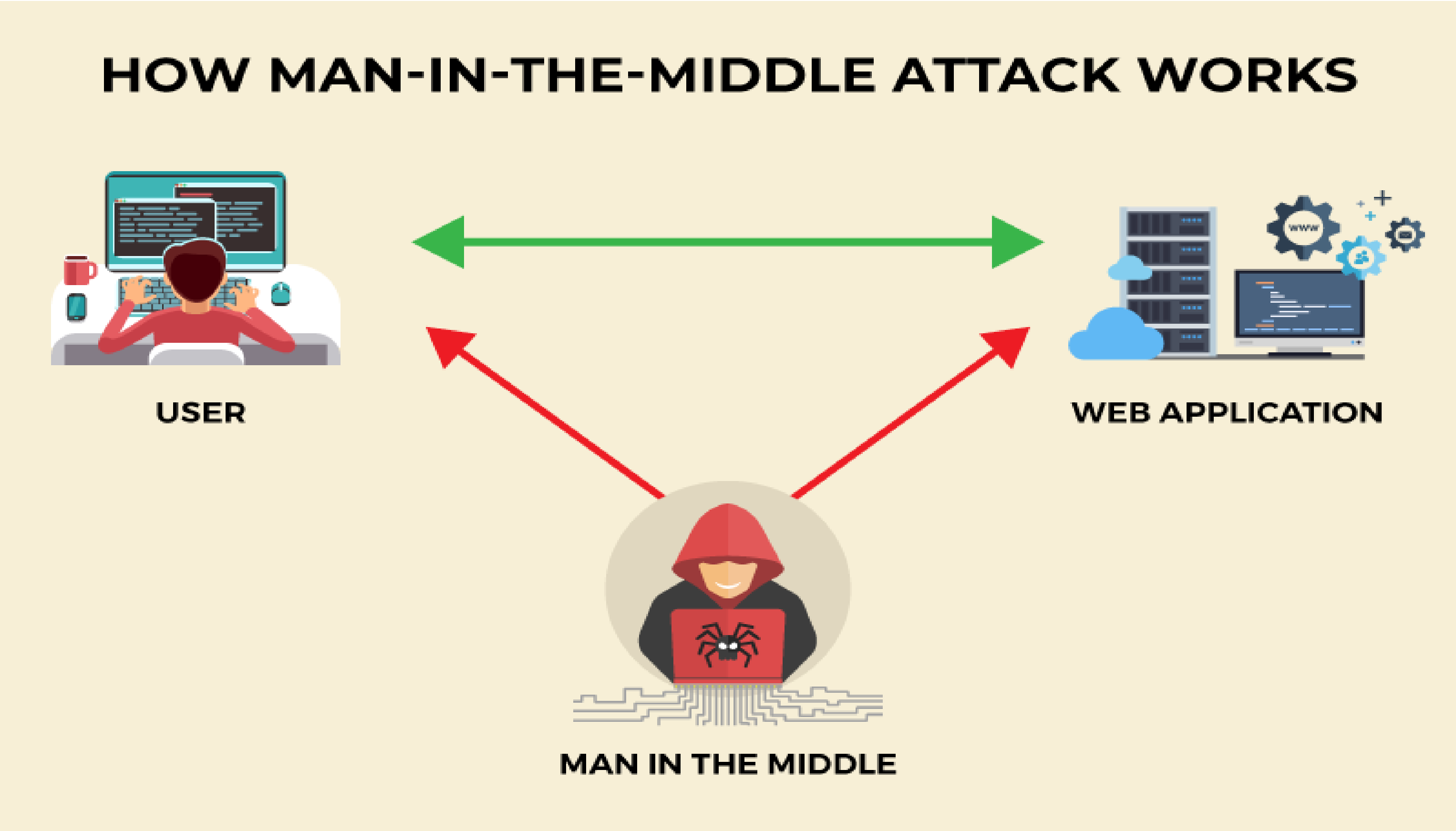
- Intercepting and listening to data transmitted over the wireless network.
- **Examples:**
- Packet Sniffing
- **Mitigation:**
- **Encryption:** Use encryption protocols
- **VPNs:** Utilize Virtual Private Networks (VPNs) to add an additional layer of encryption.

Co-funded by the European Union

Man-in-the-Middle Attacks

- Attackers intercept and possibly alter the communication between two parties without their knowledge.
- **Examples:**
- Session Hijacking: An attacker intercepts a session between a user and a network service, potentially gaining access to sensitive information.
- **Mitigation:**
- **Secure Protocols:** Use secure communication protocols like HTTPS
- **Certificate Validation:** Ensure proper validation of security certificates

Man-in-the-Middle Attacks



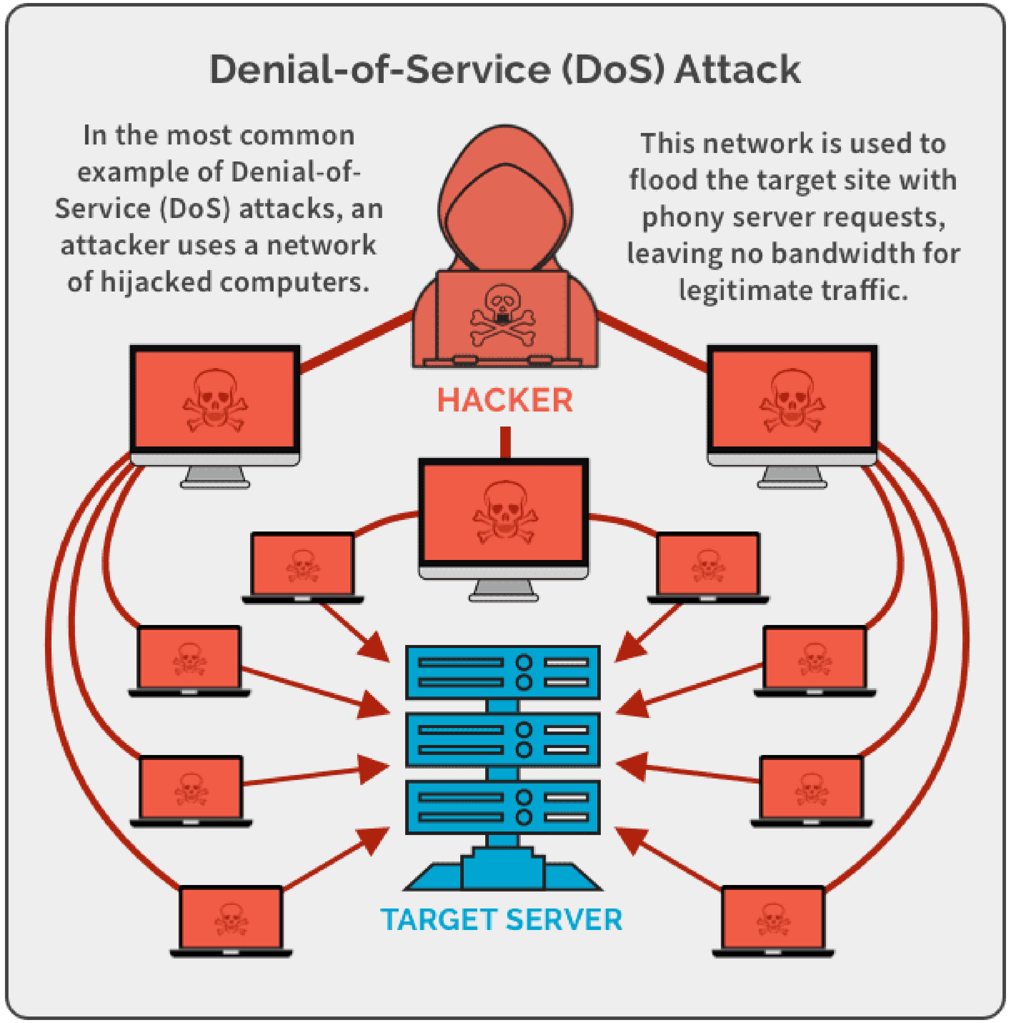
CS4ALL
CYBERSECURITY FOR ALL
Co-funded by
the European Union

Denial of Service (DoS) Attacks

- Attackers overload the network with excessive traffic, making it unavailable to legitimate users.
- **Examples:**
- **Flooding Attacks:** Attackers send a large volume of traffic to the WLAN, causing network congestion and disrupting service.
- **Mitigation:**
- **Rate Limiting:** Implement traffic rate limiting to prevent flooding attacks.
- **Network Monitoring:** Continuously monitor network traffic for unusual patterns

Co-funded by the European Union

Denial of Service (DoS) Attacks



Denial-of-Service (DoS) Attack

In the most common example of Denial-of-Service (DoS) attacks, an attacker uses a network of hijacked computers.

This network is used to flood the target site with phony server requests, leaving no bandwidth for legitimate traffic.

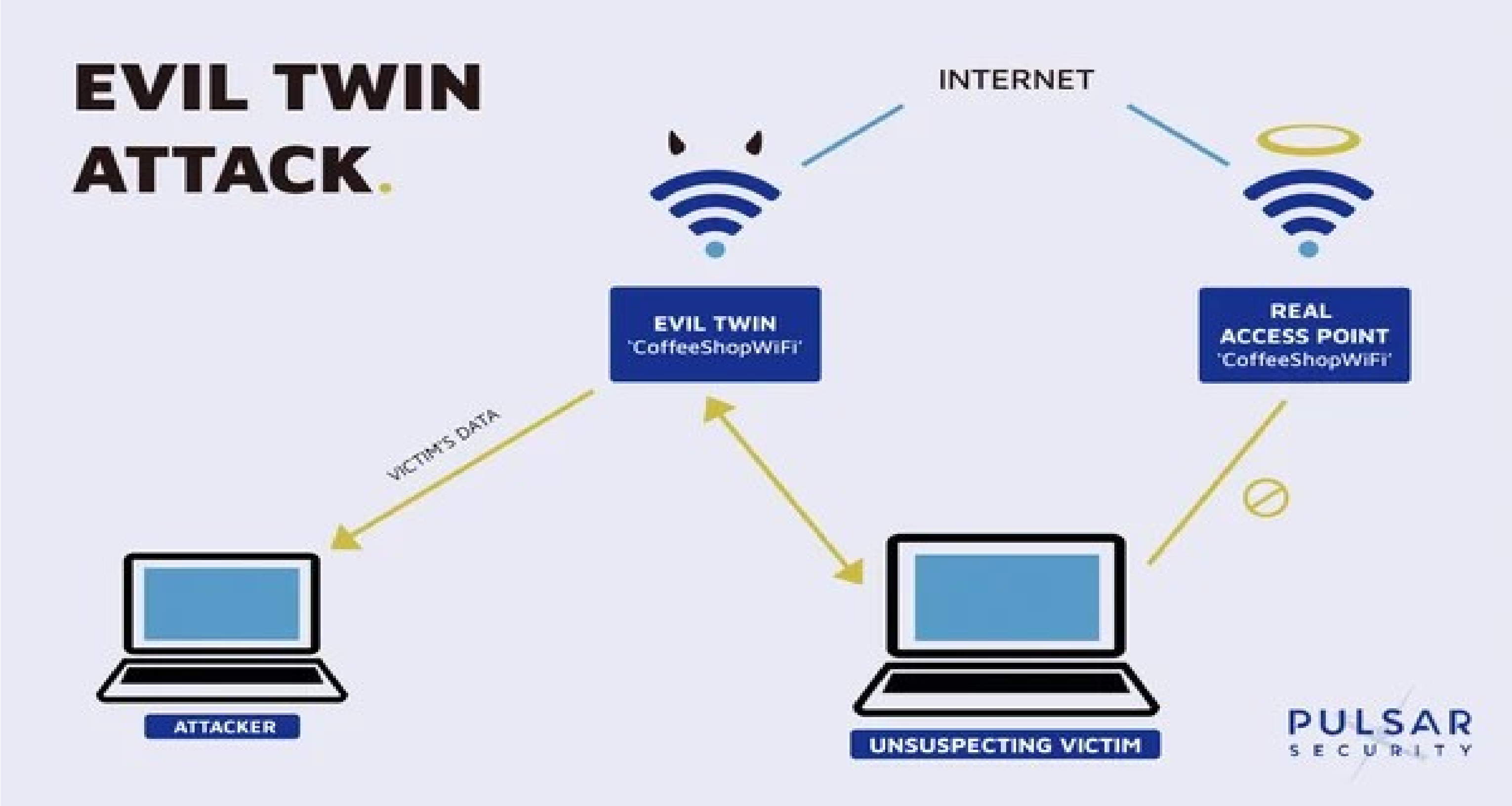
Co-funded by
the European Union

Evil Twin Attacks

- An attacker sets up a rogue wireless access point with the same name as a legitimate one to trick users into connecting to it.
- **Examples:**
- **Fake Hotspots:** Attackers create a fake Wi-Fi hotspot with a name similar to a legitimate network, luring users to connect and potentially steal their information.
- **Mitigation:**
  Network Name (SSID) Management: Use unique and non-obvious SSIDs for your network.
  Secure Authentication: Implement strong authentication and encryption to ensure that only authorized devices can connect.

Co-funded by
the European Union

Evil Twin Attacks



Co-funded by the European Union

Physical Security Risks

- Physical threats to the hardware that supports the WLAN.
- **Examples:**
- **Hardware Theft:** Attackers steal access points or routers to gain access to the network.
- **Physical Tampering:** Attackers physically tamper with network devices to compromise their functionality.
- **Mitigation:**
  Physical Security Measures: Secure network hardware in locked rooms
  Regular Audits: Perform regular checks to ensure hardware security.

CS4ALL CYBERSECURITY FOR ALL

Co-funded by the European Union

Key Strategies for WLAN Security

- To protect WLANs, it's essential to use strong authentication, encryption, secure protocols, network monitoring, and proper configuration practices.
- Regularly reviewing and updating security measures helps mitigate these threats and ensures a safer wireless environment.

CS4ALL CYBERSECURITY FOR ALL

Co-funded by
the European Union

4.10 Behavioural Analytics

- Involves monitoring and analyzing network traffic and user behavior to detect, understand, and respond to potential security threats.
- Approach focuses on identifying unusual or suspicious activities that may indicate security incidents, such as cyberattacks or data breaches.

CS4ALL CYBERSECURITY FOR ALL
Co-funded by the European Union

Key Aspects of Behavioral Analytics in Network Security

1. **Data Collection:**

- **Network Traffic:** Collect data on network traffic patterns, including data flows, protocols used, and communication endpoints.
- **User Activities:** Monitor user activities such as login attempts, file access, and application usage.
- **System Logs:** Gather logs from network devices servers, and security appliances.

Co-funded by
the European Union

Key Aspects of Behavioral Analytics in Network Security

2. **Data Processing:**

- **Normalization:** Standardize and clean data from various sources to ensure consistency and accuracy.
- **Aggregation:** Combine data from multiple sources to get a comprehensive view of network and user activities

Co-funded by the European Union

Key Aspects of Behavioral Analytics in Network Security

3. **Behavioral Analysis:**

- **Pattern Recognition:** Identify normal patterns of network and user behavior.
- **Anomaly Detection:** Detect deviations from established patterns.
- **Risk Scoring:** Assign risk scores to different behaviors based on their deviation from the norm and potential threat level.

Co-funded by
the European Union

Key Aspects of Behavioral Analytics in Network Security

4. **Response and Mitigation:**

- **Alerts and Notifications:** Generate alerts when suspicious behavior or anomalies are detected.
- **Automated Responses:** Implement automated actions to mitigate threats, such as blocking suspicious IP addresses or isolating compromised devices.
- **Incident Investigation:** Use the insights gained from behavioral analytics to investigate and understand the nature of security incidents.

Applications of Behavioral Analytics in Network Security

1. **Threat Detection:**

- **Insider Threats:** Identify abnormal behavior from legitimate users
- **External Attacks:** Detect patterns indicative of cyberattacks, such as unusual network scanning or a surge in failed login attempts that might signal a brute force attack.

Co-funded by
the European Union

Applications of Behavioral Analytics in Network Security

2. Anomaly Detection:

- **Unusual Traffic:** Spot abnormal traffic patterns, such as a sudden increase in outbound traffic which might indicate data exfiltration.
- **Strange Behavior:** Detect irregular behavior like unauthorized attempts to access sensitive data or systems.

Co-funded by
the European Union

Example Scenario

Company Network Security:

1. **Data Collection:**

Network monitoring tools collect data on user logins, file access, data transfers, and network traffic.

2. **Behavioral Analysis:**

o Normal Pattern: Typically, employees access files during business hours and from their office locations.

o Anomaly Detected: A user account that usually accesses files in the morning starts accessing a large number of files late at night and from a foreign IP address.

3. **Response:**

o Alert Generated: An alert is triggered due to the unusual behavior of accessing files from an unusual location and at odd hours.

o Automated Action: The system temporarily locks the account and requires additional verification to confirm legitimacy.

Co-funded by the European Union

Benefits of Behavioral Analytics in Network Security

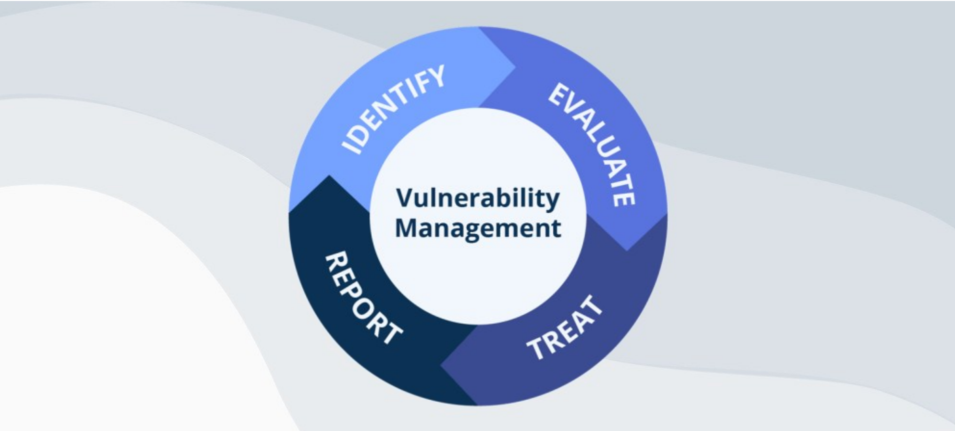
- **Improved Threat Detection:** Enhances the ability to detect sophisticated attacks
- **Reduced False Positives:** helps in distinguishing between genuine threats and benign anomalies.
- **Faster Response:** Enables quicker detection and response to potential security incidents

CS4ALL CYBERSECURITY FOR ALL

Co-funded by the European Union

4.11 Vulnerability Management

- approach to identifying, assessing, prioritizing, and mitigating vulnerabilities in a system or network to reduce the risk of exploitation by attackers.
- It involves a continuous cycle of monitoring and improving security to protect an organization's assets.



Co-funded by the European Union

Key Components of Vulnerability Management

1. **Discovery:**

- **Asset Inventory:** Maintain a comprehensive inventory of all hardware, software, and network components within the organization.
- **Vulnerability Scanning:** Use automated tools to scan systems and applications for known vulnerabilities.

CS4ALL
CYBERSECURITY FOR ALL
Co-funded by
the European Union

Key Components of Vulnerability Management

2. **Assessment:**

- **Vulnerability Assessment:** Evaluate the vulnerabilities identified during scanning to understand their potential impact and likelihood of exploitation.
- **Risk Assessment:** Determine the risk associated with each vulnerability by considering factors such as the vulnerability severity, exploitability, and the value of the affected asset.

CS4ALL CYBERSECURITY FOR ALL

Co-funded by the European Union

Key Components of Vulnerability Management

3. **Prioritization:**

- **Severity Rating:** Classify vulnerabilities based on their severity using metrics Business Impact: Prioritize vulnerabilities based on the potential impact on business operations and the criticality of the affected systems.

Co-funded by
the European Union

Key Components of Vulnerability Management

4. **Remediation:**

- **Patch Management:** Apply patches and updates provided by software vendors to fix known vulnerabilities.
- **Configuration Changes:** Adjust system configurations to close security gaps or mitigate risks.
- **Workarounds:** Implement temporary fixes or controls to reduce the risk until a permanent solution can be applied.

Co-funded by
the European Union

Key Components of Vulnerability Management

5. **Verification:**

- **Validation:** verify that the vulnerabilities have been addressed and that the fixes are effective.
- **Re-Scanning:** Perform additional scans to ensure that vulnerabilities have been successfully mitigated and no new vulnerabilities have been introduced.

Co-funded by
the European Union

Key Components of Vulnerability Management

6. Reporting and Documentation:

- **Reporting:** Document the vulnerabilities identified, the actions taken, and the status of remediation efforts. Reports help in tracking progress and compliance.
- **Documentation:** Maintain records of vulnerability assessments, prioritization decisions, and remediation actions for auditing and continuous improvement.

Co-funded by the European Union

Key Components of Vulnerability Management

7. **Continuous Improvement:**

- **Review and Adjust:** Regularly review and refine the vulnerability management process based on lessons learned, new threats, and changes in the IT environment.
- **Training and Awareness:** Ensure that staff are trained and aware of best practices for managing vulnerabilities and securing systems.

CS4ALL CYBERSECURITY FOR ALL

Co-funded by the European Union

Benefits of Vulnerability Management

- **Reduced Risk:** Identifies and addresses vulnerabilities before they can be exploited by attackers.
- **Improved Security Posture:** Strengthens the overall security of systems and networks by addressing known weaknesses.
- **Compliance:** Helps meet regulatory requirements and industry standards for security and data protection.
- **Operational Efficiency:** Minimizes disruptions and operational impact by proactively managing vulnerabilities.

CS4ALL CYBERSECURITY FOR ALL

Co-funded by
the European Union

Learning Outcome

1. Students will be able to identify and describe the key components and architecture of Intrusion Detection and Prevention Systems (IDPS) and their roles in enhancing network security.
2. Students will be able to apply anomaly detection and stateful protocol analysis to identify deviations from normal behavior within network traffic and evaluate their implications for security monitoring.
3. Students will be able to analyze the purpose and function of honeypots in cybersecurity, including their role in threat intelligence gathering and attack analysis.
4. Students will be able to utilize behavioral analytics to detect unusual patterns of activity within networks, enhancing threat detection capabilities and incident response.

Question no 1

What is the primary function of a firewall?

A) To encrypt data

B) To monitor and control network traffic

C) To provide antivirus protection

D) To optimize network speed

Co-funded by
the European Union

Question no 2

Which detection methodology relies on predefined signatures of known threats?

A) Anomaly-based detection

B) Signature-based detection

C) Stateful inspection

D) Behavioral analysis

Co-funded by
the European Union

Question no 3

Stateful protocol analysis is primarily used to

A) Detect known malware signatures

B) Monitor and analyze the state of network connections

C) Generate alerts based on user behavior

D) Conduct risk assessments

CS4ALL CYBERSECURITY FOR ALL

Co-funded by
the European Union

Question no 4

Which of the following is a common attack at the network layer?

A) SQL Injection

B) Denial-of-Service (DoS)

C) Cross-Site Scripting (XSS)

D) Phishing

Co-funded by
the European Union

Question no 5

Which type of honeypot allows for full interaction with attackers?

A) Low-interaction honeypot

B) Virtual honeypot

C) Passive honeypot

D) High-interaction honeypot

CS4ALL CYBERSECURITY FOR ALL

Co-funded by the European Union

Question no 6

Which of the following is a common threat to Wireless Local Area Networks (WLANs)?

A) Phishing

B) SQL Injection

C) Eavesdropping

D) Ransomware

Co-funded by
the European Union

Answers

1. **B)** To monitor and control network traffic
2. **B)** Signature-based detection
3. **B)** Monitor and analyze the state of network connections
4. **B)** Denial-of-Service (DoS)
5. **D)** High-interaction honeypot
6. **C)** Eavesdropping

Co-funded by
the European Union

Resources

List the resources you used for your research:

1. https://www.geeksforgeeks.org/what-is-packet-sniffing/
2. https://www.geeksforgeeks.org/types-of-network-firewall/
3. https://www.youtube.com/watch?v=2QGgEk20RXM
4. https://www.youtube.com/watch?v=5oioSbgBQ8I
5. https://www.youtube.com/watch?v=kDEX1HXybrU
6. https://www.youtube.com/watch?v=aUPoA3MSajU&t=138s
7. https://www.google.com/url?sa=i&url=https%3A%2F%2Fcertstation.com%2Fblog%2Fdetailed-analysis-intrusion-detection-systems-intrusion-prevention-systems%2F&psig=AOvVaw3gB971x3300b3ETTc4rMT8&ust=1728892443935000&source=images&cd=vfe&opi=89978449&ved=0CBQQjRxqFwoTCLjP7rvwiokDFQAAAAAdAAAAABAE

Co-funded by
the European Union

Resources

1. https://ccoe.dsci.in/blog/what-is-eavesdropping-attacks

1. https://threatcop.com/blog/man-in-the-middle-attack/

1. https://blog.pulsarsecurity.com/what-is-an-evil-twin-and-how-do-you-spot-one

1. https://botpenguin.com/glossary/behavioral-analytics

1. https://avatao.com/blog-understanding-the-importance-of-vulnerability-management/

Co-funded by
the European Union

Resources

1. https://cyberhoot.com/cybrary/honeypot/

1. https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.securitybytes.in%2F2022%2F08%2Fgetting-started-with-snort-ids-snort.html&psig=AOvVaw2_iWvfbKBrkTWEzyrOnIA_&ust=1728896589368000&source=images&cd=vfe&opi=89978449&ved=0CBQQjRxqFwoTCJiYilaAi4kDFQAAAAAdAAAAABAE

1. https://www.shutterstock.com/image-illustration/ip-traceback-form-binary-code-3d-665091475

1. https://www.google.com/url?sa=i&url=https%3A%2F%2Fspanning.com%2Fblog%2Fdenial-of-service-attacks-web-based-application-security-part-7%2F&psig=AOvVaw16AVUkPn8Ejowva7o603M8&ust=1728909907752000&source=images&cd=vfe&opi

Co-funded by
the European Union

Reference Book

- **"Network Intrusion Detection" by Stephen Northcutt and Judy Novak, 3rd Edition, Sams Publishing**
- **Mastering Security Information and Event Management (SIEM): Mastering Security Information and Event Management (SIEM) Kindle Edition**

Co-funded by
the European Union