COMP482
Cybersecurity
Week 3 - Wednesday

Dr. Nicholas Polanco
(he/him)

KALAMAZOO COLLEGE

Attendance

https://forms.office.com/r/BtVc9FH95i

COMP482 - Attendance

Important Notes

1. I have updated the schedule to shift things for our second networking day
2. I have downloaded Kali Linux pre-built VM's for people to use on their virtual machines, I have it on a flashdrive to help us avoid the internet connection in the lab.
    a. You don't need to use this, but if you are planning on doing a project with white hat hacking, this may be useful.
3. I am giving us more time to work on the Activity: Keylogger or Buffer Overflow today.
    a. Do we want to push this deadline a week? How are we doing on this?

Important Notes (continued)

*This is a reminder (and also on the syllabus), but if you choose to use Kali Linux, you need to make sure you are complying with Kalamazoo College's Terms of Use!

- You can check here if you have any questions, I would suggest not snooping around without first checking.
  - https://is.kzoo.edu/policies/ (See "Unacceptable Uses" :))
- You can configure your VM's network settings correctly so they interact only with the systems they intend (like other VMs)

Important Dates (Week 3)

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
				Reflection: Week 2 Project Deliverable: Meeting with Dr. Polanco Topic Deliverable: Topic Selection Activity: Keylogger or Buffer Overflow		

Outline

1. Port Scanning
2. Firewall
3. Intrusion Detection System (IDS)
4. Virtual Private Network (VPN)
5. Continue Activity: KeyLogger and Buffer Overflow

Port Scanning

Port Scanning

Port scanning is the process of systematically scanning a computer's ports to discover which ports are open and listening (i.e., available for communication).

- Each open port can represent a possible entry point to a device or network, potentially revealing services running on the system.
- This process can be used for both legitimate security assessments and malicious attacks.

Image Credit

Port Scanning (continued)

How Port Scanning Works:

A port scanner (a tool or software) sends packets to a range of ports on a target host. Based on the response (or lack of one), the scanner determines the state of the port

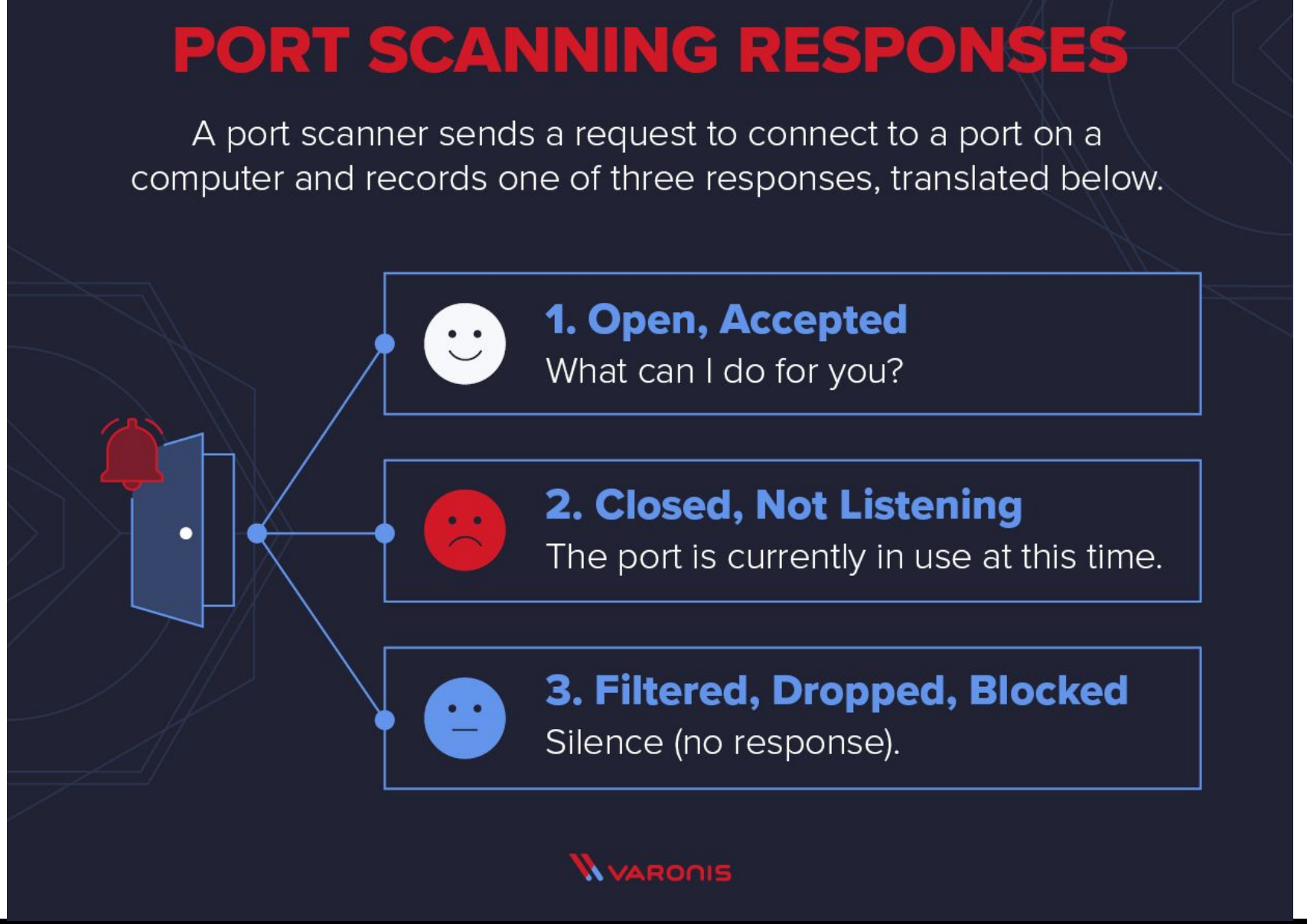

Image Credit
https://www.varonis.com/blog/port-scanning-techniques

KALAMAZOO COLLEGE

Port Number	Protocol
20, 21	File Transfer Protocol (FTP)
22	Secure Shell (SSH)
23	Telnet Protocol
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
67, 68	Dynamic Host Configuration Protocol (DHCP)
80	HyperText Transfer Protocol (HTTP)
110	Post Office Protocol (POP3)
137	NetBIOS Name Service
143	Internet Message Access Protocol (IMAP4)
443	Secure HTTP (HTTPS)
445	Microsoft-DS (Active Directory)

Image Credit
https://www.researchgate.net/figure/Commonly-used-port-numbers_tbl1_30511385

Port Scanning (continued)

Types of Port Scanning Techniques

1. TCP Connect Scan
   - Makes a full connection using the OS's network functions.
   - Easy to detect but reliable.

2. SYN Scan (Half-Open)
   - Sends a SYN packet to initiate a connection but doesn’t complete it.
   - Stealthier and faster; used by tools like Nmap.

Image Credit

Port Scanning (continued)

Types of Port Scanning Techniques

3. UDP Scan
   - Sends a UDP packet and looks for a response (or lack of one).

Less reliable due to no handshake mechanism.

4. Ping Scan
   - Checks which hosts are up before scanning ports.
   - Not a port scan by itself, but often part of reconnaissance.

Port Scanning (continued)

Types of Port Scanning Techniques

5. FIN, Xmas, and Null Scans
   - Use unusual combinations of TCP flags to elicit responses from certain OSes.
     - For example, a FIN Scan (-sF):
       - Sends packets with the FIN flag set.
       - A closed port should respond with an RST packet.
       - An open port should not respond.

Port Scanning (continued)

Why Port Scanning Matters?

For Attackers:

- Helps find vulnerabilities (e.g., outdated services, misconfigured servers).
- Identifies which systems might be exploited.

For Defenders:

- Helps assess exposure and harden security.
- Used in penetration testing to simulate attacks and find weak points.

Image Credit

Firewall

Firewall

A firewall in networking is a security system designed to monitor and control incoming and outgoing network traffic based on a set of predefined rules.

*Think of it like a gatekeeper—it decides what traffic is allowed to enter or leave your network based on security criteria.

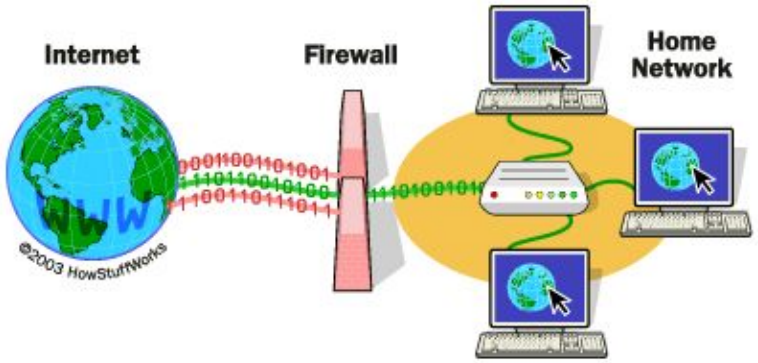

Image Credit
https://www.comodo.com/resources/home/how-firewalls-work.php

KALAMAZOO COLLEGE

Firewall Goals

1. The traffic from inside to outside (and vice versa), must pass through the firewall. This should block all access to the local network except via the firewall.
2. We only allow authorized traffic (defined by our policy) to be allowed to pass through.
3. The firewall itself should be immune to penetration.

<u>Does anyone see a problem with our goals so far? What about any thoughts?</u>

Firewall Techniques

1. Service Control - We determine the types of internet services that can be accessed, either inbound or outbound. We can filter based on specifications like IP address, protocol, or port number.
2. Direction Control - We determine the direction that service requests may be initiated and allowed to flow through our firewall.

Image Credit

Firewall Techniques (continued)

3. User Control - We control who can access a service or requesting access to it.
4. Behavior Control - We control how particular services are being used.
    a. This can filter email to eliminate spam,or enable external access to a portion of the information on a local server.

Firewall Capabilities

1. It should define a single point that attempts to keep unauthorized users out of the protected network, prohibit potentially vulnerable services from entering or leaving the network, and provide protection against IP spoofing/routing attacks

<u>Do we think the use of a single point is better or worse for security?</u>

Firewall Capabilities (continued)

2. It *should* provide us with a location for monitoring security-related events. We can also implement things like audits and alarms within these firewall systems, this helps us track our activity.
3. We can use a firewall for non-security functionality including:
   a. Address Translator - This maps the local addresses to internet addresses
   b. Network Manager - This audits or logs internet uses for an entity

Firewall Limitations

1. It can’t protect against anything that bypasses the firewall.
   a. This should feel straightforward, but I felt like I should mention this.
2. This cannot protect against insider threats, such as angry employees or anyone working with an external, malicious actor.
3. You can improperly secure your local network, and if someone can access this from the outside it cannot be stopped by the firewall.
4. The use of external devices that are connected to the local network may cause infection.

Image Credit

Firewall Types

1. Packet Filtering Firewall (Stateless)
2. Stateful Firewall

*We have many other types of firewalls, but for the purpose of a networking discussion I will cover these two.

Packet Filtering Firewall

A packet filtering firewall applies a set of rules to each incoming and outgoing IP packet and then forwards/discards the packet. The packet information can be filtered based on:

1. Source IP Address: This is the IP address of where a packet is **coming from**
2. Destination IP Address: This is the IP address of where the packet **wants to go**
3. Port Number: The TCP/UDP port number requested
4. Protocol Field: This is the transport protocol that it being used
5. Interface: The interface that it is headed towards.

Image Credit

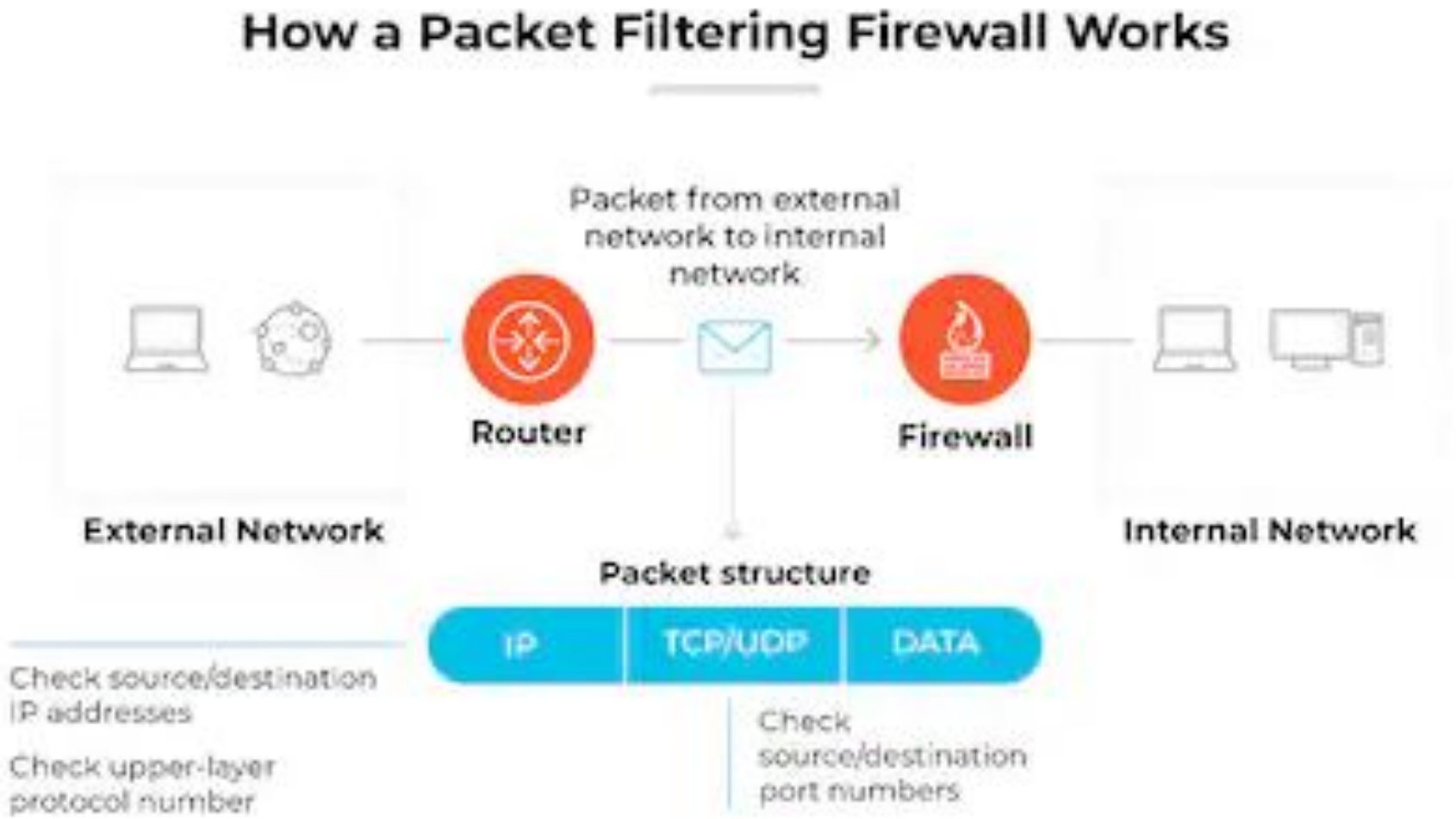

Image Credit
https://www.paloaltonetworks.com/cyberpedia/what-is-a-packet-filtering-firewall

KALAMAZOO COLLEGE

We are going to assume a * matches everything

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we dont't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

Image Credit

Packet Filtering Firewall (continued)

We can choose to set a default action to be taken for our firewall, we can choose two possible policies:

1. Default = discard: We discard anything that is not clearly permitted
2. Default = forward: We allow anything that is not clearly prohibited.

<u>Which policy would you use for your system? What are the pros/cons?</u>

Packet Filtering Firewall Advantages

1. This is a pretty straightforward, simple firewall to implement.
2. These are typically very transparent with your users, they will know what they can/can't do.
3. This is typically pretty fast.

Packet Filtering Firewall Disadvantages

1. These only focus on packets, so attacks that target other layers (like the application layer of our OSI model) will not be blocked.
2. We can't really gather too much information besides the information on a packet (source, destination, protocol, etc.) for our logs.
3. We can have breaches due to improper configuration, such as accidentally configuring a packet filter to allow a dangerous type through.

Image Credit

Stateful Firewall

A stateful firewall is a type of firewall that monitors and controls the state of active connections.

It maintains a table that records information about the connection (e.g., source/destination IP, port numbers, protocol), enabling a more informed decisions about if incoming packets should be allowed or denied based on their relationship to active sessions.

Image Credit

Stateful Firewall (continued)

Stateful firewalls maintain a state table (also called a connection table) that tracks the status of active connections.

- When a packet enters the firewall, the firewall checks this state table to determine whether the packet is part of an existing, valid connection or if it's a new, untrusted packet.

*Unlike a stateless firewall, which treats each packet of data in isolation, a stateful firewall keeps track of the state of ongoing connections.

Image Credit

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

Image Credit

Stateful Firewall Function

1. When an internal device initiates a connection to an external device, the firewall records the connection details (e.g., IP address, port, and sequence number) in the state table.
2. Then, for ongoing communication (like a response from the website), the firewall allows the incoming traffic if it matches an entry in the state table, ensuring that it belongs to an already-established, valid connection.
3. It then checks if incoming traffic doesn't match an existing connection in the table, the stateful firewall blocks it. This helps prevent unauthorized or malicious inbound connections.

Image Credit

Stateful Firewall Advantages

1. The stateful firewalls provide a higher level of security than stateless firewalls by tracking the context of network traffic.
    a. This means they can better identify and block unwanted or malicious traffic, especially when it comes to incoming unsolicited packets.
2. Since the firewall knows the state of the connection (whether it's new, ongoing, or closed), it can make context-aware decisions about which traffic should be allowed.

Stateful Firewall Advantages

3. These stateful firewalls are more efficient than firewalls that perform *deep* packet inspection (DPI), which looks into the data payload of packets.
    a. Stateful inspection focuses on headers and connection states, making it less resource-intensive.
4. The stateful firewalls manage and track multiple connections at once, allowing for more efficient handling of complex network traffic.
5. These can help block certain types of attacks that are based on exploiting the lack of stateful inspection (such as SYN floods and spoofing attacks).

Image Credit

Stateful Firewall Disadvantages

1. The maintaining of state tables and tracking the status of all active connections can consume memory and processing power, especially when dealing with a large number of connections.
2. The firewalls focus on inspecting packet headers and do not perform deep inspection of the data payload.
    a. This is the opposite of the advantage, it makes them less effective at detecting certain types of malware or application-layer attacks.
3. As the number of active connections grows, the state table can become very large, making it harder to maintain. This can lead to performance degradation or cause the firewall to fail under heavy traffic conditions.
    a. This should look similar to one of our advantages, but if it gets too large this where it can cause issues.

Stateful Firewall Disadvantages

4. The stateful firewalls rely on the establishment of a valid session or connection before traffic is allowed through.
    a. This means that they might not be ideal for certain scenarios, like stateless protocols or situations where connections are expected to be short-lived or frequently reset.
5. If an attacker can flood the firewall with a large number of connection requests (e.g., a SYN flood attack), it can exhaust the state table, causing the firewall to crash or become unresponsive.
    a. This can render the firewall ineffective in such scenarios unless other countermeasures are used.
6. The managing of state tables and ensuring proper configuration can become complex, especially in networks with diverse or dynamic traffic patterns.
    a. Misconfigurations can lead to over-blocking (where legitimate traffic is denied) or under-blocking (where malicious traffic is allowed).

Image Credit

Intrusion Detection System (IDS)

Intrusion Detection System (IDS)

Security Intrusion: A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system (or resource) without having authorization to do so.

Intrusion Detection: This is a system that monitors and analyzes system events for the purpose of finding, and providing real-time **or** *near* real-time warning of, attempts to access system resources in an unauthorized manner.

Image Credit

Intrusion Detection System (IDS) (continued)

We can roughly classify two types of IDS systems, these include:

1. Host-Based IDS: This monitors the characteristics of a single host and the events occurring within that host for suspicious activity.
2. Network-Based IDS: This monitors the network traffic for particular network segments or devices and analyzes network, transport, and application protocols to identify suspicious activity

Intrusion Detection System (IDS) (continued)

These should have a few logical components:

1. Sensors - We need to collect some data for this to function. The input can be any part of a system that can gather evidence of an intrusion, including network packets, log files, system call traces. This are then forwarded to an analyzer.
2. Analyzer - These receive input from one or more sensors, or from another analyzer. This then determines if an intrusion has occurred, and the output would show this intrusion or guidance on next steps.
3. User Interface - This enables a user to see the output and control behavior of the system.

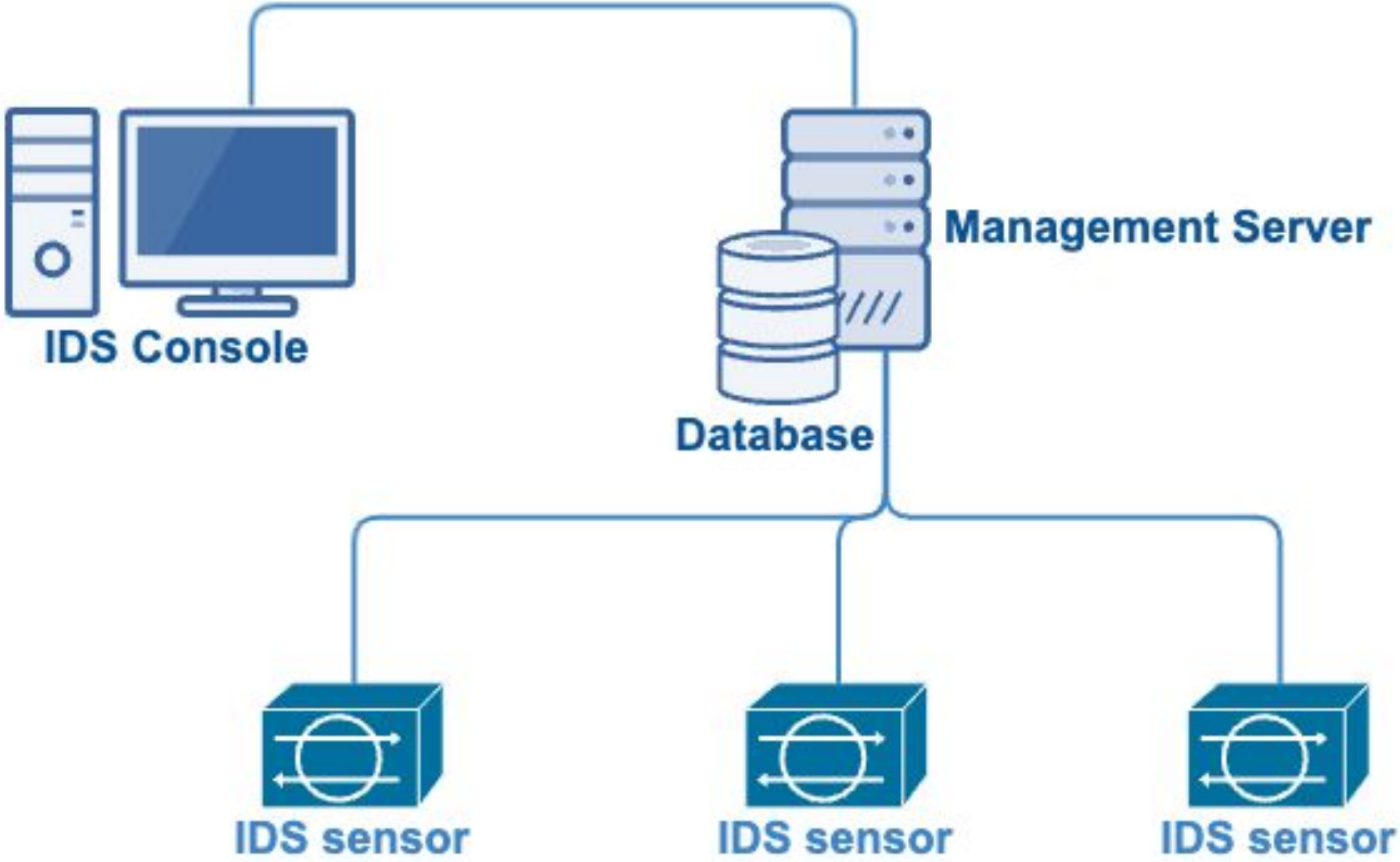

Image Credit
https://lo.unisa.edu.au/mod/glossary/print.php?id=3065178&mode=letter&hook=I&sortkey&sortorder&offset=0&pagelimit=10

KALAMAZOO COLLEGE

Pause: IDS vs Intrusion Prevention System (IPS)

The IDS primarily monitors network traffic and alerts security personnel to suspicious activity, while IPS takes proactive steps to prevent threats, such as blocking malicious traffic.

Would you consider a firewall an IDS, an IPS, or neither?

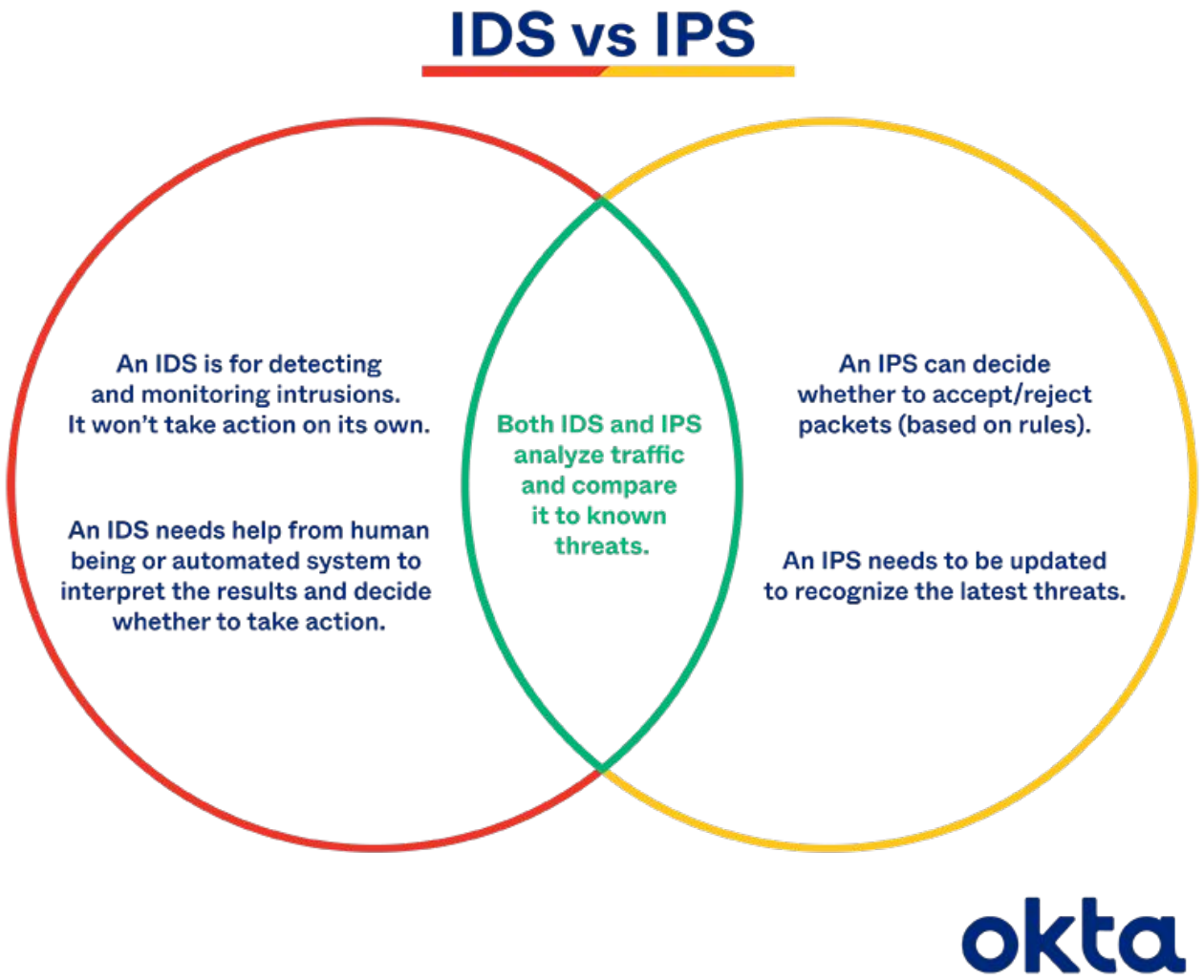

Image Credit
https://www.okta.com/identity-101/ids-vs-ips/

KALAMAZOO COLLEGE

Host-Based IDS

A type of IDS designed to monitor and protect hosts (e.g., computers, servers, and endpoints) within a network. The host-based IDS focuses on the activity that happens **on the host itself,** not the entire network.

Host-Based IDS Approaches

1. Anomaly Detection - The idea is to collect data relating to the behavior of legitimate users, then use a test to decide if it is “normal” or “abnormal”. These can do this using:
   a. Threshold - This involves setting a threshold for how frequently the occurrence of an event can occur.
   b. Profile-Based - You develop a profile of activity for all of your users, and when you detect changes you can monitor them.
2. Signature Detection - This involves defining rules or attack patterns (can leverage a database) to decide if an intruder is attacking.

*Does anyone see a problem with anomaly detection? What about signature detection?

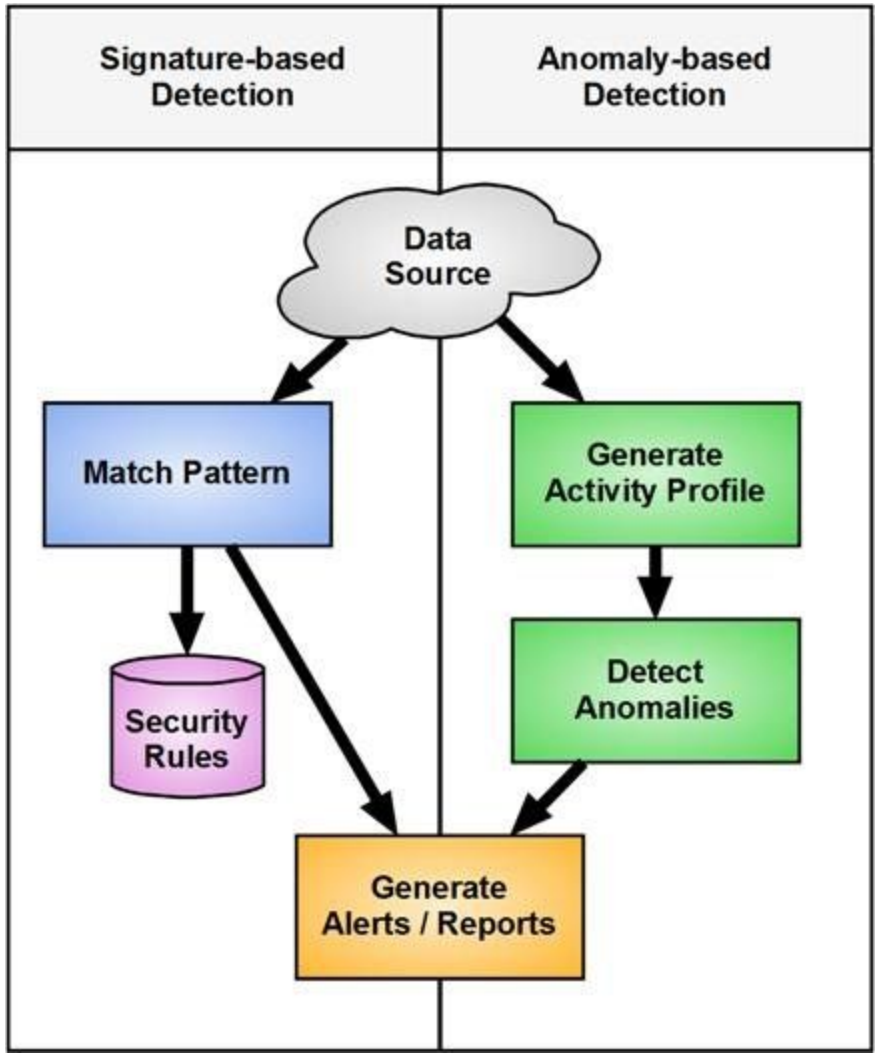

Image Credit
https://www.researchgate.net/figure/SIGNATURE-AND-ANOMALY-BASED-IDS-5_fig1_297171228

KALAMAZOO COLLEGE

Host-Based IDS Advantages

1. These are installed on individual devices, it can offer detailed insights into what's happening on those devices (e.g., file access, system calls, and process execution).
2. It can detect attacks or unauthorized activities that originate from within the organization, such as compromised user accounts or insider threats.
3. This focusing on the device level, and when complemented with a network-based intrusion detection can provide comprehensive coverage.

Image Credit

Host-Based IDS Disadvantages

1. This can be resource-intensive because it continuously monitors system activities, which may impact the performance of the host, especially on devices with limited resources.
2. If an attacker compromises the host, they could potentially disable or tamper with the IDS itself.
    a. In such cases, a network-based IDS or other layers of defense would be needed.
3. It only protects the individual host and may not be able to detect network-wide attacks unless coupled with a network-based system.

Network-Based IDS

A solution that monitors network traffic for signs of malicious activity, unauthorized access, or security policy violations. This examines the entire network or specific segments of a network to detect potential threats, instead of a single host.

Image Credit

Network-Based IDS Approaches

1. Anomaly-Based Detection - This also uses anomaly-based detection, where it establishes a baseline of normal network traffic and behavior. It then flags deviations from this baseline as potentially malicious.
2. Signature-Based Detection - Similar to host-based, this uses signature-based detection where it compares network traffic to a database of known attack patterns or "signatures."

Image Credit

Network-Based IDS Advantages

1. This provides a holistic view of the entire network traffic
   a. This is particularly useful for detecting threats like distributed denial-of-service (DDoS) attacks or lateral movement by attackers across different systems in the network.
2. This offers real-time detection of intrusions and malicious activities, helping security teams to respond quickly to potential threats and mitigate damage before it escalates.
3. This doesn’t directly impact the performance of the devices being monitored because it monitors network traffic from a central point instead of on a system.

Image Credit

Network-Based IDS Advantages (continued)

4. This can monitor multiple systems in one location, which makes it easier for security teams to manage and respond to network-based threats across large infrastructures.
5. This can be scaled easily across larger networks. As new network segments or devices are added, additional sensors can be deployed to maintain comprehensive network monitoring.

Image Credit

Network-Based IDS Disadvantages

1. This can be difficult to detect instructions in encrypted traffic.
    a. The attackers often use encryption to obfuscate their activities, making it more challenging to analyze the content and identify malicious behavior.
2. In large or high-traffic networks, it can become overwhelmed by the sheer volume of network traffic it needs to analyze.
3. It may be effective at monitoring traffic between external networks and internal systems, but it may have blind spots in traffic that happens entirely within an internal network.

Image Credit

Network-Based IDS Disadvantages (continued)

4. This can be susceptible to false positives and false negatives. This requires fine-tuning and constant updating of signatures and anomaly thresholds are required to minimize these issues.
5. This is in the name, it does not directly prevent threats. It acts as a detection tool and alerts security teams, but it relies on additional systems (such as firewalls or intrusion prevention systems) to take action against detected threats.
6. The sensors need to be strategically placed within the network to monitor traffic effectively. If sensors are poorly placed, they might miss critical traffic or fail to cover important network segments.

Image Credit

Virtual Private Network (VPN)

Virtual Private Network (VPN)

A Virtual Private Network (VPN) is a technology that creates a secure, encrypted tunnel between a user's device and a remote server, allowing for private communication over a public or untrusted network—typically the Internet.

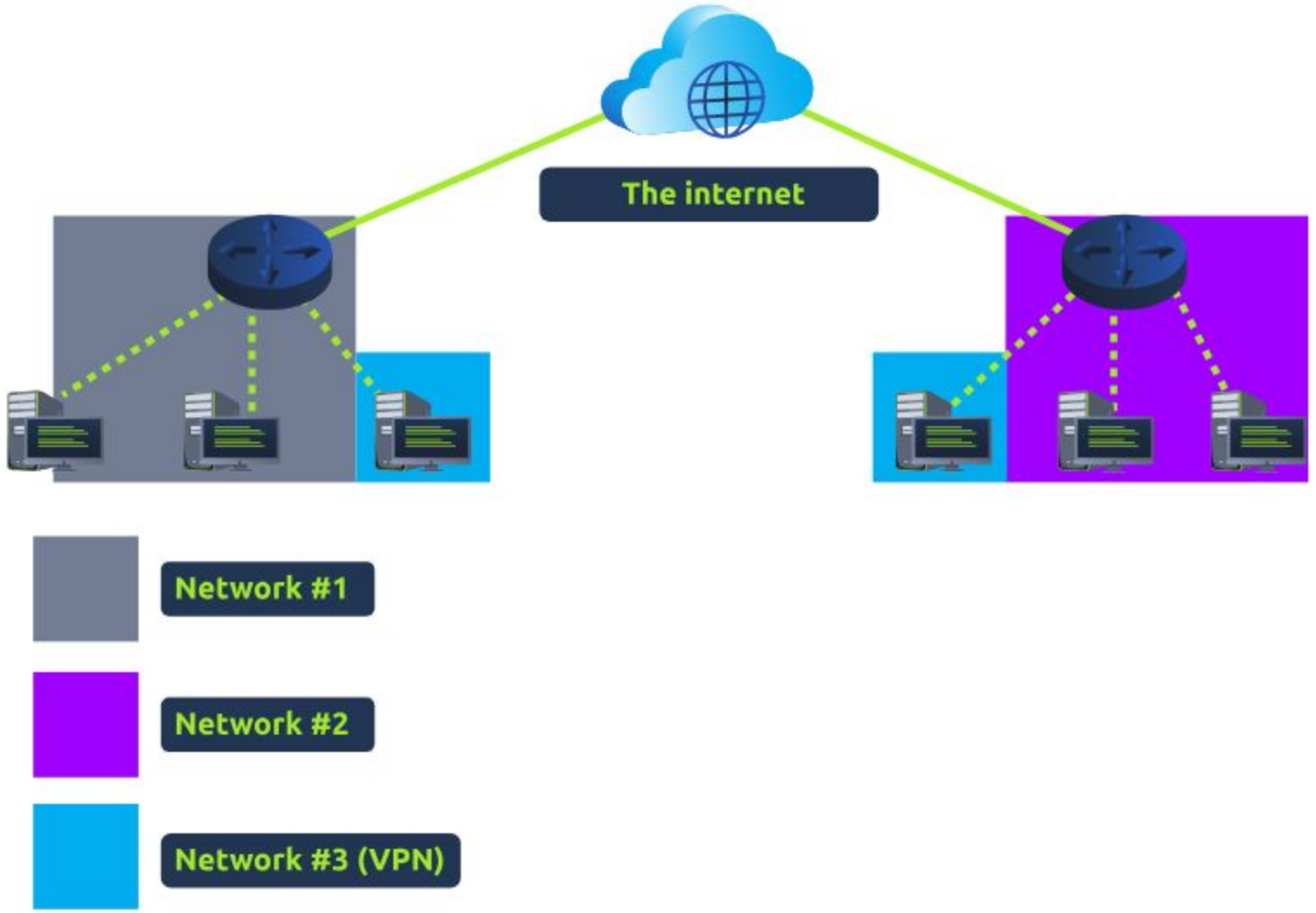

Image Credit
https://tryhackme.com/room/extendingyournetwork

KALAMAZOO COLLEGE

How Virtual Private Network Works

1. VPN Client (on the user's device) initiates a connection to a VPN Server (a computer acting as a secure gateway).
2. Encryption protocols are negotiated—commonly using protocols like IPSec, SSL/TLS, or WireGuard.
    a. The client and server authenticate each other using certificates, pre-shared keys, or usernames/passwords.
3. A secure tunnel is established, all traffic from the client is routed through the VPN server, making it appear as if it originates from the server's IP address.
    a. This can be used to “appear” in other locations!

Image Credit

Image Credit
https://1000logos.net/best-vpn-services/

KALAMAZOO COLLEGE

Virtual Private Network Advantages

1. Employees connect to a corporate LAN from remote locations.
   a. For example, I cannot make any changes to K's web pages unless I am on the network, I do this using a VPN service.
   b. Who has needed to do this for work? Does anyone have a guess as why companies do this?

2. Accessing content blocked in certain countries.
   a. Does anyone know what you can with a VPN and services like Netflix?

3. Masking IP addresses and encrypting data to avoid tracking.
   a. VPNs help defend against man-in-the-middle (MITM) attacks on open networks.

Image Credit

Widows' War (series,2024)
After an accidental death spirals into blackmail, betrayal and murder, two women find themselves pulled into a deadly family conspiracy.

globally new on 2025-04-16
Runtime:--

Twisters (movie,2024)
Thrill-seeking storm chasers and a dutiful meteorologist converge in Oklahoma as a massive tornado outbreak tears towns apart and threatens their lives.

globally new on 2025-04-16
Runtime:**2h2m20s**

Image Credit
https://unogs.com/

KALAMAZOO COLLEGE

Virtual Private Network Disadvantages

1. The VPN provider can see user traffic and **must be trusted.**
2. Potential for VPN leaks (DNS leaks, IP leaks) if not properly configured.
3. Some organizations and countries use deep packet inspection (DPI) to block VPN traffic.

Image Credit

Continue Activity/TryHackMe/Ideas

You can use the rest of the time to continue working on your Keylogger and Buffer Overflow. I have posted a few resources on the website.

OR

You can learn more about networks using the TryHackMe resources

OR

You can work on your presentation ideas or project ideas

Questions?