CSC 215: Network Security & Management, Network Monitoring and Management Tools

Lecture Objectives

- Understand network security fundamentals
  - Explain network management concepts
  - Identify monitoring protocols and tools
  - Apply security concepts using lab exercises
  - Relate concepts to Nigerian environments

What is a Computer Network?

- A computer network is a group of two or more computers and electronic devices that are connected to share data, resources, and services using communication links and agreed-upon rules called protocols.
- A computer network is a collection of interconnected computers and devices that communicate and share data and resources using communication media and protocols.

Types of Computer Networks

- LAN (Local Area Network) – School, office, laboratory
- MAN (Metropolitan Area Network) – City-wide network
- WAN (Wide Area Network) – Internet, bank branch networks

Meaning of Network Security

- Network Security refers to the collection of policies, technologies, hardware devices, software applications, and operational practices used to protect computer networks and the data transmitted across them from unauthorized access, misuse, modification, damage, or disruption.

- Network security is the protection of network infrastructure and data from unauthorized access, attacks, and damage, while ensuring confidentiality, integrity, and availability of information.

- Its main purpose is to ensure that network resources remain safe, reliable, and available to legitimate users while preventing cyber threats and attacks.

1. Protection of Network Infrastructure and Data

- Network security protects both:

Network Infrastructure

- These include:
- Routers
- Switches
- Servers
- Firewalls
- Wireless access points
- Cables and communication links
- Protection ensures that attackers cannot tamper with network devices, change configurations, or disrupt connectivity.

Data

- Data includes:
- Student records
- Bank transactions
- Emails and documents
- Research data
- Cloud files
- Security mechanisms such as encryption, access control, and backups protect data from being stolen, altered, or destroyed.

Example:

A university network encrypts student results stored on servers to prevent unauthorized viewing or tampering.

2. Prevention of Unauthorized Access and Attacks

- Network security prevents illegal users, hackers, malware, and insiders from gaining access to systems or launching attacks.
- This is achieved using:
- Firewalls – block unwanted traffic
- Authentication systems – verify user identity
- Intrusion Detection and Prevention Systems (IDS/IPS) – detect and block attacks
- Antivirus and anti-malware software
- Network segmentation and access policies

- **Common attacks prevented include:**
- Hacking and password attacks
- Phishing
- Malware infections
- Denial-of-Service attacks
- Data interception

Example:
A bank blocks unknown IP addresses trying to access its internal network

3. Ensuring Confidentiality, Integrity, and Availability (CIA Triad)

- Network security is built around three major goals:

Confidentiality

- Ensures that sensitive information is accessed only by authorized users.
- Achieved using passwords, encryption, and access control.
- Prevents data leakage and spying.

Integrity

- Ensures that data remains accurate and unaltered.
- Achieved using hashing, checksums, digital signatures, and audit logs.
- Prevents unauthorized modification of data.

Availability

- Ensures that systems and services remain accessible when needed.
- Achieved using backups, redundancy, load balancing, and disaster recovery.
- Prevents downtime and service interruption.

Example:

Online course registration must be confidential, accurate, and always available during registration periods.

- Bank ATM encryption (Confidentiality)
  - Student result database integrity
  - Internet Service Provider (ISP) uptime for internet availability

An Internet Service Provider is a company or organization that provides individuals, schools, businesses, and governments with access to the Internet.

Common Network Threats

- A network threat is any activity, event, or weakness that can harm a computer network, compromise data, disrupt services, or allow unauthorized access. These threats can originate from hackers, malicious software, careless users, or system weaknesses.

- Understanding common network threats helps network administrators design effective security controls and respond quickly to incidents.

1. Malware

- **Malware** means malicious software designed to damage, disrupt, steal data, or gain unauthorized access to systems.
- **Types of malware include:**
- **Viruses** – attach to files and spread when executed
- **Worms** – spread automatically over networks
- **Trojan horses** – disguise as legitimate software
- **Spyware** – secretly collects user information

Example:
A computer at a cyber café infected via a flash drive spreads malware to other systems on the network.

2. Phishing Attacks

- Phishing is a social engineering attack where attackers trick users into revealing sensitive information such as passwords, ATM PINs, or login credentials.
- Phishing is commonly delivered via:
- Emails
- SMS messages
- Fake websites
- Social media links

Example:
A student receives a fake portal email requesting login details and unknowingly submits their password.

Security Technologies

Security technologies are tools, systems, and techniques used to protect computer networks, devices, and data from unauthorized access, attacks, and other threats. They form the backbone of network security and cybersecurity defenses, ensuring the confidentiality, integrity, and availability of information. Key security technologies include:

1. Firewalls

A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Firewalls act as a barrier between a trusted internal network and untrusted external networks, such as the Internet.

Types of Firewalls:

- **Packet-filtering firewalls:** Inspect packets of data and allow or block them based on source/destination IP addresses, ports, or protocols.
- **Stateful inspection firewalls:** Track the state of active connections and make decisions based on the context of traffic.
- **Proxy firewalls:** Intercept and analyze requests between the user and the Internet, hiding the internal network.
- **Next-Generation Firewalls (NGFW):** Combine traditional firewall functions with advanced features like intrusion prevention, deep packet inspection, and application-level control.

Intrusion Detection and Prevention (IDS/IPS)

- Intrusion Detection and Prevention Systems are crucial security technologies designed to monitor network or system activities for malicious actions or policy violations. They are part of a layered security strategy that helps organizations detect, prevent, and respond to cyber threats.

1. IDS (Intrusion Detection System)

An IDS monitors network traffic or system activity to detect attacks or suspicious behavior. It does not block traffic but instead alerts administrators so they can respond manually.

Key Features:

- Monitors incoming and outgoing traffic.
- Analyzes traffic for known attack patterns or unusual behavior.
- Sends alerts via email, dashboards, or system logs.

Types of IDS:

- **Network-based IDS (NIDS):** Monitors network traffic across multiple devices.
- **Host-based IDS (HIDS):** Installed on individual systems to monitor file changes, logs, and system activity.

Example (Nigeria):

- A Nigerian bank's IT team may deploy IDS on its internal network to detect unauthorized login attempts, like repeated failed ATM login attempts or unusual access to customer data.

2. IPS (Intrusion Prevention System)

- An IPS performs the same monitoring functions as IDS but also actively blocks malicious traffic in real-time, preventing attacks from reaching their target.

Key Features:

- Real-time threat prevention.
- Blocks IP addresses or specific traffic patterns.
- Can automatically isolate affected devices or terminate malicious connections.

Example (Nigeria):

- A Nigerian e-commerce website could use IPS to block SQL injection attacks or brute-force login attempts, preventing hackers from accessing customer accounts.

3. Detection Methods

- IDS/IPS systems detect attacks using two main approaches:

a. Signature-based Detection

- Compares network activity against a database of known attack patterns (signatures).
- **Pros:** Accurate for known threats, low false positives.
- **Cons:** Cannot detect new, unknown attacks (zero-day threats).

Example:

- Detecting a known ransomware variant targeting Nigerian financial institutions.

b. Anomaly-based Detection

- Monitors for deviations from normal system or network behavior.

Pros: Can detect unknown or zero-day attacks.

Cons: Higher chance of false positives; requires learning normal behavior patterns.

Example:

- Detecting an unusual spike in traffic to a government portal in Abuja, which could indicate a DDoS attack.

What is Network Management?

Network Management refers to the set of processes, tools, and techniques used to administer, monitor, and maintain a computer network to ensure it operates efficiently, securely, and reliably. Organizations need to keep their networks stable, performant, and scalable as demands grow.

1. Administration of Network Resources

Network management involves allocating, configuring, and maintaining network resources, such as:

- **Devices:** routers, switches, firewalls, servers.
- **Bandwidth:** ensuring fair and efficient use of available network capacity.
- **IP addresses and subnets:** assigning and managing addresses to avoid conflicts.
- **User access:** controlling who can access which parts of the network.

Example (Nigeria):

- A Nigerian university IT department may assign different bandwidth limits for staff and students to ensure smooth access to online lecture materials.

2. Ensures Reliability and Performance

- Network management ensures that the network is always available and performs optimally. This includes:
- **Monitoring uptime and availability:** detecting downtime before it impacts users.
- **Performance tracking:** measuring latency, throughput, and packet loss.
- **Load balancing:** distributing traffic efficiently to prevent congestion.

Example (Nigeria):

- Nigerian banks like Zenith Bank continuously monitor their network to prevent downtime for online banking services, ensuring that customers can perform transactions at any time.

3. Supports Troubleshooting and Scalability

- Network management tools help identify and resolve network issues quickly, minimizing downtime. They also enable scaling the network to accommodate growth.
- **Troubleshooting:** Detect and fix problems such as network bottlenecks, configuration errors, or security breaches.
- **Scalability:** Add new devices, users, or services without disrupting existing network operations.

Example (Nigeria):

- A Lagos-based tech company expanding its offices can use network management software to seamlessly add new servers and Wi-Fi access points while monitoring the entire network's health.

FCAPS Model

The FCAPS model is a framework used in network management to organize and categorize different management tasks. It ensures that networks are reliable, efficient, and secure. FCAPS stands for Fault, Configuration, Accounting, Performance, and Security management.

1. Fault Management

- Focuses on detecting, isolating, and resolving network problems.
- Ensures minimal downtime by alerting administrators to issues.
- Tools may include monitoring systems that send alarms when a device fails.

Example (Nigeria):

- A telecom company like MTN uses fault management to detect network outages in a city and dispatch technicians quickly.

2. Configuration Management

- Involves setting up and maintaining network devices and services.
- Keeps track of hardware, software, and network settings.
- Enables updates, patches, and changes without disrupting operations.

Example:

- Nigerian banks maintain configuration management to ensure all ATMs and servers run the correct software versions.

3. Accounting (or Administration) Management

- Monitors network resource usage for billing, auditing, or planning.
- Tracks who is using bandwidth, storage, or other network services.

Example:

- Internet service providers (ISPs) in Nigeria monitor data usage per customer for accurate billing.

4. Performance Management

- Measures network performance and ensures it meets expected service levels.
- Key metrics: throughput, latency, error rates, and uptime.
- Helps plan capacity upgrades.

Example:

- Nigerian universities monitor their Wi-Fi networks to ensure students can access e-learning platforms without lag.

5. Security Management

- Ensures the network is protected from unauthorized access or attacks.
- Includes firewalls, IDS/IPS, authentication, and encryption.
- Monitors for policy violations and security breaches.

Example:

- Nigerian banks use security management to protect online banking systems from hackers and fraud

Monitoring Metrics

Monitoring metrics are key measurements used to evaluate the health, performance, and reliability of a network. Tracking these metrics allows administrators to identify issues, optimize performance, and ensure smooth network operations.

1. Bandwidth Usage

- Measures the amount of data transmitted over the network in a given time.
- Helps detect heavy traffic, bottlenecks, or overused links.

Example:

- A university monitors bandwidth usage to ensure students can access e-learning resources without congestion during peak hours.

2. Latency and Jitter

- **Latency:** Time taken for a data packet to travel from source to destination.
- **Jitter:** Variation in packet arrival times, which can affect real-time applications like VoIP.

Example:

- Nigerian telecom providers monitor latency and jitter to ensure smooth video calls for corporate clients.

3. Packet Loss

- Occurs when data packets fail to reach their destination.
- High packet loss can lead to slow network performance and application errors.

Example:

- Monitoring packet loss helps Nigerian banks prevent transaction delays on online banking platforms.

- **4. CPU and Memory Utilization**
- Measures how much processing power and memory network devices (routers, servers, firewalls) are using.
- Prevents overload and ensures devices function efficiently.

Example:

- An ISP monitors router CPU and memory usage to prevent crashes during peak traffic periods.

5. Uptime and Availability

- **Uptime:** Total time the network or device is operational.
- **Availability:** Percentage of time a service is accessible to users.
- High uptime and availability are critical for uninterrupted services.

Example:

- Nigerian banks ensure high uptime for ATMs and online banking to provide continuous service to customers.

Monitoring Protocols

- Monitoring protocols are tools and standards used to collect, analyze, and report network data. They help administrators understand device status, network traffic, and overall performance.

1. SNMP (Simple Network Management Protocol) – Device Monitoring

- SNMP is used to monitor and manage network devices such as routers, switches, servers, and printers.
- Collects data like device status, CPU/memory usage, and interface errors.
- Alerts administrators to faults or unusual behavior.

Example (Nigeria):

- A Nigerian ISP uses SNMP to monitor routers across Lagos to detect and fix connectivity issues quickly.

2. Syslog – Log Collection

- Syslog is a protocol for collecting and storing log messages from network devices and servers.
- Provides a centralized way to track system events, errors, and security incidents.

Example:

- Nigerian banks aggregate logs from ATMs and servers using Syslog to investigate failed transactions or security breaches.

3. NetFlow / sFlow – Traffic Analysis

- These protocols analyze network traffic patterns and flow data between devices.
- Helps identify bandwidth usage, top talkers, unusual traffic spikes, or potential attacks.

Example:

- Nigerian universities use NetFlow to monitor traffic spikes on campus Wi-Fi during online exams.

4. Telemetry – Real-Time Streaming

- Telemetry collects real-time, high-frequency data streams from network devices.
- Provides instant insight into network health and performance, enabling proactive action.

Example:

- Nigerian telecom providers use telemetry to continuously monitor 4G/5G network performance across cities for service optimization.

Network Monitoring Tools

- Network monitoring tools are software solutions that help administrators observe, analyze, and manage network performance, availability, and security. They provide real-time insights, alerts, and reporting for proactive network management.

1. Zabbix

- Open-source monitoring tool for networks, servers, and applications.
- Offers real-time monitoring, alerting, and dashboards.
- Supports SNMP, IPMI, and agent-based monitoring.

Example (Nigeria):

- Nigerian universities can use Zabbix to monitor campus Wi-Fi networks and server health.

2. Nagios

- Popular open-source tool for network and infrastructure monitoring.
- Monitors devices, services, and applications, providing alerts for failures and performance issues.
- Highly extensible through plugins.

Example:

- Nigerian banks use Nagios to monitor ATM networks and internal servers for uptime and faults.

Network Monitoring Tools

3. Wireshark

- A **network protocol analyzer** used to capture and inspect network traffic in detail.
- Helps troubleshoot network problems and detect security threats.

Example:

- IT teams in Lagos may use Wireshark to analyze unusual traffic on office networks, identifying potential attacks or misconfigurations.

4. SolarWinds

- Commercial network monitoring suite for large-scale network and IT infrastructure management.
- Provides dashboards, alerts, automated network discovery, and performance reporting.

Example:

- Telecom companies in Nigeria use SolarWinds to monitor nationwide network performance and prevent outages.

Network Monitoring Tools Cont…

5. PRTG (Paessler Router Traffic Grapher)

- Comprehensive network monitoring tool for bandwidth, devices, and applications.
- Uses SNMP, NetFlow, sFlow, and packet sniffing to monitor traffic and device health.
- Offers customizable dashboards and real-time alerts.

Example:

- Nigerian internet service providers monitor bandwidth usage in different regions to optimize performance using PRTG.

Security Monitoring Tools

- Security monitoring tools help organizations detect, analyze, and respond to security threats in real time. They provide visibility into attacks, policy violations, and vulnerabilities across networks, systems, and applications.

1. SIEM Platforms (Security Information and Event Management)

- Collects and correlates logs and events from multiple sources (servers, firewalls, applications).
- Provides real-time alerts, dashboards, and reports for security incidents.
- Enables threat detection and compliance reporting.

Example (Nigeria):

- Banks and telecom companies in Nigeria use SIEM platforms to monitor suspicious activities like unauthorized fund transfers or network intrusions

Security Monitoring Tools Cont…

2. IDS / IPS (Intrusion Detection / Prevention Systems)

- **IDS:** Monitors network traffic and alerts administrators to potential attacks.
- **IPS:** Goes further to block malicious traffic automatically.

Example:

- Nigerian e-commerce platforms use IDS/IPS to detect and prevent DDoS attacks or brute-force login attempts.

3. Log Analyzers

- Tools that collect, parse, and analyze logs from servers, applications, and devices.
- Helps identify unusual activity, troubleshoot issues, and maintain security compliance.

Example:

- Nigerian banks analyze server logs to investigate failed ATM transactions or unauthorized access attempts.

Security Monitoring Tools Cont…

24. Network Traffic Analyzers

- Tools that capture and inspect network traffic to detect anomalies, bottlenecks, or malicious activity.
- Helps in threat detection, troubleshooting, and network optimization.

Example:

- Nigerian ISPs use traffic analyzers to detect unusual spikes that may indicate malware infections or attempted intrusions.

Emerging Trends in Network Security Monitoring

- As networks grow more complex, modern security and monitoring strategies are evolving. These emerging trends help organizations detect threats faster, manage resources efficiently, and secure new technologies.

1. Artificial Intelligence (AI) Monitoring

- Uses AI and machine learning to analyze network traffic, detect anomalies, and predict potential threats automatically.
- Can identify zero-day attacks and unusual user behavior without manual intervention.

Example (Nigeria):

- Nigerian banks can use AI monitoring to detect unusual login patterns that may indicate fraud.

2. Cloud-Based Network Management

- Moves network monitoring and management to the cloud, allowing remote access, scalability, and centralized control.
- Reduces the need for on-premises hardware and provides real-time analytics.

Example:

- Nigerian universities can manage campus networks across multiple sites using cloud-based platforms like Cisco Meraki.

Emerging Trends in Network Security Monitoring Cont…

3. Zero Trust Architecture

- A security model where no user or device is automatically trusted, even inside the network.
- Continuous verification of identity and access is required for every device, user, and application.

Example:

- Nigerian fintech companies implement Zero Trust to ensure employees and third-party vendors only access systems they are authorized to use.

4. IoT Security Monitoring

- Focuses on monitoring and securing Internet of Things (IoT) devices like sensors, cameras, and smart devices.
- Detects vulnerabilities, unauthorized access, or device misbehavior in real time.

Example:

- Nigerian smart city projects use IoT security monitoring to protect traffic cameras and smart streetlights from cyberattacks.