Ans) Q.1. a) Investigating Unusual Network Traffic Patterns

To investigate unusual traffic patterns on a newspaper's network during non-business hours, the following steps can be taken:

1. **Initial Assessment**:
   - **Log Analysis**: Review network logs to identify specific anomalies such as unusual IP addresses, abnormal data transfer volumes, or unexpected access times.
   - **Traffic Monitoring**: Use network monitoring tools (e.g., Wireshark or SolarWinds) to capture and analyze real-time traffic data.
2. **Data Collection**:
   - **Capture Network Traffic**: Implement packet capture tools to record traffic for further analysis.
   - **Identify Affected Systems**: Determine which devices are generating unusual traffic and assess their security posture.
3. **Analysis**:
   - **Pattern Recognition**: Analyze captured data for patterns indicative of unauthorized access or malware activity.
   - **Threat Intelligence**: Use threat intelligence feeds to correlate observed behaviors with known attack signatures.
4. **Investigation of Potential Breach**:
   - **Identify Entry Points**: Investigate how an attacker might have gained access (e.g., through weak passwords or unpatched vulnerabilities).
   - **Forensic Examination**: Conduct a forensic analysis of compromised systems to understand the extent of the breach.
5. **Preventive Measures**:
   - **Network Segmentation**: Implement segmentation to limit access to sensitive areas of the network.
   - **Regular Audits and Updates**: Schedule regular security audits and ensure all systems are updated with the latest security patches.
   - **User Training**: Educate employees on recognizing phishing attempts and securing their credentials.

Ans) Q.1. b) Ransomware Attack at AIIMS

The ransomware attack on AIIMS in New Delhi occurred on November 23, 2022, when attackers encrypted critical data across the hospital's IT systems, disrupting services and forcing manual operations for patient management. The attackers reportedly exploited vulnerabilities in the hospital's network, leading to significant operational challenges.

Forensic Process Undertaken

1. **Incident Detection**: The attack was detected when staff experienced issues accessing patient records and other digital services.
2. **Data Collection**: Investigators collected logs from affected servers and network devices to identify the attack vector.
3. **Analysis of Encrypted Data**: Analysts assessed the type of ransomware used and attempted to identify decryption methods.
4. **Restoration Efforts**: Backup systems were evaluated for integrity, and data recovery processes were initiated.

Proactive Steps for Future Prevention

1. **Regular Backups**: Implement a robust backup strategy with regular offsite backups.
2. **Patch Management**: Ensure timely updates of all software and systems to mitigate vulnerabilities.
3. **Endpoint Security Solutions**: Deploy advanced endpoint protection solutions that include behavioral detection capabilities.

Technical Solutions for Cybersecurity Defense

- **Intrusion Detection Systems (IDS):** Utilize IDS to monitor network traffic for suspicious activities.
- **Multi-Factor Authentication (MFA):** Enforce MFA for accessing sensitive systems.
- **Security Information and Event Management (SIEM)**: Implement SIEM solutions for real-time monitoring and incident response.

Ans) Q.2. a) Balance Between User Privacy and Social Media Functionality

Social media platforms like WhatsApp and Facebook face challenges in balancing user privacy with functionality, especially following incidents such as data leaks or misuse of personal information in India.

Navigating Privacy Concerns

1. **Data Protection Policies**: Platforms implement privacy policies that outline how user data is collected, used, and shared.
2. **User Control Features**: Users are provided with settings to manage their privacy preferences, although these can often be complex.

Recent Cases in India

- The Cambridge Analytica scandal raised significant concerns about user data misuse, prompting discussions about stricter regulations.
- The Supreme Court ruling on privacy established it as a fundamental right, influencing how platforms handle user information.

Strategies for Improving User Privacy

1. **Simplified Privacy Settings**: Streamline settings to make them more user-friendly.
2. **Enhanced Transparency Reports**: Regularly publish transparency reports detailing government requests for user data.

Ans) Q.2. b) Digital Signature Standard (DSS)

The Digital Signature Standard (DSS) ensures the authenticity, integrity, and non-repudiation of digital documents through cryptographic mechanisms.

Components of DSS

1. **Key Pair Generation**: Involves creating a private key for signing documents and a public key for verification.
2. **Hash Function Usage**: A hash function generates a fixed-size hash value from the original document.

Mathematical Principles

DSS uses asymmetric cryptography where:

- The signature is generated by encrypting the hash with the private key.
- Verification involves decrypting the signature with the public key and comparing it with a newly computed hash.

Significance in Digital Communication

DSS is crucial in e-commerce, secure communications, and legal agreements, providing a reliable method for verifying identities and ensuring data integrity.

Vulnerabilities and Enhancements

While DSS is robust, it can be vulnerable to key compromise or outdated algorithms:

- Transitioning to stronger hash functions (e.g., SHA-256) can mitigate risks.
- Implementing hardware security modules (HSMs) can enhance key management security.

Ans) Q.3. a) MAC vs HMAC

Concepts of MAC and HMAC

- **MAC (Message Authentication Code)** ensures message integrity by using a secret key combined with the message content.
- **HMAC (Hash-based Message Authentication Code)** enhances MAC by utilizing cryptographic hash functions along with a secret key.

Comparison

Feature	MAC	HMAC
Key Type	Symmetric	Symmetric
Security	Basic	Enhanced due to hashing
Use Cases	Simple integrity checks	Secure communications

Applications

- MAC is commonly used in file integrity checks; HMAC is widely used in secure web communications (e.g., HTTPS).

Ans) Q.3. b) Role-Based Access Control (RBAC)

Definition of RBAC

Role-Based Access Control (RBAC) regulates access based on user roles within an organization, ensuring that users have permissions aligned with their job responsibilities.

Principles of RBAC

1. **Role Assignment**: Users are assigned roles that dictate their access levels.
2. **Least Privilege Principle**: Users receive only necessary permissions to perform their tasks.

Benefits in Software Companies

- Enhances security by limiting access to sensitive information.
- Streamlines user management by automating role assignments.

Q.4. a. Evil Twin Attack at NFSU

An Evil Twin attack targets Wi-Fi networks by creating a rogue access point that mimics a legitimate one:

1. **Setup Rogue AP**: An attacker sets up an access point with an SSID similar to NFSU’s legitimate Wi-Fi networks.
2. **Deauthentication Attack**: Users are disconnected from the legitimate network using deauthentication frames, prompting them to connect to the rogue AP unknowingly.
3. **Data Interception**: Once connected, all traffic can be monitored and intercepted by the attacker.

Q.4. b. Mitigating Online Banking Fraud

To combat online banking fraud:

1. **Phishing Prevention Strategies**:
    - Implement advanced email filtering solutions.
    - Educate customers about recognizing phishing attempts.
2. **Malware Mitigation Techniques**:
    - Deploy endpoint protection solutions with behavior-based detection capabilities.
    - Regularly update software applications to patch vulnerabilities.
3. **Collaboration with Law Enforcement Agencies**:
    - Establish protocols for reporting fraud incidents promptly.
    - Engage in joint task forces focused on cybercrime prevention.

By implementing these strategies, banking institutions can significantly enhance their security posture against online fraud threats while protecting customers' sensitive financial information effectively.