Question 1

1. **Inventory of Network Devices**:
   - Firstly, I gathered a list of all devices on the network based on my Nmap and Nessus scan results from Reports 1 and 3, respectively. I documented each device's IP address, hostname, MAC address, operating system, and open ports.
   - I analyzed the Nessus scan results to identify the vulnerabilities associated with each device. These vulnerabilities were then used to assess the criticality of each device, considering both the severity of the vulnerabilities and the role of the device at [REDACTED].
2. **Prioritization of Network Assets**:
   - I categorized the network devices based on their roles and functions at [REDACTED]. Devices essential for business continuity, such as routers, servers, and high-function workstations, were prioritized.
   - I applied a risk-based approach to determine which devices are vital and critical, considering factors like the severity of vulnerabilities, the device's role, and the impact on the organization if the device was compromised or unavailable.
3. **Identification of Critical Servers for Backup**:
   - I reviewed the scan results to identify servers and systems that require regular backups. Critical servers, particularly those hosting vital data or services, were identified for priority recovery and backup.
   - I considered the potential impact of data loss and system downtime to prioritize servers that must be recovered first in a disaster recovery scenario.
   - **Vulnerability Analysis for Updates**:
   - I used the Nessus vulnerability scan results to identify devices with known vulnerabilities that require immediate updates. This included analyzing the CVSS scores, exploit maturity, and risk factors associated with each vulnerability.
   - Devices with high and medium severity vulnerabilities were flagged for updates, focusing on those with high CVSS scores and recent threats.
4. **Password Management and Backup**:
   - I identified roles associated with devices that require secure password management, such as routers, servers, and key workstations.
   - I cross-referenced the devices identified in previous reports with those that require password protection and maintenance, especially those with critical access or administrative roles.

Question 2

1. **Prioritized List of Components for Recovery**:
    - **Critical Devices**:
        - **Router [REDACTED]**Critical for network connectivity.
        - **iMac [REDACTED]:** Important for domain services (Kerberos-sec), requires quick recovery. Also, this iMac is critical due to this iMac being owned and operated by [REDACTED], the agency's owner and primary agent. Highly sensitive information is stored on this machine.
        - **iMac-2 [REDACTED] & [REDACTED] iMac [REDACTED]:** These systems have no open ports but are essential for specific organizational tasks as they are used by [REDACTED]. Sensitive information is stored on both machines.
        - **iMac-3 [REDACTED]:** Contains a high-severity vulnerability and must be updated and recovered immediately. This iMac is the one operated by [REDACTED], who is *not* a crop insurance agent, so sensitive client information is not as prevalent on this machine compared to the other three. Regardless, this device is still critical for recovery.
    - **Vital Device**:
        - **Xerox Printer [REDACTED]:** Important for daily operations but not as critical as network devices.
2. **Backups to be Prepared and Maintained**:
    - **Servers**:
        - **Router [REDACTED]:** Configuration backup.
        - **iMac-3 [REDACTED]:** Full system backup due to high-severity vulnerability.
        - **iMac [REDACTED]:** Backup of domain-related services and critical data.
    - **Passwords**:
        - **Router [REDACTED]:** Admin password.
        - **iMac [REDACTED]:** Service accounts, system admin password, and user credentials.
        - **iMac-2 [REDACTED]:** Service accounts, system admin password, and user credentials.
        - **iMac-3 [REDACTED]:** Service accounts, system admin password, and user credentials.
        - **[REDACTED] iMac [REDACTED]:** Service accounts, system admin password, and user credentials.
3. **List of Devices that Need to be Updated**:
    - **iMac-3 [REDACTED]:** Update macOS to version 14.6 or later.
    - **Router [REDACTED]:** Address medium-severity vulnerabilities related to SSL certificates, IP forwarding, and outdated protocols.
    - **iMac [REDACTED]:** Review and update any outdated software and configurations.
4. **Inventory of Network Devices**:
    - **Router**: [REDACTED] (OpenWrt 21.02)

- **Xerox Printer**: [REDACTED] (Various Linux versions)
- **iMac**: [REDACTED] (Darwin/macOS 11-13)
- **iMac-2**: [REDACTED] (Mac OS X 10.4)
- **iMac-3**: [REDACTED] (macOS 14.5)
- **[REDACTED] iMac**: [REDACTED] (Mac OS X 10.4)

Question 3

1. **Key Takeaways**:
    - **Prioritization of Recovery**: Critical devices, especially those that facilitate network connectivity and essential services, must be prioritized for recovery in the event of an attack or failure.
    - **Vulnerability Management**: Regularly updating devices and addressing vulnerabilities is crucial to maintaining a secure network environment.
    - **Backup Strategy**: A robust backup strategy, including the backup of configuration files, system states, and critical data, is essential to ensure business continuity.
2. **Ransomware Insights**:
    - Ransomware attacks can severely impact an organization by encrypting vital data and systems. Being prepared with a prioritized recovery plan and up-to-date backups can significantly reduce downtime and data loss.
    - Understanding an organization's network topology and critical assets is crucial in designing an effective response and recovery strategy for ransomware attacks.
3. **Value to [REDACTED]**:
    - At [REDACTED], client data integrity is paramount. Understanding how to classify devices based on their roles helps in disaster recovery planning and ensures that the most critical components are secured and recoverable. This knowledge is valuable for preparing the organization to withstand and recover from potential ransomware attacks, ensuring business continuity and compliance with industry regulations.
    - This exercise underscores the importance of a proactive approach to network security, including regular vulnerability scanning, updating critical systems, and maintaining up-to-date backups. All are highly useful to the agency.
    - The insights gained can guide future security practices at the agency, reducing the risk of successful cyberattacks and ensuring a quicker recovery in the event of a breach.