LAB-3

Aim: Implementing disaster recovery and incident response plans for mobile and IoT environments.

Task 1: Create a Basic Disaster Recovery Plan (DRP)

1. Critical Assets

In a mobile and IoT environment, critical assets include:

- **Mobile Devices**: Smartphones and tablets used by employees or consumers.
- **IoT Sensors**: Devices such as smart thermostats, cameras, or medical equipment that transmit data.
- **Cloud Storage**: Data stored in cloud services for backup, synchronization, and sharing.
- **Network Infrastructure**: Routers, switches, firewalls, and other components necessary for maintaining connectivity and data flow.

2. Backup Strategies

- **Local Storage**: Store backups on external hard drives, NAS (Network-Attached Storage), or other local devices to ensure quick recovery.
- **Cloud-Based Backup**: Use services such as Google Drive, AWS, Azure, or others to store encrypted backups off-site. Ensure backups are automated and scheduled for regular intervals (e.g., daily, weekly).
- **Automated Backup Schedule**: Set up a schedule for automatic backups. For mobile and IoT environments, ensure that the backup includes:
  - System configurations.
  - Application settings and data.
  - Logs and historical data from IoT sensors.

3. Recovery Time Objective (RTO) & Recovery Point Objective (RPO)

- **RTO (Recovery Time Objective)**: Define the maximum acceptable downtime for each critical asset. For example:

  - Mobile devices: 4 hours.
  - IoT devices: 12 hours (depending on the device and its critical role).
  - Cloud storage or network infrastructure: 1 hour.

- **RPO (Recovery Point Objective)**: Define the maximum acceptable data loss. For example:
  - Mobile devices: 1 hour.
  - IoT devices: 12 hours.
  - Cloud storage: 30 minutes.

4. Steps to Restore Services After an Attack

- **Identify Affected Systems**: Analyze logs from devices, cloud services, and network monitoring tools to identify the systems or devices affected by the attack.
- **Restore from the Most Recent Clean Backup**: Once affected systems are identified, restore the most recent clean backup that has been verified to be free of malware or corruption.
- **Verify System Integrity Before Reconnecting**: After restoration, check the integrity of the systems to ensure that they are fully functional and secure before reconnecting to the network.

Task 2: Simulate a Security Incident and Recovery Process

1. File Recovery Using Tools

- **Windows (Recuva)**:
  - **Step 1**: Download and install Recuva from the official website.
  - **Step 2**: Launch Recuva and select the type of file you wish to recover (e.g., documents, photos).
  - **Step 3**: Scan the drive where the deleted file was located.
  - **Step 4**: Select the files to restore from the recovery list and choose a safe location for restored files.
- **Linux (extundelete)**:
  - **Step 1**: Install extundelete using the package manager (e.g., sudo apt install extundelete).
  - **Step 2**: Unmount the drive containing the lost file (e.g., umount /dev/sdX).
  - **Step 3**: Run extundelete with the command: sudo extundelete /dev/sdX --restore-file <path-to-file>.
  - **Step 4**: Review the restored file to verify its integrity.

2. Backup Restoration

- **Step 1**: Access your cloud or external backup storage.
- **Step 2**: Select the most recent backup prior to the incident and start the restoration process.
- **Step 3**: Monitor the progress of the restoration.
- **Step 4**: After restoration, verify the data integrity to ensure no corruption or incomplete recovery.

3. Verification

- **Step 1**: Open and inspect the restored data to confirm it is complete and intact.
- **Step 2**: Test any critical applications or IoT devices that use this data to confirm full functionality.
- **Step 3**: Run diagnostics to ensure no remnants of the issue remain.

Task 3: Perform a Tabletop Exercise on Incident Response

Scenario: A mobile device is infected with malware.

1. Identify the Issue

- **Analyze Logs for Suspicious Activity**: Use mobile device management (MDM) software or log aggregation tools to review device logs for abnormal behavior, such as unauthorized app installations or strange network traffic.
- **Check Security Alerts for Malware Indicators**: Review security software alerts, antivirus software logs, or cloud service security logs for known malware signatures.

2. Contain the Attack

- **Disconnect the Affected Device from the Network**: Disconnect the device from Wi-Fi and cellular data to prevent the malware from spreading.
- **Block the Malicious Application or Service**: Use MDM or security tools to isolate or block the malicious application. Disable any services associated with the malware.

3. Recover the System

- **Reinstall the OS or Factory Reset the Device**: Perform a full factory reset to remove any residual malware. Alternatively, reinstall the mobile OS to restore a clean state.
- **Restore Data from a Clean Backup**: After resetting the device, restore data from a previously clean backup, ensuring that it predates the infection.
- **Verify that the Malware Is Completely Removed**: Perform a full device scan with up-to-date antivirus software to ensure that no malware persists after restoration.