

PRACTICAL 15

LAB 4

AIM: Investigating and responding to security incidents on mobile and IoT devices and networks.

1. Initial Detection & Identification:

When you first suspect or detect an incident (e.g., through an alert or user complaint), verify the issue:

- **Example Scenario:** You receive an alert from your Mobile Device Management (MDM) system that an employee's mobile device is showing unusual network activity.

- **Practical Step:** Use your MDM or monitoring tools to check:
 - The device's recent activity (e.g., abnormal data consumption, unauthorized app installation).
 - Whether the device is jailbroken or rooted.
 - Any signs of malware or unauthorized access.

- **Practical Step:** Log into the device's management interface (if accessible) and check:
 - Network logs for unusual traffic or communication with external IPs.
 - The firmware version and ensure it's up-to-date (outdated firmware can be a big security risk).
 - Check for unauthorized devices connected to your IoT network.

2. Containment:

Once you've verified there's a security incident, contain the threat to prevent it from spreading further.

- **For Mobile Devices:**

- If the device is infected, disconnect it from your network immediately (e.g., turn off Wi-Fi and data, or use your MDM to lock the device and remove access to sensitive data).
 - If you suspect a malicious app, forcefully uninstall it using MDM or via device settings.
- **For IoT Devices:**
 - If you detect unusual activity on an IoT device (like a camera or sensor), disconnect the device from your network to prevent it from sending data out or being used for attacks like botnets.
 - Isolate the IoT device from other critical systems on your network to minimize the potential damage.

3. Investigation & Analysis:

Now that the threat is contained, start investigating the cause and scope of the incident.

For Mobile Devices:

- Use mobile forensic tools (e.g., Cellebrite, Oxygen Forensics) to extract logs and data from the device. You want to look for:
 - Evidence of malware or unauthorized apps.
 - Suspicious network connections or data exfiltration.
- Check event logs for any system or app errors that coincide with the suspicious behavior.
- Review installed apps—are there any apps that shouldn't be there or that have excessive permissions?

For IoT Devices:

- Analyze network traffic using tools like Wireshark to identify unusual patterns, like sudden spikes in data or communication with external IP addresses.
- Check device logs for any signs of unauthorized access or misconfigurations.
- If the IoT device is managed by a third-party vendor, reach out to them for help in tracing the issue.

4. Eradication:

After identifying the root cause, eradicate the threat by removing any malicious components.

For Mobile Devices:

- Remove malware: If malware was detected, use mobile security software to clean the device.
- Revert to a known good backup: If the device was severely compromised, restoring to a clean, secure backup may be necessary.
- Update device software to patch any vulnerabilities that may have been exploited.

For IoT Devices:

- Update firmware: Make sure that the device is running the latest, most secure firmware version.
- Reconfigure device settings to ensure it's secure and doesn't have any vulnerabilities (e.g., default passwords).
- If needed, replace the device entirely if the compromise is severe or if the device cannot be properly secured.

5. Recovery:

Once you've removed the threat, focus on bringing systems back online safely.

For Mobile Devices:

- Reconnect the device to your network only after ensuring it's secure and malware-free.
- Monitor the device's behavior closely for any signs of recurrence.
- Make sure the employee is re-educated on device security practices, like avoiding suspicious apps and links.

For IoT Devices:

- Reintroduce the IoT device to the network gradually, ensuring it's properly configured and isolated from sensitive systems.
- Test the device to make sure it's functioning properly and not causing issues on the network.
- Continuously monitor the device to detect any new suspicious activity.

6. Post-Incident Review and Reporting:

After the incident is resolved, it's time to document everything and improve your security posture for the future.

For Mobile Devices:

- Conduct a root cause analysis: What exactly led to the compromise? Was it a user error, outdated software, or a vulnerability?
- Update your mobile security policies: Perhaps introduce stronger access controls, a more aggressive app vetting process, or regular device audits.
- Report the incident: If it involved sensitive data, notify the necessary stakeholders (e.g., affected users, internal teams, and possibly regulatory bodies).

For IoT Devices:

- Review network traffic logs and ensure no other devices are compromised.
- Update IoT security protocols: Consider implementing better segmentation for your IoT devices, stronger device authentication, and stricter firmware update policies.
- Educate teams on best practices for securing IoT devices, such as using secure configurations, avoiding default passwords, and performing regular vulnerability assessments.

7. Preventative Measures:

To reduce the likelihood of future incidents, adopt some proactive security measures:

Mobile Devices:

- Endpoint protection: Ensure that all devices are using security solutions that include antivirus and device encryption.
- Regular software updates: Make sure that all mobile devices are kept up-to-date with the latest security patches.
- Training: Provide training for employees on how to recognize phishing attempts and secure their devices.

IoT Devices:

- Network segmentation: Isolate IoT devices on a separate network to prevent lateral movement if one device is compromised.
- Strong authentication: Use strong passwords and multi-factor authentication for device access wherever possible.
- Regular audits: Schedule periodic reviews of your IoT devices to ensure that they are secure and up-to-date.