**CSC-7303 - 11811 - Network Defense - 202501 – 001**

**Lab 6: Mobile and IoT Security Implementation**

**Name: Unnati Patel – A00327586**

**Submitted to: Prof.  Maryam Ahmed**

**Project Description**

As a cybersecurity SOC analyst, your job is to manage and secure both mobile and IoT devices in an organization. In this lab exercise, you'll implement a mobile device management (MDM) solution, establish robust mobile security, and protect IoT device communications using open-source tools. The lab setup includes Android Lineage CM, different operating systems, and open-source tools for simulation.

**Scenario**

Your organization has a mix of company-owned and employee-owned mobile and IoT devices. Securing these devices is important to avoid unauthorized access, data breaches, and malware. As an SOC analyst, your task is to set up and configure the necessary solutions in your home lab to keep these devices secure and manageable.

1. **Mobile Device Management (MDM) Implementation**

* **Install Miradore Online or ManageEngine**:

Choose your MDM solution: Either Miradore Online or ManageEngine

Installation on Windows Server 2022 or CentOS Stream 9:

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Install the MDM Client**:

* For Miradore Online, download and install the Miradore Client from the Google Play Store on the Android device

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Lost Device Lock**

1. **Demonstrate Device Lock**:
   * Go to the Miradore Online portal and locate the enrolled device.
   * Use the **Remote Lock** feature to lock the device in case it is lost.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A computer screen shot of a computer screen

AI-generated content may be incorrect.

**For CentOS**

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

1. **Mobile Security Setup**

**Enable Web Protection**

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**3. IOT Security Implementation**

A screenshot of a computer

AI-generated content may be incorrect.

* **Implement TLS/SSL for Secure IoT Communication:**

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

1. **Create a Dedicated Network Segment (VLAN/Subnet) for IoT Devices**

**A screenshot of a computer

AI-generated content may be incorrect.**

**Comprehensive Documentation**

1. **Installation Process**
2. **Miradore**

* First, head to the Miradore website and download the latest version.
* After that, run the installer and follow the prompts. It’s pretty straightforward.
* Once it’s installed, you’ll need to link it to your network and create an account.
* Next, you’ll add all the devices you want to manage — like your IoT devices.
* Set your security policies so you can monitor the devices and make sure everything’s secure.

1. **Bitdefender**

* Download the Bitdefender installer from their official website**.**
* Launch the installer and follow the on-screen instructions. Make sure you read and accept the terms.
* You’ll get a few options to choose from during the setup, like enabling automatic updates or running a full scan.
* Once it’s installed, tweak the settings to match your network’s security needs.
* Activate your software with the provided key, and you’re ready.

1. **Bevywise MQTT Broker**

* Go to the Bevywise website or repository and grab the MQTT Broker.
* Install it on your server using the easy setup wizard.
* Once installed, configure it by setting the right port and enabling user authentication to keep things secure.
* Set up any topics or subscriptions needed for your IoT devices.
* Finally, restart the service to make sure all your settings are applied.

1. **OPNsense**

* Download the OPNsense ISO from their official website.
* Burn the ISO to a bootable USB stick or optical disc to get your system ready.
* Boot up and follow the installation wizard to get it up and running on your hardware.
* Boot up and follow the installation wizard to get it up and running on your hardware.
* If needed, set up VPNs or configure routing to further protect your network.

1. **Configuration Process**
2. **Miradore Configuration**

* After installation, log in to the Miradore dashboard**.**
* Configure your device policies to make sure everything’s monitored and secure.
* Set up alerts to notify you if there’s any unusual activity.
* Double-check that your policies are properly enforced, ensuring devices stay secure.

1. **Bitdefender Configuration**

* Activate real-time protection to keep your network safe from threats at all times**.**
* Schedule regular scans and updates to stay on top of any malware that might pop up**.**
* Make sure your firewall is configured to block unauthorized access.
* Set up custom policies for specific devices or services, especially for any IoT-specific threats.

1. **Bevywise MQTT Broker Configuration**

* Ensure that you’re using the right port for communication (typically 1883 for MQTT).
* For added security, enable SSL/TLS encryption to protect data as it moves between devices.
* Set up authentication so only authorized devices can connect to the broker.
* Finally, make sure the broker is configured to handle the expected traffic load, especially if you’ve got a large number of devices.

1. **OPNsense Configuration**

* If you’re working with a lot of IoT devices, setting up VLANs will help separate them from the rest of your network.
* Create firewall rules to control which traffic is allowed to enter or exit the network.
* Enable IDS/IPS (Intrusion Detection/Prevention System) to monitor and stop any suspicious activity.
* If you’re dealing with remote devices, set up a secure VPN to protect any communications.

1. **Testing Process**
2. **Miradore Testing**

* First, check that devices are showing up correctly on the Miradore dashboard, and that their status is being reported properly.
* Test some alerts by simulating device failures or security breaches, like disconnecting a device.
* Make sure that device policies are being enforced as expected, keeping your network safe.

1. **Bitdefender Testing**

* Run a full system scan to see if Bitdefender catches any malware lurking on the network.
* Test the firewall settings by trying to access the network from an unauthorized device or location.
* Run a malware simulation (for testing) to verify that Bitdefender detects and handles the threat properly.

1. **Bevywise MQTT Broker Testing**

* Test the communication between devices and see if everything is working through the MQTT broker.
* Make sure SSL/TLS encryption is working correctly, so data is secure.
* Test the broker’s capacity by simulating multiple devices connecting and sending messages at the same time.
* Ensure the broker is rejecting any unauthorized devices that try to connect.

1. **OPNsense Testing**

* Try connecting unauthorized devices or services to your network to make sure the firewall rules are preventing it.
* Simulate a cyber attack (like a DoS attack) to see if your firewall and IDS/IPS react appropriately.
* If you’ve set up a VPN, test the connection to make sure remote devices can access the network securely.

**Incident Report**

Incident Overview:

During our routine security testing, we noticed some unusual network traffic, which raised suspicions that a malware attack might be happening on one of the IoT devices. Bitdefender flagged the traffic, and Miradore picked up on an unauthorized device trying to access our network.

**Incident Detection:**

* Bitdefender: It flagged a huge spike in network traffic, which seemed odd. When we ran a scan, we found malware on one of the IoT devices.
* Miradore: The system alerted us about an unknown device trying to connect to the MQTT broker, and this device wasn’t authorized.
* OPNsense: Firewall logs showed an external IP scanning our network, trying to exploit vulnerabilities in the IoT devices.

**Mitigation Actions:**

* Isolate the infected device: We immediately quarantined the affected IoT device using Miradore’s remote management tool to stop the malware from spreading.
* Malware removal: Bitdefender detected and removed the malware, and we ran a full scan on all the devices to make sure nothing else was infected.
* Update Firewall Rules: We updated the firewall settings on OPNsense to block the suspicious IP addresses and prevent further attacks.
* MQTT Broker Authentication: We tightened up the MQTT broker authentication settings, ensuring that only trusted devices could connect moving forward.

**Follow-up Actions:**

* We reviewed and updated our IoT network security policies to make sure they were up-to-date.
* We configured Miradore and Bitdefender to give us more detailed alerts and logs, so we can stay ahead of potential threats.
* We scheduled regular vulnerability assessments for the devices to keep things secure.

**Conclusion:**

The attack was detected and handled swiftly, preventing any major damage to the network. We’ve since improved our security measures and made the necessary updates to ensure we're better prepared in the future.