Chapter 18

IoT Hacking

Theory

Ethical Hacking

IoT (Internet of Things)

Internet of Things is the concept of connecting any device to the Internet and to other connected devices, which collect and share data about the way they are designated. The ‘thing’ in IoT could be a person with a heart monitor or an automobile with built-in-sensors, i.e., objects can collect and transfer data over a network without manual assistance or intervention. The technology, i.e., embedded in the objects help them to interact with other devices and sensors.

The information collected by different devices can be used to detect patterns, make recommendations, and detect possible problems before they occur. The data collected by connected devices enable smart decision making based on real-time information, which helps users to save time and money.

The IoT devices are often divided into consumer, enterprise, and infrastructure spaces based on the functions. The examples of IoT devices are

- Smart Thermostat.
- Switch Smart Plug.
- Smart Bulbs.
- Smart Lock.
- Smart Security System.
- SmartThings Hub
- Smart Pet Feeder.
- Smart Health Monitor
- Car Tracking Adapter
- IoT Tracking and Monitoring
- Smart Cement
- Cisco’s Connected Factory

IoT Vulnerabilities

- **Insecure Web Interface**: It can result in data loss, lack of accountability, denial of access and can lead to complete device takeover.
- **Insufficient Authentication/Authorization**: It can result in complete compromise of the device and user accounts.
- **Insecure Network Services**: It can result in the facilitation of attacks on other devices.
- **Lack of Transport Encryption/Integrity Verification:** It can result in data expose, and could open doors to compromise the device or user accounts.
- **Privacy Concerns**: Collecting personal data and storing it without applying any protection can lead to the identity theft.
- **Insecure Cloud Interface**: It could cause a threat to user data which can be used to take control of the device.
- **Insecure Mobile Interface**: It can be easy to discover by simply reviewing the connection to the wireless networks and by using the password reset mechanism to identify valid accounts which can lead to account enumeration.
- **Insufficient security configurability:** It could lead to compromise of the device whether intentional or accidental.

- **Insecure Software/Firmware**: Capturing update files via unencrypted connections, the update file itself is not encrypted, or they can perform their malicious update via DNS hijacking. The attack could come from the local network or the internet.
- **Poor Physical Security**: Using vectors such as USB ports, SD cards or other storage means to access the Operating System and potentially any data stored on the device.

IoT Device Hacking

The objective is to compromise smart devices like automobiles, printers, door locks, washing machines, etc., to gain unauthorized access to network resources and IoT devices. By hacking IoT devices, a hacker can gain following benefits:

- Create a botnet of the compromised IoT devices to launch DDoS attacks.
- Sell compromised data in black markets.
- Carry out malicious activities on compromised IoT devices.
- Install ransomware to block access to an IoT device and demand for ransom.
- Compromised IoT device could be used to steal the identity of a victim and carry out credit card related frauds.
- Compromised smart cameras could be used to snoop on families.

Attacks on IoT devices

- DDoS attack.
- The attack on HVAC systems.
- Rolling code attack.
- Blue borne attack.
- Jamming attack.
- Remote access using the backdoor.
- Remote access using telnet
- Man in the middle attack.

Countermeasures

- Default configurations should be changed during the initial setup.
- Password recovery mechanisms must be robust.
- Ensure that user credentials are properly protected.
- Implement two-factor authentications to guard against unauthorized access.
- Make sure that only the necessary ports are exposed and available.
- Ensure that services are not vulnerable to DoS or buffer overflow attacks.

- Use secure protocols such as SSL and TLS while transiting data over the network.
- Make sure that cloud-based web interface is not susceptible for XSS, SQL Injection or CSRF attacks
- Services should have the ability to separate regular users from users with administrative privileges.
- All smart devices must be updated on a regular base.