What is IoT Pentesting

- What is IoT?
- "The **Internet of things** (**IoT**) describes the network of physical objects "things"—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet." – Wikipedia
- According to surveys, there will be 55.7B IoT devices worldwide by the end of 2025. The huge no. of IoT devices will create a huge network of all the devices like self-driving cars, energy grids, smart appliances. **The massive the network the massive the security risks**. One has to constantly evaluate the IoT security Risks before it's too late.

What is IoT Security?

- IoT security is to protect the connected devices and network from all the security risks. As the technologies evolve, new techniques to break these technologies also evolve. New vulnerabilities are discovered all the time and to protect the network and devices from these vulnerabilities the IoT security is all about.

Previous IoT Security Hacks

- Let’s see some famous IoT security issues happens in the past.

- 1. Nest Thermostat
- In the past Nest, devices are exploited by hackers. There was a Vulnerability in Nest Thermostat in which by holding a button for 10 seconds to reboot the device. At this stage, the device can be made to communicate with USB media, which contains malicious firmware. There are few more vulnerabilities that are discovered in Nest thermostats

2. Philips Smart Home

- Philips smart home also suffered from numerous security issues. The most famous vulnerability in Philips smart home was the ZigBee vulnerability. Philips uses Zigbee to exchange data and authenticate it. so hackers hardcoded the Zigbee packet and gain control over all the connected devices.

3. The Jeep hack

- The Jeep hack is the most popular one. Two security researchers Dr. Charlie Miller and Chris Valasek demonstrated in 2015 how they can remotely control and takeover a jeep using the vulnerability in the Uconnect system. This hack can lead 1.4 million vehicles to be remotely controlled from home. Basically, this was one of the most dangerous vulnerabilities in IoT devices at that time.

- These are some of the past IoT security issues in some famous companies. There are lots of other hacks in past like Lifx Smart Bulb, Belkin Wemo home automation, Insulin Pump, Smart Door Locks, Even Smart Guns and Rifles. All these hacks are happens because of lack of security awareness among developers, lack of macro perespective, Usage of Insecure framework and third-party libraries

IoT Vulnerabilities

- Like OWASP top 10 for web application security there is a OWASP top 10 for IoT.
- 1. OWASP Top 10 IoT
- **Weak, guessable, or hardcoded passwords**
- **Insecure network services**
- **Insecure ecosystem interfaces**
- **Lack of secure update mechanism**
- **Use of insecure or outdated components**
- **Insufficient privacy protection**
- **Insecure data transfer and storage**
- **Lack of device management**
- **Insecure default settings**
- **Lack of physical hardening**

OWASP TOP 10 INTERNET OF THINGS 2018

1 **Weak, Guessable, or Hardcoded Passwords**
Use of easily bruteforced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems.

2 **Insecure Network Services**
Unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control...

3 **Insecure Ecosystem Interfaces**
Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.

4 **Lack of Secure Update Mechanism**
Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.

5 **Use of Insecure or Outdated Components**
Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain.

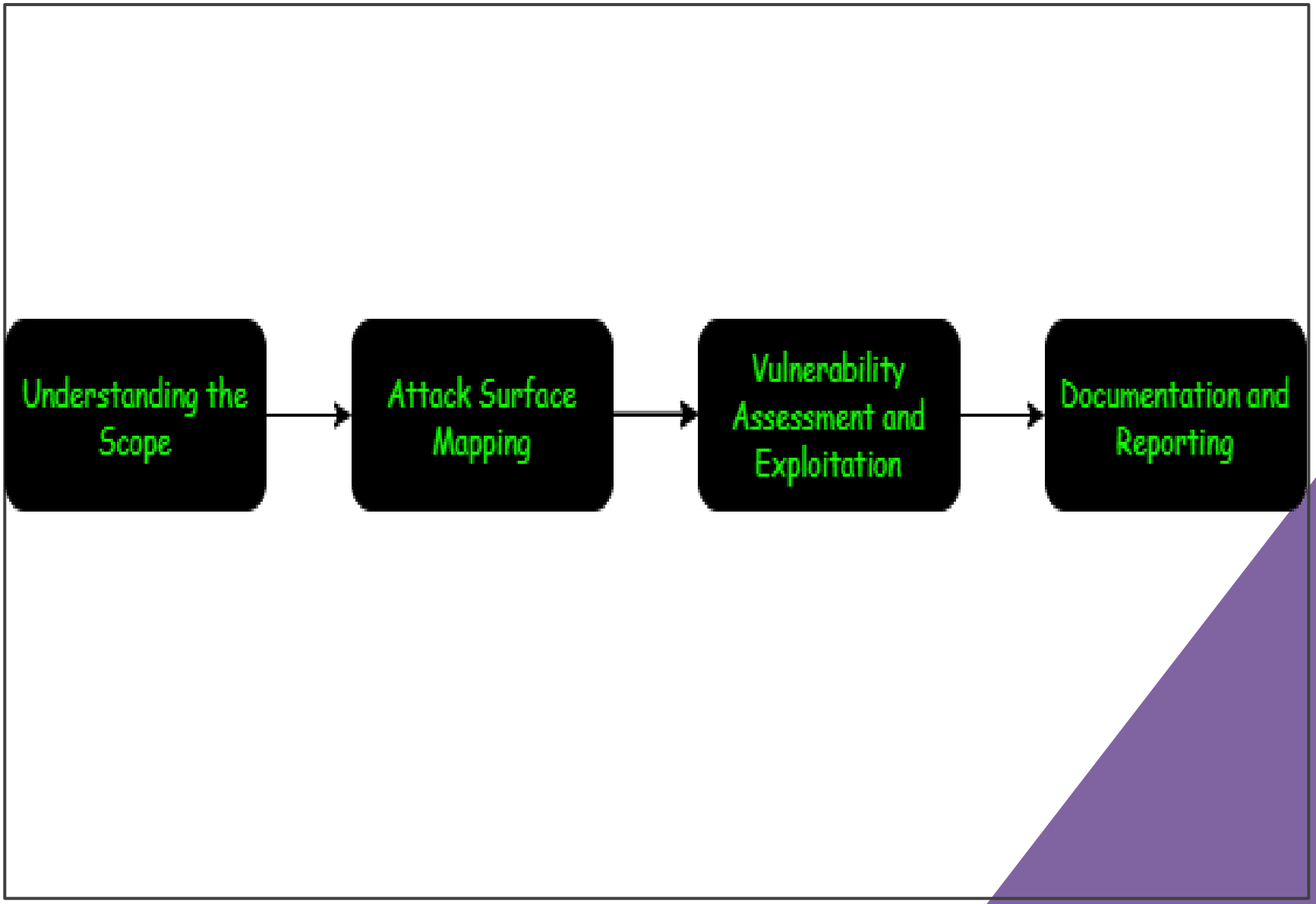
6 **Insufficient Privacy Protection**
User's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.

7 **Insecure Data Transfer and Storage**
Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.

8 **Lack of Device Management**
Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities.

9 **Insecure Default Settings**
Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations.

10 **Lack of Physical Hardening**
Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.


Understanding the Scope
Attack Surface Mapping
Vulnerability Assessment and Exploitation
Documentation and Reporting

IoT Pentesting Methodology

- 1 Understanding Scope

- For any pentest, pentesters need to understand the scope of the target. The scope consists of constraints and limitations. the condition for penetration testing varies from product to product. so in the first step of IoT pentest, the tester needs to understand the scope and make plans accordingly.

IoT Pentesting Methodology

- 2. Attack surface mapping

- In attack surface mapping the tester maps out all the entry points that an attacker could potentially exploit or abuse in an IoT device. The attack surface mapping also involves the creating of a highly detailed architecture diagram highlighting all the possible entry points for an attacker.

There are many ways to do Attack surface mapping. So, let’s discuss the basic role of attack surface mapping

when the tester is creating architecture of the system, the entire architecture can be broadly divided into three categories:

1. **Embedded device**

- Embedded devices can be used for several different purposes according to the situation. It can be a sensor that collects data, smart lightbulbs, switches, smart homes all are examples of embedded devices.
- Some vulnerabilities in Embedded devices are:
- Serial Ports Exposed
- Insecure authentication mechanism
- Ability to dump the firmware over JTAG
- External Media-based attacks

2. Firmware, Software, and Applications

- After the hardware exploitation the next component is software exploitation of IoT device. This includes everything from the firmware in mobile devices to the cloud components
- Some Vulnerabilities related to them are:

1. Firmware

  - Ability to modify
  - Insecure Signatures
  - Private certificates
  - Outdated components with known vulnerabilities

2. Firmware, Software, and Applications

2.Mobile applications

1. Reverse Engineering
2. Dumping the Source
3. Side-channel data leaks
4. Insecure Network Communication

3.Web application

1. Injections
2. XSS
3. CSRF
4. Sensitive data leaks

3. Radio Communications

Basically, radio communications provide a way to communicate with each other.
Some of the common radio protocols used in IoT are:
1.Wi-Fi
2.BLE
3.ZigBee
4.Wave
5.6LoWPAN
6.LoRa

3. Radio Communications

Some Vulnerabilities in Radio Communications are:
1.MITM
2.Replay-based attacks
3.Insecure Cyclic Redundancy check
4.Jamming attacks
5.DoS
basically, these are the basics of attack surface mapping

Vulnerability Assessment and Exploitation

- As the name suggests, in this step the tester exploits all those vulnerabilities found in previous steps and tries to crack the IoT device. Again, there are hundreds of ways a hacker can exploit the target.
- Some of them are:
- Exploiting using I2C and SPI
- JTAG debugging
- Firmware Reverse Engineering
- Hard coded Sensitive values
- etc.

Documentation and Reporting

In this step the tester have to make a in-depth detailed report of all the technical and non-technical summary.
Also the tester have to give all the proof of concepts, demos, code snippet, everything they used in the process.
Sometimes the tester have to reassess the bug after they get patched up.
These are all the four steps in the methodology of IoT pentesting.