The Method to the Madness of IoT Hacking

Dale Meredith
AUTHOR/TRAINER/SECURITY DUDE

@dalemeredith www.daledumbsitdown.com

What We'll Cover

- Let's define IoT hacking
- Phase 1: Reconnaissance
- Phase 2: Looking for vulnerabilities
- Phase 3: Attacks
- Phase 4: Achieve access
- Phase 5: Maintaining access

Let’s Define IoT Hacking

Let’s Define IoT Hacking

Hacking refers to the practice of modifying or altering any device, software, or even life forms to make “it” do something outside of it’s original purpose or design

Let's Define IoT Hacking

How Can Attackers Benefit?

Phase 1: Reconnaissance

Phase 1: Reconnaissance

Passive

No direct interaction with the target

Active

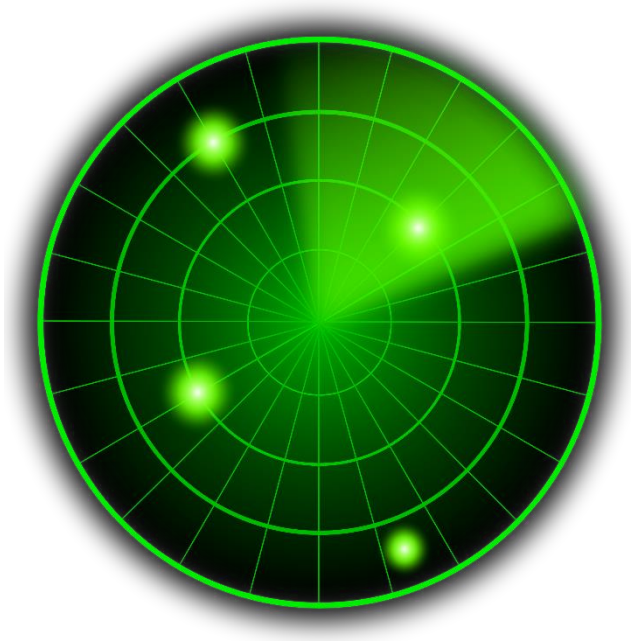
Direct interaction with the target

Which Type of Reconnaissance

- Port Scanning
- Ping
- Websites
- Doing a “Whois” Lookup
- Checking a Registrar for DNS

Phase 2: Looking for Vulnerabilities

Phase 2: Looking for Vulnerabilities



Gather Info

ID systems

Vulnerabilities

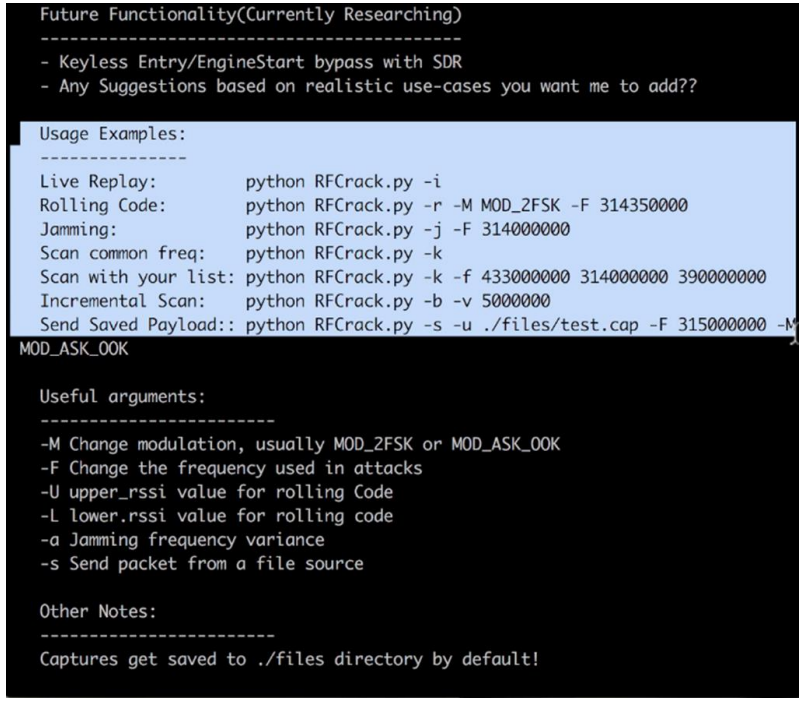
Tools Used

Port Scanners

Vulnerability Scanners

Phase 3: Attacks

Dealing with Rolling Codes



https://github.com/cclabsInc/RFCrack

Rolling code attacks

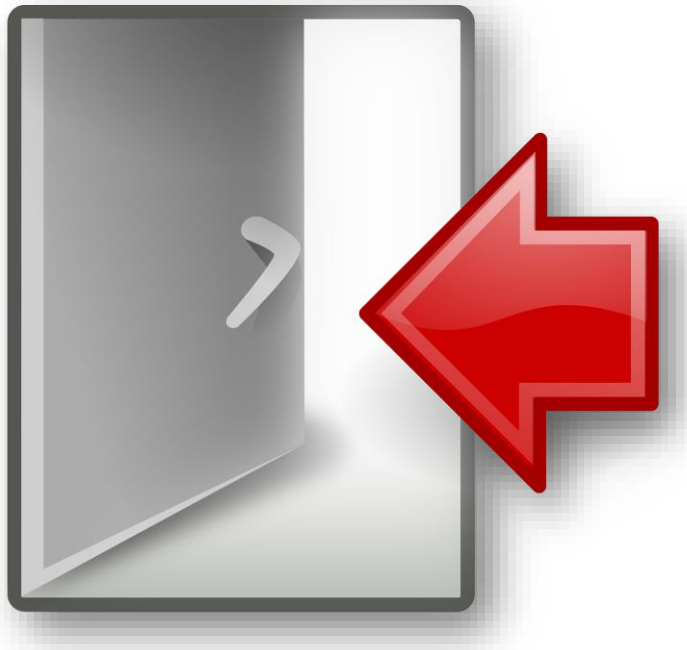
Jams

Scans

Replay attacks

Phase 4: Achieve Access

Phase 4: Achieve Access



Path

- Via network
- Via OS
- Via application
- Our goal?
  - To escalate privileges

Phase 5: Maintaining Access

Phase 5: Maintaining Access

- PWNing the system
- Use system as a pivot point
- Exploit the firmware
- Use resources
- Harden up

What We Talked About

- Let's Define IoT Hacking
- Phase 1: Reconnaissance
- Phase 2: Looking for vulnerabilities
- Phase 3: Attacks
- Phase 4: Achieve access
- Phase 5: Maintaining access