

# The Method to the Madness of IoT Hacking

---



**Dale Meredith**

AUTHOR/TRAINER/SECURITY DUDE

@dalemeredith [www.daledumbsitdown.com](http://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 its original purpose or design



# Let's Define IoT Hacking



# How Can Attackers Benefit?

Data

Ransomware

Malicious  
events

Pivot points

Prying



# 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

```
Future Functionality(Currently Researching)
-----
- Keyless Entry/EngineStart bypass with SDR
- Any Suggestions based on realistic use-cases you want me to add??

Usage Examples:
-----
Live Replay:      python RFCrack.py -i
Rolling Code:    python RFCrack.py -r -M MOD_2FSK -F 314350000
Jamming:         python RFCrack.py -j -F 314000000
Scan common freq: python RFCrack.py -k
Scan with your list: python RFCrack.py -k -f 433000000 314000000 390000000
Incremental Scan: python RFCrack.py -b -v 5000000
Send Saved Payload:: python RFCrack.py -s -u ./files/test.cap -F 315000000 -M
MOD_ASK_00K

Useful arguments:
-----
-M Change modulation, usually MOD_2FSK or MOD_ASK_00K
-F Change the frequency used in attacks
-U upper_rssi value for rolling Code
-L lower_rssi value for rolling code
-a Jamming frequency variance
-s Send packet from a file source

Other Notes:
-----
Captures get saved to ./files directory by default!
```

<https://github.com/cclabsInc/RFCrack>

Rolling code attacks

Jams

Scans

Replay attacks

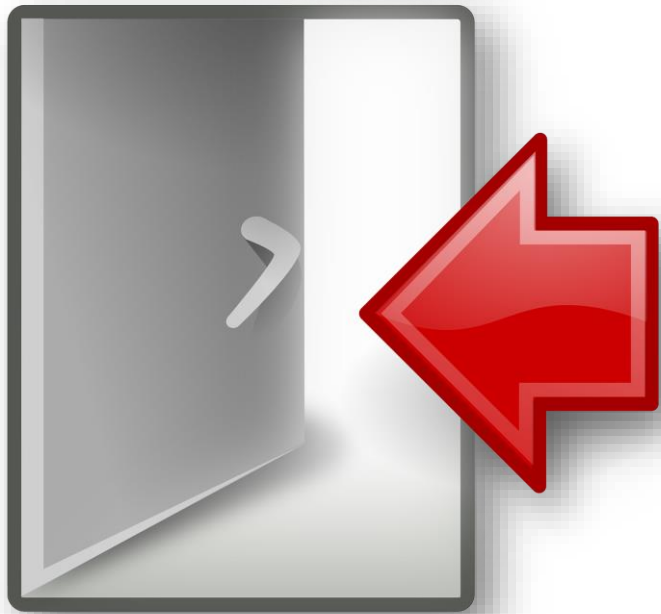


# Phase 4: Achieve Access

---



# Phase 4: Achieve Access



## Path

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



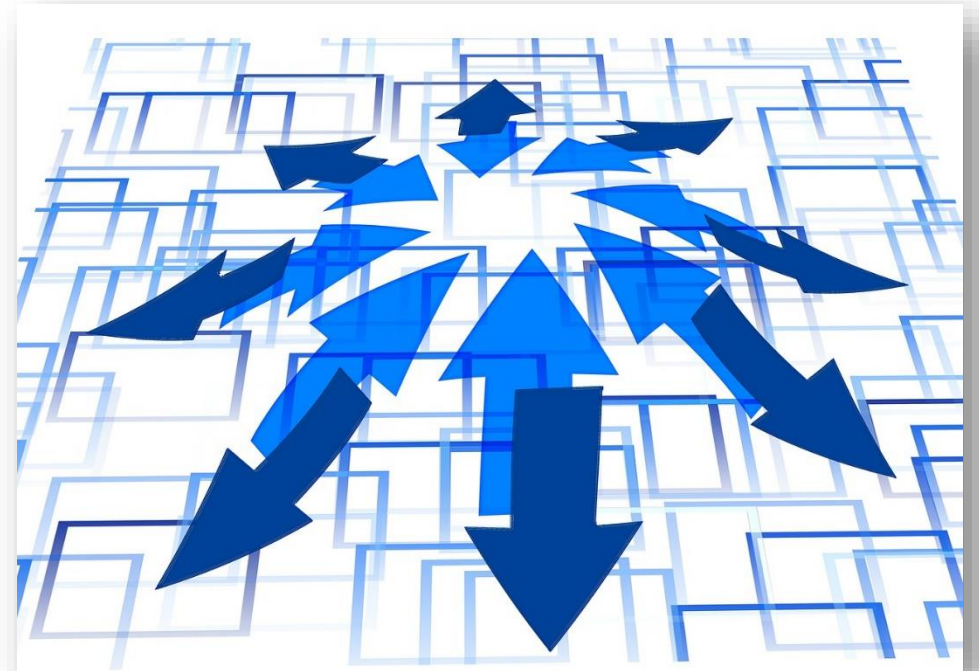
# Phase 5: Maintaining Access

---



# 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**

