Understanding IoT and OT Hacking Methodologies

Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith

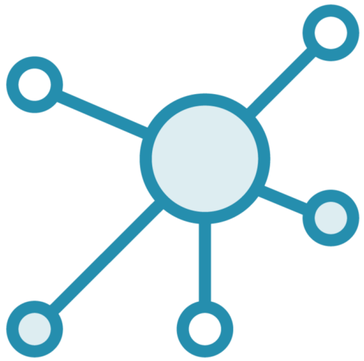
Reconnaissance

Network Reconnaissance

Network reconnaissance is the practice of covertly discovering and collecting information about a system. This method is often used in ethical hacking or penetration testing.

IOT

Scanning for common vulnerabilities



Endpoints

Specialized Tools

Metasploit
Shodan
Nmap

Default passwords

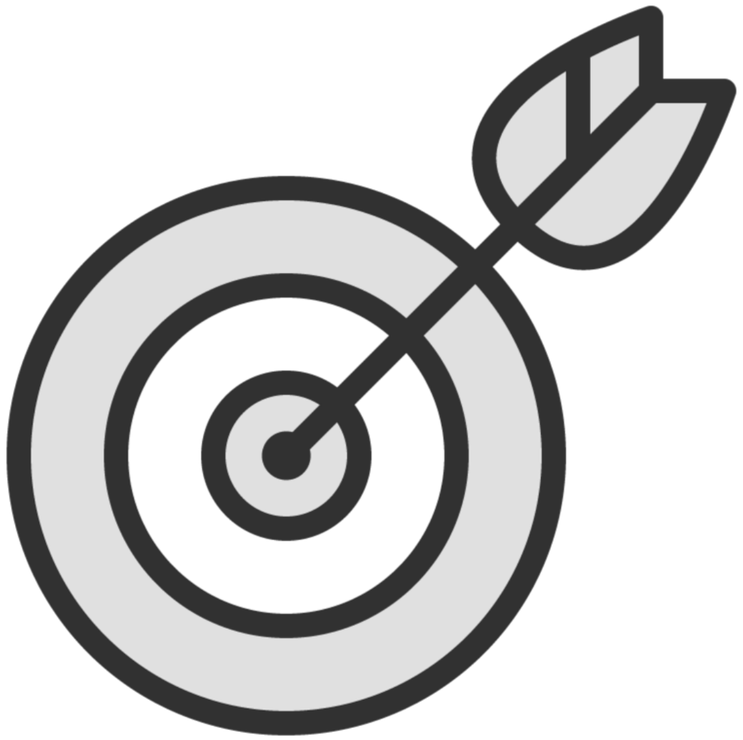
Research and Recommendations

Federal Communications Commission
https://www.fcc.gov/oet/ea/fccid

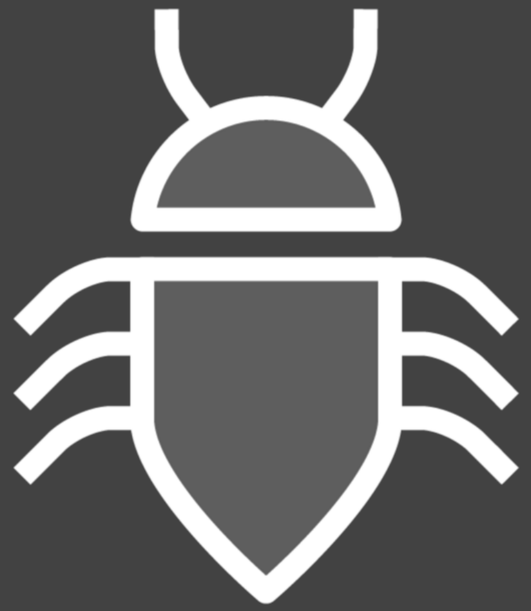
MutiPing and IoTSeeker

Vulnerability Scanning

Vulnerability Scanning



- **Exploits available to the public identify vulnerabilities**
- **Third-party research groups**
- **United States Computer Emergency Readiness Team (US-CERT)**



nmap commands

HMI devices
```
nmap -Pn -sT -p 46824 <Target IP>
```

SMATIC S7 PLCs
```
nmap -Pn -sT -p 102 --script s7-info <Target IP>
```

Modbus
```
nmap -Pn -sT -p 502 --script modbus-discover <Target IP>
```

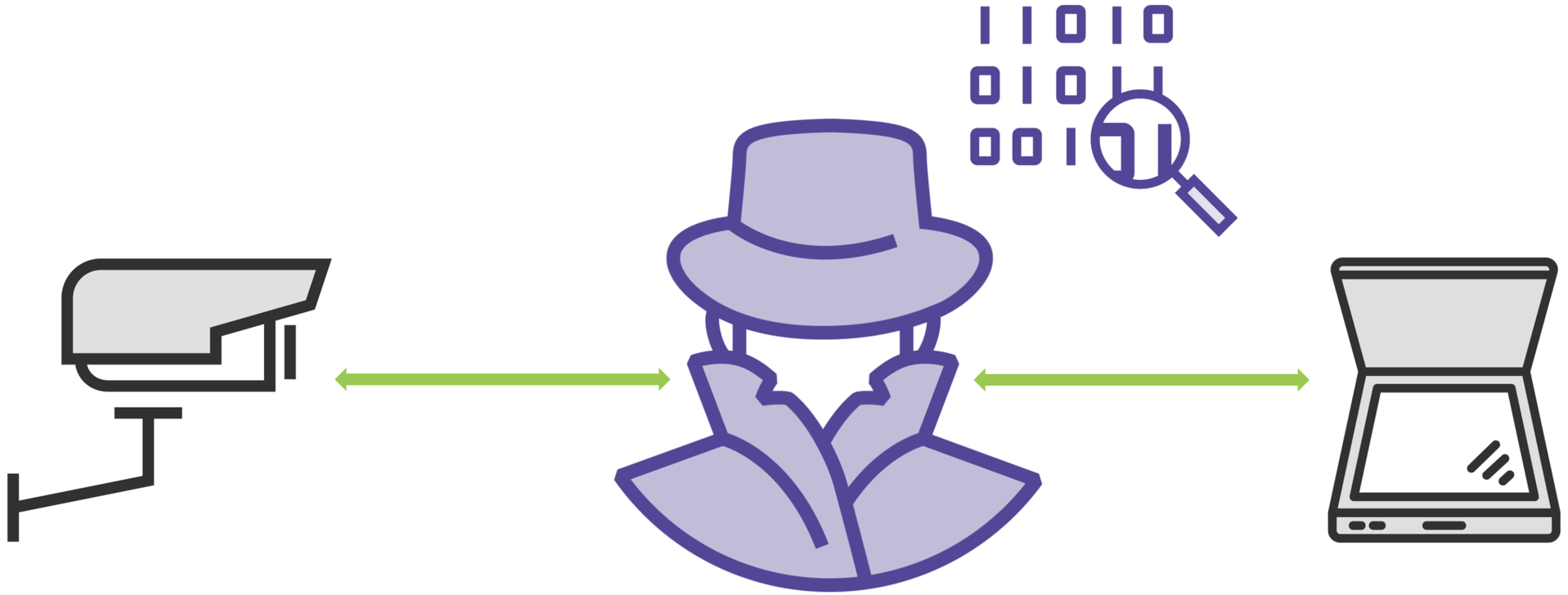
PCWorx
```
nmap -Pn -sT -p 1962 --script pcworx-info <Target IP>
```

nmap commands

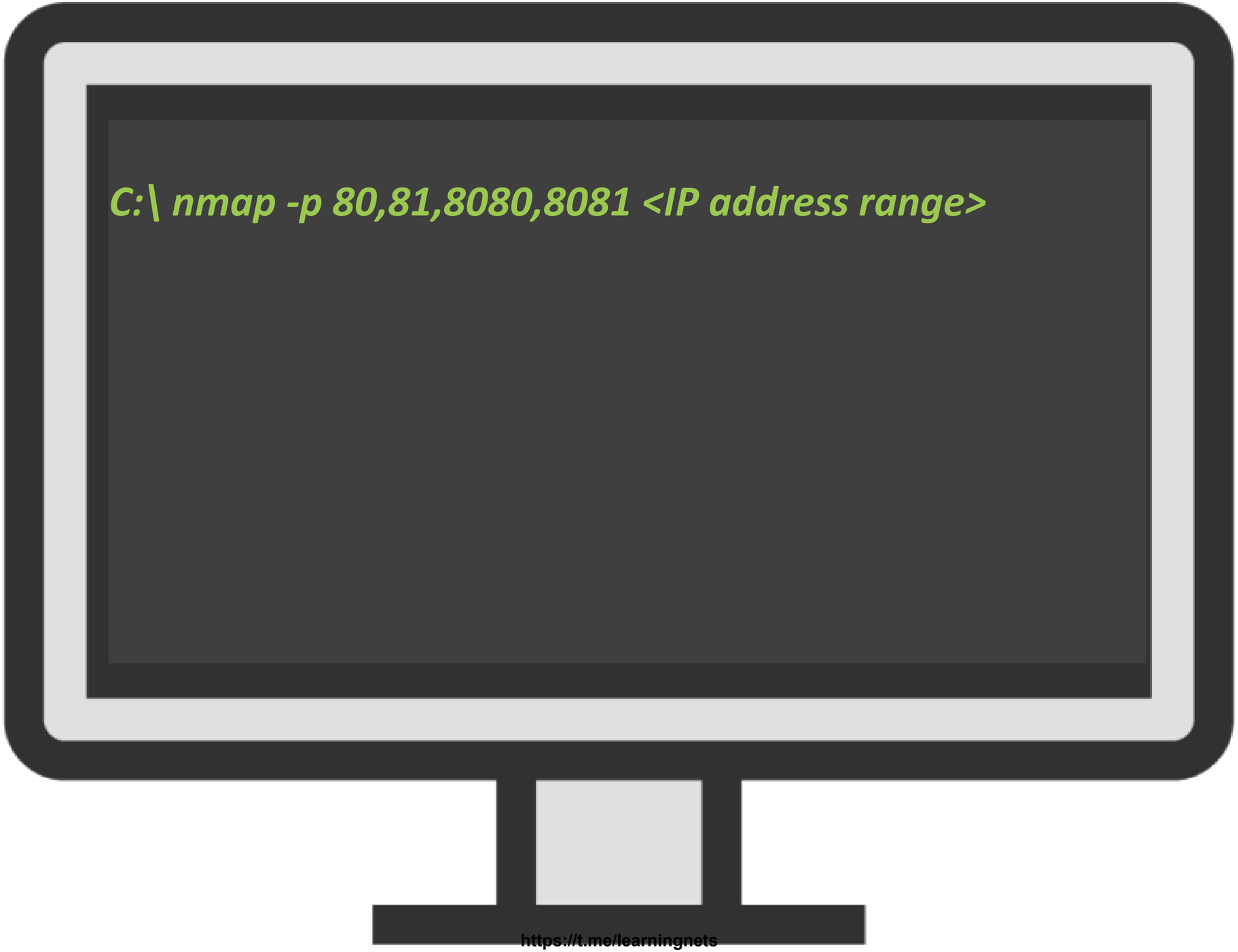
```
nmap -Pn -sT -p XXXX --script name <Target IP>

BACnet = --script bacnet-info
Niagara Fox = --script fox-info
ProConOS = --script proconos-info
```

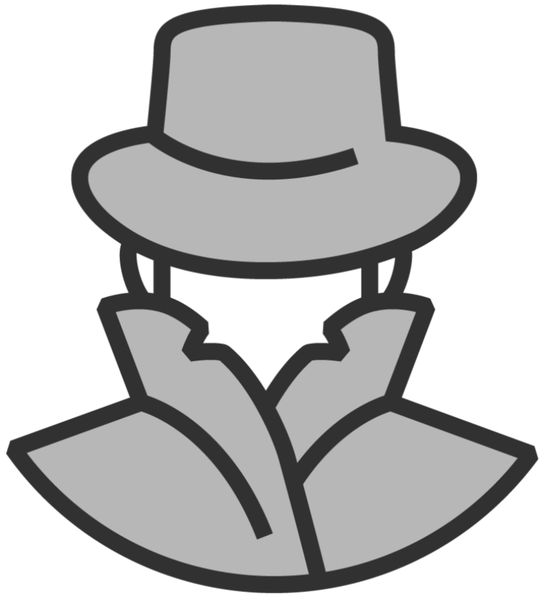
Sniffing for Devices

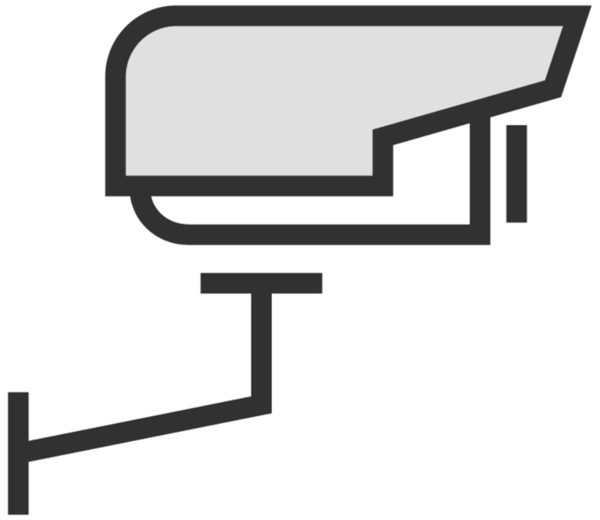


Majority of IoT devices communicate using unencrypted protocols



Always use a lab environment when practicing your skills





Gaining and Maintaining Remote Access

Gaining Remote Access

Conducts test to determine if the device has been compromised

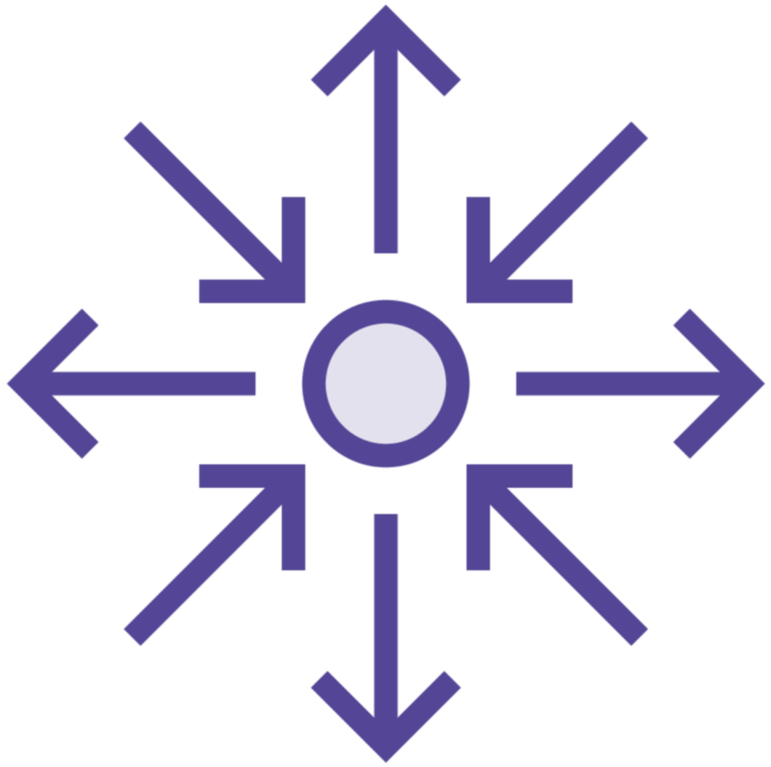
Determines what user-level access is available

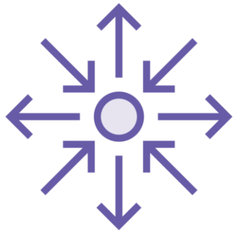
Identifies an open telnet port

Learns what information is shared between the connected devices

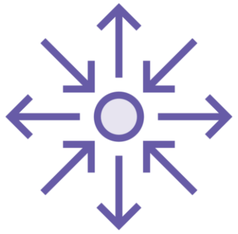
Performs further attacks by exploiting vulnerabilities

Infiltrate and Exfiltrate Data





Upload and execute scripts



Establish a remote shell

Move laterally within devices

Maintaining and Extending Access

Remain hidden by deleting logs, upgrading firmware, and deploying malicious applications

Utilize specialized tools to exploit firmware

Firmware Analysis

The process of examining the firmware of a targeted device to identify underlying flaws and risks

Used to find passwords, API tokens, endpoints, backdoor accounts, and configuration files

Attackers will use reverse engineer the firmware to discover weaknesses and backdoors as a means to maintain future access

Attackers will be prepared for multiple contingencies by having specialized tools on hand

Learning Check

Learning Check

- **FCC (Federal Communications Commission)**
- **Telnet**
- **US-CERT**
- **Port and script name (--script modbus-discover)**
- **Delete logs, upgrade firmware, or deploy backdoors**

Up Next:
Exploring IoT and OT Hacking Tools