THREAT MODELING BASED PENETRATION TESTING: THE OPEN ENERGY MONITOR CASE STUDY

Massimiliano Rak
University of Campania L. Vanvitelli
massimiliano.rak@unicampania.it

Giovanni Salzillo
University of Campania L. Vanvitelli
giovanni.salzillo@unicampania.it

Felice Moretta
University of Campania L. Vanvitelli
felice_moretta@hotmail.it

Table of Contents

Introduction - Contributions

- Enhancement of our *Penetration Testing methodology* with the integration of the *CAPEC knowledge-base*.
- *Threat model* and extension of our *Threat Catalog* for the MQTT protocol and multiple MQTT-based devices.
- Testing of a real-world Home Automation System: Open Energy Monitor
  - Threats;
  - Attacks;
  - Countermeasures.

Security Testing: Penetration Testing

- Human-driven and it’s quality is highly based on the skills of the penetration tester (Costs & Time consuming).
- No standard and no-complete & no-redundand methodology has been defined so far.

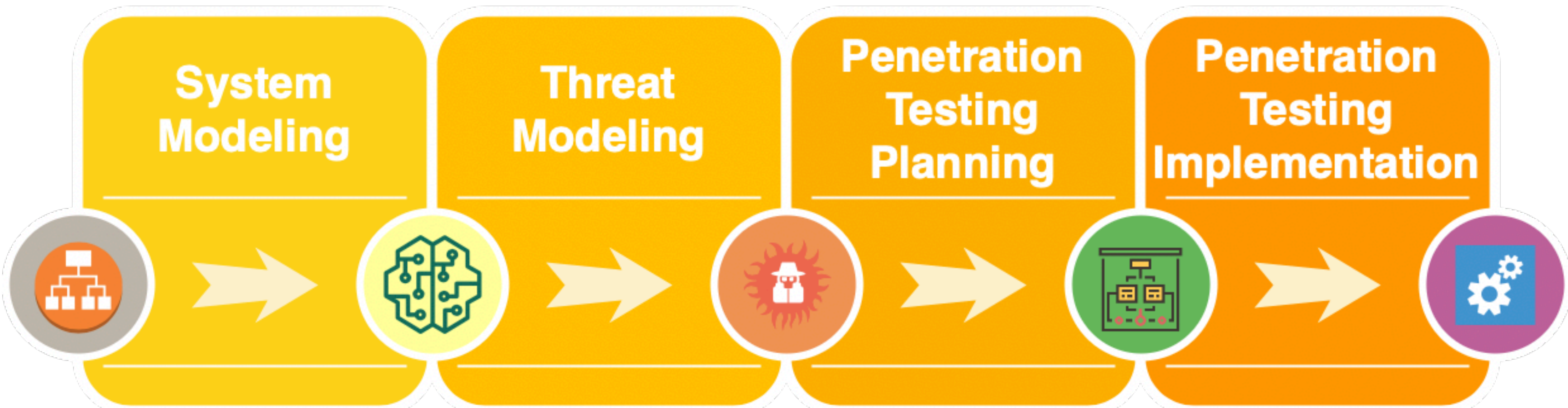
- Several **methodologies** defined in recent years: *NIST SP 800-115, OWASP, PTES, ISSAF.*
- As well as many **technical guidelines** and **tools** for specific technology domains: *OSSTMM, PTS, MFS*

Security Testing: Penetration Testing

Additionaly, the available methodologies mainly focus on technical analysis:

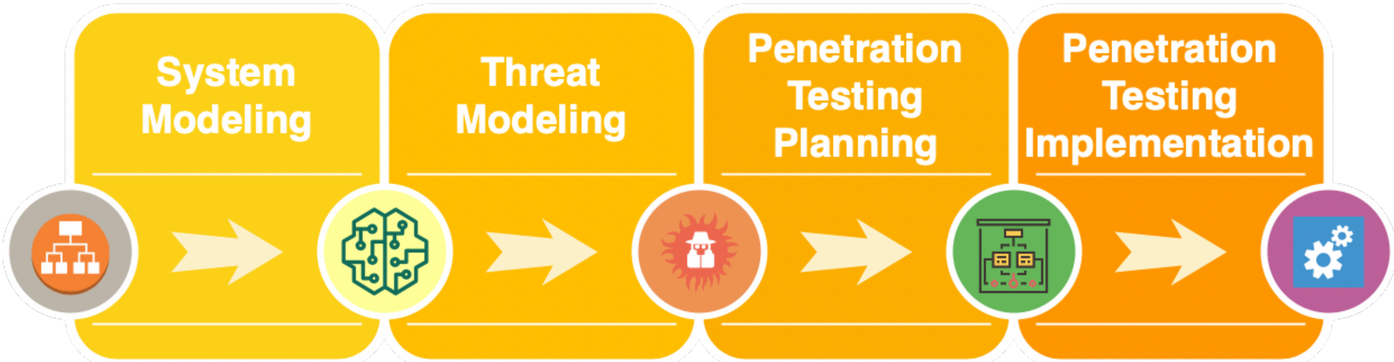
- Good to address security vulnerabilities and exploitable attack paths.
- Well suited for security certification processes.
- Expensive & Hard to understand to the end user.

The Proposed Methodology



A four-step methodology guided by the *TM* and *RA* processes, that enables less-skilled pen-tester to perform security evaluations on a per threats-basis.

The Proposed Methodology (1)

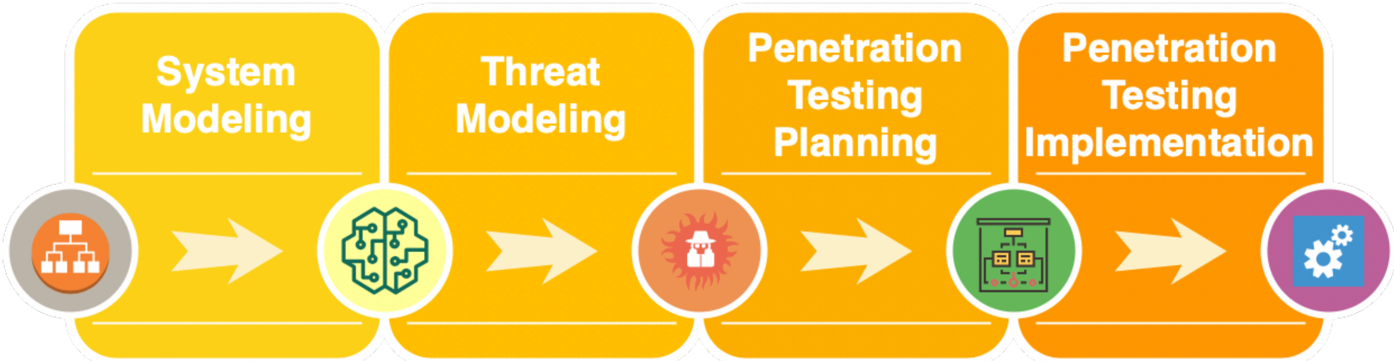


1. **System Modeling**: (semi-)formal description of the SuT.

The methodology entirely relies on the correctness and the accuracy of the SuT model, *thorugh the **MACM** formalism*, which is then used to drive the following activities. Three modeling approaches:

- (i) White-box, (ii) Grey-box, (iii) Black-box.

The Proposed Methodology (2)



2. Threat Modeling: threats identification

Threat enumeration and identification by the means of a threat catalogue.

It is a knowledge-base developed in the context of two EU projects (SPECS & MUSA), containing several well-known threats grouped by multiple attributes.

The Proposed Methodology (2)

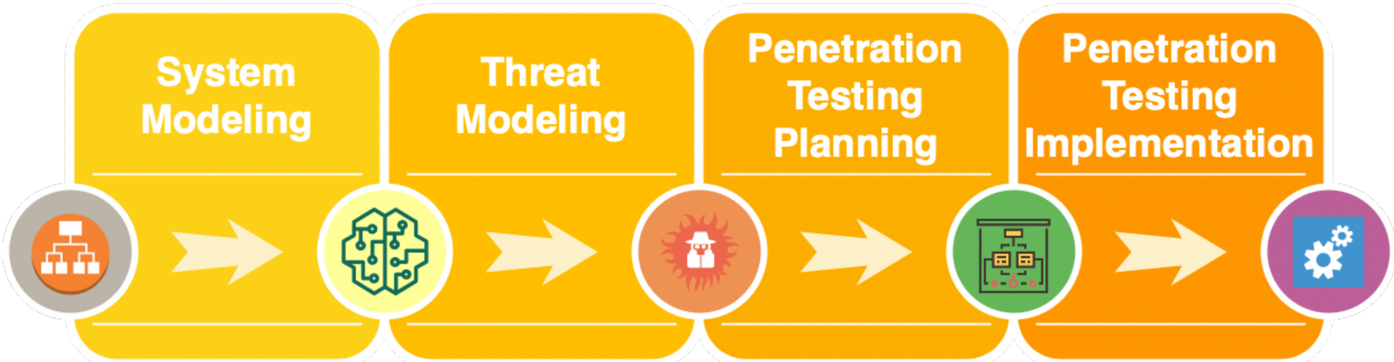
2. Threat Modeling: threats identification.

It includes threats for many software components and protocols *(Ethernet, IP, TCP, TLS, XMPP, OAUTH, Zigbee, Bluetooth, BLE, GSM,)* and it is constantly updated.

It is constructed in such a way that *MACM* nodes coincide to the threat *asset-type* field.

Threat model is created by querying and composing threats from the threat catalogue.

The Proposed Methodology (3)



3. Planning: planning the tests and possible attacks to perform.

Penetration testers select the right test planning schemes from a pre-build knowledge base, which is continuously updated with exploitation techniques (tools and actions to execute), mapped to specific threats.

The Proposed Methodology (3) – CAPEC Integration

3. Planning: planning the tests and possible attacks to perform.

MITRE - Common Attack Pattern Enumeration and Classification

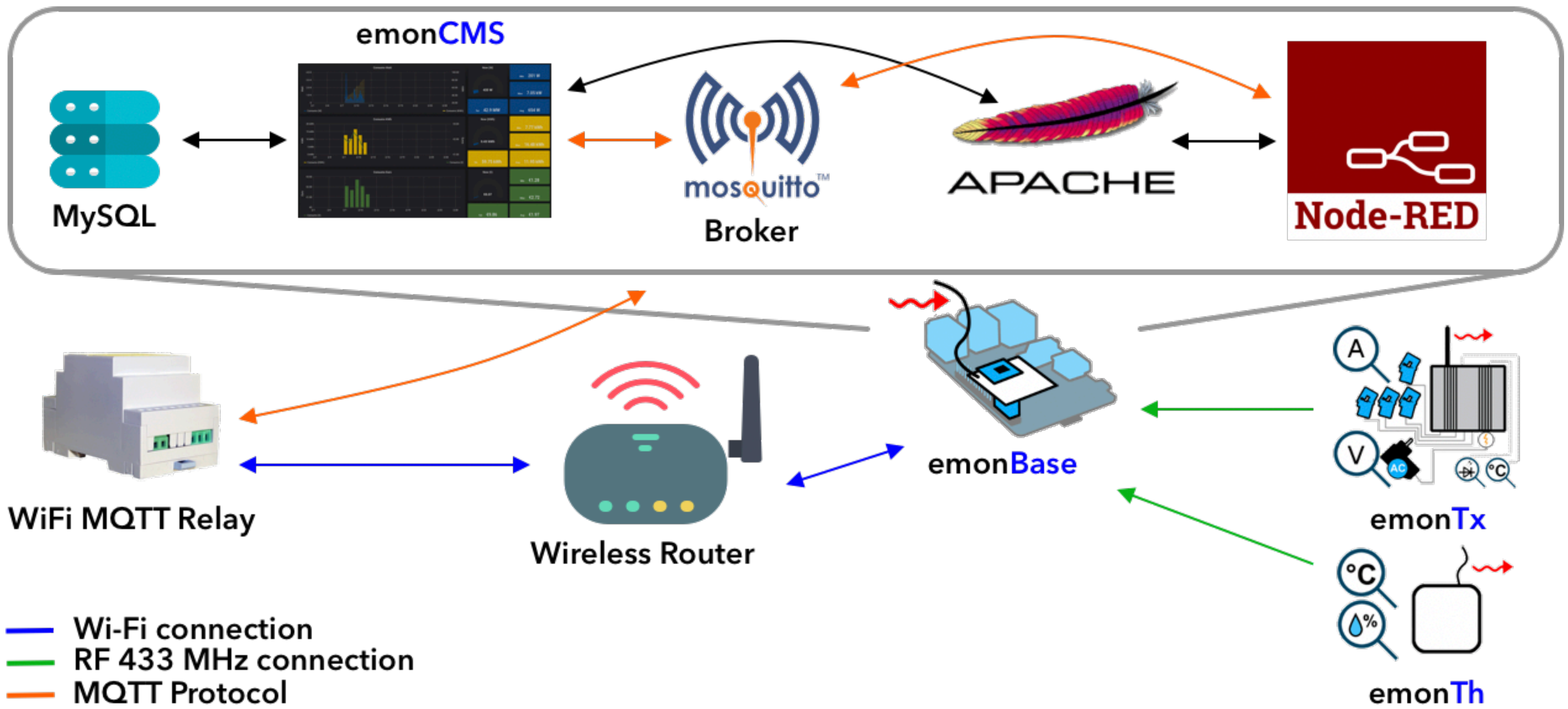
Catalog of common attack patterns employed by adversaries to exploit known weaknesses.

500+ elements, classified in three hierarchical description levels (META, STANDARD, DETAILED).

4. Implementation: actual execution of the attacks.

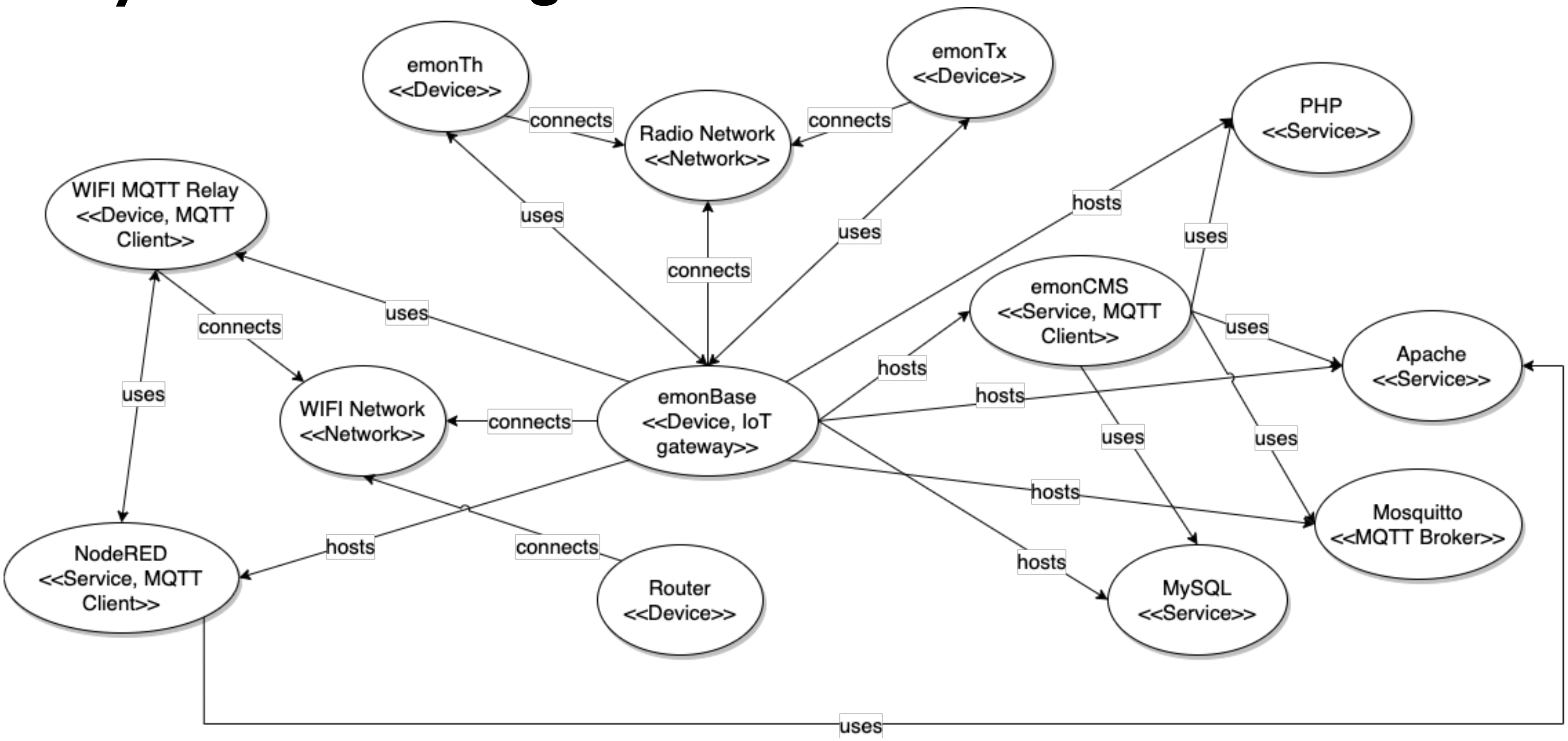
Our case study: Open Energy Monitor

An open-source platform for control automation and monitoring of several home appliances



Our case study: Open Energy Monitor

1. System Modeling



MACM entities:

Nodes (6): {**Device, IoTGateway, Network, Service**} + {**MQTTClient, MQTTBroker**}

Relations (3): {**use, host, connect**}.

Our case study: Open Energy Monitor

2. Threat Modeling – MQTT Threats

In order to support the technologies involved within the case study, we enriched the catalogue with MQTT-related known threats.

ID	Threat	Description	Asset	STRIDE	CIA
T1	Device Isolation	An attacker can make the asset (an IoT Device acting as MQTT client) unable to send or receive messages.	MQTT Client	Denial of Service	Availability
T2	Communication Lock	An attacker can make the MQTT communication unavailable.	MQTT Broker	Denial of Service	Availability
T3	Eavesdropping (Global)	An adversary retrieve data accessing communication among multiple assets communicating through MQTT.	MQTT Broker	Information Disclosure	Confidentiality
T4	Eavesdropping (Local)	An adversary retrieve valuable data from the transmitted packets that are sent from the device.	MQTT Client	Information Disclosure	Confidentiality
T5	Action Spoofing	An attacker can access to reserved topic, to publish or receive messages.	MQTT Broker	Elevation of Privilege	Confidentiality
T6	Impersonation	An adversary can easily retrieve credentials from the transmitted packets that are sent from asset.	MQTT Client	Spoofing	Confidentiality
T7	Message Tampering	An adversary intercept and modify the packets' content sent using the asset.	MQTT Broker	Tampering	Integrity
T8	Device Message Tampering	An adversary intercept and modify the packets' content sent from the asset.	MQTT Client	Tampering	Integrity
T9	Data Leakage	An adversary can access to local data of the asset.	MQTT Broker	Information Disclosure	Confidentiality

Table 1: MQTT threats, excerpt of Threat Catalogue

Our case study: Open Energy Monitor

2. Threat Modeling – OEM TM

We retrieved the threat model in an automated way through ad-hoc queries on the threat catalogue, mapping threats to assets.

Component	Asset Type	Threats
EmonBase, EmonPi	IoT Gateway, IoT Device	Data Leakage, Denial of Service, Impersonation, Device isolation
EmonCMS	Service, MQTT Client	Denial of Service, Impersonation, Eavesdropping, Data Leakage
EmonTh, EmonTx	IoT Device	Denial of Service, Impersonation, Data Leakage, Exhaustion of Power, Device isolation
Radio Network	Network	Eavesdropping, Message tampering, Message elimination, Message injection, Network partitioning, Jamming
WiFi Network	Network	Eavesdropping, Message tampering, Message elimination, Message injection, Network partitioning, Jamming, Network access, Topology disclosure
Mosquitto	MQTT Broker	Denial of Service, Action spoofing, Eavesdropping, Impersonation, Message tampering, Communication lock
WiFi MQTT Relay	MQTT Client, IoT Device	Impersonation, Denial of Service, Data Leakage, Eavesdropping, Device message tampering
Node-RED	MQTT Client, Service	Denial of Service, Impersonation, Eavesdropping, Data Leakage, Device isolation

Table 2: Open Energy Monitor Threat Model

Our case study: Open Energy Monitor

3. Penetration Testing Planning – CAPEC

For each threat of our threat model, we identified the related meta-level attack(s), and the subsequent standard and detailed patterns that could implement a feasible attack.

ID	Name	Type	Description	Child Of
125	Flooding	Meta	An adversary consumes the resources of a target by rapidly engaging in a large number of interactions with the target.	N/A
227	Sustained Client Engagement	Meta	An adversary attempts to deny legitimate users access to a resource by continually engaging a specific resource in an attempt to keep the resource tied up as long as possible.	N/A
482	TCP Flood	Standard	An adversary may execute a flooding attack using the TCP protocol with the intent to deny legitimate users access to a service.	227
117	Interception	Meta	An adversary monitors data streams to or from the target for information gathering purposes.	N/A
157	Sniffing Attacks	Standard	An adversary may intercept information transmitted between two third parties. The adversary must be able to observe, read, and/or hear the communication traffic, but not necessarily block the communication or change its content.	117
158	Sniffing Network Traffic	Detailed	An adversary intercepts information transmitted between two parties. The adversary must be able to observe, read, and/or hear the communication traffic, but not necessarily block the communication or change its content.	157

Table 3: CAPEC Attack Patterns

Our case study: Open Energy Monitor

3. Penetration Testing Planning

ID	Attack	Threat(s)	Meta	Standard	Detailed	Related
A1	Packets Sniffing	T3, T4	117	157	158, 65	N/A
A2	Identity Spoofing	T6	151	194, 195	633	T4
A3	Brute Force	T6	112	49	16, 70	N/A
A4	Data Stealing	T9	122	1, 180	N/A	T5
A5	Privilege Escalation	T5	122	1, 180	N/A	T6
A6	Snarfing	T7, T8	94	384, 185	385, 389	N/A
A7	CONNECT Flood	T2	125	488	N/A	N/A
A8	PUBLISH flood	T1, T2	125	488	N/A	N/A
A9	DoS Impersonation	T6	227	N/A	N/A	T6

Table 4: Attack Plan Table

Our case study: Open Energy Monitor

3. Penetration Testing Planning

ID	Attack	Threat(s)	Meta	Standard	Detailed	Related
A1	Packets Sniffing	T3, T4	117	157	158, 65	N/A
A2	Identity Spoofing	T6	151	194, 195	633	T4
A3	Brute Force	T6	112	49	16, 70	N/A
A4	Data Stealing	T9	122	1, 180	N/A	T5
A5	Privilege Escalation	T5	122	1, 180	N/A	T6
A6	Snarfing	T7, T8	94	384, 185	385, 389	N/A
A7	CONNECT Flood	T2	125	488	N/A	N/A
A8	PUBLISH flood	T1, T2	125	488	N/A	N/A
A9	DoS Impersonation	T6	227	N/A	N/A	T6

Tabl : Attack Plan Table

T3	Eavesdropping (Global)	An adversary retrieve data accessing communication among multiple assets communicating through MQTT.	MQTT Broker	Information Disclosure	Confidentiality
T4	Eavesdropping (Local)	An adversary retrieve valuable data from the transmitted packets that are sent from the device.	MQTT Client	Information Disclosure	Confidentiality

Our case study: Open Energy Monitor

3. Penetration Testing Planning

ID	Attack	Threat(s)	Meta	Standard	Detailed	Related
A1	Packets Sniffing	T3, T4	117	157	158, 65	N/A
A2	Identity Spoofing	T6	151	194, 195	633	T4
A3	Brute Force	T6	112	49	16, 70	N/A
A4	Data Stealing	T9	122	1, 180	N/A	T5
A5	Privilege Escalation	T5	122	1, 180	N/A	T6
A6	Snarfing	T7, T8	94	384, 185	385, 389	N/A
A7	CONNECT Flood	T2	125	488	N/A	N/A
A8	PUBLISH flood	T1, T2	125	488	N/A	N/A
A9	DoS Impersonation	T6	227	N/A	N/A	T6

Table 4: Attack Plan Table

117	Interception	Meta	An adversary monitors data streams to or from the target for information gathering purposes.	N/A
157	Sniffing Attacks	Standard	An adversary may intercept information transmitted between two third parties. The adversary must be able to observe, read, and/or hear the communication traffic, but not necessarily block the communication or change its content.	117
158	Sniffing Network Traffic	Detailed	An adversary intercepts information transmitted between two parties. The adversary must be able to observe, read, and/or hear the communication traffic, but not necessarily block the communication or change its content.	157

Our case study: Open Energy Monitor

Prerequisites

The target must be communicating on a network protocol visible by a network sniffing application.

The adversary must obtain a logical position on the network from intercepting target network traffic is possible. Depending on the network topology, traffic sniffing may be simple or challenging. If both the target sender and target recipient are members of a single subnet, the adversary must also be on that subnet in order to see their traffic communication.

Skills Required

[Level: Low]
Adversaries can obtain and set up open-source network sniffing tools easily.

Resources Required

A tool with the capability of presenting network communication traffic (e.g., Wireshark, tcpdump, Cain and Abel, etc.).

Consequences

The table below specifies different individual consequences associated with the attack pattern. The Scope identifies the security property that is violated, while the Impact describes the negative technical impact that arises if an adversary succeeds in their attack. The Likelihood provides information about how likely the specific consequence is expected to be seen relative to the other consequences in the list. For example, there may be high likelihood that a pattern will be used to achieve a certain impact, but a low likelihood that it will be exploited to achieve a different impact.

Scope	Impact	Likelihood
Confidentiality	Read Data	

Mitigations

Obfuscate network traffic through encryption to prevent its readability by network sniffers.

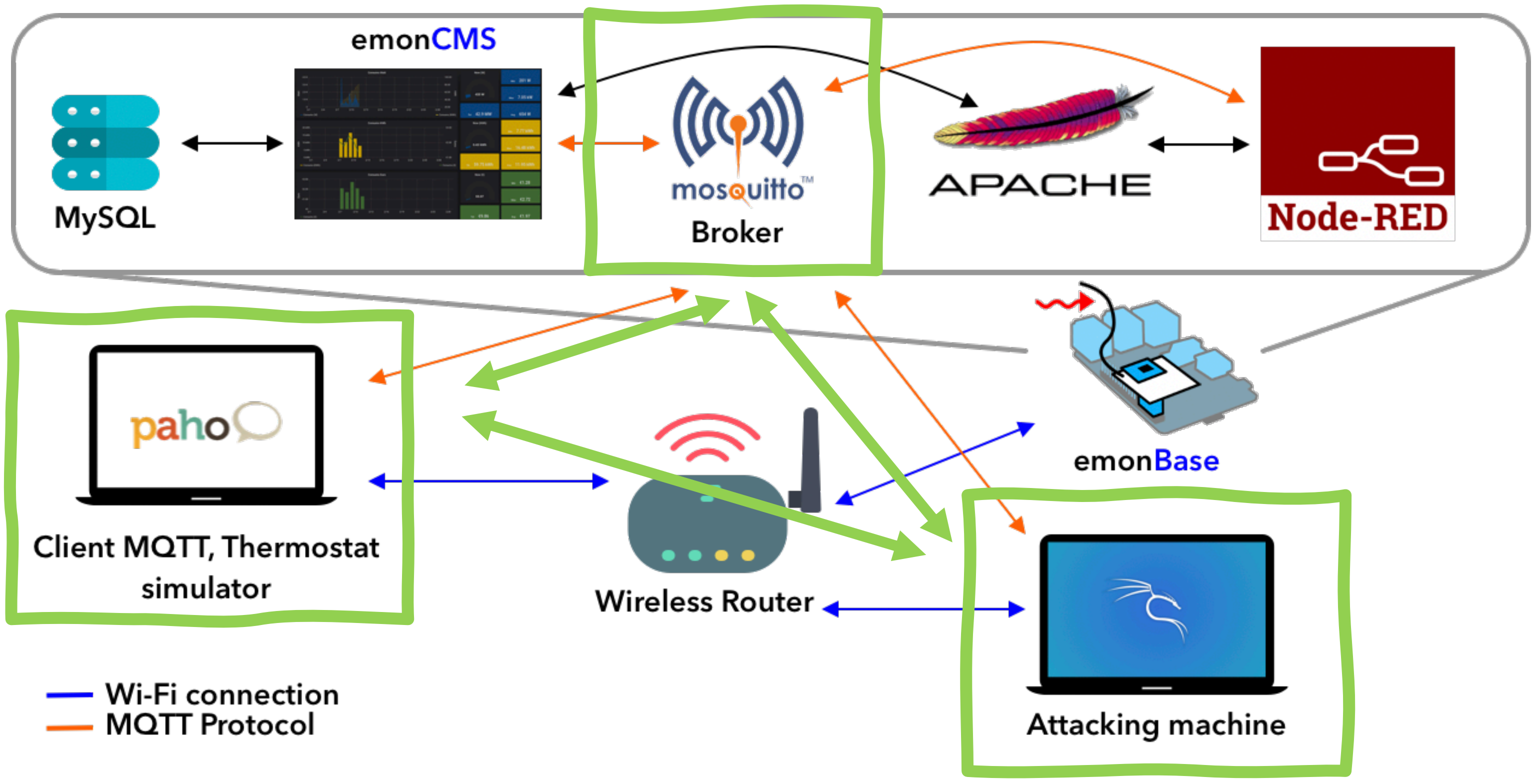
Employ appropriate levels of segmentation to your network in accordance with best practices.

	Interception	Meta	An adversary monitors data streams to or from the target for information gathering purposes.	N/A
	Sniffing Attacks	Standard	An adversary may intercept information transmitted between two third parties. The adversary must be able to observe, read, and/or hear the communication traffic, but not necessarily block the communication or change its content.	117
158	Sniffing Network Traffic	Detailed	An adversary intercepts information transmitted between two parties. The adversary must be able to observe, read, and/or hear the communication traffic, but not necessarily block the communication or change its content.	157

Our case study: Open Energy Monitor

4. Penetration Testing Implementation – MQTT Packet Sniffing

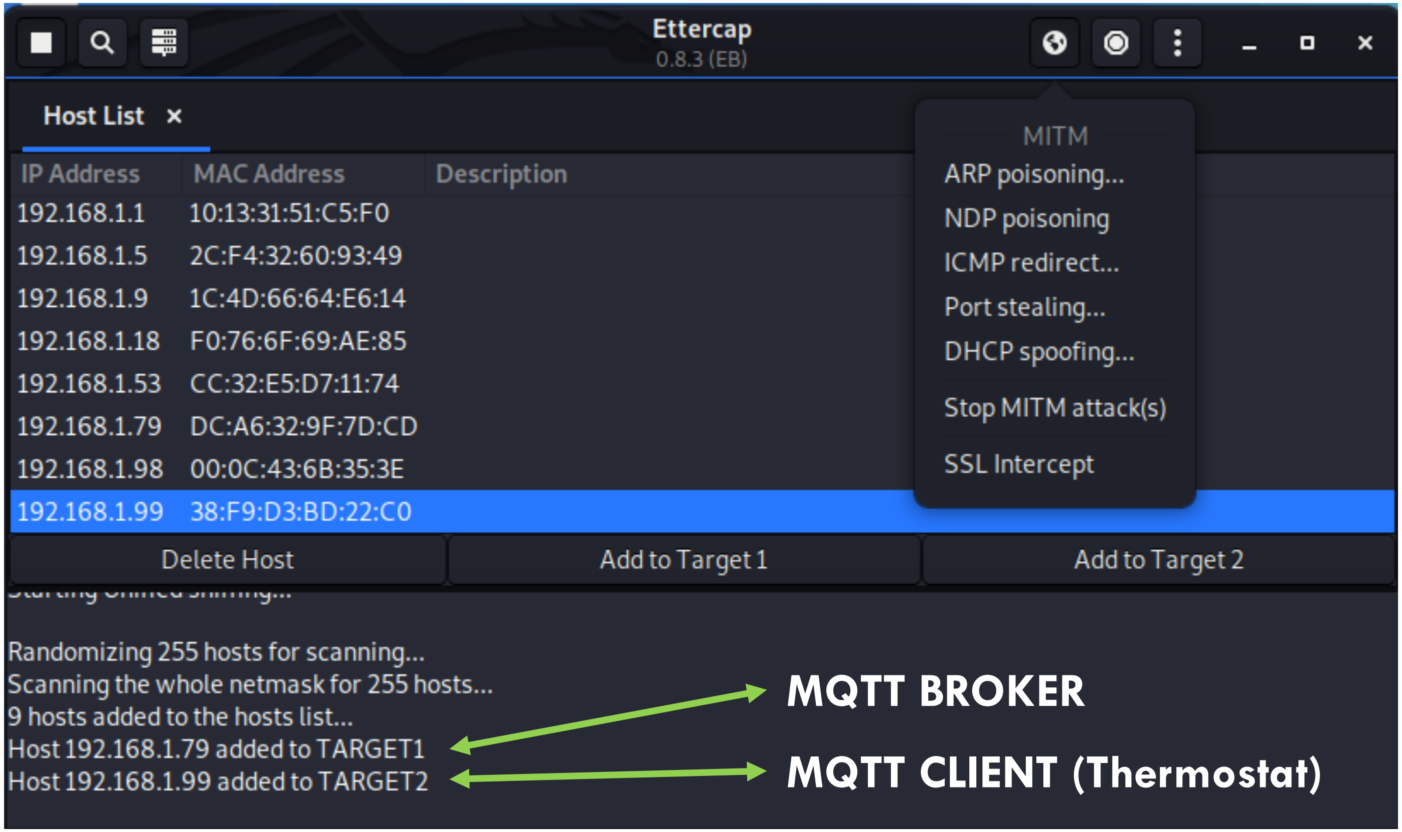
Our Testbed



Our case study: Open Energy Monitor

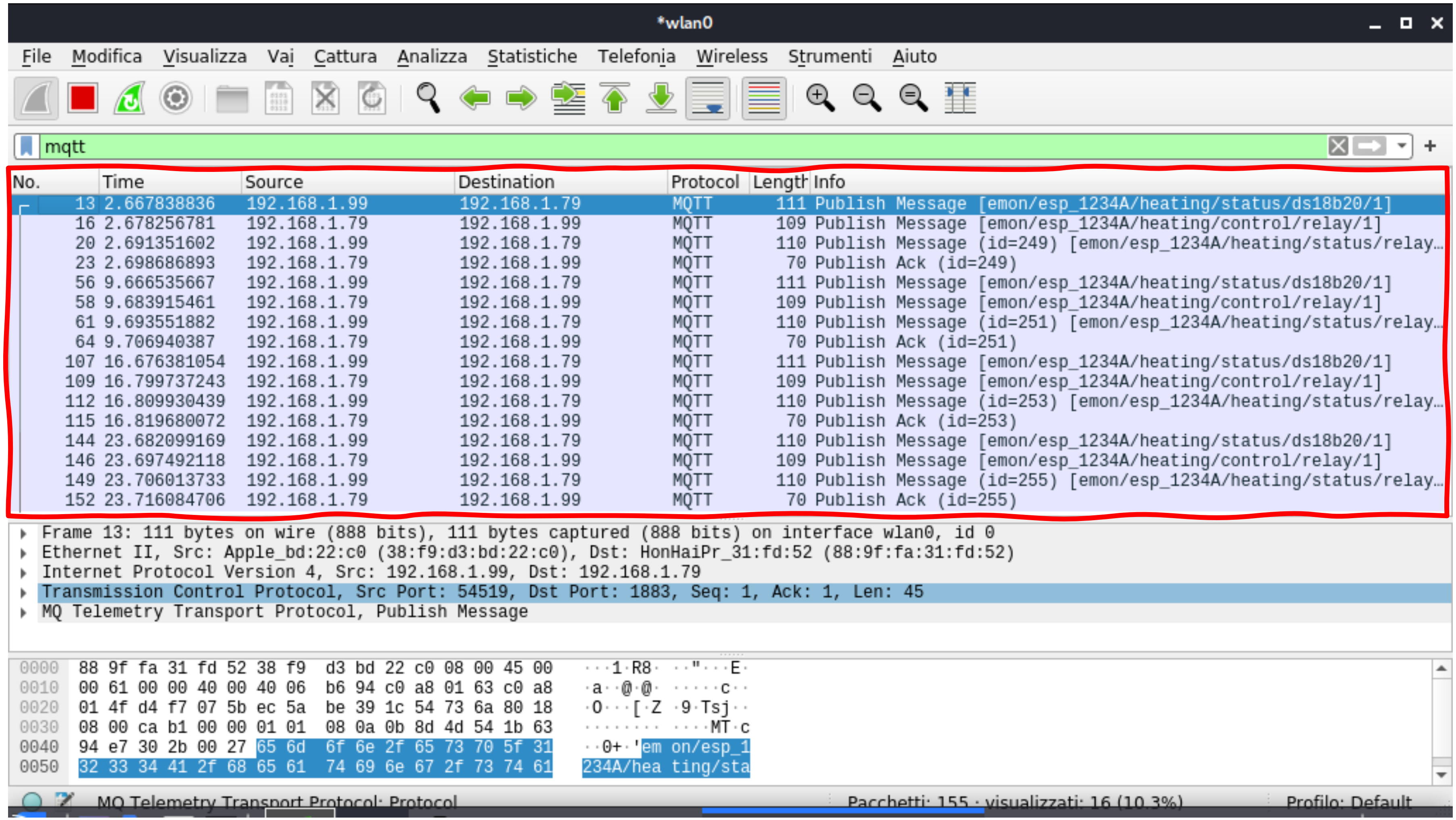
4. Penetration Testing Implementation – MQTT Packet Sniffing

Toolchain:
- **Ettercap** (L2 MITM, through ARP poisoning)
- **Wireshark** (packet logging & analysis).



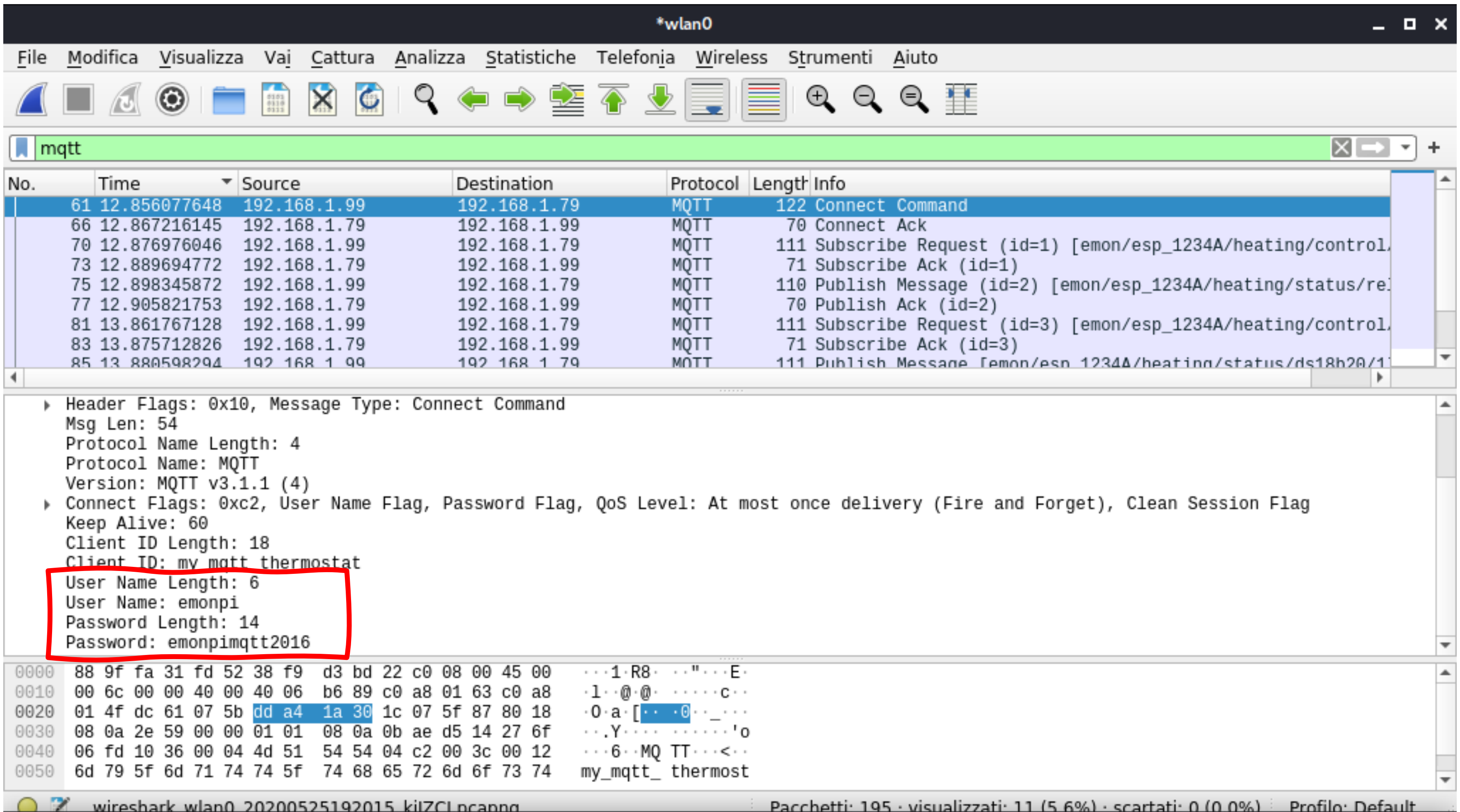
Our case study: Open Energy Monitor

4. Penetration Testing Implementation – Packet Sniffing



Our case study: Open Energy Monitor

4. Penetration Testing Implementation – Packet Sniffing



Our case study: Open Energy Monitor

Results

ID	Attack	Threat	ER	Critical issues	Countermeasures
A1	Packet Sniffing	T3, T4	✓	Packets' payload are sent in clear	TLS
A2	Identity Spoofing	T6	✓	Credentials are sent in clear	TLS
A3	Brute Force	T6	✓	No sleep delay between consequent requests	Limit the incoming requests rate
A4	Data Stealing	T9	✓	Topics with basic level "$SYS" are accessible to all	Access Control List
A5	Privilege Escalation	T5	✓	Each client can subscribe to all topics	Access Control List
A6	Snarfing	T7, T8	✓	No integrity check of data packets	TLS or HMAC
A7	CONNECT Flood	T2	✓	No delay between consequent CONNECT requests	Limit the incoming requests rate
A8	PUBLISH Flood	T1	✓	No delay between consequent PUBLISH requests	Limit the incoming requests rate
A9	DoS Impersonation	T1	✓	No warnings upon multiple authentication attempts	Warning system, additional auth features

Table 5: OEM Penetration Test Summary

Many of the suggested mitigation techniques are already supported by the MQTT standard and by many of the MQTT implementation, although they must be often explicitly enabled on most of the systems, including OEM.

Conclusion & Future Works

- The penetration testing methodology we adopted supports IoT-based systems and enable professionals with limited computer security skills to identify and demonstrate suitable attacks.
- Available software, as OEM, should improve and enforce security-by-default configuration preset & requirements.

In the next future we plan to:

- extend our model by building a set of tools to automate threats verification and automated testing &
- enrich the attack plan generation by integrating other sources of Cyber Threat Intelligence.

Thanks for your attention

QA

Threat Modeling based Penetration Testing: The Open Energy Monitor Case study

Massimiliano Rak
University of Campania L. Vanvitelli
massimiliano.rak@unicampania.it

Giovanni Salzillo
University of Campania L. Vanvitelli
giovanni.salzillo@unicampania.it

Felice Moretta
University of Campania L. Vanvitelli
felice_moretta@hotmail.it

SINCONF2020 - Wednesday, Nov. 4, 2020, Online Conference