Damn Vulnerable Infrastructure

Lorenzo Corbinelli
University of Florence
Florence, Italy
lorenzo.corbinelli@edu.unifi.it

Giulia Giamberini
University of Florence
Florence, Italy
giulia.giamberini@edu.unifi.it

***Abstract*—This report aims to describe an hypothetical critical industrial infrastructure, examining various scenarios of potential attacks that could be executed by a malicious actor. The study will analyze different scenarios, identifying various types of vulnerabilities and lateral movements that an attacker might exploit based on their ultimate objective.**

***Index Terms*—SCADA systems, cybersecurity, industrial control systems, vulnerabilities, CVEs, VPN, DNS, LiDiTE, MQTT, OpenPLC, OpenWRT, databases, MariaDB, MySQL, Modbus, PLC, Remote Desktop, BeEF**

I. Introduction

Industrial infrastructures are critical systems, and any attempt by an attacker to compromise them can result in significant damage and potentially even victims. To mitigate these risks, digital twins of real systems are developed.
This report uses the digital twin for the critical infrastructure described in the paper **LiDiTE: a Full-Fledged and Feather-weight Digital Twin Framework.** [1]

In particular, the network topology of the infrastructure has been meticulously designed to **include intentional vulnerabilities**. This setup allows the study of attacker behavior, in a controlled environment. By incorporating these vulnerabilities, it is possible to observe **how attackers exploit weak points** and perform lateral movements within the network.

II. Related work

The report's goal is quite similar to the one of the ICS Goat project [2]. The objective of ICS Goat project is mainly focused on industrial vulnerabilities while our work focuses more on the network infrastructure and lateral movements.

III. Infrastructure Overview

The network's topology will be described in the following subsections.
Note: Each component described in the topology is not physically replicated for studying purposes, but the network will be prototyped using Docker images [3], [4].

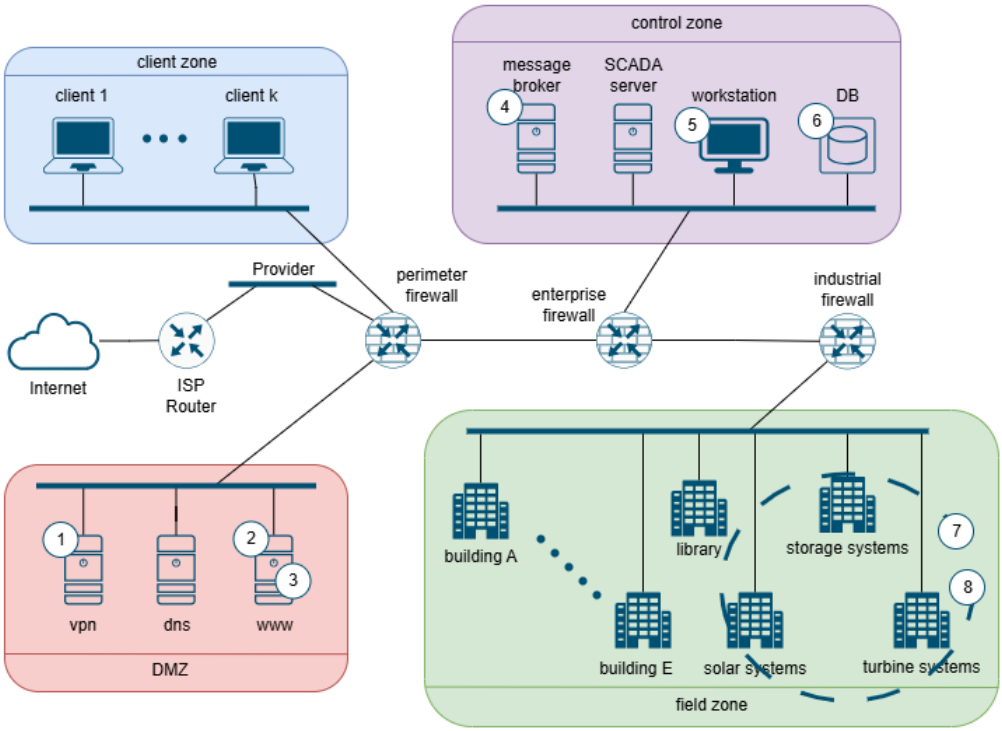

Fig. 1: Network infrastructure

No.	Vulnerability	Description
1	CVE-2017-12166	OpenVPN versions before 2.3.3 and 2.4.x before 2.4.4 are vulnerable to a buffer overflow vulnerability when key-method 1 is used, possibly resulting in code execution.
2	XSS Stored	It allows an attacker to inject malicious script into a web page, which is then executed when the victim visits that page.
3	RCE	The attacker is able to inject and execute arbitrary code in the vulnerable application.
4	CVE-2018-12551	Eclipse Mosquitto version 1.0 to 1.5.5 configured to use a password file for authentication, if contains malformed data these are considered valid. In particular, a blank line will be treated as a valid empty username.
5	CVE-2019-0708 CVE-2019-1181 CVE-2019-1182	A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability'. This vulnerability is pre-authentication and requires no user interaction.
6	CVE-2012-2122	sql/password.c in Oracle MySQL (specific versions [6]) allows remote attackers to bypass authentication by repeatedly authenticating with the same incorrect password.
7	CVE-2024-34026	A stack-based buffer overflow vulnerability exists in the OpenPLC Runtime EtherNet/IP (OpenPLC _v3 b4702061dc14d1024856f71b4543298d77007b88). Crafted EtherNet/IP request can lead to remote code execution.
8	CVE-2022-2081	If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot.

TABLE I: Table of Vulnerabilities in the Network Infrastructure

EXTERNAL NETWORK

Managed by a service provider.

CLIENT ZONE

It's composed of devices for the staff and students.

DMZ

It contains three servers:

- **VPN:** is modeled with OpenVPN with a version before 2.3.3 or after 2.4.x and before 2.4.4, in order to have the vulnerability CVE-2017-12166 [5];
- **DNS:** is modeled with BIND9;
- **WWW:** it exposes a web application with several vulnerabilities (e.g. RCE).

CONTROL ZONE

It's composed by:

- **SCADA server**
- **Message Broker:** it's implemented using a Mosquitto version 1.0 to 1.5.5 in order to have the vulnerability CVE-2018-12551 [7];
- **Workstation:** it's a Windows machine that is used by the staff in order to interact with the SCADA server. This machine contains a vulnerability of the Remote Desktop Protocol (CVE-2019-0708 [8], CVE-2019-1181 [9], CVE-2019-1182 [10] depending on the Windows version installed);
- **DB:** a MySQL (or MariaDB) database that is used by SCADA, for saving data. This database has a version that contains the vulnerability CVE-2012-2122 [6].

FIELD ZONE

This zone contains some buildings of the campus, the turbines and the storage system. For the IoT part there are some **PLCs modeled with OpenPLC** where some of them use the default credential and some other contains the vulnerability CVE-2024-34026 [11].

There is also the **ModBus protocol** that manages the controller PLCs. The protocol used in the Hitachi Energy's RTU500 series has this known vulnerability CVE-2022-2081 [12].

IV. Attack scenarios

In this section, will be exposed several scenarios of **possible attacks**. For some of them, there will be more than one possible attack vector, described in the last part of this section. Each scenario is associated with the attack tree representation. In each tree, all the sub-goals are considered with the OR operator except the ones with the curved arrow that are considered with the AND operator.

INFRASTRUCTURE TAKEOVER

The goal of the attacker will be the **infrastructure takeover**, taking control over the **Mosquitto broker**:

P1. From outside the network, the attacker must be capable of reaching the DMZ, in which can be found a **web server**. In the web server, **several vulnerabilities can be exploited** to gain control over it, for example a custom-made **RCE**;

P2. After gaining access to the *Control zone*, the attacker can exploit the **Mosquitto Broker vulnerability** [7], which allows to take control of it due to mishandling of the credentials file.

Leveraging this vulnerability can allow the attacker to **forge messages from the SCADA server to the PLCs**, to turn off the systems or over-use them, or forge messages from the PLCs systems, to **falsify the data** that the server will render to the SCADA management staff. This can lead to a falsified representation of reality, that can cause **potentially high damage**.

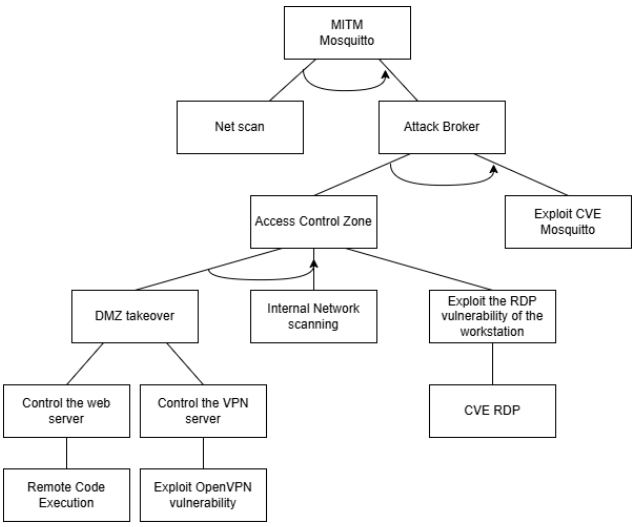

Fig. 2: Attack tree of the infrastructure takeover scenario

DoS OF PLCs

This scenario has the goal to cause a **Denial of Service attack to the PLCs** due to a vulnerability [12] in the ModBus protocol.
With this vulnerability it is possible to send specifically **crafted messages** to the PLCs at a high rate, causing the **reboot** of the PLCs. The phases of the attack could be carried out as follows:

P1. From outside the network, the attacker must be capable of reaching the DMZ zone, in which can be found a web server that contains an RCE vulnerability that allows the attacker to gain access to the server;
P2. At this point the attacker can exploit the ModBus vulnerability sending specific messages in order to cause the reboot of the PLCs.

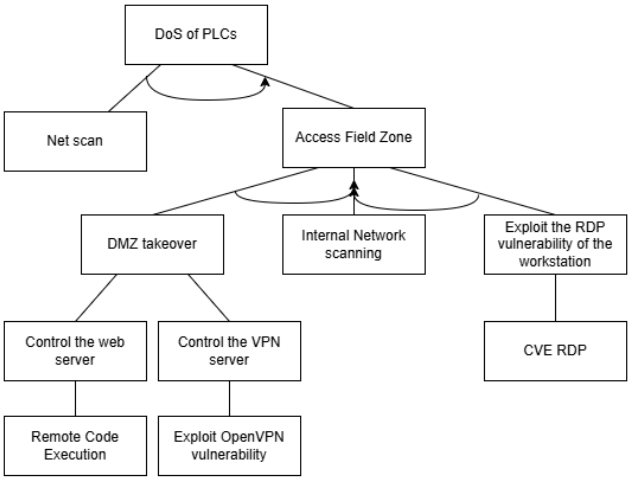

Fig. 3: Attack tree of the DoS of PLCs scenario

DATA EXFILTRATION

In this scenario the attacker can **exfiltrate sensitive data** that are stored into the DB used by the SCADA server.
The **database's vulnerability** [6] allows an attacker to bypass the authentication mechanism. The phases of the attack could be carried out as follows:

P1. From outside the network, the attacker must be capable of reaching the DMZ zone, in which can be found a web server that contains an RCE vulnerability that allows the attacker to gain access to the server;
P2. After gaining access to the network containing the DB, the attacker can exploit the vulnerability, repeating several times the authentication process with the same incorrect password.
Some examples of the exploit can be found here:
- Nmap script [13]
- Vulhub gitHub [4]
- rapid7 post [14]

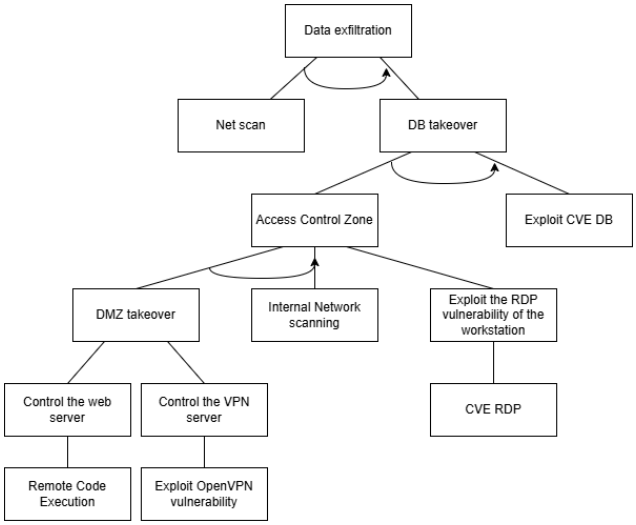

Fig. 4: Attack tree of the data exfiltration scenario

PLCs TAKEOVER

In this scenario, the attacker can take the control of the PLCs. The phases of the attack could be carried out as follow:

P1. From outside the network, the attacker must be capable of reach the DMZ zone, in which can be found a web server that contains an RCE vulnerability that allows the attacker to gain access to the server;
P2. At this point, the attacker can perform two different actions in order to take control of the PLCs:
- Some PLCs are developed with the **default credentials** and if are not changed by the administrator, the attacker can log-in into the PLC interface;
- Another solution is to use the **vulnerability** [11] **of OpenPLC** [15] that can lead to remote code execution. Other information for this exploit can be found here [16].

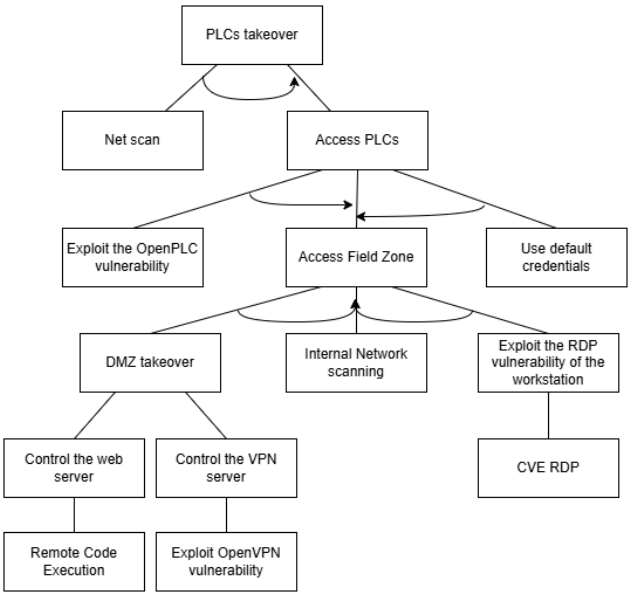

Fig. 5: Attack tree of the PLCs takeover scenario

WORKSTATION TAKEOVER

The goal of this scenario is to take control of the workstation in the *Control zone*.
This machine is running Windows with a vulnerable version for the **Remote Desktop Protocol** [8] [9] [10]. The RDP is used to let the staff to be able to connect to the workstation also from remote.
The attacker can exploit this vulnerability directly and **execute arbitrary code** in the workstation machine.

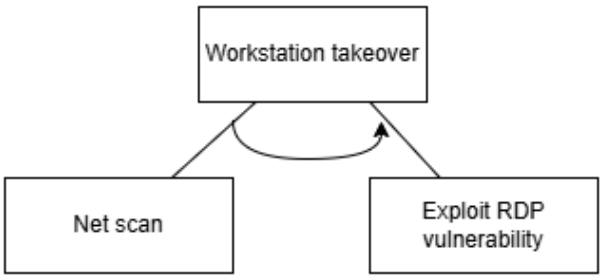

Fig. 6: Attack tree of the workstation takeover scenario

EXECUTION OF MALICIOUS CODE

In this scenario, the web server is exposing a service that allows a client user to provide a new paper, book or journal. This web application contains a **stored XSS vulnerability**:

P1. From outside the network, the attacker must be able to send a proposal paper, book or journal in a PDF format where the title contains an XSS payload;
P2. The application reads and displays the title of the documents proposed in the client web interface;
P3. When a client or some library staff interact with the web application and visualizes the list of proposed documents, they will **unconsciously execute malicious code**.

This exploitation process can be carried out by using some tools like **BeEF** [17] that can launch further attacks against the infected host.

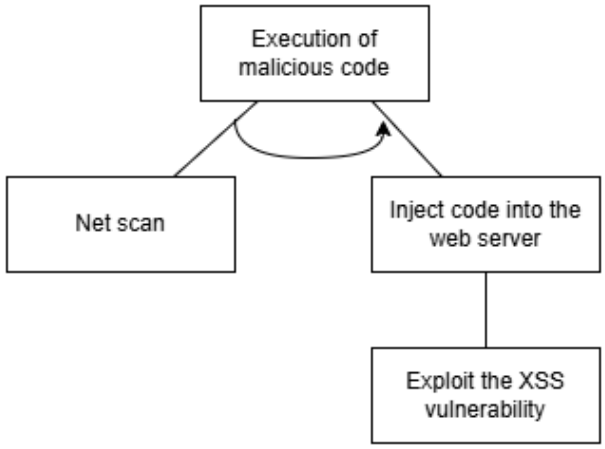

Fig. 7: Attack tree of the execution of malicious code scenario

NOTES

In each scenario described earlier, we assume that the **firewall's policies** have some **misconfigurations** that allow the traffic to pass. This can be carried out by implementing some rules in the **wrong way** or use **default credentials**, enabling the attacker to access the firewall dashboard and change some rules.

ALTERNATIVES

The first phase of each scenario can also be carried out by leveraging the VPN server's vulnerability or the remote desktop's vulnerability (in the workstation).

Server VPN vulnerability
The OpenVPN [18] server in the DMZ has a vulnerability [5] that can cause a remote code execution.

Remote Desktop vulnerability
The workstation in the *Control zone* has a vulnerability in the Remote Desktop Protocol that is described in the WORKSTATION TAKEOVER's section.

REFERENCES

[1] E. Russo, G. Costa, G. Longo, A. Armando, and A. Merlo, "Lidite: A full-fledged and featherweight digital twin framework," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 6, p. 4899–4912, Nov. 2023. [Online]. Available: http://dx.doi.org/10.1109/TDSC.2023.3236798

[2] ICSGoat, "Icsgoat : A damn vulnerable ics infrastructure." [Online]. Available: https://github.com/ine-labs/ICSGoat

[3] Docker, Inc., "Docker," 2025. [Online]. Available: https://docs.docker.com/get-started/docker-overview/

[4] Vulhub, "Vulhub github," 2024. [Online]. Available: https://github.com/vulhub/vulhub

[5] NIST, "CVE-2017-12166," NIST, Oct. 2017. [Online]. Available: https://nvd.nist.gov/vuln/detail/cve-2017-12166

[6] ——, "CVE-2012-2122," Oracle Corporation, Jun. 2012. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2012-2122

[7] ——, "CVE-2018-12551," Eclipse Foundation, Mar. 2019. [Online]. Available: https://nvd.nist.gov/vuln/detail/cve-2018-12551

[8] ——, "CVE-2019-0708," Microsoft Corporation, May 2019. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2019-0708

[9] ——, "CVE-2019-1181," Microsoft Corporation, Aug. 2019. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2019-1181

[10] ——, "CVE-2019-1182," Microsoft Corporation, Aug. 2019. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2019-1182

[11] ——, "CVE-2024-34026," Talos, Sep. 2024. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2024-34026

[12] ——, "CVE-2022-2081," Hitachi Energy, Jan. 2024. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2022-2081

[13] P. Calderon, "Script mysql-vuln-cve2012-2122." [Online]. Available: https://nmap.org/nsedoc/scripts/mysql-vuln-cve2012-2122.html

[14] H. Moore, "Cve-2012-2122: A tragically comedic security flaw in mysql," rapid7, Jun. 2012. [Online]. Available: https://www.rapid7.com/blog/post/2012/06/11/cve-2012-2122-a-tragically-comedic-security-flaw-in-mysql/

[15] Autonomy, "Openplc," 2025. [Online]. Available: https://autonomylogic.com/

[16] J. Rittle, "Openplc openplc_v3 openplc runtime ethernet/ip parser stack-based buffer overflow vulnerability," Cisco Talos, Sep. 2024. [Online]. Available: https://talosintelligence.com/vulnerability_reports/TALOS-2024-2005

[17] beefproject, "The browser exploitation framework project," beefproject. [Online]. Available: http://beefproject.com/

[18] OpenVPN, "Openvpn," 2025. [Online]. Available: https://openvpn.net/community-resources/how-to/