

Article

Study the Level of Network Security and Penetration Tests on Power Electronic Device

Ivan Nedyalkov 

Faculty of Engineering, South-West University “Neofit Rilski”, 2700 Blagoevgrad, Bulgaria; i.nedqlkov@swu.bg

Abstract: This work demonstrates the feasibility of using Kali Linux in the process of power electronic device research. The novelty in this work is the use of Kali Linux in the process of power electronic device research. This operating system is mainly used for the penetration testing of various communication devices but not for power electronic device research. The aim of this work is to study the level of network security (the type of security vulnerabilities that a power electronic device has) and whether the data exchange between the power electronic device and the monitoring and control center is secure. Additionally, penetration testing has been carried out. Kali Linux was used to implement these tasks. Penetration testing was performed to verify how the studied power electronic device reacted to various TCP DoS attacks—could it be accessed, was it blocked, etc. Kali Linux and some of the tools built into the operating system—Nmap, hping3, Wireshark, Burp Suite Community Edition—were used for this study. During the penetration tests, a characterization of the traffic being processed/generated by the studied power electronic device was carried out to evaluate and analyze what impact each TCP DoS attack had on the device’s performance. In order to conduct the study, an experimental setup was designed. This experimental network was not connected to other networks, so the cyber attacks were controlled and confined within the experimental network. The research carried out validated the use of Kali Linux for the study of power electronic devices. From the obtained results, it is found that the studied power electronic device provides a certain level of network security, but the data exchange is insecure.

Keywords: cyber security; hping3; Kali Linux; network monitoring; network security; Nmap; penetration testing; power electronic devices; TCP DoS flood attacks



Citation: Nedyalkov, I. Study the Level of Network Security and Penetration Tests on Power Electronic Device. *Computers* **2024**, *13*, 81. <https://doi.org/10.3390/computers13030081>

Academic Editor: Pedro Alonso Jordá

Received: 27 February 2024

Revised: 13 March 2024

Accepted: 14 March 2024

Published: 19 March 2024



Copyright: © 2024 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The research related to power electronic devices (PEDs) is mainly aimed at creating new circuit solutions or improving existing ones, as well as at improving the efficiency of PEDs, improving the switching of power elements, etc. [1–11]. In the last few years, the research related to renewable energy sources, electric vehicles, and energy storage cells has also been increasing due to their rapid integration into people’s daily lives. These studies are focused on contactless energy transmission, energy flow control, battery–supercapacitor co-operation, etc. [12–23]. All of these studies are very important for the development of PEDs, and their results contribute to the technological development of PEDs.

With the addition of the possibility of connecting PEDs to IP networks and especially to the Internet, PEDs can be remotely controlled, and certain parameters can be monitored. With PEDs being connected to the Internet, the danger of various cyber attacks appears. That is why, now, research focused on the communication capabilities of PEDs—the characterization of the generated communication traffic and penetration testing—is of great importance. Currently, there are few studies of this type on power electronic devices. Therefore, this work presents this type of research.

Power distribution units (PDUs) are devices that are used to manage the power supply to various communication devices—network devices, servers, etc. PDUs can be conventionally divided into two groups. Basic PDUs cannot be controlled but make

various measurements related to the power supply (the value of the voltage, current, power consumption, etc.) or to external parameters such as the temperature, humidity, etc. Intelligent PDUs have additional functionalities that can be used to remotely control the individual power outlets that are used as a power supply for the various devices; they can remotely turn the individual outlets on/off (when there are no devices connected to them) or remotely hard-restart plugged-in devices (when it is not possible to restart the communication devices using their own commands). PDUs are part of the power electronics group. Through them, energy flows can be managed (distributing energy from one power source to all consumers) evenly and efficiently between all devices that are connected to the PDU. Inverters, PV controllers, and other power converters and power supplies perform the same functions. Just like the power converters, the switches in the PDU are made of power transistors that control the switching between the two states (on–off). Older PDU models use a combination of relay and power transistors to provide galvanic contact isolation and relay contact “welding” protection.

The aim of this work was to study the security vulnerabilities of an intelligent power distribution unit (PDU), find out whether the exchange of data is secure, and conduct penetration testing (the PDU was subjected to various TCP DoS attacks). All of this was achieved by using some of the built-in tools of Kali Linux; this is the novelty of this work. Additionally, the proposed research methodology is easy to implement. Notwithstanding its simplicity, the methodology is effective. The motivation behind this work was to demonstrate that Kali Linux can be used in the process of power electronic device research. This type of study had not previously been performed, as Kali Linux is generally used for the penetration testing of network communication devices. This work will enrich the research related to the communication capabilities of power electronic devices. In addition, this work will extend the application of Kali Linux into another area that is not specific to Kali Linux—the use of the operating system for studying power electronic devices.

2. Article Structure and Table of Acronyms

This article has the following structure:

- Section 1—Introduction. Here, we present a brief description of the state of the problem under consideration;
- Section 2—Structure of the article;
- Section 3—Related work. Here, we present a review of various works that are related or very close to the problem discussed in this practical study;
- Section 4—Experimental setup and the tools and research methodology used. Here, we explain the setup, the tools used, and the research methodology;
- Section 5—Results. Here, we present the results obtained from the study;
- Section 6—Discussion and analysis of the obtained results;
- Section 7—Conclusions.

The abbreviations and definitions used in the text are listed in Table 1.

Table 1. List of abbreviations used in the text.

Abbreviation	Definition	Abbreviation	Definition
TCP	Transmission Control Protocol	DoS	Denial of Service
PED	Power Electronic Device	PDU	Power Distribution Unit
IP	Internet Protocol	DC	Direct Current
Wi-Fi	Wireless Fidelity	RTD	Round Trip Delay
HTTP	Hyper Text Transfer Protocol	ICMP	Internet Control Message Protocol
VLAN	Virtual Local Area Networks	VPN	Virtual Private Network
HTML	Hyper Text Markup Language		

3. Related Work

In [24], the authors consider vulnerabilities in low-voltage networks and what would happen to a network when it is subjected to a cyber attack. In this work, the authors have conducted an in-depth analysis of the risk of cyber attacks on the low voltage network and what the results of these attacks would be.

In [25], the authors look at possible cyber attacks and how they affect the performance of smart meters. In particular, an overview is given of the security vulnerabilities in the Internet of Things (IoT) that could cause harm to people using such meters.

In [26], the authors propose a testbed that includes a hardware simulation of power system operations, real-time data collection and management using the OSIsoft PI system, and a common set of power management devices. Additionally, the authors provide a discussion of the capabilities of this simulator for supply chain cybersecurity. The simulator is used to emulate the operation of a remote terminal module, a supplier, a utility company, and an attacker that performs a malicious operation on the power system.

In [27], the authors propose a model of overcurrent protective relay that is compatible with IEC 61850 communication standard. The model is open source and integrates the behavioral interactions between protective relays and their physical, communication, and cybersecurity operations. For validation purposes, the authors have developed a model of a transmission substation in MATLAB/Simulink®. The impact of the communication operations and cybersecurity threats on physical relay operations has been studied under different case studies and attack scenarios.

In [28], the authors provide an in-depth literature review of the vulnerabilities, countermeasures, and test environments associated with Grid-Connected Power Electronics Converters (GCPECs). From the review and the analysis, it is found that GCPEC vulnerabilities include both cyber and physical layers that are easily accessible to malicious hackers. These vulnerabilities must be considered simultaneously. Finally, based on the review and the analysis, the authors derive four recommendations for future research on the cybersecurity of GCPECs and their applications in smart grids.

In [29], the authors propose a novel deep learning method for False Data Injection Attack (FDIA) detection. In the proposed method, Convolutional Long Short-Term Memory (ConvLSTM) is applied as an extractor to capture the inherent dynamic features and spatiotemporal correlations of the smart grid. Furthermore, a self-monitoring (SA) mechanism is introduced to realize efficient FDIA detection in smart grids under uncertain power fluctuations. The experiments show that the proposed method outperforms most existing technologies in terms of detection rate and robustness.

In [30], the authors review the cybersecurity best practices of smart inverters. The authors consider emerging cyber threats to smart inverters, including malware attacks and hardware attacks. Finally, they propose a new security and resilience method for protecting smart inverters as well as cyber-resilient smart inverters against advanced/future threats.

In [31], the authors propose a supervised artificial intelligence (SAI)-based control strategy to secure the DC link in a single-phase dual active bridge (SP-DAB) converter against cyber attacks. The proposed approach involves developing an automated learning system and fine-tuning the SAI model to detect and remediate cyber attacks based on erroneous voltage and power output values of the DC link of the converter. To further verify the capability of the proposed strategy, the authors applied different forms of malicious data including standing data, triangle waves, and sine waves. To show that the method is effective in detecting and removing cyber attacks on the DC link of the DAB converter, the proposed method is evaluated with the use of simulations in the MATLAB/SIMULINK environment.

Additional work by other authors can be reviewed in [32–48]. As can be seen from the review, the use of Kali Linux [49] in the process of studying the network security level of PEDs has not been proposed. Kali Linux is basically used for the penetration testing of various IP network communication devices. The use of Kali Linux in power electronic device studies is not popular. Therefore, this work is innovative and presents how the

built-in tools of Kali Linux can be used to carry out various studies related to finding security vulnerabilities and studies related to the penetration testing of PEDs.

4. Experimental Setup, Used Tools, and Research Methodology

4.1. Experimental Setup

Figure 1 presents the experimental setup for studying the network security level and penetration testing of the tested PED. The experimental setup consists of a workstation with Kali Linux installed on it. “Kali Linux” and the “Monitoring center” are connected to the “Studied PDU” using Wi-Fi technology. The experimental network is closed and it is not connected to the Internet. The managed switch is connected to the wireless router. The studied PED and the mobile workstation are connected to this switch. A managed switch is chosen to be used due to the support of the mirror port feature. Due to this functionality, all the traffic that is handled by the switch is copied to this port. The mobile workstation is connected to this port and, with the installed monitoring tools, it monitors the traffic exchanged between the PED and the monitoring center.

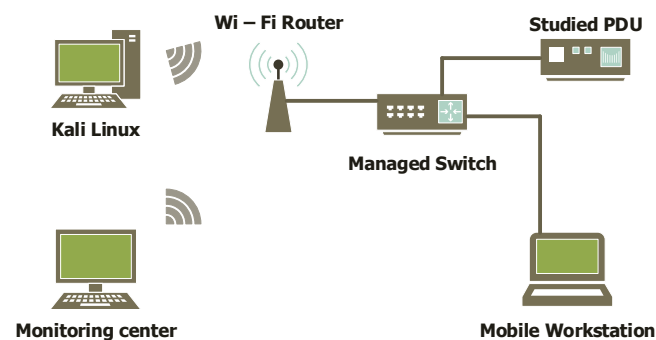


Figure 1. Experimental setup.

4.2. Used Tools

Several tools for network security testing and traffic monitoring were used for the study, such as:

- Network analyzer: Colasoft Capsa free (version 11.1) was used [50]. It is a network analyzer through which various parameters can be monitored, such as generated traffic, number of TCP packets, traffic generated by protocols, etc.;
- Nmap (version 7.94): This is a tool that is used for discovering the security vulnerabilities of various communication devices. In addition, this tool has a different set of scripts through which it finds out the most common cybersecurity vulnerabilities of the devices [51];
- hping3 (version 3.0.0): This is a tool for creating and sending custom TCP/IP packets. The tool can be used to perform additional tasks such as network scanning, network security testing, etc. Different types of TCP DoS attacks can be simulated with hping3, making it a valuable tool for testing the network security of different devices [52];
- Wireshark (version 4.0.7): This is a network protocol analyzer that “captures” all packets that are exchanged between communication devices. These captured packets can then be examined and analyzed extensively. This tool can also be used to find out whether the data exchange between communication devices is secure [53];
- Burp Suite Community Edition (version 2023.9.1): This tool is used to test/study the security of applications. It can also be used to find out whether the data exchange is secure [54];
- The Colasoft ping tool (version 2.0) [55] is used to measure the round-trip delay (RTD) between the monitoring center and the studied PDU in the experimental network;
- Mathematical distributions for packet size: The purpose of these distributions is to graphically represent the percentage packet size distribution of individual packets relative to the total number of packets [56,57].

4.3. Research Methodology

For the purpose of this study, an Intelligent Power Distribution Unit (PDU) will be studied. It is used by telecommunication operators to manage the power supply of their network communication devices. The tested PDU can manage the power supply of up to 8 communication devices. It is also possible to connect additional sensors to monitor the temperature and/or the humidity in the room where the communication equipment is located.

The present study is conventionally divided into two parts. In the first part, studies were carried out to find out what the security vulnerabilities of the tested PDU are, as well as finding out whether the data exchange between the tested PDU and the command and control center is secure. In the second part, studies were carried out to find out how the studied PDU responds to various TCP DoS attacks, i.e., penetration testing.

The sample interval of the Colasoft Capsa was set to 1 s. Thus, more accurate measurements would be obtained. The scan range of Nmap and hping3 was set for all possible ports from 1 to 65,535. Thus, the whole port range would be scanned and no ports would be missed. hping3 was also used for the penetration testing. The size of the TCP packets during the various attacks was configured to be 1024 bytes. This is the maximum packet size at which Wireshark operates normally. When a larger packet size is set, the Wireshark, which is running on the Mobile Workstation, “freezes” (not responding) and cannot operate normally. Packets are sent approximately every 10 μ s. The duration of each attack is 10 min. This packet size was chosen to be able to study whether the PDU can process packets of this size and how these packets affect the network operability of the PDU.

Finally, the results were analyzed and a summary assessment of the network security level was made.

5. Results

5.1. Studying the Level of Network Security

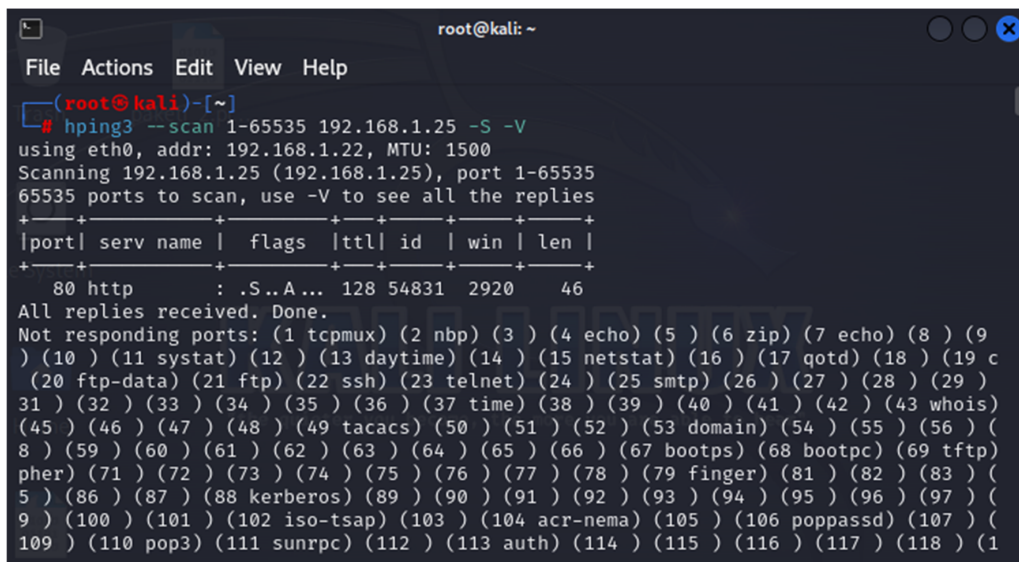
In the first part of this study, port scanning for open ports was performed. Such a study is of particular importance because it is the first level of defense of a communication device. Every hacker does this first—scanning for open ports through which he can “enter” the system or the communication device. For the purpose of this study, the Nmap and hping3 tools were used.

Figure 2 presents the results of the port scanning. The command “-sS” means that the Nmap port scanner uses the TCP protocol and the 3-way handshake procedure. The IP address of the studied PDU is 192.168.1.25. As can be seen from the results, the only open port is port 80 (http), which is used for remote access to the studied PDU.

```
root@kali: ~  
File Actions Edit View Help  
  
(root@kali)-[~]  
└─# nmap -sS -p 1-65535 192.168.1.25  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 18:03 EET  
Nmap scan report for 192.168.1.25  
Host is up (0.0040s latency).  
Not shown: 65534 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
80/tcp    open  http  
MAC Address: EC:F2:36:00:49:3F (Neomontana Electronics)  
  
Nmap done: 1 IP address (1 host up) scanned in 104.99 seconds  
  
(root@kali)-[~]  
└─#
```

Figure 2. Nmap output.

Figure 3 presents the results of the scanning for open ports by using the hping3. As can be seen from the figure, it is similar to the Nmap result. The only open port is 80; the rest are closed.



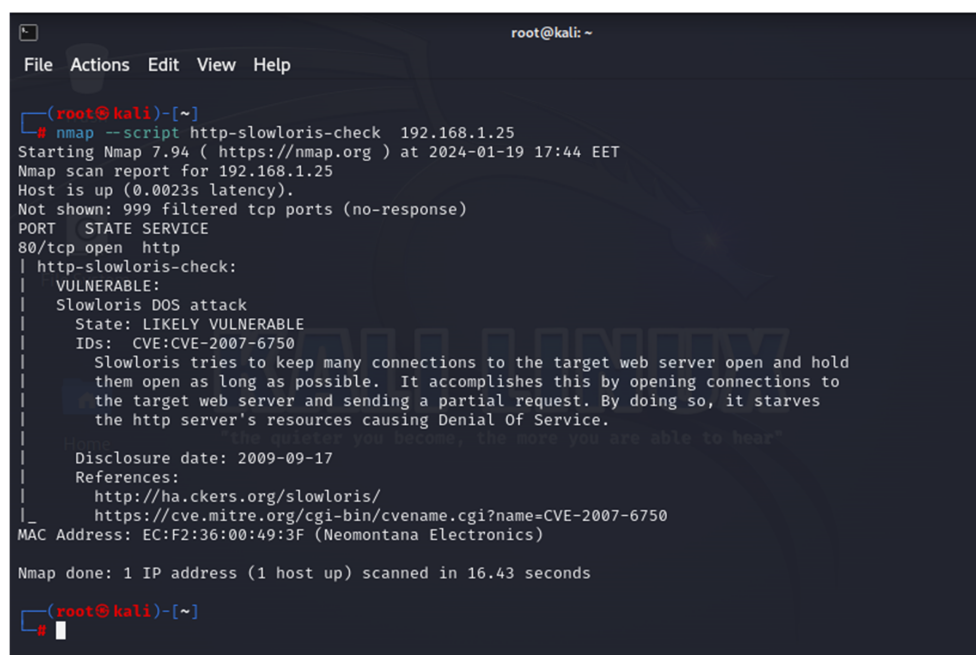
```

root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
# hping3 --scan 1-65535 192.168.1.25 -S -V
using eth0, addr: 192.168.1.22, MTU: 1500
Scanning 192.168.1.25 (192.168.1.25), port 1-65535
65535 ports to scan, use -V to see all the replies
+-----+-----+-----+-----+-----+-----+
|port| serv name | flags |ttl| id | win | len |
+-----+-----+-----+-----+-----+-----+
80 http      : .S..A... 128 54831 2920 46
All replies received. Done.
Not responding ports: (1 tcpmux) (2 nbp) (3 ) (4 echo) (5 ) (6 zip) (7 echo) (8 ) (9
) (10 ) (11 systat) (12 ) (13 daytime) (14 ) (15 netstat) (16 ) (17 qotd) (18 ) (19 c
) (20 ftp-data) (21 ftp) (22 ssh) (23 telnet) (24 ) (25 smtp) (26 ) (27 ) (28 ) (29 )
31 ) (32 ) (33 ) (34 ) (35 ) (36 ) (37 time) (38 ) (39 ) (40 ) (41 ) (42 ) (43 whois)
(45 ) (46 ) (47 ) (48 ) (49 tacacs) (50 ) (51 ) (52 ) (53 domain) (54 ) (55 ) (56 ) (
8 ) (59 ) (60 ) (61 ) (62 ) (63 ) (64 ) (65 ) (66 ) (67 bootps) (68 bootpc) (69 tftp)
pher) (71 ) (72 ) (73 ) (74 ) (75 ) (76 ) (77 ) (78 ) (79 finger) (81 ) (82 ) (83 ) (
5 ) (86 ) (87 ) (88 kerberos) (89 ) (90 ) (91 ) (92 ) (93 ) (94 ) (95 ) (96 ) (97 ) (
9 ) (100 ) (101 ) (102 iso-tsap) (103 ) (104 acr-nema) (105 ) (106 poppassd) (107 ) (
109 ) (110 pop3) (111 sunrpc) (112 ) (113 auth) (114 ) (115 ) (116 ) (117 ) (118 ) (1

```

Figure 3. hping3 output.

Nmap has the ability to use special scripts that can be used for finding out if specific vulnerabilities are present on the studied device [58]. Figure 4 shows the result of using the “http-slowloris-check” script. This script is used to find out whether the studied PDU is vulnerable to DoS attacks, without such attacks being performed. The result “LIKELY VULNERABLE” means that the studied PDU was subject to an attack but, depending on the architecture of the used inner http server and the resource constraints, a complete denial of service is not always possible. Carrying out complete testing requires the application of actual DoS attacks and studying the server response of the studied PDU. Such studies are presented in Section 5.2.



```

root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
# nmap --script http-slowloris-check 192.168.1.25
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 17:44 EET
Nmap scan report for 192.168.1.25
Host is up (0.0023s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.
|
| Disclosure date: 2009-09-17
| References:
| http://ha.ckers.org/slowloris/
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
| MAC Address: EC:F2:36:00:49:3F (Neomontana Electronics)
Nmap done: 1 IP address (1 host up) scanned in 16.43 seconds
(root@kali)-[~]
#

```

Figure 4. Output from the “http-slowloris-check” script.

Figure 5 shows the result of running the “vuln” script. Using this script activates all vulnerability testing scripts in the Nmap library. As can be seen from the result, the only vulnerability discovered was one that was already known about.

```

root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
└─# nmap --script vuln 192.168.1.25
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 18:43 EET
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).
Nmap scan report for 192.168.1.25
Host is up (0.0029s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|     Slowloris tries to keep many connections to the target web server open and hold
|     them open as long as possible.  It accomplishes this by opening connections to
|     the target web server and sending a partial request.  By doing so, it starves
|     the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
MAC Address: EC:F2:36:00:49:3F (Neomontana Electronics)

Nmap done: 1 IP address (1 host up) scanned in 66.04 seconds
(root@kali)-[~]
└─#

```

Figure 5. Output from the “vuln” script.

Some of the built-in tools of Kali Linux can be used to find out whether the exchanged information is secure or not and, if it is secure, to identify the security level. For this study, the Wireshark and the Burp Suite Community Edition were used.

Figure 6 shows a sample of one of the captured packets that was exchanged between the studied PDU (192.168.1.25) and Kali Linux (192.168.1.22), acting as the management and monitoring station. The figure shows an unpacked packet, which was used for exchanging user credentials, that allows remote access to the PDU. As can be seen, the password and username were encoded and transmitted using only Base64, which is very easy to decode, as shown by the result. Wireshark immediately decodes the encoded username and password and shows what they actually are.

Figure 7 shows how the data were exchanged when the username and password were about to be changed—the account management page of the studied PDU was open. As can be seen, when the changing username and password page was opened, the information was transmitted in plain text.

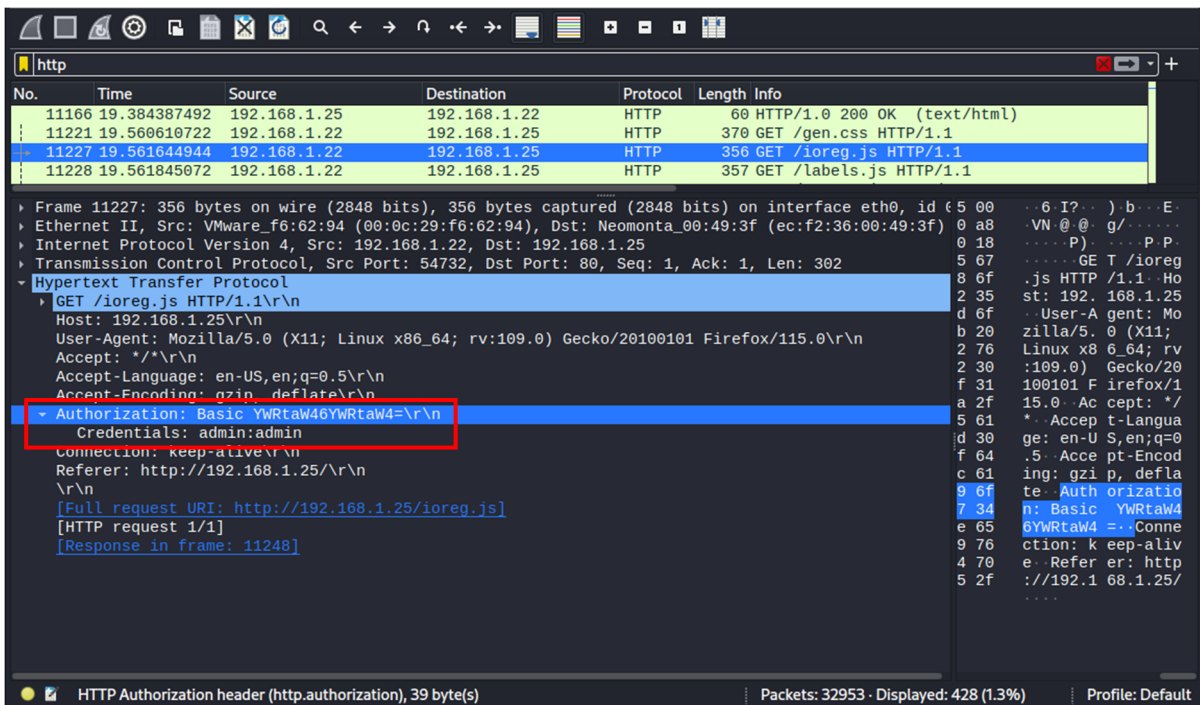


Figure 6. Output from Wireshark showing the password and the username.

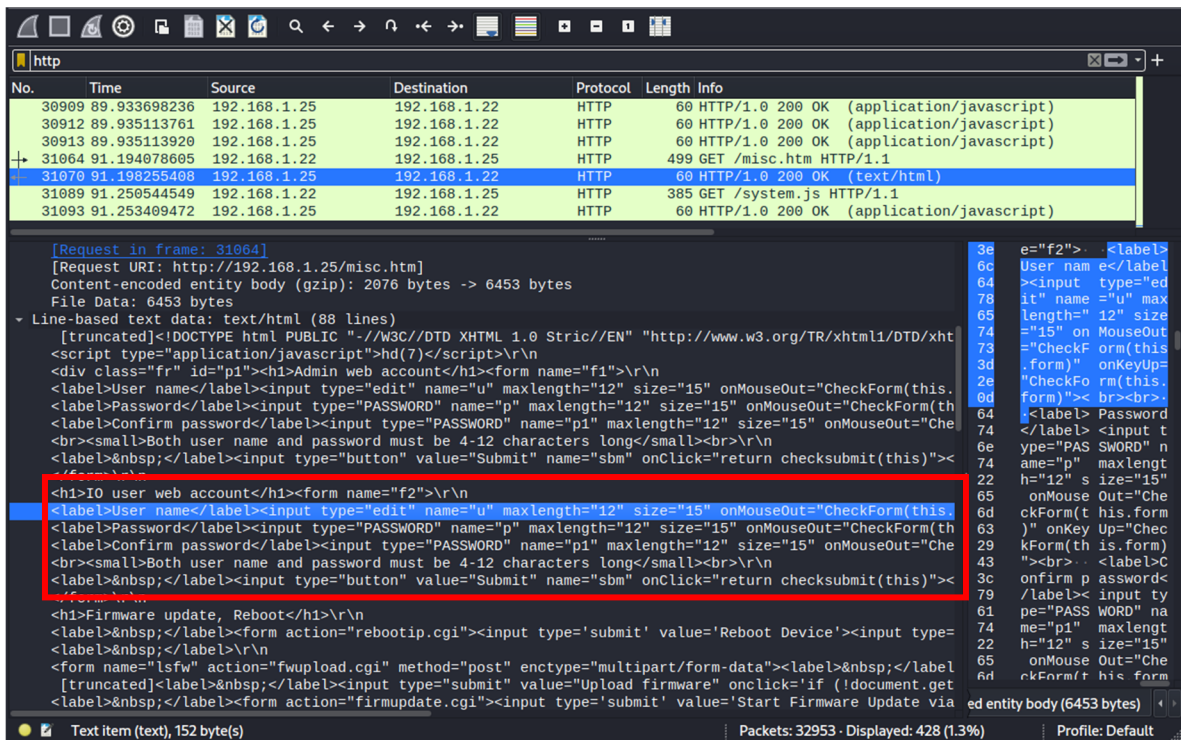


Figure 7. Output from Wireshark showing the source code for the user web account.

The Burp Suite Community Edition was used to validate the results obtained from Wireshark. Figure 8 presents a result that confirms the results obtained with Wireshark about the way the username and password were exchanged.

The screenshot displays the Burp Suite interface. The top menu includes Burp, Project, Repeater, View, and Help. The main toolbar contains Dashboard, Target, Proxy, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. The Site map shows a single target at http://192.168.1.25. A table of requests is visible, with columns for Host, Method, URL, Params, Status code, Length, MIME type, and Title. The selected request is a GET to /misc.htm with a status code of 200 and a length of 6633. The Request/Response pane shows the following details:

```

Request
1 GET / HTTP/1.1
2 Host: 192.168.1.25
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: rf=0; sh=0
9 Upgrade-Insecure-Requests: 1
10 Authorization: Basic YWRtaW46YWRtaW4=
11
12
Response
15 (0xf)
Selected text
YWRtaW46YWRtaW4
Decoded from: Base64
admin:admin
Request attributes: 2
Request cookies: 2
Request headers: 9

```

Figure 8. Output from the Burp Suite Community Edition showing the password and the username.

Figure 9 shows how the information was exchanged when the page where the administrator's username and password can be changed was opened. Again, the information was transmitted in plain text. Additional methods, techniques, and technologies need to be applied to secure the studied device from unauthorized access. Such methods, techniques, and technologies are discussed in [59–63].

The screenshot displays the Burp Suite interface with the Logger tab selected. The main toolbar includes Dashboard, Target, Proxy, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. The Logger filter is set to 'Showing all items'. A table of log entries is visible, with columns for #, Time, Tool, Method, Host, Path, Query, Param count, Status code, Length, Start response timer, and Comment. The selected log entry is a GET request to /misc.htm with a status code of 200 and a length of 6633. The Request/Response pane shows the following details:

```

Request
1 GET /misc.htm HTTP/1.1
2 Host: 192.168.1.25
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Basic YWRtaW46YWRtaW4=
8 Connection: close
9 Referer: http://192.168.1.25/aevents.htm
10 Cookie: rf=0; sh=0
11 Upgrade-Insecure-Requests: 1
12
13
Response
Admin web account
</h1>
<form name="f1">
<label>
User name
</label>
<input type="text" name="u" maxlength="12" size="15" onmouseover="CheckForm(this.form)" onkeyup="CheckForm(this.form)">
<br>
</label>
Password
</label>
<input type="password" name="p" maxlength="12" size="15" onmouseover="CheckForm(this.form)" onkeyup="CheckForm(this.form)">
<br>
</label>
Confirm password
</label>
<input type="password" name="p1" maxlength="12" size="15" onmouseover="CheckForm(this.form)" onkeyup="CheckForm(this.form)">
<br>
<small>
Both user name and password must be 4-12 characters
long
</small>

```

Figure 9. Output from the Burp Suite Community Edition showing the source code for the admin web account.

5.2. Penetration Testing

The hping3 tool was used to find out the response of the studied PDU when subjected to different types of TCP DoS attacks.

Figure 10 represents the communication traffic proceeded by the studied PDU. This graph represents the processed traffic during normal operation mode. The device was not under attack. The results were obtained from Capsa Colasft Free. As can be seen, the traffic was minimal, which is normal for the PEDs. This graph will be used as a reference graph for comparison with the following results, which were at times when the device was subjected to various TCP DoS attacks.

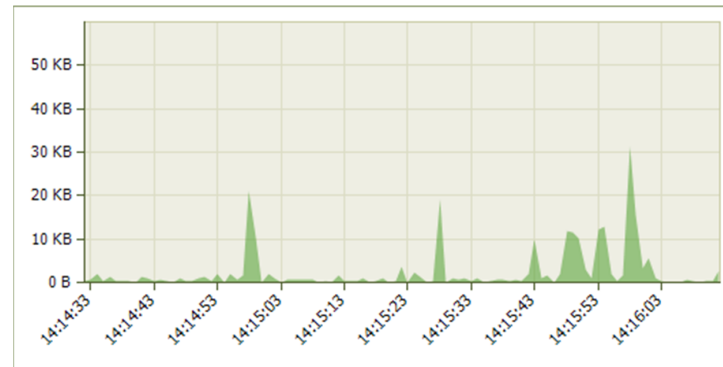


Figure 10. Processed traffic from the PDU during normal operation.

Figure 11 shows the distribution of the different TCP packets. Again, the results were obtained from Capsa Colasft Free. Again, these graphs represent the normal mode of operation. The graphs will be used as a reference for comparison with the following results. As can be seen from the graphs, the values of the different TCP packets for the studied device were normal. Since the PDU was only accessed by a browser, a continuous exchange of TCP packets was therefore required to maintain the HTTP session. As can be seen from the graph, there were TCP SYN and TCP SYNACK packets as well as TCP FIN packets. This is evidence of a successful three-way handshake, a completed TCP session with data exchange and termination of the TCP session after the data exchange was completed.

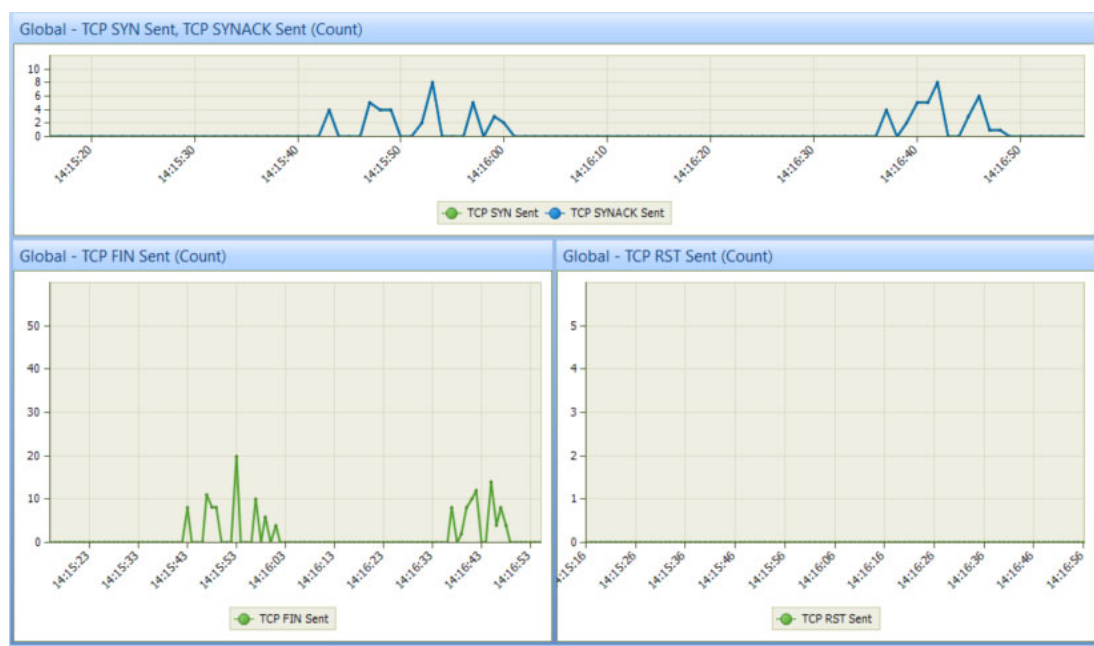


Figure 11. TCP packets during normal operation.

5.2.1. TCP SYN Flooding

This TCP DoS attack consists of flooding the attacked device with TCP requests that the attacked device cannot respond to because it is continuously flooded with more and more TCP requests [64].

Figure 12 represents the traffic being handled by the studied PDU. As can be seen from the graph, the amount of traffic it processed was huge compared to the normal operation mode. This is because the device was flooded with a huge number of TCP requests. This is what a TCP Syn flood attack looks like, in terms of traffic load.

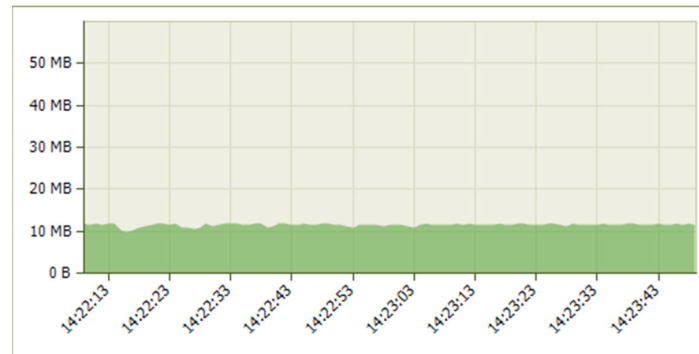


Figure 12. Processed traffic from the PDU during TCP SYN flood attack.

Figure 13 shows the values of the different TCP packets. As can be seen from the graph, the number of the TCP SYN packets sent was huge. Compared to the normal mode of operation, the number of the TCP SYN packets was constantly around 10,000. Zero TCP SYNACK packets were sent because the PDU cannot send such packets to the device requiring TCP session establishment (the Kali Linux attacker). This is a perfect example of a TCP SYN flood attack. There were some TCP RST packets that were generated by the embedded web server that attempted to interrupt the session, but the TCP SYN packets were much more numerous and the three-way handshake could not be interrupted. The device was unreachable.

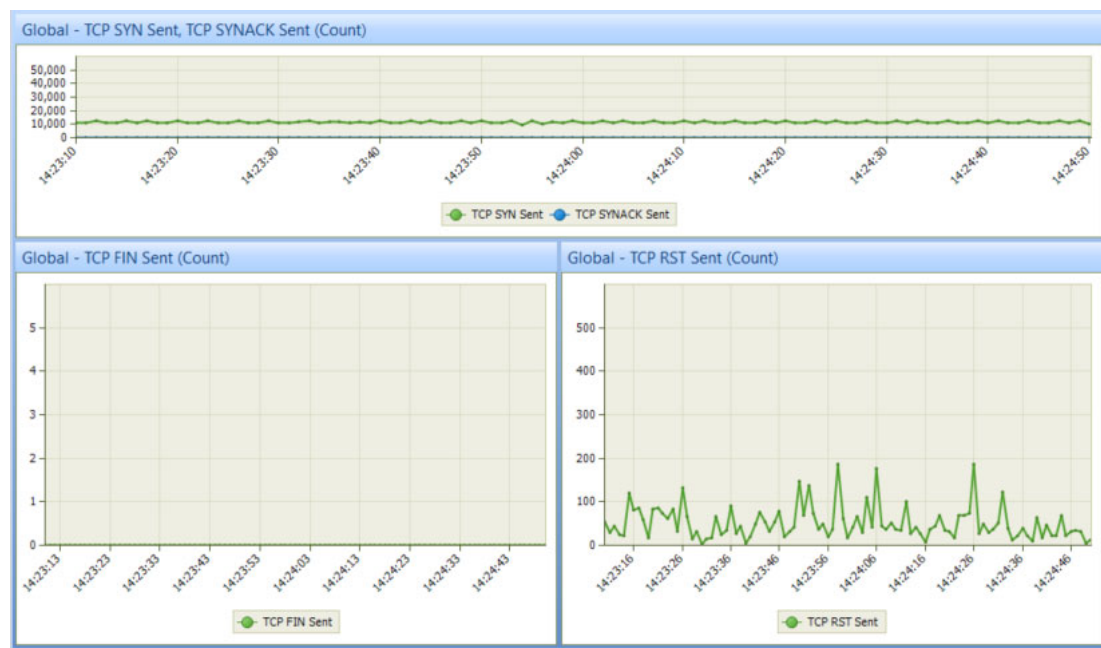


Figure 13. TCP packets during the TCP SYN flood attack.

5.2.2. TCP ACK Flooding

In this attack, the attacked device is flooded with TCP ACK packets. These packets are exchanged during a three-way handshake and are used to confirm that the device has received the TCP SYN packet and is ready to establish a TCP session with the other device that sent the TCP SYN packets [65].

Figure 14 represents the traffic being processed by the PDU during the attack. As can be seen from the graph, the result for the amount of the processed traffic is the same as that of the traffic that was processed during the TCP SYN attack. The traffic was constant.

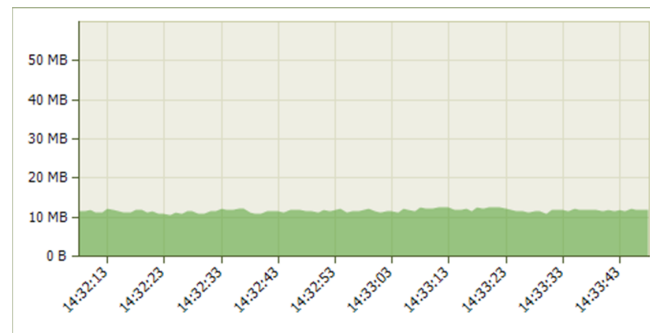


Figure 14. Processed traffic from the PDU during TCP ACK flood attack.

Figure 15 represents the values of the individual TCP packets during the attack. There was a huge increase in the TCP RST packets that were generated by the PDU. This increase was due to the TCP ACK attack, where a huge number of TCP ACK packets were sent but there were no TCP SYN packets. Therefore, the internal web server was generating TCP RST packets to terminate the session. The interesting thing to mention here is that, during the TCP ACK attack, the PDU was accessed remotely. This is evidenced by the presence of the TCP SYN sent packets and the presence of the TCP SYNACK sent packets, through which the TCP session establishment was confirmed. The presence of the TCP FIN packets, which terminate the TCP session after the data exchange has completed, proves the successful remote access of the PDU.

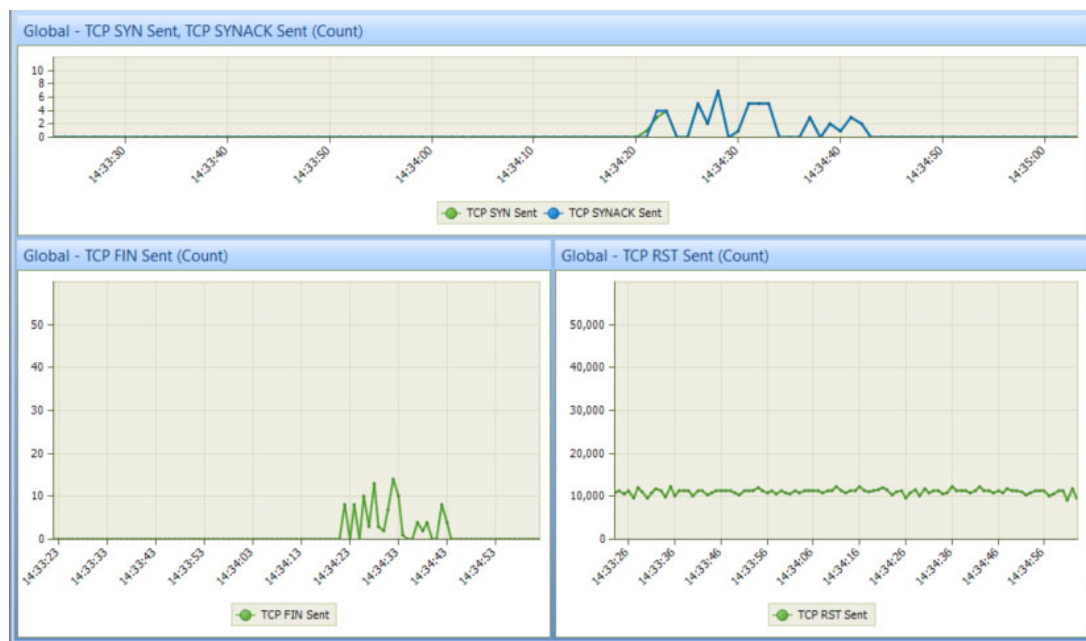


Figure 15. TCP packets during the TCP ACK flood attack.

5.2.3. TCP RST Flooding

TCP RST flood is a type of DDoS attack that aims to disrupt network connectivity/connection by flooding the bandwidth and computational resources of the attacked device by continuously sending TCP RST packets. This stream of packets can also be used as a deflection attack in more sophisticated attacks [66].

Figure 16 shows the traffic that the PDU had to process during this attack. The results were the same as in the previous attacks.

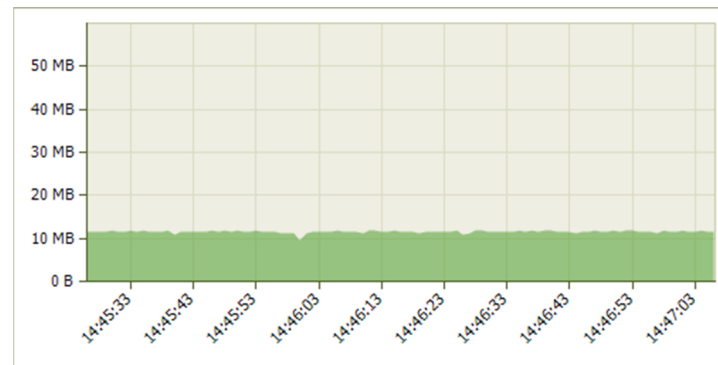


Figure 16. Processed traffic from the PDU during TCP RST flood attack.

Figure 17 shows the values of the individual TCP packets during the attack. There was a tremendous increase in the number of TCP RST packets that were generated by the PDU; this is the result of the attack. The internal web server of the studied PDU detects a problem with the session and the web server generates TCP RST packets to terminate the problematic session. The interesting thing observed during this attack was that the PDU is remotely accessed without any problem. This is evidenced by the successful three-way handshake—the presence of the TCP SYN, the TCP SYNACK packets, and the presence of the TCP FIN packets, which terminate a successfully completed TCP session.

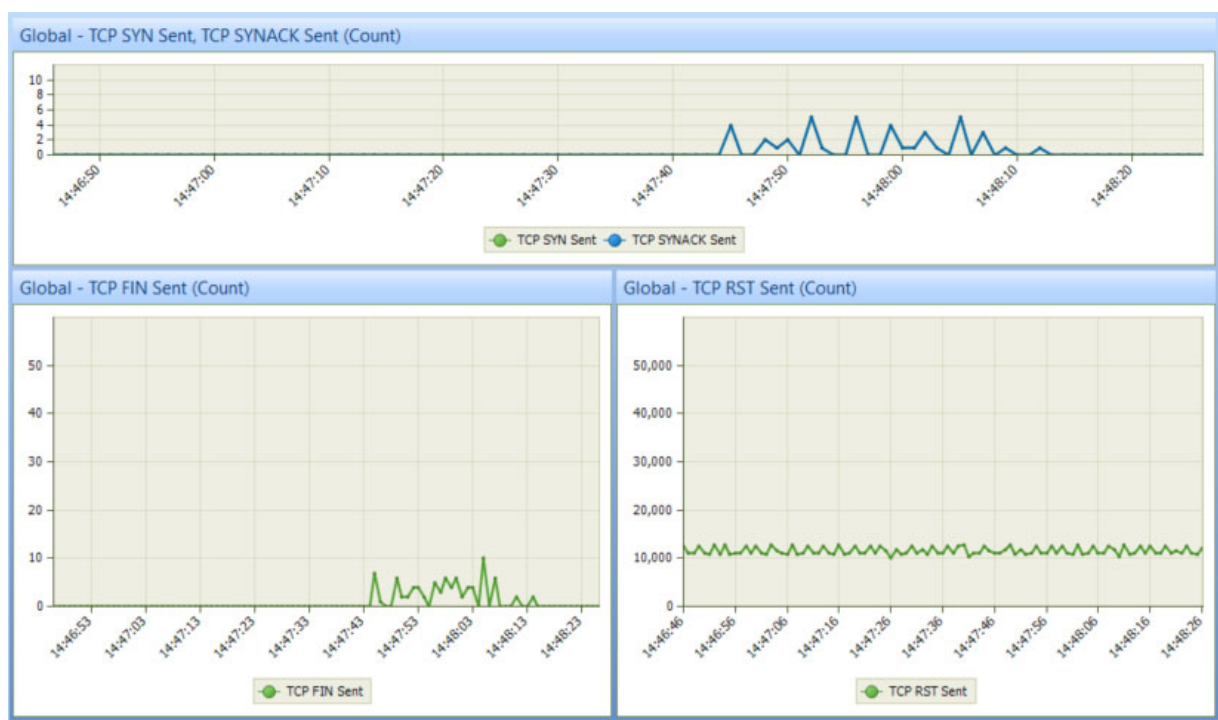


Figure 17. TCP packets during the TCP RST flood attack.

5.2.4. TCP FIN Flooding

In a TCP FIN flood attack, a victim receives a stream of TCP FIN packets that are not associated with any of the already-established TCP sessions in the attacked device's database. When a device is the target of a TCP FIN attack, it is forced to dedicate a significant portion of its computational resources to processing the incoming TCP FIN packets and associating them with currently built TCP sessions, resulting in a degraded working performance of the attacked device. Sometimes this attack may result in the inability to access the attacked device [67].

Figure 18 represents the traffic that the PDU had to process during the attack. Again, the results were the same as those obtained so far.

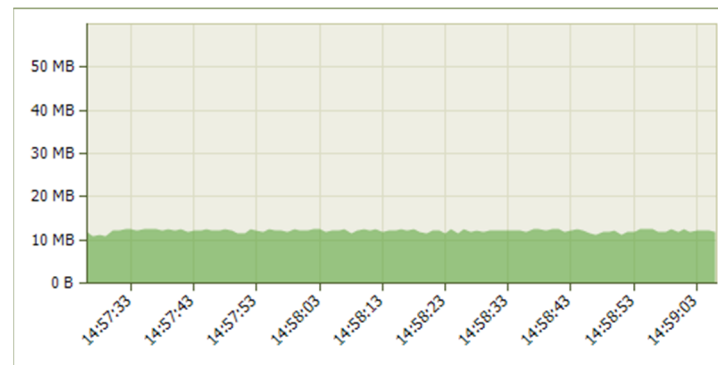


Figure 18. Processed traffic from the PDU during TCP FIN flood attack.

Figure 19 shows the values of the different TCP packets. Because the embedded web server had detected a problematic session (non-existent), it was generating TCP RST packets to terminate the non-existent TCP session. Because of the received TCP FIN packets, the internal web server of the PDU was also generating TCP FIN packets. Again, the studied PDU was accessed remotely. This is confirmed by the presence of the TCP SYN and the TCP SYNACK packets.

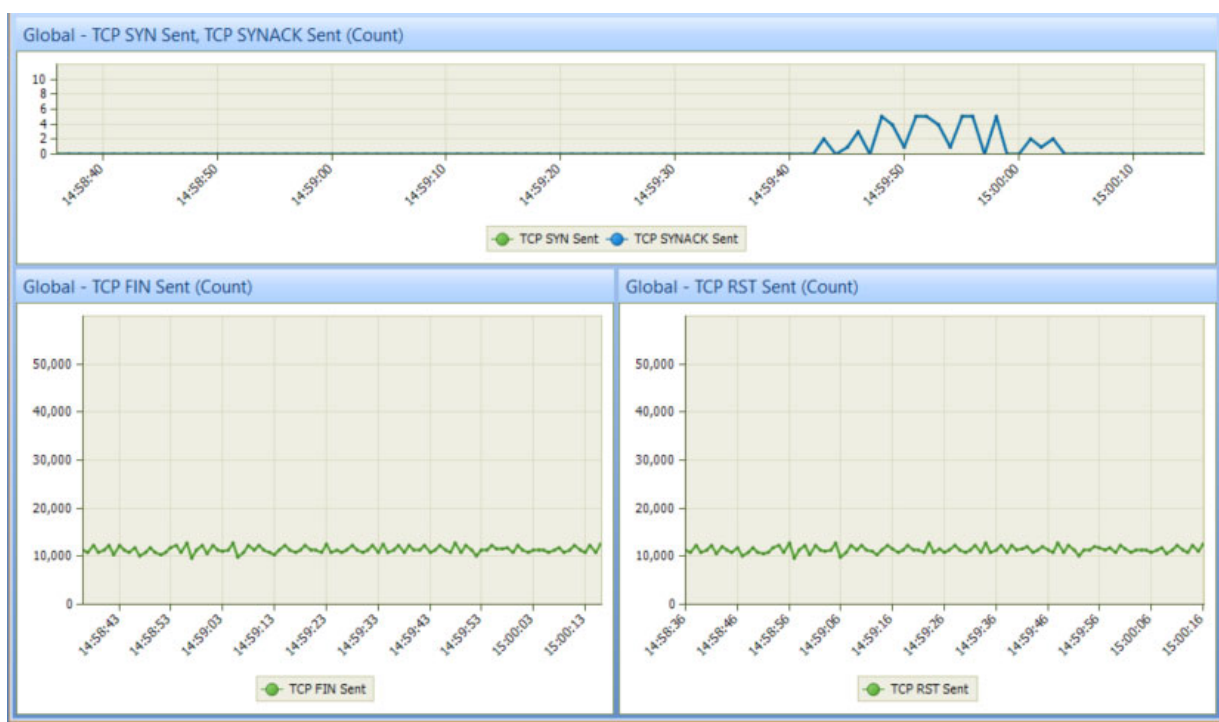


Figure 19. TCP packets during the TCP FIN flood attack.

5.2.5. TCP PUSH Flooding

When a client wants to establish a connection with a server, the client can send an acknowledgement that the request was received by sending a TCP ACK packet or by sending a TCP PUSH packet to cause the server to process the information in the packet using the PUSH flag in the TCP PUSH packet. By flooding the server with spoofed TCP PUSH packets, an attacker can prevent the server from responding to valid requests [68].

Figure 20 represents the traffic that was handled by the PDU. The results were similar to those obtained so far.

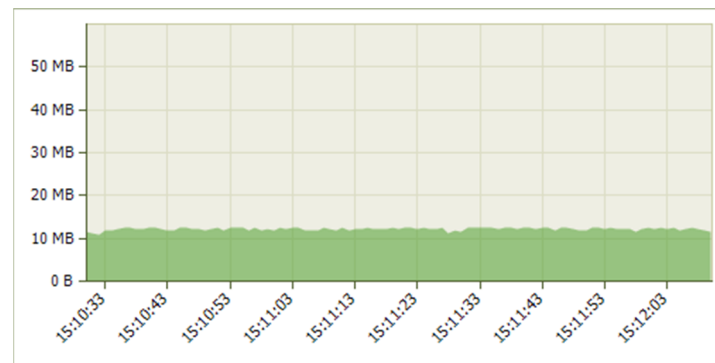


Figure 20. Processed traffic from the PDU during TCP PUSH flood attack.

Figure 21 shows the values of the different TCP packets during the attack. Again, as can be seen, the embedded web server has detected a problematic (non-existent) TCP session, therefore TCP RST packets were generated to terminate this problematic session. Regardless of the applied TCP PUSH flood attack, the PDU was remotely accessed. This was confirmed by the presence of the TCP SYN and the TCP SYNACK packets.

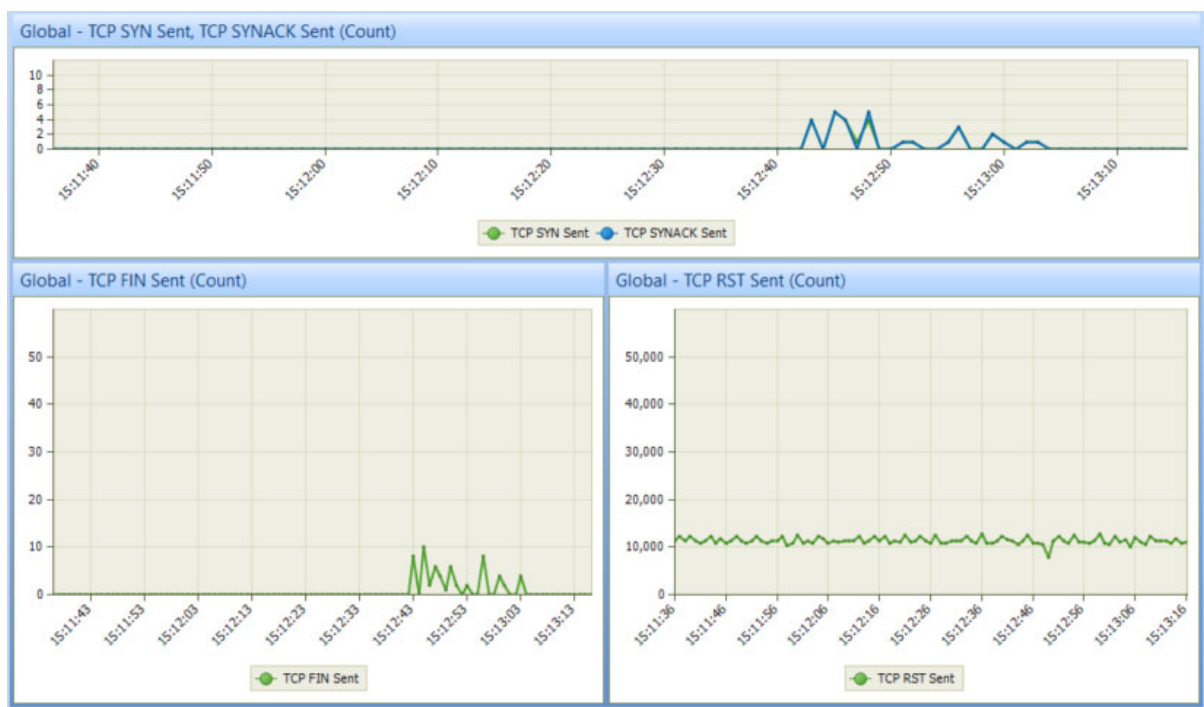


Figure 21. TCP packets during the TCP PUSH flood attack.

5.2.6. TCP URG Flooding

A URG-RST flood is a DDoS attack the purpose of which is to disrupt the network activity on the attacked device. This is achieved by flooding the bandwidth and computational resources of the attacked device with TCP URG-RST packets. During the attack, URG-RST packets are continuously sent to the attacked device. As was the case with TCP RST flooding, this stream of packets can also be used as a deflection attack when attacking with more sophisticated attacks. URG-RST packets are disabled, relative to the TCP RFC [69] standard. These packets are not used, but may be used for some personal testing, development, or research. Therefore, different communication devices may react differently to these packets—they may cause unexpected problems or behaviors in the working performance of the attacked device [70].

Figure 22 represents the traffic that the PDU had to process during this attack. As can be seen from the graph, again the results were the same as the results obtained so far.

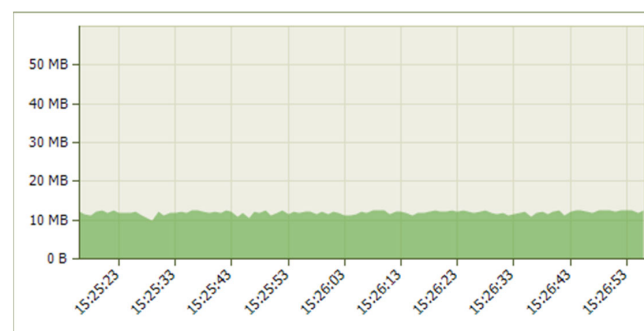


Figure 22. Processed traffic from the PDU during TCP URG-RST flood attack.

Figure 23 shows the values of the different TCP packets during the attack. As can be seen from the graphs, the embedded web server was generating a stream of TCP RST packets to terminate the problematic session. Regardless of the applied TCP URG-RST attack, the device was accessed remotely. This was confirmed by the presence of the TCP SYN, the TCP SYNACK, and the TCP FIN packets, which were evidence of a successful three-way handshake.

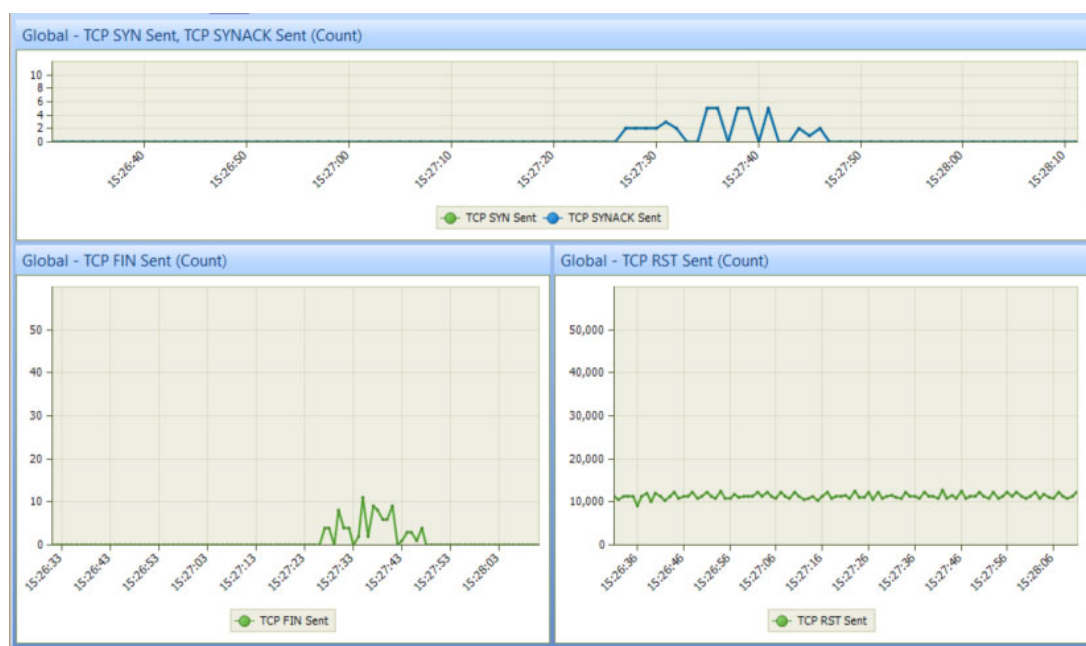


Figure 23. TCP packets during the TCP URG-RST flood attack.

5.2.7. Additional Summary Results

Figure 24 represents the total traffic that the PDU had to handle for the entire study period. As can be seen, the traffic that was handled by the PDU was uneven. During the attack periods, the amount of traffic it processed was huge. In the periods between the attacks (in normal operation mode), the amount of traffic was small or almost absent (Figure 10).

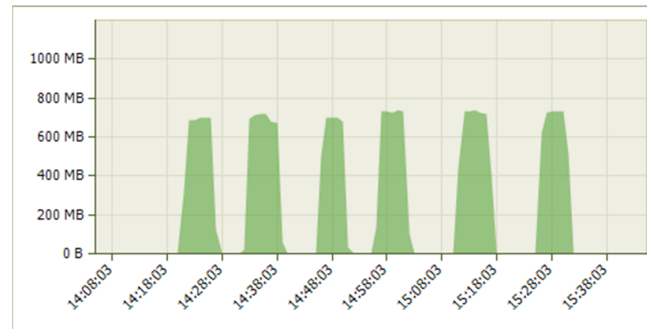


Figure 24. Processed traffic from the PDU during the whole study period.

Figure 25 presents the values of the individual TCP packets during the entire study period. As can be seen from the graphs, only during the TCP SYN flood attack was there a dramatic increase in these packets. During the other attacks there was only a minimal number of TCP SYN and TCP SYNACK packets—only when there was a successful remote access of the PDU. Due to the TCP FIN flood attack, there was only one interval of a huge amount of TCP FIN packets. During the other attacks, these packets were very few in number. For the TCP RST packets, there were several intervals where there was a huge number of TCP RST packets. These intervals correspond to the individual TCP flood attacks. Only during the TCP SYN attack was the number of these packets very small compared to the other attacks.

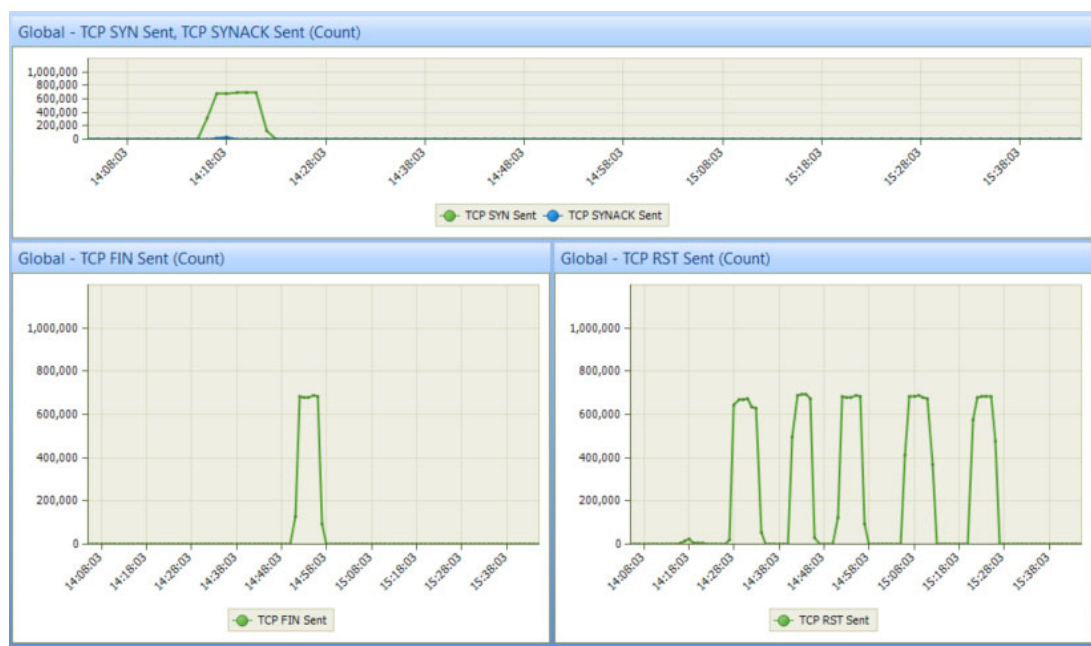


Figure 25. TCP packets during the whole study period.

Figure 26 presents the variation of the round-trip delay (RTD) between the workstation acting as the monitoring and control center and the PDU for the entire study period. As

can be seen from the graph, the RTD varies in the range from 0 to 31 ms. The interesting thing to note is that, even during the different TCP attacks, the studied PDU responds to the ICMP packets. During the six attacks, the values of the RTD are the highest. During the periods when the PDU is not attacked, the delay varies in the range 0–5 ms.

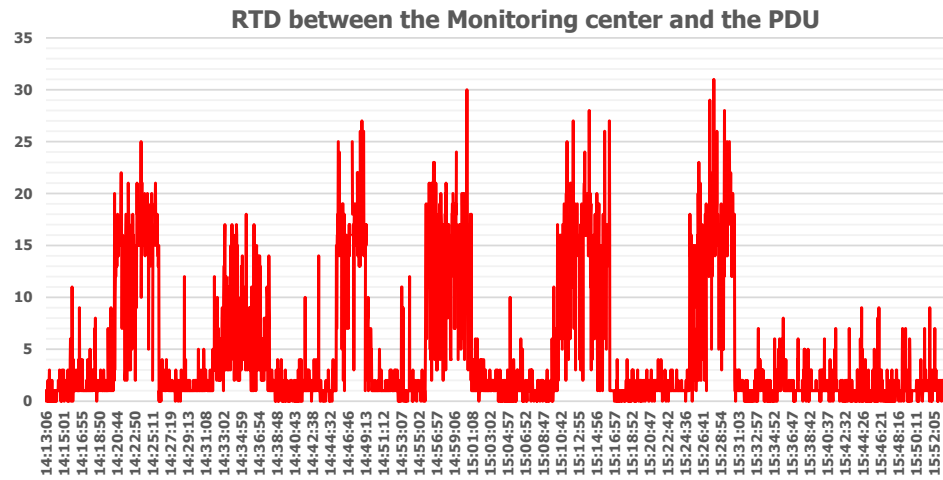


Figure 26. Variation of the RTD during the whole study period.

Figure 27 presents the mathematical distribution of the packet size with Gamma approximation. This distribution is made from the packets exchanged between the studied PDU, Kali Linux, and the monitoring center. The idea of this distribution is to give an additional graphical view of what kind of packets are exchanged during the DoS attacks. The “x” stands for the packet sizes and “y” stands for percentage of the total packets each size accounts for. The blue bars are the different packet sizes and the pink line is the Gamma approximation. As can be seen from the distribution, packets of size 1024 bytes have the largest percentage share. This is the size of the packets with which the individual attacks were performed. The remaining packets are the ICMP packets through which the RTD is measured and the packets that are exchanged between the monitoring center and the PDU during normal modes of operation.

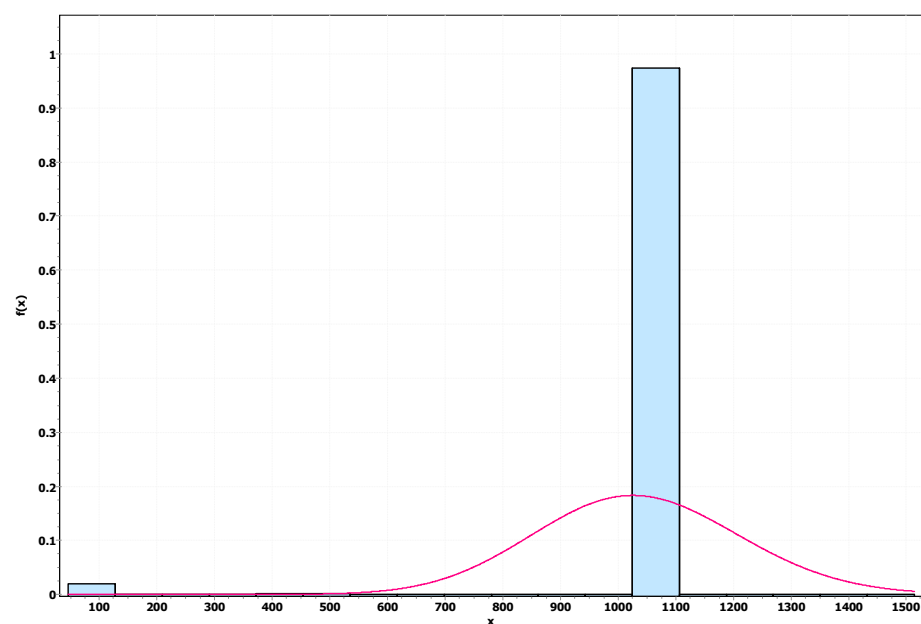


Figure 27. Mathematical distribution by packet size.

6. Discussion

Penetration testing (ethical hacking) is used by organizations to detect potential security vulnerabilities in their computer networks, applications (programs or software), and devices. Ethical hacking is simulation of a real cyber attack in order to detect vulnerabilities in a computer network, program, or other devices of an organization. Although penetration testing is a way of discovering security vulnerabilities, certain ethical rules must also be followed, such as authorization, transparency, confidentiality, and responsibility.

6.1. Discussion for the Results from Section 5.1

From the results obtained scanning for open ports, both tools found the same port to be open, port 80, through which remote access to the PDU occurs. This result is very good from a cyber security perspective because there is only one open port. All other ports were closed. This will make it much easier to build additional network security on the PDU.

From the studies carried out using specialized scripts for finding out standard and well-known network vulnerabilities, it was found that the PDU is “LIKELY VULNERABLE”, which means that the embedded http server is designed in such a way that not every DoS attack will make the PDU inaccessible, which was confirmed by the studies carried out with various DoS attacks. This result is also very good, meaning that there is no need to take additional measures to prevent DoS attacks, besides the well-known ones such as:

- Network segmentation by creating VLANs (Virtual Local Area Networks) and using hardware firewalls;
- Load balancing—distributing traffic across multiple servers;
- Blocking traffic from known or suspected IP addresses that have been linked to DoS attacks in the past or present;
- Limiting the speed of traffic, which can prevent a DoS attack from overloading the server;
- Using Content Delivery Networks (CDNs)—this distributes the content of the website across multiple locations, so a DoS attack could not bring down the entire site.

From the studies undertaken to find out whether the exchanged information is secure or not, the results were not so good. The results of both tools show that the exchanged information is insecure—it is not encrypted. Simple encoding was used—Base64—when transmitting the username and password. Other information, such as HTML scripts, which are used for the Graphical User Interface (GUI) for the individual pages of the management menu and monitoring of the PDU parameters (like temperature, voltage, user account management etc.), were transmitted in plain text. This is a serious network vulnerability of the device that could easily lead to its hacking and subsequent manipulation. It is imperative that information sent between this PDU and the monitoring center must pass through a VPN to be as secure as possible.

6.2. Discussion for the Results from Section 5.2

From the performed penetration testing, the results obtained from the analysis with specialized scripts, via Nmap, were confirmed—the PDU could be accessed during some of the DoS attacks. Only during the TCP SYN flood attack could the PDU not be accessed. During the other attacks—the TCP ACK, the TCP RST, the TCP FIN, the TCP PUSH, and the TCP URG-RST flood attacks—the PDU was accessible, individual power outlets could be managed, and any settings/changes could be made to the PDU menus. This is confirmed by the presence of the TCP SYN and the TCP SYNACK packets, which was evidence of a successful three-way handshake and an established TCP session.

It is interesting to note that, during all attacks, the device responded to the ICMP requests, which was unexpected. The expectation was that the RTD would be huge (thousands of milliseconds) or it would not be measured. The RTD values varied from 0 to 32 ms.

7. Conclusions

The use of Kali Linux in the PED research process was proposed.

By using Kali Linux, it is very easy to test/study the network security level of a PED, and to find out whether the data exchange between the PED and the monitoring center is secure or not.

From the study on the level of network security, it was found that the studied PDU has a fairly good level of network security—only one open port (80) through which remote access, management, and monitoring of the PDU takes place. This result was confirmed by two tools.

From the analysis performed for the most common network vulnerabilities, it was found that the studied PDU has a vulnerability towards DoS attacks, which is normal because no network device has 100% protection against such attacks. The obtained results showed that the internal web server used in the studied PDU was made in such a way that not all DoS attacks would be successful. This was confirmed by subsequent research.

From the studies carried out to find out whether the data exchanged is secure or not, it was found that the data exchange was insecure. The information that was exchanged was not encrypted. Some of the information is transmitted using simple encoding (Base64) and other information is transmitted in plain text. This is unacceptable in today's world—a device used to manage the power supply of communication devices offers no method for secure data exchange.

From the penetration tests, it was found that not all TCP DoS attacks succeeded in completely blocking the access to the PDU. Only the TCP SYN attack completely blocked remote access to the PDU. During the other attacks, the device was accessed without problems, despite the huge amount of traffic that the embedded web server had to handle during all attacks. These results prove the result of the network vulnerability analysis, that not all DoS attacks would be successful.

It is interesting to mention that, during all the attacks, the PDU could be pinged. This result is surprising given that the expectation was that pinging the device during the attacks would be impossible. This may be due to the way the embedded web server is built.

The results show that the developers of the device had developed or used a ready-made web server that responds very well to the various DoS attacks.

The obtained results show and confirm that the use of Kali Linux in the process of studying PEDs is applicable. The results obtained through this operating system, together with its built-in tools, can be taken into account before connecting a PED to an already-established IP network, in order to enhance the network security of the IP network.

Funding: This research received no external funding.

Data Availability Statement: All data were presented in the main text.

Conflicts of Interest: The author declares no conflicts of interest.

References

1. Wu, Y.-E.; Lin, P.-J. Design of a High Efficiency High Step-Up/Step-Down Bidirectional Isolated DC–DC Converter. *Processes* **2022**, *10*, 50. [\[CrossRef\]](#)
2. Wu, Y.-E.; Ke, Y.-T. A Novel Bidirectional Isolated DC-DC Converter with High Voltage Gain and Wide Input Voltage. *IEEE Trans. Power Electron.* **2021**, *36*, 7973–7985. [\[CrossRef\]](#)
3. Sahin, Y.; Ting, N.S.; Yesilyurt, H. A novel capacitor-voltage reduced bidirectional PWM DC-DC buck-boost converter for renewable energy battery charge system. *Int. J. Circ. Theor. Appl.* **2023**, *51*, 2875–2888. [\[CrossRef\]](#)
4. Stefanov, I.T.; Kishkin, K.Y.; Arnaudov, D.D. Examination of LLC based DC/DC Resonant Converter at Different Modes of Operation. In Proceedings of the XXXII International Scientific Conference Electronics (ET), Sozopol, Bulgaria, 13–15 September 2023.
5. Kishkin, K.; Kanchev, H.; Arnaudov, D. Modeling the Influences of Cells Characteristics in Battery Bank. In Proceedings of the 22nd International Symposium on Electrical Apparatus and Technologies (SIELA), Bourgas, Bulgaria, 1–4 June 2022.
6. Kroics, K.; Zarembo, J. Concept of Inductor with a Virtual Air Gap for Increasing Fault Current Capability in Traction Drive Applications. In Proceedings of the 13th National Conference with International Participation (ELECTRONICA), Sofia, Bulgaria, 19–20 May 2022.

7. Dankov, D.; Marinov, P. Study of Power GaN MOSFET Gate Drivers. In Proceedings of the 13th National Conference with International Participation (ELECTRONICA), Sofia, Bulgaria, 19–20 May 2022.
8. Grigorova, T.; Vuchev, A. A Study of a Phase-Shifted Full-Bridge LLC Resonant Converter Operating in Continuous Conduction Mode with ZVS. In Proceedings of the 13th National Conference with International Participation (ELECTRONICA), Sofia, Bulgaria, 19–20 May 2022.
9. Lidow, A. The Path Forward for GaN Power Devices. In Proceedings of the 2020 IEEE Workshop on Wide Bandgap Power Devices and Applications in Asia (WiPDA Asia), Suita, Japan, 23–25 September 2020; pp. 1–3.
10. Zeng, J.; Zhang, G.; Yu, S.S.; Zhang, B.; Zhang, Y. LLC resonant converter topologies and industrial applications—A review. *Chin. J. Electr. Eng.* **2020**, *6*, 73–84. [[CrossRef](#)]
11. Zhou, K.; Wang, X.; Yang, Q. Research on the performance of LLC resonant converter considering the influence of parasitic parameters. In Proceedings of the IEEE Sustainable Power and Energy Conference (ISPEC), Chengdu, China, 23–25 November 2020.
12. Madzharov, N.; Iliiev, D. Wireless Power Transfer System with Four Degrees of Freedom. In Proceedings of the 2022 57th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST), Ohrid, North Macedonia, 16–18 June 2022; pp. 1–4.
13. Sapundzhi, F. Study of the Effect of the Energy Produced from a Grid-Connected Rooftop Solar PV System for Small Households. *Int. J. Online Biomed. Eng.* **2022**, *18*, 147–154. [[CrossRef](#)]
14. Sapundzhi, F.; Baeva, S.; Lazarova, M.; Ivanova, L. An analysis of seasonal fluctuations and forecasting of some production capacities generated by photovoltaic power system. In Proceedings of the 48th International Conference “Applications of Mathematics in Engineering and Economics”, Sofia, Bulgaria, 7–13 June 2022.
15. Kishkin, K.; Arnaudov, D.; Penev, D. Algorithm for Charging a Supercapacitor Energy Storage System. In Proceedings of the 43rd International Spring Seminar on Electronics Technology (ISSE), Demanovska Valley, Slovakia, 14–15 May 2020.
16. Semsar, S.; Luo, Z.; Nie, S.; Lehn, P.W. Integrated Wireless Charging Receiver for Electric Vehicles with Dual Inverter Drives. *IEEE Trans. Power Electron.* **2024**, *39*, 1802–1814. [[CrossRef](#)]
17. Zhang, Z.; Ding, L.; Hou, A.; Bao, W. A Novel Control Strategy of Wind-Energy Storage Integrated System to Suppress Wind Power Fluctuation. In Proceedings of the IEEE International Conference on Advanced Power System Automation and Protection (APAP), Xuchang, China, 8–12 October 2023.
18. Milczarek, A.; Martinez-Caballero, L. Control Strategy of Hybrid Energy Storage System for High-Dynamic Load Changes. In Proceedings of the IEEE 17th International Conference on Compatibility, Power Electronics and Power Engineering (CPE-POWERENG), Tallinn, Estonia, 14–16 June 2023.
19. Deng, Q.; Qiu, D.; Xie, Z.; Zhang, B.; Chen, Y. Online SOC Estimation of Supercapacitor Energy Storage System Based on Fractional-Order Model. *IEEE Trans. Instrum. Meas.* **2023**, *72*, 1–10. [[CrossRef](#)]
20. Cui, Y. Regenerative Braking System of FSAE Racing Car Based on Simulink. In Proceedings of the 3rd International Conference on Energy, Power and Electrical Engineering (EPEE), Wuhan, China, 15–17 September 2023.
21. Damatopoulou, T.; Angelopoulos, S.; Christodoulou, C.; Gonos, I.; Kladas, A.; Hristoforou, E. Magnetic Shielding for Electric Car Power Cables. *IEEE Trans. Magn.* **2023**, *59*, 1–7. [[CrossRef](#)]
22. Hamednia, A.; Hanson, V.; Zhao, J.; Murgovski, N.; Forsman, J.; Pourabdollah, M.; Larsson, V.; Fredriksson, J. Charge Planning and Thermal Management of Battery Electric Vehicles. *IEEE Trans. Veh. Technol.* **2023**, *72*, 14141–14154. [[CrossRef](#)]
23. Jia, Z.; Li, J.; Zhang, X.-P.; Zhang, R. Review on Optimization of Forecasting and Coordination Strategies for Electric Vehicle Charging. *J. Mod. Power Syst. Clean Energy* **2023**, *11*, 389–400. [[CrossRef](#)]
24. Alasali, F.; AlMajali, A.; Abudayyeh, M.; Aldeiri, B.; El-Naily, N.; Zarour, E. Enhancing Cyber-Physical Threat Assessment in Power Distribution Networks. In Proceedings of the 11th International Conference on ENERGY and ENVIRONMENT (CIEM), Bucharest, Romania, 26–27 October 2023.
25. Jambi, J.R.A.; Wong, W.K.; Juwono, F.H.; Motalebi, F. Smart Energy Meter Implementation: Security Challenges and Opportunities. In Proceedings of the 2023 International Conference on Digital Applications, Transformation & Economy (ICDATE), Miri, Sarawak, Malaysia, 14–16 July 2023.
26. Keller, J.; Paul, S.; Hutto, K.; Grijalva, S.; Mooney, V.J. Developing Simulation Capabilities for Supply Chain Cybersecurity of the Electricity Grid. In Proceedings of the IEEE PES Innovative Smart Grid Technologies Latin America (ISGT-LA), San Juan, PR, USA, 6–9 November 2023.
27. Elrawy, M.F.; Tekki, E.; Hadjidemetriou, L.; Laoudias, C.; Michael, M.K. Protection and Communication Model of Intelligent Electronic Devices to Investigate Security Threats. In Proceedings of the IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 16–19 January 2023.
28. Fu, R.; Lichtenwalner, M.E.; Johnson, T.J. A Review of Cybersecurity in Grid-Connected Power Electronics Converters: Vulnerabilities, Countermeasures, and Testbeds. *IEEE Access* **2023**, *11*, 113543–113559. [[CrossRef](#)]
29. Hu, D.; Dong, Y.; Wang, J.; Shi, D. Detection of False Data Injection Attacks in Smart Grids Under Power Fluctuation Uncertainty Based on Deep Learning. In Proceedings of the International Conference on Power System Technology (PowerCon), Jinan, China, 21–22 September 2023.
30. Ahn, B.; Kim, T.; Ahmad, S.; Mazumder, S.K.; Johnson, J.; Mantooth, H.A.; Farnell, C. An Overview of Cyber-Resilient Smart Inverters based on Practical Attack Models. *IEEE Trans. Power Electron.* **2023**, *39*, 4657–4673. [[CrossRef](#)]

31. Ryan, J.T.; Mehrasa, M.; Selvaraj, D.F. Supervised Learning for DC-Link Protection of Dual-Active Bridge Converter against Cyber-Attacks. In Proceedings of the North American Power Symposium (NAPS), Asheville, NC, USA, 15–17 October 2023.
32. Ye, J.; Guo, L.; Yang, B.; Li, F.; Du, L.; Guan, L.; Song, W. Cyber-Physical Security of Powertrain Systems in Modern Electric Vehicles: Vulnerabilities, Challenges, and Future Visions. *IEEE J. Emerg. Sel. Top. Power Electron.* **2021**, *9*, 4639–4657. [[CrossRef](#)]
33. Amin, M.; El-Sousy, F.F.; Aziz, G.A.A.; Gaber, K.; Mohammed, O.A. CPS Attacks Mitigation Approaches on Power Electronic Systems with Security Challenges for Smart Grid Applications: A Review. *IEEE Access* **2021**, *9*, 38571–38601. [[CrossRef](#)]
34. Dobrea, M.A.; Vasluianu, M.; Neculoiu, G.; Bichiu, S. Data Security in Smart Grid. In Proceedings of the 2020 12th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Bucharest, Romania, 25–27 June 2020; pp. 1–6.
35. Li, F.; Li, Q.; Zhang, J.; Kou, J.; Ye, J.; Song, W.; Mantooth, H.A. Detection and Diagnosis of Data Integrity Attacks in Solar Farms Based on Multilayer Long Short-Term Memory Network. *IEEE Trans. Power Electron.* **2021**, *36*, 2495–2498. [[CrossRef](#)]
36. Bogosyan, S.; Gokasan, M. Novel Strategies for Security-hardened BMS for Extremely Fast Charging of BEVs. In Proceedings of the 2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC), Rhodes, Greece, 20–23 September 2020; pp. 1–7.
37. Guzmán, R.E.P.; Rivera, M.; Wheeler, P.; Mirzaeva, G.; Espinosa, E.; Rohten, J.A. Microgrid Power Sharing Framework for Software Defined Networking and Cybersecurity Analysis. *IEEE Access* **2022**, *10*, 111389–111405. [[CrossRef](#)]
38. Kharlamova, N.; Hashemi, S.; Træholt, C. The Cyber Security of Battery Energy Storage Systems and Adoption of Data-driven Methods. In Proceedings of the 2020 IEEE Third International Conference on Artificial Intelligence and Knowledge Engineering (AIKE), Laguna Hills, CA, USA, 9–13 December 2020; pp. 188–192.
39. De Dutta, S.; Prasad, R. Cybersecurity for Microgrid. In Proceedings of the 2020 23rd International Symposium on Wireless Personal Multimedia Communications (WPMC), Okayama, Japan, 19–26 October 2020; pp. 1–5.
40. Xu, S.; Xia, Y.; Shen, H.L. Analysis of Malware-Induced Cyber Attacks in Cyber-Physical Power Systems. *IEEE Trans. Circuits Syst. II Express Briefs* **2020**, *67*, 3482–3486. [[CrossRef](#)]
41. Tu, H.; Xia, Y.; Tse, C.; Chen, X. A Hybrid Cyber Attack Model for Cyber-Physical Power Systems. *IEEE Access* **2020**, *8*, 114876–114883. [[CrossRef](#)]
42. Hosseinzadeh, M.; Sinopoli, B. Active Attack Detection and Control in Constrained Cyber-Physical Systems Under Prevented Actuation Attack. In Proceedings of the 2021 American Control Conference (ACC), New Orleans, LA, USA, 25–28 May 2021; pp. 3242–3247.
43. Bergs, C.J.; Bruiners, J.; Fakier, F.; Stofile, L. Cyber Security and Wind Energy: A Fault-Tolerance Analysis of DDoS Attacks. In Proceedings of the 16th International Conference on Cyber Warfare and Security (ICWS 2021), Tennessee Tech, Cookeville, ST, USA, 25–26 February 2021; pp. 443–453.
44. Tuyen, N.D.; Quan, N.; Linh, V.; Van Tuyen, V.; Fujita, G. A Comprehensive Review of Cybersecurity in Inverter-Based Smart Power System Amid the Boom of Renewable Energy. *IEEE Access* **2022**, *10*, 35846–35875. [[CrossRef](#)]
45. Kim, T.; Ochoa, J.; Faika, T.; Mantooth, H.A.; Di, J.; Li, Q.; Lee, Y. An Overview of Cyber-Physical Security of Battery Management Systems and Adoption of Blockchain Technology. *IEEE J. Emerg. Sel. Top. Power Electron.* **2022**, *10*, 1270–1281. [[CrossRef](#)]
46. Gumrukcu, E.; Arsalan, A.; Muriithi, G.; Joglekar, C.; Aboulebdh, A.; Zehir, M.A. Impact of Cyber-attacks on EV Charging Coordination: The Case of Single Point of Failure. In Proceedings of the 2022 4th Global Power, Energy and Communication Conference (GPECOM), Nevsehir, Turkey, 14–17 June 2022; pp. 506–511.
47. Arsoon, M.M.; Moghaddas-Tafreshi, S.M. Modeling Data Intrusion Attacks on Energy Storage for Vulnerability Assessment of Smart Microgrid Operation. In Proceedings of the 2021 11th Smart Grid Conference (SGC), Tabriz, Iran, 7–9 December 2021; pp. 1–5.
48. Pasetti, M.; Ferrari, P.; Bellagente, P.; Sisinni, E.; de Sá, A.O.; do Prado, C.B. Artificial Neural Network-Based Stealth Attack on Battery Energy Storage Systems. *IEEE Trans. Smart Grid* **2021**, *12*, 5310–5321. [[CrossRef](#)]
49. Kali Linux Documentation. Available online: <https://www.kali.org/docs/> (accessed on 27 January 2024).
50. Capsa Free Network Analyzer. Available online: <https://www.colasoft.com/capsa-free/> (accessed on 27 January 2024).
51. Nmap Network Scanning. The Official Nmap Project Guide to Network Discovery and Security Scanning. Available online: <https://nmap.org/book/toc.html> (accessed on 27 January 2024).
52. hping3. Available online: <https://www.kali.org/tools/hping3/> (accessed on 27 January 2024).
53. Wireshark User Guide. Available online: https://www.wireshark.org/docs/wsug_html_chunked/ (accessed on 27 January 2024).
54. Burp Suite Documentation. Available online: <https://portswigger.net/burp/documentation/desktop> (accessed on 27 January 2024).
55. Colasoft Ping Tool. Available online: https://www.colasoft.com/ping_tool/ (accessed on 27 January 2024).
56. Marinov, M.B.; Nikolov, N.; Dimitrov, S.; Todorov, T.; Stoyanova, Y.; Nikolov, G.T. Linear Interval Approximation for Smart Sensors and IoT Devices. *Sensors* **2022**, *22*, 949. [[CrossRef](#)]
57. Marinov, M.B.; Nikolov, N.; Dimitrov, S.; Ganey, B.; Nikolov, G.T.; Stoyanova, Y.; Todorov, T.; Kochev, L. Linear Interval Approximation of Sensor Characteristics with Inflection Points. *Sensors* **2023**, *23*, 2933. [[CrossRef](#)]
58. Nmap Scripts. Available online: <https://nmap.org/book/nse-usage.html#nse-categories> (accessed on 27 January 2024).
59. Ivanov, I.; Andreev, K.; Vetova, S.; Arnaudov, R. Cryptographic algorithm for protection of communication in drones control. *J. Reason.-Based Intell. Syst.* **2021**, *13*, 32–38. [[CrossRef](#)]

60. Cherneva, G.P.; Hristova, V.I. Evaluation of FHSSS Stability against Intentional Disturbances. In Proceedings of the 28th National Conference with International Participation (TELECOM), Sofia, Bulgaria, 29–30 October 2020.
61. Dimitrov, W.; Spasov, K.; Trenchev, I.; Syarova, S. Complexity Assessment of Research Space for Smart City Cybersecurity*. *IFAC-PapersOnLine* **2022**, *55*, 1–6. [[CrossRef](#)]
62. Jekov, B.; Dimitrov, W.; Panayotova, G.S.; Kovatcheva, E. Intelligent protection of Internet of things systems. In Proceedings of the 2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Maldives, Maldives, 16–18 November 2022.
63. Popov, G.; Popova, A. Application of System Diversity for Increasing Security and Reliability of Distributed Systems. In Proceedings of the 2022 XXXI International Scientific Conference Electronics (ET), Sozopol, Bulgaria, 13–15 September 2022; pp. 1–4.
64. TCP SYN Flood Attack. Available online: <https://www.imperva.com/learn/ddos/syn-flood/> (accessed on 8 March 2024).
65. What Is an ACK Flood DDoS Attack? Available online: <https://www.cloudflare.com/learning/ddos/what-is-an-ack-flood/> (accessed on 8 March 2024).
66. RST Flood. Available online: <https://kb.mazebolt.com/knowledgebase/rst-flood/> (accessed on 8 March 2024).
67. FIN Flood. Available online: <https://kb.mazebolt.com/knowledgebase/fin-flood/> (accessed on 8 March 2024).
68. ACK–PUSH Flooding. Available online: <https://kb.mazebolt.com/knowledgebase/ack-psh-flood/> (accessed on 8 March 2024).
69. TCP RFC. Available online: <https://www.ietf.org/rfc/rfc793.txt> (accessed on 27 January 2024).
70. URG Flood. Available online: <https://kb.mazebolt.com/knowledgebase/urg-flood/> (accessed on 8 March 2024).

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.