

KALI LINUX – A SIMPLE AND EFFECTIVE WAY TO STUDY THE LEVEL OF CYBER SECURITY AND PENETRATION TESTING OF POWER ELECTRONIC DEVICES

Ivan Nedyalkov, Georgi Georgiev*

South – West University “Neofit Rilski”, Blagoevgrad
Bulgaria

* Corresponding Author, e-mail: i.nedqlkov@swu.bg

Abstract: The work presents the possibility to use Kali Linux in the process of power electronic devices research, which has not been applied before. Several of the built-in tools of Kali Linux have been used for the purpose of the research. Nmap has been used for vulnerability testing - scanning for open ports and finding out specific, well-known security vulnerabilities by using specific scripts. Wireshark and Burp Suite have been used to find out if the exchanged information is secure or not. hping3 has been used to scan for open ports and generating different TCP DoS attacks, thus studying what is the response of the power electronic device when it is subjected to different TCP DoS attacks – can it be accessed or not, has it experienced any performance violation, etc. Based on the results of this research, it can be argued that Kali Linux is applicable and can be used during the process of power electronic device research.

Key words: Cyber security, DoS attacks, Kali Linux, Network monitoring, Power electronic devices.

1. INTRODUCTION

The main researches related to power electronic devices (PEDs) are mainly focused on discovering new circuit/schematic solutions; improving existing circuit/schematic solutions; improving the efficiency of PEDs; using new chemical components, in the production of power electronic components (transistors, diodes, etc.); solutions to improve the transistors switching process, etc [1, 2]. Studies focusing on the communication capabilities of the PEDs, such as characterizing the generated communication traffic or studies related to finding out security vulnerabilities or finding out if the information exchange secure or not, are not as numerous [3, 4]. These types of researches are equally important due to the capability of the PEDs to connect to the Internet and be remotely controlled and monitored. Currently, any device connected to an IP network/Internet is a potential victim of different cyber-attacks. That's why, this kind of researches are also of great importance.

In this work, the use of Kali Linux [5] in the process of PEDs research has been proposed which to our opinion is novelty. Kali Linux is used for penetration testing of various IP network communication devices, not for PED researches. Kali Linux has many different tools that can be used to find out if the data exchange between the PED and the monitoring center secured. The applicability of Kali Linux has been presented with results from a case study of a PED. Additionally, the response of the studied PED when it is a subject to a TCP DoS attacks has been studied - under which attacks it can be accessed and under which attacks remote access will be impossible.

2. RELATED WORK

In [6], the authors have provided a comprehensive overview in which they consider various cyber-attacks that can be applied to different devices in smart microgrids and what impact each of the considered attacks have. They have paid special attention to false data injection (FDI) attack as it is one of the dangerous cyber-attacks for microgrids. The authors have also looked at ways to protect against these attacks. Additionally, they have paid attention to the ways of composing the attack as well as the ways of preventing this attack.

In [7], the authors have provided a comprehensive review on cyber-physical (CP) attacks, vulnerabilities and ways to mitigate the negative impact of these attacks on power electronic devices. They have done a review on the security of power electronic devices deployed in smart grids. Some of the most massive cyber-attacks applied on cyber-physical systems have been discussed. The authors have reviewed various methods to mitigate the effect of applying these attacks on cyber-physical systems. Additionally, the authors discussed on what would be the future, in terms of security of cyber-physical systems.

In [8], the authors have created physics-guided machine learning to detect cyber-attacks against electric vehicles based on different driving scenarios. The proposed model detects the presence of a cyber-attack by continuous monitoring the current and voltage parameters of the electric motor as well as data from the physical dynamics of the vehicle. For validation, the authors have used the OPAL-RT hardware-in-the-loop (HIL) platform.

In [9], the authors consider the cyber-physical security of PV systems from the perspective of firmware, network, PV inverter management, and grid security. They discuss the vulnerabilities of PV systems when they have been attacked by various cyber-attacks. Model-based and data-driven methods to detect threats and reduce the likelihood of their realization have been discussed. The authors have carried out numerous simulation and experimental studies to demonstrate the effect of attacks on the converters and the overall system.

3. EXPERIMENTAL SETUP AND RESEARCH METHODOLOGY

3.1. Experimental setup

Figure 1 presents the experimental setup. It consists of a Wi-Fi router, a managed switch and two mobile workstations - one running Kali Linux and the other running

various IP network traffic monitoring tools. The managed switch has been used because of the mirror port feature, by which all the traffic that is processed by the switch is copied to that port on which the mobile workstation has been connected, through which the traffic that has been exchanged between the studied Power Distribution Unit and the Kali Linux has been monitored. The studied PED is a Power Distribution Unit (PDU) which is used by ISPs (Internet Service Providers) to manage the power supply of their communication equipment as well as to monitor certain parameters such as temperature, humidity, availability of power supply etc.

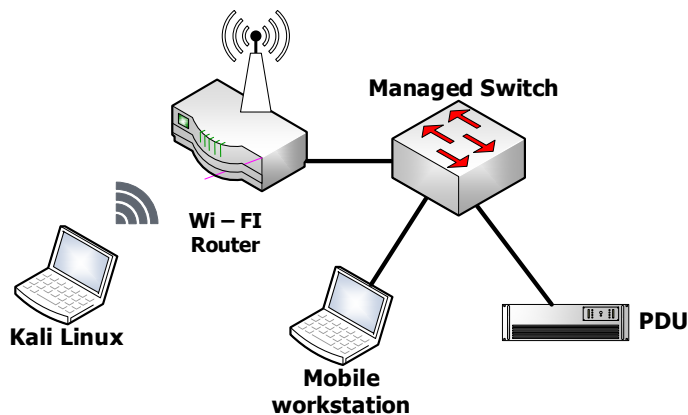


Figure 1. Experimental setup/network.

3.2. Research methodology

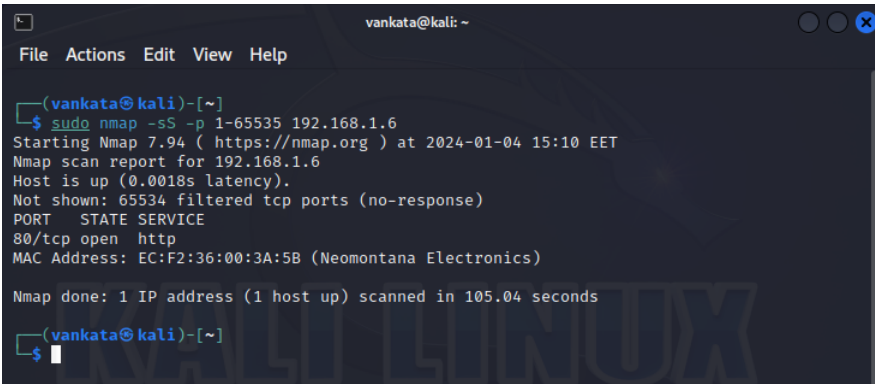
Through the various built-in tools of Kali Linux, it will be found out what is the security status of the studied PDU (by using port scanning tools, protocol network analyzers and other tools). Based on the obtained results from these tools, an analysis will be made about the level of security of the PDU and if the data exchange between the PDU and the monitoring and control center secure or not.

Additionally, the studied PDU will be subjected to various TCP DoS attacks. The results of these attacks will be analyzed to summarize what impact each of the attacks have on the performance of the studied PDU.

4. RESULTS FROM THE STUDY

4.1. Vulnerability testing results

Figure 2 presents the results for finding out open ports. For this purpose, the Nmap tool has been used to scan for open ports and to find out various well known security vulnerabilities. In this example, the TCP SYN scan (“-sS” command) was used to scan all ports (“-p 1- 65535”). In this port scan method, full TCP three-way handshake has been used. As it can be seen, only port 80 is open. This is so because the PDU can only be accessible and managed through a browser. The rest of the ports are closed. This is very good from a security point of view because only one port will need to be secure.

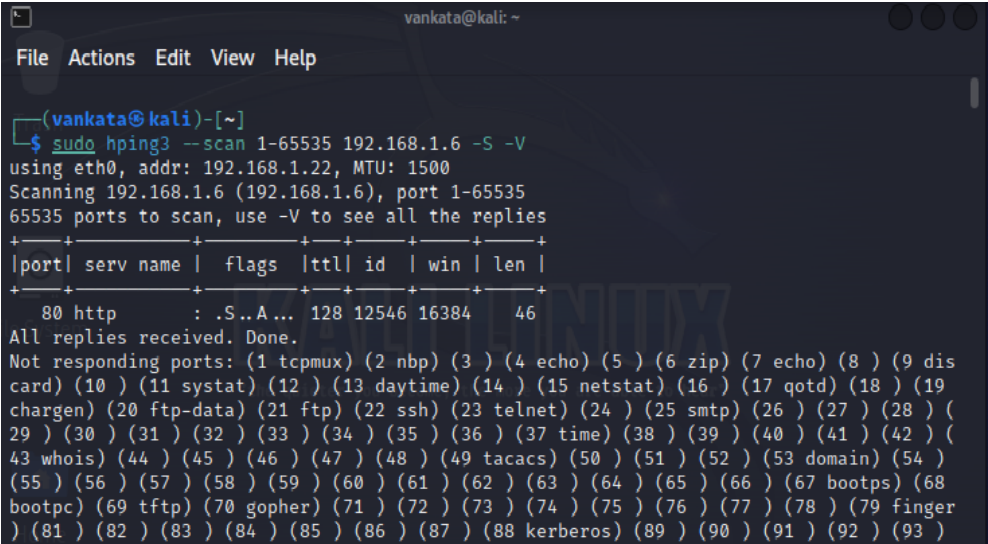


```
vankata@kali: ~  
File Actions Edit View Help  
  
(vankata@kali)-[~]  
$ sudo nmap -sS -p 1-65535 192.168.1.6  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-04 15:10 EET  
Nmap scan report for 192.168.1.6  
Host is up (0.0018s latency).  
Not shown: 65534 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
80/tcp    open  http  
MAC Address: EC:F2:36:00:3A:5B (Neomontana Electronics)  
  
Nmap done: 1 IP address (1 host up) scanned in 105.04 seconds  
  
(vankata@kali)-[~]  
$
```

Figure 2. Result from the port scanning from Nmap.

Figure 3 shows the results of running the “hping3” tool. As it can be seen the results are the same with the results from the Nmap scan - only port 80 is open, all others are closed.

Nmap also supports features for finding out specific, well known security vulnerabilities. This has been done by using scripts of execute specific commands to find out a particular vulnerability. Figure 4 shows the result of such a test - a vulnerability testing to DoS attacks. The script "http-slowloris-check" tests the internal web server for vulnerability to the Slowloris DoS attack without starting a real DoS attack. The result, "LIKELY VULNERABLE", means that the studied PDU can be a victim to such attack, but depending on the embedded web server architecture and certain constrains, a complete denial of service is not always possible. This has been noticed in the subsequent tests with different TCP DoS attacks applied on the PDU.



```
vankata@kali: ~  
File Actions Edit View Help  
  
(vankata@kali)-[~]  
$ sudo hping3 --scan 1-65535 192.168.1.6 -S -V  
using eth0, addr: 192.168.1.22, MTU: 1500  
Scanning 192.168.1.6 (192.168.1.6), 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 12546 16384 46  
All replies received. Done.  
Not responding ports: (1 tcpmux) (2 nbp) (3 ) (4 echo) (5 ) (6 zip) (7 echo) (8 ) (9 dis  
card) (10 ) (11 systat) (12 ) (13 daytime) (14 ) (15 netstat) (16 ) (17 qotd) (18 ) (19  
chargen) (20 ftp-data) (21 ftp) (22 ssh) (23 telnet) (24 ) (25 smtp) (26 ) (27 ) (28 ) (29 ) (30 ) (31 ) (32 ) (33 ) (34 ) (35 ) (36 ) (37 time) (38 ) (39 ) (40 ) (41 ) (42 ) (43 whois) (44 ) (45 ) (46 ) (47 ) (48 ) (49 tacacs) (50 ) (51 ) (52 ) (53 domain) (54 ) (55 ) (56 ) (57 ) (58 ) (59 ) (60 ) (61 ) (62 ) (63 ) (64 ) (65 ) (66 ) (67 bootps) (68 bootpc) (69 tftp) (70 gopher) (71 ) (72 ) (73 ) (74 ) (75 ) (76 ) (77 ) (78 ) (79 finger) (81 ) (82 ) (83 ) (84 ) (85 ) (86 ) (87 ) (88 kerberos) (89 ) (90 ) (91 ) (92 ) (93 )
```

Figure 3. Result from the port scanning from hping3.

```

vankata@kali: ~
File Actions Edit View Help

(vankata@kali)-[~]
$ nmap --script http-slowloris-check 192.168.1.6
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-04 16:12 EET
Nmap scan report for 192.168.1.6
Host is up (0.0020s 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
|_
Nmap done: 1 IP address (1 host up) scanned in 16.09 seconds

(vankata@kali)-[~]
$

```

Figure 4. Result from executing the script *http-slowloris-check*.

Nmap supports many different scripts to find out different well known security vulnerabilities. These scripts are many and testing them individually is time consuming. There is also a global vulnerability test option that includes all vulnerability testing scripts. This is the "vuln" script. Figure 5 shows the result of running this script. As it can be seen from the obtained result, the only vulnerability found out by the tool is the one found out earlier when using the "http-slowloris-check" script. No other vulnerabilities have been found, which is great, because the tested PED is very limited in terms of communication capabilities, due to its working principle - to manage the power supply of communication equipment.

In this work, Wireshark has been used to find out if the data exchange between the PED and the monitoring and control center secured or not. The tool has been integrated in Kali Linux. Figure. 6 shows the result of the study. 192.168.1.6 is the IP address of the tested PED and 192.168.1.22 is the IP address of the Kali Linux. The obtained result shows that the account information is exchanged insecure - username and password are just Base64 encoded but not encrypted. Thus, this information has been transmitted almost as a plaintext and can be hacked very easily.

Burp Suite Community Edition which is a tool that can also be used for finding out if the data exchange secure or not. Figure 7 shows the result of using the tools. As it can be seen the result, is the same as the Wireshark result. Since simple encoding is used (Base64) and no encryption, the tool immediately decodes the username and password.

```
vankata@kali: ~  
File Actions Edit View Help  
(vankata@kali)-[~]  
$ sudo nmap --script vuln 192.168.1.6  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-04 17:11 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 192.168.1.6  
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://hackers.org/slowloris/  
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750  
|_ http-csrf: Couldn't find any CSRF vulnerabilities.  
|_ http-dombased-xss: Couldn't find any DOM based XSS.  
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
```

Figure 5. Result from executing the script “vuln”.

The image shows a Wireshark packet capture of an HTTP transaction. The packet list on the left shows a GET request (No. 1974) and a 200 OK response (No. 1980). The selected packet (No. 1980) is expanded to show the raw data and the corresponding HTTP message. The raw data is shown in hexadecimal and ASCII. The ASCII part shows the HTTP response structure, including the status line '200 OK (text/html)', the 'Content-Type' header, and the 'Authorization' header. The 'Authorization' header is highlighted in blue and contains the text 'Basic YWRtaW46cGZlc3dvcnQ='. The 'Credentials' field is also highlighted in blue and contains the text 'admin:password'.

No.	Time	Source	Destination	Protocol	Length	Info
837	8.100803875	212.95.165.25	192.168.1.22	OCSP	954	Response
1433	13.814598192	192.168.1.22	192.168.1.6	HTTP	403	GET / HTTP/1.1
1500	14.317553206	192.168.1.6	192.168.1.22	HTTP	60	HTTP/1.0 401 Authorization Required
1974	20.044337732	192.168.1.22	192.168.1.6	HTTP	446	GET / HTTP/1.1
1980	20.048775032	192.168.1.6	192.168.1.22	HTTP	60	HTTP/1.0 200 OK (text/html)

Host: 192.168.1.6\r\n
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/109.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
Cookie: rf=0\r\n
Cookie pair: rf=0\r\n
Upgrade-Insecure-Requests: 1\r\n
Authorization: Basic YWRtaW46cGZlc3dvcnQ=\r\n
Credentials: admin:password\r\n
[Full request URI: http://192.168.1.6/]
[HTTP request 1/1]
[Response in frame: 1980]

HTTP Authorization header (http.authorization), 43 byte(s) Packets: 114137 - Displayed: 84 (0.1%) Profile: Default

Figure 6. Result from Wireshark.

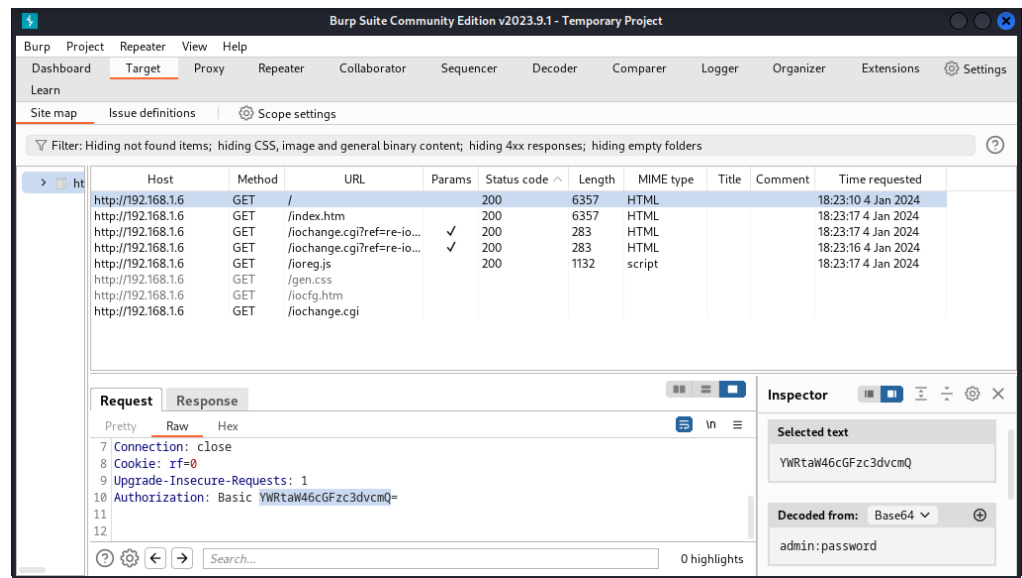


Figure 7. Result from Burp Suite Community Edition.

The results from both tools show that important information such as the username and password has been exchanged insecure (not encrypted), but only encoded to be transmitted over the line. This is unacceptable because the studied PED can be hacked and manipulated very easily. The easiest and fastest way to solve this problem is to use the VPN (Virtual Private Network) technology. In this technology, a "virtual tunnel" is created between communicating devices, through which information is exchanged encrypted. This will solve the problem of insecure data exchange. Other technologies, techniques and methods to secure the exchange of insecure information can be found in [10, 11, 12].

4.2. Results from the penetration testing

In this work, the ability of Kali Linux for generating various TCP DoS attacks will be used. This will reveal how each DoS attack affects the network performance of the studied PDU. For the purpose of this work the "hping3" tool has been used to generate the DoS attacks.

The network traffic exchanged between the PDU and the monitoring and control center during normal operation mode is shown on figure 8. There is very little network traffic. It is generated when the device is remotely accessed/managed. This traffic is due to packets being exchanged to support the HTTP session on, sending control commands, and sending statistical information such as temperature, humidity, and more. Almost no traffic is generated/exchanged at the times when the PDU is not accessed or managed.

Figure 9 presents the amount of TCPSYN and TCP SYNACK packets. Again, the results are for normal operation mode. The graph shows, that the amount of these packets is small.

Figure 10 presents the results of the processed traffic during a TCP SYN DoS attack. The graph shows that the network traffic processed by the studied device is very large, unlike the normal mode of operation. This traffic represents TCP SYN packets that are sent from Kali Linux to the PDU. The PDU could not be accessed remotely because it is flooded with TCP SYN packets and cannot manage to process all TCP requests.

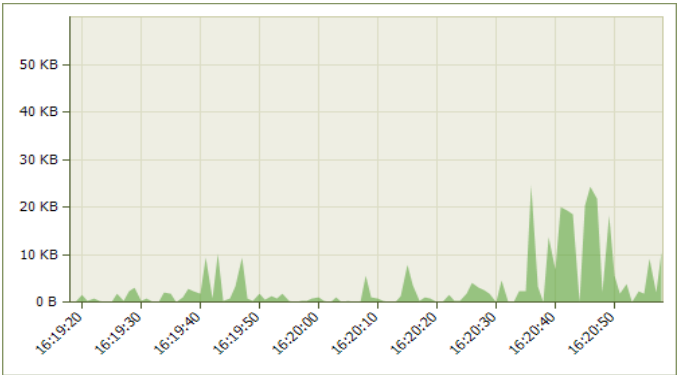


Figure 8. Total traffic during normal operation mode.

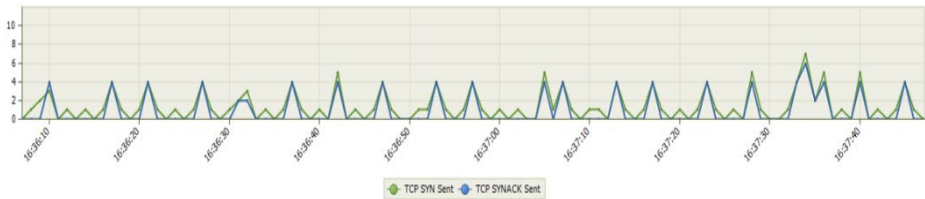


Figure 9. TCP SYN and TCP SYNACK packets in normal operation mode.

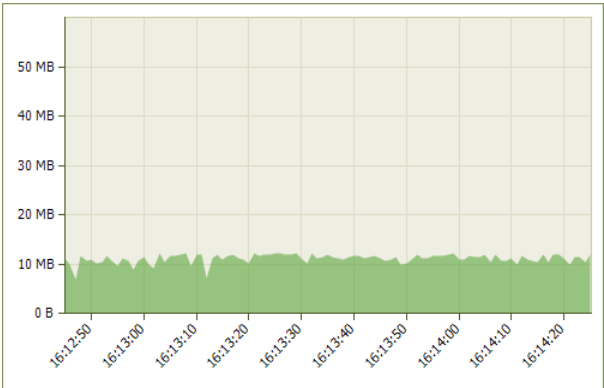


Figure 10. Total traffic during TCP SYN attack.

Figure 11 presents the results for the amount of TCP SYN and TCP SYNACK packets that are processed by the PDU. As it can be seen the amount of the TCP SYN

packets is much higher than during the normal operation. TCP SYN ACK packets are almost zero. This result is normally given when TCP SYN attack has been used.

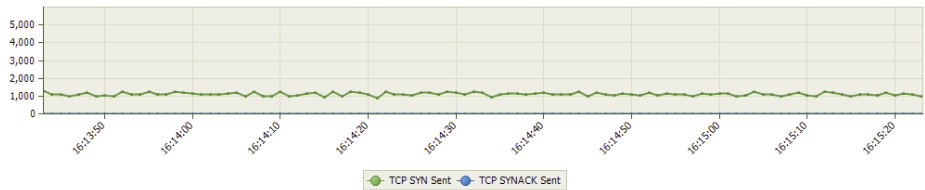


Figure 11. TCP SYN and TCP SYNACK at the time of the TCP SYN attack.

Figure 12 presents the network traffic processed by the PDU during a TCP ACK DoS attack. During this attack, Kali Linux sends only TCP ACK packets to the device. Again the graph shows that the network traffic is high. What is special about this DoS attack is that the PDU has been accessed remotely without problems, regardless of the large number of TCP ACK packets it has to process.

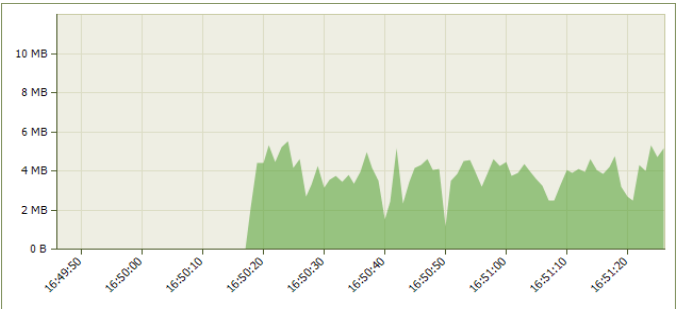


Figure 12. Total traffic during TCP ACK attack.

Figure 13 presents the amount of TCP SYN and TCP SYNACK packets. As it can be seen from the graph, TCP ACK attack does not affect the TCP session, so the PDU can be accessed remotely. This study confirms the result of PDU vulnerability testing, where the result was that not every DoS attack applied on the test PDU will be successful.

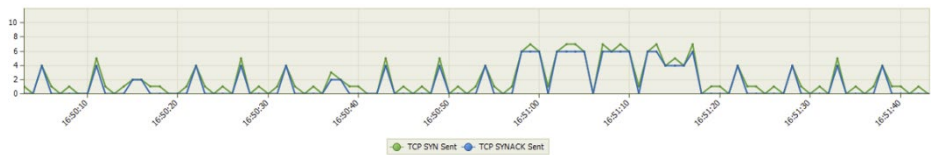


Figure 13. TCP SYN and TCP SYNACK at the time of the TCP ACK attack

Figure 14 represents the traffic processed by the PDU during a TCP RST attack. During this attack, Kali Linux transmits a huge amount of TCP RST packets to the PDU. Again, the processed traffic is very large due to flooding with TCP RST packets. Despite this flooding, the PDU can be accessed remotely.

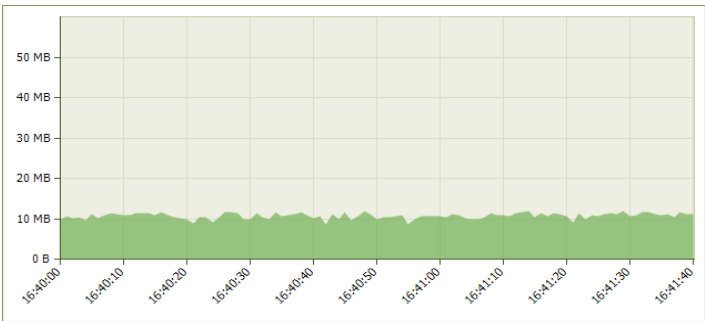


Figure 14. Total traffic during TCP RST attack.

Figure 15 represents the amount of TCP RST packets that have been exchanged during the attack. The graph shows that the number of these packets is significant. This is normal for this attack.

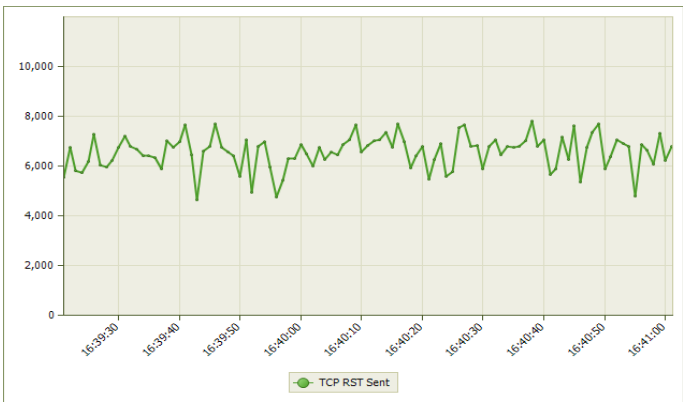


Figure 15. TCP RST packets at the time of the TCP RST attack.

Figure 16 shows the results for the amount of the TCP SYN and the TCP SYNACK packets exchanged at the time of the TCP RST attack. The graph shows that the TCP RST attack does not have any impact on the amount of TCP SYN and TCP SYNACK packets. These results reconfirm the vulnerability analysis done by Nmap that not all DoS attacks can be successful.

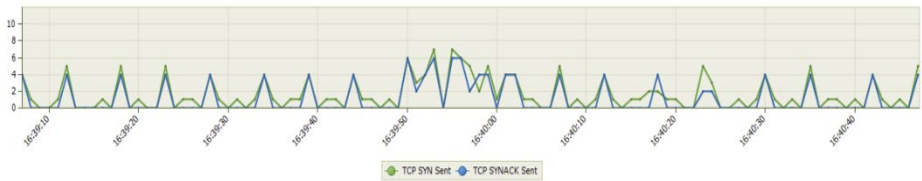


Figure 16. TCP SYN and TCP SYNACK at the time of the TCP RST attack.

Figure 17 shows a summary of the traffic that the PDU processed during all DoS attacks. As it can be seen from the graph, only when there was a DoS attack the traffic was significant. During normal operation, the traffic was minimal.

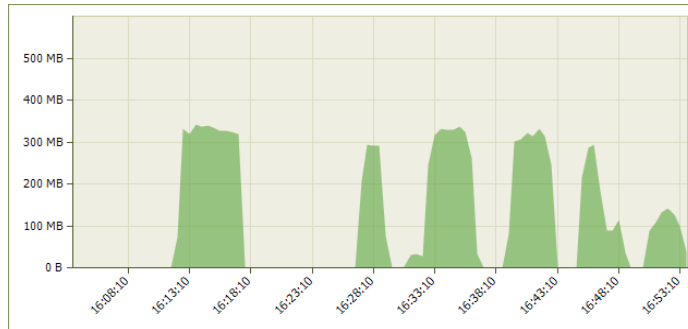


Figure 17. Total traffic for the whole study period.

5. CONCLUSION

Using Kali Linux in the PEDs research process has been proposed. The applicability of Kali Linux has been proven by the practical study that has been done with it.

With Kali Linux, various studies/tests can be carried out to find out what is the security level of a given PED as well as what would be the response of a given PED during certain cyber-attacks.

The studied PDU was tested for vulnerabilities with Kali Linux. From the obtained results, it was found that the PDU had only one open port, port 80, through which remote access to the PDU was performed. This was determined using the Nmap and hping3 tools.

Vulnerability analysis was performed using scripts and the Nmap tool. From the analysis it was found that the internal Web (HTTP) server of the PDU was set up in such a way that not every DoS attack would be successful. This was confirmed by the performed tests with different TCP DoS attacks - only during the TCP SYN attack the studied device could not be accessed or managed - the DoS attack was successful. During the other DoS attacks – the TCP ACK and the TCP RST attacks, the studied PDU was accessed remotely, i.e. the DoS attacks were not successful.

The carried-out research proved the applicability of Kali Linux in the process of PED research. The results of such research can be taken into account when installing power electronic devices in IP networks to provide their cyber security.

REFERENCES

- [1] Nikolay L. Hinov, Polya V. Gocheva, Valeri P. Gochev. Fuzzy reasoning on buck DC-DC power converter. *International Journal on Information Technologies and Security*, vol.14, no.4, 2022, pp. 33-34.
- [2] Bogdan Gilev, Nikolay Hinov, Kiril Genev. A MATLAB Based approach for control synthesis of DC-DC converters. *International Journal on Information Technologies and Security*, vol.16, no.1, 2024, pp. 77-88. <https://doi.org/10.59035/MOPG4304>

- [3] Marwan Albahar, Mohammed Thanoon, Abdulaziz Albahr. The use of fractal dimension (FD) analysis in detection of anomalies, sabotages, and malicious acts in a cyber-physical system using Higuchi's algorithm. *International Journal on Information Technologies and Security*, vol.14, no.2, 2022, pp. 111-121.
- [4] J. Ye et al. Cyber-Physical Security of powertrain systems in modern electric vehicles: Vulnerabilities, challenges, and future visions. *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 4, Aug. 2021, pp. 4639-4657
- [5] Kali Linux documentation, <https://www.kali.org/docs/> (Accessed on 02.03.2024)
- [6] Nejabatkhah, F.; Li, Y.W.; Liang, H.; Reza Ahrabi, R. Cyber-security of smart microgrids: A survey. *Energies* 2021, vol.14, 2021, p.27. <https://doi.org/10.3390/en14010027>
- [7] M. Amin, F. F. M. El-Sousy, G. A. A. Aziz, K. Gaber, O. A. Mohammed. CPS attacks mitigation approaches on power electronic systems with security challenges for smart grid applications: A review. *IEEE Access*, vol. 9, 2021, pp. 38571-38601. doi: 10.1109/ACCESS.2021.3063229.
- [8] L. Guo, J. Ye and B. Yang. Cyberattack detection for electric vehicles using physics-guided machine learning. *IEEE Transactions on Transportation Electrification*, vol. 7, no. 3, Sep 2021, pp. 2010-2022. doi: 10.1109
- [9] J. Ye et al. A review of Cyber-Physical Security for photovoltaic systems. *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 10, no. 4, Aug 2022, pp. 4879-4901. doi: 10.1109/JESTPE.2021.3111728
- [10] Willian Dimitrov, Kamen Spasov, Ivan Trenchev, Svetlana Syarova. Complexity assessment of research space for Smart city cybersecurity. *IFAC-PapersOnLine*, vol.55, no.11, 2022, pp.1-6
- [11] Dimitrov, W, Analysis of the need for cyber security components in the study of advanced technologies. *Proceedings of the 14th International technology, education, and development conference (INTED 2020)* March 02-04, 2020
- [12] PL. Chithra, R. Aparna. Blockchain enabled dual level security scheme with spiral shuffling and hashing technique for secret video transmission. *International Journal on Information Technologies and Security*, vol.15, no.2, 2023, pp. 97-108. <https://doi.org/10.59035/UBSN9044>

Information about the authors:

Ivan Nedyalkov – I completed a PhD degree in Technical University - Sofia. I am Assoc. Prof. PhD in the South - West University "Neofit Rilski" at the Faculty of Engineering. I am a member of the Union of Electronics, Electrical Engineering and Telecommunications (CEEC) My field of research covers: monitoring of IP - based networks, characterization of the traffic flows in IP networks.

Georgi Georgiev– He completed a PhD degree in Technical University - Sofia. Member of the Union of Electronics, Electrical Engineering and Telecommunications (CEEC) and a chief assistant in the South – West university “Neofit Rilski”, Faculty of Engineering. The subjects of scientific researchers are: IP network planning, monitoring of IP networks, cloud computing.

Manuscript received on 02 March 2024