DOI: 10.2507/34th.daaam.proceedings.015

DETECTING SECURITY VULNERABILITIES ON INTERNET-CONNECTED DEVICES

Ema Lovric, Zlatan Moric, Jasmin Redzepagic & Damir Regvart

This Publication has to be referred as: Lovric, E[ma]; Moric, Z[latan]; Redzepagic, J[asmin] & Regvart, D[amir] (2023). Detecting Security Vulnerabilities on Internet-connected Devices, Proceedings of the 34th DAAAM International Symposium, pp.0103-0110, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-41-9, ISSN 1726-9679, Vienna, Austria
DOI: 10.2507/34th.daaam.proceedings.015

Abstract

With the development of technology and the growth of the number of devices connected to the Internet, cyber security is decreasing, and it has become a real challenge to secure systems and protect personal data. OSINT intelligence collects data from all publicly available and open-source databases, which makes enormous amounts of data available to everyone, including cybersecurity experts and attackers. Using the OSINT tool Shodan, this paper shows the vulnerabilities of certain European Union countries' protocols, devices, and services. Except for the analysis, the paper compares the obtained results to show how much certain countries invest in cyber security. This paper aims to increase awareness about cyber security flaws so that users can detect and protect them.

Keywords: Shodan, security investment; security problems; vulnerability scan

1. Introduction

One of the biggest challenges of today's time, accompanied by the rapid development of technology, is to protect private information and secure it against data theft. Users leave traces in the form of confidential data by using the Internet daily for any purpose. The amount of personal data on the Internet is enormous and entails specific security threats. When accessing certain websites and using social networks, blogs, and forums, data on the Internet is remembered and linked to individual persons, organizations, and devices. Accordingly, anyone can find much information about each individual or organization using a particular type of intelligence – OSINT (open source intelligence).

OSINT is a type of intelligence that collects information from publicly available data sources. With the growth of the number of users on the Internet and the amount of information available, several tools have developed that automatically collect information from various sources and make connections between individual entities. One of the OSINT tools is Shodan [1], which scans the IP addresses of devices and all available data by searching devices on the Internet. This paper presents the concept of OSINT and the exposure of information, i.e., the vulnerability of individual protocols, types of devices, and services in the Countries of the European Union. By analyzing the data, a comparison of the obtained results was made, and security recommendations for individual vulnerabilities were proposed. The paper aims to highlight how much respective countries invest in the security of devices exposed to the Internet and draw attention to possible shortcomings.

2. What is OSINT

OSINT is a type of intelligence that collects information and data from free and publicly available data sources. The term OSINT appeared in the 1980s and referred to conventional ways of gathering information such as newspapers, television, radio, or business reports. Information is collected from publicly available and open-source data sources, such as blogs, forums, or social networks. With the development of social networks and their popularization, an intelligence oriented explicitly to social networks – SOCINT began to develop.

With the development of the Internet and its capabilities, the way of collecting data has also developed. Information is often collected using search engines like Google, Bing, Yahoo, and others. In addition to classic search, information is collected through the deep and dark web. Deep web represents every page not indexed on web browsers, i.e., every website to which it is necessary to log in with user data. The dark web allows for secure search and implies every page whose access requires Tor protocol or any other way of protecting anonymity.

2.1. Tools used in OSINT

Maltego [2] is an OSINT tool for collecting data from publicly available data sources. The advantage of Maltego is that for each input, such as an e-mail address, name, IP address, organization, or website, it searches various databases to collect as much information as possible about the given information. With the information collected, the tool processes the data creates links between parts of collected data, and visually displays these links. All complex links of individual entities are presented, which significantly facilitates users to understand the information searched. The Maltego tool is one of the most commonly used tools for penetration testing in the reconnaissance phase where penetration testers seek to gather as much information as possible about the system they intend to attack.

SpiderFoot [3] is another OSINT tool that automatically collects information from various data sources. This open-source tool uses more than 100 publicly available sources to collect and connect information in one place. The advantage of this tool is the excellent documentation provided, which allows users to install the tool and run it easily and allows them to understand the tool itself, its processes, and its properties, and is available on all operating systems. SpiderFoot tool, like other OSINT tools, collects and processes data on domains, IP addresses, DNS records, networks, services, and many other information. When penetrating testing, SpiderFoot dramatically facilitates the collection of information and its analysis.

Metagoofil [4] is an OSINT information-gathering tool that collects metadata from publicly available documents, such as PDF, DOC, XLS, and PPT documents. Metagoofil is a free and open-source tool. To collect publicly available information, Metagoofil first searches available documents through Google then stores them locally and uses Hachoirh and PdfMiner tools to extract metadata from those documents. Like other tools, Metagoofil collects certain information about the default entity and associates it with specific user names, software versions, services, and devices.

3. Shodan

Shodan.io is a search engine that uses a database of all publicly available IP addresses and collects data on all devices connected to the Internet. In addition to searching the database of devices connected to the Internet, Shodan offers several additional tools that participate in better quality data processing. Shodan as a tool allows users to search for not only "normal computers" but also the Internet of Things devices, specialized devices connected to the Internet usually to serve a single purpose. When executing a Shodan search query, only the caption from the detected service is retrieved primarily, the metadata is not searched [5].

Banner grabbing is a method used to obtain information about a device, i.e. information about services, type, and version of software, and operating system, by searching for devices connected to the Internet and scanning for open ports such as HTTP (80), FTP (21) and SMB (445).

Banner grabbing uses tools to establish a connection to the device, such as telnet, nmap, wget, and curl. When a connection to the device is established, a request is sent to the device to which the remote device responds with *a banner* message. This message can then be used to gain additional info on the probed device.

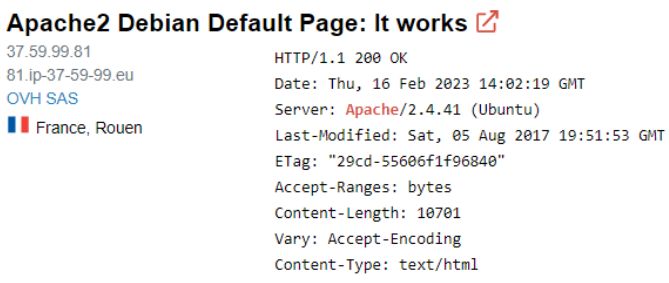

Fig. 1. Banner message

For example, a *search query* "Apache" was performed, which retrieves the results about Apache server users. In the above example in figure 1., a *banner* message is visible from which you can read information about the operating system and the latest changes on the website. To view the metadata of devices and services, the search query is not enough, but certain Shodan filters are used for this, which provide more specific search results. All filters are written as *"filter name": "value*". The table below shows some of the most common filters, which are later combined to perform more complex searches.

Filter Name	Description	example
Country	2-letter country code	country: HR
City	Name of the city	City: Zagreb
axis	Operating system	axis: windows
Org	The organization assigned the netblock	org: google
Port	Port number for the service	port:80

Table 1. Example shodan filter

If these are values consisting of two or more words, then those words are enclosed in quotation marks: City: "Novi Vinodolski". Any filter with a label before the filter's name indicates that the specified value is ignored, that is, we want to exclude it from the search. For example, to show all IoT devices in Croatia, except those in Zagreb: Country:City: Zagreb

As noted earlier, filters can be combined. For example, if you search for devices/services in Croatia, running on HTTP or HTTPS protocols, ports 80 and 443 will be added to the filter.
Country:HR port:80,443

4. Previous research - overview

In 2017, the study "Vulnerability Scanning of IoT Devices in Jordan Using Shodan" was conducted [6]. Internet of Things and IoT devices are always connected, providing the users with a set of data or some other functionality intended for online use. The problem is that users are not aware of or ignore that these devices are exposed to the Internet and that all their information is publicly available. The work seeks to raise awareness of IoT device vulnerabilities and potential loss of privacy and security and encourage more use of said devices.

The paper brings together IoT device vulnerability research with statistical analysis in May 2017. The study revealed 40849 IoT devices, of which 9.2% have UPnP (Universal Plug and Play) enabled. By enabling UPnP, the device automatically opens ports and becomes visible to other devices in the network. By analyzing some of the most common services on the Internet, it was found that of all devices that have HTTP enabled, 62% of them have successful HTTP connections. 41% of devices using the SMB protocol have authentication disabled and 26% have anonymous logon enabled, leading to the potential to compromise shared data.

The paper states that the use of telnet protocol, which does not encrypt data, is twice as popular or more frequent than SSH, which is safer. By analyzing other services, it was concluded that only 8% of FTP connections are successful and that a screenshot was created for 35% of RDP devices. A search of the device in Jordan found 16 devices exposed to the Ticketbleed vulnerability and 41 devices exposed to the Heartbleed vulnerability.

As a result of the analysis, the authors propose following experts' recommendations, which implies avoiding vulnerable services and disabling unused services. Users are advised to update devices and their services and appropriate device adjustment and authentication.

Another paper: “Vulnerability Analysis of Internet Devices from Indonesia Based on Exposure Data in Shodan” collected information for all networks publicly available in Indonesia using the Shodan tool [7]. The paper aimed to draw the attention of organizations that manage public networks to the exposure of Internet-connected devices in Indonesia and to become aware of these devices' vulnerabilities. Since there is a large number of IP addresses in Indonesia, categorized into 1699 separate networks (each having its own ASN - Autonomous System Number), in this paper, by a special method of grouping, IP addresses are divided into four categories depending on the level of exposure.

For the largest number of networks, 1075 of them do not have any information on Shodan. The low exposure category houses 614 networks and the medium exposure level category contains 9. Only one network is in the category of high level of exposure.

In the research of the work, all networks were scanned using a bash script that automatically scans all subnets for each network. For the 624 public networks about which there is information on Shodan, 289,715 queries were made and data on ports, services, domains, IP addresses, and operating systems were scanned. Of the nearly 12,000 unique ports found, 13.95% of the information found is related to the HTTP protocol, port 80. The collected operating system information shows that 35.87% of devices use Linux 3. x, followed by Windows Server 2012 R2 Standard with a significantly smaller 9.45%.

Further analysis found 98,152 information points about services that are predominantly distributed across the following services: MikroTik bandwidth-test server (33.37%), Apache httpd(16.54%) and OpenSSH (7.78%). For domain queries, the results of two top-level domains are highlighted – out of a total of 3350, 1881 are unique .id domains and 1242 are domain .com. The study concluded with the discovery of 145,543 unique IP addresses and 790 unique organizations.

5. Analysis of protocol vulnerabilities

In this part of the paper, one of the most commonly used protocols was analyzed – FTP, RDP, SMB, Telnet, and SSL. Some of these protocols do not use encryption at all and their use is not advised [8]. In contrast, other protocols are vulnerable only to some parameters and the correct configuration can protect the entire system [9]. Unless stated otherwise, each query contained the following filter for the countries: country: at, be, bg, hr, cy, cz, dk, ee, fi, fr, fr, de, gr, hu, ie, it, lv, lt, lu, mt, nl, pl, pt, ro, sk, si, es, se.

5.1. Results

After the analysis, the state of vulnerability of individual protocols for the countries of the European Union was determined. In this part of the paper, a comparison of the obtained results is done and the relationship of individual protocols with individual vulnerabilities is presented. Also prominent are the states with the best and worst results.

5.1.1 FTP protocol

By analyzing the FTP protocol, all open ports in the European Union countries were first scanned, then a query was made for these ports that have the possibility of anonymous access. The graph shows the relationship between open ports about the vulnerability enabled by anonymous access.

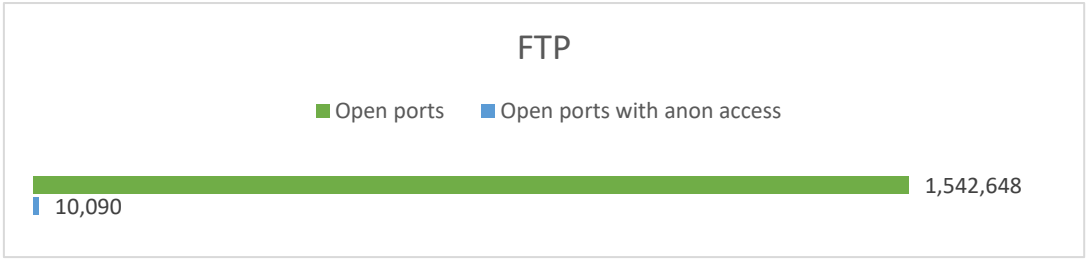

Fig. 2. FTP by port type

By querying the FTP protocol out of a total of 1,542,648 results, 35.76% of the results were found to originate from Germany. By analyzing ftp protocol vulnerabilities, i.e. analyzing ftp protocols with the possibility of anonymous access, it was found that 0.47% of scanned devices are vulnerable in Germany. The results obtained for Germany are twice as high as France's, which is placed second. The fewest scanned devices were detected in Montenegro, with 423 results, or 0.02% of the total results, and two found results of successful anonymous connection, making 0.47% of their devices vulnerable. Croatia is at the bottom of the scale with 3,663 results, of which 0.6% have the possibility of anonymous access. Given that certain countries have a larger population and thus a larger number of devices connected to the Internet is expected, the normalization of the results obtained for the two largest and two smallest results, as well as for Croatia, has been done. The following table shows the normalization of the results found about the number of Internet users to get a more faithful view of the results.

State	Number of Internet users	Open FTP ports	Percentage of open ports relative to the number of Internet users (%)	Open FTP ports with anonymous access capability	Percentage of vulnerable ports relative to the number of Internet users (%)
Germany	79,127,551	551,723	0,6972	2,608	0,0032
France	60,421,689	253,507	0,4195	1,336	0,0022
Cyprus	1,320,400	1,991	0,1508	8	0,0006
Montenegro	547,000	423	0,0773	2	0,0004
Croatia	3,787,838	3,663	0,0967	22	0,0006

Table 2. Normalization of results - FTP protocol

By analyzing the normalized results, it is realized that the number of scanned open ports, as well as the number of vulnerable ports, is still the highest in Germany.

5.1.2 RDP protocol

A search of devices that have port 3389 open for RDP protocol found 453956 results of which as many as 35.74% have a screenshot taken. A graphical representation establishes the relationship between these analyzed results.

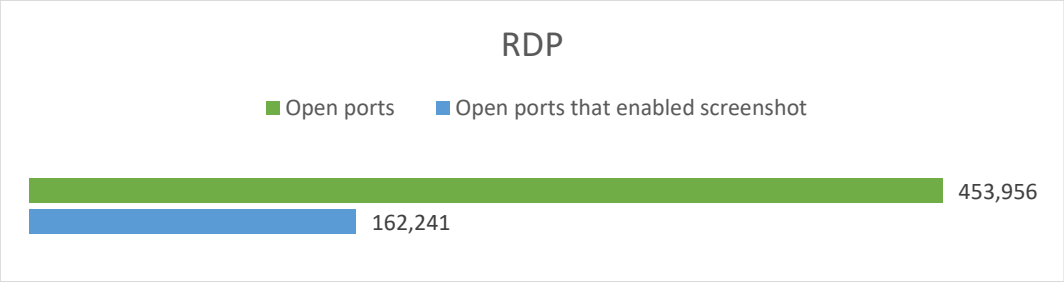

Fig. 3. RDP by ports

Further analysis of the results determined the re-lead of Germany, which contains 34.27% of the total score. In Germany, as in the FTP protocol analysis, twice as many devices were scanned as the country ranked second in the ranking, in this case, the Netherlands. The last country on the table is Montenegro with 220 scanned results, which is 0.04% of the total result. 1,856 results were found for Croatia, which makes up 0.4% of total scanned ports. The following table shows the normalization of the results found about the number of Internet users.

State	Number of Internet users	Open RDP ports	Percentage of open ports relative to the number of Internet users (%)
Germany	79,127,551	155,578	0,1966
Netherlands	16,383,879	79,507	0,4852
Cyprus	1,320,400	478	0,0362
Montenegro	547,000	220	0,0402
Croatia	3,787,838	1,856	0,0489

Table 3. Normalization of results - RDP protocol

By examining the normalized results, it is evident that Germany has a lower percentage of open RDP ports compared to the Netherlands, although in Germany twice as many open RDP ports were scanned. Table 2. also shows the same results obtained in Croatia and Montenegro.

5.1.3 SMB protocol

By analyzing the SMB protocol, queries were made for the total number of open ports, the number of ports using SMBv1, and the number of open ports with disabled authentication. The graph shows the ratio of the results of the above parameters.

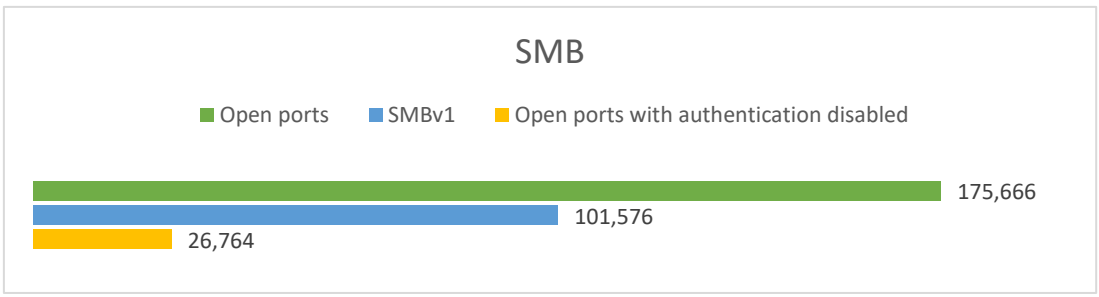

Fig. 4. SMB by protocol type

As in the previous two analyses, scanning the SMB protocol, it was found that Germany has the highest number of results, of the scanned 175 666 of which 51.85% are SMB of the first version and 7.99% of the results with untuned authentication.

Although the most overall results were found in Germany, France, which ranks second with 35,292 results, has the most results in the analysis of disabled authentication and is 63.09% unsafe due to the use of SMBv1. 13.28% of the results obtained in France have disabled authentication on SMB protocols. Montenegro is again in the last place of the rankings with 119 results, of which 50.42% is the first version and only 20.16% with authentication disabled. Croatia has 721 scanned SMB protocols, which ranks 22nd in the overall standings. Of the 721 results listed, as many as 71.56% are SMB of the first version and 33.28% with authentication disabled. The following table 3. shows the normalization of the results found about the number of Internet users.

State	Number of Internet users	Percentage of Open SMB Ports relative to Internet users (%)	Percentage of open SMB ports of the first version compared to Internet users (%)	Percentage of open SMB ports with authentication disabled relative to Internet users (%)
Germany	79,127,551	0,0667	0,0345	0,0053
France	60,421,689	0,0584	0,0368	0,0069
Luxembourg	636,565	0,0232	0,0153	0,0026
Montenegro	547,000	0,0043	0,0109	0,0044
Croatia	3,787,838	0,0190	0,0136	0,0063

Table 4. Normalization of results - SMB protocol

The normalization table noted partially more faithful results of the SMB protocol vulnerability. Compared to internet users in a particular country, Germany has the most scanned SMB ports, but in France, the number of vulnerabilities is greatest. France has the most SMBv1 vulnerabilities and the highest percentage of SMB ports with disabled authentication. Of these countries, Croatia has the highest percentage of vulnerabilities for disabled authentication, while in countries with a smaller number of Internet users, we see lower percentages of vulnerable devices.

For analysis of telnet, ports using OpenSSH were also scanned. Since it is heavily advised to use SSH protocol, the relationship between the obtained results is satisfactory. The use of OpenSSH tools is significantly more frequent than Telnet, which is evident in the following graph:

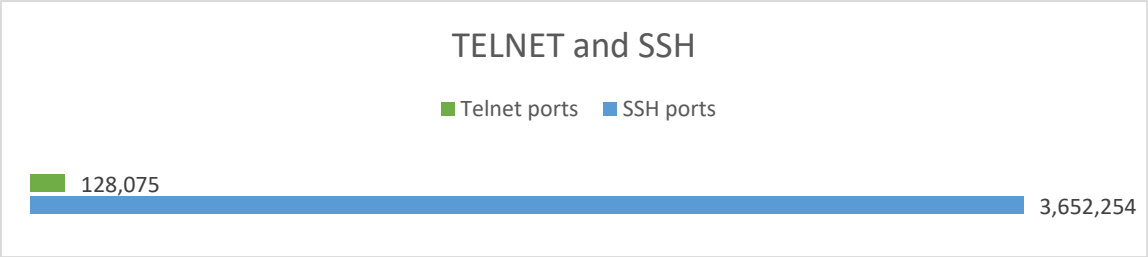

Fig. 5. Telnet and SSH – comparison by number of ports

By querying devices using Telnet (table 4.), 132,300 results were found. In the first place of the ranking of results by country is Italy, with 21.2% of the total. The last place is occupied by Luxembourg with only 97 results, or 0.07%. In Croatia, 1 556 open telnet ports contained 1.18% of total scanned ports. Given that SSH is a safe alternative to Telnet, the number of results for Telnet ports should be smaller, i.e. the expected share for individual countries should be smaller.

State	Number of Internet users	Percentage of Telnet ports open relative to Internet users (%)	Percentage of open SSH ports relative to Internet users (%)
Italy	54,798,299	0,0512	0,1765
France	60,421,689	0,0360	0,9442
Luxembourg	636,565	0,0152	0,9221
Montenegro	547,000	0,0230	0,0780
Croatia	3,787,838	0,0413	0,1156

Table 5. Normalization of results - Telnet and SSH

The normalized data for scanned Telnet and SSH ports revealed that Italy had the highest proportion of Telnet ports, followed by Croatia. Regarding SSH usage normalized by the number of internet users, France leads the pack. This notably impacts the security of devices connected to the internet nationwide.

By analyzing the SSL protocol, i.e. SSL certificates, a significant number of results were found, namely 2,445,148 expired certificates. A large proportion of these results, namely 814,544 (33.35%) are in Germany. The largest number of certificates issued by users themselves, i.e. *self-signed* certificates for the example.com domain, was also scanned in Germany, where 38.42% of such certificates were found. In Montenegro, 0.03% of expired certificates were scanned, which is a noticeably lower score than all other countries. When analyzing expired SSL certificates, Croatia positioned itself at the bottom of the scale with 0.19% of total searched certificates. For *self-signed* certificates for example.com, 110 results were recognized in Croatia, making 0.07% of the total results.

State	Number of Internet users	Expired certificates relative to Internet users (%)	Self-signed certificates for example.com about Internet users (%)
Germany	79,127,551	1,0294	0,0750
France	60,421,689	0,8141	0,0473
Cyprus	1,320,400	0,4071	0,0042
Montenegro	547,000	0,1592	0,0011
Croatia	3,787,838	0,1275	0,0029

Table 6. Normalization of results – Certificate expiration

With the normalization of the obtained results, a table was presented in which the percentage of expired certificates for Internet users in Germany is significantly higher than in other countries. Behind Germany, there is France with a slightly smaller percentage, but still large enough compared to other states. It is also evident that of the above results in table 5., Croatia has the lowest percentage of expired certificates.

6. Recommendations for protection against attacks

By analyzing device vulnerabilities by certain protocols, it was found that many devices are unprotected and can be compromised. Users do not necessarily have confidential or sensitive information, but it violates the privacy of the data. Given that these are frequently used protocols, several security recommendations for protection against attacks exist.

Earlier in the paper, it was noted that several FTP servers allow anonymous login, so the first step in security protection is to disable anonymous login, i.e. to force authentication on servers. Since the FTP protocol itself is not a secure protocol because it does not encrypt data, it is advisable to use a secure version of the protocol – FTPS (FTP Secure) or SFTP (SSH FTP) [20]. FTPS is an upgraded version of FTP that uses SSL/TLS to encrypt data, and SFTP is an upgraded FTP that runs on an SSH connection. Both protocols transmit encrypted data, but the difference is that FTPS is based on FTP and still uses TCP port 21, unlike SSH-based SFTP which uses TCP port 22. Unlike the FTPS protocol, SFTP does not offer the possibility of anonymous logins to the server.

By allowing the RDP protocol directly from the Internet, users are exposed to potential *BruteForce* attacks where attackers use automated tools to try to decipher the user account's password. The first step in protecting the RDP protocol is to set strong or complex passwords and adjust the system so that only a certain number of incorrectly entered passwords are allowed, after which the user account is locked. Users are advised to update the software regularly as updated software versions may contain patches of potential vulnerabilities. Also, when protecting the RDP protocol, it is necessary to take into account the restriction of access and connections on firewalls for RDP port 3389. The analysis shows that some devices do not have SMB authentication set. As a first security recommendation, authentication is necessary to secure the device. Furthermore, the use of the SMB protocol of the first version is not recommended due to certain security vulnerabilities that are listed earlier in the paper, but it is recommended to use the latest SMB version.

All traffic used by Telnet is not encrypted and not secure, therefore it is advised to avoid using Telentin in all cases. As an alternative to Telnet, a good practice is using the SSH protocol because all traffic, including login information, is encrypted. OpenSSH is a tool that allows users to connect to a remote computer with data encryption and secure transfer between devices.

The SSL protocol is considered outdated, and security experts advise using the TLS protocol, an upgraded version of SSL that ensures secure access to web servers. Given that the work has done an analysis of expired certificates and that a significant number of results have been found, users need to be aware of the importance of using the correct certificates and their renewal. Setting up automatic certificate renewal will avoid some of the vulnerabilities of SSL certificates. The use of certificates created and issued by users themselves, i.e. self-signed certificates, can endanger not only individual users, but also the entire system, so it is advised to avoid using them. When creating a website, users can use free SSL certificates to confirm their identity. If self-signed certificates are used, it is a necessary step to ensure that the attacker cannot reach the root certificate, otherwise, all the authorities to which he issued the certificate would be endangered[10] [11].

7. Conclusion

The development of technologies and the increase in the number of devices connected to the Internet have increased their security exposure. Most private users leave devices connected to the Internet with predefined configuration and predefined access data, which poses significant security threats and challenges against them. Especially when it comes to devices from the Category of Internet of Things whose purpose is to facilitate the daily life of users. but for this to be so, it is necessary to be aware that all these devices are publicly available and that predefined settings cannot be a satisfactory solution.

In parallel with the development of technologies, intelligence has been developed whose primary purpose is to collect data on all available and public devices on the Internet – OSINT. Although OSINT is often used with negative intentions, it is necessary to take advantage of this intelligence's benefits to find vulnerabilities and ensure. One of the OSINT tools useful in searching all devices connected to the Internet is Shodan, a browser that can find devices such as desktop computers to nuclear power plants. The paper presents a Shodan search of all European countries according to FTP, RDP, SMB, Telnet, and SSL protocols and analyzes the results obtained. Given that the number of found results depends on the number of inhabitants of a particular country, i.e. the number of Internet users, the paper normalized prominent data.

Potential future research directions should include development of more comprehensive and user-friendly tools for scanning and auditing of the devices connected to the internet. These tools could extend their scope beyond the protocols discussed in the text to encompass a broader array of services and devices. Exploring the utilization of machine learning and artificial intelligence for the analysis of the extensive data gathered through OSINT tools like Shodan holds significant promise as a research work. Such an approach has the potential to facilitate automated detection of vulnerabilities and mitigation of threats.

8. References

[1] Matherly, J. (2018). The Complete Guide To Shodan: Collect. Analyze, Amazon, ASIN: B01CDIU880, Amazon.com Services LLC

[2] https://www.maltego.com/about-us/, (2023). Maltego Technologies website, Accessed on: 2023-09-05

[3] https://www.spiderfoot.net/, (2023). Spiderfoot subsite, part of Intel471. Accessed on: 2023-09-05

[4] https://github.com/opsdisk/metagoofil, (2023). Kali Linux Fork of Metagoofil Tool Tepository. Accessed on: 2023-09-05

[5] Albataineh, A. & Alsmadi, I. (2019). IoT and the Risk of Internet Exposure: Risk Assessment Using Shodan Queries, 2019 IEEE 20th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), Washington, DC, USA, pp. 1-5, ISBN:978-1-7281-0271-9, DOI: 10.1109/WoWMoM.2019.8792986

[6] Al-Alami, H.; Hadi, A. & Al-Bahadili, H. (2017). Vulnerability Scanning of IoT Devices in Jordan using Shodan, 2017 2nd International Conference on the Applications of Information Technology in Developing Renewable Energy Processes & Systems (IT-DREPS), ISBN: 978-1-5386-1987-2, DOI: 10.1109/IT-DREPS.2017.8277814

[7] Novianto B.; Suryanto, Y. & Ramli, K. (2020). Vulnerability Analysis of Internet Devices from Indonesia Based on Exposure Data in Shodan. Proceedings of International Conference on Science, Technology, Engineering and Industrial Revolution (ICSTEIR 2020), Vol 1115, ISSN 1757-8981, DOI: 10.1088/1757-899X/1115/1/012045

[8] Dakic, V.; Jakobovic, K. & Zgrablic, L (2022). Linux Security in Physical, Virtual, and Cloud Environments, Proceedings of the 33rd DAAAM International Symposium, pp.0151-0160, B. Katalinic (Ed.), Published by DAAAM International, Vol. 33, No.1, ISBN 978-3-902734-36-5, ISSN 1726-9679, DOI: 10.2507/33rd.daaam.proceedings.021, Vienna, Austria

[9] Perakovic, D.; Husnjak, S. & Remenar, V. (2012). Research Of Security Threats In The Use Of Modern Terminal Devices, Annals of DAAAM for 2012 & Proceedings of the 23rd International DAAAM Symposium, Volume 23, No.1, ISSN 2304-1382 ISBN 978-3-901509-91-9, CDROM version, Ed. B. Katalinic, Published by DAAAM International, Vienna, Austria

[10] Babic, M.; Stanojevic, M.; Ostojic, G.; Tegeltija, S. & Stankovski, S. (2022). Industrial Cyber Security Aspects in ICS Applications, Proceedings of the 33rd DAAAM International Symposium, pp.0326-0331, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734- 36-5, ISSN 1726-9679, DOI: 10.2507/33rd.daaam.proceedings.045, Vienna, Austria

[11] Reithner, I.; Papa, M.; Lueger, B.; Cato, M.; Hollerer, S. & Seemann, R. (2020). Development and Implementation of a Secure Production Network, Proceedings of the 31st DAAAM International Symposium, pp.0736-0745, B. Katalinic (Ed.), ISBN 978-3-902734-29-7, ISSN 1726-9679, DOI: 10.2507/31st.daaam.proceedings.102, Vienna, Austria