Engineering Applications

https://publish.mersin.edu.tr/index.php/enap

e-ISSN 2979-9201

Training of information technology personnel through simulations for protection against cyber attacks

Fatmir Basholli [*1], Besjana Mema [2], Albina Basholli [3]

[1] *Albanian University, Department of Engineering, Albania, fatmir.basholli@albanianuniversity.edu.al*
[2] *Mediterranean University of Albania, Department of Information Technology, Albania,* besjana.mema@umsh.edu.al
[3] *Polytechnic University of Tirana, Faculty of Mathematics Engineering and Physics Engineering, Albania, a.basholli@fimif.edu.al*

Cite this study: Basholli, F., Mema, B., & Basholli, A. (2024). Training of information technology personnel through simulations for protection against cyber-attacks. Engineering Applications, 3 (1), 45-58

Keywords
Simulation
Platforms
Cyber security information
Cyber attacks

Research Article
Received: 24.08.2023
Revised: 04.01.2024
Accepted: 10.02.2024
Published: 16.02.2024

Abstract

Nowadays, the development of information technology, robotics and artificial intelligence, has brought radical changes in every aspect of people's lives and this has made our lives have a lot of access to contemporary information and technology. These technological developments in many areas of business and telecommunications, in addition to their benefits, have also increased the risks. Users should be very careful when using social networks, various applications and navigating the Internet world because the risk of cyber-attacks by irresponsible persons with malicious intentions is very frequent. So, web applications make it possible for website visitors to record data or access data through the browser, where all this data is stored in the website's database, which is often the target of cyber-attacks where the attacker has read access, attempts to modify and delete data from the database. This paper aims to provide the necessary information about attacks and cyber hygiene, where we will recommend the review and analysis of these attacks using tools from the MetaSploit library which is a framework that makes hacking easier and is also a tool essential for many attackers and defenders. So MetaSploit helps developers and web administrators from this library to keep up with the times and take preventive measures against the tricks of irresponsible people.

1. Introduction

In the early days of the Internet, most web pages contained various and important definitions, documents, files, references or studies. And since that time there are cyber attackers with the motto " Hit and Go ". In most cases, these attacks are aimed at modifying documents and most of these attacks were carried out for fame and reputation, where at that time most organizations only had a firewall between the organization's network and the Internet [1-3]. Today in trend are institutional platforms taking on the proportions of a cyber war, social networks that are increasing every day, and with this development the insecurity of the users of these platforms and networks is also increasing, where personal data and national security [4-7].

In September 2018, a cyber-attack was reported on Facebook accounts, which admitted that an unknown hacker or group of hackers exploited a vulnerability in its social media platform that allowed them to steal more than 50 million accounts. which were used for double authentication to access Facebook. In the month of July, September of 2022, the Albanian national platform e-albania was "severely" attacked by Iranian hackers, temporarily interrupting services to citizens and violating elements of national security [8-9].

Today, cyber-attacks are modified and well organized which are analyzed and prepared in a special way for the organization they are targeting, modern attacks are undertaken from which hackers aim to benefit material or financial goods. So, the best protection against Internet attacks is achieved when we understand how these cyber-attacks actually work, where below we will tell about the types of computer attacks and what we currently have available for their protection and avoidance. While cyber security is the objective measurement of behaviors taken to maintain security and strengthen defenses against cyber-attacks, cyber hygiene relates to internet security

knowledge and practices related to further enhancing security. In conclusion, to improve cyber security, we need to improve cyber education and training [10-12].

2. Material and Method

In carrying out the study, we used data collected from global, regional and national (Albanian) infrastructures for vital assets, IT systems, physical or virtual networks that must be highly protected.

2.1. Statistics about cyber attacks

In Google search engines, one in ten web pages contain different codes or scripts with profit purposes, where 70% of web pages are exposed to attacks and that approximately every 40 seconds, a cyber-attack by hackers occurs in the world, while only 38% of the world's organizations are prepared against a modern cyber-attack [13-15]. From the annual report of the year 2022, of the Albanian National Authority for electronic certification and cyber security, the sectors and infrastructures that are continuously monitored have been identified and classified, of which we can mention: - First, the Energy sector with 14 critical information infrastructures and 13 important information infrastructure. - The second Transport sector with 31 critical information infrastructures and 6 important information infrastructures. -The third banking sector and the Insurance Market with 20 critical information infrastructures and 52 important information infrastructures. - The fourth Health sector with 17 critical information infrastructures and 8 important information infrastructures. -The fifth Water Supply sector with 6 critical information infrastructures and 44 important information infrastructures. - The sixth Digital infrastructure with 54 critical information infrastructures and 25 important information infrastructures [16-18].

Globally, the three most attacked sectors in 2022 were education/research, public administration and health. The global volume of cyber-attacks reached a historical record in the fourth quarter, with an average of 1,168 weekly attacks per organization. Cyberattacks are on the rise worldwide, with an average weekly increase in corporate networks of 38% in 2022 compared to 2021. Academic institutions have become popular ground for cybercriminals, especially after the rapid digitization that they undertook in response to the COVID-19 pandemic. In fact, the education/research sector is the first most attacked sector globally, with a 43% increase in 2022 compared to 2021, where an average of 2,314 weekly attacks per organization were observed. Schools and universities also face the unique challenge of having to deal with children or young people, many of whom use their own devices, work in shared locations and often connect to public WiFi, not thinking about security complications [19 -21].

2.2. Types of cyber attacks

The main goal of a cyber-attack in most cases is to steal and expose sensitive data, whether it is customer credit card data or other personal data, which is used to manipulate people's personal identity online.

DDoS is an abbreviation for Distributed Denial of Service attacks. DoS attacks are among the simplest attacks today which do not aim to steal, modify or destroy information, but aim to prevent a user from using a job. A DoS attack comes in many forms, from as simple as severing a system's power, or flooding a system until it is intercepted in network traffic. The public nature of the Internet makes it particularly vulnerable to DoS attacks that go so far as to question the validity of a server [22]. Some of the types of attacks (DOS) are: TCP SYN Flood Attack; UDP; Ping of Death Attacks; ICMP

The simplest ICMP message types are:

Echo Reply; Destination Unreachable; Source Quench; Redirect; Alternate Host Address; Echo; Router Advertisement; Router Request; Time Exceeded; Problem Parameter; timestamp; Timestamp Reply; Information Request; Information Reply; Address Mask Request; Address Mask Reply; Traceroute; TTL Expiration; Smurf Attacks; Teardrop Attacks; Bonk Attacks; Land Attacks; Malware.

A virus is a piece of computer code, which is attached to an application program or a file. Some viruses can cause damage, such as damaging programs, deleting programs, deleting files and even the entire contents of the data storage disk (hard drive). Some viruses that are used more often today are: Trojan; Horse; Spyware; Rootkits; Password Attacks (Brute Force).

Brute-force attack, which involves trying different passwords until the correct password is found. A dictionary attack uses a program that tries different combinations of words in a dictionary, while a keylog attack tracks a user's keystrokes, including their ID and password.

Phishing, with some of its types:

Spear phishing – Phishing attempts directed at specific individuals or specific companies are called spear phishing. Attackers can collect personal information about their target thus increasing the chance of success. This technique is known to be the most successful on the Internet, accounting for 91% of all phishing attacks.

Clone phishing – A type of phishing where a legitimate email previously sent with the content of a link or tab has hijacked the recipient's content and address to create an almost identical cloned email. The tab or link in the email is replaced with a fake version and sent to the recipient appearing as legitimate and original.

Whaling – Various phishing attacks directed at senior executives and other high-profile targets in the business world have received the term whaling. In this type of attack, the fraudulent website or email takes a more serious form at the executive level. The content will be designed to target a senior manager and the person's role in the company.

Rogue Wifi – Attackers set up free Wifi access points and configure them to play the role of Man in the middle, often with tools like SSLStrip.

Phone Phishing - Not all phishing attacks necessarily require a fake website. Messages that appear to be from a bank telling users to contact a phone number about problems with their bank account. Once the phone number (owned by the attacker and with VOIP service) is contacted, the user is told to give the account number and pin.

Vishing (Voice phishing) - sometimes use fake caller ID to make it look like the call is coming from a trusted organization.

Link manipulation - Most phishing methods use some form of technical deception designed to make a link in an email appear to belong to the organization. Modified URLs or the use of subpages are common tricks used by scammers.

Ransomware is a type of malware that infects a computer, where, as the name implies, it demands a ransom. Usually, the use of ransomware either removes access to your computer and demands money in return for access, or threatens to publish your personal information unless you pay a certain amount of money. Recently, Ransomware is one of the fastest growing cyber-attacks.

One of the Ransomware viruses is the WannaCry virus, which encrypts your data on the personal computer and then asks for an amount of money (Bitcoins) to decrypt your data by sending you a Key. This virus began its operation on May 12, 2017, where within 48 hours it reached about 230,000 victims from 150 different countries of the world. WannaCry infiltrated systems through a bug in Microsoft Windows more precisely (SMB) through which it spread the virus to all the other computers that were connected to that network, so the easy way to penetrate other computers made from this virus suffer many victims. With WannaCry, all those users who use the Microsoft Windows operating system can be infected or be targeted. Most victims of WannaCry were infected by clicking on various links that the hackers distributed in emails.

Zero-Day attacks are the type of attacks that are known to be the greatest anxiety of developers. These are software or system flaws that a hacker discovers before developers or security staff are aware of them. What gives this attack its advantage is that these flaws can remain undetected for months, even years until they are discovered and avoided.

These were some of the most frequently used cyber-attacks that we examined from the very long list that also includes other attacks, where it seems that this list will be added even more in the future as long as there are new discoveries and developments technological [23-24].

2.3 Creation of a Metasploit project on methods for studying attacks

Metasploit is basically a versatile testing and penetration framework, it can perform literally all the tasks involved in a testing lifecycle. Also, since it is a complete Framework and not just an application, it can be configured (customized) and extended according to our requirements [25]. MetaSploit is used to test and analyze the vulnerabilities of computer systems for access to system control and is among the main tools of Ethical Hackers or White Hat's or groups responsible for cyber security, not only for identifying any errors or defects. Its specialty is that it allows you to be a step or two ahead of ordinary attackers.

Gather information - Use tools such as Discovery Scan, Nexpose scan, or import tools to supply Metasploit Pro with a list of targets and services of open ports associated with those targets.

Exploit- Use smart exploit or manual exploit to launch attacks against targeted machines. Additionally, you can perform bruteforce attacks to escalate account privileges and gain access to exploited machines.

Perform post-exploitation - Use post-exploitation modules or interactive sessions to further interact with information from compromised targets. Metasploit Pro provides you with several tools that you can use to interact with open sessions on an exploited machine. For example, you can view shared file systems on the compromised target to identify information about internal applications [26].

Clean up open sessions - Use the Clean Up option to close any open sessions on an exploited target and remove all evidence of any data used during the penetration test. This step restores the original settings on the target system.

Generate Reports - Use the reporting engine to generate a report detailing penetration test findings. Metasploit Pro provides several types that allow you to define the type of information that the report includes.

From the monitoring of some state institutions and Internet Service Providers (ISPs) operating in Albania for the year 2021, (Table 1) which generated malware with a source in Albania and destination in different countries, the following extracted data were identified from this monitoring. Below are tables with relevant data for two institutions and for four ISPs, identifying them with institution 1 and institution 2, as well as ISPs, with ISP-1 to ISP-4.

Table 1. The number of malware generated in the months of May-June 2021.

The year 2021	Number of Malware			Number of Malware		
Months	Institution-1	Institution-2	ISP-1	ISP-2	ISP-3	ISP-4
May	882	1286	17109	85759	15494	73210
June	1155	1078	21256	89745	15135	1792
July	334	1771	19358	87572	7171	114
August	109	115	11200	50322	3785	326
September	135	261	11154	38159	416	410
October	178	193	16516	54494	60	796
November	100	250	15431	47861	51	912
December	148	267	15360	38613	52	892

2.4 Metasploit vulnerable services emulator

Many IT professionals and engineers want to learn and train in security as it is a current area of concern. There are many tools, one of the most famous is Metasploit. A common route for someone to teach themselves security is to download Metasploit and play around with it. However, without tangible services to test, it is difficult to play with Metasploit. This tool can be run on Linux (Ubuntu) and Windows platforms. It is designed to reproduce or emulate tangible servers in order to test Metasploit modules, help with Metasploit training. To make adding a replicated service as easy as possible, we design it to be language independent. The service playback is in JSON format, one can add/remove/modify the JSON very quickly. A small but interesting feature is that we make it easy to create SSL Sockets, all TCP Sockets can be automatically promoted to SSL [27].

2.5 Hacking Hackazon

It is a free and tangible trial site, which is an online store built with the same technologies used by the most affluent customers and mobile applications. Hackazon has an AJAX interface, strict workflow and RESTFUL API'S used by a partner application providing training with unique effects and basic training for IT professionals, and is packed with your favorite vulnerabilities like SQL Injection, Cross -Site Scripting and others. Today's web sites and applications, as well as site services host new technologies that are not regularly tested for vulnerabilities, it is critical for security IT professionals to have a tangible page that they can use to test the effectiveness of their tools and advance their skills. Hackazon allows users to configure application firewalls to change the appearance of vulnerabilities to prevent "known vulnerability testing" or other types of "cheats". Since the application includes RESTful interfaces that enable AJAX functionality and mobile clients (JSON, XML, GwT, AMF), users will need the latest testing tools for application security, and techniques to detect all vulnerabilities (vulnerabilities). Hackazon also needs detailed testing of strict functionality, such as shopping carts that are often used in applications [28-30].

2.6 VM-automation

The virtual machine automation (vm-automation) repository was created to simplify interaction with virtual machines (vm). Specifically, it was built to support automated testing by simplifying interaction with VMs (virtual machines). Currently, it supports VMWare Workstation through vmrun.exe and ESXi.

2.7 InsightVM

By analyzing the vulnerabilities detected in the scans, an essential step can be taken in improving your security posture. This is a phenomenon that InsightVM tries to address, by examining the frequency, affected assets, level of risk, exploitability and other characteristics, you can then prioritize fixes and improvements and manage your security resources effectively (Figure 1).

Every vulnerability discovered in the scanning process is added to the vulnerability database. This extensive and highly searchable full-text database also stores information on downloaded fixes, reference content, and security vulnerabilities. The application keeps the database current through a subscription service that maintains and updates the definition of vulnerabilities. This application contacts this service for new information every six hours (Figure 2).

The database is certified to be compliant with MITER Corporation's Common Index of Vulnerabilities and Exposures (CVE), which standardizes vulnerability names across products. The index evaluates its vulnerability according to MITRE's Common Vulnerabilities Scoring System (CVSS) version 2 and version 3, if available.

Viewing vulnerabilities and their risk scores helps you prioritize remediation projects. You can also find out which vulnerabilities have been exploited, enabling you to verify those vulnerabilities.

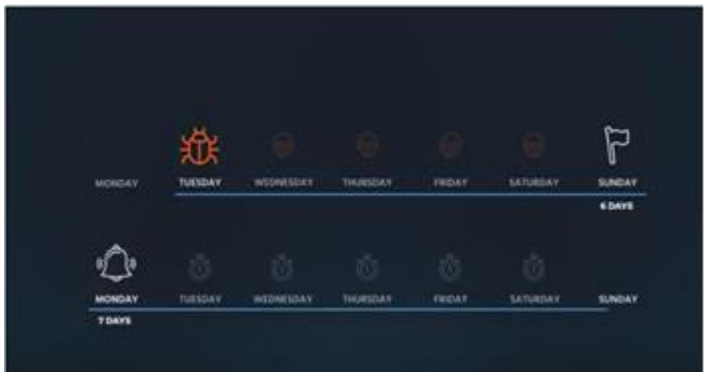

Figure 1. Overview of InsightVM.

Figure 2. InsightVM runtime.

2.8 InsightIDR

InsightIDR is your security hub for incident detection and response. The InsightIDR app identifies unauthorized access from external and internal threats and highlights suspicious activity, so you don't need to sift through thousands of data streams. This application is a Software as a Service (SaaS) tool, which collects data from your existing network security tools [31-32].

InsightIDR then aggregates the data into an on-premises aggregator or dedicated host that centralizes your data (Figure 3).

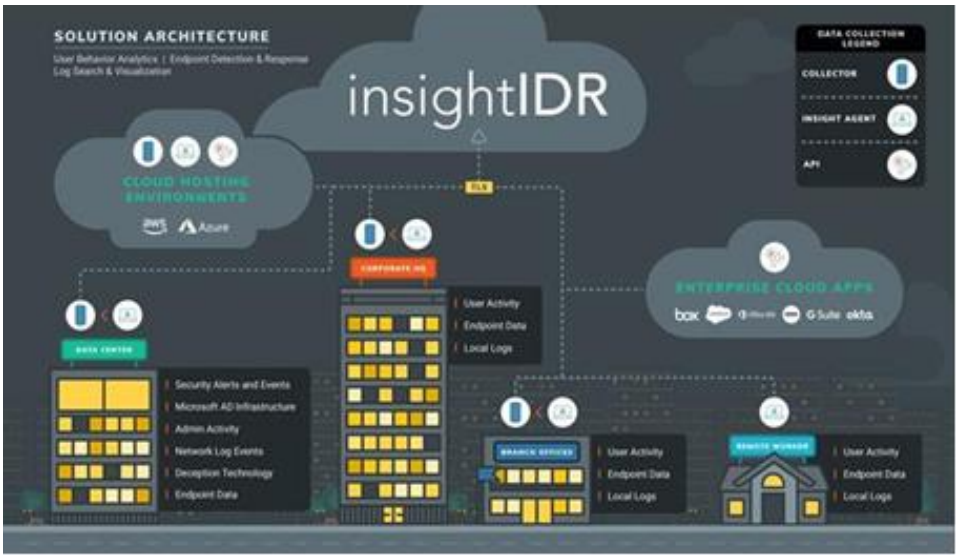

Figure 3. Overview of InsightIDR.

When you connect all the different data streams in InsightIDR, you can benefit from all the following features [33]:

- Unify your data into a single security view.
- Analyze raw logs, endpoint data, and network traffic.

- Receive alerts for suspicious activity.
- Prioritize events.
- Investigate the events.

3. Results

3.1 Protection from cyber attacks

The way of life that is developing today has made people and many businesses exposed to attacks by many hackers, this has been made possible by the increase in the number of smartphones, various technological devices that have increased the potential for these to happen attacks. Another phenomenon that is considered a weakness by cyber attackers, but for many businesses it increases the company's profitability, is also Internet banking and mobile banking, through which hackers steal information in order to assume your personal identity and then use it for something other, such as transferring money, obtaining a loan, etc.

Today's market includes several basic types of software used for protection against cyber-attacks, which simultaneously provide different levels of protection for individuals and organizations [34-35].

Antiviruses are the most common software that will protect you from most types of malwares. Various companies build antivirus software that is based on several essential functions:

Allows you to schedule scans to automatically work for you.

It allows you to start a scan of a specific file or your entire computer, or even a CD or flash drive at any time.

Removes any detected malicious code. They tell you about the "health" of your computer.

Firewalls can be implemented as hardware or software, which provide an additional protection mechanism preventing a user from accessing a computer or network in an unauthorized manner. Most modern operating systems, such as Windows 10, have incorporated a firewall program [36-38].

Keep your software up-to-date, as a computer that doesn't get its system updates is more exposed to crashes, security vulnerabilities, and cyber-attacks than a computer that gets updates regularly. The job of hackers is to constantly scan for security weaknesses in systems and networks, and if you keep those weaknesses for a long time without fixing them, then you increase the likelihood of falling victim to a cyber-attack [39].

Employee cyber hygiene education ensures your company's employees are aware of the ways cybercriminals can infiltrate your system, educate employees to recognize the signs of a security breach, and train them on how to maintain security while using your company's network, especially when working remotely (home) [40].

Applying formal security policies is essential to sealing your system against attacks. Securing the network should be everyone's concern, as everyone who uses it presents a point of weakness that a hacker can exploit. Organize regular meetings and seminars on Internet security best practices, such as using strong passwords, identifying and reporting suspicious e-mails, clicking on links or downloading e-mail attachments, etc. [41].

You should keep in mind that there is no one-size-fits-all security solution, so you should first carry out a risk assessment preferably by a specialist external firm, and after a thorough analysis of the risk and ways of its solution to decide on the best possible alternative [42].

If you want to protect your small or medium business and its data, you can consider some of the practical tips listed in order of importance:

The first is the data storage solution (Backup), so that data that may be compromised or lost during a security breach can be returned from an alternative location.

The second is to use encryption software to protect sensitive data, such as employee data, financial data, and customer data.

The third is to use two-factor authentication or some password security software for internal company programs to reduce the possibility of password cracking.

3.2 Simulation project with DoS attacks

A DoS cyberattack is an attack in which the attacker seeks to make a machine or network resource unavailable to its user, temporarily or indefinitely disrupting the services of a host connected to the Internet. Denial of service is typically accomplished by flooding the target machine or resource with excessive requests in an attempt to overload systems and prevent some or all legitimate requests from being met (Figure 4).

The DoS (Denial of service attack) simulation begins when the client tries to connect to the system using the TCP protocol (HTTP or HTTPS), where it first requires handshakes to be performed before exchanging data between them.

In SYN flood, the attacker sends large content in packets towards the system where he forces the system to return a response and leaves the port half-open, where he expects a response from the client which does not exist.

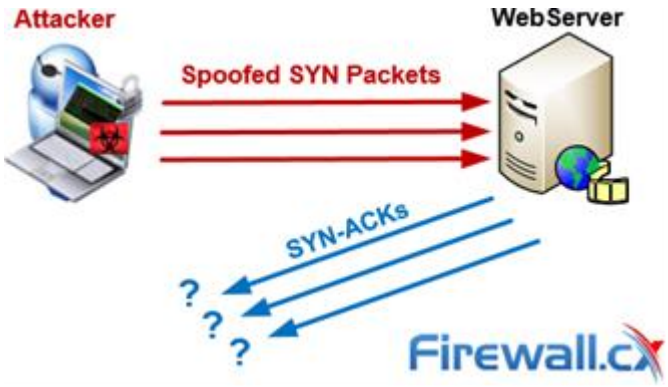

Figure 4. DoS attack presentation.

So before we start the simulation, we identify the attacker and the victim where both use Windows operating systems. The steps we must follow to simulate the attack are the commands after opening the MetaSploit Framework. Now we will illustrate the simulation steps through pictures (Figure 5-11) step by step: Msfconsole is the command that activates the Metasploit Framework [43-47].

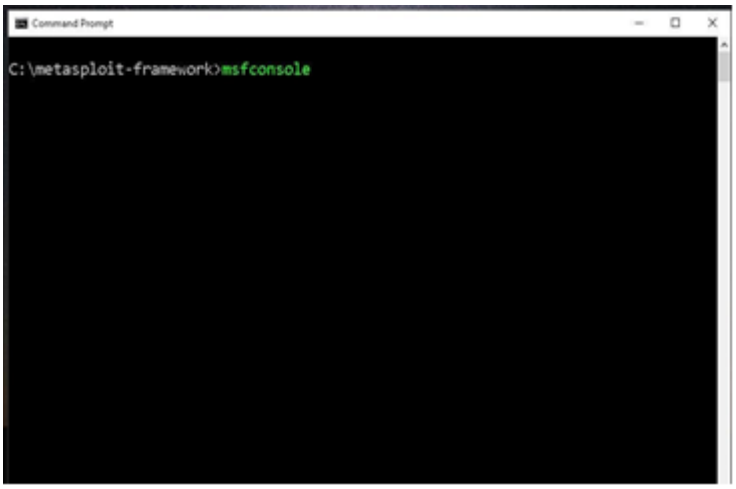

Figure 5. Msfconsole command view.

In the second image Metasploit is activated with 1926 exploits- 1075 auxiliary- 330 post, 556 payloads -45 encoders- 10 nops, 7 evasion.

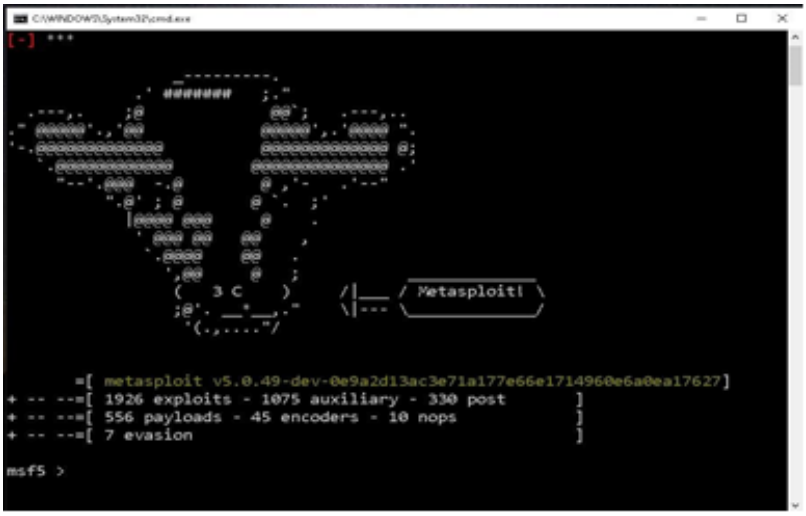

Figure 6. Metasploit view.

-We use the command "use auxilitary/dos/tcp/synflood" to demonstrate the DoS attack
-“set RPORT 80” sets port 80 for synflood in Metasploit.

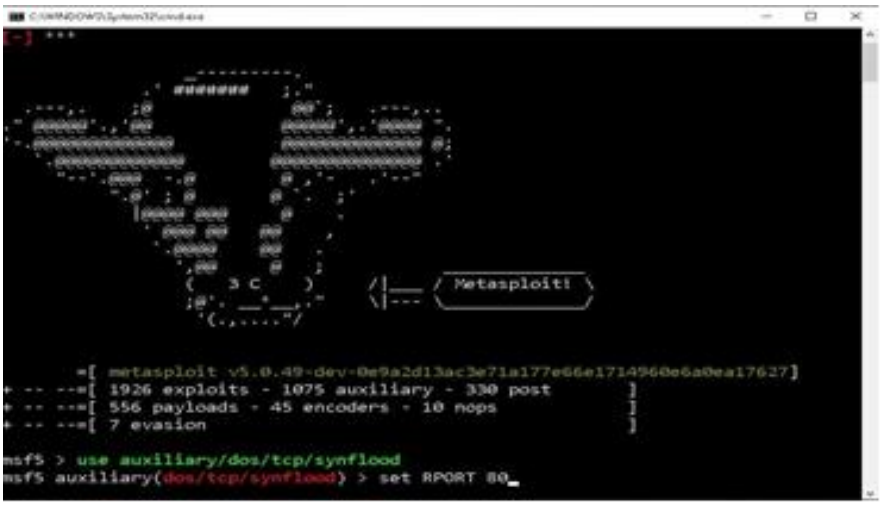

Figure 7. The view of Metasploit after using the "auxiliary" command.

-“set RHOST 192.168.0.29” cakton IP si destinacion per ekzekutimin e DoS attack.
-"set RHOST 192.168.0.29" sets the IP as the destination for executing the DoS attack.

Figure 8. Results of the "auxiliary" command.

-“exploit” ekzekuton sulmin DoS në IP, portin e caktuar me exploit-in që ofron Metasploit.
-"exploit" executes the DoS attack on the IP, port specified with the exploit provided by Metasploit.

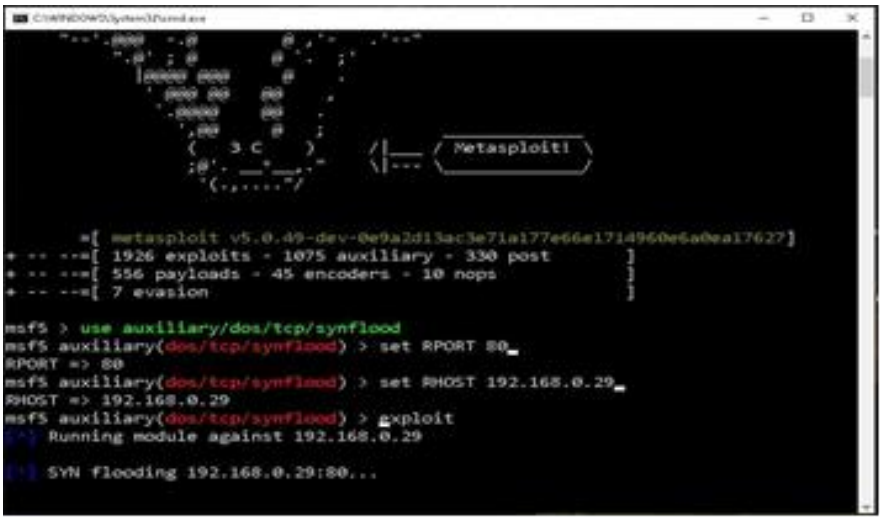

Figure 9. Execution of the "exploit".

In this part it is seen how the execution of the Auxiliary module of SYNflooding is completed for the IP and port specified above.

Figure 10. Execution of the "Auxiliary" module of "SYNflooding".

"exit" command closes the processes of Metasploit Framework and with this ends the simulation of DoS SYNflood cyber-attack according to Metasploit.

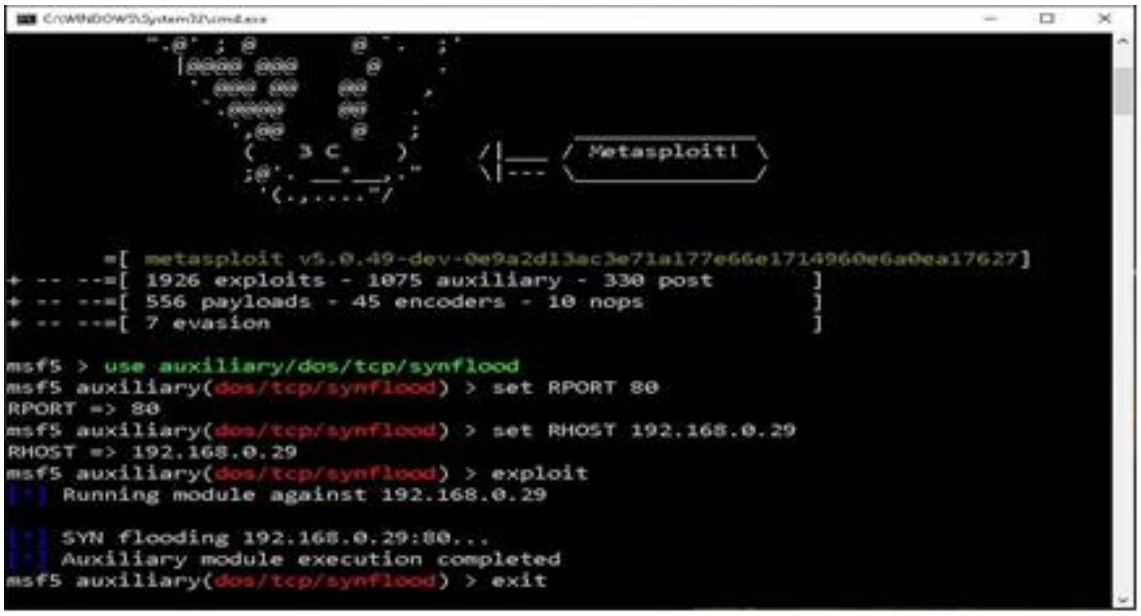

Figure 11. Execution of the "exit" command.

4. Discussion

After the DoS SYNflood cyberattack on Metasploit towards the Windows operating system with IP Address 192.168.0.29 and port 80, to analyze the effects of the simulation on the above-mentioned host we used WireShark software and taskmanager to see the effects caused by the simulation of demonstrated above with Metasploit. So, the administrator is able to identify the attack based on TCP Traffic which has been overloaded.

To filter packets without approval from the system, we use the command: " tcp.flags.syn == 1 and tcp.flags.ack == 0"

In this case, the Figure 12, which presents packets with very large contents in a very short time, where each packet comes from the attacker's address with destination port 80.

To see how many packets converge with the system, use the command: "tcp.flags.syn == 1 and tcp.flags.ack == 1".

Where we notice that the number of packets (Figure 13). that converge is very small, from the ratio 259298:261 that made us understand that we were dealing with a DoS attack [48-54].

The Figure 14 shows the normal state of the CPU and RAM before the DoS TCP Syn Flood attack.

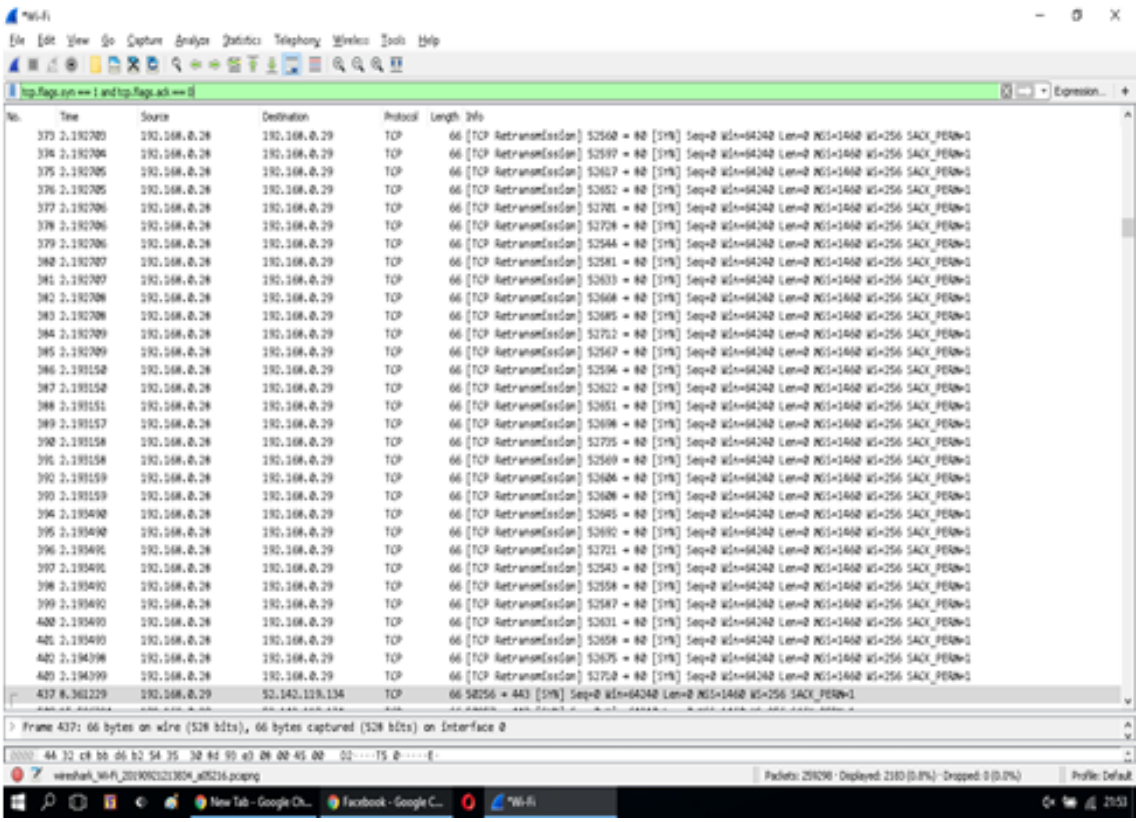

Figure 12. Pamja e paketave nga adresa e sulmuesit me destinacion portin 80.

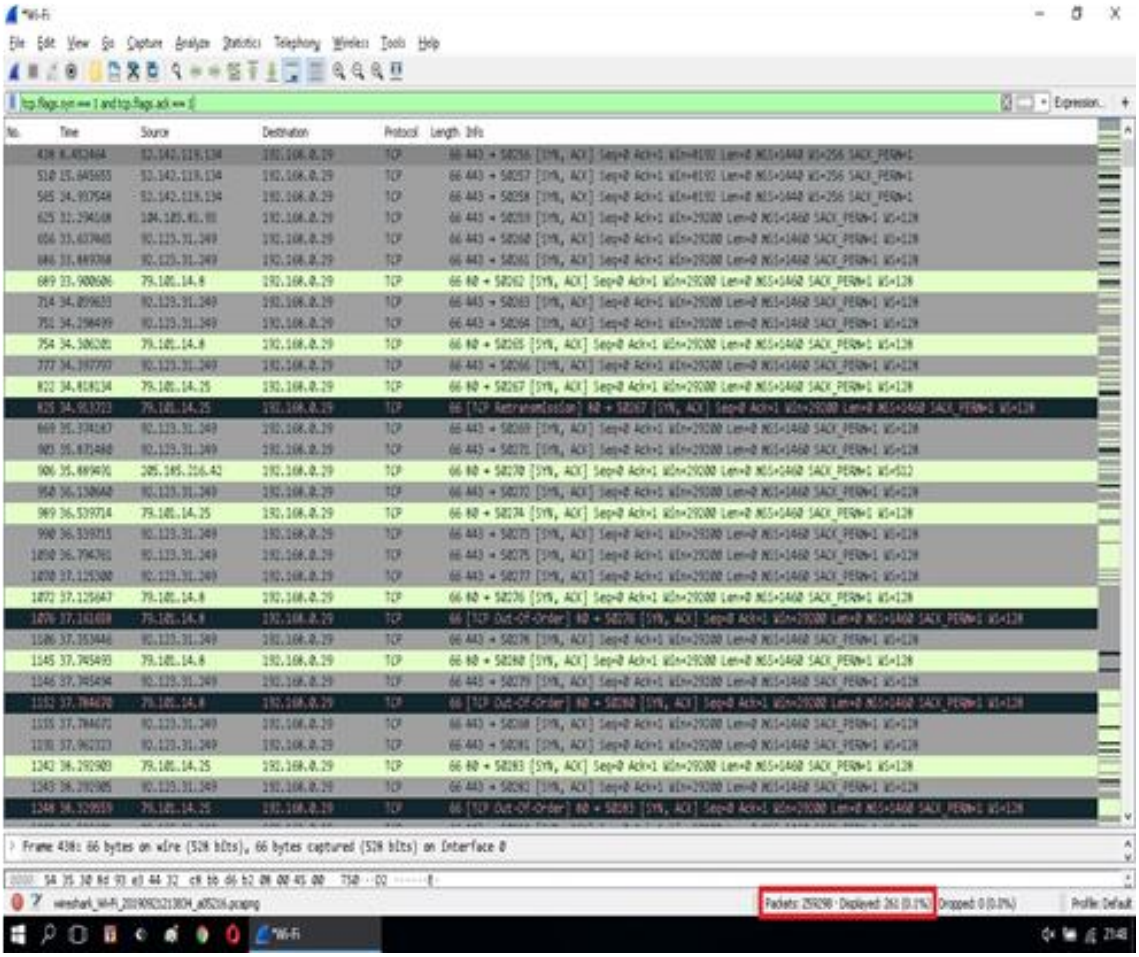

Figure 13. Number of converged packets.

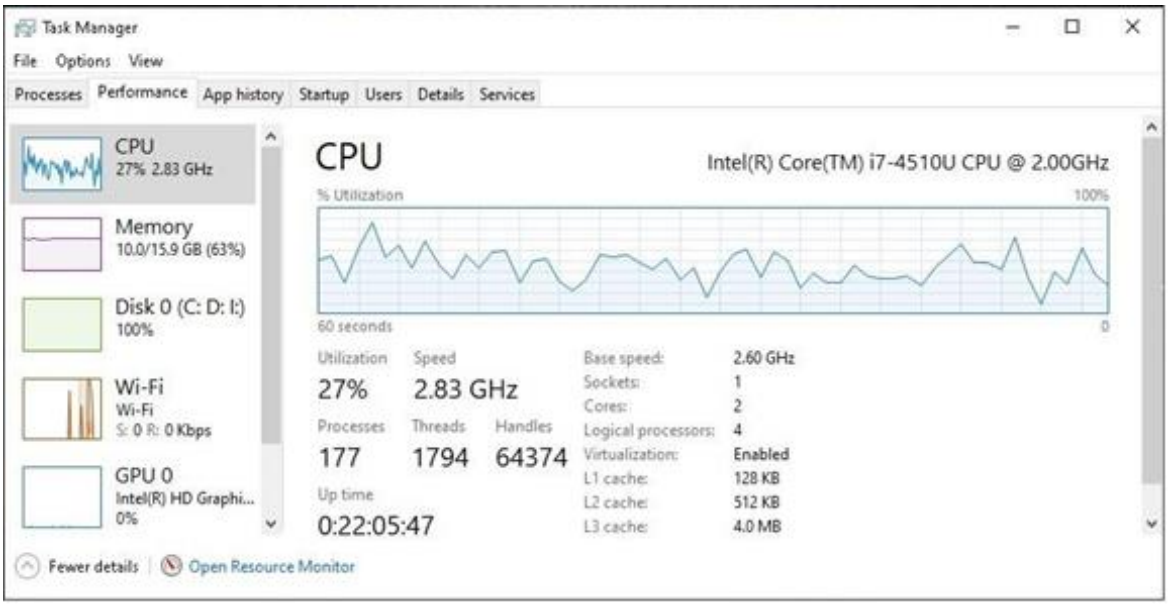

Figure 14. State of CPU and RAM before the attack.

Also, how does the DoS attack affect the System resources in the CPU and RAM (Figure 15).

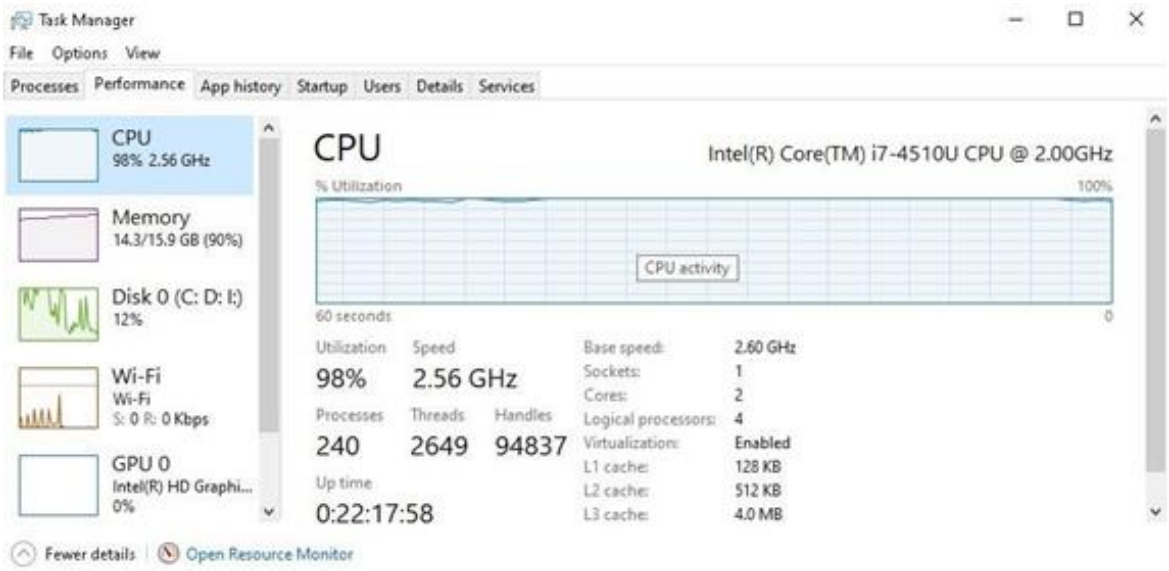

Figure 15. State of CPU and RAM after the attack.

5. Conclusion

Cyber-attacks include a field for which we must work and study a lot, in order to fundamentally understand the problems that this phenomenon can cause. The consequences that can come from this phenomenon can be from embarrassing posts on the Internet, to the theft of money from the bank account and interference in institutional platforms. People who may be victims of these attacks must be informed about cyber hygiene, accurately and be prepared with regard to any security offered on the market for this phenomenon, so that they can overcome the consequences caused by the attacks.

Despite the advantages and rapid development that technology brings, it has shown that it also has dark sides. Users of web applications are often not aware of their actions, and through social engineering, the attacker tricks the user into indirectly handing over all personal data to the attacker. Therefore, it is not possible to completely stop attacks, but we must try to minimize them as much as possible.

Since with the expansion of technology and the opportunities it offers us, the use of the Internet also increases, the likelihood of cyber-attacks increases, so we must fight this by training IT staff and informing them of new developments in the field, as well as we train user personnel with cyber hygiene [55-61].

Acknowledgement

We are grateful to the Editorial Board of the AED 7 symposium for allowing us to participate in this international conference. We thank ACESK Albania for providing data on problems in the field of cyber security [62].

Funding

This research received no external funding.

Author contributions

Fatmir Basholli: Conceptualization, Methodology, Software, Data curation, Writing-Original draft preparation. **Besjana Mema:** Validation, Software, Visualization. **Albina Basholli:** Investigation, Writing-Reviewing and Editing.

Conflicts of interest

The authors declare no conflicts of interest.

References

1. Gluschke, G., Casin, M. H., & Macori, M. (2018). Cyber security policies and critical infrastructure protection. Institute for Security and Safety Press.
2. Hyka, D., & Basholli, F. (2023). How secure is our medical data? Is Albania ready for the digitalization of the health care system?. Engineering Applications, 2(3), 235-242.
3. Breda, F., Barbosa, H., & Morais, T. (2017). Social engineering and cyber security. 11th International Conference on Technology, Education and Development,6-8. https://doi.org/10.21125/inted.2017.1008
4. Basholli, F. (2022). Cyber warfare, a new aspect of modern warfare. VI International Scientific Conference CONFSEC, 52-54.
5. Panda Security. (2018). Type of Cybercrime. https://www.pandasecurity.com/mediacenter/panda-security/types-of-cybercrime/
6. Government of the Netherlands. (2016). Forms of Cybercrime. Available at: https://www.government.nl/topics/cybercrime/forms-of-cybercrime
7. Van Hee, C., Jacobs, G., Emmery, C., Desmet, B., Lefever, E., Verhoeven, B., De Pauw, G., Daelemans, W., & Hoste, V. (2018). Automatic detection of cyberbullying in social media text. PloS One, 13(10), e0203794. https://doi.org/10.1371/journal.pone.0203794
8. Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Future internet, 11(4), 89. https://doi.org/10.3390/fi11040089
9. Rahalkar, S. (2017). Metasploit for beginners. ISBN: 978-1788295970
10. Basholli, A., Mema, B., Basholli, F., Hyka, D., & Salillari, D. (2023). The role of education in cyber hygiene. Advanced Engineering Days (AED), 7, 178-181.
11. Timalsina, U., & Gurung, K. (2015). Metasploit framework with kali linux. Technical Report.
12. Handy, N. (2018). Kali Linux & Metasploit: Getting Started with Pen Testing. https://medium.com/cyberdefenders/kali-linux-metasploit-getting-started-with-pen-testing-89d28944097b
13. Morgan, S. (2017). Cybercrime report, cybercrime damages will cost the world us $6 trillion by 2021," Cybersecurity Ventures, Herjavec Group. Online Report.
14. Anti-Phishing Working Group. (2018). Phishing Activity Trends Report, 1st Quarter 2018. Unifying the Global Response To Cybercrime. APWG.
15. Hyka, D., & Basholli, F. (2023). Health care cyber security: Albania case study. Advanced Engineering Days (AED), 6, 121-123.
16. Anti-Phishing Working Group. (2018). Phishing Activity Trends Report, 2nd Quarter 2018. Unifying the Global Response To Cybercrime. APWG.
17. Gallaher, M. P., Link, A. N., & Rowe, B. (2008). Cyber security: Economic strategies and public policy alternatives. Edward Elgar Publishing.
18. Microsoft (2022). https://www.cisa.gov › news-events
19. Daberdini, A., Basholli, F., Metaj, N., & Skenderaj, E. (2022). Cyber security in mail with Fortiweb and Fortinet for companies and institutions. Advanced Engineering Days (AED), 5, 81-83.

20. Mema, B., Basholli, F., & Hyka, D. (2023). ChatGPT in Albanian higher education: Transformation of learning and virtual interaction. Advanced Engineering Days (AED), 8, 23-27.
21. Spahiu, A., Panxhi, D., & Dhamo, D. (2022). Increasing productivity and energy efficiency in cement industry by using VSM. Advanced Engineering Days (AED), 5, 64-67.
22. Singh, J., Kaur, S., Kaur, G., & Kaur, G. (2016). A detailed survey and classification of commonly recurring cyber attacks. International Journal of Computer Applications, 141(10), 15-19.
23. Popoola, S. I., Iyekekpolo, U. B., Ojewande, S. O., Sweetwilliams, F. O., John, S. N., & Atayero, A. A. (2017, October). Ransomware: Current trend, challenges, and research directions. Proceedings of the World Congress on Engineering and Computer Science, 1, 169-174.
24. Metalla, J., Dume, G., Basholli, F., & Ndokaj, E. (2023). Modeling and simulation of robotic hand pressure sensor in Simscape. Advanced Engineering Days (AED), 7, 151-154.
25. Igbe, O., Ajayi, O., & Saadawi, T. (2017, October). Denial of service attack detection using dendritic cell algorithm. 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), 294-299. https://doi.org/10.1109/UEMCON.2017.8249054
26. Bendovschi, A. (2015). Cyber-attacks–trends, patterns and security countermeasures. Procedia Economics and Finance, 28, 24-31. https://doi.org/10.1016/S2212-5671(15)01077-1
27. Basholli, F., & Daberdini, A. (2023). Monitoring and assessment of the quality of electricity in a building. Engineering Applications, 2(1), 32-48.
28. Wu, M., Miller, R. C., & Garfinkel, S. L. (2006, April). Do security toolbars actually prevent phishing attacks?. In Proceedings of the SIGCHI conference on Human Factors in computing systems, 601-610. https://doi.org/10.1145/1124772.1124863
29. Patel, R. S. (2013). Kali Linux Social Engineering: Effectively perform efficient and organized social engineering tests and penetration testing using Kali Linux. Birmingham, VIC: Packt Publishing Ltd.
30. Mouton, F., Leenen, L., Malan, M. M., & Venter, H. S. (2014). Towards an ontological model defining the social engineering domain. In ICT and Society: 11th IFIP TC 9 International Conference on Human Choice and Computers, HCC11 2014, Turku, Finland, July 30–August 1, 2014. Proceedings 11, 266-279. https://doi.org/10.1007/978-3-662-44208-1_22
31. Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. Computers & Security, 59, 186-209. https://doi.org/10.1016/j.cose.2016.03.004
32. Basholli, F., Daberdini, A., & Basholli, A. (2023). Possibility of protection against unauthorized interference in telecommunication systems. Engineering Applications, 2(3), 265-278.
33. InsightIDR Overview, (2019). Insightidr.help.rapid7.com
34. Basholli, F. (2022). Assessment of airspace surveillance and control in Albanian territory from the current and historical prospective. Advanced Engineering Days (AED), 5, 71-73.
35. Townsend, M. (2017). What is the different between cyber-crime and cyber- attack?. https://www.quora.com/What-is-the-different-between-cyber-crime-and- cyber-attack
36. Cisco Corporation. (2023). What Is Cybersecurity?. https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html
37. Basholli, F., Minga, J., & Grepcka, A. (2023). Protection of buildings on a university campus from lightning strikes. Advanced Engineering Days (AED), 8, 35-38.
38. Hyka, D., Hyra, A., Basholli, F., Mema, B., & Basholli, A. (2023). Data security in public and private administration: Challenges, trends, and effective protection in the era of digitalization. Advanced Engineering Days (AED), 7, 125-127.
39. Dey, P. K. (2016). Prashant's algorithm for password management system. International Journal of Engineering Science, 2424.
40. Basholli, F. (2022). Electronic interference and protection from it. Advanced Engineering Days (AED), 5, 74-76.
41. Basholli, F., Mezini, R., & Basholli, A. (2023). Security in the components of information systems. Advanced Engineering Days (AED), 7, 185-187.
42. Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. CyberPsychology, Behavior, and Social Networking, 15(3), 181-183. https://doi.org/10.1089/cyber.2011.0352
43. Hopkins, M., & Dehghantanha, A. (2015, November). Exploit Kits: The production line of the Cybercrime economy?. In 2015 second international conference on Information Security and Cyber Forensics (InfoSec), 23-27. https://doi.org/10.1109/InfoSec.2015.7435501
44. Basholli, F., & Daberdini, A. (2022). Monitoring and evaluation of the quality of electricity in a building. Advanced Engineering Days (AED), 5, 77-80.
45. Sheme, E., Tafa, I., & Basholli, F. (2023). BattSim-GDC Simulator: How much battery your green datacenter needs?. Advanced Engineering Days (AED), 6, 162-164.
46. Pajaziti, A., Basholli, F., & Zhaveli, Y. (2023). Identification and classification of fruits through robotic system by using artificial intelligence. Engineering Applications, 2(2), 154-163.
47. Kurniawan, A., & Fitriansyah, A. (2018). What is Exploit Kit and How Does it Work?. International Journal of Pure and Applied Mathematics, 118(20), 509-516.

48. GREAT-Global Research and Analysis Team. (2017). Attacks with Exploits: From Everyday Threats to Targeted Campaigns. https://media.kaspersky.com/en/business-security/enterprise/KL_Report_Exploits_in_2016_final.pdf
49. Basholli, F., Daberdinİ, A., & Basholli, A. (2023). Detection and prevention of intrusions into computer systems. Advanced Engineering Days (AED), 6, 138-141.
50. Samani, R., McFarland, C. (2015). Hacking the human operating system: The role of social engineering within cybersecurity. Santa Clara, CA: McAfee.
51. Broadhurst, R., & Chantler, A. N. (2008). Social Engineering and Crime Prevention in Cyberspace
52. Frumento, E., Puricelli, R., Freschi, F., Ariu, D., Weiss, N., Dambra, C., Cotoi, I., Roccetti, P., Rodriguez, M., Adrei, L., Marinelli, G., Kandela, G., Pachego, B. (2016). The role of social engineering in evolution of attacks.
53. Mema, B., & Basholli, F. (2023). Internet of things in the development of future businesses in Albania. Advanced Engineering Science, 3, 196-205.
54. Vaisla, K. S., & Saini, R. (2014). Analyzing of zero day attack and its identification techniques. In Proceedings of First International Conference on Advances in Computing & Communication Engineering (ICACCE-2014)
55. Yeboah-Boateng, E. O., & Amanor, P. M. (2014). Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. Journal of Emerging Trends in Computing and Information Sciences, 5(4), 297-307.
56. Harizaj, M., Bisha, I., & Basholli, F. (2023). IOT integration of electric vehicle charging infrastructure. Advanced Engineering Days (AED), 6, 152-155.
57. Remorin, L., Flores, R., & Matsukawa, B. (2018). Tracking trends in business email compromise (BEC) schemes. Trend Micro, 18(1).
58. De Ryck, P., Nikiforakis, N., Desmet, L., & Joosen, W. (2013, May). Tabshots: Client-side detection of tabnabbing attacks. In Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security, 447-456. https://doi.org/10.1145/2484313.2484371
59. Koops, B. J., & Leenes, R. E. (2006). ID theft, ID fraud and/or ID-related crime-definitions matter. Datenschutz und Datensicherheit, 30(9), 553-556.
60. Cornell Law School, Legal Information Institute. (2011). U.S. Code § 1028.Fraud and related activity in connection with identification documents, authentication features, and information. https://www.law.cornell.edu/uscode/text/18/1028
61. Moore, R. (2014). Cybercrime: Investigating high-technology computer crime. Routledge.
62. Basholli, F., Hyka, D., Basholli, A., Daberdini, A., & Mema, B. (2023). Analysis of cyber-attacks through simulation. Advanced Engineering Days (AED), 7, 120-122.