Journal of Electrical Engineering and Information Technologies, Vol. **7,** No. 2, pp. 67–75 (2022)
Article 197
Received: Octomber 10, 2022
Accepted: November 11, 2022
In print: ISSN 2545–4250
On line: ISSN 2545–4269
UDC: 004.7.056:004.416'2
DOI: https://doi.org/10.51466/JEEIT2272197067g

Original scientific paper

ANALYSIS AND DESIGN OF SECURITY SOLUTIONS IN INTERNET NETWORK

Filip Gligorov, Toni Janevski

Faculty of Electrical Engineering and Information Technologies,
"Ss. Cyril and Methodius" University in Skopje,
Rugjer Bošković bb, P.O. Box 574, 1001 Skopje, Republic of North Macedonia
tonij@feit.uki.edu.mk

Abstract: The birthday of the Internet is considered January 1, 1983, by standardizing the IP and TCP. Even though its use and purpose have changed over time, one of the main challenges has been constantly present throughout the years, and that is security. Security in the Internet network includes all activities that individual users, organizations, enterprises, and institutions undertake to protect their value as well as the integrity and continuity of operations in telecommunication networks and systems. Besides the development of tools and mechanisms for enabling a safe and secure network, there is a parallel "development" of tools and mechanisms for breaking into those security systems. This paper analyzes the various scenarios and possible threats and attacks on the Internet and in general on IP-based networks and provides an overview of network security design with the implementation of system solutions.

Key words;; security analysis; security attacks; threats; vulnerabilities; intrusion

АНАЛИЗА И ДИЗАЈН НА РЕШЕНИЈА ЗА БЕЗБЕДНОСТ ВО ИНТЕРНЕТ-МРЕЖАТА

Апстракт: Појавата на Интернетот во форма која денес се користи датира од 1983 година, со стандардизацијата на IP и TCP. Иако неговата употреба и намена се имаат променето со текот на времето, сепак еден од главните предизвици низ годините е постојано присутен, а тоа е безбедноста. Безбедноста во Интернет-мрежата ги вклучува сите активности што индивидуалните корисници, организациите, претпријатијата и институциите ги преземаат за да ја заштитат својата вредност, како и интегритетот и континуитетот на операциите во телекомуникациските мрежи и системи. Всушност, со развојот на алатки и механизми за овозможување безбедна и сигурна мрежа паралелно се одвива и „развивањето" на алатки и механизми за пробивање на тие безбедносни системи. Овој труд ги анализира различните сценарија и можни закани и напади на Интернет и, генерално, на мрежте базирани на IP, и дава осврт на дизајн на безбедност за мрежата со имплементација на системски решенија.

Клучни зборови: безбедносна анализа; безбедносни напади; закани, пропусти; упад

1. INTRODUCTION

"In this age of universal electronic connectivity when the world is becoming a global village, different threats like viruses and hackers, eavesdropping and fraud, undeniably there is no time at which security does not matter.

Volatile growth in telecommunication systems and networks has increased the dependence of both organizations and individuals on the information stored and communicated using these systems. This leads to a sharp awareness of the need to protect data and resources to disclosure, to guarantee the authenticity of data and messages, and protection of systems from network-based attacks." [1]

Securing a telecommunication network is a complicated job. Different levels of security are appropriate for different organizations. Organizations and individuals can ensure better security by using a systematic approach that includes analysis, design, implementation and maintenance. The analysis phase requires that you thoroughly investigate your entire network, both software and hardware, from inside and outside. This helps to establish if there are any vulnerabilities. The analysis shows what is in place today and what you may require for tomorrow [2].

The main focus of this paper is to come up with a better understanding of network security applications and standards. To achieve these goals, the following parameters have been investigated:

- security threats and vulnerabilities,
- security attacks,
- security techniques and tools,
- security solutions.

This paper is organized based on the aforementioned arguments. The second section presents an overview of the most common weaknesses and vulnerabilities in a telecommunication network. Section 3 covers the possible attacks that can be executed on a network, and the next section, section 4, explains the techniques and tools that can prevent and secure the network from attackers. Lastly, section 5 gives the mechanisms for implementing security solutions.

2. SECURITY THREATS AND VULNERABILITIES

Network security is the protection of networks, their applications or services against unauthorized access that prevents modification, disclosure or destruction of data. It also assures that the network is performing correctly with no harmful side effects [3]. Each organization defines its security policy that describes the level of access, which is permitted or denied. So any organization must make such a security mechanism that is broad in scope and helps to deal with new types of attacks.

Vulnerabilities are defined as weaknesses in any network that can be exploited by a threat. One telecommunication network consists of different network devices, appliances, computers, as well as applications running onto the mentioned hardware. Protecting these bits and pieces of the telecommunication network is the most important task in the process of making a secured telecommunication environment. There are different hardware and software tools that can contribute to protecting the network from attacks, such as firewalls, Intrusion Detection Systems (IDS), antivirus software and vulnerability scanning software. Following are some of the common threats to the network.

One of the main advantages of any network is the ability to share resources. As a part of a network, different types of services can be shared, like file and printer sharing. Gaining illegal access to these resources causes unauthorized access in the network. Password sharing, guessing and capturing are the most common methods to gain illegal access. Password sharing and guessing can be achieved using different techniques like:

- Try default passwords.
- Try dictionary words.
- Try short words (1–3 characters long).
- Try the user's personal number, home address, and personal information like birth date, family name, etc.

Password capturing is a technique in which a hacker unknowingly steals a user's ID and password. The Trojan horse program is specifically designed for this purpose. Below is some recommended information that can prevent unauthorized access:

- Use strong passwords, at least 10 characters long, containing letters, numbers and special characters and avoid using dictionary words.
- Use hardware and software firewalls.
- Use protection software.

Companies have different departments and users, some users may have inappropriate access to network resources, mostly because the users are not from the same department or may be such users who are from outside the company. Moreover, information stored in the network may require a level of confidentiality. Illegal access occurs when someone who is not authorized tries to read that data.

So far mentioned threats can be classified as compromising data that reside in a system or computer. The second type of data breach is while transferring from machine to machine or while sharing among the network users. These two types of data fall under two types of security, computer and network security. The tools that are designed to protect the first type of data fall under computer security while the protection of data during transmission is called network security. During the transmission of data two things are important that assure the integrity of data, one is that data is coming from a trusted host and the second is that data contents are not altered or changed. Spoofing occurs when someone pretends to be a trusted host. IP spoofing, Email spoofing, Web spoofing, etc, are some types of spoofing. Messages transmitted over any network consist of some address information, sender address and receiver address. An intruder or hacker who initially finds the IP address of a trusted host after compromising the host can modify the message (packet header) so that it appears that the message is coming from that trusted host [3], as shown in Figure 1.

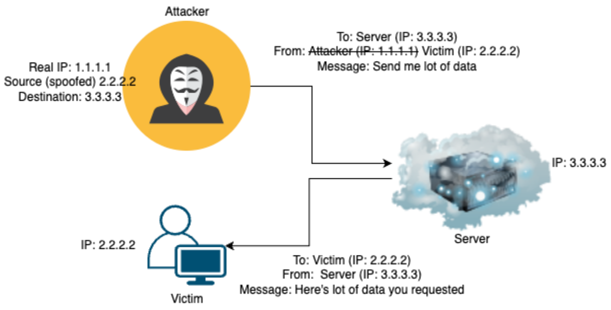

Fig. 1. IP spoofing

When a network does not provide the needed functionality on time means that a disruption has occurred. Several reasons may lay behind that: the network cannot detect the traffic, it has a single point of failure, it has a hardware failure, improper maintenance of network equipment, etc. Knowing all these threats and vulnerabilities in a telecommunication network, the implementation of a security mechanism sometimes cost too much, therefore some administrators simply tolerate the expected losses and find the most cost-effective solution.

3. NETWORK SECURITY ATTACKS

The way of locking down an "open" system to avoid its usage by anyone represents the security of that system. Any action that compromises security is called a security attack. A system which is providing the services required by the user accurately and preventing the illegal use of system resources is called a secure system. Attacks can be categorized into following basic categories [4]:

- Interruption: For using the data or resources they must be available 24/7 for the authorized parties, when and where they need it. An attack on the availability of data is called interruption. Availability can be affected by intentional or unintentional acts. Unintentional acts are, accidental system crashes, deletion and overwriting of data and sometimes due to non-human factors like floods, fires and earthquakes. Examples of intentional acts are attacks by hackers that crash the system, such as denial of service (DOS) and distributed denial of service (DDOS) attacks.
- Interception: The core concept is that the data should be hidden from unauthorized users. If someone who is unauthorized sees or copies the data then that data can be used in an intensive active attack. Such an attack is known as an attack on confidentiality.
- Modification: The integrity of data deals with the prevention of intentional or unintentional modification of data. An attack on the integrity of data is called a modification. Protection of data from modification is a foremost concern than detection.
- Fabrication: An attack on authenticity is called fabrication. Authenticity means that message is coming from the apparent source.

Above mentioned attacks are shown in Figure 2. Based on these four attacks, we can further classify security attacks as passive and active attacks. Passive attacks are only involved in the monitoring of the information (interception). The goal of this attack is to obtain transmitted information. Passive attacks are hard to detect because they do not involve in alteration. Active attacks are involved in the modification of data (interception, modification, fabrication) or the creation of false data. The information which hackers obtained from a passive attack is used in a more aggressive active attack [5–7].

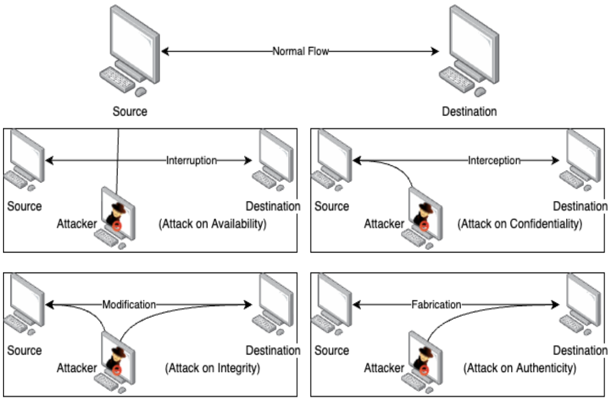

Fig. 2. Types of security attacks

Gathering information against a targeted host or network is called a reconnaissance attack. Attacker analyzes the target host and tries to discover details like live IP addresses, open ports of the network, failure of an operating system, and types of services and protocols running on the network. Reconnaissance attacks are common, they are not so dangerous because they are not involved in any kind of alteration or destruction of data but, on the other hand, they show the vulnerabilities in the network. Following is presented some of the reconnaissance attacks (packet sniffing, port scan/ping sweep and Internet information queries).

A packet sniffer is a tool or device that can be used for capturing the packet at the data link layer. A packet sniffer is not only a hacker's tool but it can be used both by the hacker for eavesdropping and by the administrators for network monitoring and troubleshooting. Tcpdump, Windump, Wireshark (ethereal) and Dsiniff are examples of different sniffing tools. Sniffing can be passive or active.

When using hubs in the network, each machine in that network decides whether to accept or discard the broadcasted packet. In passive sniffing, this filter in the machine is disabled, thus the machine can capture the traffic and then analyze the content of the packages [8, 10]. Figure 3 shows the passive sniffing.

In a network where switches are used, the packages are directed from the source to the destination machine. In such a case, an active sniffing mechanism takes over, like MAC Flooding and Spoofed ARP Messages. Switches worked based on MAC addresses. They maintain an ARP table in a special type of memory called Content Addressable Memory (CAM). ARP table has all the information of which IP address is mapped on which MAC address. The act of overloading the CAM is known as MAC flooding. At this stage, the switch goes to a fail-open mode [9, 10] and cannot perform IP to MAC mappings, starts behaving like a hub, and starts transmitting the data to all machines.

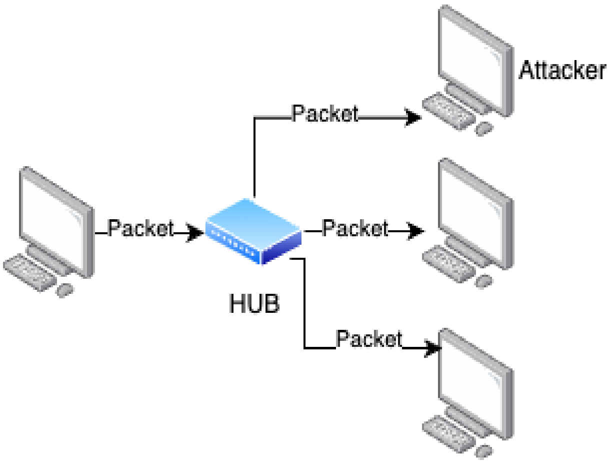

Fig. 3. Passive sniffing

In the active sniffing technique, spoofed ARM messages, the attacker tries to be the destination machine. Poisoning the ARP cache of a central entity of the network, the attacker maps his MAC address to the IP address of the switch (or router). In this way, all the traffic first goes towards the attacker and then the router [11]. Active sniffing is shown in Figure 4.

Port scan and ping sweep are two common network probes typically used to run various tests against a host or device to find vulnerable services. They are helpful to examine the IP address and the services which are running on a device or host. In port scanning, a packet is sent to each target port and the reply message indicates that either the port is open or closed which is further helpful to launch an attack against a specific service [12].

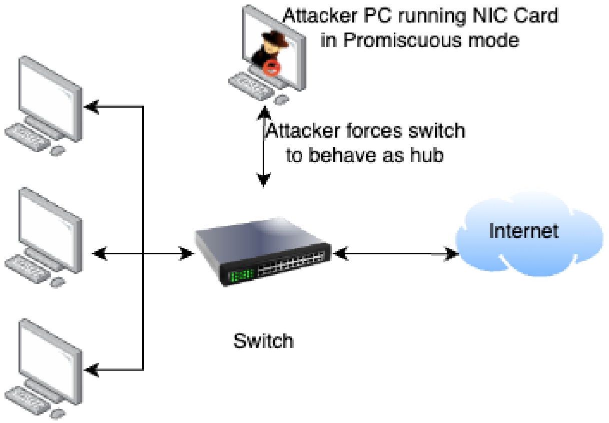
Attacker PC running NIC Card in Promiscuous mode
Attacker forces switch to behave as hub
Internet
Switch

Fig. 4. Active sniffing

The most popular probing tool is Nmap. The method of finding which IP addresses are live is called ping sweep. The aim is to find out machines which are alive and which are not alive. These ICMP replies from different machines are logged into a file for future reference. Fping is a tool used for performing ping sweep. Working on the round robin function, it takes a list of IP addresses, sends a ping packet to an IP address, and immediately proceeds toward the next IP address.

The reconnaissance attacks are completed with internet information queries. DNS queries provide the particular information of the domain and the addresses associated with that particular domain. IP queries display the range of IP addresses and for which domain those addresses are associated. Ping sweep presents a clear picture of a particular environment. After these queries port scan starts by the hacker which leads him to find out which ports are open and which services are running on these ports. Finally, the whole information can be helpful when a hacker tries to compromise any system through these services.

Other than the reconnaissance attacks, there are also access attacks. Access attacks occur when a hacker exploits the vulnerabilities of the services running on a system and succeeds to access confidential information. Different types of network attacks are password attacks, trust exploitation, port redirection, and man-in-the-middle attack.

Several methods can be used for password attacks. Trojan horse, IP spoofing and packet sniffers can show the detail of the user like user name and password. The password attack can be referred to as repeated attempts to find the user information (user name or password). Once an intruder succeeds then he/she has the same access right that the compromised account has. In Table 1, the different type of password cracking attacks are presented.

Table 1

Type of password attacks

	Dictionary attack	Brute force attack	Hybrid attack
Speed of the attack	Fast	Slow	Medium
Passwords cracked	Finds only words	Finds every password (A–Z, 0–9, special characters)	Finds only the passwords that have dictionary word as the base

When a hacker attacks – a computer that is outside a firewall and that computer has a trust relationship with another computer that is inside the firewall, the hacker can exploit this trust relationship. Figure 5 explains trust exploitation.

The port redirection is another type of trust exploitation attack in which a hacker bypasses the security mechanism. Figure 6 shows the port redirection attack.

When hackers succeed to intrude between two communication parties this type of attack is called a MITM (Man-in-the-Middle) attack. In this way hackers can intercept data between source and destination host, can modify data and retransmit it to the destination host, and can also inject any type of false data. MITM attacks can affect on availability, confidentiality, integrity, and authenticity of data.

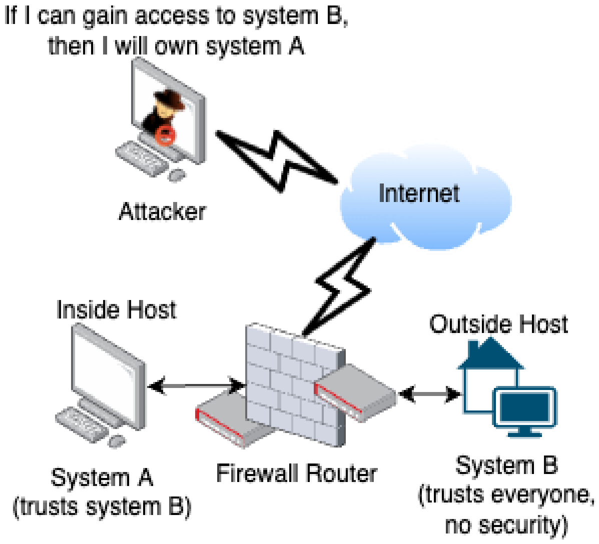
If I can gain access to system B, then I will own system A
Attacker
Internet
Inside Host
Outside Host
System A (trusts system B)
Firewall Router
System B (trusts everyone, no security)

Fig. 5. Trust exploitation attack

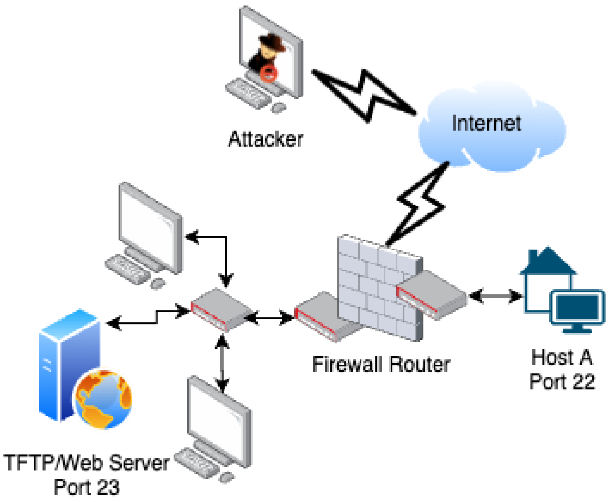

Fig. 6. Port redirection attack

Types of attacks that bring the network down in such a way that resources are not available even for authenticated users are known as DOS attacks. Attackers may target a single machine to make it impossible for outgoing connections on the network or may attack the whole network to make it impossible for incoming and outgoing traffic. Ping of death, SSPing, Land, Win Nuke, and SYN flood are some examples of DOS attacks. In an SYN flood attack, a hacker sends an SYN packet to a target host which then responds with SYN acknowledgment, at the end attacker does not send any ACK packet to the target host which causes the connection to remain in a half-open state. TCP connection does not remove this connection from its table and wait to expire this session, the attacker takes the advantage of this and continues sending new SYN packets until the TCP SYN queue is filled and cannot accept new connections [13].

4. SECURITY COUNTERMEASURE TECHNIQUES AND TOOLS

The security countermeasure techniques are directly related to such parameters that survive in the form of network bugs or vulnerabilities and their effects on a communication network. After analyzing the effect of these parameters, appropriate security countermeasure techniques for the network can be selected.

The selection and implementation of these countermeasure techniques in a network environment depend on the network administration team. It depends upon their updated knowledge and awareness about the network, standard network architecture, traffic parameters in the form of application behavior (OSI and TCP/IP layer network protocols knowledge and working role), network hardware performance, security threats, and existing weak points in the network. A rough or out-of-date knowledge can become a cause of network bugs and vulnerabilities.

By considering the above measurements many research organizations have assigned some most essential key security countermeasure techniques for a standard-level network infrastructure [14].

A strong security policy performs an efficient role in a network. If policy develops after analyzing the network and behavior of its components then it results in a much more secure and smooth network.

The authorization of systems or network resources has an important role in security countermeasures. After a fair survey of the network, a proper level of authority for accessing the system resources can be assigned. The policies of antivirus or the access control list of routers or firewalls can define the authority for properly accessing network resources.

The presence of an intrusion detection system has an important role in security countermeasures. The study and analyzing the log files against malicious activities in the network can save a system. It provides a futuristic safety approach against many other malicious aims.

The symptoms of a malicious attack give us an idea about which type of protection is required for a system against that attack. We can re-adjust or reconfigure our security system parameters by generating a strong resistive block against the attack.

By fixing basic problems in a system or network we can save the system or network. These basic but core problems are hidden spot that exists in any common network or system, like improper updating of system applications, out-of-date applications, and updated virus patches (not on proper time) these all can create a security flaw in any network [15].

As a complement to countermeasure techniques are the countermeasure tools, such as cryptography, conventional or symmetric encryption, and public key or asymmetric encryption.

Cryptography is used to protect data from interception. It is the study of methods to send data in unrecognizable form so that only the intended user can recognize and read the message. Cryptography concerns with two things, data is coming from an apparent or trusted source and the contents of data are not altered. Goals that can be achieved from cryptography are confidentiality, data integrity, authentication, and non-repudiation.

Conventional or symmetric encryption has been the only encryption scheme available before public-key encryption. One secret key is shared among the sender and the receiver. The whole procedure of conventional encryption consists of five stages:

1. Plain text: The original message or data that needs to be encrypted.
2. Encryption algorithm: The encryption algorithm performs different transformations on the data.
3. Secret key: Secret key is the input to the encryption algorithm. Different transformations performed by the encryption algorithms depend on the secret key.
4. Cipher text: This is the output of a scrambled message.
5. Decryption algorithm: Reverse the encryption algorithm, and produces the plain text with the help of the same secret key and the cipher text.

One important thing is that the security of conventional encryption depends on the secret key, not on the algorithms. Even if the cipher text and algorithms are known, it is practically impossible that a message can be decrypted with the help of cipher text and encryption/decryption algorithm. In most symmetric algorithms two communication parties use the same key for encryption and decryption which is why it is also called a secret-key, single-key, or one-key algorithm. For safe communication, the key must remain secret. It is also necessary to change the key frequently so that attacker could not compromise the key. The strength of any cryptographic system depends on the key distribution process. There are several ways to distribute the keys between two parties A and B [16].

- Key could be selected by party A and physically delivered to party B.
- Any third party could select a key and physically deliver it to A and B.
- If A & B have previously used a recent key, one party could transmit the new key to the other, which is encrypted by the old key.
- In case of encrypted connection of A & B to a third party C, the third party C could deliver the key to A & B on encrypted links.

Instead of using one key which is used in conventional encryption, asymmetric uses two separate keys. The use of two keys makes communication more secure and authenticated. The asymmetric scheme has six ingredients:

1. Plain text: The original message or data.
2. Encryption algorithms: The encryption algorithm performs different transformations on the data.
3. Public and private key. The transformation by the encryption algorithm totally depends on these keys. These keys are selected in such a way that if one is used for encryption, the other is used for decryption.
4. Cipher text: This is the output scrambled message.
5. Decryption algorithm: Reverse the encryption algorithm.

Public and private keys are used in public-key encryption, as name suggests that public key is used publicly while private key is only used by its owner. The following steps are followed in public-key encryption:

1. Each and every user in a network generate a pair of keys, one is used for encrypting the message while other is for decrypting the message.
2. From those two keys each user places one key in a public register, so that every other user can access that key. In this way each user has a collection of public keys of all the users in network.
3. If user A wants to send a message to user B, A encrypts a message with B’s public key.
4. When user B receives the message, he/she decrypts it by using his/her private key. No one else can decrypt this message.

The major weakness in public-key encryption is that public key is public. Thus, anyone can forge such type of public announcement. An intruder could pretend to be user A and can send its public key to any other participant or even can broadcast his public key. The solution is to use public-key certificate issued by a third party which is called Certificate Authority (CA). This authority is trusted by the user community it can be any governmental organization that issues a certificate which consists of public key, user ID of the key owner and at the end whole block is signed by the CA. X.509 is a standard scheme used in most network security applications for certification [17].

5. SECURITY SOLUTIONS

Once the network threats and vulnerabilities are known as well as the techniques for establishing the secure network, the next step is implementing solutions that make the telecommunication network reliable and protected. Depending on their implementation, security solutions mainly can be categorized as application-level solutions and system-level solutions.

Application security solutions start with the authentication. The verification of any identity is called authentication which also verifies the integrity of the data. For the telecommunication networks, Kerberos and X.509 are used to keep the data integrity.

In traditional networks, a user types a password to verify his identity, this is called authentication. Password-based authentication is not a good solution because passwords are sent across the network and any intruder can intercept these passwords. Strong authentication-based cryptography is required so that intruders could not gain information that will help to impersonate him. The most common example of this type of authentication is Kerberos, which is based on conventional encryption. It is a distributed authentication service in which the server verifies a user without sending information on the network [18].

X.509 is another authentication protocol based on a public-key certificate. The authentication protocols defined in X.509 are widely used, for example in S/MIME, IP Security, and in SET. The Certificate consists of a public key of the user, signed by the private key of that trusted party and that party is called Certificate Authority (CA).

The most widely used and growing network application across all platforms is electronic mail. To keep the confidentiality of e-mail two schemes are used, PGP and S/MIME.

Pretty Good Privacy (PGP) combines the features of the two cryptographic schemes. First, it compresses the message and then creates a one-time secret key for data encryption, this key is called a session key. The data is encrypted with this one-time session key and the session key is also encrypted by the recipient's public key. This encrypted session key and cipher text then are transmitted to the recipient. On the recipient's side, PGP recovers that session key with the help of a private key and this recovered session key then is used to decrypt the cipher text.

Secure/Multipurpose Internet Mail Extension (S/MIME) provides security for MIME data by signing the data and by use of public-key encryption. It provides authentication of data by using a digital signature and integrity of data by encryption.

Applying security on the IP level ensures secure communication for the applications that have security mechanisms as well as for the security ignorant applications. Internet Protocol Security (IPSec) provides encryption and authentication to all traffic at the IP level with the help of strong cryptography. Authentication and encapsulation are two basics of IPSec. Two protocols that provide authentication and encapsulation are Authentication Header (AH) and Encapsulation Security Payload (ESP). These two protocols are used in combination or alone to provide the desired set of security services for the IP layer.

The web is visible to everyone. Browser side risks and wrong configuration in web servers are some types of risks that help intruders to unauthorized remote access and interception of data. SSL is one of the most commonly used security mechanisms available on the Internet. Like other security protocols SSL is also based on cryptography. After SSLv3, Internet Engineering Task Force (IETF) renamed it TLS. SSL/TLS encrypts the data at the transport layer. Instead of HTTP port 80, SSL comes up with a special URL identity "HTTPS" which uses port 443 to establish a secure SSL session. SSL-supported browsers are used mostly for sensitive data like credit card information. TLS provides end-to-end authentication and then secure communication using cryptography.

Secure Electronic Transaction (SET) is a security protocol designed for protecting credit card transactions over the Internet. For confidentiality of information and integrity of data DES and RSA are used with SHA-1 hash codes. X.509v3 certificate is used for authentication of cardholder account and merchant account. Privacy is achieved through dual signatures.

System-level security solutions are divided into IDS, IPS, antivirus applications, firewalls, and honeypots.

The Intrusion Detection System (IDS) detects any unauthorized access or intrusion in a system or network. It is a security solution that has a passive position in a system or a network against intrusions. In a network deployment, the function of the IDS is to monitor the traffic or the network activity without impacting the traffic [19]. It means that an IDS in a network only detects or identifies any changes in the network but does not perform a resistive action against such changes.

The Intrusion Prevention System (IPS) performs the role of protection against intrusions that occur in a network or local system. It works based on the output of IDS system log files. Due to this reason, the IPS system is an extension of the IDS system. Unlikely IDS, IPS works in an active mode. IPS acts when it founds any packet dropping or unauthorized connection [20, 21].

A firewall is a barrier that performs isolation between two different networks or systems. It decides which kind of traffic can pass through a network and in which direction. Firewalls provide an additional level of defense providing the capabilities to add much tighter and more complex rules of communication between different network segments or zones [14]. Firewalls can be divided into four categories: packet filter, application gateway, circuit-level gateway, and stateful filer firewall [1, 22, 23].

A honeypot is a network-attached system set up as a decoy to lure cyber attackers and detect, deflect and study hacking attempts to gain unauthorized access to information systems. The function of a honeypot is to represent itself on the internet as a potential target for attackers, usually a server or other high-value asset, and to gather information and notify defenders of any attempts to access the honeypot by unauthorized users.

6. CONCLUSION

Security is not about a specific firewall, product, brand, and operating system. Properly configured firewalls, strong passwords that are changed on regular basis, antivirus updates regularly, etc., all these elements are used collectively for good security practices. Each organization, depending on its business needs, budget constraints, and organizational requirements, needs to draw up a security policy and that policy will determine the mix of components that need to be installed, to meet security goals. Deficiencies in bad products can be defeated with good practice, whereas bad processes can dilute otherwise excellent products. It is better to have no security devices instead of incorrectly configured security devices. Sometimes deployment of security can affect the QoS of the network. The bottom line is that a network cannot be 100% secure. However, by analyzing the network the security level can be increased. This analysis will help to find out the vulnerabilities in the network.

“The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.” – Sun Tzu.

REFERENCES

[1] Stallings, W. (2017): *Network Security Essentials Applications and Standards,* , 6th Edition, Pearson Education, Inc.

[2] Yang, X., Euchner, M., Sebek, G., Bertine, H., Kremer, A., Youl Youm, H., Hee Oh, K., Harrop, M. (2020): *Security in Telecommunications and Information Technology*, International Telecommunication Union, 7.

[3] Osanaiye, O. A. (2015): IP spoofing detection for preventing DDoS attack in Cloud Computing, *18th International Conference on Intelligence in Next Generation Networks*, pp. 139–141. DOI: 10.1109/ICIN.2015.7073820

[4] Vacca, J. R. (2017): *Computer and Information Security Handbook,* Morgan Kaufmann.

[5] Brenner, W. Susan (2020): *Cybercrime and evolving threats from cyberspace*, 2nd Edition, Praeger.

[6] Jha, M., Anand C. S., Mahawar, Y., Kalyan, U., Verma, V. (2021): Cyber Security: Terms, Laws, Threats and Protection, *International Conference on Computing Sciences (ICCS)*, pp. 148–151.

[7] Melnik Sergey, Smirnov Nikolay, Erokhin Sergey (2017): Cyber security concept for Internet of Everything (IoE), *Systems of Signal Synchronization, Generating and Processing in Telecommunications (SINKHROINFO)*, pp. 1–4, DOI: 10.1109/SINKHROINFO.2017.7997540

[8] Bailey, Matthew (2015): *Complete Guide to Internet Privacy, Anonymity and Security*, 2nd Edition, Nerel Online,.

[9] Piper, Ben (2017): *Cisco Network Administrator*, Manning.

[10] Watts. Neal A., (2012): *Packet Analysis of Unmodified Bluetooth Communication Devices,* BiblioScholar.

[11] Harwood, Mike (2015): *Internet Security: How to Defend Against Attackers on the Web,* 2nd Edition, Jones & Bartlett Learning.

[12] Singh Chauhan Ajay (2018): *Practical Network Scanning: Capture network vulnerabilities using standard tools such as Nmap and Nessus,* Packt Publishing.

[13] Gbouri El, Sam (2018): *The 2016 Dyn DDOS Cyber Attack Analysis: The Cyber Attack that Broke the Internet for a Day*, CreateSpace Publishing Platform.

[14] Du, David (2020): *Preventing DDoS Attacks Using I Ptables* Linux server.

[15] Rahalkar, Sagar (2018): *Network Vulnerability Assessment: Identify security loopholes in your network's infrastructure,* Packt Publishing.

[16] Duraiswamy, K., Rani R., Uma (2017): *Security through Obscurity*.

[17] Gilchrist, Alasdair (2017): *A Concise Guide to SSL/TLS for DevOps*, 2nd Edition.

[18] Spivey, B., Echeverria, J. (2015); *Hadoop Security: Protecting Your Big Data Platform*, O'Reilly Media.

[19] Kim, K., Aminanto, M. E., Tanuwidjaja, H. C. (2018): *Network Intrusion Detection using Deep Learning*: *A Featurwe Learning Approach*, Springer, Singapore.

[20] Oke, J. T., Agajo, J., Nuhu, B. K., Kolo, J. G., Ajao, L. (2018): Two Layers Trust-Based Intrusion Prevention System for Wireless Sensor Networks, *Advances in Electrical and Telecommunication Engineering*, 1, pp. 23–29.

[21] Brotherston L., Berlin A. (2017):: *Defensive Security Handbook*, O'Reilly Media.

[22] Stewart, M. J. (2020): *Network Security, Firewalls, and VPNs*, 3rd Edition, Jones & Bartlett Learning.

[23] Jithin, A. (2018): *Being a Firewall Engineer: An Operational Approach: A Comprehensive guide on firewall management operations and best practices*.