Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, January 2023

Network Security Essentials: Understanding Its Key Attacks and Potential Security Mechanism

Shruti Sharma
Assistant Professor
Electronics & Communication Engineering
Arya Institute of Engineering and Technology, Jaipur, Rajasthan

Rajkumar Saini
Assistant Professor
Computer Science Engineering
Arya Institute of Engineering and Technology, Jaipur, Rajasthan

Sumit Saini
Research Scholar
Computer Science Department
Arya Institute of Engineering and Technology, Jaipur, Rajasthan

Tushar Sharma
Research Scholar
Computer Science Department
Arya Institute of Engineering and Technology, Jaipur, Rajasthan

ABSTRACT

Security is an essential component in the field of computing and networking technology. The prioritisation of a robust security policy should be the primary and fundamental concern for the design, planning, construction, and operation of any network. The prioritisation of network security has become increasingly important for individuals utilising personal computers, corporations, and military organisations. The issue of security has become a significant worry since the emergence of the internet. The inherent nature of the internet has facilitated the emergence of a multitude of security concerns. The growing significance of network security stems from the accessibility of intellectual property through online platforms. A wide range of

http://doi.org/10.36893/IEJ.2023.V52.174-184

attack types can be propagated over a network. Understanding various attack techniques is crucial for the effective implementation of appropriate security measures. To safeguard their operations from potential online threats, numerous enterprises employ various measures. There exist various types of network attacks that can be launched. Understanding different attack types enables the development of suitable security measures. Numerous enterprises employ firewalls and encryption technologies as protective measures against potential cyber threats. Networking infrastructures globally include a substantial volume of personal, economic, military, and government information, necessitating diverse security procedures for each category. This paper aims to examine a wide range of attacks and explore several security mechanisms that can be implemented based on the specific requirements and structure of the network.

KEYWORDS
Network Security, attacks, hackers, Cloud-environment security, zero-trust model, Trend Micro internet security.

INTRODUCTION

The administration of network security varies across different contexts and is necessary due to the increasing prevalence of internet usage. In contrast to large enterprises, which necessitate sophisticated software and hardware solutions to mitigate the risks of hacking and spamming, households and small offices typically require more rudimentary security measures. According to the source provided, [1]. The emergence of novel threats necessitates the development of innovative strategies, given that the network serves as the gateway to an organisation for both authorised users and potential assailants. Over an extended period, information technology professionals have constructed protective measures aimed at thwarting any unauthorised access that may pose a threat to the integrity of an organization's network. Network security is of utmost importance in the process of designing, planning, developing, and running networks, since it encompasses the implementation of robust security policies. Network security is a dynamic field that undergoes continuous evolution as a result of factors such as the expansion of network traffic, shifts in usage patterns, and the ever-evolving landscape of potential threats.

The whole subject of network security is examined through the exploration of the historical aspects pertaining to security in networks.

This paper examines the architecture of the Internet and explores its security vulnerabilities.

http://doi.org/10.36893/IEJ.2023.V52.174-184

This paper aims to discuss the various types of internet attacks and the corresponding security solutions employed to mitigate these threats.

• Network Security in the Context of Internet Connectivity.

The present advancements in hardware and software for network security.

When contemplating network security, it is imperative to underscore the paramount importance of ensuring the overall security of the entire network. The scope of network security extends beyond the protection of individual computers located at the endpoints of a communication chain. In the context of data transmission, it is imperative to ensure that the communication channel is resistant to potential attacks, particularly those that possess a higher likelihood of successfully compromising the integrity and security of the transmitted data.

When considering the potential targeting of communication by a hacker, it is important to address the development of a secure network.

The concept of accessibility refers to the provision of communication capabilities for authorised users to transmit and receive data within a certain network.

2. Confidentiality is a crucial aspect of network security, ensuring that information remains private and preventing unauthorised disclosure.

Authentication is a crucial process that verifies the identity of network users, ensuring that individuals are indeed who they claim to be.

Integrity is a crucial aspect to consider in ensuring the preservation of message authenticity during transmission. It is imperative that the content remains unaltered and consistent with its original form upon receipt.

http://doi.org/10.36893/IEJ.2023.V52.174-184


Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, January 2023
Non-repudiation refers to the assurance that the user cannot deny their utilisation of the network.

TYPES OF ATTACKS

Networks are susceptible to security breaches initiated by malevolent entities. The prevalence of internet connectivity has led to a significant rise in the occurrence of cyber attacks. The primary classifications of attacks can be divided into two categories: "Passive" attacks, where a network intruder intercepts data being transmitted via the network, and "Active" attacks, where an intruder executes commands to disrupt the normal operation of the network [6]. In order to effectively mitigate the impact of attacks, it is imperative for a system to possess the capability to restrict damage and swiftly restore its functionality. In addition, it is necessary to consider several additional sorts of attacks.

Passive attacks involve the monitoring of unencrypted network traffic with the intention of identifying clear-text passwords and other sensitive information that can subsequently be exploited in various sorts of attacks. Passive attacks refer to the unauthorised monitoring and interception of communication channels by malicious actors. The activities encompassed within this scope involve the analysis of traffic patterns, the monitoring of communications lacking adequate protection, the decryption of traffic that is inadequately encrypted, and the acquisition of authentication data, such as passwords. The act of passively intercepting network processes offers enemies the ability to observe forthcoming actions. Passive attacks entail the unauthorised revelation of information or data files to an assailant, occurring without the user's awareness or agreement.

2. In the context of cybersecurity, an active attack refers to the deliberate actions taken by an unauthorised individual or entity to circumvent or breach the security measures implemented inside a communication system. This can be achieved by covert methods such as stealth, computer viruses, worms, or Trojan horses. Active assaults encompass many strategies aimed at bypassing or compromising protective mechanisms, introducing malevolent code, and illicitly acquiring or altering sensitive data. Active attacks refer to the actions undertaken by an unauthorised attacker who engages in monitoring, listening to, and modifying the data stream within a communication channel.

http://doi.org/10.36893/IEJ.2023.V52.174-184

A distributed attack entails the adversary's insertion of malicious code, such as a Trojan horse or back-door programme, into a trusted component or software. This compromised component or software is subsequently disseminated to several other firms and users. Distribution assaults mostly centre on the malevolent alteration of hardware or software either at the manufacturing stage or during the distribution process. These assaults involve the insertion of malicious code, such as a backdoor, into a product, with the intention of obtaining unauthorised access to information or system functions at a future time.

According to a survey conducted by Cyber Security Watch, it was determined that insiders were responsible for 21 percent of security breaches, while an additional 21 percent of breaches were potentially attributable to the acts of insiders. A majority of participants in a recent poll expressed the view that the task of identifying and thwarting insider assaults has become more challenging in the present era compared to 2011. Furthermore, 53 percent of the respondents indicated their intention to allocate additional financial resources towards enhancing security measures in order to address the issue of insider threats. A considerable proportion of security breaches can be attributed to either malicious or dissatisfied personnel, including those who have left the organisation. However, it is important to acknowledge that a substantial percentage of breaches are also instigated by well-intentioned employees who are merely attempting to fulfil their job responsibilities. The implementation of Bring Your Own Device (BYOD) programmes and the utilisation of file sharing and collaboration services like as Dropbox have presented challenges in maintaining strict control over business data due to the actions of well-intentioned yet irresponsible employees.

5. Close-in Attack- A close-in attack refers to the deliberate proximity of an individual to network components, data, and systems with the intention of gaining unauthorised access and acquiring further knowledge about the network. Close-in attacks involve individuals who intentionally approach networks, systems, or facilities in close physical proximity with the objective of altering, acquiring, or obstructing access to information. Social engineering

http://doi.org/10.36893/IEJ.2023.V52.174-184

is a widely recognised method of executing close-in attacks. In the context of cybersecurity, a social engineering attack refers to the act of an assailant infiltrating a network or system by leveraging interpersonal communication with an individual, typically through means such as email or telephone correspondence. There are several techniques that individuals can employ to ascertain the level of security within an organisation. The data disclosed by the victim to the hacker is likely to be utilised in a subsequent offensive manoeuvre aimed at illicitly infiltrating a system or network.

The spyware assault is a significant computer security concern, since it refers to the presence of any software that watches an individual's online activities or installs programmes without their explicit authorization, with the intention of generating profit or obtaining personal information. The captured information is subsequently exploited for illegitimate purposes by unauthorised individuals who assume the identity of the legitimate user for that specific type of job.

In a hijack attack, an unauthorised individual assumes control of a communication session between two parties and intentionally disrupts the connection with the other party. The user expresses concern on the potential for mistakenly sharing private information with a hacker, while maintaining the belief that they are communicating with the intended recipient.

In the context of cybersecurity, a spoof attack involves the deliberate alteration of the source address of sent packets by a malicious actor, resulting in the falsification of their origin to appear as if they are originating from a different entity. This might perhaps be an endeavour to circumvent the established firewall regulations.

A password attack refers to the deliberate attempt made by an unauthorised individual to decipher the passwords that are contained within a network account database or a file that is protected by a password. The three primary categories of password attacks encompass a dictionary attack, a brute-force attack, and a hybrid attack. A dictionary attack is a method that involves utilising a word list file, which consists of a compilation of probable passwords [9]. A brute-force attack refers to the method employed by an attacker wherein they systematically attempt every conceivable combination of characters in order to gain

http://doi.org/10.36893/IEJ.2023.V52.174-184

unauthorised access or compromise a system.

A buffer overflow refers to a type of attack wherein an adversary intentionally transmits a greater amount of data to an application than what is anticipated. Typically, a buffer overflow attack leads to the unauthorised acquisition of administrator privileges within the system, granting the attacker command prompt or shell access.

The exploit attack refers to a malicious act where the perpetrator possesses knowledge of a security flaw present in an operating system or programme. This knowledge is then utilised to take advantage of the vulnerability and carry out the assault.

TECHNOLOGIES FOR PROVIDING SECURITY TO THE NETWORK

The persistence of internet risks remains a significant concern within the global context, owing to the ongoing accessibility and transmission of information via the internet. Various defence and detection systems have been developed in response to the aforementioned threats. This section addresses several mechanisms and advanced concepts.

Cryptographic systems are regarded as a valuable and extensively employed tool in contemporary security engineering. The process entailed the utilisation of codes and cyphers to convert information into incomprehensible data.

The firewall serves as a conventional means of border control or perimeter defence. The primary objective of a firewall is to restrict incoming traffic from external sources; however, it can also be employed to impede outgoing traffic from internal sources. A firewall serves as the primary defensive mechanism against unauthorised individuals attempting to get access to a computer system. The system in question has been specifically engineered to mitigate the risk of unauthorised ingress or egress to a private network. Firewalls have the capability to be deployed using either hardware or software, or a combination of both [9]. The firewall is the prevailing approach for addressing the challenges associated with Internet security, as it has widespread adoption and sales. The aforementioned device functions as an intermediary

http://doi.org/10.36893/IEJ.2023.V52.174-184

between a localised network and the global Internet, effectively discerning and eliminating potentially detrimental network traffic. The concept of a solution packaged within a container holds significant allure for numerous entities, and has attained such widespread acceptance that it is now seen as an indispensable component of corporate scrutiny. Firewalls are available in three primary variations, which are distinguished by their filtering capabilities at different levels of network communication. These levels include IP packet filtering, TCP session filtering, and application-level filtering.

In order to enhance efficiency and bolster security measures, Intel endeavours to integrate various security technologies into different components of its platforms, such as the processor, chipset, and network interface controllers (NICs). This approach aims to drive security measures down to the hardware level and optimise overall performance. These technologies offer foundational components that can support the establishment of a secure and efficient network architecture. The aforementioned technologies encompass Virtualization Technology, Trusted Execution Technology, and Quick Assist Technology.

Intrusion Detection Systems (IDS) are security mechanisms designed to detect and respond to unauthorised access attempts or malicious activities within a computer network. Another defence mechanism that assists in the prevention of computer breaches is an intrusion detection system (IDS). Intrusion Detection Systems (IDS) encompass both hardware and software components, serving as effective instruments for the identification and detection of potential attacks. Intrusion Detection Systems (IDS) tools are employed to monitor network connections and detect instances of active attacks. Some individuals make efforts to prevent the assault, but certain Intrusion Detection Systems (IDS) just observe and notify on the occurrence of an attack. An illustration of an intrusion detection system can be observed in the conventional antivirus software package. Intrusion detection systems encompass a broad range of technologies utilised for preemptively identifying and detecting malicious activities. The observation that numerous systems exhibit inadequate utilisation of log and audit data has stimulated a swift expansion within the realm of intrusion detection in corporate and governmental networks.

http://doi.org/10.36893/IEJ.2023.V52.174-184

Anti-malware software and scanners are tools designed to detect and remove malicious software, commonly known as malware, from computer systems. Viruses, worms, and Trojan horses are all instances of malevolent software, commonly referred to as Malware. Special software tools, sometimes referred to as anti-malware tools, are employed for the purpose of identifying and remedying infections within a computer system. The Secure Socket Layer (SSL) is a cryptographic protocol that ensures secure communication across a network. The Secure Sockets Layer (SSL) protocol is specifically engineered to provide a highly secure communication channel, commonly referred to as a tunnel, between a web browser and a web server. This tunnel ensures that any data transmitted between the two parties is safeguarded and confidential inside the confines of the secure channel. The Secure Sockets Layer (SSL) protocol facilitates the authentication of clients to servers by employing certificates. The server is provided with a certificate by clients as a means of verifying their identity.

The security solution offered by Observable, known as Dynamic Endpoint Modelling, gives a novel perspective on IT security. The system replicates the characteristics of every device within your network, enabling you to comprehend typical patterns and promptly respond to any anomalous behaviour exhibited by a device. There is no necessity to deploy agents on the devices or employ deep-packet inspection, thereby providing a robust solution to address these emerging security challenges. According to a security expert, the utilisation of biometrics on mobile devices is expected to have a significant impact on the authentication of users for network services. The utilisation of biometrics is becoming increasingly prevalent on mobile endpoints, manifesting either in the form of programmes that collect users' behavioural data or as specific features on mobile endpoints that employ personal feature scanning.

REFERENCES

[1] R. K. Kaushik Anjali and D. Sharma, "Analyzing the Effect of Partial Shading on Performance of Grid Connected Solar PV System", *2018* 3rd International Conference

http://doi.org/10.36893/IEJ.2023.V52.174-184

and Workshops on Recent Advances and Innovations in Engineering (ICRAIE), pp. 1-4, 2018.

[2] R. Kaushik, O. P. Mahela, P. K. Bhatt, B. Khan, S. Padmanaban and F. Blaabjerg, "A Hybrid Algorithm for Recognition of Power Quality Disturbances," in IEEE Access, vol. 8, pp. 229184-229200, 2020.

[3] Kaushik, R. K. "Pragati. Analysis and Case Study of Power Transmission and Distribution." J Adv Res Power Electro Power Sys 7.2 (2020): 1-3.

[4] Akash Rawat, Rajkumar Kaushik and Arpita Tiwari, "An Overview Of MIMO OFDM System For Wireless Communication", International Journal of Technical Research & Science, vol. VI, no. X, pp. 1-4, October 2021.

[5] Sharma, Richa and Kumar, Gireesh. "Availability Modelling of Cluster-Based System with Software Aging and Optional Rejuvenation Policy" Cybernetics and Information Technologies, vol.19, no.4, 2019, pp.90-100. https://doi.org/10.2478/cait-2019-0038

[6] G. Kumar and R. Sharma, "Analysis of software reliability growth model under two types of fault and warranty cost," 2017 2nd International Conference on System Reliability and Safety (ICSRS), Milan, Italy, 2017, pp. 465-468, doi: 10.1109/ICSRS.2017.8272866.

[7] P. Rawat, K. D. Singh, H. Chaouchi, and J. M. Bonnin, Wireless Sensor Networks: A Survey on Recent Developments and Potential Synergies,J. Supercomput., 68(1), 1–48, 20 14.

[8] R. Rajkumar, I. Lee, L. Sha and J. Stankovic, Cyber-Physical Systems: The Next Computing Revolution, In Proc. of the 47th Design Autom.Conf., 731–736. 2010.

[9] F. Mattern and C. Floerkemeier, From the Internet of Computers to the Internet of Things, In From Active Data Management to Event-Based systems and More, Springer Berlin, 242-259, 2010.

[10] Y. Mo et al., Cyber-Physical Security of a Smart Grid Infrastructure, Proc. of the IEEE, 100(1), 195-209, 2012.

[11] G. Lu, D. De, W.-Z. Song, SmartGridLab: A laboratory-based smart grid testbed, in: Proc. of IEEE Conference on Smart Grid Communications, 2010.

[12] A. Huang, M. Crow, G. Heydt, J. Zheng, S. Dale, The future renewable electric energy delivery and management (FREEDM) systems: the Energy Internet, Proceedings of the IEEE (1) (2011) 133–148.

http://doi.org/10.36893/IEJ.2023.V52.174-184

[13] Office of the National Coordinator for Smart Grid Interoperability, NIST framework and roadmap for smart grid interoperability standards, release 1.0, NIST Special Publication 1108 (2010) 1–145.

[14] V.C. Gungor, F.C. Lambert, A survey on communication networks for electric system automation, Computer Networks (2006) 877–897.

[15] T.-I. Choi, K.Y. Lee, D.R. Lee, J.K. Ahn, Communication system for distribution automation using CDMA, IEEE Transactions on Power Delivery 23 (2008) 650–656.

http://doi.org/10.36893/IEJ.2023.V52.174-184