International Journal of Computer Science & Communication (ISSN: 0973-7391)
Volume 11 • Issue 1 pp. 46-50 Sept 2019 - March 2020 www.csjournals.com

The Computer Network Security, Cyber-Attack Models and Threats in Computer Network Systems

[1]Rafeak M Salem Abu Alead, [2]Nabil Abulgasem Ali Abrebish, [3]Sasi Salih Maetouq Alhamri
[1]Assistant Lecturer, [2]Lecturer, [3]Assistant Lecturer
[123]Department of Computer Science, Higher Institute of Science and Technology, Tiji, Libya

Abstract -Today's attacks are succeeding far too frequently, all caused by the limitations of legacy security tools. Since the majority of the technologies concerning security arose in the modern era—at the time when attacks that targets information that is sensitive are somehow straightforward to recognize—these tools usually do not succeed in their work if they fail to identify a threat vector or an attack that was previously launched. In recent years, the sophistication and the scale of security that concerns IT threats at an explosive rate have grown. Organizations have to focus on industrialized attacks. Such attacks, in different situations, rival the sophistication and the size of the largest legitimate efforts involving computing. The organizations should also have to implement security against an adversary that is focused on the capabilities and the resources to target highly sensitive information, often through long-term attack campaigns. This paper presents a review of how to secure our computer network.

I. INTRODUCTION

In this innovative age of global connectivity and e-commerce, interconnections via networks have made it possible to heighten, creating a state of complete dependence for both individuals and organizations through vulnerable systems for storage and transfer of information. Never before did people had so much power in their own hands. The power to deface websites access personal mail accounts and worse more the potential to bring down entire governments, and the financial institutions through open-source software documentation codes [12]. This paper illustrates the exploits concerning the components of the typical computer network that are possible; it will also cite the real-life scenarios and causes. The conclusion is also provided to guide all contributors to the development of more secure measures that hinder all network attacks [9].

Related work

Network security is one topic that has been extensively studied by the community that carries out research. According to research, attacks are grouped as Close-in attack, Active attack, Insider attack, Distributed attack, and Passive attack. Attacks can also be on different infrastructure levels including as on the routers or cloud DDoS. [1],[2]. In (Kamal Ahmat, 2015), the author addressed the importance of network attacks at the cloud level and some key mitigation techniques. He explained that different attacks could bring about great harm to Cloud Computing, affecting the most important security aspects (integrity, availability, isolation, confidentiality, etc.). Among those attacks, the DDoS attacks and the DoS attacks mount easily and are usually more destructive, yet there is an existence of huge gaps to efficiently deal with those attacks. The research community studied extensively the DDoS attacks [12]. [1] have given a proposal of a pattern of matching attack detection techniques that overcomes the drawbacks resulting from other detection techniques of the DDoS attacks. Checking of traffic flows through a computer network is based on a particular pattern and can identify easily whether the packet is malicious or is not malicious. This technique of attack detection is advantageous because it has a lower cost of infrastructure because it only uses network switches and routers, which are in existence already. The technique does not use resources of high technology such as multi-core CPU.

In [1] and Martine Bellaiche presented some state-of-the-art solutions: Others were rather incorporated easily in the Cloud infrastructures for the providers of the cloud to reduce DDoS and DoS attacks. [12], various detection and prevention techniques are used to mitigate the network from various types of attacks, and they also give a survey about these types of DDoS attacks and measures taken to mitigate them. It aids to give a fundamental idea of different methods to the reader who would like to get started his research on network security. According to Ammar

Elnour and Kamal Ahmat, threats at the packet level can be introduced as a simple yet effective technique to solve this issue [2].

Network security involves the tasks that are designed to provide security to a network. Some activities are to provide reliability, usability, and security of data and network infrastructure of a business. While effective network security focuses on different types of threats and hinders them from penetrating or spreading into the network, various attack models on the networks have advanced to a serious problem. The figure below represents various cyber-attack models. Some threats in computer network systems are said to include:

Spy programs (Trojan horses and spyware)

Denial of functions attacks (DOS)

Data interception and theft [8.]

While trying to understand network security enhancements, we'll have to review the various classifications of network attacks. The first classification is passive attacks. This type of network attack involves the usage of information stored in the system without harming the system resources. Here, the attacker only observes the data or information transmitted between the sender and the receiver. Passive attacks are usually harmful and will cause disclosure of important information or stored data in files without the user's knowledge. This is because at first, the attacker ensures to have a path to a private and important data such as passwords, usernames and other confidential messages of the user. While passive attacks use ways such as traffic analysis in decrypting weakly encrypted traffic, monitoring unprotected communications and capturing authentication data such as login usernames and passwords. passive attacks have continued to become a major threat to the network security as it threatens the confidentiality of the system with the reason being difficult to detect because it usually gets the required information without necessarily altering the system.

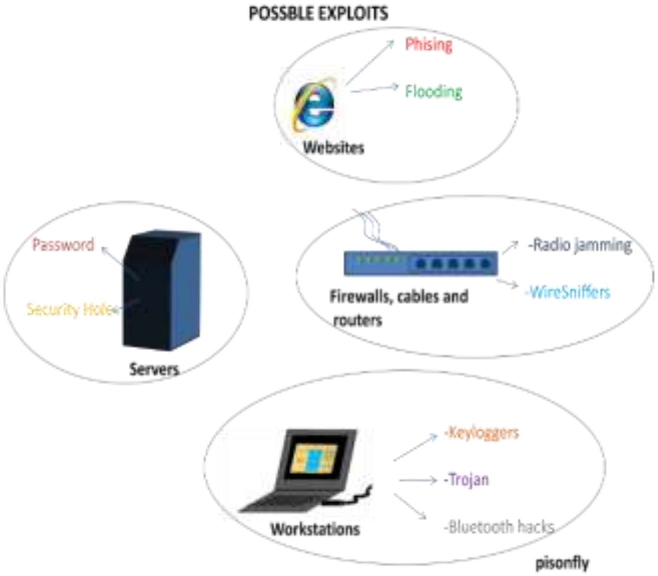

Fig 1: common network attack models

Below is an explanation of the attack models as stated in the above figure.

A. Flooding

This is a model that uses flood net (an application that was created by the American elite group in 1998 to set the Mexican president's 'webpage for political reasons). Flood net is generally a java applet that automates the 'refresh' button to click repeatedly. The users would run the specific application and cause the continuous refreshing of the site's server until it can't anymore thus create a halt to disable the active webpage. In a case, an attacker has used an application that is similar to put into hostage websites that are commercial in exchange for a certain ransom. Flooding is can be a critical threat for a network thus an organization should have a perceptive security expert for an emergency since the web technology has continued to be dynamic with the ever-changing trends in the web scripting languages as well as browser configurations.

Key loggers

Key loggers are simple software codes that aim at exploiting the 'hooks' on a computer's kernel. Hooks are the vital hardware traffic that includes mouse movements as well as keystrokes. The software-based key loggers are programmed to capture any button stroke typed on the keyboard and in turn save words as a text file. This is inclusive of private information typed in such as passwords, google searches, emails, numbers of credit cards and other confidential information

[7]. This information can, in turn, provide the attacker with access to information in the system making the network security vulnerabilities. To avoid this, users should consider updating their antivirus regularly. The use of USB password applications should also be applied to the users' computers to avoid the hardware key loggers which are mostly presented through flash disks [3].

TROJANS

A Trojan is a concealed application that runs in the background easily created by experienced programmers and has a great impact as it allows the attacker to pretend to be a ghost user on someone else's computer. Using Trojan, the attacker can monitor when a specific user's computer is online to deliver captured keystrokes to the address that the attackers prefer. Trojan provides the attacker with a platform to always use in uploading malicious codes that kill your antivirus, take a snap via webcam and records your office conversations from your laptop via the microphone. Research has found out that Trojan comes tucked away neatly on pirated software. It is usually advisable that the network users should use genuine software although expensive so that to avoid this pitfall [3].

B. Bluetooth

Bluetooth has emerged as a versatile technology in networking that is used for establishing connections between workstations and printers, smartphones, etc. Although this technology is currently not in existence according to my knowledge, nevertheless, there is a huge practical possibility.

C. Phishing

This is a scenario where emails appear to come from popular organizations and usually pop up on your screen, sending you various links that request for private information such as credit card numbers, the passwords of some accounts or sometimes even congratulates you for winning. Look-alike websites are also common. They can easily have your authentication and 'refill' your bio-data, after that they can use your information to make some online transactions based on your name or if they appear to be harmful enough, they will deny you to access your account. To avoid this model of the network attack, it is, therefore, advisable to connect your business with the cybersecurity forums and workshops that exist where one can always learn ways to have an edge over scammers and keep your business team informed,[11].

A. Radio jamming

This is usually a very rare technique Denial of Service used to disrupt information flow in a wireless router network accomplished by the application of noise-generating radio devices. However, there is special equipment that exists and can be used tracking of sources of radio-noise, and how the interference is usually detected.

B. Wire sniffers

Attackers usually insert at cable junctions wire sniffing hardware's. It is important to ensure that switchboards and cable terminals are always locked so as their access be granted only to users who are authorized [14].

C. Compromised servers

A compromised server refers to a specific server that is not wholly under your power. This means that another user can easily have gained control of a server that belongs to you. These users can use these servers for their motives or reasons. The usage of weak passwords is usually one way a hacker will easily gain access to your server through guessing your server's password. In most cases, different users prefer to use simple passwords so that not to forget them. Such include specific dates, names of a lover or a pet, the name of the office surroundings, etc. Caution must, therefore, be exercised through a combination of alphabetic letters with different numbers to create a simple but very strong password.

D. Server security holes.

Security of a server can be compromised with security holes in various applications such as add-ons/plugins like WordPress. It is therefore advisable to use only connections that are secure if possible. This is inclusive of usage of SSL connections for email and SFTP (secure file transfer protocol) instead of the more common but insecure FTP protocol [14].

D. Zero-day/hour attack

The 'sticky keys' is a better accessibility characteristic that gives permission a user of an application to press specific keys only once at a particular time. This software runs on the authentication window when the user happens to click the shift key five times even before the entry of their passwords. One specifically requires giving a different name to the command prompt shell (cmd.exe) to sethc.exe on an authenticated computer [14]. Through this, the attacker will be able to gain a full control of your workspace computer any moment later without having to pass through any popular user account in Zero hours in a day attacks take advantage of software vulnerabilities that are yet to catch the eye of a software manufacturer (Bryson, H. et.al, 2017). If you happen to discover such a bug, you should always report to the software manufacturers requesting for an update patch to make up for this identified bug in later software releases. Otherwise, a hacker will be able to discover the same loophole later and can decide to use it maliciously.

II. CONCLUSION

In conclusion, a dedicated network security organ is vital for protecting infrastructures. If you have good network security, your company or organization protected against interruption, employees remain productive. Network security helps you meet compulsory regulatory compliance (Kumar, G. et.al, 2016). Protecting your client's data means no lawsuits emanating from cases about data theft or tampering. It is usually advisable for organizations and businesses to embrace the components of a dedicated security organ on their networks. Some components

include, constantly updated anti-virus software on PC, Installation of firewall that blocks

unauthorized access to the PC USB ports, LAN as well as WIFI [13]. An Imaginary Private Networks to secure remote admission is also a recommended network security system.

REFERENCES

[1] Ahmad Sanmorino and Setiadi Yazid. "DDoS attack detection method and mitigation using the pattern of the flow." International Conference of. IEEE, 2015.

[2] Adrien Benguet, Martine Bellaiche. A Survey of Denial of Service and Distributed Denial of Service and Defence in Cloud Computing, Future Internet. 2017; 9(43).

[3] Brewer, R. (2016). Ransomware attacks: detection, prevention, and cure. Network Security, 2016(9), 5-9.

[4] Bryson, H., Dodds, M., Lu, W., & Palmer, J. (2016). U.S. Patent Application No. 14/912,665.

[5] Bryson, H., Dodds, M., Lu, W., & Palmer, J. (2016). U.S. Patent Application No. 14/912,665.

[6] Fisch, E. A., White, G. B., & Pooch, U. W. (2017). Computer system and network security. CRC press.

[7] International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 3855-3857). IEEE.Kamal Ahmat "Emerging Cloud Computing Security Threats" in arxiv.org/1512.01701

[8] Gandhi, K. (2016, March). Network security problems and security attacks. In 2016 3rd

[9] Kumar, G. D., Singh, M. K., & Jayanthi, M. K. (2016). Network Security Attacks and Countermeasures. IGI Global.

[10] Network Security. In seventh International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2017, Warsaw, Poland, August (pp. 28-30).

[11] Rak, J., Bay, J., Kotenko, I., Popyack, L., Skormin, V., & Szczypiorski, K. (2017). Computer

[12] Sakshi Kakkar and Dinesh Kumar in "A Survey on Distributed Denial of Services (DDOS) in International Journal of Computer Science and Information Technologies, Vol. 5 (3), Classification of attacks. http://computernetworkingnotes.com (1)

[13] Rao, J. D. P., Rai, S., & Narain, B. (2017). A study of Network Attacks and Features of Secure Protocols. Research Journal of Engineering and Technology, 8(1), 4.

[14] Wang, J., & Kissel, Z. A. (2015). Introduction to network security: theory and practice. John Wiley & Sons.