IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 8, August 2019

A Survey on Computer and Network Security Attacks

Eng. Anwar J. Alzaid

The Public Authority for Applied Education and Training - PAAET, Kuwait

Abstract: Computer networks and information systems are used in almost all modern organizations, and the assurance of their safety and security is critical to the organization business continuity. Network administrators and security professionals deploy security tools and equipment to ensure network security and protect organization assets. Hackers and cybercriminals use malicious methods and tools to initiate network attacks and gain access to target organization assets. This paper defines different types of network attacks and their classes also explain the stages and steps of network attacks.

Keywords: Network Security, Data Integrity, Encryption, Authentication, Authorization, Nonrepudiation, Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS)

I.INTRODUCTION

Today in the digital transformation era, Communication play vital rule in our life, and almost all government and business sectors rely on computer networks to help them accomplish tasks and provide services. This can be done by first transforming information into digital form and store it in the organization network servers. Cybercriminals attack the network servers aiming for insufficiently protected services and data. In 2017 more than 2.6 billion data records were Breached, as shown in Fig. 1, only 3.1% of the breached records were protected by encryption [1].

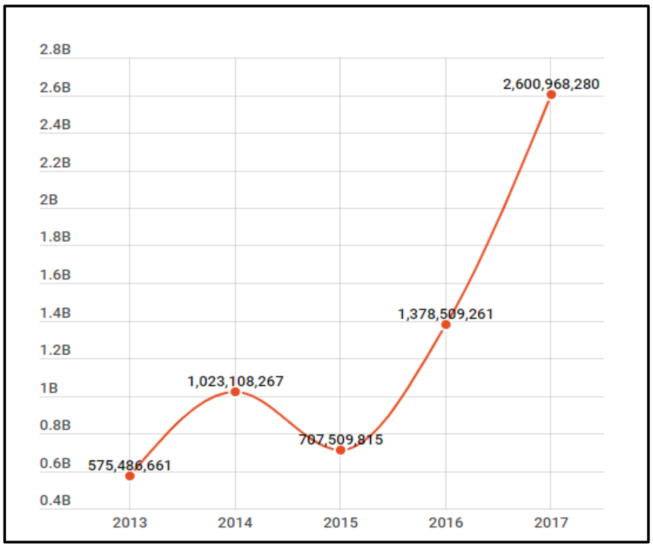

Figure 1 - Number of Breached Data Records [2013 - 2017]

Cybercriminals and attackers intend to terminate, expose, modify, restrict, steal, or gain unauthorized use of one or more digital asset. On the other hand, network security professionals aim to protect their network assets against hacking, misuse, and unauthorized changes.

II.INFORMATION SECURITY GOALS

The objective of information security is to protect information from being stolen, exposed, modified or deleted. Information security is measured by the level of protection a system can provide to the CIA triad, CIA triad is a model that contains the information security properties confidentiality, integrity, and availability. To enforce the CIA triad while developing a secured system, developers and system administrators must utilize tools like authentication, authorization, and Nonrepudiation.

DOI 10.17148/IJARCCE.2019.8806

Confidentiality: Information confidentiality remains intact if the data has only been accessed by an authorized user or process. Encryption and Access control methods can be used to maintain data confidentiality.

Integrity: Integrity is another data security property that focus on the accuracy and correctness of the data. To ensure data integrity, it must be free from unauthorized change. Hashing, digital signature, and digital certificates are cryptographic functions that can be used to check data integrity.

Availability: Availability is to make sure data is always available to authorized users. Redundancy and backups are used to improve data and service availability.

Authentication: Before any system is accessed, the entity requesting the access must be identified and authenticated. Authentication is the first step used by secured systems to verify the identity of a user, process, or a machine. The process of authentication relies on one or more authentication factors like passwords, biometrics, tokens, cell phones, and smart cards to confirm the identity of a user.

Authorization: After authentication, comes the second step which is the authorization. Authorization is a process of giving rights to entities to allow them to access local or network resources. A logged-in user may request some actions by issuing commands. The authorization process decides whether the user has the right to execute such commands. System administrators enforce organization policies by implementing them in the authorization process.

Nonrepudiation: Nonrepudiation is a security approach used in communication systems to provide proof of the document origin (sender identity) and integrity of the message. Using cryptographic functions like digital signature, the receiver can validate the identity of the sender and the integrity of the message. The sender can not deny (repudiate) sending and signing the message.

III.ATTACK STAGES

Based on the cyber kill chain developed by Lockheed Martin [10], a structured cyber-attack can be broken into seven stages. Knowing and understanding the phases of the cyber kill chain will help security professionals to break the chain to reduce or stop attacks on their networks.

A. Stage 1. Reconnaissance.

The first step in any attack, the attacker starts to gather information about the victim. The information the attacker may look for may include the version of operating systems and applications installed, type of hardware and networking devices used, services running in the network, organization policies, security measures employed, etc.

B. Stage 2. Weaponization.

Based on the information gathered in the first step the attacker starts to build an arsenal of tools to be used in the victim's network penetration.

C. Stage 3. Delivery.

Tools selected in the previous step are transmitted to the target's network. The attack tools may be sent as an email attachment or through an infected web server.

D. Stage 4. Exploitation.

In this stage, the attacker utilizes any vulnerability found in the first step. Typically, exploitation focuses on a vulnerable application or operating system, but it also could make use of a social engineering technics to trick a user into taking a specific action.

E. Stage 5. Installation.

At this step, the attacker installs attacking tools on the target system. Installed tools tries to open a backdoor to be accessed by the attacker at a later stage.

F. Stage 6. Command and Control.

In this step, the infected system is programmed to communicate with the attacker's network and create a command and control channel. The attacker uses this channel to control the victim's system remotely.

G. Stage 7. Actions on Objectives.

The attacker now can start to perform the actions required to achieve his objectives and goals.

DOI 10.17148/IJARCCE.2019.8806

IV.NETWORK SECURITY ATTACKS

Computer Networks are built to facilitate information exchange between users, this very fact makes them vulnerable to attacks. A network attack is a malicious and planned act to violate one or more of the information security goals employing various malicious tools and methods to interrupt, modify, or delete data, service, or information system.

A. Security Attack types

Types of security attacks are briefly described below:

1. Normal Flow: Information flow from the source to the destination in a normal fashion as shown in Fig. 2, without any attack.

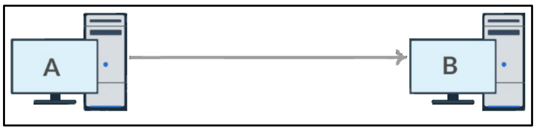

Figure 2- Normal Flow of Data

2. Interception: Interception is a passive attack in which attackers intend to acquire a copy of the information while in transition. Attackers do not alter the original message to avoid exposure. Interception is an attack on confidentiality. Traffic analysis, sniffing, and key loggers are some examples of Interception attacks. See Fig.3.

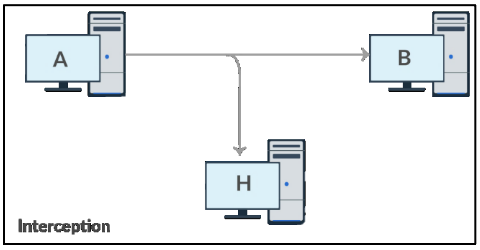

Figure 3- Interception

3. Interruption: In interruption attacks, attackers try to destroy or disable a network asset. Interruption puts the availability of an asset in danger as shown in Fig. 4. Denial of Service, Distributed Denial of Service, and SQL Injection are examples of interruption attacks.

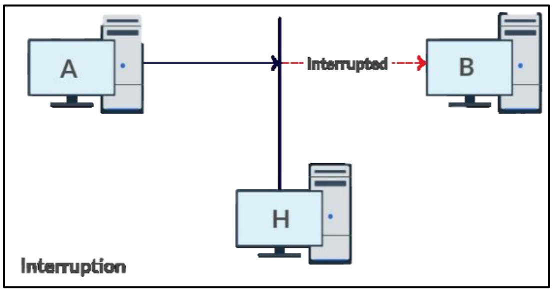

Figure 4- Interruption

4. Modification: In this type of attacks, the attacker tries to modify a part or all of the transmitted data. Modification attacks violate the integrity of data. Man in the middle attack is an example of modification attacks. Refer to Fig. 5.

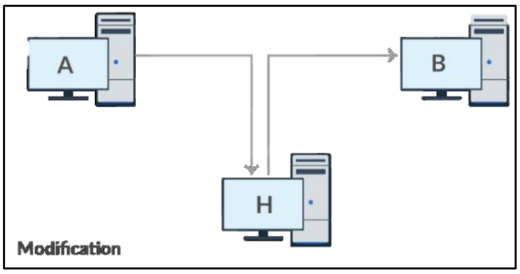

Figure 5- Modification

DOI 10.17148/IJARCCE.2019.8806

5. Fabrication: As shown in Fig. 6, fabrication attacks are attacks on Authenticity, where an attacker pretends to be a legitimate user. A Fabrication is accompanied, as a rule, by another active attack as modification or interruption. Replay and masquerading attacks are examples of fabrication attacks.

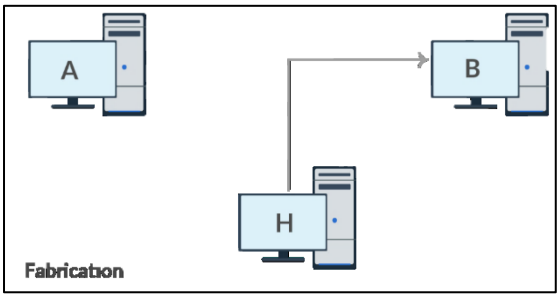

Figure 6-Fabrication

B. Examples of Common Security Attacks:

1. Malware

Malware, which is short for Malicious software is a damaging executable code or script designed to be secretly planted in a system. Examples of malware include viruses, worms, spyware, trojan horses, Ransomware, and crypto-jacking.

- Ransomware: A type of malware that has become very common in the past few years. When Ransomware infects a device, it renders all the user's stored files useless by encrypting them. The user will not be able to open his files unless he pays the ransom and gets the decryption key.
- Crypto-jacking: A relatively new type of malware where the hacker steals the computing power of victims machines. The stolen computing power is used to mine cryptocurrencies for the hacker. The rise in the prices of crypto-currencies in 2017 led to an increase in the crypto-jacking attacks.

2. Denial-of-service attacks

Both Denial-of-service (DoS) and Distributed Denial-Of-Service (DDoS) attacks aim to achieve the same objective, the attacker intends to obstruct a system or service. To achieve this goal, the attacker usually manages to issue a large number of fake requests to the target service which lead it to halt. Attackers use Botnets to launch DDoS attacks by commanding the infected Bot computers to issue fake requests. TCP SYN flood attack, Smurf attack, and Ping of death attack are examples of Denial of service attacks

3. Man in the Middle

Man in the middle is a form of attacks in which the attacker uses a spoofing technique to places himself between two communicating devices and listen to their conversation. Spoofing tricks both the sender and the receiver to think that the attacker is the legitimate other party of the conversation, which places the attacker between them.

4. Phishing and Spear phishing

Phishing attacks aim to trick the victim into surrendering sensitive and personal information to the attacker. The attacker usually uses social engineering techniques and services like E-mail or text messaging to deceive the victim. Using botnets, the attackers can send phishing messages to thousands of recipients. Spear phishing is a personalized and more targeted form of phishing where the attacker crafts the message to be more relevant to the victim. Due to this fact, spear phishing is very hard to detect and to defend against.

5. SQL injection

One of the frequently used attacks to target database-driven websites. Usually, this type of websites contains form pages in which the visitor can enter data in fields. A website can be vulnerable to SQL injection if it has no or a weak data check to the data collected from the form fields. The attack happens when the hacker input an SQL statement in the data field instead of the expected data. The injected SQL statement can erase, alter, or retrieve any amount of records from the database.

6. Cross-site Scripting (XSS)

Cross-site scripting attacks exploit a vulnerable website to target and infect its visitors. The attacker injects a vulnerable website with a malicious code which will be executed on victim machines when they visit the infected website.
Steps of an XSS attack:

DOI 10.17148/IJARCCE.2019.8806

- Attacker finds a website vulnerable to script injection.
- Malicious script is injected to the website.
- Malicious script is downloaded to the website visitors.
- Malicious script is executed on target machine to achieve objectives.

7. Botnets

A botnet is a large number of infected devices with malicious software making them act as obeying robots hens the name Botnet. Attackers control their Botnet remotely to carry out assaults against target systems. Regularly, a botnet is used to flood systems with a very large amount of fake service requests forcing the service to stop or slow down.

8. IoT attacks

Internet of things (IoT) is a network resulted by connecting new type of devices to the Internet. IoT is an extension to the Internet providing connectivity to smart electronic devices and everyday objects like TVs, speakers, door locks, surveillance equipment, and HVAC thermostat. Most of the IoT devices in the market have weak security measures because manufacturers prefer to increase ease of use on the expense of the security. Mirai botnet, which was responsible for one of the most powerful DDoS attacks [11], exploited 148000 IoT devices to achieve 1.1Tbps in 2016.

V.CONCLUSION

It is simple to conclude that network and information system threats will continue to be an issue that must be addressed security professionals. In this paper, information security goals, network attack phases, and network attack types and examples where surveyed. It is crucial for any user today to be familiar with the sources of online and network threats to have a safer online experience.

REFERENCES

[1]. Gemalto. (2019). Data Breach Statistics by Year, Industry, More. [online]. Retrieved from https://breachlevelindex.com/

[2]. Donaldson, S.E., Siegel, S.G., Williams, C.K., & Aslam, A.Q. (2015). Enterprise Cybersecurity. *Apress*.

[3]. Ten, C., Manimaran, G., & Liu, C. (2010). Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, 40*, 853-865.

[4]. Jang, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80, 973-993.

[5]. Bicakci, K., & Tavli, B. (2009). Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks. Computer Standards & Interfaces, 31, 931-941.

[6]. Mahan, R. Introduction to Computer & Network Security. Washington State University, 2000.

[7]. Q. Gu, Peng Liu, “Denial of Service Attacks,” Texas State University, San Marcos.

[8]. Khalil, R. (2010). A Study of Network Security Systems. IJCSNS International Journal of Computer Science and Network Security.

[9]. 2018 Internet Security Threat Report. Symantec, https://www.symantec.com/security-center/threat-report

[10]. Hutchins, E.M., Cloppert, M.J., & Amin, R.M. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Leading Issues in Information Warfare & Security Research. 1.

[11]. Angrishi, K. (2017). Turning Internet of Things (IoT) into Internet of Vulnerabilities (IoV): IoT Botnets. ArXiv, abs/1702.03681.

DOI 10.17148/IJARCCE.2019.8806