International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 6 June 2023, pp: 434-439 www.ijaem.net ISSN: 2395-5252

Threat Attacks on Network Security and Its Solutions

Dr.Abdualla Mahmoud Alshibani Mousbah
(Faculty of Science Bani walid University, Libya.)

Date of Submission: 05-06-2023 Date of Acceptance: 16-06-2023

ABSTRACT

Network security incorporates various technologies, processes, and devices into a broad strategy that protects the integrity, confidentiality, and accessibility of computer networks. Organizations of all sizes, industries, or infrastructure types require network security to protect against an ever-evolving cyber threat landscape.The security is a most important part of every network design. Planning, building, and operating a network, it should understand the importance of a strong security rule. Network Security is a security rule that defines what people can and can't do with network components and resources. The fundamental purpose of a network security is to protect against attacks from the Internet. There are many different ways of attacking a network such as: Hacker attacks whereby a remote Internet user attempts to gain access to a network, usually with the intention to destroy or copy data. The major attacks to network security are passive attack, active attack, distributed attack, insider attack; close in attack, Phishing Attack, Hijack attack, Password attack etc. However a system must be able to limit damage and recover rapidly when attacks occur. So there are various solutions when any of above attacks occurs. Some of the common solutions of these attacks are firewalls, user account access controls and cryptography. The first major challenge for network security is the rapid evolution of the cyber threat landscape. Technologies evolve quickly, and attackers find new ways to infiltrate and exploit corporate networks, requiring businesses to implement new defenses to protect their networks.

I.INTRODUCTION

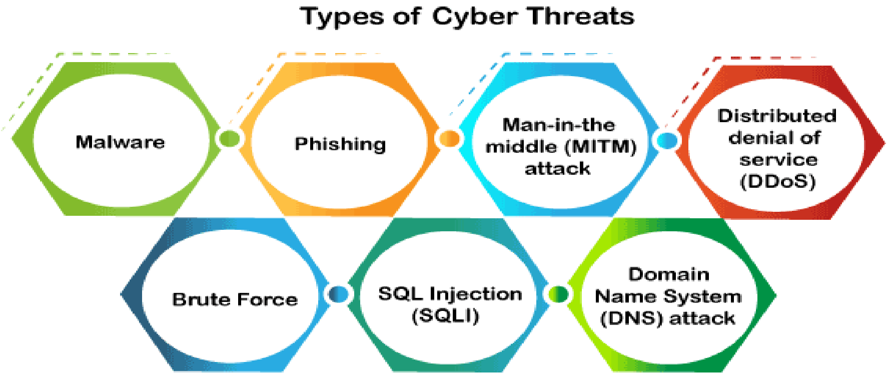
Network security starts with authenticating, commonly with a username and a password. Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Antivirus software or an intrusion prevention system (IPS) helps to detect and inhibit the action of such malware. An anomaly based intrusion detection system may also monitor the network like wires traffic and may be logged for audit purposes and for later high level analysis. Communication between two hosts using a network may be encrypted to maintain privacy. With an increasing amount of people getting connected to many networks, the security threats that cause very harm are increasing also. Network Security is a major part of any network that needs to be maintained because information is passing through or passed between many routers, computers etc. and it is very vulnerable to attack.

In the past, hackers were highly skilled programmers who understood the details of computer communications and how to exploit vulnerabilities. Today almost anyone can become a hacker by downloading tools from the Internet. These complicated attack tools and open networks have generated an increased need for network security and dynamic security policies.

The easiest way to protect a network from an outside attack is to close it off completely from the outside world. A closed network provides connectivity only to trusted known parties and sites; a closed network does not allow a connection to public networks. As they have no Internet connectivity, networks designed in this way can be considered safe from Internet attacks. However, internal threats still exist. Network security is the key to keeping that sensitive information safe, and as more private data is stored and shared on vulnerable devices, network security will only grow in importance and necessity.

Ways to Attack on security

Classes of attack might include passive monitoring of communications, active network attacks, close in attacks, exploitation by insiders, and attacks through the service provider. Information systems and networks offer attractive targets and should be resistant to attack from the full range of threat agents, from hackers to nation states. A system must be able to limit damage and recover rapidly when attacks occur.


Types of Cyber Threats
Malware
Phishing
Man-in-the middle (MITM) attack
Distributed denial of service (DDoS)
Brute Force
SQL Injection (SQLI)
Domain Name System (DNS) attack

- **Passive Attack**

A passive attackmonitors unencrypted traffic and looks for cleartext passwords and sensitive information that can be used in other types of attacks. Passive attacksinclude traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords. Passive interception of network operations enables adversaries to see upcoming actions. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user.

- **Active Attack**

In an active attack, the attacker tries to bypass or break into secured systems. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information. These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks result in the disclosure or dissemination of data files, DoS, or modification of data.

➢ **Distributed Attack**

A distributed attackrequires that the adversary introduce code, such as a Trojan horse or back: door program, to a “trusted” component or software that will later be distributed to many other companies and users Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution. These attacks introduce malicious code such as a back door to a product to gain unauthorized access to information or to a system function at a later date.

➢ **Insider Attack**

An insider attackinvolves someone from the inside, such as a disgruntled employee, attacking the network Insider attacks can be malicious or no malicious. Malicious insiders intentionally eavesdrop, steal, or damage information; use information in a fraudulent manner; or deny access to other authorized users. No malicious attacks typically result from carelessness, lack of knowledge, or intentional circumvention of security for such reasons as performing a task.

➢ **Close in Attack**

A close in attackinvolves someone attempting to get physically close to network components, data, and systems in order to learn more about a network Close: in attacks consist of regular individuals attaining close physical proximity to networks, systems, or facilities for the purpose of modifying, gathering, or denying access to information. Close physical proximity is achieved through surreptitious entry into the network, open access, or both.

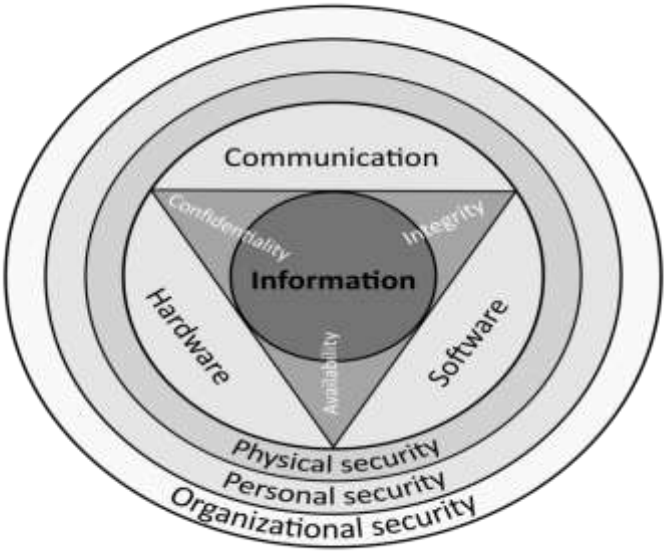
One popular form of close in attack is social engineeringin a social engineering attack; the attacker compromises the network or system through social interaction with a person, through an e:mail message or phone. Various tricks can be used by the individual to revealing information about the security of company. The information that the victim reveals to the hacker would most likely be used in a subsequent attack to gain unauthorized access to a system or network.

➢ **Phishing Attack**

In phishing attack the hacker creates a fake web site that looks exactly like a popular site such as the SBI bank or PayPal. The phishing part of the attack is that the hacker then sends an e-mail message trying to trick the user into clicking a link that leads to the fake site. When the user attempts to log on with their account information, the hacker records the username and password and then tries that information on the real site.

➢ **Hijack Attack**

Hijack attack in a hijack attack, a hacker takes over a session between you and another individual and disconnects the other individual from the communication. You still believe that you are talking to the original party and may send private information to the hacker by accident.



Some more of the most prevalent types of network security attacks any IT professional should be aware of include the following:

- Data Theft: Also called data exfiltration, data theft occurs when an attacker uses their unauthorized access to obtain private information from the network. Attackers frequently use stolen login credentials to read protected files or steal the data while it is in transit between two network devices.

- Malware Attacks: A malware attack occurs when a malicious code (malware) inserts undesired, unauthorized software onto a network device. Malware can easily spread from one device to another, making it very difficult to get rid of entirely.
- Password Attacks: Any type of attack that involves someone attempting to use a password illegitimately is considered to be a password attack. The hacker may obtain access either by guessing, stealing or cracking a password.
- Social Engineering: These attacks use deception and falsehoods to convince others to give up private information, such as an account password, or to violate security protocols. Social engineering attacks often target people who are not tech-savvy, but they may also target technical support staff with false requests for help.

II. SOLUTION ON SECURITY ATTACKS

The recommendations to protect your company against Phishing and Spear Phishing include:
1. Never open or download a file from an unsolicited email, even from someone you know (you can call or email the person to double check that it really came from them)
2. Keep your operating system updated
3. Use a reputable antivirus program
4. Enable two factor authentications whenever available
5. Confirm the authenticity of a website prior to entering login credentials by looking for a reputable security trust mark
6. Look for HTTPS in the address bar when you enter any sensitive personal information on a website to make sure your data will be encrypted.

Some of the most common types of network security solutions include:

Antivirus Software: Antivirus software can be installed on all network devices to scan them for malicious programs. It should be updated regularly to fix any issues or vulnerabilities.

Encryption: Encryption is the process of scrambling data to the point of unintelligibility and providing only authorized parties the key (usually a decryption key or password) to decode it. This way, even if data is intercepted or seen by an unauthorized user, they are unable to read it.

Firewalls: Firewalls are a software program, hardware device or combination of both that blocks unsolicited traffic from entering a network. They can be configured to only block suspicious or unauthorized traffic, while still allowing access to legitimate requests.

Multi-Factor Authentication: Multi-factor authentication is simple: users must provide two separate methods of identification to log into an account (for instance, typing in a password and then typing in a numeric code that was sent to another device). Users should present unique credentials from two out of three categories — something you know something you have and something you are — for multi-factor authentication to be fully effective.

Network Segmentation: Network segmentation involves breaking down a larger network into various subnetworks or segments. If any of the sub networks are infiltrated or compromised, the others are left untouched because they exist independently of each other.

➢ **Security measures**

A state of computer "security" is the conceptual ideal, attained by the use of the three processes: threat prevention, detection, and response. These processes are based on various policies and system components, which include the following:

1. User account access controls and cryptography can protect systems files and data, respectively.

2. Firewalls are by far the most common prevention systems from a network security perspective as they can (if properly configured) shield access to internal network services, and block certain kinds of attacks through packet filtering. Firewalls can be both hardware: or software based.

3. Intrusion Detection Systems (IDSs) are designed to detect network attacks in progress and assist in post attack forensics, while audit trails and logs serve a similar function for individual systems.

4. "Response" is necessarily defined by the assessed security requirements of an individual system and may cover the range from simple upgrade of protections to notification of legal authorities, counter attacks. In some special cases, a complete destruction of the compromised system is favored, as it may happen that not all the compromised resources are detected.

➢ **Preventing network attacks**

There is also Denial of Service (DoS) and distributed DoS attacks resulting in loss of services such as email, Internet connectivity or causing servers to run almost at a standstill. A correctly configured firewall will prevent most attacks and may use a combination of the following processes to offer protection:

1. Steal the network: This is a process in which the firewall effectively 'hides' the protected network so that it does not appear on the Internet.

2. Packet inspection technology analyses each packet as it travels through the firewall to make sure that it is legitimate and that the source and destination of each packet are valid.

3. Network Address Translation (NAT): NAT removes the IP addresses of computers behind the firewall and replaces them with a single public IP address.

4. Closing unused ports:Depending on the configuration of the firewall unused ports, often the subject of hacking attacks can be closed.

➢ **Protection of Network from Cyber Attacks:**

1. Install IDS/IPS with the ability to track floods.

2. Install a firewall that has the ability to drop packets rather than have them reach the internal server. The nature of a web server is such that you will allow HTTP to the server from the Internet. You will need to monitor your server to know where to block traffic.

3. Have contact numbers for your ISP's emergency management team (or response team, or the team that is able to respond to such an event). You will need to contact them in order to prevent the attack from reaching your network's perimeter in the first place.

4. Ensure that HTTP opens session’s time out at a reasonable time. When under attack, you wish to reduce this number.

5. Ensure that TCP also time out at a reasonable time.

6. Install a host based firewall to prevent HTTP threads from spawning for attack packets.

III. NETWORK PROTECTION TIPS

Grant Access Sparingly

Always be aware of who has access to your network or servers. After all, not everyone in your organization needs to be able to physically or electronically access everything on your network. Don’t give blanket access to every employee in your organization; only give out what information is necessary to help reduce the chance of unauthorized access, purposeful or unintentional tampering, or security breaches.

Follow Password Best Practices

It’s a basic principle, but following password best practices is a simple and highly effective way to maintain network security. Many people create passwords that aren’t strong, reuse previous passwords and don’t use unique passwords for each of their accounts. Encourage all employees to follow password best practices, especially for their work accounts, as it can help keep everyone’s data safe.

Secure Servers and Devices

Physically protect your servers and your devices. Keep them in a safe location, and do not grant general access to this room or area. Be sure the room is locked when it’s not in use and keep an eye on the area when it is unsecured or in use.

Test Your Security

You should never assume that your network is completely secure. Continually test and troubleshoot your network to see what is substandard or to identify any vulnerability. Be sure to make fixes and updates as needed.

IV. CONCLUSION

Web security threats are a form of internet-borne cybersecurity risk that could expose users to online harm and cause undesired actions or events. Web security issues can severely damage businesses and individuals. Common types of web security threats include computer viruses, data theft, and phishing attacks. While they are not limited to online activity, web security issues involve cyber criminals using the internet to cause harm to victims. They typically cause problems like denial of access to computers and networks, unauthorized access to and usage of corporate networks, theft and exposure of private data, and unauthorized changes to computers and networks.Web security threats and approaches have evolved in sophistication with the rise of faster mobile networks and smart devices. Increased web adoption through popular communication and productivity tools, as well as the Internet of Things, has outpaced the security awareness and readiness of most businesses and end-users.These web security issues will only increase as people become more reliant on the web, creating new vulnerabilities for attackers to exploit.Network Security is a very broad field and being a Network Security manager is not an easy job. There are still threats such as password attacks that have no prevention. Many of the threats set out to get personal information. In some attacks, the attacker tries to break the security systems through stealth, viruses, worms, or Trojan horses. In attacks like phishing attack the hacker creates a fake web site that looks exactly like a popular site such as the SBI bank and thus fools the user and retrieves the information. Computer and network technologies have intrinsic security weaknesses. Different types of web security threats include computer viruses, data theft, and phishing attacks. Web security threats typically lead to issues like denial of access and unauthorized changes to devices and networks and data exposure.

REFERENCES

[1]. Case Study: Network Clarity Archived 2016-05-27 at the Wayback Machine, SC Magazine 2014

[2]. Cisco. (2011). What is network security?. Retrieved from cisco.com Archived 2016-04-14 at the Wayback Machine

[3]. Security of the Internet (The Froehlich/Kent Encyclopedia of Telecommunications vol. 15. Marcel Dekker, New York, 1997, pp. 231–255.)

[4]. Introduction to Network Security Archived 2014-12-02 at the Wayback Machine, Matt Curtin, 1997.

[5]. http://www.itsecurity.com/features/network:security:thre ats:011707

[6]. http://www.itsecurity.com/features/network:security:thre ats:011707

[7]. http://en.wikipedia.org/wiki/Computer_security

[8]. http://fastnet.co.uk/help:and:support/troubleshooting:knowledge/knowledge:base/network/779.html

[9]. http://www.sophos.com/en:us/security:news:trends/security:trends/how:to:protect:your:network:from:cyber:attacks .aspx

[10]. Security Monitoring with Cisco Security MARS, Gary Halleen/Greg Kellogg, Cisco Press, Jul. 6, 2007. ISBN 1587052709

[11]. Self-Defending Networks: The Next Generation of Network Security, Duane DeCapite, Cisco Press, Sep. 8, 2006. ISBN 1587052539

[12]. Security Threat Mitigation and Response: Understanding CS-MARS, Dale Tesch/Greg Abelar, Cisco Press, Sep. 26, 2006. ISBN 1587052601

[13]. Securing Your Business with Cisco ASA and PIX Firewalls, Greg Abelar, Cisco Press, May 27, 2005. ISBN 1587052148

[14]. Network Security: PRIVATE Communication in a PUBLIC World, Charlie Kaufman | Radia Perlman | Mike Speciner, Prentice-Hall, 2002. ISBN 9780137155880

[15]. Network Infrastructure Security, Angus Wong and Alan Yeung, Springer, 2009. ISBN 978-1-4419-0165-1