Data Network security issues

What is a Network?

The computers connected through intranet together in an order to serve a number of users in a particular area like in an office can be termed as a Network.

What is Network Security?

Network security deals with aspects like prevention of unauthorized access, termination of misuse and denial of the service problems. Security may be referred to as complementing factors like: confidentiality, integrity and availability (CIA). If you are thinking that this is it, you are absolutely wrong.

Different types of Network Threats

Following are the types of threats against which a network is vulnerable to:

Threat #1 DOS Error & DDOS Error

DOS, a short form of Denial of Service and DDOS short form of Distributed Denial of Service are superior amongst all the threats as they are very difficult to get rid of. In addition, they easily get launched and are cumbersome to track.

How can one generate such an attack?

It is very simple; just keep sending more and more requests to the system than that it can handle all along.

With the invention of the toolkit, it has become way easy to disturb any website's availability.

In DOS an attacker's program will establish a connection on a service port, obviously counterfeiting the packet's header details and then leaves the connection. Now if the host can handle 20 requests per second and the attacker is sending 50 requests per second, then it may cause the host server down due to mass fake requests. In this case, the server cannot accept the legitimate requests as well due to fake requests and it shows the unavailability of the server to a legitimate user.

Security Solutions

- Monitoring the packets to save your server from the entrance of the counterfeit packets.
- Timely upgrading of the security patches on your host's operating system.
    - Beware of the running your server very close to the last level of the capacity.

Threat #2 Unauthorized Access

This is the most harmful threat as it leads to the loss of significant information and also to further attacks which could be worse than this. An attacker unknowingly gains access to your authorized section and steals sensitive resources. Suppose a host also playing the role of a web server has to provide web pages as per the request. But the host should not allow anybody to access the command shell without being sure about the identity of the user.

Security Solutions

- Enforce strong authentication strategies.
- Keeping usernames and passwords secret from the unreliable sources.
- Not providing unnecessary access to any user or even to any employee.

Threat #3 Eavesdropping

Another greatest security threat in the network. During eavesdropping, an intruder intercepts the packages of data transferred over HTTP (through monitoring software), modifies the data and misuses them in order to harm the network. It is really a dangerous threat as there are many tools named as Sniffers available and developed frequently to intercept the data packages.

Security Solutions

- Entertaining encryption strategy will secure you a way out from eavesdropping. Using encryption measures like digital certificates (SSL certificates) will definitely lessen the risk of eavesdropping attacks.
- Apply network segmentation which will prevent eavesdropping as well as other network attacks.
- Employing Network Access Control enhances the security of your network by checking the authenticity of every device before establishing any connection.

Threat #4 IP Spoofing

IP spoofing means presuming the IP of a network, creating an illusion of being a valid IP by creating Internet Protocol packets with disguised intentions of harming the actual owner of the IP address.

By forging the headers in order to insert fallacious information in the e-mail headers to mislead the receiver from the original destination is also a type of spoofing which is known as Spamming.

Security Solutions

- Filtering of packets entering into the network is one of the methods of preventing Spoofing. On other hand, filtering of incoming and outgoing traffic should also be implemented.
- ACLs help prevent Spoofing by not allowing falsified IP addresses to enter.
- Accreditation to encryption should be provided in order to allow only trusted hosts to communicate with.
- SSL certificates should be used to reduce the risk of spoofing to a greater extent.

Threat #5 Man-in-the-middle-attack

MITM is one of the most dreadful network threats. An intruder here establishes an independent connection with both sender and receiver, intercepts their messages one by one, modifies those messages and relays them back to the sender and receiver. This all occurs so smoothly that both the sender and receiver never come to know that they are being overheard by someone. In addition, it exposes your network to several other threats.

Security Solutions

- Using Public Key Infrastructures based authentications. It not only protects the applications from eavesdropping and other attacks but also validates the applications as a trusted ones. Both the ends are authenticated hence preventing (MITM) Man-in-the-middle-attack.
- Setting up passwords and other high-level secret keys in order to strengthen th e mutual authentication.
- Time testing techniques such as Latency examination with long cryptographic hash functions confirming the time taken in receiving a message by both ends. Suppose if the time taken by a message to be delivered at one end is 20 seconds and if the total time taken exceeds up to 60 seconds then it proves the existence of an attacker.

Threat #6 Brute Force Attacks

A brute Force attack is performed to guess the maximum combination of passwords. It is researched that 5% of attacks are responsible for Brute Force attack. An attacker does not interfere in the user's task but works on each keystroke a user types and guess the combination of username and passwords. The attacker checks all passphrases and passwords until a correct match is not found.

Security Solutions

- A user should increase the password's length, and the complexity of a password should be increased.
- A limited login should be enabled like after three failed attempts; a user will be locked.
- Multi-factor Authentication can help to avert brute force attack as it works as an additional layer when a login attempt is made.

Threat #7 Browser Attacks

Browser attack is intended to expose sensitive information like a credit card, login details, and other details. When a browser is compromised, the attackers gain access end-user system. Attackers can infiltrate the network by hijacking the browser and spread malicious code to steal the information. Browser attack includes social engineering attack, buffer overflow, XSS attack, man-in-the-browser attack.

Security Solutions

- Enterprise can use browser isolation where a website runs in a cloud to access it.

- Antivirus is a solution to prevent browser attack at some point.
- Operating system isolation is an option where each device is divided into multiple segments and its operating system. Each device will connect to the invisible network virtualization layer.

Threat #8 SSL/TLS Attacks

SSL creates a protected tunnel using strong authentication for data transmission between the client and a server. The attacker uses an unencrypted session to attack flowing plain text data. Almost 6% of total network attacks accounted for SSL attacks. To prevent SSL attacks, network testing is performed and shielded from upcoming attacks.

Security Solutions

- The network admin can perform penetration testing, intrusion testing, as well limit network access control.
- Implement an HSTS policy in which a browser is forced to allow open HTTPS pages only.
- Enable HTTPS on a domain name. Educate users about the use of HTTPS.

Threat #9 DNS Query attack

DNS Query attack refers to a manipulated act in which an attacker finds a DNS vulnerability (Domain Name System) and takes advantage of it. Attackers sniff a plain text communication between the client and DNS servers. DNS converts the domain name into an IP address. The zero-Day attack, Denial of Service, DDoS attack, DNS amplification, Fast-Flux DNS are few types of DNS Query attack. In few cases, attackers steal login credentials of the DNS provider's website and use them to redirect DNS records.

Security Solutions

- Prevent cache by limiting users' access to resolver as hackers could not manipulate a resolver's cache. It would help if you closed any open resolver on the network.
- Do audit your DNS zones, including CNAME, MX records, and IP addresses. Moreover, it would be best to keep an updated DNS server in case of your servers.
- Keep authoritative and resolving functions separately using different servers.

Threat #10 Ping sweep attack

Ping is a utility that confirms whether the host is alive (active) or dead (shut down). The host can be a computer, system, website, printer, or network. Ping sweep attack refers to collect the information by finding alive hosts, which uses Internet Control

Message Protocol (ICMP) or two-way handshake protocol. Ping sweep attack includes two-way communication like sending data from a single host and validates the data by another host along with acknowledgment. The acknowledgment shows either a ping was sure-fire or not.

Security Solutions

ICMP functionality should be disabled about a specific router or any device. Disable the send and receive ability of ICMP includes request processing and Echo reply. Consequently, the device will not accept any ping request.

Threat #11 Packet capturing attack

Packet capturing attack refers to sniffing and capturing data packet that passes through a network. Administrator watches and tracks data traffic. Attackers can capture data packets from the network and extract information like passwords, login details, payment-related information.

Security Solutions

- Users should avoid free public Wi-Fi or any unsecured network to avoid data sniffing over the network.
- Use of encryption that binds travelling information between network and users.
- Scan and monitor the traffic on the network to find any suspicious activity.
- Hire a certified ethical hacker to watch over network activities.

Threat #12 Reconnaissance Attack

A reconnaissance attack is a piece of collecting information through physical reconnaissance, network examining, social engineering. Ping sweep, phishing, packet sniffing are few examples of Reconnaissance attacks. Attackers keenly observe social media profiles and find loopholes in the network, applications, and services and search the area to take advantage of them.

Security Solutions

- Do continuous inspect network traffic to stop port scanning.
- Run security awareness training for users to give them an idea about what to share and what not to.
- Conduct audit of logical and physical security in the office

These were some of the vulnerabilities prevailing in network security. Other prevalent vulnerabilities consist of data loss, data modification, sniffer attack, application-layer attack, password-based attacks and so on.

Security stands as the toughest challenge as it gets more and more vulnerable to attacks day by day.

As far as the network security is concerned, paying attention to some of the aspects will help to achieve proper secure environment such as:

- Backing up the data regularly
- Store the data on a reliable medium.
- Update your patches
- Install SSL certificates to stay ahead of threats
- Upgrading Firewalls with ACLs (Access Control Lists), Demilitarized Zone (DMZ), Proxy and routers.

Keeping in mind the needs as well as the threats against which your network is vulnerable to, you should use the best security mechanism to protect your organization.

Ref.: https://www.clickssl.net/blog/network-security-threats-and-their-solutions

……………………

1. Ransomware

This is one of the most feared and unpredictable network security issues, as it leaves costly damage to businesses. Usually, attackers infect the systems, encrypt data, and threaten to delete or corrupt the files if they're not paid some expensive ransom.

The best way to defend against and resolve ransomware is to use antivirus software, teach team members how to distinguish phishing attacks, and update your system's security patches. To minimize the impact, focus on the importance of network security and create a solid recovery and backup strategy.

2. Insufficient Network Security Team

Another common network security issue for many businesses is that even when they have the best cybersecurity solutions, their team might not have enough people to manage such solutions properly. Once it happens, your team might miss some critical cybersecurity alerts, and cyberattacks might not be prevented in time to reduce damage.

Finding enough people for your internal network security team to manage your needs can be time-consuming and expensive. Take note that most qualified professionals are highly in demand. Working with a dedicated partner that offers quality services or solutions would be a good option to build a team to handle your network security issues quickly.

3. Unknown Assets On Your Network

More often than not, most businesses don’t have a complete inventory of the digital assets tied into their network, which can be a massive problem over time. If you’re clueless about the assets on your network, how will you be able to keep it safe and secure?

The best possible solution for this is to review all the devices connected to your network and to determine the different platforms they’re using. Once you do this, you’ll know the access points on your network, and this will help you determine which ones require security updates.

4. Insider Threats

At present, most attacks are actually carried out by insiders. Whether it’s misuse of account privileges, intentional leaks, honest mistakes made by sending information to wrong email addresses, or identity theft due to a phishing campaign that compromises user account data, your team members could be one of the security problems you’ll face.

Since insider threats come from trusted systems and users, they’re also the hardest to stop and identify. However, there are some ways to reduce your risk in case of insider attacks. For instance, if your business company uses a policy of least privilege (POLP) for user access, you may limit the damage that misused user accounts can do. In this kind of policy, users' access to the different databases and systems on your network is restricted to only what they need to do their jobs.

5. Lack Of Defense

Lack of defense is another common network security issue. You have to remember that despite your best efforts, attackers may succeed in breaching your network security. But the damage they can do may depend on how secure your network is. For this reason, you may need a multilayered defense.

Usually, the problem is that several businesses have an open network structure where attackers are in the trusted system, giving them access to your network's systems. If your network has strong segmentation to keep its discrete parts separated, it's possible to slow down the attackers enough to keep them out of the crucial systems. At the same time, your security team can work to identify, contain, and eliminate the breach.

6. Unpatched Security Vulnerabilities

Most businesses are worried about zero-day exploits, which are unknown issues with security in systems and programs that have yet to be used against anybody. But a zero-day vulnerability isn't the problem. The primary problem is an unpatched known vulnerability.

The simplest solution for this network security issue is to keep a strict schedule for security patches. Gradually changing your network's operating systems and programs to make them the same can simplify the entire process. For instance, if all your systems are Mac-based or Windows-based, you should keep track of these operating systems' security patch alerts and schedules.

Conclusion

Network security issues could happen at any time. The good news is that there are ways to resolve them immediately. As long as you're armed with knowledge about network security, you can be ready for the inevitable. If you think you can't handle the situation, do not hesitate to work with experts in network security to get the best possible solutions for the problem.

-

Ref.: https://www.bbntimes.com/companies/6-common-network-security-issues-and-how-to-resolve-them

……………

What are some of the vulnerabilities prevailing in network security?

- These were some of the vulnerabilities prevailing in network security. Other prevalent vulnerabilities consist of data loss, data modification, sniffer attack, application-layer attack, password-based attacks and so on. Security stands as the toughest challenge as it gets more and more vulnerable to attacks day by day.

  ….

- The primary problem is an unpatched known vulnerability. The simplest solution for this network security issue is to keep a strict schedule for security patches. Gradually changing your network's operating systems and programs to make them the same can simplify the entire process.