Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

13

A study on Network Threats, Attacks & Security Measures

Vishal Udaykumar Harsora

Research Scholar, Department of Computer Science, Surendranagar University, Wadhwan

Corresponding Author E-mail: Mohsen.soori@emu.edu.tr

Abstract

Networks are accessible accessories due to their basal affection of facilitating alien admission and abstracts communication. The advice in the networks needs to be kept anchored and safe in adjustment to accommodate an able advice and administration accessory in the web of data. Due to challenges and threats of the abstracts in networks, the arrangement aegis is one of the best important considerations in advice technology infrastructures. As a result, the aegis measures are advised in the arrangement in adjustment to abatement the anticipation of accessing the anchored abstracts by the hackers. The purpose of arrangement aegis is to assure the arrangement and its apparatus from crooked admission and corruption in adjustment to accommodate a safe and anchored advice accessory for the users. In the present analysis assignment a analysis in contempt development of arrangement threats and aegis measures is presented and approaching analysis works are additionally suggested. Different attacks to the networks and aegis abstinent adjoin them are discussed in adjustment to access aegis in the web of data. So, new account in the arrangement aegis systems can be presented by allegory the appear affidavit in adjustment to move advanced the analysis field.

Keyword: Network Security, Data Protection, Cyber security, Network Threats, Access Control, Data Encryption, Hacker Attacks, Future Research

INTRODUCTION NETWORK

Network Security is one of the best important considerations in the acreage of advice aegis today with the amplification of business arrangement dependencies on IT-based infrastructures. The abridgement of aegis measures in IT basement can account irreparable accident to organizations and companies which is not adorable for business and business process. The purpose of arrangement aegis is primarily to anticipate accident from abstracts misuse. There are a cardinal of abeyant problems that can action if arrangement aegis is not implemented properly. Every business will charge to accumulate some analytical and classified advice from the admission of its competitors. The abstracts accident can abatement the added amount in the action of allotment assembly and marketing. Moreover, the accurate way of affective in the business and artefact business can be absent due to the abstracts abetment as a after-effect of abridgement of aegis measures in the banking information. As a result, the abridgement of aegis admeasurements in the web of abstracts can account abuse of acquaintance in the altered businesses and business of products. Therefore, it is basic for any arrangement ambassador.

A. Network Security Threats and Attacks

In order to provide the security measures in the network of data, the attacks should be clearly defined. An attack is dangerous or non-dangerous attempt to modify or use a resource accessible through the network in a way that was not intended. The network attacks can be classified into three general categories:

1- Unauthorized access to resources and information through the network.

2- Unauthorized manipulation of information on a network.

3- Attacks that lead to disruption of service delivery and are called Denial of Service [1].

The key word in the first two categories is to perform actions illegally. Defining an authorized or unauthorized action is the responsibility of the network security policy which can be defined as an attempt by a user to view or modify information that is not allowed. Unauthorized access can be one of the most common attacks on any network. In this way, the attacker tries to access the restricted area of information and the network. Breaking passwords, creating sub-paths, creating fake identities or using malware are the main ways to carry out these attacks, Information destruction is one of the most destructive attack networks. In this way, the attacker tries to destroy certain information by performing commands in the database. This can be limited or very extensive. Depending on the type of attacker, the network can lose all your information in a matter of seconds. Attacks that lead to disruption of service delivery are another form of unauthorized access. In this method, the person enters the user or management area to execute the command or a set of commands which are normally prohibited. In this way, the attacker may write, modify, send email, copy information, or delete certain information in order to find a way to access to the restricted data. The extent of the attack depends on the capabilities of the attacker. Network security threats fall into one or two general categories as Logic Attacks or Recourse Attacks. Rational attacks, as the name implies, are a for-profit strategy used to eliminate any weakness in the system. Weaknesses can include software vulnerabilities such as backdoors and security errors in the code. The purpose of the attack is to enter the system in order to corrupt or gain unauthorized access of the system. Resource attacks are aimed at destroying resources of networks. The trick became more popular in the 1990s, but gradually declined in popularity. In this method, the network system is forced to be destroyed, which is therefore vulnerable. These attacks are carried out in different ways in order to apply forces to the web of data. The fastest way is for the server to face a huge flood of service requests that are out of its control. Also, some resource attacks involve installing malware on the network, which will make it vulnerable [2].

Types of Network Security Threats

Threats	**Description**	**Security measures**
Insider attacks	The insider is a part of the organization that has full access and authorization of the network system. The insider can be of malicious or accidental nature and can be a threat to organization's	Implementing dual control principle helps more than one person to control login credentials for organization's servers.

	confidentiality and integrity	
Lack of contingency	Many organizations suffer due to lack of planning for situations involving bad data failure. As a result, they do not have a backup system for restoring the lost data.	Developing sound information assurance methodologies helps develop personalized policies benchmarked from other organizations.
Poor configuration leading to compromise	Many organizations with lack of funds and experience often install networking gear without having skilled personnel to handle them.	Automated vulnerability audit scan is a method which performs check of the entire network and must be conducted at regular basis.
Reckless use of hotel networks and kiosks	Many attackers leave a key logger to access passwords and credential information from personal devices connected in an infected hotel network that are not much protected enough counter such attacks.	Forbidding turning off defenses through certain anti-virus solutions which are configured in such a way that they cannot be turned off without proper authorization
Reckless use of Wi-Fi hotspots	Similar to key logger in hotel networks, the attackers put up an unsecured Wi-Fi network to capture secured information such as username and passwords of employees without making them aware of any threat to their computer.	Using encrypting connections which can be connected via Virtual Private Networks and encrypts the communication streams preventing eavesdroppers to listen to the data wirelessly.
Data lost on portable	It is a common problem with	Centralized management of

device	most of the users who accidently leave their storage devices such as mobile phones, pen drives or USB stick in hotel rooms, taxis or trains making it easily available for attackers to retrieve sensitive information.	mobile devices through servers and software such as RIM's Blackberry Enterprise Server help the organization ensure encrypted transmissions and are capable of remotely wiping out data of lost devices.
Web server compromise	Poorly written customer application on websites have made easier for the attackers to penetrate thousands of servers with automated SQL injection attacks.	Auditing web app code is a measure which helps the users identify whether the developed code has been performing proper input validation or not
Malicious HTML email	This is a common email attack which links the user to a malicious website and triggers a drive by download by a single click.	Implementation of outbound web proxy which includes setting up of LAN system redirecting all HTTP requests and responses to a web proxy server which monitors all the web traffic

Types of Network Attacks

The networking attacks can be aggregate into two major categories namely acquiescent attacks and alive attacks. Detailed description of both kinds of attacks is accustomed below.

1. **Passive attacks**

   In passive attacks the attacker eavesdrops or monitors the data transmitted to find the content of data transmitted or to analyse the nature of communication. Such attacks analyse traffics, monitors unprotected communications, decrypts weakly encrypted data and captures authentic information such as passwords. Such attacks can lead to disclosure of sensitive information without the knowledge or consent of the user. These attacks are hard to detect as there is no loss and alteration of data.

2. **Active attacks**

In active attacks, the attacker tries to circumvent or break into protected systems in the on-going communication networks. Such kind of attacks includes breaking into secured features, injecting a malicious code and stealing or modifying sensitive information [10]. In these kinds of attacks the data transmitted can be altered by the attacker or the whole data stream can be changed. Active attacks can be detected but these are difficult to prevent. Various error detection and correction techniques are used at various network layers to acquire a safe data transmission. Active attacks can take place in four ways: Masquerading, Replay, and Modification of message and Denial of Service.

There are other kinds of network's attacks which pose serious threat to the confidentiality of the organization. Some these attacks are listed below.

1. **Distributed Denial-of-Service Attack**

   A malicious actor deploys networks of bonnets (large networks of malware-compromised devices) to direct high volumes of false traffic at an enterprise network. This fraudulent traffic overwhelms servers, prevents legitimate users from accessing a website, and may cause website crashes. A DDoS attack can cripple an organization's entire IT infrastructure.

2. **Man-in-the-Middle Attack**

   In MITM attacks, attackers intercept legitimate traffic between networks and external data sources (such as websites) or internally within the network. These eavesdropping attacks usually happen due to weak security protocols that allow bad actors to obtain user credentials, hijack user sessions, and steal data (credit card numbers, for example) in real-time transactions.

3. **Unauthorized Access**

   Unauthorized network access is one of the most common types of cyber attacks aimed at enterprise networks. Weak passwords are a common cause of unauthorized access attacks; an attacker guesses the password to a legitimate user’s account, and then logs into the network under false pretenses.

Other causes are unencrypted networks or data, previously compromised accounts, insider threats where privileges are abused, the misuse of inactive accounts with administrator rights, social engineering, and phishing or spear-phishing attacks.

Social engineering attacks are difficult to prevent since they rely on human weaknesses. Technical vulnerabilities can be addressed more systematically with stronger cyber security protections.

4. **Insider Threats**

Insider threats are also a growing problem. The number of insider threat-related incidents increased by 47 percent from 2018 to 2020. The total average cost of insider threats in 2020 increased to $11.45 million.

Insider threats can come from anywhere, including current or former employees, vendors, contractors, partners, and so forth. Any “insider” with access to the organization’s computer systems and data increases the risk of a network attack. Such attacks are difficult to detect and prevent because the attacker already has access to the systems and data inside the network.

5. **Privilege Escalation**

Clever attackers use privilege escalation to expand their reach within the target system or network. In horizontal attacks, they gain access to adjacent systems; in vertical attacks, they gain higher privileges within the same system.

To prevent privilege escalation and protect high-value data from unauthorized access, organizations must employ strict adherence to the “principle of least privilege” (PoLP). In PoLP, all users — employees, third parties, applications, systems, and connected IoT devices — are given only the minimum levels of access needed to perform their job functions.

6. **SQL Injection Attacks**

Some less mature websites accept user inputs but don’t validate or moderate those inputs. That leaves the networks at risk of SQL injection attacks.

In such attacks, attackers might fill out a support request form, leave a comment, or make an API call. The attacker leverages user input fields to submit malicious code instead of the expected data values. Once this code is executed on the server, the hacker can compromise the network and access sensitive data.

SQL injection attacks are common on poorly designed websites and web applications, especially websites using SQL-based databases.[3][4]

SECURITY MEASURES

1. Firewalls

A firewall can be defined as a device which may be a computer or router acting between the internet and the organization network. Firewall lets only those packets to be transmitted through it into an organization's internal network which fulfils its perimeters configured by the firewall administrator to be a safe data packet and filters the other packets. Firewall acts at network, transport and application layers. Packet –filter firewall acts at network and transport layer and proxy firewall acts on the application layer. Firewall checks the traffic according to the specific rules it has been configured for but there may be chances when the attacker can portray the harmful data to have perimeters which firewall finds safe to be transmitted through it.

2. Antivirus Systems

These systems are used to detect and eradicate malware from our systems. The antivirus system should be kept updated with the latest updates so that it would be easy for it to scan the latest virus signatures. Sometimes an antivirus system is not able to detect the infected file if it is encrypted or zipped.

3. Intrusion detection systems

It is a network monitoring device or software application which keeps track of any malicious actions and policy desecrations and if found it immediately reports about the intrusion to the administrator. They are a set of programs which help detect intrusions and save the system from getting affected. There are two kinds of intrusion detection systems, namely Anomaly Intrusion Detection and Misuse Detection or Signature Based IDS. The Anomaly Intrusion Detection system includes neutral networks and prediction pattern generation, while the Misuse Detection or Signature Based IDS includes state transition tables, pattern matching, genetic algorithms, fuzzy logic, immune systems, and Bayesian method and decision tree [5]. These systems may be Host –based IDS or Network –based IDS.The system matches the traffic with the attack pattern and if match is detected it gives the alarm to the administrator. However, the attacker may be clever enough to change the signature of the malicious traffic which the IDS fail to detect.

CONCLUSION

Globally expanding information networks have become vulnerable to emerging threats and attacks from malicious sources and pose a serious challenge for business and create research gaps for scholars. Researching and developing counter measures is a dire need for the organizations to protect their sensitive data from getting infected from unauthorized sources. Network security has now become an integral part of organization’s confidentiality as it prevents unauthorized users from accessing the network systems, ensures safe transferring of sensitive data and provides a robust system of warning against alarm and fixing issues in case of security breach. This study provides a description of various kinds of threats and attacks on network systems and the common counter measures to mitigate the situation. Further studies can be conducted on organizations mapping the degree of damage they receive as a consequence of becoming victims of such attacks. Case studies on network organizations can also be conducted to understand the grey areas of networking security and aspects which needs to be addressed.

REFRENCES:

1. NETWORK THREATS, ATTACKS AND SECURITY MEASURES: A REVIEW (October 2017)
2. Cyber Security Threats and Predictions: A Survey (Feb – 2023)
3. https://reciprocity.com/blog/most-common-types-of-network-security-attacks/
4. A Review in Recent Development of Network Threats and Security Measures ((January 2021)
5. M. K. Asif, T. A. Khan, T. A. Taj, U. Naeem, and S. Yakoob, "Network Intrusion Detection and its strategic importance Network Intrusion Detection and its Strategic Importance," IEEE Bus. Eng. Ind. Appl. Colloq., pp. 140– 144, 2013.