International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 08 | Aug - 2021 ISSN: 2582-3930

A REVIEW ON NETWORK SECURITY, ATTACKS, TOOLS AND TECHNIQUES

Alva's Institute Of Engineering and Technology, Moodbidre

Department Of Information Science and Engineering

Vedhanth , Nikhil S Acharya , vaibhavi bhat , Pooja p

Abstract: In the last years, we have seen an increase in the use of wireless networks due to new forms of communication. The Internet is expanding with the tremendous speed so as its security. Security is an important field that consists of the provisions made in underlying computer network infrastructure, policies adopted by the network administrator to protect the network. Secure network has become organisation's requirement. The methodology adopted in this paper is a review of papers with keywords network security, network attacks and threats and techniques. The aim of this paper is to critically review the studies on network security, categorising various attacks, threats and techniques that need to be implemented for protection. The paper also describes various concepts related to cryptography and encryption.

Keywords: Network security, Cryptography, Encryption, Network threats and attacks, Techniques.

I. INTRODUCTION

Network security is a challenge for network operators and internet service providers in order to prevent it from the attack of intruders. Network security can be referred as protecting websites domains from various forms of attack. Network Securitymeans considering vulnerabilities, threats, attacks and acceptable risks [1]. Recent advancements in the field of information and technology competitiveness on real time data have led to an increase in the transmission of data and information globally. The sensitive information being transmitted within the network can easily accessed by an unauthorised user for malicious purposes [2].Network security is thus mainly focused on the data networks and on the devices which are used to link to the internet.

confidentiality, to maintain integrity and to ensure availability [1].Network security is the practice of preventing and protecting against unauthorised

Maintaining network security is continuous process that involves comprehensive approaches spanning all phases of design and development. Security problems can be mitigated acceptably by enforcing robust security policies and applying extensive security mechanisms: encryption of data, cryptography. As a result, the information security has become an extremely important aspect in ensuring safe and secured transmission of data through global networks.

II. NETWORK SECURITY

Network security is the process through which we can protect the digital information. It is so crucial for all networks must be protected from threats and the risks. The objectives of network security are to protect the

intrusion into corporate networks. Network security is implemented by the tasks and tools [7].Network security has

become a major component in the organisation structure because the information maintained passes through large number of systems and devices such as computers, routers and becomes vulnerable to threats and attacks [6].

III. TYPES OF ATTACKS

All network face one or more issues, it is the responsibility of the network administrator to keep the network secure for malicious software, worms, threats and from other attacks. An attack is an information security threat through which the intruder attempt to obtain, alter or reveal confidential information without authorised permissions. The networking attacks can be grouped into two major categories namely passive attacks and active attacks [1], [2].

A. 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. Communication decrypts weakly encrypted data and captures information such as passwords. These attacks are hard to detect as there is no loss and alternation of data [6].

B. 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 [2]. 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.

There are other kinds of networks attacks which pose serious threat to the confidentiality of the organisation. Some these attacks are listed below:

Table 1: Attack Type and severity

Attack category	Description	Severity
Attempted-admin	Attempt to obtain administrator privileges	High
Shellcode-detect	Executable code detected	High
Successful-admin	Successfully acquired administrator rights	High
Attempted-dos	Attempt to cause a denial of service	Medium
Attempted-recon	Attempt to cause information disclosure	Medium
Network-scan	Detected network scan	Low
String-detect	Detected suspicious string	Low
Attempted-user	Attempt to obtain user rights	High
Trojan-activity	Detected internet trojan	High
Successful-user	Successfully acquired user rights	High
Misc-attack	Mixed attack	Medium
Suspicious-login	Suspicious user login	Medium
Unknown	Unknown traffic	Low
Icmp-event	General ICMP events	Low

Source: [4]

A. Phishing attacks

These kinds of attackers pretend to be as trustworthy persons with an intension to capture sensitive information through fraud email and message. They often create a fake website such as PayPal and try to trick the users by getting them click on a link and later

on record their personal information including username and password [2],[9].

B. Denial of service(DOS)

It is very hard to prevent the occurrence of DOS attacks because of all the vulnerabilities of Software, hardware and the network. Here users are deprived of access to the network or its resources. DOS are the major threat to the network security in today's scenario because they can be easily launched with some basic knowledge [1].

C. Hijack

This is a kind of an attack in which the hacker intercepts or takes over session between the user and another system and finally disconnects the later from the communication. The user remains under the impression that system is still connected and may send sensitive and confidential information to the hacker by accident [5].

IV.TYPES OF THREATS

Network security is highly threatened by the presence of various threats and attacks that can lead to disclosure of sensitive and confidential information. The basic difference between a threat and an attack is that while threat is a presence of constant danger to the integrity of information, an attack is an actual act of breaching the security of the network.

Table 2: Network 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 confidentiality and integrity.	Implementing dual control principle helps more than one person to control login credentials for organization's servers.
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 protected enough counter such attacks.	Forbidding turning off defences 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	Using encrypting connections which can be connected via Virtual Private Networks and

	capture secured information such as username and passwords of employees without making them aware of any threat to their computer.	encrypts the communication streams preventing eavesdroppers to listen to the data wirelessly.
Data lost on portable device	It is a common problem with 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.	Centralized management of 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.
Reckless web surfing by employees	Various spams, Trojans and viruses penetrate into the organization's network systems when the employees surf websites other than related to their business and end up getting victimized by pool of malware.	Web content filtering such as WatchGuard's Web Blocker which maintains updated URL of blocked websites
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.
Automated exploit of a known vulnerability	Such kind of attacks affect the SMEs who are not able to install Windows patches within the same month their release and later on fall prey to attacks in the form of malicious patches.	1. Investing in patch management which maintains the network up to date by scanning the systems and identifying missing patches and software updates. 2. Building an inexpensive test network which helps the organisation to simulate a patch by installing it into a test system and studying its behaviour.

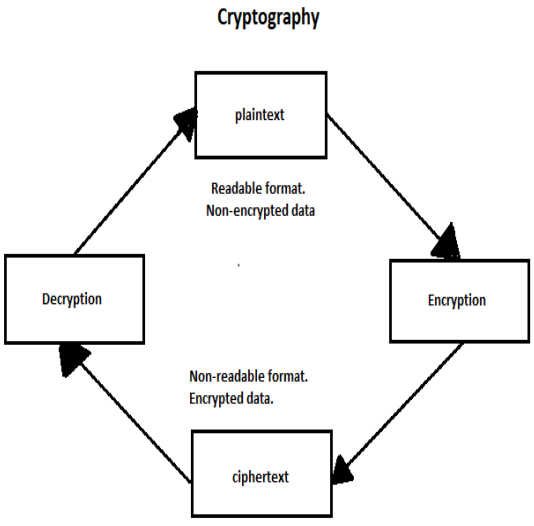
Source: [2], [1]

V. SECURITY TECHNIQUES

A. *Cryptography*

Cryptography is a strategy to store and transmit information in a specific frame so that it can be read and processed by those for whom it is expected. Cryptography is the secret code science of reading. More specifically, protocols that block adversaries are designed and analyse of various aspects in information security such as data privacy, data integrity, encryption and non-repudiation are fundamental to modern cryptography. Encoding message with an unambiguously protected key that is known only through sending and receiver finishing is a remarkable perspective for achieving good sensor organising security.

(fig.1: cryptography process)



B. *Dataencryptionstandard (DES)*

DES was the result of research project set up by international business machines (IBM). DES is based on a cipher known as the Feistel block cipher. It continues for 16 rounds. This algorithm divides plain-text message is received to be encrypted, it is arranges into 64 bit blocks required for input. It is then split into 2 sub blocks each of 32 bit sub blocks. We then combine the result with right and left 32 bit original data to give the final data [8].

C. *Firewalls*

A firewall can be defined as a device which may be a computer or router acting between the internet and the organisation network. Firewall lets only those packets to be transmitted through it into an organisations internal network which fulfils its perimeters configured by the firewall administrator to be a safe data packet and filters the other packets. Packet filter acts at network and transport layer and proxy firewall acts on the application layer. Firewall checks the traffic according to 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 to it [2].

D. *Blowfish*

It is one of the most public domain encryption algorithms designed by Bruce Schneider. Blowfish is the symmetric key block cipher. It uses a 64 bit blocks and variable key length varying from 32 bits to 448 bits. Blowfish has varying ranging having maximum of 16 rounds. Blowfish is a very secure cipher. It is fast and efficient in 32 bit microprocessor. It can be used in compact devices with memory less than 5KB.No attack

is successful against Blowfish, although it suffers from weak key problem [8].

E.Intrusion detection systems

An IDS is a listen only devices or software application thatmonitors network or system activities for malicious activities.Intrusion prevention systems (IPS) extended IDS solutionsby adding the ability to block threats in addiction to detecting them. IDS are placed out-of-band out of network infrastructure that is not a real-time communication path between the receivers of the information [1].There are a set of programs which helps to detect intrusion and save the system from getting affected.

VI. CONCLUSION

The information security turned out to be incredibly important. Information security for the user is a central issue over the internet. Due to fast-moving nature of the information network landscape, and the practicalities of managing systems across large organisation, it must be extremely flexible platforms; able to rapidly deploy new modules, plug in legacy system and integrate new point solutions from a variety of vendors securing the network is just as important as securing the computers and encrypting the message. We have to perform regular network security testing.

Network security has now become an integral part of organisations confidentiality as it prevents unauthorised 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. Globally expanding information networks have become vulnerable to emerging threats and attacks pose a serious challenge for business and research scholars.

This study provides description of various kinds of attacks, threats, tools and techniques on network systems. The paper shows various tools that are used for network security purposes as part of cryptography.

Classification of mystery information from unapproved customers is managed by key management. This paper address easily the concept of network safety, reflects on the risk of network system security. Various Security mechanisms and protocols are available for each of attacks and algorithms are developed for future security threats.

VII. REFERENCES

[1] Harish Singh, “Network Security, a challenge” vol 5, Issue 3, March 2016.

[2] Ruzaina Khan and Mohammad Hasan, “Network threats, attacks and security measures: a review” vol 8, No. 8, Sep: Oct 2017.

[3] Pedro Assuneao, “A zero trust approach to Network Security,” 10.1128/dpsc, 01.01.007.

[4] Weiwei Zhang,”A distributed security situation evaluation model for global network”, ACIT 2018, June 1-3, 2018.

[5]Umesh Kumar and Sapna Gambhir, “A literature review of security threats to wireless networks”, vol 7, No. 4 (2014), PP.25-34.

[6]P.Golchha, R.Deshmukh and P.Lunia, “A review on network security threats and solutions”, vol 3, No. 4, PP.3-5, 2014.

[7] Mohan v.pawar, Anuradha J, “Network security and Types of attacks in network”, ICC-May 2015.

[8] C.Sridevi, “A survey on network security attacks and preventive measures”, vol 12, issue 1, Jan.18.

[9] Amit Kumar and Santhosh Malhotra, “Network security threats and protection models”, CSE-101507.

[10]kjell Hausken and Gregory Levitin,”Review of systems defences and attacks models”, 355-366,2012.

[11]Ms Aswal, Paramjeet Rawat,Tarun Kumar”Threats and vulnerabilities in wireless mesh networks”, 155,2009.

[12]Shio kumar Singh,Mp Singh,Dharmendra K singh,”A survey on network security and attacks

defense mechanism for wireless sensor networks",9-17,2011.