iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VI **Month of publication:** June 2020

DOI: http://doi.org/10.22214/ijraset.2020.6359

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VI June 2020- Available at www.ijraset.com

A Review on Information Security

Sahana B S[1], Neethu S[2]
[1]*B.E Scholar,* [2]*Assistant Professor, Telecommunication Engineering, R.V College of Engineering, Bengaluru, India*

Abstract: Internet has become the integral part of today's generation and network security is one of the important aspects to protect communication. This research paper mainly gives basic knowledge of the information security. Main objective of the research paper is it explains about the different types cyber-attacks that can be taken place and about the E-mail phishing and how firewalls can be used to manage the information security.
Keywords: Phishing attack, Network security, Firewall, E-mail phishing, Information security, Cyber-attack.

I. INTRODUCTION

Information security and network security is one of the important aspects to protect communication. Information Security is the practice of detecting and preventing unauthorized access. Information can be bank account details, debit, credit card secret number. The field of information is seen growing due to the approach of new technologies.

Information Security refers to the processes and methodologies which are designed and implemented to protect personal information, information about the organization, private and confidential information from unauthorized access, eavesdropping, misuse, disclosure, destruction, modification. Information security is information assurance, the act of maintaining the confidentiality, integrity, and availability (CIA) of information, ensuring that information is not compromised by any kind of cyber threats. The objective of this research is to understand the different types of phishing attacks and understanding the basics of firewall for information security. This paper will illustrate the lifecycle of E-mail phishing attack and fundamentals of firewall.

II. THEORY

A. Cyber attack

Upon It is a type of cyber-attack where hacker is trying to obtain the personal details, bank account details, credit card or debit card number. Attacker masquerading as the trusted entity and drops a mail, message, attachment or link, system gets hacked when the victim replies to the message/mail or opens the attachment or link. Phishing attacks also include email spoofing, DNS spoofing, IP address spoofing etc. E-mail spoofing: Email spoofing is the creation of email messages with a forged sender address to obtain the authorized information. It is a common prank which is used to mislead the recipient. Sender pretends as a trusted entity to mislead the recipient. DNS spoofing: DNS stands for Domain Name System. Domain Name System is used to convert IP address into URL and vice versa. DNS spoofing is a type of information security attack in which corrupt DNS data is introduced into the DNS resolver's cache which causes name server to return an incorrect IP address. [13] IP address spoofing: Spoofing attack creates IP packets with false IP address. MAC spoofing: Attacker modifies the MAC (Media Access Control) address of network interface to pose as a valid user on a network

B. E-mail phishing

Phishing is a type of online scam where criminals send an email that appears to be from a legitimate company and ask you to provide sensitive information. This is usually done by including a link that will appear to take you to the company's website to fill in your information – but the website is a clever fake and the information you provide goes straight to the crooks behind the scam. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

III.FUNDAMENTAL OF PHISHING ATTACK AND FIREWALL

A. Lifecycle of E-mail Phishing

An attacker starts with observation on the target. Attacker will create a mail with malicious content, link, or attachment in it. And then mail will be sent to the target. If the mail from that sender was identified as spam, then sender will be blocked by antispam or anti phishing solution. But if it does not identified as spam then the mail along with malicious content will reach the target mail inbox and the target may click on the link or open the attachment and enters his credentials.

©IJRASET: All Rights are Reserved

If the target clicks on the link, traffic will go out to a web site to establish communication. This is when the firewall blocks the traffic as it is not permitted by the firewall. But if firewall fails to block the traffic that malicious web site starts attacking the organization. The malicious web site or the attacker will usually launch exploit attacks at the target to gain access to the system. But the firewall and IPS (Intrusion Prevention System) tries to block the attack, but if it does not: a tunnel is created by the attacker and the malicious site can launch malware into the organization. When malware seeks entry to the system, system must be protected with antivirus or antivirus or other tools in the end point. If it fails, then attacker gets executable code into system where it can run. Once the malicious code starts running in the system, it tries to access credentials, move laterally in search of sensitive data and collect/stage it within the organization. But to complete its mission, it needs to exfiltrate that data out to a command & control server. At this point application control, IP reputation, botnet and other protections come into play. But if these technologies do not block traffic system get breached.

B. Fundamentals of Firewall

Firewall provides security to the network to filter the incoming and outgoing traffic based on the user defined rules and regulation. Firewall separates the trusted and untrusted traffic, or it will separate the internet and home/ business network as shown in the Fig 3.1. Firewall is implemented in network layer or application layer of OSI model. Is useful as it can detect if an unwanted service or application is trying to bypass the firewall using a disallowed protocol on an allowed port or detect if a protocol is being abused in any harmful way.

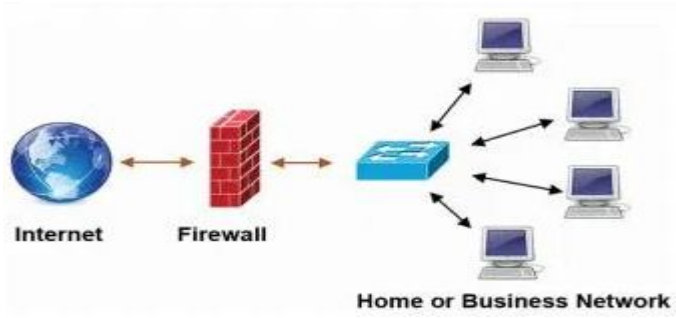


Fig.1 Traditional firewall [5]

Two types of firewall are Network based and Host based firewall. Network based firewall is positioned at the gateway of WAN, LAN etc. It may be a software or hardware firewall. Host based firewall provides end point security, it may be a part of operating system or it is an agent installed at the end point. Firewall blocks unwanted network traffic for the free flow of network communication based on the user defined rule. The word mentioned in the rules defines what action must be taken by the firewall, for example to 'accept', 'drop' or 'reject' the traffic. **Accept** means to allow the traffic through, **reject** means to block the traffic but reply with an "unreachable" error, and **drop** means to block the traffic and send no reply. The remaining content in the rule consists of the condition that each packet is matched against.[14]

IV. RELATED WORK

Russell Couturier[1], explains the phishing attacks and preventing techniques. Researcher has monitored a total of 19,066 phishing attacks over a period of ten months and found that over 90% of these attacks were replicas or variations of other attacks in the database. The drawbacks of the tools that are present

Mikey Veenstra [2] explains about top tools which are used in cyber security to detect the threats, vulnerabilities, and other types of cyber-attacks. Explains information gathering and analysis, testing, malware analysis and explains how the attacks are resolved using new tools and using present technologies like AI and machine learning.

Martin Brinkmann [3] gives brief description about the Hybrid analysis tool. Hybrid Analysis by Payload Security is a free malware analysis service that runs files that is upload to it in a virtual sandbox environment. Working of the tool, advantages, and steps to be followed while analyzing the email in the tool are explained.

Shrushti Patil and Sudhir Dhage [4] introduced and studied on phishing is a security attack to acquire personal information like passwords, credit card details or other account details of a user by means of websites or emails. Presents a focused literature survey of methods available to detect phishing websites. Step wise procedure of designing an anti-phishing model is discussed to construct a framework.

©IJRASET: All Rights are Reserved

Andreea Bendovschi[6] displayed technology is rapidly evolving in a world by automated processes, online transaction, social network, and cloud computing. But the evolution in the technology leads to the cybercrimes, different types of cyberattacks. Different tools allow the attackers to penetrate more co plex environment and increases the damage to the network. Different types of attacks, impact of the attacks, different types of security countermeasures which can be taken internally and externally such as continuous risk assessment, authentication, using security controls are explained.

Mohammad Imran, Abdulrahman, Bihal Ahmad [7] explained firewall is used to protect the network or computer and confidential information. There are different types of attack such as Trojan attack, unpatched software, phishing attacks, and network worms. Qualities of the good firewall are explained. There are two policies for firewall to work i.e. deny policy and allow policy. There are about 5 types of different firewall. Each firewall has their own policy and new features in it.

Muhammad Baykara and Zahit Ziya [8] explained phishing is a type of crime where attackers imitate a person or institution or entity through email or other communication medium. The attacker sends either link or attachment in the mail or there may be any threats in the mail. Information that usually be stolen from the phishing attacks are account number, username, password, other credit card information. Classification technique can be used. To estimate the result the classification algorithm works on set of qualification or training set with relevant result. Algorithm tries to find the result. Based on this classification all the common spam messages and phishing attacks are detected and it can be blocked before it enters the network.

Glenn Surman [5] displayed OSI (Open Source Interconnection) model breakdown and different IT (Information Technology) vulnerabilities are explained**.** Vulnerabilities that takes in each layer of OSI model is explained with solution to the problem area. In every layer of OSI there may be a attack due to poor defence. Defending the system is ongoing process. Prevention should be taken considering the new cyber-attacks. Dividing the risk into more manageable components gives us a better chance at addressing vulnerabilities and protects the assets.

Aarushi Madan, Aarushi Tuteja and Bharti [9] Proposed that is important to understand the structure and function of network before looking into the attacks in each layer. There are 7 layers in the Open System Interconnection model. Application, presentation, session, transport, network, data link layer and physical layer has its own function. The main benefits of the OSI model are, it helps user to understand the network picture, gives the idea of how hardware and software is interrelated, it converts the complex network into simple modules. Physical layer includes the components such as wiring system components, hub, repeater, cable less systems etc. Data link layer includes Network Interface Card (NIC), ethernet and switches. This link layer is responsible to exchange data. Transport layer performs end to end communication. Session layer develops the connection between transport layer and presentation layer. Transport layer is responsible for synchronizing data, connecting different parameter. Presentation layer deals with format of incoming messages. Application layer provides interface between the user and presentation layer. Application layer directly links to different applications such as e-mail or web browsers.

v. CONCLUSION AND FUTURE SCOPE

E-mail is the most important communication method in organizations. Increase in the use of service has also caused more traffic congestion, receiving more spamming mails, phishing attack etc. which may decreases the productivity and may also leak the companies information. Due to the increase in cyber attcks different methods of protection are developed. Examined the essential of firewall and different kinds of attacks that occurs in the organisation. Firewalls acts as a powerful protective. mechanism and it plays an important role in securing the network. The future scope of the work involve do analysis on new technologies to provide more flexible and powerful protection for the network in the organisation and make more secure to protect it from different kinds of cyber-attacks.

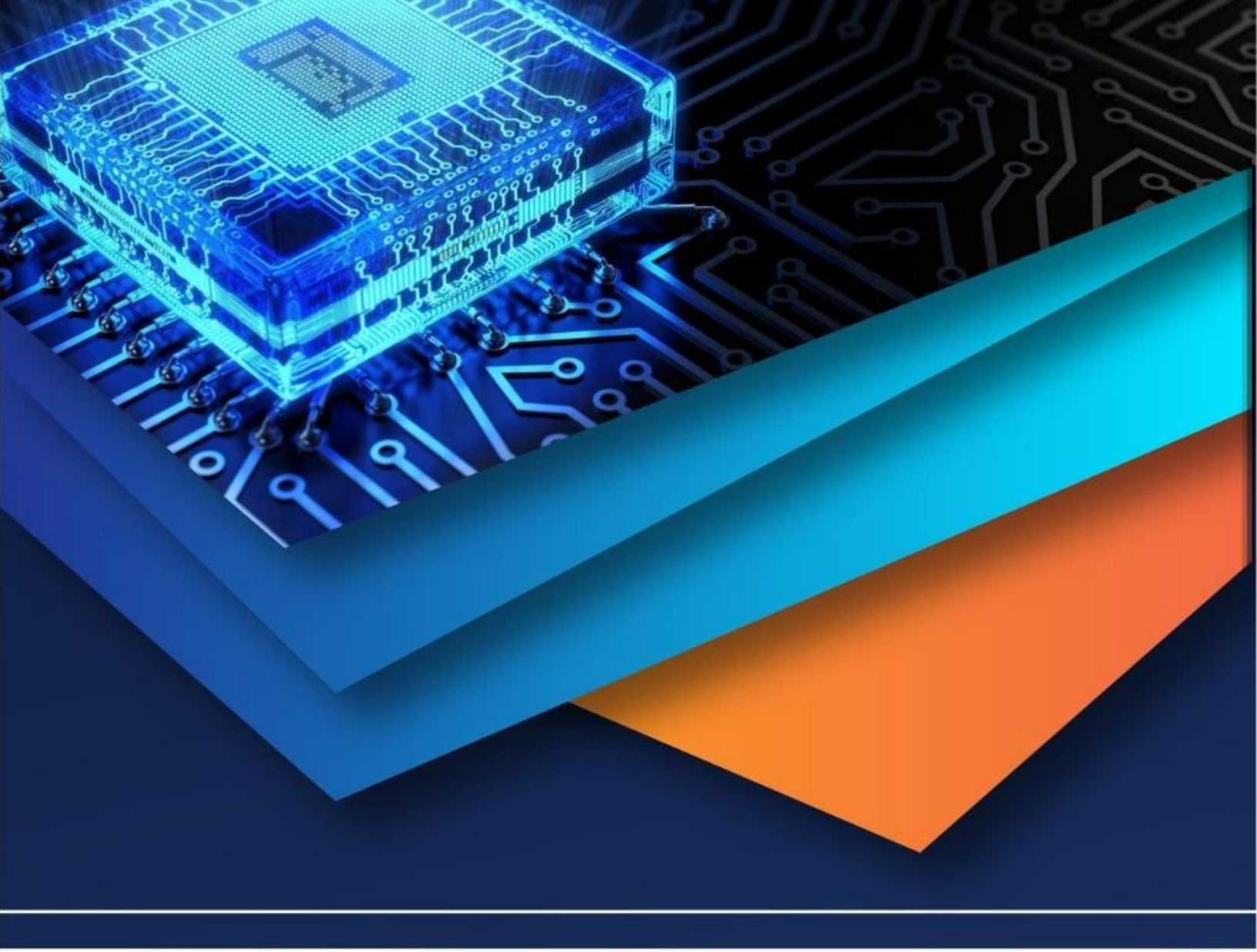
REFERENCES

[1] Russell Couturier, “Tracking of phishing attacks”, International World Web Conference WWW, April 3-7, 2017.
[2] Mikey Veenstra, “General security, research, Word press security”, 2018
[3] Martin Brinkmann, “Hybrid Analysis: analyze Windows files in a browser sandbox”, Ghacks Technology News Back May 11,
[4] Shrushti Patil and Sudhir Dhage,” A Methodical Overview on Phishing Detection along with an Organized Way to Construct an Anti-Phishing Framework “, IEEE 5th International Conference on Advanced computing and communication system, March 2019
[5] Glenn Surman, “Understanding Security Using OSI Model”, SANS Institute-Information Security Reading Room, 2002, last updated in 2020.
[6] Andreea Bendovschi.”, Cyber-Attacks – Trends, Patterns and Security Countermeasures’, Research gate publication, December 2015.
[7] Mohammad Imran, Abdulrahman, Bihal Ahmad,” Role of Firewall Technology in Network Security, Internal journal of Innovation & Advancement in Computer Science.
[8] Muhammad Baykara and Zahit Ziya,” Detection of Phishing Attacks”, IEEE publication, 2018Glenn Surman, “Understanding Security Using OSI Model”, SANS Institute-Information Security Reading Room, 2002, last updated in 2020.

©IJRASET: All Rights are Reserved

[9] Aarushi Madan, Aarushi Tuteja and Bharti," OSI Reference Model", International Journal of Advanced Research in Computer Science and Software Engineering 2014.
[10] Shailaja Pandey." Modern Network Security- Issues and Challenges", International Journal of Engineering Science and Technology, 2018.
[11] Monali S. Gaigole and M.A Kalankar," The Study of Network Security with its Penetrating Attacks and Possible Security Mechanisms", International Journal pf Computer Science and Mobile Computing, May 2015.
[12] Ramesh Babu, Lalitha Bhaskari and CH Satyanarayana," A Comprehensive Analysis of Spoofing", International Journal of Advanced Computer Science and Application, December 2010.
[13] Ammar, Samer Atawneh, A. Meulenberg and Eman Almomani," A Survey of Phishing Email Filtering Techniques", IEEE publication.
[14] S.C Tharaka, R.L.C. Silva, S. Sharmila, "High Security Firewall: Prevent Unauthorised Access Using Firewall Technologies", International Journal of Science and Research Publication, April 2016.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)