Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 5, May 2017, pg.61 – 63

Threats and Security Issues in TCP/IP Layers: A Review

Komal
Assistant Professor, Department of CSE, Amity University Haryana, India
komal.sang@gmail.com

Abstract— Network security has become the most crucial aspect of network design and implementation with the TCP/IP model and protocol suite being used worldwide. However, security attacks are increasing many folds on Networks with every passing day. In order to prevent the possible attacks on our networks (public/private/restricted), it is essentially required to understand the architecture of TCP/IP model, functionality of its layers and security loopholes within these layers. Hackers and black hat community are acquiring enormous skills to understand the intricacies of computer communications and ways to exploit vulnerabilities. The widespread use and keenness to various security compromising tools and open network policies and usage has generated an increased need for network security and dynamic security policies. This paper explores the attacks on the layers of TCP/IP protocol suite and suggests mitigation measures for such attacks.

Keywords— TCP/IP, Network, Hacker, Security Policy, Attacks, Protocol.

I. INTRODUCTION

The Transmission Control Protocol/ Internet Protocol (TCP/IP) suite is a stack of protocols used together for communication over Internet. The internet has become part and parcel of everybody's life and it has expanded enormously in past few years, thereby, connecting large number of communities and organizations all over the world. It has become a obligation for all the internet users including individuals, government agencies, private organizations and corporate to enhance security for their data and network so as to assist their day to day transactions. With the rapid growth, the security measures that have been put in place lack some features that are required to provide maximum security over insecure networks [1]. Many Networks are exploited by hackers with specialized tools such as sniffers to capture sensitive information that is sent across these networks [2].

Besides all the security tools available in market and all security techniques being used including authentication, authorization and encryption, the security issues still persist. Recently, much attention has been shifted to the aspects of network security at application level instead of adequate attention to the basic security loopholes and vulnerabilities in the basic network implementation and configuration. Researchers are focusing on data mining [3] and decision tree algorithm [4] for data processing and analysis. Attackers are still developing new ways of using these loopholes to gain access to Networks and data. Thus, the objective of this paper is to spread awareness among internet community and to sensitize network administrators about detailed and specific security attacks and their preventative security policies. This research paper describes a variety of basic flaws in

TCP/IP protocols and their implementations. It also suggests preventative mechanisms to help resolve these problems.

II. ROLE OF TCP/IP LAYERS

TCP/IP protocol suite represents the set of protocols used at the various layers of Internet architecture. Following four layers play a significant role in transmitting information from one host/device to another over internet:

A. *Application Layer*- Application layer is also known as 'User Interaction layer' as it is the entry point of data originating from a user/ device/ application software. It is also responsible for encryption and presentation of information/data in various formats.

B. *Transport Layer*- Transport layer is responsible for delivery of information between two specific processes/ applications running on same or different devices. Some applications need reliable delivery while others requirement is fast delivery. Transport layer fulfils both requirements using TCP and UDP protocols.

C. *Internet Layer*- Internet layer is the actual connecting backbone of internet infrastructure that enables transmission of data between different networks using IP addressing and various routing protocols.

D. *Network Interface Layer*- This layer is responsible for placing and retrieving information in the form of frames on physical transmission media. It also delivers data to individual hosts on a network.

III. ASSESSMENT OF ATTACKS & CORRESPONDING SECURITY MEASURES

Major network security attacks are broadly classified into two categories- Active attacks and Passive attacks. The purpose of active attacks is to disrupt the integrity of communication stream and/or to disseminate falsified information to the targeted group. However, passive attacks aim to sneak through the communication stream to fetch confidential and private data without the awareness of network users such as eavesdropping and traffic analysis. Such attacks are difficult to detect and may cause serious repercussions. The table provided below details about the more specific security attacks at different TCP/IP layers.

TABLE I
CATEGORIZATION OF ATTACKS & SECURITY MEASURE

TCP/IP layer	**Security Threats & Mitigation Measures**			
	Types of attacks [7][9]	**Vulnerable Protocol [9]**	**Consequences of attacks**	**Security measures for preventing such attacks [8]**
Application Layer [5]	• Man in the Middle attack • DNS Cache Poisoning • Denial-of-Service attack	Domain Name System (DNS)	➢ Illegitimate information processing. ➢ Unreachable network/web resources.	1. Use of Digital Certificates. 2. Proper Encryption techniques. 3. Service request timestamp and attempt restriction.
	• Malware • SQL Injections • Distributed Denial-of-Service attack	Hypertext Transfer Protocol (HTTP)	➢ System files corrupted. ➢ Dynamic script languages compromised (ASP, PHP, JSP, and CGI) ➢ Hosts unknowingly attack on targeted system.	1. Security tools/patches/ Scripts embedded with web browser. 2. Intrusion Detection System/ tool such as Snort can be used to identify SQL injection. 3. Penetration testing[6]
	• Email Spoofing • Shellshock attack • Smurf attack • Email Spamming • Worms	Simple Mail Transfer Protocol (SMTP)/ IMAP	➢ Mistrust issues and innocent victims. ➢ Frustrated User. ➢ System files affected/encrypted.	1. Use of Anti-spam softwares. 2. Updated Anti-virus applications. 3. Use of Access Control Lists (ACLs).

	• Brute Force attack • Bounce attack	File Transfer Protocol (FTP)	➢ Unauthorized access to personal PINs, passwords, ports.	1. Use of Access Control Lists (ACLs). 2. Blocking port scanning in network.
Transport Layer	• Port Scan/ Port sweeps • TCP Hijacking • SYN flood attack	Transmission Control Protocol (TCP)	➢ Session monitoring ➢ Session privacy compromised. ➢ Session unwanted termination.	1. No open ports. 2. Session security using keys and authorized information.
Internet Layer	• IP Spoofing • Routing loop attack • Route Poisoning • Neighbour Discovery Message Attack	Internet Protocol Version 4 /Version 6 Routing Protocols	➢ Internet threats of all kinds. ➢ Non-delivery of routing packets. ➢ Malware host auto-configuration.	1. Using Strict ACL and firewall rules. 2. Using NAT (Network Address Translation)/PAT (Port Address Translation) 3. Enabling Routing protocol authentication.
Network Interface Layer	• ARP Poisoning • MAC address spoofing	Address Resolution Protocol (ARP)	➢ Promotes other attacks in network. ➢ Dodge firewalls and proxies.	1. Restricted Access 2. Switchport port-security feature.

IV. CONCLUSIONS

Network and data security has become the paramount concern of all organizations and individuals working on Internet every day. In Internet Threat Security Report 2016 by Symantec, thousands of new security vulnerabilities have been discovered. Therefore, the need of the hour is to have Security Policies that are revised from time to time to identify the weakness in the security architecture with the help of various security tools like firewalls, packet analyzers and vulnerability scanning tools. Users of applications, network infrastructure, and various software/hardware platforms should be educated well about the flaws and security capabilities. Stricter cyber laws and government policies should be formed to penalize the intruders and attackers earnestly. Moreover, multi-layer and multi-protocol security architecture needs to be implemented.

References

[1] Saleh Almanei, Mohammed Alqattan, Rabha Kamis, Yousaf Hussein, "TCP/IP Protocols possible attacks,"Computer and Network Security Spring Term 2000.

[2] (2010) Computer Networking Notes website. [Online]. Available: http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/types-of-attack.html.

[3] Rashi Chauhan, Sarika Chaudhary, and Pooja Batra, "An Efficient Approach for Test Suite Reduction using Density based Clustering Technique," International Journal of Computer Applications, vol. 97, Issue 11, July 2014.

[4] Sanjay Malik, and Sarika Chaudhary, "Comparative Study Of Decision Tree Algorithms For Data Analysis," International Journal of Research in Computer Engineering & Electronics, vol. 2, Issue 3,pp. 1-8, June 2013.

[5] Ajay Sharma, and Poonam Sharma, "Hiding/Disabling Applications based on Secure Zones," International Journal of Advanced Foundation and Research in Computer, vol. 2, Issue 5, pp.121-126, May 2015.

[6] Shivangi Kaushal, and Jagpuneet Kaur Bajwa, "Analytical Review of User Perceived Testing Techniques," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, issue 10, pp. 213-216, 2012.

[7] Komal, "Compromised Security of Wireless Ad-Hoc Networks & its Implications," International Journal of Computer Applications, IJCA Proceedings on Innovations in Computing and Information Technology (Cognition 2015), COGNITION 2015 - Number 2, pp. 25-30, 2015.

[8] (2005) Network Security Policy: Best Practices White Paper, Cisco website [Online], Available: http://www.cisco.com/c/en/us/support/docs/availability/high-availability/13601-secpol.html.

[9] B. Harris, and R. Hunt , "TCP/IP security threats and attack methods," Computer Communications, Vol. 22, Issue 10, pp. 885–897 June 1999.

