DOCTORAL PROGRAM IN ENGINEERING SCIENCES AT ITESO

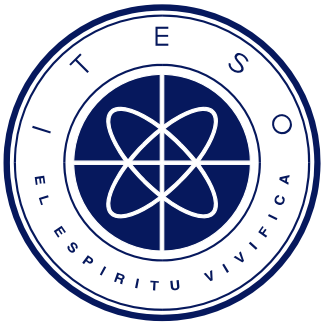
CHALLENGES AND OPPORTUNITIES IN COMPUTER NETWORK SECURITY

Alvaro I. Parres-Peredo, Hugo I. Piza-Davila, and Francisco Cervantes-Alvarez

PhDEngScITESO-15-20-R.docx

December 10, 2015
Tlaquepaque, Mexico 45604

Doctoral Program in Engineering Sciences
ITESO (*Instituto Tecnológico y de Estudios Superiores de Occidente*)



© Alvaro I. Parres-Peredo, Hugo I. Piza-Davila, and Francisco Cervantes-Alvarez 2015

No part of this document may be copied, translated, transcribed or entered in any form into any machine without written permission. Address inquires in this regard to the authors or to the Chair of the Doctoral Program in Engineering Sciences at ITESO (dci@iteso.mx). Excerpts may be quoted for scholarly purposes with full acknowledgment of source. This document may not be lent or circulated without this cover page.

CHALLENGES AND OPPORTUNITIES IN COMPUTER NETWORK SECURITY

Alvaro I. Parres-Peredo, Hugo I. Piza-Davila, and Francisco Cervantes-Alvarez

December 10, 2015

Doctoral Program in Engineering Sciences
ITESO (*Instituto Tecnológico y de Estudios Superiores de Occidente*)

Tlaquepaque, Mexico 45604
Tel +52 33 3669 3598
E-mail: dci@iteso.mx

Keywords *Computer Network, Network Security, Computer Security, IDS,*

Abstract

In 1980, Anderson made a first approach to a new layer on information security, the intrusion detection layer. Since then, there have been many research works around security mechanisms for intrusion detection. Most of these works focus on border security, which consists in detecting outside intruders and remote attacks. Nevertheless, many security threats occur from inside the network. This report presents two challenges on computer network security regarding to detection of internal attacks: identifying abnormal behaviors of privileged users and profiling "script kiddies". In addition, it describes the types of network attacks as well as the approaches that have been followed to implement intrusion detection systems.

I. INTRODUCTION

The Internet has been growing up very fast and is being used as a global communication way. Nowadays, many kinds of information are travelling on the Internet: from simple emails to huge money transfers. This makes the computer network security more important and critical than ever.

New types of attacks against information systems appear day after day; these attacks are becoming more complex and less technical skills are required to perform them [1].

The term computer security is defined by the NIST [2] as follows: the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (including hardware,

This work was supported in part by ITESO's Program for Academic Level Enhancement *(Programa de Superación de Nivel Académico, PSNA)* through an assistantship granted to A. I. Parres-Peredo.

software, firmware, information/data and telecommunications).

Migga [3] defines computer security as a branch of computer science that focuses on creating secure environments for the use of computers. It focuses on the behavior of computers and related technologies users, as well as on the protocols required to create a secure environment for anyone. When we talk about computer network security, the secure environment involves all network resources: computer, data, devices and users.

Traditional authors like Stalling [4] defines three types of network: Local Area Network, Metropolitan Area Networks and Wide Area Networks; based on the geographical scope of the network. Modern authors like Edwards Wade [5] defines new types of network like the Campus Area Network(CAN), which is defined as a group of LAN Segments interconnected within a building or group of buildings that form one network. Typically, the company owns the entire network, including the wiring between buildings, in contrast to Metropolitan Area Networks.

We focus this report on CAN because these networks present a considerably large number of nodes and users in a same common network.

The present document is organized as follows. Section II classifies the computer network attacks. Section III introduces the intrusion detection systems as a new layer of security mechanism. Section IV presents some challenges in computer security networks, specifically on internal network security. Finally, Section V concludes the report.

II. COMPUTER NETWORK ATTACKS

Computer networks attacks can be classified according to different criteria; for instance, based on their objectives, types of target, or the way they are executed.

Stallings [6] classifies security attacks into two big categories: passive attacks and active attacks. A passive attack attempts to learn or make use of information from the system but does not affect system resources. An active attack attempts to alter system resources or affect their operations.

Kandall [7] proposes a classification which is widely used in research works. He defined the following classes:

a) Denial of Service (DOS): is an attack in which the attacker makes some computing or memory resource too busy or too full to handle legitimate requests, or denies legitimate users access to a machine.

b) User to Root: is a type of "exploit" program in which the attacker starts out with access to a normal user account on the system and is able to exploit some vulnerability in order to gain root access to the system.
c) Remote to User: occurs when an attacker with the ability to send packets to a machine over a network but not having an account on that machine, exploits some vulnerability to gain local access as a user of that machine.
d) Probe: refers to a program that can automatically scan a network of computers to gather information or to find known vulnerabilities.

On the other hand, Heerden [8] provides other taxonomy of network attacks that he calls attack scenarios, and includes the following: denial of service, industrial espionage, web deface, spear phishing, password harvesting, snooping for secrets, financial theft, amassing computer resources, industrial sabotage and cyber warfare.

III. DETECTING COMPUTER NETWORK ATTACKS

On current computer networks, the traditional security methods including only firewalls and access control systems are no longer enough to protect computer systems; day after day, intruders find new ways to attack computers and systems. This motivated the rise of a new layer of security called: Intrusion Detection System (IDS). The first approach of an IDS was proposed by Anderson [9] in 1980. An IDS intends to identify intruders (or attackers) by monitoring and analyzing the events on systems, computers or networks. Fig. 1 shows the security methods on a simple computer network diagram.

Currently, there are two types of IDS: 1) signature-based and 2) anomalies-based. The signature-based ones are very efficient on detecting known attacks but inefficient on detecting new ways to execute attacks. Those based on anomalies classify as "bad traffic" or "intruder" everything that falls out a given definition of normal traffic. These IDS have the following properties: high rates of false positives and high efficiency on detecting new types of attacks. Because of the second property, anomalies-based IDS are considered as one of the foremost research areas in network security [10].

Many research works have been developed around the classification of network traffic using different machine-learning techniques, with the aim of achieving 100% of intrusion detections and a low rate of false positives. Two classes of machine learning techniques are used:

single and hybrid classifiers. Single machine-learning classifiers include: support vector machines, self-organizing maps, neural networks and k-nearest neighbors. Hybrid machine-learning classifiers have the purpose of acquiring a superior probable accuracy for intrusion detection; these classifiers combine many machine-learning techniques to improve their performance [10].

Most of network traffic-classification research uses KDD CUP 99 as the dataset for testing their proposals. This dataset was developed by Kristopher Kandall with the aim of assessing intrusion detection systems [7].

IV. CHALLENGES IN COMPUTER NETWORK SECURITY

In order to visualize the opportunity areas on computer network security, we distinguish border security from internal security. The former focuses on protecting network components from external attacks, i.e., those from outside networks. The latter focuses on protecting devices from attacks performed from another device on the same network.

Most of computer network research has focused on border security, more specifically, on detecting denial of service attacks or unprivileged access, by analyzing the network traffic. However, there are currently many issues and threats on internal security not yet been studied by current research. We identify two types of such threats as follows: 1) privileged users at networks and 2) script kiddies at campus area networks.

A. Privileged Users at Networks

The 2015 annual CISCO Security report [11] identifies as a key discovery that both users and their equipment have become unwitting parts of security problems. Some examples that CISCO gives about this are:

a) Online criminals rely on users to install malware or help exploit security gaps.
b) Malware creators are using web browser add-ons as a medium for distributing malware and unwanted applications. This approach to malware distribution has proved to be successful for a malicious actor because many users inherently trust add-ons or simply view them as benign.
c) User's careless behavior when using the Internet, combined with targeted campaigns by adversaries, place many industry verticals at higher risk of web malware exposure.

One vulnerable element for a system is a user that has rights over it. One challenge of

computer network security is to prevent privileged users from being accomplices of attackers that employs users' computers to gain access to information systems and/or network services.

B. Script Kiddies at Campus Area Network

Nowadays, there exists many tools, software applications, and scripts capable to perform penetration testing on information systems and computer networks, with the sole intention of attacking them. Kali Linux[1], a Linux distribution, includes over 600 pre-configured penetration-testing tools, which can be treated as penetration test tools, or forms of attack.

We define script kiddie as a user that thinks of himself as a hacker but has very low technical skills. He/she does not write his/her own code; instead, he/she runs scripts written by more skilled attackers [1].

Script kiddies inside a considerably large network, such as a CAN, represent a serious security risk; their own amateurism, poor knowledge about what they are doing, and few technical skills might result in the following scenarios:

a) They might open a backdoor for a professional attacker. Because of the download and execution of programs and scripts that comes from unknown sources, the script kiddie can download a malware that can generate a back door.
b) The incorrect execution of some types of attacks, like man in the middle, can provoke a downtime on the network for an unknown period of time that also generates a lower service level.
c) On public networks, like coffee shop's hotspot, the presence of script kiddies can generate an uncomfortable experience to regular network users.

The challenge of computer network security is to identify *script-kiddie* behaviors in the computer network of an organization, such that the corresponding risk can be prevented.

V. CONCLUSIONS

In this report, we presented how the computer network security is becoming more important and critical for organizations, because of the high value of the information that travels across the network, and the costs of IT systems downtime.

The computer network attacks are been studied for a long time and new technologies for

[1] Debian based Linux Distribution for Penetration Testing. http://www.kali.org

preventing them are being developed. Most research works focus on designing or improving intrusion detection systems in order to detect more kind of attacks than a simple firewall, or access control system.

The intrusion detections systems have been employed also to detect new patterns of attacks using machine-learning algorithms, each time more efficient and precise. Most of these systems work at the border of the network or at some specific points, regularly, between the datacenter and the network. Since many attacks come from inside the organization network, we have identified opportunities for improving network security by profiling end-users according to their normal network behavior and monitoring their devices.

REFERENCES

[1] C. Paquet, *Authorized Self-Study Guide Implementing Cisco IOS Network Security (IINS)*. Indianapolsis: Cisco Press, 2009.

[2] B. Guttman and E. A. Roback, *An Introduction to Computer Security: the NIST Handbook*. DIANE Publishing, 1995.

[3] J. M. Kizza, *Guide to Computer Network Security*, Second edition. London ; New York: Springer, 2013.

[4] W. Stallings, *Data and Computer Communications*, International Ed. Pearson Education Limited, 2015.

[5] W. Edwards, T. Jack, T. Lammle, T. Skandier, R. Padjen, A. Pfund, and C. Timm, *CCNP Complete Study Guide: Exams 642-801, 642-811, 642-821, 642-831*. John Wiley & Sons, 2006.

[6] W. Stallings, *Cryptography and network security: principles and practice*, Seventh edition. Boston: Pearson, 2014.

[7] K. Kandall, *A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems*, B.S. and M.Sc. Thesis, Dept. of Electrical Eng. and Computer Science, MIT, Boston, MA, USA, 1999.

[8] R. van Heerden, L. Leenen, and B. Irwin, "Automated classification of computer network attacks," in *2013 International Conference on Adaptive Science and Technology (ICAST)*, Pretoria, Nov. 2013, pp. 1–7.

[9] J. P. Anderson, "Computer security threat monitoring and surveillance," NIST, Report Contract 79F296400, Fort Washington, PA, 1980.

[10] S. Juma, Z. Muda, M. A. Mohamed, and W. Yassin, "Machine learning techniques for intrusion detection system: a review," *J. Theor. Appl. Inf. Technol.*, vol. 72, no. 3, pp. 422–429, Feb. 2015.

[11] CISCO, *2015 Annual Security Report*, San Jose, CA, 2015.

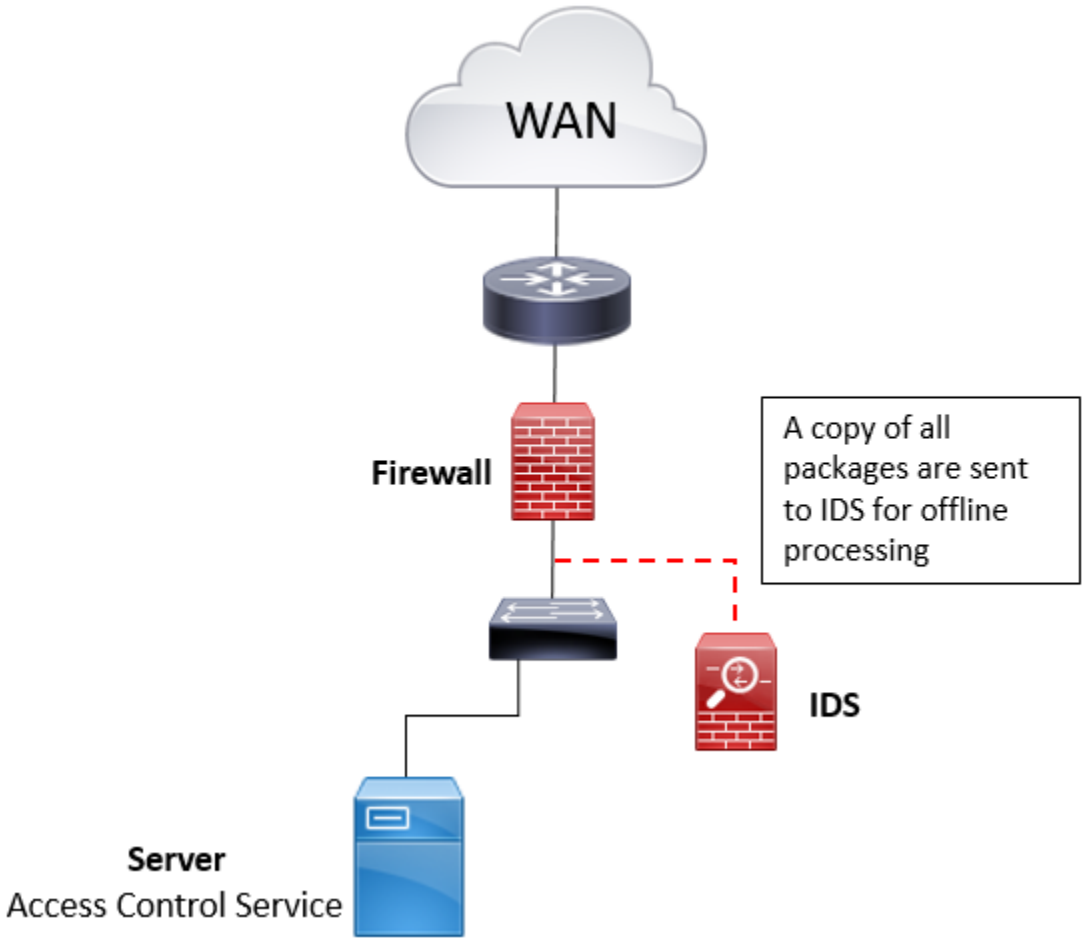


Fig. 1. Simple network diagram with a Firewall and IDS.

APPENDIX OF FILES USED

Filename	Author	Short Description