Scientific Journal Impact Factor (SJIF): 5.278
International Journal of Modern Trends in Engineering and Research
IJMTER
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

A CASE STUDY ON VARIOUS NETWORK SECURITY TOOLS

Rajatha[1] and Chaitra Acharya[2]
[1,2]*Department of Information Science, SCEM*

Abstract—Advancements in technology have facilitated the growth of different cyber attacks. The number of hackers is increasing exponentially. By 2019, cyber crime costs may reach up to $2.1 trillion. Security is a very important aspect for computers to have in today's world. Therefore it is very important to provide Network Security to safeguard the availability, confidentiality, and integrity of the data irrespective of our business. Network security addresses a wide range of threats and the associated attacks. In this paper, we analyze how network security works and a brief overview of the various tools that are required to detect and handle the attacks generated from the various threats.

Keywords — Network Security, Wireshark, Nessus, Snort, John the Ripper, NetStumbler.

I. INTRODUCTION

Network Security is a set of activities designed to protect our network. It consists of the policies and procedures designed to prevent and protect systems from various active and passive attacks like unauthorized access, modification, misuse, eavesdropping, phishing, spoofing, malware and other such attacks. Network security has the following basic characteristics:

1. Data Integrity: It assures that the information cannot be modified by unauthorized entities.
2. Data Confidentiality: It assures that the private and confidential information is not disclosed to unauthorized entities.
3. Data Availability: It assures the timely and reliable access of data to the authorized users [2].

Network Security begins with authentication of users with username and password. Since it deals with one user, it is also termed as One-factor authentication. Two-factor authentication has user entering password along with extra security factor like an OTP or a pin. Similarly three-factor authentication has an extra security feature like biometric verification along with the security features of two-factor authentication. Once authentication is done, intruders are detected and prevented through firewalls and intrusion detection and prevention systems like honeypots and honeynets.

Networks are often attacked by malicious sources. The attacks are of two basic types: active and passive. While passive attacks include snooping, eavesdropping, scanning and traffic analysis; the active attacks include much more. The most popular and common attacks are DOS(Denial-of-Service),Man-in-the-middle,spoofing,phishing,malware and much more [1]. To prevent these attacks we need network security tools which safeguard our systems and thereby prevent loss or modification of data. Network security tools include packet sniffers, port scanners, vulnerability scanners, brute-force password crackers, debugging and exploration tools, WEP and WPA crackers and network intrusion detectors.

II. TYPES OF NETWORK SECURITY TOOLS

2.1. Vulnerability scanners

A Vulnerability scanner is a computer program designed to scan computer systems, networks and applications for highly detailed information in order to determine security holes and weaknesses.

It identifies and detects the vulnerabilities that reside on network-based assets like firewalls, routers, servers and so on. There are various types of vulnerability scanners like port scanners, network vulnerability scanners, host based vulnerability scanners, database security scanners, web-application security scanners, ERP security scanners and single vulnerability tests [1]. The most popular vulnerability scanner tool is Nessus developed by Tenable Network Security. It is open-source software available for personal use. It allows for scanning of the following vulnerabilities such as misconfiguration, DOS, security holes, invalid mangled packets.

2.2. Packet Sniffers

A packet sniffer also called as network protocol analyzer, is a network tool that intercepts packets from the network and analyzes them. It provides the necessary information to the network technicians to diagnose and solve network- related issues [3]. Contrarily, it can also be used by the hackers to eavesdrop on the network activities or to analyze the pattern of the packets to decode the passwords. Packet sniffers intercept and logs into network traffic to keep tab on the activities through wired or wireless network interfaces. [1] As the data stream flows through the network, sniffers captures each of these packets to decode and analyze it and further presents it in the human readable format to facilitate the person using packet sniffing to view and understand the details.

Packet sniffers are available in both commercial and open-source forms. The popular commercial sniffers are: Sniffers and packet analyzers. Sniffer is a commercial tool used to monitors the data travelling over the network. Packet analyzer, holds an essential part in Network management toolkit, is a tool to trace and capture files, and then decodes them into the component parts. Open source sniffers include Wireshark and Snort.

2.3. Password crackers

Password crackers also known as password hackers are the tools used to identify the unknown or the forgotten password. It also helps the human hackers to obtain the forbidden and unauthorized access to the resources. [1] Password crackers use two methods to crack the passwords: brute force and dictionary searches. Brute force cracking is a technique in which the hacker runs through the various combinations of password and passphrases, until the correct ones are found. Whereas, in dictionary search, the hacker searches each words in the dictionary entries to find the correct password.

Most popularly known password cracker is John the ripper.

2.4. Honeypots

Honeypots belong to the class of powerful security tools designed to lure attackers and to trap and divert them away from the potential critical systems. They are also known as decoys, lures and flytraps [1]. Honeypot systems do the following activities:

a) Divert attackers from the critical systems.

b) og the activities of attackers and alert administrators to respond to the attacks.

A collection of honeypots on a network is referred to as a Honeynet.

Honeypots can be classified as:

a) Pure Honeypots- use bug tap to monitor attacker activity.
b) High-interaction Honeypots- imitates the system services making attacker waste his time.
c) Low-interaction Honeypots- imitates only the services requested by the attacker.

2.5. Wireless Security tools

Wireless networks are at higher risk of attack as compared to wired networks [5]. So wireless network security is more challenging than wired network security. A wireless security tool should be capable of sniffing traffic, scan wireless hosts and check the level of privacy and confidentiality provided on the network. Some of the popular wireless security tools are Aircrack, NetStumbler, Kismet and inSSIDer.

III. POPULAR NETWORK SECURITY TOOLS

Network security tools play an important role in cyber security. The top 5 security tools currently in the market are given below:

3.1. Wireshark

Wireshark also known as ethereal is the most widely used network protocol analyzer or a packet sniffer.[4] It is similar to tcpdump and has additional graphical user interface with sorting and filtering options. It contains the following features:

a) Analyzes both captured data packets and packets being transmitted over the network.
b) Supports data reading and analysis for various range of networks.
c) A graphical user interface which makes it easier for the user to differentiate the packets.
d) An organized data display of the captured filtered packets.

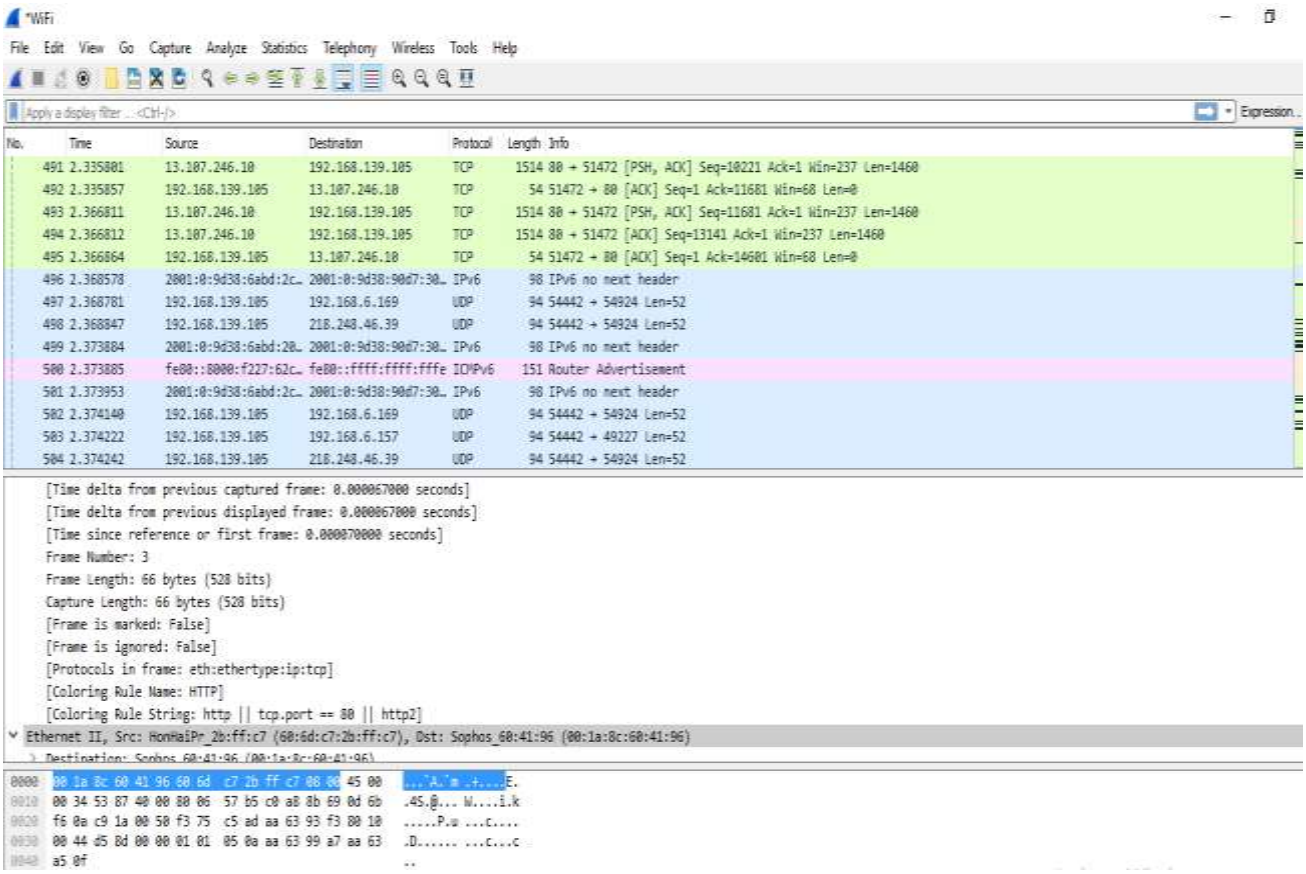

Figure 1. Wireshark

3.2. Nessus

Nessus is the world's most popular, open-source vulnerability scanner developed by Tenable Network Security [4]. It uses Nessus Attack Scripting Language (NASL) to describe individual threats and potential attacks. Nessus consists of two main components: Nessusd, which scans networks and Nessus, which gives results to the user. The characteristics of Nessus include:

a) Nessus is compatible with all computers and servers.
b) Detects security holes in both remote and local hosts.
c) Detects security updates and also the patches for the bugs.
d) Simulates attacks to find the vulnerabilities in a system.
e) Schedules and executes the security audits.

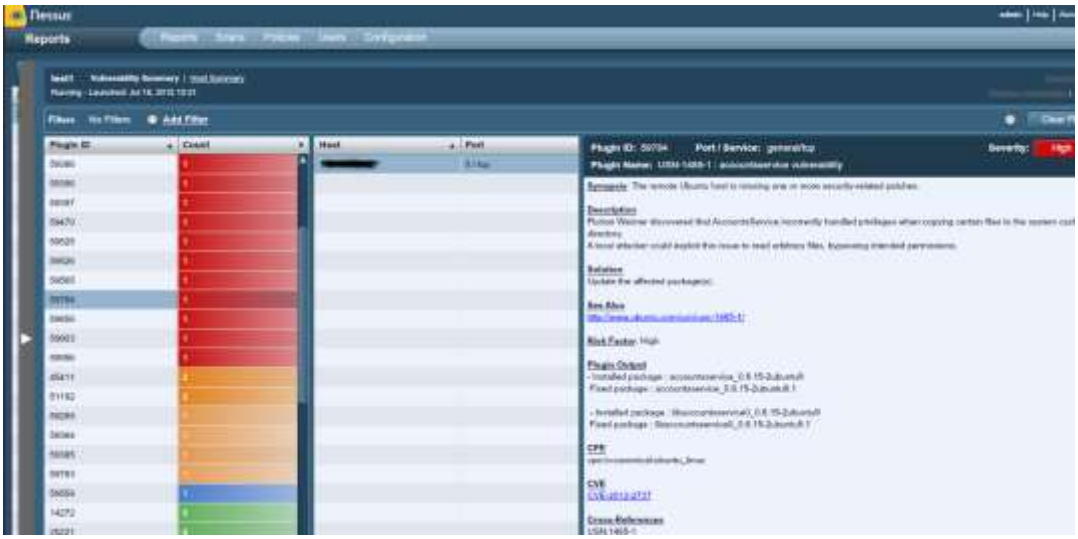

Figure 2. Nessus

3.3. Snort

Snort is an open-source network intrusion detection and prevention system. It performs real-time traffic analysis and packet logging on IP networks [3]. The different modes in which snort operates are:

a) Sniffer
b) Packet logger
c) Network intrusion detection

In sniffer mode, the program reads the network packets and displays to the user. In packet-logger mode, it logs packets to the disk. In intrusion detection mode, it will monitor the network traffic and analyze it. The characteristics of Snort include:

i) Content searching and matching.
ii) Detects varieties of attackers.
iii) Protocol analysis
iv) Sends real-time alert to syslog- a separate alert file.

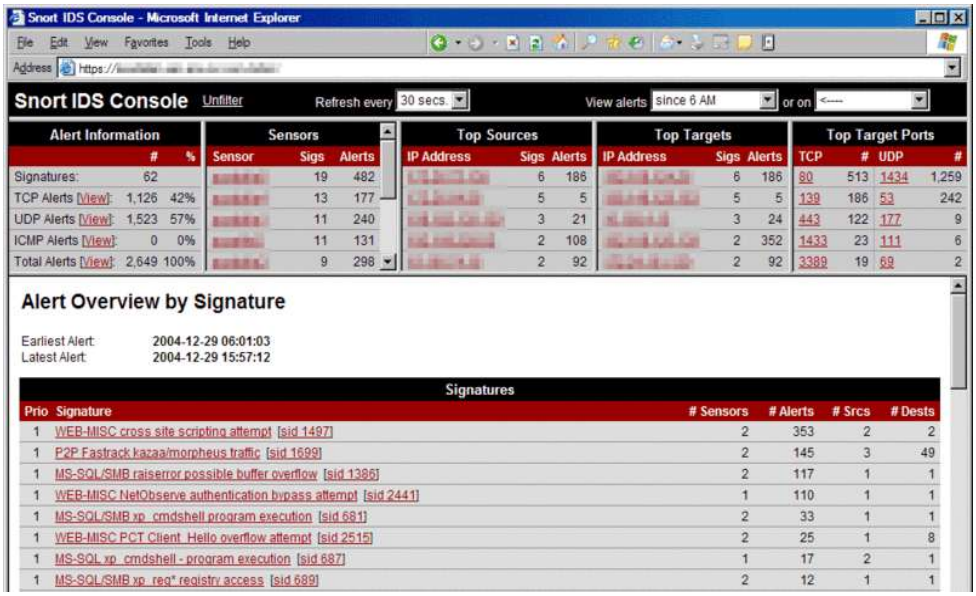

Figure 3. Snort

3.4. John the ripper

It is a password-cracking software tool. It is the most popular password cracker as it combines various password crackers into a package [3]. It is compatible with various platforms. John the ripper is an open-source, free password cracking tool which offers both brute force and dictionary attack modes. In brute force mode, it scans all the possible texts and hashing each one of them and then compares it with the input hash. In dictionary attack mode, it takes string samples, usually made up of wordlist found in dictionary, encrypts them in the exact format the way the password being examined has been encrypted, and then compares the output to the encrypted string.

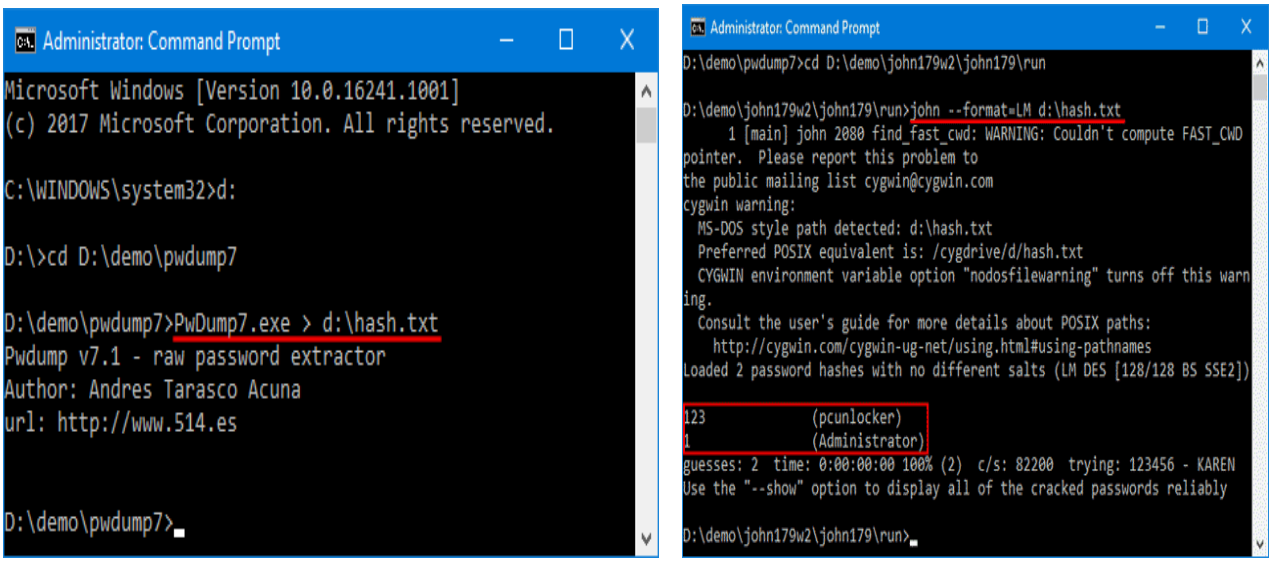

Figure 4.John the Ripper

3.5. NetStumbler

NetStumbler also known as Network Stumbler is a Windows based tool that detects Wireless LAN's using 802.11a, 802.11b and 802.11g wireless LAN standards. NetStumbler is most helpful in gathering details of wireless networks, followed by configuring, securing and optimizing the networks [4]. NetStumbler supports the following scripting languages like VBScript,Perlscript,Jscript and Python.

The characteristics of NetStumbler include:

i) Wardriving which detects WiFi wireless networks while driving.
ii) Verifying network configurations.
iii) Finding locations having poor coverage.
iv) Detecting access points which are unauthorized.
v) Detecting the wireless interference causes.

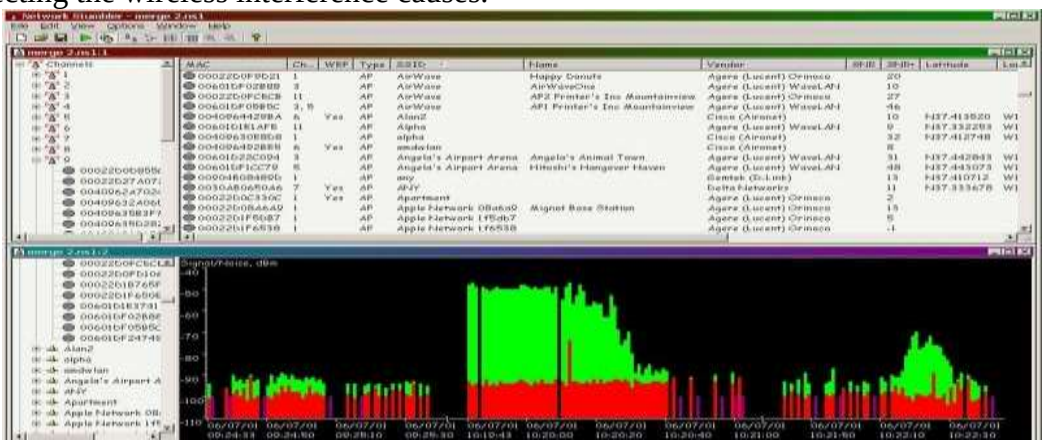

Figure 5.NetStumbler

IV. CONCLUSION

Network security tools are a necessity in today's world of attackers and intruders .These tools detect the threats to security as well as system vulnerabilities and alert the administrator to take preventive measures.This paper deals with the various types of security tools and gives a brief overview of the most popular tools in security field.

REFERENCES

[1] Amanpreet Kaur and Monika Saluja , "Study of Network Security along with Network Security Tools and Network Simulators , " International Journal of Computer Science and Information Technologies,, Vol. 5 (1) , 2014,88-92.
[2] William Stallings, "Network Security Essentials:Applications and Standards,"Fourth Edition, Pearson Publication,ISBN 13: 978-0-13-610805-4, 2011.
[3] Michael E. Whittman and Herbert J.Mattord, "Principles of Information Security ," Fourth Edition,Pearson Publication , ISBN-13: 978-1-111-13821-9, 2012
[4] Toney Bradley, " Insecure.org's Top 125 Network Security Tools" , Survey-Driven List of the Best Network Security Tools, July 2017
[5] Noel network and PC services INC., "The 4 different types of network security and why do you need them", March 2017

