ISSN: 2278-4632
Vol-13, Issue-01, No.01, January 2023

Study of Network Security along with Network Security Tools and Network Simulators

Dr. Malladi Ramakanth Reddy [1], Mr. Korivi Vamshee Krishna [2]
Department of Computer Science Engineering, Samskruti College of Engineering and Technology

***Abstract* -With the increase of hacking, different attacks, viruses, worms and other networking threats, security is a major problem in today's networks. 10, 15 years ago, security was a simple issue requiring simple solutions. In those days, the internet was small and had only a small number of businesses, organizations, universities and government agencies connected to it. Aging passwords were used to protect accounts and simple packet- filtering firewalls were used to restrict traffic flows. The entire field of network security is vast and in an evolutionary stage. The range of study encompasses a brief history dating back to internet's beginnings and the current development in network security. In order to understand the research being performed today, background knowledge of the internet, its vulnerabilities, attack methods through the internet, and security technology is important and therefore they are reviewed.**

In this paper, we analyzed the various network simulators and network security tools. This paper highlights the working of Wireshark as a network protocol analyzer and also accentuates its flexibility as an open source utility. Wireshark is used to analyze network data and then that data is classified into normal data and abnormal data.

***Keywords*- Nmap, Nessus, Network Security, Snort, Wireshark.**

I. INTRODUCTION TO NETWORK SECURITY

Network security [2] refers to any activities designed to protect your network. It consists of the technologies and processes that are deployed to protect networks from internal and external threats. Network security involves all activities that organizations, enterprises, and institutions undertake to protect the value and ongoing usability of assets and the integrity and continuity of operations. Effective network security targets a variety of threats and stops them from entering or spreading on your network.

A. Goal of Network Security

The primary goal of network security is to provide controls at all points along the network perimeter
which allow access to the network and only let traffic pass if that is authorized, valid and of acceptable risk.
The purpose of network security is to protect networks, network devices and network messages from unauthorized access, usually by outsiders.
Objective 1: To provide control all points along the network perimeter in order to block network traffic that is malicious, unauthorized or that otherwise presents risk to the network.
Objective 2: To detect and respond to attempted and actual intrusions through the network.
Objective 3: To prevent network messages that is sent across networks from being intercepted or modified.

B. Differentiating Data Security and Network Security

Data security is the aspect of security that allows a client's data to be transformed into unintelligible data for transmission. Even if this unintelligible data is intercepted, a key is needed to decode the message. This method of security is effective to a certain degree. Strong cryptography in the past can be easily broken today. Cryptographic methods have to continue to advance due to the advancement of the hackers as well.
When transferring cipher text over a network, it is helpful to have a secure network. This will allow for the cipher text to be protected, so that it is less likely for many people to even attempt to break the code. A secure network will also prevent someone from inserting unauthorized messages into the network. Therefore, hard ciphers are needed as well as attack-hard networks [2].

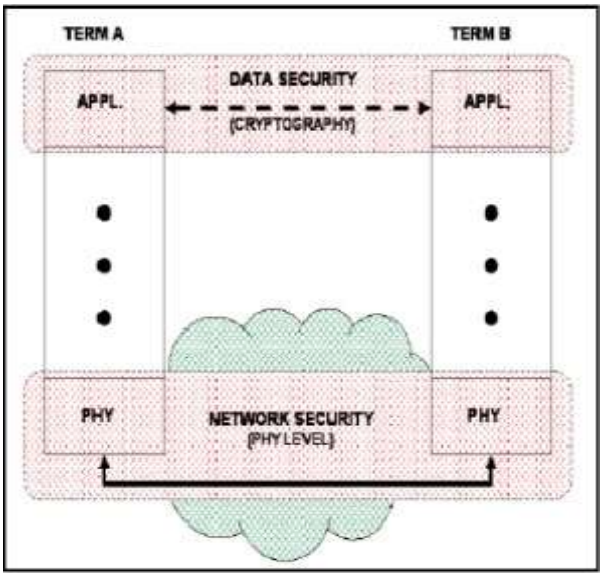

Figure 1: Based on the OSI model, data security and network security have a different security function [2].

ISSN: 2278-4632
Vol-13, Issue-01, No.01, January 2023

II. CATEGORIES OF INTRUDERS AND ATTACKER

This section will briefly discuss different types of network attacks and intruders. Before getting into the details of attack types, it is important to know about the person behind the scene.

A. Types of Attacker

These are people who want to get into the system and compromise its security. They range from those who have little experience to those who are highly skilled. Here, experience refers to their technical abilities in the field of computers and network systems.

- White hat hacker
  White hat hackers generally termed as "ethical hackers". They are the better half of this dark world of hacking. They represent those who have the knowledge and technical ability to easily break into the system, but they never exercise this. On the contrary, they use this knowledge for the good and fill in jobs like network security engineers or administrators. White hat hackers are amongst the most highly paid individuals in the US [5].
- Black hat hacker
  Black hat hackers, as the name implies, is the evil side of hacking, and their main objective is to take over the network by hook or crook, and destroy or sabotage the network resources [8]. Black hat hackers hold conferences on how to improve their hacking capabilities. These people are very experienced and know almost all the ways of how to break into the network. There is no particular purpose of the black hat hackers as to why they want to hack, but their intentions may include revenge, or stealing money, or maybe just to check how far they have improved in this field. Black hat hackers possesses the same knowledge as that of white hat hackers with the only difference that white hat hackers work towards securing the network unlike their black hat counterparts.
- Gray hat hacker
  Gray hat hackers can be thought of as white hat hackers who occasionally stray away from their goal of protecting the network and, instead, act unethically. Grey hat hackers are not permanently employed at companies; rather, they are called in for security audits. Given opportunities, the gray hat hackers might, for their own personal gain, hack into the system and steal desired data.
- Script kiddy
  Script kiddies [11] are not true hackers, and have almost no knowledge of hacking, but could download killer applications and use them with little research to attack the network. E.g. Nessus is a free security auditing tool.
- Hactivist
  Hactivists [7] are those who are driven by political motivation to hack into any network. Often, it is terrorists or foreign agencies who hack into other countries‟ sites to steal sensitive information only to gain their political motives.
- Academic Hacker
  Academic hackers [5] hack for their academic careers. They are kids who want to break into the university firewalls to change their grades or steal a paper to get good scores in exams.

III. CATEGORIES OF ATTACK

This section will discuss how a hacker can perform an attack on a network [3].

A. Passive attack

Passive attacks also know as reconnaissance attack is the first step the hacker takes in order to perform hacking. During this phase, the hacker tries to gather information with the aid of packet sniffing, scanning active ports or performing ping scans to see what IP addresses are active around the networks. This is the initial phase of hacking and usually it is very difficult to detect any such activity.

B. Active attacks

After a passive attack, an intruder has enough information about active ports, IP addresses around the network and also have queried enough to launch an active (access) attack. In this phase, the attacker usually performs "Man in the Middle" attack. Man in the Middle attack is one of the most dangerous attacks and resides in the midway communication between the gateway and the client. It is transparent in nature, hence eliminating the possibility of it being detected while it sniffs sensitive data. Trust exploitation and password attacks also fall in this category.

IV . SEVEN STEPS TO HACK A NETWORK

If we think like a hacker, there are seven steps to hack into a system. The order does not matter in this process. The following is a brief description of how the whole process is carried out.

- Perform reconnaissance
- Identify active applications and type and version of operating system
- Gain system to the network
- Log in with user credentials, escalate privileges
- Create and gather other usernames and passwords
- Create backdoor
- Use system

V. NETWORK SIMULATION

A network simulator [6] is a technique of implementing the network on the computer. Through this the behavior of the network is calculated either by network entities interconnection using mathematical formulas, or by capturing and playing back observations from a production network.

"The Network Simulator provides an integrated, versatile, easy-to-use GUI-based network designer tool to design and simulate a network with SNMP, TL1, TFTP, FTP, Telnet and Cisco IOS device."[3]

ISSN: 2278-4632
Vol-13, Issue-01, No.01, January 2023

There are different network simulators with different features. Some of the network simulator are OPNET, NS2, NS3, NetSim, OMNeT++, REAL, J-Sim and QualNet.

NS2 (Network Simulator version2): NS2 is a [7] discrete event simulator targeted at networking research. It provides support for simulation of TCP, routing, and multicast protocols over all networks (wired and wireless).

NS3 (Network Simulator version3): NS3 is also an open sourced discrete-event network simulator which targets primarily for research and educational use. NS3 is licensed under the GNU GPLv2 license, and is available for research and development.[1]

OPNET (Optimized Network Engineering Tools): It is extensive and powerful simulation software with wide variety of possibilities to simulate entire heterogeneous networks with various protocols

NETSIM (Network Based Environment for Modelling and Simulation): It is [6] an application that simulates Cisco Systems networking hardware and software and is designed to aid the user in learning the Cisco IOS command structure.

OMNET++ (Optical Micro-Networks Plus Plus): It is an extensible, modular, component-based C++ simulation library and framework, primarily for building network simulators.

JSIM (Java-based simulation): It is a Java-based simulation system for building quantitative numeric models and analyzing them with respect to experimental reference data. JSim is an application development environment based on the component-based software architecture.

QUALNET: It is a commercial [7] version of GloMoSim used by Scalable Network Technologies for their defense projects.

REAL (REalistic And Large): It is a network simulator originally [7] for studying the dynamic behavior of flow and congestion control schemes in packet-switched data networks. It provides users with a way of specifying such networks and to simulate their behavior.

VI. NETWORK SECURITY TOOLS

System and network technology is a key technology for a wide variety of applications. Security is crucial to networks and applications. Although, network security is a critical requirement in emerging networks, there is a significant lack of security methods that can be easily implemented.

A. List of some Network Security tools are:-

1. WireShark or Ethereal
2. Nmap
3. Nessus
4. Snort

Wireshar [1] is the world's most popular network protocol analyzer. It has a rich and powerful feature set and runs on most computing platforms including Windows, OS X, Linux, and UNIX. Network professionals, security experts, developers, and educators around the world use it regularly. It is freely available as open source, and is released under the GNU General Public License version 2. It has been developed and maintained by a global team of protocol experts, and it is an example of a disruptive technology. Wireshark formerly used to be known as Ethereal.

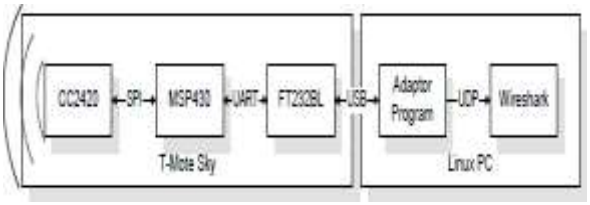

Figure 2. Packet Sniffer System Architecture.

Step 1: Start Wireshark on your computer.

Figure 3. Wireshark default view changes.

Step 2.

Wireshark [1] provides users the capability of capturing the packets traveling over the entire network on a particular interface at a particular time. One of the primary tools is the capture tool. The interface option as shown in figure 4 below lists all available interfaces on the node and can enable capturing for any of these nodes. Options tab provides more sophisticated approach for each interface one at a time. The go menu items provide the capabilities of going through packets in the capture list. The View menu provides tools for listing packets, time display formats and coloring rules.

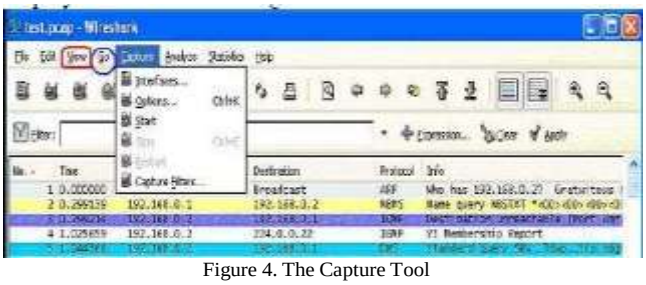

Figure 4. The Capture Tool

Step3.

Wireshark provides amazing flexibility over other IDS/IPS devices in the field of log maintenance. Log files can be captured at an hourly or weekly rate based on the requirement

ISSN: 2278-4632
Vol-13, Issue-01, No.01, January 2023

of the network and the capability of handling devices. Thus, files can be easily captured over a fast processing node and transferred to a slower database. Another interesting aspect is the feature of exporting the capture file into various other and more understandable formats- the plain text, post script, the CSV etc. based on the analyzer tool used.

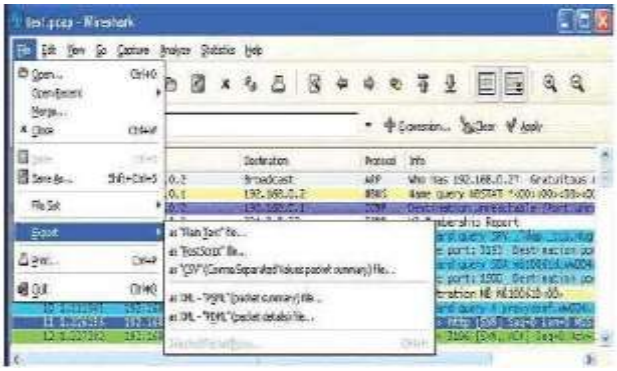

Figure 5. The Analyzer tool

B. Features of Wireshark:

- Available for UNIX and Windows.
- Capture live packet data from a network interface.
- Open files containing packet data captured with tcpdump/WinDump, Wireshark, and a number of other packet capture programs.
- Import packets from text files containing hex dumps of packet data.
- Display packets with very detailed protocol information.
- Save packet data captured.
- Export some or all packets in a number of capture file formats.
- Filter packets on many criteria.
- Search for packets on many criteria.
- Colorize packet display based on filters.
- Create various statistics.

C. What Wireshark not do for your Network

- Wireshark isn't an intrusion detection system. It will not warn you when someone does strange things on your network that he/she isn't allowed to do. However, if strange things happen, Wireshark might help you figure out what is really going on.
- Wireshark will not manipulate things on the network, it will only "measure" things from it. Wireshark doesn't send packets on the network or do other active things (except for name resolutions, but even that can be disabled).

VII. NMAP DETECTION AND COUNTERMEASURES

Nmap (Network Mapper) [4] is a security scanner originally written by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich) used to discover hosts and services on a computer network, thus creating a "map" of the network. To accomplish its goal, Nmap sends specially crafted packets to the target host and then analyzes the responses. The software provides a number of features for probing computer networks, including host discovery and service and system detection. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features. Nmap is also capable of adapting to network conditions including latency and congestion during a scan. Nmap is under development and refinement by its user community.

A. Features of Nmap

- Host discovery – Identifying hosts on a network. For example, listing the hosts that respond to pings or have a particular port open.
- Port scanning – Enumerating the open ports on target hosts.
- Version detection – Interrogating network services on remote devices to determine application name and version number.[6]
- OS detection – Determining the operating system and hardware characteristics of network devices.
- Scriptable interaction with the target – using Nmap Scripting Engine.

B. Typical uses of Nmap:

- Auditing the security of a device by identifying the network connections which can be made to it.
- Identifying open ports on a target host in preparation for auditing.[8]
- Network inventory, network mapping, maintenance and asset management.
- Auditing the security of a network by identifying new servers.[9]

C. Reporting results of Nmap

Nmap provides [4] four possible output formats. All but the interactive output is saved to a file. Nmap output can be manipulated by text processing software, enabling the user to create customized reports.

- Interactive
  It presented and updated real time when a user runs Nmap from the command line. Various options can be entered during the scan to facilitate monitoring.
- XML
  Xml format that can be further processed by XML tools. It can be converted into a HTML report using XSLT.
- Grepable
  Output that is tailored to line-oriented processing tools such as grep, sed or awk.
- Normal
  Normal the output as seen while running Nmap from the command line, but saved to a file.
- Script kiddie
  It meant to be an amusing way to format the interactive output replacing letters with their visually alike number representations. For example, *Interesting ports* becomes *Int3rest1ng p0rtz*.

ISSN: 2278-4632
Vol-13, Issue-01, No.01, January 2023

VIII. NESSUS

Nessus [9] is a proprietary comprehensive vulnerability scanner which is developed by Tenable Network Security. It is free of charge for personal use in a non-enterprise environment.

A. Operations of Nessus

Nessus allows scans for the following types of vulnerabilities [9] :

- Vulnerabilities that allow a remote hacker to control or access sensitive data on a system.
- Misconfiguration (e.g. open mail relay, missing patches, etc.).
- Default passwords, a few common passwords, and blank/absent passwords on some system accounts. Nessus can also call Hydra (an external tool) to launch a dictionary attack.
- Denials of service against the TCP/IP stack by using mangled packets.

B. How Nessus Works

- It works by locating hosts starting with a target file
- It works by port scanning the targets located
- By probing for vulnerabilities in applications listening at open ports.

IX. SNORT

Snort fills [10] an important “ecological niche" in the the realm of network security: a cross-platform, lightweight network intrusion detection tool that can be deployed to monitor small TCP/IP networks and detect a wide variety of suspicious network traffic as well as outright attacks. Snort is a tool for small, lightly utilized networks. Snort is useful when it is not cost efficient to deploy commercial NIDS sensors. Modern commercial intrusion detection systems cost thousands of dollars at minimum, tens or even hundreds of thousands in extreme cases. Snort is available under the GNU General Public License [GNU89], and is free for use in any environment, making the employment of Snort as a network security system more of a network management and coordination issue than one of affordability.

A. *Applications uses of Snort*

Snort was designed to fulfill the requirements of a prototypical lightweight network intrusion detection system. It has become a small, flexible, and highly capable system that is in use around the world on both large and small networks.

It has attained its initial design goals and is a fully capable alternative to commercial intrusion detection systems in places where it is cost inefficient to install full featured commercial systems.

X. CONCLUSION

With the increased use of Information Systems in society, security is becoming more and more important for strategic and operational concerns. Particularly network security is of more immediate consideration for protecting the system externally and internally. In this paper, we have discussed various network simulations and network security tools. And the network security tools uses as sniffing tool in networks. This paper also highlights the working of Wireshark as a network protocol analyzer and also accentuates its flexibility as an open source utility to allow developers to add possible functionalities of intrusion detection devices in it. Along with wireshark, we have also discussed the uses and detection of other network security tools such as Nmap, Nessus and Snort.

REFERENCES

1. Usha Banerjee and Ashutosh Vashishtha “Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection” in the *International Journal of Computer Applications, Volume 6– No.7, September 2010.*
2. Kartalopoulos, S. V., "Differentiating Data Security and Network Security," *Communications, 2008. ICC '08. IEEE International Conference on*, pp.1469-1473, 19-23, May 2008.
3. Adeyinka, O., "Internet Attack Methods and Internet Security Technology," *Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on*, vol., no., pp.77-82, 13-15 May 2008.
4. Nmap Scripting Engine (http://nmap.org/book/nse.html#nse-intro). Nmap.org. Retrieved on 2013-02-01.
5. *What is a Packet Sniffer?* http://www.wisegeek.com/what-is-a-packet-sniffer.htm [Accessed March 28, 2010]
6. http://en.wikipedia.org/wiki/Network_simulation
7. http://www.boson.com/netsim-cisco-network-simulator
8. “Black Hat”, criminal hackers http://www.blackhat.com/ 2010-02-07
9. “Nessus”, tool for security audit of the network.http://www.nessus.org/nessus/ 2010-02-07
10. Martin Roesch “s n o r t — l i g h t w e i g h t i n t r u s i o n D e t e c t i o n f o r n e t w o r k s
11. “Scriptkiddie” http://www.wordspy.com/words/scriptkiddie.asp 2010-02-07