© INNOVATIVE RESEARCH THOUGHTS | Refereed | Peer Reviewed | Indexed

ISSN : 2454 – 308X | Volume : 06 , Issue : 05 | May 2020

Network Vulnerability Detection Using Ant Colony Optimization-A Review

Shruti Jindal[1,]
shrutijindal1129@gmail.com[1]

ABSTRACT: A Computer Network is often refers to as a network, is used to share resources, applications and information through devices connected to the network. Computer network is a collection of autonomous computer interconnected by a single tech- nology. The computers aresaidto be interconnected if they are able to exchange information. The connection need not be a copper wire, fiber optics, microwaves, infrared and communication satellites can be used. Networks come in many sizes, shapes and forms. Network Security is becoming an important issue for all the organizations, and with the increase in knowledge of hackers and intruders they have made many successful attempts to bring down high-profile company University network sand web services.

[1]INTRODUCTION

A Computer Network is often refers to as a network, is used to share resources, applications and information through devices connected to the network. Computer network is a collection of autonomous computer interconnected by a single tech-nology. The computer aresaidto be interconnected if they are able to exchange information. The connection need not be a copper wire, fiber optics, microwaves, infrared and communication satellites can be used. Networks come in many sizes, shapes and forms. e m n issue here is resource sharing and the goal is to make all programs, equipment and especially data available to anyone on the network without regard to physical location of the resources and the user. There are two types of computer network configuration peer-to-peer networks and client/server networks. Peer-to-peer are commonly implemented where less than ten computers are involved and where strict security is not necessary. Client/server networks are more suitable for larger networks. Network security is the process of preve ti g and detecting unauthorized access to your network. Prevention measures help you to stop unauthorized users (also known as ”intruders”) from accessing any part of your Network. Detection helps you to determine whether or not someone attempted to break into your system, if in a safe, and thrown at the bottom of the ocean.” Network security refers to all hardware and software functions, characteristics, features, operational procedures, accountability

measures, access controls, and ad-ministrative and management policy required to provide an acceptable level of pro-tection for hardware, software, and information in a network .

[2] LITERATURE SURVEY

Vulnerability has been discussed in brief University in the previous chapter, however if we go through the literature, we came to know about the r s archers who have previously worked upon this topic. How to overcome from vulnerabilities, what are the major types of vulnerability, detection of the arability. ACO has been in the spot light for almost two decades, many of the work have been done in this field by researchers. Ant Colony Optimization as the name suggest is he problem for finding out the optimal result. Started in the early 90s, a researcher Marco Dorigo, during his PhD thesis, came to know about the behavior of the real Ants, how they came to know about the food from the nest, and how they communicate with each other to tell other where the food is. Marco with his colleague name Di Caro and Gambardella have worked upon Ant Colony Optimization. Vulnerability in the system means having weakness in system. These weaknesses are greatly exploits by the hacker to gain access into your system. Any vulnerable system is open to the hacker they can do anything to your system. They can steal any type of information from your computer. Main cause of presence of any type of vulnerabilities in the system is due to lack of programming. And it is due to some flaws in the Software. When hackers came to know about this weaknesses about your system they can easily hook on to your system and can exploits them up to any extent. Some methods need to adopted to overcome from these weaknesses. Main cause of Vulnerabilities is as follows:

Step1Complexity: large, complex systems increase the probability of flaws and unintended access points.

Step2 Familiarity: Using common, well-known code, software, operating system, and hardware increases the probability University an attack erhasorcan find the knowledge and tools to exploits the flaw.

Step3Connectivity: More physical connections, privileges, ports, protocols, and services and time each of those are accessible increase vulnerability.

Step4 Password management flaws: The computer user uses weak passwords that

could be discovered by brute force. The computer user stores the password on the computer Thapar where program can access .Users re-use passwords between many programs and websites.

Step1Operating system design flaws: The operating system designer chooses to enforce sub optimal policies on user/program/ management. For example operating systems with policies such as default permit grant every program and every user full access to the entire computer. This operating system flaw allows viruses and mal ware to execute commands on behalf of the administrator.

Step2 Fundamental operating system design flaws: The operating system de-signer chooses to enforce sub optimal policies on user/program/ management. For example operating systems with policies such as default permit grant every program and every user full access to the entire computer.

[3] PROPOSED WORK

We have discussed the proposed work in following step:-

Step 1 Get data from file and store in packet

Step 2 Perform xor operation on the data to encode

Step 3 Perform AES to encrypt the data

Step 4 Perform AES to encrypt the data

Step 5 Perform XOR operations on the data to

Step 6 Get data from file and store in packet.

In this research we have enhanced the security of data transmission using encryption decryption mechanism along with XOR operation. We have also used aunt colony optimization technique to restrict the transmission of packet for 5 minutes after transmission. It would reduce the chances of misuse of packet as well as it would minimize the probability of congestion in network. The used of pattern based security with AES has overcome the loopholes in existing security system. Even if craker knows the pattern he must know in which sequence button in pattern must be clicked.

[4] JAVA SOCKET PROGRAMMING

Step1 Java Socket programming has been used for communication btw applications running on different JRE.

Step2Java Socket programming could be connection-oriented or connection-less.

Step3Socket & Server Socket classes are used for connection-oriented socket programming & Datagram Socket & DatagramPacket classes are used for connection-less socket programming.

PORT

Sockets are UNIQUELY identified by Internet address, end-to-end protocol, and port number. That is why when a socket is first created it is vital to match it with a valid IP address and a port number. In our labs we will basically be working with TCP sockets. Ports are software objects to multiplex data between different applications. When a host receives a packet, it travels up the protocol stack and finally reaches the application layer. Now consider a user running an ftp client, a telnet client, and a web browser concurrently.

Port	**Service Name,Alias**	**Description**
1	Tcpmux	TCP port service multiplexer
7	Echo	Echo server
9	Discard	Like/dev/nu11
13	Daytime	Systemsdate/time
20	ftp-data	FTP data port
21	ftp	Main FTP conection
23	telnet	Telnet conection
25	Smtp,mail	UNIX mail
37	Time,timeserver	TIME server
42	Nameserver	Time server
70	Gopher	Text/menu information
79	Finger	Current users
80	www,http	Web server

Table 4.1 Port Table

[5] PROPOSED WORK

We have discussion the proposed work in following step:-

Step 1 Get data from file and store in packet

Step 2 Perform xor operation on the data to encode

Step 3 Perform AES to encrypt the data

Step 4 Perform AES to encrypt the data

Step 5 Perform xor operation on the data to encode

Step 6 Get data from file and store in packet.

[6] CONCLUSION

In this research we have enhanced the security of data transmission using encryption decryption mechanism along with XOR operation. We have also used aunt colony optimization technique to restrict the transmission of packet for 5 minutes after transmission. It would reduce the chances of misuse of packet as well as it would minimize the probability of congestion in network. The used of pattern based security with AES has overcome the loopholes in existing security system. Even if craker knows the pattern he must know in which sequence button in pattern must be clicked.

REFERENCES

[1] Introduction to Network Security, Dr. Rahul Banerjee, BITS-Pilani, India www.discovery.bits pilani.ac.in/rahul/CompNet/index.htm

[2] http://www.cert.org/tech tips/homeUniversitynetworks.html A Brief History of Network Security and the N d for Adherence to the Software Process Model, by Paul Innella, www.tdisecur .com/resources/assets/NetSec.pdf

[3]Network Security fundamentals, By Gert De Laet, Gert Schauwers, Cisco press.

[5]] Network Attack nd Defence, By Roger Needham and Butler Lamson. www.cl.cam.ac.uk/ rja14/Papers/SE-18.pdf

[6] Ecient countermeasures for software vulnerabilities due to memory manage-ment errors,Prof. Dr. ir. W. JOOSEN, Prof. Dr. ir. F. PIESSENS.

[7] Computer Vulnerabilities, Written by Eric Knight, C.I.S.S.P. Original Publication: March 6, 2000.www.ussrback.com/docs/papers/gener al/compvuln$_d$raf t.pdf

[8] http://www.antcolonies.net/howantscom municate.html

[9] http://en.wikipedia.org/wiki/Ant colony optimization

[10] http://www.javvin.com/etrac/networ k-vulnerabilities.html

[11] http://searchmidmarketsecurity.techtarge t.com/sDefinition /0,,sid198 gci1176511,00.html