Global Journals LaTeX JournalKaleidoscope™

Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

Enhancing Network Security using Ant Colony Optimization

Parul Chhikara[1] and Arun K. Patel[2]

[1] GITM, GURGAON, INDIA

Received: 16 December 2012 Accepted: 2 January 2013 Published: 15 January 2013

Abstract

Security of the information in the computer networks has been one of the most important research area. To preserve the secure condition it is essential to be aware of the behavior of the incoming data. 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-pro le company networks and web service. The technology of artificial intelligence breaks a new way in the area of network security. Ant-colony optimization algorithm is an evolutionary learning algorithm which could be applied to solve the complex problems. Applying the idea of ant colony optimization into network vulnerability detection and enhancing security can improve the performance of network security management. This paper attempts to apply ACO Algorithm to find out vulnerabilities in the network and ensure its security.

Index terms— ACO, network security, pheromone intensity, NMAP, NESSUS.

1 Introduction

etwork Security can be views as local or global point of view depending upon the network design. Managing Security means understanding risks and deciding how to overcome if any security is violated. Network security is a level of guarantee that all the machines in a network are working optimally and the users of these machines only possess the rights that were granted to them. Network security is the most vital component in information security because it is responsible for securing all information passed through networked computers **??**1]. After gaining access to the network with a valid IP address, the attacker can modify, reroute, or delete your data **??**2]. A stack overflow attack on the BIND program, used by many Unix and Linux hosts for DNS, giving immediate account access **??**14]. In this paper we attempt to augment NESSUS Script using Java Plugin to include ACO behaviour in order to detect common vulnerabilities with ease. II.

2 Literature Review

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. 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. a) Trojan A Trojan in software security means a seemingly attractive or innocuous program that hides malicious software inside. Trojans can also be staged on download sites and disguised as utility programs, games, etc. and the victim is tricked into downloading them because they look like a useful program the victim might want to use **??**10].

3 b) Network Vulnerability

Network vulnerabilities are present in every system. Network technology advances so rapidly that it can be very difficult to overcome vulnerabilities altogether. Following are the type of vulnerabilities an administrator should take care of this: ??11] Internal network vulnerabilities result over extension of bandwidth (user needs exceeding total resources) and bottlenecks (user needs exceeding resources in specific network sectors).

DOS and DDOS are external attacks as the result of one attack or a number of coordinated attacks, respectively.

A war dialer is a tool used to scan a large pool of telephone numbers to detect vulnerable modems to provide access to the system. Following are the list of most vulnerable ports [12]:

? 139 (SMB over NetBIOS)

? 80 (HTTP)? 25 (SMTP) ? 23 (Telnet) ? 20 21 (FTP)

Vulnerability analysis consists of several steps [13]:

? Defining and classifying network or system resources. ? Assigning relative levels of importance to the resources. ? Identifying potential threats to each resource.

4 III.

5 Ant Colony Optimization

In a colony of social ants, each ant usually has its own duty and performs its own tasks independently Year from other members of the colony. However, tasks done by different ants are usually related to each other in such a way that the colony, as a whole, is capable of solving complex problems through cooperation ??5, ??]. For example, for survival-related problems such as selecting the shortest walking path, finding and storing food, which require sophisticated planning, are solved by ant colony without any kind of supervisor.

Ants communicate through pheromone trails to exchange information about which path should be followed. As ants move, a certain amount of pheromone is dropped to make the path with the trail of this substance. Ants tend to converge to the shortest trail (or path), since they can make more trips, and hence deliver more food to their colony. The more ants follow a given trail, the more attractive this trail becomes to be followed by other ants. This process can be described as a positive feedback loop, in which the probability that an ant chooses a path is proportional to the number of ants that has already passed through that path ??4, ??].

Researchers try to simulate the natural behavior of ants, including mechanisms of cooperation, and devise ant colony optimization (ACO) algorithms based on such an idea to solve the real world complex problems, such as the travelling salesman problem [7], data mining ??6].

ACO algorithms solve a problem based on the following concept:

? Each path followed by an ant is associated with a candidate solution for a given problem. ? When an ant follows a path, it drops varying amount of pheromone on that path in proportion with the quality of the corresponding candidate solution for the target problem. ? Path with a larger amount of pheromone will have a greater probability to be chosen to follow by other ants. The process is thus characterized by a positive feedback loop, where the probability with which an ant chooses a path increases with the number of ants that previously chose the same path [3].

6 Experimental Design a) Operating System Fingerprinting

Network scanning, and particularly remote OS/application detection, is generally the first step in mapping out a network; whether for penetration testing or simply maintaining a network device inventory. Remote active operating system finger-printing is the process of determining the identity of a remote host's operating system. This is done by actively sending packets to the remote host and analyzing the responses. Tools like Nmap and Xprobe 2 take the responses and form a finger-print that can be queried against a signature database of known operating systems. Learning which operating system is running on a remote host can be very valuable for both pen testers and black-hats. scans, stealth FIN scans, XMAS tree scans, NULL scans, UDP scans, and ping scans.

7 i. OS Fingerprinting through NM AP

Nmap is a network exploration tool and security scanner. It is designed to allow users to scan networks to determine which hosts are up and what services they offer. Nmap supports a number of scanning techniques that use the following protocols: TCP, ICMP, UDP and IP. Nmap also includes features like remote OS detection, parallel scanning and port filtering detection.

8 c) Fuzzing

Fuzzing is the art of automatic bug finding. This is done by providing an application with semi-valid input. The input should in most cases be good enough so applications will assume it's valid input, but at the same time be broken enough so that parsing done on this input will fail. Such failing can lead to unexpected results such as crashes, information leaks, delays, etc. It can be seen as part of quality assurance, although only with negative test cases. Fuzzing is mostly used to uncover security bugs, however, it can often also be used to spot bugs that aren't security critical but which can non-the-less improve robustness.

9 d) NESSUS

Nessus was created to be a free, powerful, remote security scanner. It is one of the top-rated security software products, and is endorsed by professional information security organizations such as the SANS Institute. The

"Nessus" security scanner is a software which will audit remotely a given network and determine whether someone (or something -like a worm) may break into it, or misuse it in some way. Nessus can perform over 900 security checks.

i. Web server Fingerprinting with NASL include("http func.inc"); sock=open sock tcp(80); req=string("GET / HTTP/1.0 ","Accept: */* ","" "); send ??socket:sock,d This method builds a solution to the problem by detecting vulnerability moving from node to node and constructing graph G. Ants move by applying a stochastic local decision policy that makes use of the pheromone values (NVD score: Candidate or Non Candidate) on running apps. When adding a component to the current partial solution, an ant can update the values of the pheromone trails that were used for this construction step. This kind of pheromone update is called online step-by-step pheromone update. Once an ant has built a solution, it can retrace the same path backward and update the pheromone trails of the used apps according to the quality of the solution it has built. This is called online delayed pheromone update. Another important concept in Ant Colony Optimization is pheromone evaporation. Pheromone evaporation is the process by means of which the pheromone trail intensity on the apps decreases over time. It implements a useful form of forgetting, favoring the exploration of new areas in the search space. Each attack scenario is depicted by an attack path which is essentially a series of exploits with a severity score that presents a comparative desirability of a particular network ser-vice. In an attack graph with a large number of attack paths, it may not be feasible for the administrator to plug all the vulnerabilities.

Following nessus script is fabricated to create new packets and send over the network using send packet() function. Ip = forge ip packet(ip hl : 5; ip v : 4; ip tos : 0; ip len : 20; ip id : 12; ip off : 0; ip ttl : 255; ip p : 2; ip src : 172:31:9:15); ACO NVD() Display(this host(),""); Send packet(ip,pcap active: FALSE); 172.31.9.91

The ip packet can be created using the function forge ip packet. This function takes up a large number of parameters. The first four bits is the version of ip used, 4 and set this value as the ip_c parameter. The next four bits are the length of the ip header and in this case as nothing is added to ip, it is 5.The length of the ip header can vary minimum 20 to maximum 60 as four bits hold a number from 0 to 15. The parameter name is ip_hl. Then we have the type of service which signifies the importance of packets to the routers. Unfortunately most routers ignore this field called ip_tos. Then there are two bytes that give the total length of Most of the time this field is ignored. Packet has an id of 12.

V.

10 Results and Conclusion

Graph showing the comparison of Java Nessus. ACO API with the network vulnerability tool. It takes much less time in comparison with other algorithm. Thus, validating the research work. [1] [2]

1

Figure 1: Figure 1 :

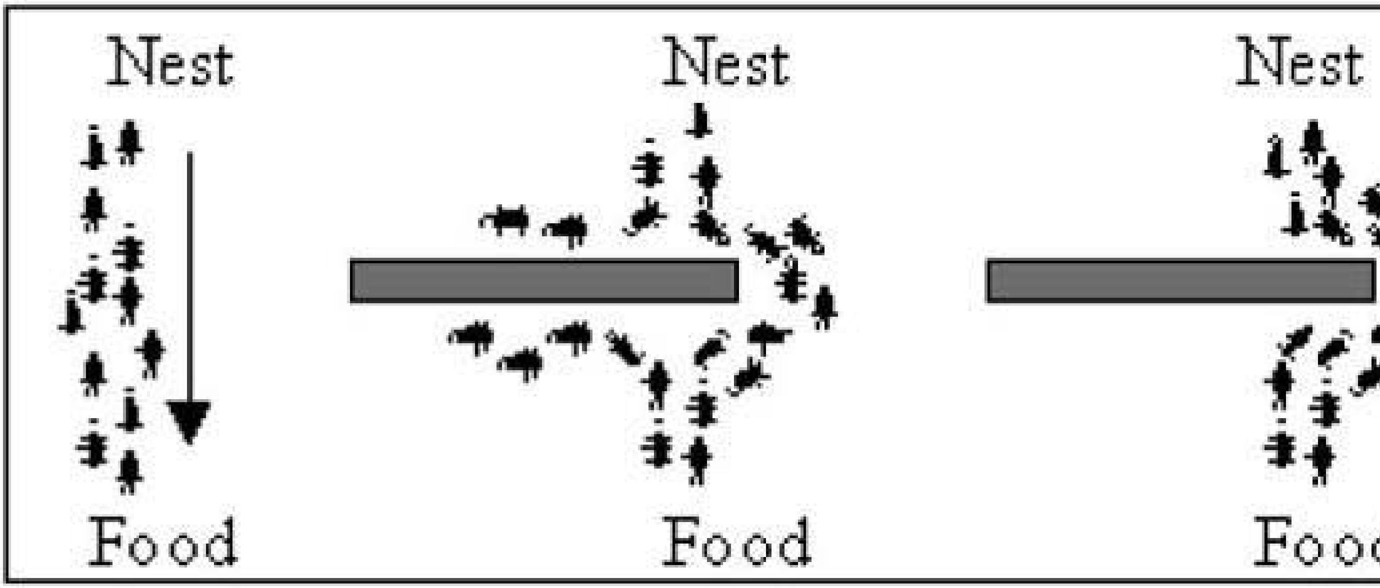

Figure 2:

2

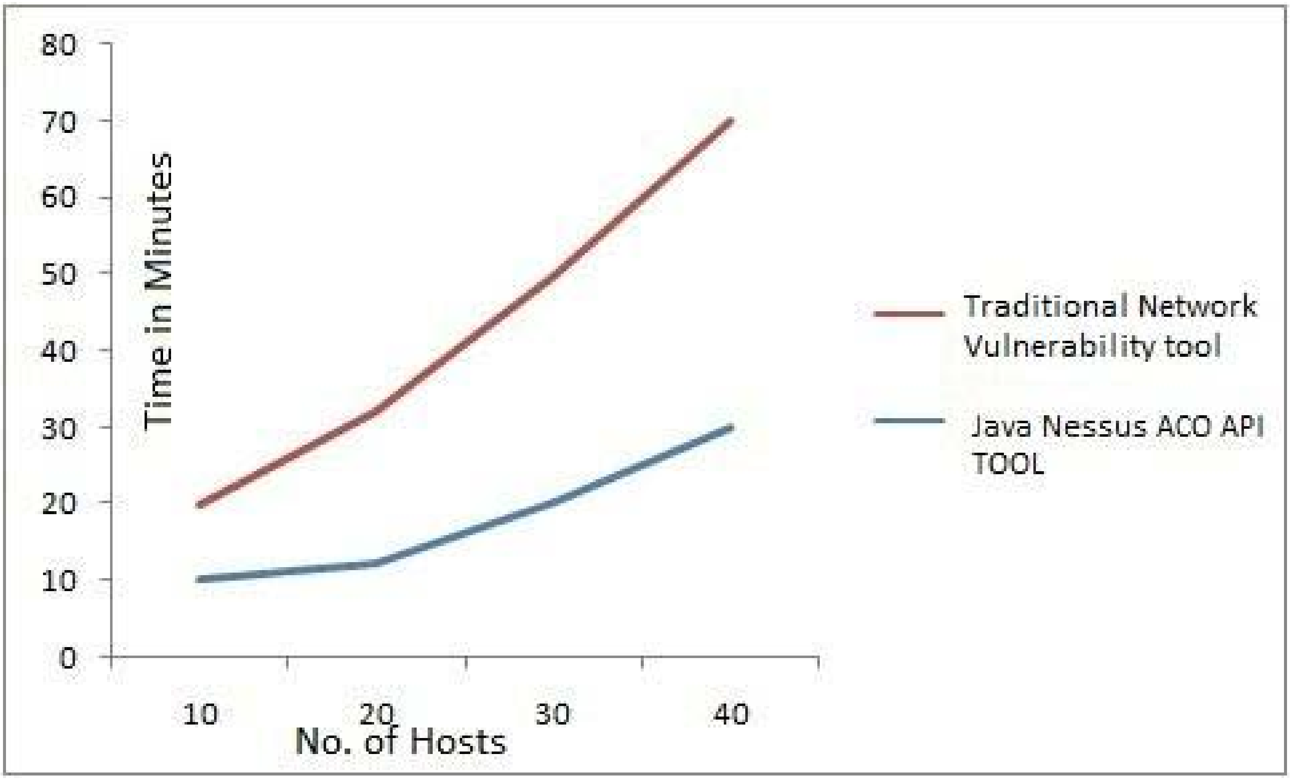

Figure 3: Figure 2 :

). The ant system: Optimization by a colony of cooperating agents. IEEE/ACM Transactions on System, Man

4. Dorigo M, Di Caro G, Gambardella LM (1999) Ant algorithms for discrete optimization. Artificial Life 5(

Figure 4:

[2]. http://technet.microsoft.com/enus/library/cc959354. asp.11. http://www.javvin.com/etrac/networkvulnerabilities.html