Volume 4, Issue 7, July 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

An Efficient Network Management System to Detect Attacks in a Network

Jinu Mathai
School of Computer Sciences
Mahatma Gandhi University,
Kerala, India

Abstract— ***This paper proposes a new method for network management. It is a method to find which network infrastructure is down or running, which of the ports are open or which link is down, which of the machines generates broadcast messages above a threshold level in a network and the number of messages sent by each machine at a time interval, which of the service ports are available in a machine or server etc. It uses a database that stores all information about the nodes in a network such as switches, servers, routers, PCs, etc. The database stores default status of nodes and compares it with currently generated status. Deviations will be flashed to admin consoles or will be logged. Results are given to the users of the system. Network diagram showing current status will be generated based on current status. Port mapping of servers and PCs and updating the same in real time will help to weed out infected machines from the network. The database will be storing the system configuration of each node in the network, OS version, application running, etc. By using this new system, we can easily find which systems are affected by any attacks and take necessary actions to remove them. It identifies the Dos attacks and interruption of the packet transmission etc. It will help to perform repairs and upgrades in a network. It allows the network to run smoothly. It improves the network performance and availability.***

Keywords- Network Management, DoS attack, Network Diagram.

I. INTRODUCTION

Network management deals with how to manage a computer network. It includes all the activities for managing each and every device in a network. Network management functions can be classified into fault management, configuration management, accounting management, performance management and security management. It includes the procedures to controlling, planning, allocating, deploying, coordinating and maintaining all nodes in a network [4].

In early days, Network management is carried out entirely by humans. The network administrators and operators are doing this job. They check physically all devices in the network to find the status of the network or use some commands to find the problems. Then take the necessary actions for that. They should have well knowledge about all systems in the network, their location and ip address to identify the problems and misbehaviour of the network devices. It is a time consuming method and is very difficult to understand the problems if it is a large network.

Then network management soft wares came into play. They have been using in some organization to manage the network. They monitor all devices in a network. The output of the network management software is the some reports of data relating to the status of the devices. Most of them use network management protocols for collecting the information for management.

Network management system refers to the tools that may be hardware or software which helps a person to monitor the individual nodes of a network. It deals with the operations like Network device discovery, Network device monitoring, network performance analysis, intelligent notifications etc.

Network can be affected by various types of attacks such as interruption, interception, modification and fabrication.

Interruption makes resources to unavailable. One of the main type of attack include in this category is the DoS attack.

Interception allows unauthorized access to a system in a network. It is mainly by means of packet sniffing or copying information.

Modification attack modifies the content of packets that are transmitted between two systems. It can be redirect the information to unintended user.

Fabrication includes mimicking or impersonating information. It is also known as counterfeiting. This type of attack usually inserts new information or captures extra information in a file. It allows access to a particular data or resources.

The proposed system is mainly deals with interruption and DoS attacks. It manages both wired and wireless networks.

II. RELATED WORK

The following are the already existing network management systems:

OpenNMS is the first enterprise grade NMS. It is an open source NMS fully developed in java. It mainly deals with performance management. The main features of OpenNMS are event report generation, service monitoring etc.

Nagios is also an open source monitoring software. Nagios was designed to run on Linux. It monitors network services, network host resources and remote systems. Data storage is via text files.

Cacti is a web based network monitoring and graphing tool. The results are graphed in this software. It is mainly used to graph the data like CPU Utilization etc. Its front end can handle multiple users at a time.

Ganglia is another network monitoring tool which is mainly used for clusters and grids. It can be run on multiple platforms. It is written in C, Perl, python and PHP. The users can view live and historical statistics such as CPU utilization for all machines in a network. XML is used for data representation.

III. PROTOCOLS OVERVIEW

A. Telnet Protocol

Telnet is a well known network protocol for accessing remote devices. It is a user command and underlying TCP/I P protocol. Telnet allows a network administrator to enter into someone's computer remotely. A person can get all the privileges that have been granted to a regular user of the system. It is mainly used by program developers and anyone who have a need to use specific applications or data located at a particular host computer [1].

Telnet is used on the Internet or local area networks. It provides a bidirectional interactive text-oriented communication facility using a virtual terminal connection. Telnet was originally developed in 1969 with RFC 15 standard, later extended in RFC 854. It is also standardized as Internet Engineering Task Force (IETF) Internet Standard STD 8.

Telnet is basically a client server protocol using reliable connection oriented transport. It uses the port number 23 where a telnet server is listening.

There are a large number of industrial and scientific devices which use Telnet for communication. Sometimes Telnet is used an option for debugging the network services such as HTTP, SNMP, FTP and POP3 in which client issues commands to a server and examine the responses. But among all these protocols only FTP really uses Telnet data format.

Here telnet is implemented using a telnet socket programming. A telnet client is created which communicate with telnet server to get the information. The step involve in that are as follows:

- Enable telnet service on the computer
- Take a telnet prompt
- Log on to the device to access
- Enter the username and password of that device
- Select mode of access
- Make necessary communication(via commands)

B. Internet Control Message Protocol

Internet Control Message Protocol (ICMP) is a major protocol in the internet protocol suite. It is not used as a method of communication like TCP and UDP which are the common data transfer protocols in use. ICMP is mainly used for network troubleshooting and managing networks. It has only limited set of commands specifically designed for the task of exploring host and network connectivity and routing.

The most common command ICMP protocol is "ping". It is called against a remote system's ip address. The output of a ping command will return a small amount of information back to the user. Ping reply tells the user whether the target machine is operational or not and whether they responding to the basic network requests. It can be used in all networks.

Ping gives basic information such as network route's latency, number of hops between source and target machine etc. Ping reply provides information regarding the connectivity between the user and the target machine. It includes the number of milliseconds required to complete the round trip request. It has a greater emphasis on the connection's latency. Bandwidth congestion, rate of errors trough any of the links between source and target and processing issues through any of the connected devices in a path are the main reasons for latent networks.

The number of hops required in completing the travel from source and target in a ping response is a function of the Time to Live (TTL) field of the packet header. It is calculated by subtracting the configured TTL from the actual TTL value. Windows OS use a default value of 128 for TTL value, which is reduced by one at each hop from source to destination.

The size of the data being transferred from source to destination influences the transfer speed. Usually ping sends a 32 byte string of repeating alphabetical characters as its payload during a request. In order to increase the performance, large sized data is fragmented during transit. Ping provides options for customizing the payload size and a setting that determines whether it can be fragmented or not. These options can be used to verify how well a connection is performing based on the size and contents of ping request's payload.

C. Simple Network Management Protocol

SNMP is the widely used network management protocol. It uses the concept of manager and agent. The manager controls and monitors a set of agents. The manager is the host and routers and servers are comes under agents. SNMP uses two other protocols. They are Structure of Management Information (SMI) and Management Information Base (MIB).

A unique identifier called object identifier is assigned for each register on a device. It is unique across every device and is represented in dotted decimal notation. The object identifier starts with .1.3.6.1.2.1. For example, to access the sysDescr object, the OID is 1.3.6.1.2.1.1.1.

The SMI component provides guidelines to SNMP. The functions of SMI are naming objects, defining the type of data that can be stored in an object and determine how to encode data for transmission over the network.

The MIB is a collection of all objects that the manager can manage. MIB, version 2 is used now days. All objects in MIB 2 can be divided into 10 groups. They are system, interface, address translation, ip, icmp, tcp, udp, egp, transmission and snmp.

The SNMP operations are mainly based on request-response communication between a client (manager) and server (agent). It uses GET and GET-NEXT commands for their operation. These two commands retrieve a particular piece of information from a device. The GET command followed by address of the information will give the desired information. GET-NEXT is used to get the next piece of information from the object hierarchy. SNMP uses two UDP ports 161 and 162 for their operation. The port 161 is used as a server and the 162 as client [1]. SET command is used to update the information with the OID.

IV. PROPOSED SYSTEM

To design a system that detects problems and attacks in a network, a dynamic approach needs to be used. Here proposed method uses the default and currently captured information for managing the network.

In our design, first it stores the default status information regarding all network devices into the database when the network is established. Then it captures the current status whenever required and compare it with the default status and other threshold limits to identify the problems. Finally, a network diagram will generated which reflects the basic information about the devices along with their status. This diagram will reflect the deviations from the default status and the threats in the network. This system is implemented in java. Fig.1 gives an overview of the design of proposed system. The proposed system works in four steps. They are:

A. Storage of default status information of devices

The default status information of all devices in a network is to be stored into a database. It reflects the normal condition of a network when network is established. The stored information will be used to identify the network problems.

The information regarding all devices such as PCs, servers, switches, routers are stored into the database. It includes port details, service port availability, bandwidth, speed, type of antivirus, interface details, broadcast message threshold etc.

B. Capture the information regarding all devices in a network

In this module it captures the network information regarding all the devices such as switches, routers, Pcs, servers etc. The information including type, OS version, applications running etc. The current status of the network components are taken dynamically.

Programs for obtaining information about different devices in a network are carried out. They include the following steps:

1) Systems-Up/Down Status: Ping operation checks whether a machine is up or down. Here a java program is developed to perform ping operation on all devices to find whether it is up or down. Also there is an option for selectively perform ping operation on needed devices. This information is necessary because it checks the connectivity between two systems.

2) Servers-Up/Down Status: The up/down status of the service ports that are enabled by administrator is checked in this step. It stores the all active ports and checks whether it is active at a time or not and displays this information to the user. This information is necessary because it checks whether any person change the default status of the service ports.

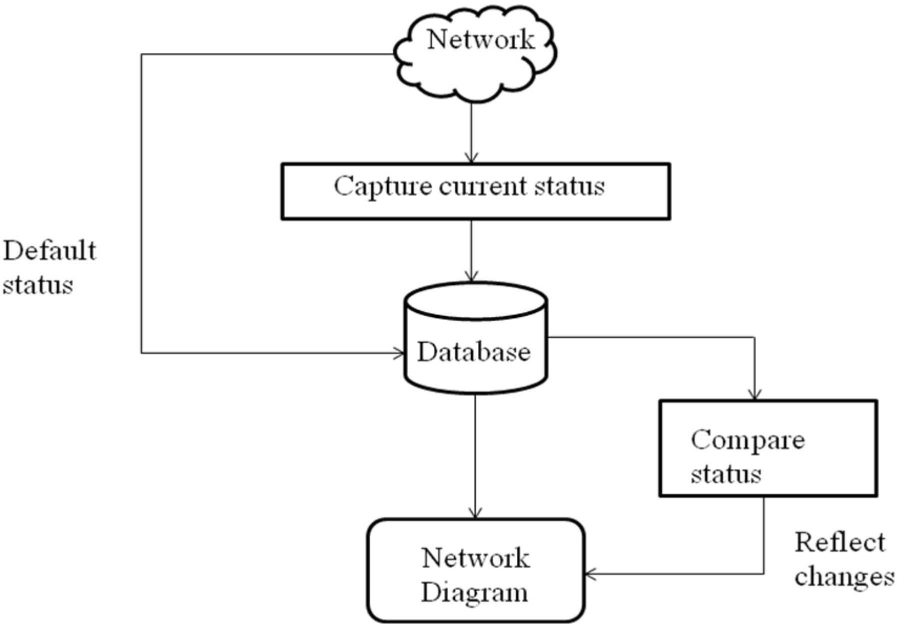

Fig. 1: Flowchart of Proposed System.

3) Servers-Service Port Availability: This step check which of the service ports are available for a particular PC and displays information to the user. In this step, create a socket connection to every port of the machine. If it is successful, it means that the server listening to that port. Otherwise server is not listening to that port. It checks for all service ports in the system.

   This information allows us to know which of the service ports are available at a time.

4) Switches-Port Status (Telnet): Port status of the certain devices such as switches is to be captured for tracing the problems in the network. Telnet socket programming is used for this. It is a multithreaded java program which checks the port status of all devices stored in the database in synchronized manner using "show interfaces" command. It also gives more information about each interface. It could result information about all interfaces of a device and displays it to the user. It shows which of the ports are up and down and their hardware address. This information is stored into the database.

   Switch port status is very important because it identifies the interruption. If any packet loss occurs, it may because of the disconnection of device from the switch interface. Then all the traffic through that interface will get affected and it is necessary to take necessary actions immediately [5].

5) Switches-Port Status (SNMP): The information about the all interfaces of a switch is captured using SNMP protocol. It uses GET-NEXT method for finding the information. It uses the object identifier for .1.3.6.1.2.1.2.2.1.8(ifOperStatus) which gives the status of each interface of the switch. If its value is 1, means that the interface is up. If it is 2, then the interface is down. A value of 3 denotes testing state which indicates that no operational packets can be passed. It also gives the information like interface name, hardware address and speed. The corresponding SNMP object identifiers are .1.3.6.1.2.1.2.2.1.2(ifDescr), .1.3.6.1.2.1.2.2.1.6(ifPhysAddress), .1.3.6.1.2.1.2.2.1.5(ifSpeed). The captured information is presented to the user. This can be extended to other devices also.

6) Systems-Broadcast Messages: Broadcasting is the process of transmitting a packet that will be received by every node on the network. Broadcasting is mainly confined to local area networks (LAN) such as Ethernet and token ring, where the performance impact of broadcasting is not as larger as it would be in a wide area network.

IPv6 does not implement the broadcast method, so as to prevent disturbing all nodes in a network when only a few may be interested in a particular communication [3]. Both Ethernet and IPv4 use a unique broadcast address as destination address to indicate a broadcast packet.

In broadcast checking, the main aim is to find the systems which generates broadcast abnormally. The broadcast may be of two types: arp and ip broadcast. Arp broadcast is to find a mac address of a particular device if its ip address is known. Then the source sends the broadcast packet to all systems in the network with a destination address of the network. It is layer 2 broadcasting. In ip broadcast, a source sends broadcast message into all systems in the network with a destination address of network id.255. Here first capture the entire transmitted packets in a network and stores the information like source address, destination address, time, type into the database. Then it fitter out the broadcast packets and based type, again categorize them into arp or ip. Count the no of broadcast packets sent by each source. The packet capturing is a continuous process which is scheduled for each 1 minute interval. This is done using task scheduling in java and a java utility such as JnetPcap is used to capture the packets. Then make a option for displaying results to user. In this user can check the broadcast packets sent by each source at different time intervals such as current time, before half an hour, before an hour etc. Then 2 frames are created which will display the top 5 broadcast senders. This information will be refreshed for every 3 minutes.

Sometimes broadcasting may be used to perform a special type of DoS attack known as Smurf attack. The Smurf attack can be defined as a distributed denial of service attack in which large number of Internet Control Message protocol (ICMP) packets are broadcast to a computer network using the spoofed source IP address of a victim computer [6]. In this, the attacker sends fake ping requests to the victim machine. Most of the devices will respond to this ping request by sending reply to the source IP address. As a result, the victim machine is flooded with responses of a large number of machines in the network. This will slow down the target machine such that it becomes impossible to work on.

Smurf attack can be treated as a variant of a flooding DOS attack on the internet. It uses misconfigured network devices for sending packets to all machines in a network via the broadcast address of the network [2]. This type of network then serves as a smurf amplifier. The attacker will send large number of packets with the source address faked to the address of the victim machine. It makes the network bandwidth quickly used up and results in prevention of legitimate packets from getting through to their destination.

7) Systems-SNMP Tables: In this step, SNMP tables stored in the network devices are retrieved. They are:

   - iftable
     It shows the information about the interface details which have the fields like ifNumber, ifIndex, ifDescr, ifType, ifMtu, ifSpeed, ifPhysAddress, ifAdminStatus, ifOperStatus, ifOutUcastPkts,ifOutNUcastPkts,

ifOutDiscards,ifOutErrors, ifOutQLen, ifSpecific etc. Their corresponding object identifiers are used to get the value.

- *ifaddresstable*
  It gives the addressing information having the fields like ipAdEntAddr, ipAdEntIfIndex, ipAdEntNetMask, ipAdEntBcastAddr, ipAdEntReasmMaxSize etc.

- *Ifroutetable*
  It gives the routing information having the fields like ipRouteDest, ipRouteMetric1, ipRouteMetric2, ipRouteMetri3,ipRouteMetric4,ipRouteNextHop,ipRouteType,ipRouteProt, ipRouteAge, ipRouteMask, ipRouteMetric5, ipRouteInfo.

- *ipNetToMediaTable*
  It gives the IP address translation information.

8) IP To MAC Resolver: IP to MAC resolver finds the MAC address corresponding to a particular ip address. It uses the ICMP protocol. It sends a ping command to the target ip address so that its IP-MAC entry gets added in the arp table of the user machine. Then apply 'arp –a' command to retrieve the all IP-MAC address pairs that has been resolved recently and filter out only the required pair and displays to the user. It eliminates the need of remembering or storing the IP-MAC address pair values.

9) Bandwidth Utilization: Bandwidth refers to the data transfer rate in a computer network. That is the amount of data that can be transmitted from one point to another in a particular time period. Usually bandwidth is expressed in bits per second (bps).

Usually, the bandwidth is calculated for both input and output interfaces of a machine in a network. Input and output utilizations are calculated by dividing the number of bits per seconds by interface speed.
The input and output utilization of each interface of a network device can be found by SNMP using the following equations.

$$\text{Input utilization} = \frac{\Delta\text{ifInOctets x 8 x 100}}{(\text{number of seconds in }\Delta)\text{ x ifSpeed}}$$

$$\text{Output utilization} = \frac{\Delta\text{ifOutOctets x 8 x100}}{(\text{number of seconds in }\Delta)\text{ x ifSpeed}}$$

ifInOctets and ifOutOctets are the incoming and outgoing data in octets respectively. ifSpeed is the interface speed. These parameters are retrieved through SNMP.

10) Rogue Detection: Rogue detection means identify the devices that enter the network without the permission of network administrator. Here first maintain a white list of legal ip addresses of the network. Each time this system is used, it will find all active devices' ip address and check whether they are in the white list. If any ip address is not present in the white list, then mark it as rogue and inform the administrator. Nmap utility is used to find the all active devices in a network for a particular time.

Each time when above steps are running, the captured information is stored into the database. In case of broadcast message, the senders address, destination address, type of broadcast and time are stored into the database. The address may be MAC address or ip address depending on the type of broadcast. While implementing telnet protocol, there is a need of username and password of each device. They are also stored into the database. The default status information and the necessary captured information of all devices in a network are also added into the database.

C. Comparison of default and current status

The current status of the network components and their default status stored in the database are compared. This will helps to identify the problems in the network.

If a port that is that is normally closed will turn into open, it may because of any virus attacks. Using this, it is possible to identify which devices are connected to network recently, whether a network working under normal conditions, or whether a connection is open or closed etc.

D. Generate network diagram

It is the last module. Here a network diagram showing the current status of each machine in the network will be drawing. It is the output of the entire system which will show the current status of the network such as which components are active at a time, which components shows the abnormal behaviour etc. It should take the output from the above module as the input to this one. If any deviations from default status are there, the diagram will flash those deviations. Attacks and bugs are also being displayed in the diagram.

V. TEST APPROACH

The proposed system is a new network management system to identify the attacks in a network. It captures the current status of the network device dynamically. The captured status is then compared with default status to identify the attacks in a network and the results are displays to the user. The system is intended to work with all networks. So it has to be tested against all possible inputs.

The completed modules are tested against many network devices. The up/down status of the system testing is carried out with almost all systems in the network and it works well. The server up/down status is checked against some of the servers in the network and it gives the correct output. Server's service port availability is also works well with these servers.

The port status of the switches using SNMP is tested against all types of the switches in the network including different make such as hp, D-Link, Cisco etc. It works properly. The only requirement is to enable SNMP in that system and a community string is to be retrieved.

The port status using Telnet is working properly with the telnet enabled switches. IP to MAC resolver is tested with about 50 systems and each one works properly. SNMP tables are also tested against 20 devices and all are produced correct results.

Bandwidth is calculated for 100 systems in a network. They results in the correct bandwidth results. The broadcast checking is for whole network. It works for all systems and captures 100 packets each in every 1 minutes and find the top ip and arp broadcasting sources.

VI. CONCLUSION

The proposed system captures the current status and compares it with the default status. Then dynamically generate the network diagram showing status of devices in a network. The deviations and other threats in a network can be flashed. The modules are working properly with all systems in a network.

This system will be an improvement over all existing systems. It will improve the performance of the network. It can manage all devices in the network. It is useful for Small and large organization.

REFERENCES

[1] Hyojoon Kim, Nick Feamster, Georgia Institute of Technology, "Improving Network Management with Defined Networking", IEEE Communication Magazine, February 2013.

[2] Computer Emergency Response Team, "TCP SYN and IP Spoofing Attacks," CERT Advisory CA-1996-21, Sept. 1996;

[3] Tatsuya Baba , Shigeyuki Matsuda "Tracing Network Attacks their Sources"

[4] Z.Cai, Maestro: Achieving Scalability and Coordination in Centralized Network Control Plane, Ph.D. thesis, 2011.

[5] M. Casado et al., "Rethinking Packet Forwarding Hardware, Proc. 7th ACM SIGCOMM HotNets Workshop, Nov. 2008.

[6] M. Chetty et al., "You're Capped: Understanding the Effects of Bandwidth Caps on Broadband Use in the Home," Proc.2012 ACM Annual Conf. Human Factors in Computing Systems, CHI '12, New York, NY, 2012 pp. 3021–30.

[7] A. R. Curtis *et al.*, "Devoflow: Scaling Flow Management for High-Performance Networks," *Pro ACM.SIGCOMM'11*, New York, NY,2011 pp. 254–65.