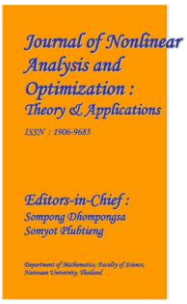
Journal of Nonlinear Analysis and Optimization : Theory & Applications
ISSN : 1906-9685
Editors-in-Chief :
Sompong Dhompongsa
Somyot Plubtieng

COLLECT AND ANALYZE NETWORKPACKETS USINGPACKET SNIFFING

Ashwin P Student, III Year (Digital Cyber Forensic Science) Rathinam College of Arts and Science, Coimbatore-21
Dr. Ramraj M., Ph.D. Assistant Professor Department of Digital Cyber Forensic Science Rathinam College of Arts and Science, Coimbatore-21

INTRODUCTION

This project is intended to develop a tool called Packet Sniffer. The Packet Sniffer allows the computer to examine and analyze all the traffic passing by its network connection. It decodes the network traffic and makes sense of it.When it is set up on a computer, the network interface of the computer is set to promiscuous mode, listening to all the traffic on the network rather than just those packets destined for it. Packet Sniffer is a tool that sniffs without modifying the network's packet in anyway. It merely makes a copy of each packet flowing through the network interface and finds the source and destination Ethernet addresses of the packets.It decodes the protocols in the packets given below:IP (Internet Protocol), TCP (Transmission Control Protocol), UDP (User DatagramProtocol).The output is appended into normal text file, so that the network administratorcan understand the network traffic and later analyze it.The main program will have an infinite loop which keeps an eye on each and every incoming packet. The moment it collects that packet it starts invoking respective modules andthose modules will internally redirects that information to respective Linux terminal The utilities used in this project are Linux Terminal using Command mode.This Project deals with a packet capture utility and Network monitoring. This Project is useful to the Network Administrators to observe each and every incoming packet for security enhancements.The Linux terminal is a text-based interface used to control a Linux computer. It's just one of the many tools provided to Linux users for accomplishing any given task, but it's widely considered the most efficient method available. Outside of writing code, it's certainly the most direct method possible.

OBJECT OF THE PROJECT:

The Linux terminal is a text-based interface used to control a Linux computer. It's just one of the many tools provided to Linux users for accomplishing any given task,but it's widely considered the most efficient method available. Outside of writing code, it's certainly the most direct method possible. It's so popular, in fact, that Apple changed its foundation to Unix and has gained the **Bash and Z shell**, and Microsoft developed PowerShell, its very own open source command line.A **command** is a special keyword you can use in a terminal to tell your computer to perform an action. Most commands are tiny little applications that get installed withthe restof your operating system. You may not realize they're on your computer becausethey're generally kept in relatively obscure directories like /bin, /sbin, /usr/bin, and/usr/sbin, but your terminal knows where to find them (thanks to something called the PATH). Other commands are built into your terminal. You don't have to worryabout whether a command was installed or comes built-in because your terminal knows the commands either way.

Development tools:

Python languages a set of development tools, including Pycharm Community Version and Linux Terminal a comprehensive class library for building web services and Terminal as well as the Common Language Runtime to execute objects built within this framework.

Web services:

An offering of commercial web services, recently announced as project Hailstorm; for a fee, developers can use these services in building applications that require knowledge of user identity.

Devices:

Python-enabled non-PC devices

The Python Platform:

PyCharm is the most well-known Python IDE, which offers fantastic featuresincluding superb code completion and inspection with a comprehensive debugger andcompatibility for web programming and several frameworks. .

PyCharm offers some of the best features to its users and developers in thefollowingaspects −

- Code completion and inspection
- Advanced debugging
- Support for web programming and frameworks such as Django and Flask

Security:

Computer networks let programmers share Pycharm code including Pythonprograms across the network. This collaborative effort lets you and your programming team creates python programs much more quickly than one person alone. The problem with collaborating over a network is that unauthorized users from within or outside your network may try togain access to your python program code. Visual Studio python provides built-in security features so you or the leader of your programming team can determine who on your networkgets access to your program code and resources. You can also set different levels of securityfor different people in case you want only certain people to have access to certain program code.

XML:

Extensible Markup Language (XML) is a more powerful version of Hypertext Markup Language (HTML), the standard Web page language. Visual Studio .NET and C# letyou document your program using XML and then extract the XML code into a separate file. Visual Studio .NET supports XML so that you can integrate your C# programs with the World Wide Web. You can document your C# code using XML and then use XML for creating Web Services and Web controls that let you and your code interact with a Web site.

<table>
<tr><td colspan="2">Version</td><td colspan="2">IHL</td><td colspan="3">Type of Service</td><td colspan="2">Total length</td></tr>
<tr><td colspan="3">Time to live</td><td colspan="3">Protocol</td><td colspan="3">Header checksum</td></tr>
<tr><td colspan="5">Identification</td><td colspan="4">Flags Fragment Offset</td></tr>
<tr><td colspan="9">Source Address</td></tr>
<tr><td colspan="9">DestinationAddress</td></tr>
<tr><td colspan="9">Options (+padding)</td></tr>
<tr><td colspan="9">Data (variable)</td></tr>
</table>

IP Subnet Addressing:

IP networks can be divided into smaller networks called sub-networks (or subnets).Sub-netting provides the network administrator with several benefits, including extraflexibility, more efficient use of network addresses, and the capability to contain broadcast traffic (a broadcast will not cross a router).Subnets are under local administration. As such, the outside world sees an organization as a single network and has no detailed knowledge of the organization's internal structure.A given network address can be broken up into many sub networks. For example, 172.16.1.0, 172.16.2.0, 172.16.3.0, and 172.16.4.0 are all subnets withinnetwork 171.16.0.0. (All 0s in the host portion of an address specifies the entire network.

Address Resolution Protocol (ARP) Overview:

For two machines on a given network to communicate, they must know the other machine's physical (or MAC) addresses. By broadcasting Address Resolution.Protocols (ARPs), a host can dynamically discover the MAC-layer address corresponding to a particularIP network-layer adAfter receiving a MAC-layer address, IP devices create an ARP cache to store the recently acquired IP-to-MAC address mapping, thus avoiding having to broadcast ARPS when they want to re-contact a device

In addition to the Reverse Address Resolution Protocol (RARP) is used to map MAC- layer addresses to IP addresses. RARP, which is the logical inverse of ARP, might be used by diskless workstations that do not know their IP addresses when they boot. RARP relies on the presence of a RARP server with table entries of MAC-layer- to-IP address mappings.

Internet Routing:

Internet routing devices traditionally have been called gateways. In today's terminology, however, the term gateway refers specifically to a device that performs application-layer protocol translation between devices. Interior gateways refer to devices that perform these protocol functions between machines or networks under the same administrative control or authority, such as a corporation's internal network.

Routers within the Internet are organized hierarchically. Routers used for information exchange within autonomous systems are called interior routers, which use a variety of Interior Gateway Protocols (IGPs) to accomplish this purpose. The Routing Information Protocol (RIP) is an example of an IGP.

Routers that move information between autonomous systems are called exterior routers. These routers use an exterior gateway protocol to exchange information between autonomous systems. The Border Gateway Protocol (BGP) is an example of an exterior gateway protocol.

IP Routing:

IP routing protocols are dynamic. Dynamic routing calls for routes to be calculated automatically at regular intervals by software in routing devices. This contrasts with static routing, where routers are established by the network administrator and do not change until the network administrator changes them.

An IP routing table, which consists of destination address/next hop pairs, is used to enable dynamic routing. An entry in this table, for example, would be interpreted asfollows:to get to network 172.31.0.0, send the packet out Ethernet interface 0 (E0).

IP routing specifies that IP datagrams travel through internetworks one hop at a time. The entire route is not known at the onset of the journey, however. Instead, at each stop, the next destination is calculated by matching the destination address within the datagram withan entry in the current node's routing table.

Each node's involvement in the routing process is limited to forwarding packets basedon internal information. The nodes do not monitor whether the packets getto their final destination, nor does IP provide for error reporting back to the source whenrouting anomalies occur. This task is left to another Internet protocol, the Internet Control-Message Protocol (ICMP), which is discussed in the following section.

Internet Control Message Protocol (ICMP):

The Internet Control Message Protocol (ICMP) is a network-layer Internet protocol that provides message packets to report errors and other information regarding IP packet processing back to the source. ICMP is documented in RFC 792.

ICMP Messages:

ICMPs generate several kinds of useful messages, including Destination Unreachable, Echo Request and Reply, Redirect, Time Exceeded, and RouterAdvertisement and Router Solicitation. If an ICMP message cannot be delivered, no second one is generated. This is to avoid an endless flood of ICMP messages..When an ICMP destination-unreachable message is sent by a router, it means thatthe router is unable to send the package to its final destination. The router then discards the original packet. Two reasons exist for why a destination might be unreachable. Most commonly, the source host has specified a nonexistent address. Less frequently, the router does not have a routeto the destination.Destination-unreachable messages include four basic types: network unreachable,host unreachable, protocol unreachable and port unreachable. Network- unreachable messages usually mean that a failure has occurred in the routing or addressing of a packet.

Host-unreachable messages usually indicate delivery failure, such as a wrong subnet mask. Protocol-unreachable messages generally mean that the destination does not support the upper-layer protocol specified in the packet. Port- unreachable messages imply that the TCP socket or port is not available.

An ICMP echo-request message, which is generated by the ping command, is sent by any host to test node reachability across an inter network. The ICMP echo- replymessage indicates that the node can be successfully reached.

An ICMP Redirect message is sent by the router to the source host to stimulate more efficient routing. The router still forwards the original packet to the destination. ICMP redirects allow host routing tables to remain small because it is necessary to knowthe addressof only one router, even if that router does not provide the best path. Even after receiving an ICMP Redirect message, some devices might continue using the less- efficient route.

The router sends an ICMP Time-exceeded message if an IP packet's Time-to- Live field (expressed in hops or seconds) reaches zero. The Time-to-Live field prevents packets from continuously circulating the internetwork if the internetwork contains a routing loop. The router then discards the original packet.

Transmission Control Protocol (TCP):

The TCP provides reliable transmission of data in an IP environment. TCP corresponds to the transport layer (Layer 4) of the OSI reference model. Among the services TCP provides are stream data transfer, reliability, efficient flow control, full- duplex operation, and multiplexing.

With stream data transfer**,** TCP delivers an unstructured stream of bytes identified by sequence numbers. This service benefits applications because they do not have to chop data into blocks before handing it off to TCP. Instead, TCP groups bytes into segments and passes them to IP for delivery.

The system has been tested and implemented successfully and thus ensured that all the requirements as listed in the software requirements specification are completely fulfilled.In case of erroneous input corresponding error messages are displayed.

No.	**Test case Title**	**Description**	**ExpectedOutcome**	**The requirement in RS that is being tested**	**Result**
1	Test the functionality of afile downloaded from internet	ser saves the file and views it later	File is saved	RS4	Passed
2	Test that GUI is able to show network traffic	Jser sees the traffic in graphical form.	Successful representation of traffic.	RS1	Passed
3	Test the mappingof files to the destination IP address	User views the destination IP address attached to each file.	Correct IP address is mapped to the file	RS2	Passed
4	Test the functionality of afile downloaded from internet	User opens the saved file for viewing it.	File is opened	RS5	Passed
5	Test the functionality of afile downloaded from internet	User prints the file.	The file is printedon the default printer.	RS6	Passed
6	Test the decoded information of the selected file.	User chooses from the list to view packet information.	The output isdisplayed correctly	RS3	Passed

Acknowledgment

This article / project is the outcome of research work carried out in the Department of **Computer Science** under the DBT Star College Scheme. The authors are grateful to the Department of Biotechnology (DBT), Ministry of Science and Technology, Govt. of India, New Delhi, and the Department of **Computer Science** for the support.

Conclusion

In practice, there is not a typical network problem that can’t be discovered and solved using packet sniffer technology. Sniffers can be used as the first method of attack on anumber of issues that vary from overloaded networks to unresponsive switches to lost packets.As a number of networks and nodes continue to grow and as network speeds accelerate, it becomes more and more difficult to monitor a LAN by using traditional tools, such as RMON(Remote Monitoring) probes. Packet sniffers, by contrast, monitor traffic on network right down to the Header information on each series of data. This means that u can actually track data from starting point to its end point. Packet sniffers can also be used to identify the types of packetson a network and discover whether or not the specific packet hasany errors.