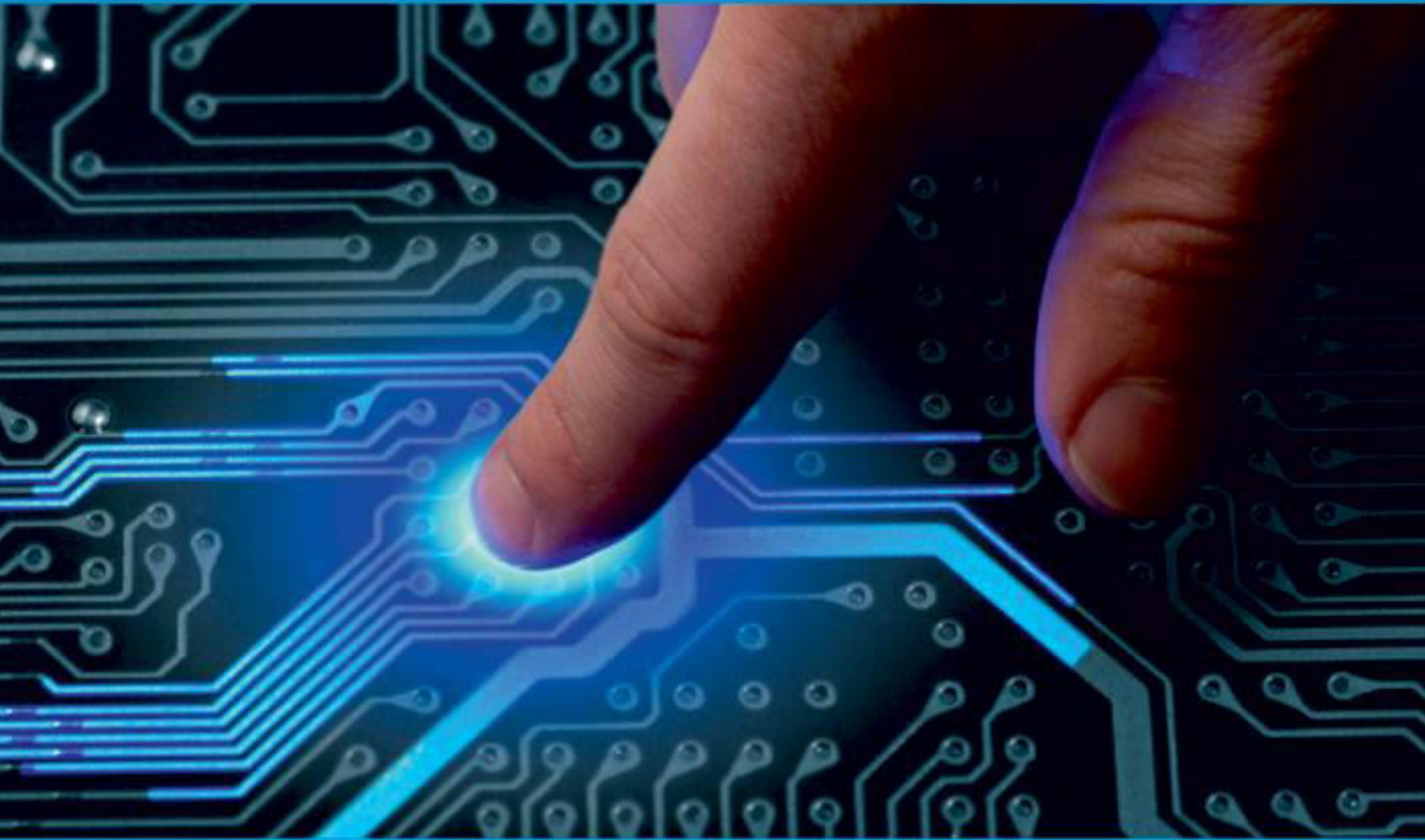
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 6, June 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006011 |

Network Traffic Analysis Using Wireshark

Sreepriya TS, Usha C

MCA Student, University BDT College of Engineering, Davangere, Karnataka, India

Faculty, Department of MCA, University BDT College of Engineering, Davangere, Karnataka, India

ABSTRACT: Nowadays the network performance has rapidly increasing due to the high availability of the resources that can be lead to increasing of the attackers in the society. Ensuring the security in the network is great deal. As the technology improves the attackers are also increasing to gain the information .The levels of the authentication are added to the information but still the security cannot be reached as to the extent. Securing the flow of packets through the network are also been done using the different algorithm such as CRC and etc. In network every layer has the problem such as phishing, deniel-of –service attack,virus, malware ,poisoning the network and etc. These are the serious issues that must be resolved and safeguard the network.

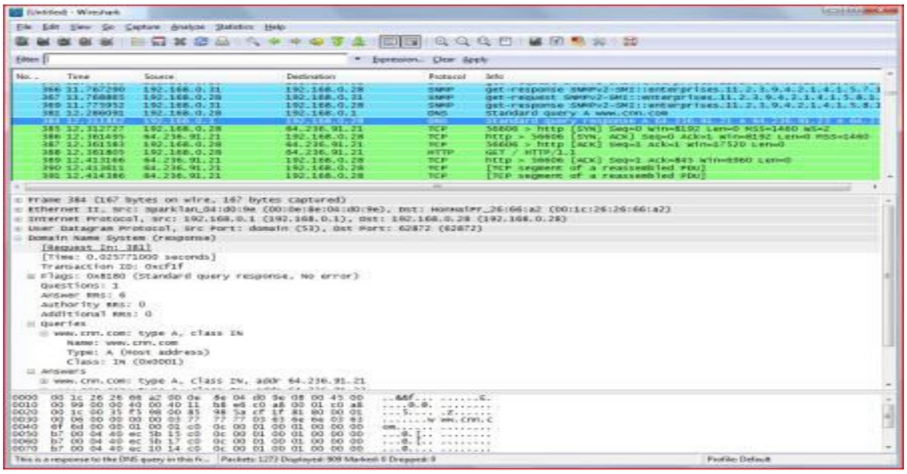
The necessary actions to be carried out to overcome the cyberattacks against your company or business .Regardless whether your company data is sent via electronic mail or stored in the hard disk can be also under the risk of cyber-attacks. To overcome the problem some of the tools such as wireshark can able to detect and analyse your network.

KEYWORDS: Network packet analyser, wireshark, LAN attack,DOS attack,ARP poisoning.

I. INTRODUCTION

Network traffic analyser is the process which includes capturing, filtering and analyzing the filtered traffic. Analyzing the network traffic can reveal the important information related to network devices activities, type of data shared between them, bandwidth utilization for such transfer and for detecting anomalies. Analyzing network traffic and detecting anomalies are the important tasks that need to performed at regular interval of time by security analysts. The large amount of traffic makes it difficult for the analyst to detect the anomalies in the network traffic. Need for such type of system to analyze network traffic arises as the number of network attacks are increased. The different types of network attacks are carried out to obtain the unauthorized data. Attackers nowadays hosting a websites which contains malicious code, which when accessed can steal the important information such as user login credentials from the user's system. Downloading the restricted content which is not legal and not proprietary which has copyright issues are the problems in the network systems. We need to trace such users to take correct actions against them. So need arises to develop such type of system which tracks the location of users.Wireshark is used as the main support tool to help detect and analyze the problems generated by these attacks. At the same time, different solutions to resolve each of these attacks are proposed.

II. OVERVIEW OF WIRESHARK TOOL AND CAPTURE OF PACKET


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No. .  Time        Source          Destination     Protocol  Info
  366 11.767290   192.168.0.31    192.168.0.28    SNMP      get-response SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.7.1
  367 11.768885   192.168.0.28    192.168.0.31    SNMP      get-request SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.8.1
  369 11.775952   192.168.0.31    192.168.0.28    SNMP      get-response SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.8.1
  381 12.286091   192.168.0.28    192.168.0.1     DNS       Standard query A www.cnn.com
  384 12.311187   192.168.0.1     192.168.0.28    DNS       Standard query response A 64.236.91.21 A 64.236.91.23 A 64.
  385 12.312727   192.168.0.28    64.236.91.21    TCP       58606 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
  386 12.361495   64.236.91.21    192.168.0.28    TCP       http > 58606 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
  387 12.361583   192.168.0.28    64.236.91.21    TCP       58606 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
  388 12.361805   192.168.0.28    64.236.91.21    HTTP      GET / HTTP/1.1
  389 12.413166   64.236.91.21    192.168.0.28    TCP       http > 58606 [ACK] Seq=1 Ack=843 Win=6960 Len=0
  390 12.413611   64.236.91.21    192.168.0.28    TCP       [TCP segment of a reassembled PDU]
  391 12.414386   64.236.91.21    192.168.0.28    TCP       [TCP segment of a reassembled PDU]

⊞ Frame 384 (167 bytes on wire, 167 bytes captured)
⊞ Ethernet II, Src: Sparklan_04:d0:9e (00:0e:8e:04:d0:9e), Dst: HonHaiPr_26:66:a2 (00:1c:26:26:66:a2)
⊞ Internet Protocol, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.28 (192.168.0.28)
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port: 62872 (62872)
⊟ Domain Name System (response)
    [Request In: 381]
    [Time: 0.025771000 seconds]
    Transaction ID: 0xcf1f
  ⊞ Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 6
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ www.cnn.com: type A, class IN
        Name: www.cnn.com
        Type: A (Host address)
        Class: IN (0x0001)
  ⊟ Answers
    ⊞ www.cnn.com: type A, class IN, addr 64.236.91.21

0000  00 1c 26 26 66 a2 00 0e  8e 04 d0 9e 08 00 45 00   ..&&f... ......E.
0010  00 99 00 00 40 00 40 11  b8 e6 c0 a8 00 01 c0 a8   ....@.@. ........
0020  00 1c 00 35 f5 98 00 85  98 5a cf 1f 81 80 00 01   ...5.... .Z......
0030  00 06 00 00 00 00 03 77  77 77 03 63 6e 6e 03 63   .......w ww.cnn.c
0040  6f 6d 00 00 01 00 01 c0  0c 00 01 00 01 00 00 00   om...... ........
0050  b7 00 04 40 ec 5b 15 c0  0c 00 01 00 01 00 00 00   ...@.[.. ........
0060  b7 00 04 40 ec 5b 17 c0  0c 00 01 00 01 00 00 00   ...@.[.. ........
0070  b7 00 04 40 ec 10 14 c0  0c 00 01 00 01 00 00 00   ...@.... ........
```

This is a response to the DNS query in this fr...
Packets: 1273 Displayed: 909 Marked: 0 Dropped: 0
Profile: Default

Fig .1 The overview of the wireshark tool.

To access the wireshark in your personal computer first we need to install the wireshark in the local machine using the wireshark.org with latest version. It is the one of the mostly network protocol analyser that captures the internet packetie,TCP-IP packets that goes through your network.We can install the wireshark in the windows,Linux .The activity of the packet can be seen in the window .The window shows the no of packets , time , source , destination and protocol with information. The IP address that shows the packet information and shows the source and destination with checksum, timestamp data with size and length etc these values are represented in X values that is present at the bottom of the wireshark tool. This tool also provides the wide range of filters over 1200 protocol.FormerlyEthereal, its prime objective is to provide network troubleshooting, analysis, and the networking research.The capturing of the packets are made through this tool. Wireshark can be installed be in user and connect hub between user and server so that the packets traffic can captured to user terminal.Remote packet capture can be used for capture remotely.ARPsnoofing is an offensive method of capturing the data in critcal situation this process can be done by infecting the cache of machine.

III.OTHER TOOLS FOR NETWORK TRAFFIC ANALYSIS

TCP DUMP

Tcpdump is a command line based packet capturing utility that can capture and monitor the network packets . It allows to sniff packets from all the layers of the OSI model from layer 1 to 7 that can be stored and analysed.It is a reliable tool to sniff the packets from the network.it is also used for the penetration testing. It is used for filtering that specifies the addresses, ports and TCP Flags.Tcpdump uses the libpcap library for packet capturing.Libpcap is the c or c++ based library that used for packet capture.

WIN DUMP

Windump is the windows version of the tcpdump that is used for unix system. It is also the command line network packet sniffer tool. It diagnose and saves the disk network packet analyser.windump uses winpcap library for packet capture. Winpcap library is for capturing the link layer network access in windows environment that includes the kernel level packet filtering and transmit packet bypassing in protocol stack.

AUVIK

Auvik is the network packet analyser that is used for deep analysing the packet traffic flow through the network.It allows us to to identify the user traffic a simple world map.It is a cloud based networking management it uses the tool Nmap to identify the host in network.

IV. METHODLOGY

Wireshark tool is installed in the operating system .The home page of the browser is set to blank and then opened the wireshark tool on the system and started capturing the packets.The tool consist of filters.These filter enables to view only data packets or protocols that are of interest to the user. The below to protocol list to view all packets being captured real time. These consist of protocol type, flag ,checksum, port etc.The tool we can find user network card in hexademimal format.

V. LAN ATTACK

To safeguard a LAN from the threats IT managers need to understand the where the attacks are from, these methods are been detected and potential risk they present to network. The most common types of attack along with the techniques are discussed as follows:

5.1 DDoS(Distributed Denial-of-service)ATTACKS:

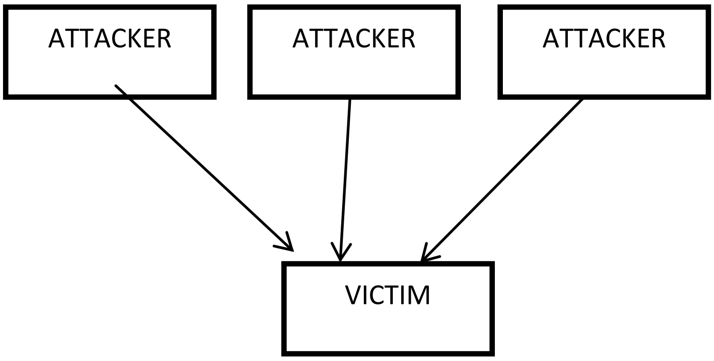


Fig2. Representing Dos attack

The main idea of DOS attack is making a certain services unavailable. Every service is in reality, running on a machine. The service can be made Unavailable if the performance on the machine can be brought down. Some DOS attack are executed by flooding the servers with connection request until the servers is overloaded and made it useless .Other are done by sending the unfragmented packets to the server which they are unable to handle.When many hosts coordinate to flood the victim with an abundance of attack packets, and the attack takes place simultaneously from multiple points it is called a Distributed DOS (DDoS) attack.A successful DDOS attack can damage the reputation of the brand and also huge financial loss. These attacks sometimes used for distracting cyber security operation such as data theft or network infiltration and so on.

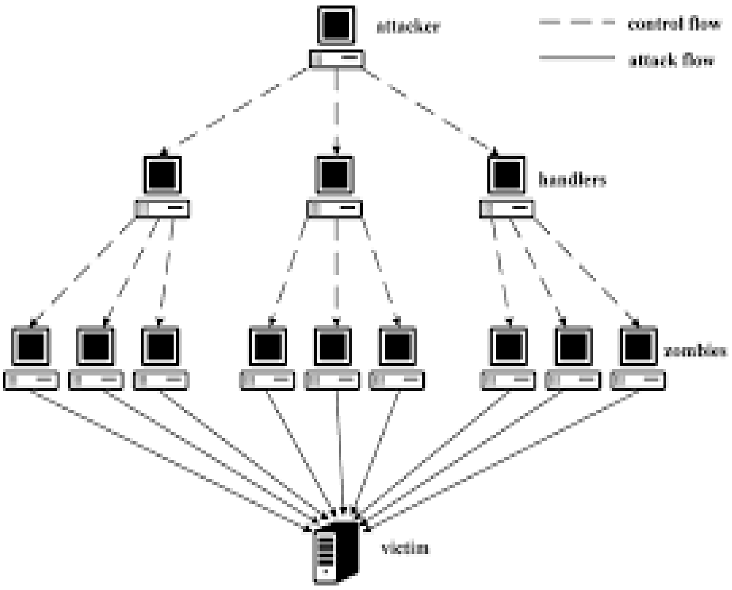


Fig 3. Representation of DDOS attack

UNDERSTANDING DDOS ATTACK

In wireshark, the packet sequence can be graphically seen by selecting from the menu Statistics ->Flow Graph. This tool enables to track the behavior of TCP connectionsIt illustrates, using arrows, the source and target of each packet, highlighting the active flags that interfere in the connection flow. It can be easily noticed that there is a short period of time when a number of connection attempts are made by the IP addresses for example consider IP address 10.0.0.200 to port 80 of machine 10.0.0.101. This is a rather suspicious scenario. The server has tried to resolve the MAC of the client many times, but when no acknowledgement is received, it cannot send an ACK-SYN to the same machine to continue the three-step handshake connection. Hence TCP/IP stack of server has to wait until it receive the connection.

During this idle time more packets keep arriving that trigger new connections. For each new connection TCB (Transmission Control Block) is created and used by the TCP/IP stack of the operating system to identify each connection.

Proposed Solution:
Based on our findings strengthen security against DDoS attack is important. They include: Every single user who accesses your router should be given a username and password. . Contacting the ISP seems the most appropriate action to monitor such attacks. Make sure you have RPF on the interface of every static connection. Use TACACS (Terminal Access Controller Access Control System) for password verification or Multiple factor authentication can be also used for security.

VI. CONCLUSION

Wireshark is one of thepacket sniffing software that are available today. In this paper we had discussed about packet analysing using this tool.Wireshark is a useful tool that offers countless functions that help to analyze multiple network problems.Packet sniffers like Wireshark can be a boon for network monitoring, but sometimes it is necessary to prevent packet sniffers from collecting sensitive information like passwords, in order to maintain security in the IT industry. This paper also discuss aboutDDoSattack . DDOS becoming a major component of a long term threat campaign and the level of attack automation has escalated.

VII. ACKNOWLEDGMENTS

Sincere thanks to Mrs.Usha C, Faculty of the Department of MCA for providing excellent laboratory facilities to carry out the experiment using wireshark listed under the paragraph “ METHODOLOGY’ .

REFERENCES

[1] Wireshark Documentation: http://www.wireshark.org/docs/wsug_html_chunked/inde x.html
[2] Stolze M, Pawlitzek R and Hild S (2009a) Task Support   for Network Security Monitoring. In ACM CHI Workshop on System Administrators Are Users, Too: Designing Workspaces for Managing Internet-Scale Systems.
[3] Madsen, P., Koga, Y., Takahashi, K.: Federated identity management for protecting users from ID theft Proceedings of the 2005 workshop on Digital identity management Fairfax, VA, USA (2010) 77-83
[4] Gouda, M.G., Liu, A.X., Leung, L.M., Alam, M.A.: Single Password, Multiple Accounts. Proceedings of 3rd Applied Cryptography and Network Security Conference (industry track), New York City, New York (2008)
[5] Riley, S.: Password Security: What Users Know and What They Actually Do. Usability News, Vol. 2006. Software Usability Research Laboratory, Department of Psychology, Wichita State University, Wichita (2009)
[6] 2010 18th IEEE Symposium on High Performance Interconnects Innovating in Your Network with OpenFlow: A Hands-on Tutorial
[7] IEEE 2008 publication: Bottleneck Analysis of Traffic Monitoring using Wireshark
[8] I. Kim, J. Moon, H. Y. Yeom, "Timer-Based Interrupt Mitigation for High Performance Packet Processing," in Proc. 5th International Conference on High-Performance Computing, (Asia-Pacific Region, 2011).
[9] J. Cleary, S. Donnelly, I. Graham, "Design Principles for Accurate Passive Measurement in Networks," in Proc. PAM2000 Passive and Active Measurement Workshop (Apr. 2000).
[10] Traffic Analysis with Wireshark, February 2011, Author: Borja Merino Febrer, The National Communications Technology Institute (InstitutoNacional de Tecnologías de la Comunicación - INTECO) Manuel Belda, from Valencia's Computer Security Incident Response Team (CSIRT-cv) and Eduardo CarozoBlumsztein from the ANTEL CSIRT of Uruguay. [14] Di Guangqun, Hu Guijang. “Development and implementation of packet sniffer”, CNKI: SUN: WJSJ.0.2009-21- 082.pp.1-5, 2009
IJCATM
[11] 2011 Fourth International Joint Conference on Computational Sciences and Optimization: Application Design of Data Packet Capturing Based on Sharpcap .
[12]Jideep Singh, SandeepDhariwal and Rajeev Kumar “A Detailed Survey of ARP Poisoning Detection and Mitigation Techniques” I J C T A, 9(41), 2016.
[13]SushmitaChakraborty, Praveen Kumar, Dr. BhawnaSinha “A Study on DDOS attacks, danger and its prevention” IJRAR E-ISSN 2348-1269, P- ISSN 2349-5138 ,2019

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.165

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

Scan to save the contact details

www.ijircce.com