Packet Sniffer to Sniff Sensitive Credentials Only

Author: Roshan Poudel

Abstract

The world has witnessed the extreme growth of internet penetration rate due to which packet sniffer are extensively used for monitoring the network. This paper is concerned with the development of the security tool "Secret Credentials Packet Sniffer" which sniff only the secret credentials flowing in network traffic. Secret credentials include username, cookie, password etc. The current scenarios regarding internet penetration and project as solution to those is also discussed. Moreover, the paper also elaborates the possibility of packet sniffing on widely used various networking protocol**.** Practical approach has been considered a high priority for which case study and proof of concept is demonstrated and evaluated. Furthermore, advantages , disadvantages and prevention measures of sniffing is also discussed. The paper is prepared after comprehensive research carried out from various sources like **IEEE, SANS**, research gate, google scholar etc. Finally, Nepal electronic act 2063 was followed as legal and ethical guidelines during the report.

Keywords: sniffing, packet, network, protocols, credentials

Abbreviations:

FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
OSI	Open Systems Interconnection
TCP	Transmission Control Protocol
UDP	User datagram Protocol
ICMP	Internet Control Management Protocol
SSL	Secure Socket Layer
POC	Proof of Concept

Table of Contents

Table of Figures

1.0 Introduction

Over the recent years the world has seen a subsequent growth in internet penetration rate. According to internet world stat, the global internet penetration rate is **53%** which continues to grow. With such growth , packet sniffers are extensively used to analyze and monitor the network.

Packet sniffer is the tool which can be a piece of software or hardware to monitor network**.** Packet Sniffing is technique used to monitor the packets that travel through the network. Packet Sniffer capture every packet that pass through it. Using the information captured by the packet sniffers an administrator can identify issue in the network and maintain efficient network data transmission. The security threat presented by sniffers is their ability to capture all incoming and outgoing traffic, including clear-text passwords, usernames or other confidential data. Network Protocols use network packets transmit information between nodes of the communication channel. Majority of network protocols like **HTTP** , **FTP** which transfer information in plain text are suspecible to packet sniffing attack. Since, network packet carry secret information cyber criminals search for secret information in packets and can manipulate packet data. So**,** encryption technology is used while transferring secret information over the networks. Packet Sniffing is often considered as insider threat by various organizations. The statistics below represent growth of internet users in Nepal (2074-75) extracted from Nepal telecommunication authority justifies the growth of internet users in Nepal.

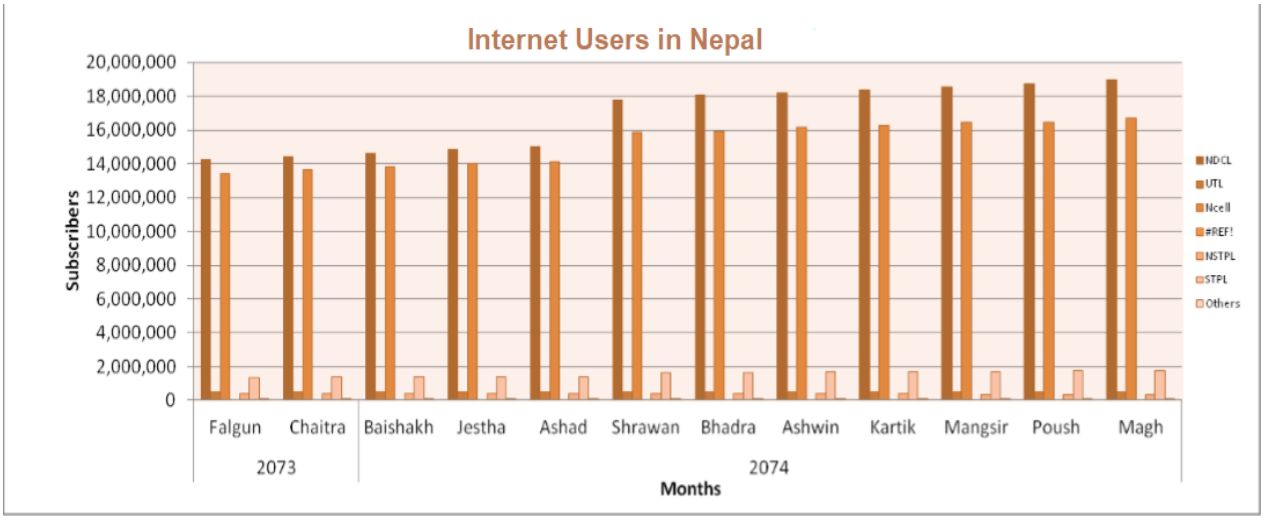


Figure 1: Growth of Internet Users in Nepal (src: Nepal Telecommunication Authority, 2018)

1.2 Problem Domain

According to Nepal telecommunication authority, Nepal's internet penetration rate is 63% as of 2018. With these increasing number, the responsibility of network monitoring has increased for network and security professionals. They are highly dependent upon the traditional packet sniffer tools like Wireshark, tcpdump. However, the data provided by such tools is very large and sometimes even network professional have difficult time to filter and get the required result. Also, these industry standard tools require sound knowledge of networking protocols which makes them unsuitable for laymen and end users.

1.3 Proposed Solution

After, reviewing some of the problems from diverse range of internet background, we can conclude that http protocol is excessively used in Nepal's internet space for transferring web credentials(shodan,2019). This definitely justifies that majority of end users are unknown about basic security concepts about the ssl and encryption. Similarly, majority of data provided by traditional packet sniffer are almost useless. In order to capture a basic cookie or password in network packets traditional tools provide data of whole seven layers. It is quite difficult to filter if the sniffers are operated for a long time to get secret confidential values. Hence, packet sniffer to sniff secret credentials can be a handy tool for network and security professionals either for troubleshooting or penetration testing purpose.

1.4 Aims and Objectives:

The primary aims of this paper is to develop advance sniffer to sniff secret credentials; unlike traditional tool that provide big chunk of data and consumes large time to filter required result.

1.4.1 Objectives

In order to conquer the aim some the objectives that will be followed are:

- Comprehensive study of networking protocols like **TCP, UDP, ICMP** etc. for the development of the sniffer.
- Intense research on packet sniffing from various sources like **IEEE**, **SANS**, research

gate to study relevant journals and research papers.

- Practical approach will be taken for which proof of concept and real time case study will be included as the part of the report.
- Critical evaluation of advantages ,disadvantages and prevention of packet sniffing will be performed.
- *"Nepal electronic act 2063"* will be taken into legal and ethical consideration during the development of the security tool *secret credentials sniffer*.

Chapter 2: Background and Literature Review

2.1 In Depth: Packet Sniffer

Packet sniffer is a program running in a network attached Device that passively receives all data link layer frames passing through the device's network adapter. It is also known as Network or Protocol Analyzer or Ethernet Sniffer. The packet sniffer captures the data that is addressed to other machines, saving it for later analysis. It can be used legitimately by a network or system administrator to monitor and troubleshoot network traffic. Using the information captured by the packet sniffer an administrator can identify erroneous packets and use the data to pinpoint bottlenecks and help maintain efficient network data transmission. The security threat presented by sniffers is their ability to capture all incoming and outgoing traffic, including clear-text passwords and usernames or other sensitive material. In theory, it's impossible to detect these sniffing tools because they are passive in nature.

(Pallavi Asrodia, 2012)

Applications of packet sniffing program :

- Logging network traffic. Solving communication problems (either the system or the transmission medium.)
- Analyzing network performance. This way the bottlenecks present in the network can be discovered, or the part of the network where data is lost can be found.
- Detecting network intruders

(Nimisha P, 2014)

2.3 Case Study

2.3.1 Troubleshooting IP Phone Service with Packet Sniffing

This case study is related to troubleshooting the ip phone service with packet sniffing**.** A customer using an IP phone service at a call center reported that calls would suddenly be disconnected several times a day during peak calling periods**.** The problem persisted despite replacing the VoIP gateway**.** Network Professionals checked calling conditions using the captured-data analysis support tool and found that the event would typically occur when the number of calls had risen dramatically, which occurred just after 10:00 AM. Hence**,** it is considered the possibility that the non-transmission of RTCP packets from the VoIP gateway was related in some way to the large number of calls.

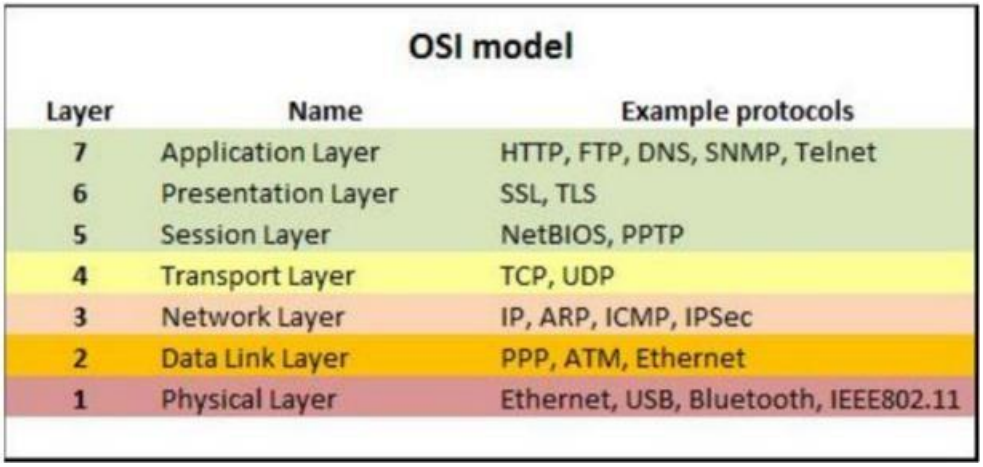
(NTT Technical, 2015)

2.3.1 Analysis of Case Study

The practical implementation of packet sniffing in real time scenario was elaborated above. The problem in the ip phone which was solved by trouble shooting the network. Packet Sniffers were uses during the phase of trouble shooting. While troubleshooting RTCP packets were captured and the issue was identified. The identification of problem and issue present in VOIP calls was facilitated by Packet Sniffing technique. Packet Sniffing can be used in more complex scenarios like wise.

2.4 Open Systems Interconnection Model (OSI Model)

OSI model is theoretical strategy that describes how the data and information goes across the internet . It is composed of seven sub layers which govern the protocols and network devices. The model operates from the top as application layer and ends to physical layer. The various protocols either the web protocols like HTTP, FTP or network protocols like ARP operate depending upon the principle of OSI Model. The original objective of the OSI model was to provide a set of design standards for equipment manufacturers so they could communicate with each other. The OSI model defines a hierarchical architecture that logically partitions the functions required to support system-to-system communication.



OSI model		
Layer	Name	Example protocols
7	Application Layer	HTTP, FTP, DNS, SNMP, Telnet
6	Presentation Layer	SSL, TLS
5	Session Layer	NetBIOS, PPTP
4	Transport Layer	TCP, UDP
3	Network Layer	IP, ARP, ICMP, IPSec
2	Data Link Layer	PPP, ATM, Ethernet
1	Physical Layer	Ethernet, USB, Bluetooth, IEEE802.11

Figure 2: Hieratical of OSI Model (src: oracle, 2018)

The basic functionality of OSI layers are as follows **:**

7. Application: It Provides different services to the application and interact with the user. Web protocols like http, ftp operate in this layer.

6. Presentation: Converts the information to various encoding and encryption methods. This layer is inclined with the syntax and semantics of the information transmitted.

5. Session: Handles problems which are not communication issues to maintain persistence session.

4. Transport: Accepts data from session layer and provides end to end communication control.

3. Network: Control operation of subnet, facilates routing congestion , control and accounting.

2. Data Link: Provides error control. Majorly deals with LAN protocols.

1. Physical: Connects the entity to the transmission media

2.4.1 Packet Sniffing with respect to Networking Protocols

Network Protocols operate in various layers of OSI Model. Networking protocols are used for communication and transferring information into various nodes of the network**.** Network Protocols rely upon network packets for transferring information and credentials. Hence, Network Packets are key targets of packet sniffing programs. Various networking protocols have different mechanism for transferring information. Some of the application layer protocols like http, ftp, telnet transfer the information and credentials in plain text. This

makes these protocol suspecible

to packet sniffing attack**.** An attacker can launch various attacks like ARP spoofing to capture credentials that are transferred in plain text. At such, the confidentiality and integrity of information is completely disturbed as s/he can manipulate and bring amendment in the data. Presentation layer protocols ssl, tls, converts information into various encrypted text . with combination of protocols from application layer and presentation layer like https, ssh transfer credentials in encrypted form which makes them resistant to packet sniffing attack. These networking protocols implement cryptographic algorithm to convert information into encrypted cipher which prevents sniffing attack. Some of the protocols are secure version over their unsecure protocol. Example, https over http, ssh over telnet etc. Finally, to maintain confidentiality, integrity and availability of information, encrypted and secure protocols should be always be used that transfer information in encrypted text.

2.5 Advantages of Packet Sniffer

- Network Professional use it to troubleshoot network and security professional use it in penetration testing purposes.
- Students use them for educational purpose in academics.

2.6 Disadvantages of Packet Sniffer

- Cyber Criminals use them to sniff for secret credentials and disrupt confidentiality and integrity of network packets.
- Sniffer can corrupt the packet data which impacts integrity of information shared**.**

2.7 Proof of Concept on HTTP Protocol of Application Layer:

In this section the practical demonstration of sniffer program is performed. For this purpose , a site without **SSL** is hosted in local host. Authentication Credentials are entered, and sniffer program was successful in sniffing the secret credentials only. Some dependencies of program are:

S.N	Purpose	Tool
1	Operating System	Elementary OS

2.	Programming language	Python

Phase 1:

In this phase the sniffer program is operated to examine all the incoming and outgoing secret credentials that transfer in plain text. These secret credentials could be username, email, passwords, token , hash etc. They can be provided by user with proper regular expression.

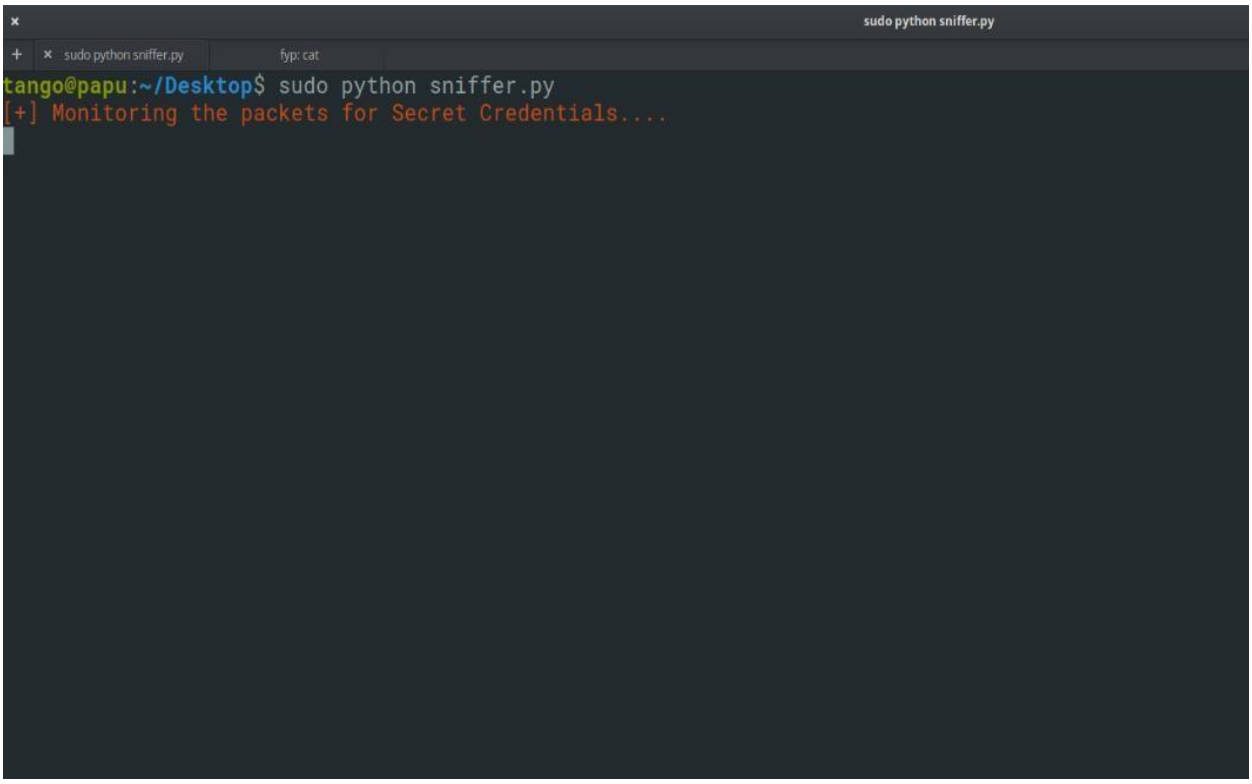


Figure 3: Packet Sniffer running in background

Phase 2:

The website without SSL was hosted in localhost. Secret Authentication Credentials are entered in it which obviously travels in plain text due to absence of https. The sniffer program is active in background and continuously monitoring each single packet for secret credential that are passing through computer**.**

Figure 4: Entering credentials in http website (hosted in localhost)

Phase 3:

In this phase , the performance and working of sniffer program is demonstrated. Since the secret credentials are entered into the website each single packet was monitored by program. As, soon as the program discovers the username and password travelling in plain text, it ejects the result with the time of capture and other useful information**.** The program captures other credentials like cookie, session id with regex match provided

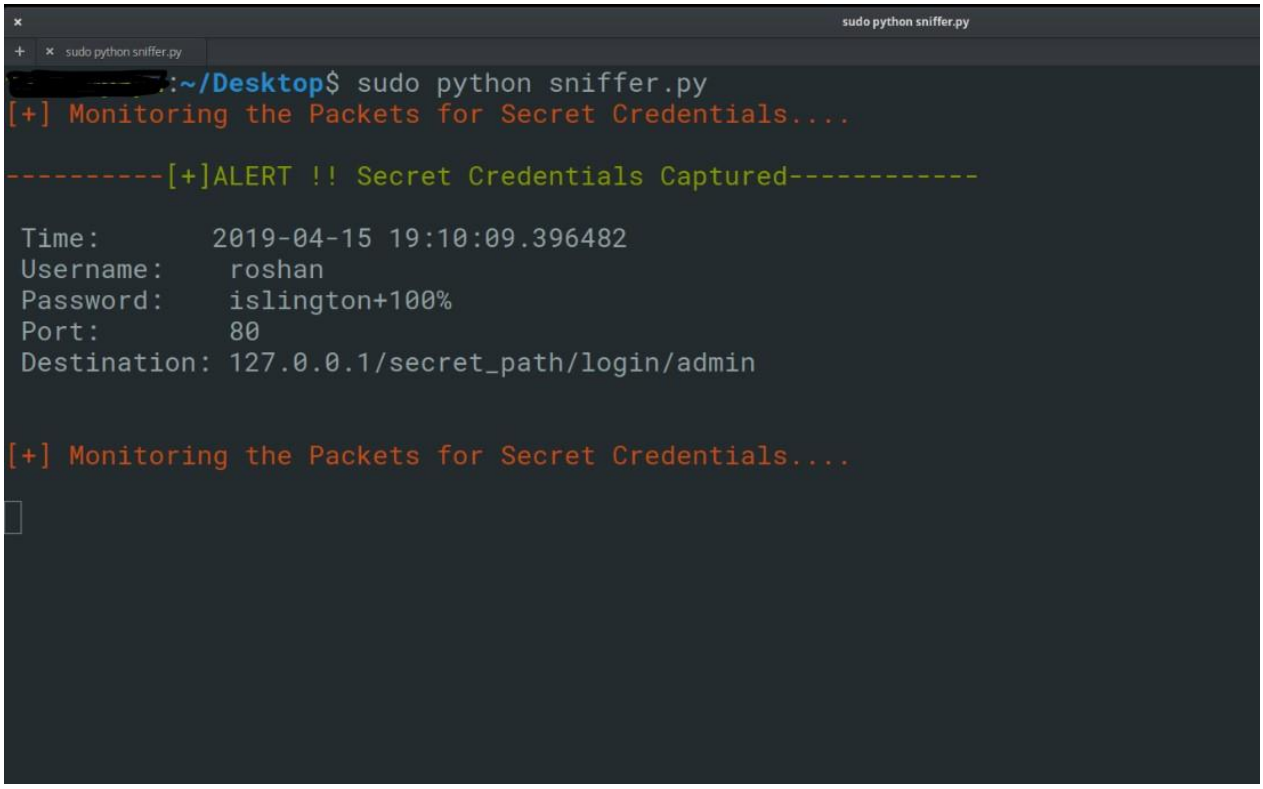


Figure 5: : Capture of secret credentials by python script

2.8 Prevention against Packet Sniffing

Packet Sniffing is serious issue and encryption stand with us in this regard.

Prevention mechanisms are:

- All the secret and confidential information should only be transferred via secure channel. Using HTTPS, the secure version of HTTP, will prevent packet sniffers from seeing the traffic on the websites we are visiting.
- One effective way to protect from packet sniffers is to tunnel connectivity with virtual private network VPN. A VPN encrypts the traffic being sent between computer and the destination.

Chapter 3: Conclusion and Further Work

3.1 Conclusion

Network packet sniffers are an integral part of the layered defense model. Packet sniffer are handy tool can be used for genuine as well as malicious purposes. The consequences depend for which purpose they are used in. It can be used for network traffic monitoring, traffic analysis, troubleshooting and educational purposes as well as attacking purposes also. It can also be used by attackers in order to steal plaintext data or eavesdropping on user's actions. Some measures can be taken during implementation of the protocols to assure that they are not used for unintended purposes. Similarly, case study proved that packet sniffing Finally, this paper delivered practical operation of packet tracer along with preventions measures of packet sniffing.

3.2 Further Work

The future work in the project is concerned on advancing the packet sniffer. Some of the key areas of investigation and development are ability of packet sniffer to operate in ipv6 and ability of sniffer to decrypt the encrypted traffic after the encryption keys are provided. The program will be released in GitHub under public license and contribution, feedbacks are highly appreciated. Availability, of this paper in research gate provides excellent environment for future researchers in this topic domain.

Chapter 4: Social, Legal and Ethical Guidelines

4.1 Social Issues

The components in the report avoid any information that have the potential found to be offensive or harmful for the readers. The information on the report is suitable for all interested readers and does not have age restrictions. Consequently, with wide angle of topic domain it addresses to aware community about security prospects of systems we use. However, for the security aware personalities this report does not aim to bring violence in the name that packet sniffers can violate our privacy.

4.2 Ethical Guidelines

All the ethical guidelines and law of the London metropolitan university is strictly followed during the investigation of this paper. The research papers are consulted from all the legitimate sources

authored by famous and intellectual personalities. During the proof of concept, the packet sniffing was carried on my personal network within my devices. Further assure that no-one was made victim during the POC Phase. This report will be release with General Public License means anyone in the future can use this research paper for their investigation.

4.3 Legal Guidelines with respect to Nepal Electronic Act 2063

Nepal Electronic Act **2063** states, "If any person knowingly and with a malicious intention to cause wrongful loss or damage to any institution destroys, damages, deletes, alters, disrupts any information of any computer source by any means, such a person shall be liable to the punishment with the fine not exceeding two thousand Rupees and with imprisonment not exceeding three years or with both.". These guidelines are strictly followed during the paper:

- Nobody's information or data was accessed, damaged during the proof of concept.
- The provision of this paper is only for educational purpose. Author is not responsible if used for any kind of unintended purposes in future.
- Monitoring the personal host machine network is not illegal and is part of personal data security.

Chapter 5: References and Bibliography

5.1 References

1. Miller, R. (2019). *The OSI Model: An Overview.* SANS Institute., Page(s):5-12

2. Nimisha P, R. G. (2014). *Packet Sniffing: Network Wiretapping.* IEEE International Advance Computing Conference.

3. Pallavi Asrodia, H. (2012). *Network Traffic Analysis Using Packet Sniffer .* International Journal of Engineering Research and Applications .

4. Magers Daniel.(2002). *Packet Sniffing: An Integral Part of Network Defense* ,SANS Institute

5. Qadeer M.A., Zahid M., Iqbal A., Siddiqui M.R "*Network Traffic Analysis and Intrusion Detection Using Packet Sniffer*" ICCSN '10 Second International Conference, 2010, Page(s): 313 - 317

6. A. Dabir, A. Matrawy, "*Bottleneck Analysis of Traffic Monitoring Using Wireshark", 4th International Conference on Innovations in Information Technology,* 2007, IEEE Innovations '07, 18-20 Nov. 2007, Page(s):158 – 162

7. Rupam, Atul Verma, Dr, and Ankita Singh. "An Approach to Detect Packets Using Packet Sniffing." International Journal of Computer Science & Engineering Survey (2013): n. page. Web.

8. Nucci A & Papagianaaki, K (2009). *Design, Measurement and Management of Large-Scale IP Networks*

9. Sanders, C., & Smith, J. (2014). *Applied Network Security Monitoring*

10. Protocol Layers and the OSI Model [2018] , Online

Available at https://docs.oracle.com/cd/E19455-01/806-0916/ipov-7/index.html

Accessed on [2019.04.28].

11. Nepal Internet Penetration Rate MIS Report [2018] [Online]

*Available at https://nta.gov.np/wp-content/uploads/2018/04/MIS_Magh_2074.pdf [*Accessed on 2019/4/14]

5.2 Appendix

Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol.4, No.4, 2013

Network Traffic Analysis: A Case Study of ABU Network

SB .A. Mohammed
Department of Electrical and Computer Engineering, ABU, Zaria, Nigeria

Dr.S.M Sani
Senior Lecturer, Department of Electrical and Computer Engineering, ABU, Zaria, Nigeria

Dr. D.D. DAJAB
Director ICT, ABU Zaria
Electrical and Computer Engineering, ABU, Zaria, Nigeria

Abstract
The Internet is being viewed as a critical component of success by the researchers, teachers and students in the Universities and Colleges. The Objectives of thesis is to identify unproductive network based applications responsible for consuming valuable bandwidth of University network system and to enhance utility of productive applications on a University network. This research work, geared towards analysis on the internet traffic network's of Ahmadu Bello University (ABU), Zaria as a case study. the monitoring of network traffic was conducted by bandwidth monitoring software, a packet sniffer (using Wireshark Version 165, SVR Rev 40429) configured as a gateway between the University network system and the internet over a 90-day monitoring period in a schedule of 15 minutes daily, 30 minutes weekly and 2 hours monthly. The data (packets) captures was further analysed using MATLAB which is a tool for graphing network data from which conclusions from the graphs was drawn that ABU's current network traffic is underutilized and far from optimal in terms of Internet Inbound/Outbound traffic generated by its users (staff/students). It has also been observed that defensive bandwidth management is insufficient in respect to the institution's aims and objectives on its network usage. This emphasises the need for improved bandwidth management and optimization.
Keyword: Network monitoring traffic, Monitoring software (packet sniffer), Packet capture and Traffic analysis.

1. Introduction

The rapid growth of the Internet in size, complexity and traffic types has made network management a challenging task. The ability of a monitoring system to provide accurate information about the nature and type of the network traffic cannot be over emphasized. Information about who is generating the most traffic, what protocols are in use, where is the traffic originating from or where is the destination of the traffic can be very important to solving congestion problems. Many network administrators spend a lot of time trying to know what is

Packet Sniffing: What it's Used for, its Vulnerabilities, and How to Uncover Sniffers

Mathurshan Vimalesvaran
Tufts University

Abstract

Packets are the base of all data sent on the internet, yet they are often used insecurely. Tampering with live packets and the process it takes in order to alter packets traveling along the network are getting easier. Current exploits that attackers use are easily attainable by even novice attackers. There is a range of different packet scanning techniques used for sniffing. The purpose of this paper is to explain the nature and of packets and expose the vulnerabilities that attackers exploit. This paper also covers practices set in place to protect against packet manipulation and sniffing, and detection of sniffers on a network.

I. Introduction

Packet sniffing is commonly described as monitoring packets as they go across a network. Packet sniffers are typically software based, but can be hardware pieces their own network. For example, if a computer is having problems communication with another computer, an administrator can view the packet from one machine to the other machine and determine the cause of the issue.

The security risk appears when an adversary uses a sniffing tool to collect plaintext sensitive material such as passwords. Sniffers are, for most organizations, an internal threat [7].

II. To the Community

I chose to write on this topic, because packets are the underlying mechanism in how machines communicate and therefore it is important to understand how they work and the vulnerabilities related to them.

There was a lot of work done in securing data sent over the wire and there is a lot to learn in this area. It is vital to know how our data is being handled and interpreted in

International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.3, June 2013

An Approach to Detect Packets Using Packet Sniffing

Rupam[1], Atul Verma[2], Ankita Singh[3]

Department of Computer Science, Sri Ram Swroop Memorial Group of Professional Colleges Tiwari Gang Faizabad Road, Lucknow, Uttar Pradesh, India.

[1]rupamsrvstv@gmail.com
[2]atulverma16@gmail.com
[3]ankitasingh9126@gmail.com

ABSTRACT

In the past decades computer network have kept up growing in size, complexity and along with it the number of its user is also being increased day by day. Hence the amount of network traffic flowing at each node has increased drastically. So to keep a track on these nodes a packet sniffer is used. Sometimes a packet sniffer is called a network monitor or network analyzer. Many system administrator or network administrator use it for monitoring and troubleshooting network traffic. Packet sniffers are useful for both wired and wireless networks. The purpose of this paper is to show the basics of packet sniffer, how it works in both switched and non switched environment, its practical approach, its positive vs negative aspects and its safe guards.

KEYWORDS

Network monitor, switched environment, non switched environment, promiscuous mode, spoofing and intrusion.

1. INTRODUCTION

Packet sniffing is defined as a technique that is used to monitor every packet that crosses the

5.3 Codes:

```
from scapy.all import
* import time
import datetime
G = '\033[92m' #
green Y = '\033[93m' #
yellow B = '\033[94m'
# blue
```

```
R = '\033[91m' # red
W = '\033[0m' #
white
current_time=datetime.datetime.today()
def sniff_for_secret_credentials(packet):
        a=open('secret_text.txt','r').readlines()
        if packet:
                print('%s[+] Monitoring the Packets for Secret Credentials. '%R)
                print(" ")
                time.sleep(6)
                print('----------%s[+]ALERT !! Secret Credentials Captured -------'%G)
                print(" ")
                print('%s Time:     '%W  +     str(current_time))

                print('Username:  ' + packet['Username'] or packet[a])
                print('Password:  ' + packet['Password']or packet[a])
                print('Port:      ' + str(packet.dport))
                print('Destination:' +
                                        packet[IP].dst
                ) print('\n')

sniff(prn=sniff_for_secret_cr
```
edentials)