An Approach to Sniff Sensitive Information by Packet Sniffing

Dr. Dayanand Lal N
Assistant Professor
Department of Computer Science and Engineering
GITAM, Deemed to be University, Bengaluru, Karnataka, India

Mr. Parikshith Nayak
Assistant Professor
Department of Computer Science and Engineering
GITAM, Deemed to be University, Bengaluru, Karnataka, India

Mrs. Veena R C
Assistant Professor
Department of Computer Science and Engineering
GITAM, Deemed to be University, Bengaluru, Karnataka, India

Dr. Brahmananda S.H
Professor
Department of Compute Science and Engineering
GITAM, Deemed to be University, Bengaluru, Karnataka, India

Mrs. Sahana D S
Assistant Professor
Department of Computer Science and Engineering
GITAM, Deemed to be University, Bengaluru, Karnataka, India

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 sniffs 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 are 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 are 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

I. 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 screen the network. Packet Sniffer is the device that can be a network surveillance program or hardware. Packet sniffing is the method used to track network transport packets. Every packet moving through it is detected by Packet Sniffer. The administrator will detect network problems and ensure secure network data transfer by means of the information gathered by packet snippers. Sniffers protection

vulnerability resides in the potential to monitor all incoming and outgoing messages, including passwords, usernames or other sensitive material. 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 progress of internet users in Nepal (2074-75) extracted from Nepal telecommunication authority justifies the progress of internet users in Nepal.

The rest of the paper is organized as follows. Background and Literature Review II. Problem Definition is presented in section III. Proposed Solution are given in section IV. Aim and Objectives are given in section V. Case study explained in section VI. Conclusion and Future work are given in section VII.

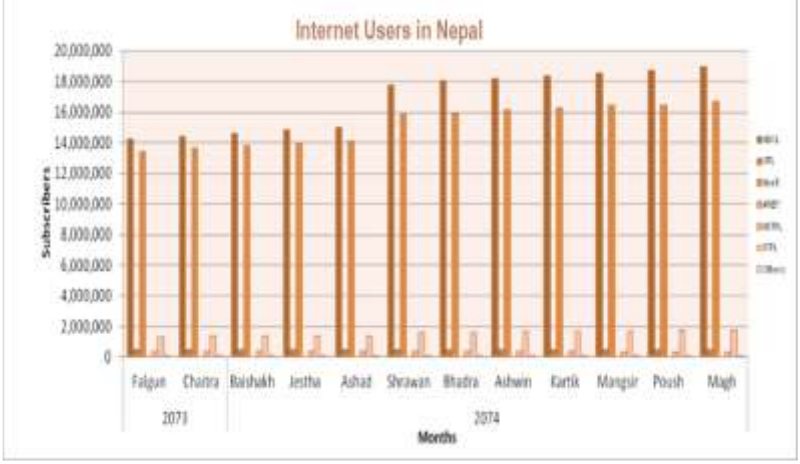


Figure 1: Growth of Internet Users in Nepal

II. BACKGROUND AND LITERATURE REVIEW

Packet Sniffer is a networked computer application that passively accepts frames of all data-linking layers moving via the network adapter of a system. This is also known as the Ethernet Sniffer or Network Analyzer. The packet sniffer gathers and stores data for further study that is forwarded to other computers. This can be legally used to track and address network traffic by a network or device administrator. Using the data gathered from the packet sniffer, a director is able to detect incorrect packets and use them to locate bottlenecks and ensure a secure transfer of network traffic. Sniffers protection risks consist of their ability, like passwords and usernames or other confidential material to catch all incoming and outgoing traffic. In principle, since they are inactive in design, it is difficult to detect this sniffing device.(Pallavi Asrodia, 2012)

2.1 Applications of packet sniffing program

- Logging data throughout the network. Solving connectivity challenges (both machine and transmitting media). Connectivity issues.
- Network output review. Therefore, it is possible to locate the bottlenecks in a network or identify the portion of the network through which data was missing.
- Detecting network intruders. (Nimisha P, 2014)

III.PROBLEM DEFINITION

According to Nepal telecommunication authority**,** Nepal's internet penetration rate is 63% as of 2018**.** With this 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 Wire shark, tcp dump**.** 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.

IV.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.

V. AIM AND OBJECTIVES

The primary aim 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.

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

- Comprehensive study of networking protocols like TCP, UDP, and 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.

VI. CASE STUDY

6.1 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.

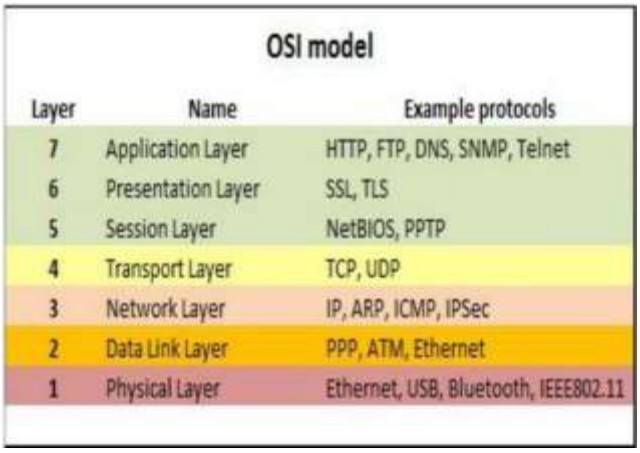
6.2. *Analysis of Case Study*

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.

6.3. Open Systems Interconnection Model (OSI Model)

OSI model is theoretical strategy describes how 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 OSI Model was initially designed to provide device manufacturers with a collection of design specifications for contact. The OSI model describes an architectural framework which logically partitions the functions needed to facilitate 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

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 operates 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, facilities 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

6.4 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, and 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.

1) 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) 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**.**

6.5 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:

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 rejects the result with the time of capture and other useful information**.** The program captures other credentials like cookie, session id with regex match provided.

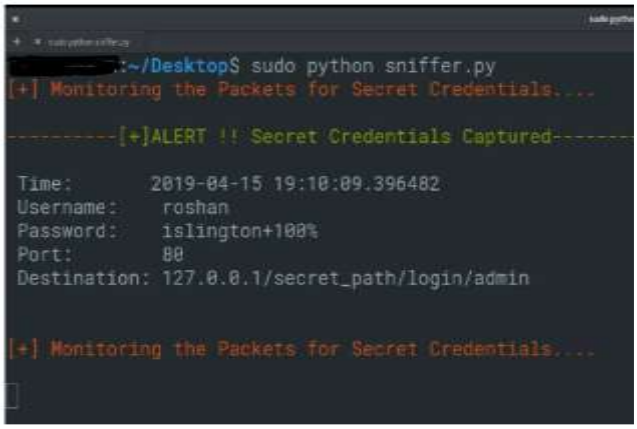


Figure 5: Capture of secret credentials by python script

6.6 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 encrypted HTTP standard, stops packet sniffers from accessing the data on the domains we use.

- Another efficient means of defending from packet sniffers is to tunnel access via VPN virtual private network. A VPN encrypts the communication between your device and the destination.

6.7 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.

- 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.

6.8 *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 have being 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.

VII. Conclusion and Future Work

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. This may also be used for network traffic control, data processing, troubleshooting and instructional purposes, and also for purposes of attack. It may also be used by attackers to capture plaintext data or search user behavior. 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. 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**.**

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].