International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 04 | Apr 2021 www.irjet.net p-ISSN: 2395-0072

NANO SNIFFER - Network Security & Reconnaissance Framework

Ameya Surve[1], Jobi Mathew[2], Shreya Vettiyatil[3], Vivek Vaishya[4]

[1-4]*Student, Dept. of Computer Engineering, PCE, Navi Mumbai, India - 410206*

Abstract- *Network Security is a serious concern in all organisations, leading to loss in resources. Such cases are not easy to deal with, due to the lack of time and resources available. Software solutions available are difficult to set up in an online environment. The Packet Sniffer proposed sniffs and spoofs packets passing through a network and analyses them for detecting network intrusion attempts on the same network or on other network users and critical servers and collects sensitive information such as server to server communications or performing penetration testing to test infrastructure and network security. This helps you target new resources when expanding your network capacity, manage your bandwidth, ensure delivery of business services, enhance security, and improve end-user experience. Nano Sniffer has the ability to perform both sniffing in combination with spoofing which gives the advantage in security testing for organisation's networks as well as foreign networks. It can be used directly with a network switch to perform DHCP spoofing to test security functionality of the switch.*

Keywords- *DHCP spoofing, sslstrip module, HTTPS traffic, Arp spoof, DNS spoof, Raspberry Pi Zero W*

I. INTRODUCTION

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 the network. Packet Sniffing is a technique used to monitor the packets that travel through the network. Using the information captured by the packet sniffers, an administrator can identify issues 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 to transmit information between nodes of the communication channel. Majority of network protocols like HTTP , FTP which transfer information in plain text are susceptible to packet sniffing attacks. Since, network packets 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 an insider threat by various organizations.

II. LITERATURE SURVEY

A. Discussion of suspicious activities in network traffic

NEEDHAM and Lampson(2014) acknowledge that IP is the most popular networking protocol that is used by most devices in a networked environment. Owing to the nature of operation of the IP protocol where it does not provide authentication services or confidentiality, most attacks can emanate from this vulnerability and compromise the network or the systems in the network. These attacks can be launched from within the LAN or be within the WAN.

i) Attacks on Local Area Networks

This kind of attack requires the victim machine to be powered off so that they cannot be alerted when this theft of identity happens. Either attackers can be patient enough to execute this or they can decide to launch another attack that forcefully brings down the victim's machine.

ii) Attacks that take advantage of WAN connections

Servers are the target for these kinds of attacks. Message redirecting in networks is also an activity that goes on silently without the administrator noticing there is an attacker, effectively saying,"You should have sent this message to the other gateway instead".

iii) The broad umbrella of DDoS attacks

DDoS attacks are an extrapolation of Denial of Service attacks (Visbal, 2015). As much as DoS prevents legitimate users from using a system, DDoS will do the same thing but the method of deployment is what sets these attacks apart.

B. Existing techniques used to detect suspicious activities in network traffic

An anomaly detection technique in networks refers to the problem of finding exceptional patterns in network traffic that do not conform to the expected normal behaviour. Detection of anomalies is moving from the manual process where the security analysts are required to continuously audit network activities and make sound judgments when detecting network outliers. Network anomaly detection techniques that Bhuyan et al. (2014) broadly discusses in his work can be categorized into four classes. They are statistical, classification-based, clustering and outlier-based. A statistical method usually bases its aberration detection procedure by looking at activities from a given data set that have a low probability of being generated. Applying statistical inferences, the technique can then decide if the activity belongs to the statistics model or not.

C. System developed for detecting suspicious activities in network traffic

Minnesota Intrusion Detection System (MINDS) employs the use of data mining to detect network intrusion (Ertoz et al., 2005). It collects data through flow tools that act as its input, the system then looks at the packet header information and builds a one-way session to the flows. Integrating ElasticSearch and Kibana (ELK stack) and packet capturing applications like Wireshark in doing real time network analysis Kibana is a web interface for Elasticsearch.

D. Summary of Related Work

The summary of methods used in literature is given in Table 1.

Table 1 Summary of literature survey

Literature	Advantages and Disadvantages
Roshan Poudél	Advantages: SecretCredentials Packet Sniffer Disadvantages: Doesn't monitor the whole network
Henry N. O. and Agana M.	Advantages: Sniff packets in LAN, at IP, MAC layer from switch, limited HTTP packets Disadvantages: Only analysing small
Ahsan N., Ahsan W. and Sirajuddin Q.	Advantages: Passive network monitoring for LAN, Uses ntop apart from usual Wireshark, Analysis on Application layer protocols Disadvantages: Only Software solution
Nimisha Patel, Rajan Patel, Dr. Dhiren Patel	Advantages: Discusses potential use of Sniffing on non-switched networks, Also discusses AntiSniff to detect sniffers on network Disadvantage: The research is quite old and doesn't stand to today's standard

III. SYSTEM ANALYSIS AND METHODOLOGY

A. Proposed Work

It can be used directly in the network switch to perform DHCP spoofing to test security functionality of the switch. It uses various modules such as ARP spoof, DNS spoof etc to sniff the entire network.Reliable because of its portability and automation.It is implemented on hardware which makes itself a standalone hardware sniffer which can be used anywhere in the entire network or other places to perform security testing.

B. System Architecture

The system architecture is given in Figure 1.

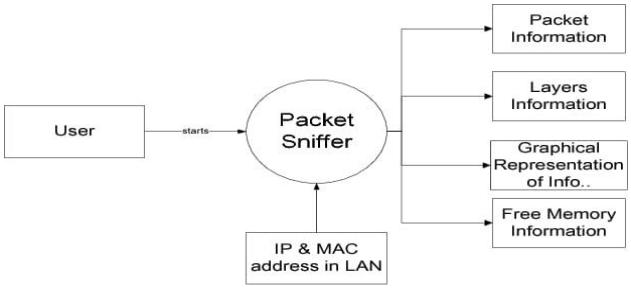

Fig. 1 Proposed system architecture

The Nano Sniffer performs 3 types of spoofing viz ARP spoofing,DNS spoofing and DHCP spoofing.

i) ARP spoofing

ARP spoofing is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network. This results

in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network. Once the attacker's MAC address is connected to an authentic IP address, the attacker will begin receiving any data that is intended for that IP address. ARP spoofing can enable malicious parties to intercept, modify or even stop data in-transit. ARP spoofing attacks can only occur on local area networks that utilize the Address Resolution Protocol.The effects of ARP spoofing attacks can have serious implications for enterprises. In their most basic application, ARP spoofing attacks are used to steal sensitive information.

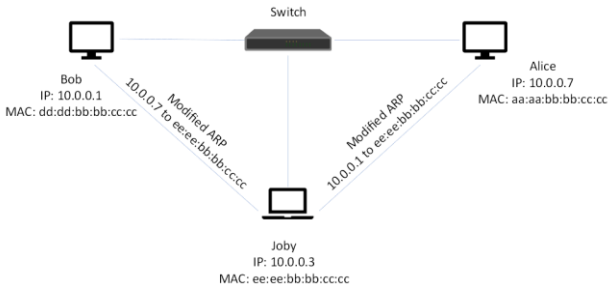

Fig. 2 ARP Spoofing

ii) DNS Spoofing

Domain Name Server (DNS) spoofing (a.k.a. DNS cache poisoning) is an attack in which altered DNS records are used to redirect online traffic to a fraudulent website that resembles its intended destination. Once there, users are prompted to login into (what they believe to be) their account, giving the perpetrator the opportunity to steal their access credentials and other types of sensitive information. Furthermore, the malicious website is often used to install worms or viruses on a user's computer, giving the perpetrator long-term access to it and the data it stores. Methods for executing a DNS spoofing attack include:-

1. Man in the middle (MITM)- The interception of communications between users and a DNS server in order to route users to a different/malicious IP address.

2. DNS server compromise- The direct hijacking of a DNS server, which is configured to return a malicious IP address.

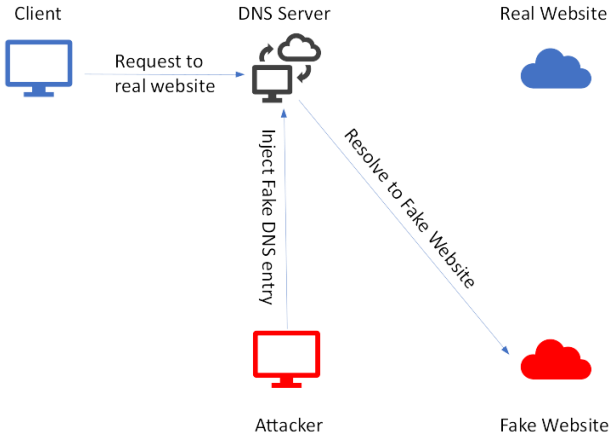

Fig. 3 DNS Spoofing

iii) DHCP Snooping:

This module's purpose is attacking Microsoft Windows hosts by replying to DHCPv6 messages and providing the target with a link-local IPv6 address and setting the attacker host as default DNS server. DHCP spoofing occurs when an attacker attempts to respond to DHCP requests and trying to list themselves (spoofs) as the default gateway or DNS server, hence, initiating a man in the middle attack. With that, it is possible that they can intercept traffic from users before forwarding to the real gateway or perform DoS by flooding the real DHCP server with requests to choke ip address resources.

C. Requirement Analysis

The implementation detail is given in this section.

Table 2 Hardware details

Hardware	Raspberry Pi Zero W
Mini HDMI	B-type
SD card	8 gb
Networking	Simple Switch

Table 3 Software details

Operating System	Debian Kali Linux ARM image
Programming Language	Golang, Python, Bash
Modules	net.recon, net.show, net.probe, net.sniff, net.fuzz, wol.etc MAC, spoofers-arp.spoof, dns.spoof, dhcpv6.spoof, Https.proxy, caplets,

	libpcap, libnetfilter-queue

IV. APPLICATIONS

Every administrator should have packet sniffing software in their arsenal for detailed insight into response time. A network packet sniffer will tell you directly if an application or the network is affecting the end-user experience. Administrators know unanticipated spikes in network traffic can spell trouble - like mail server problems, malware, or a full-blown security breach. This network packet sniffer's Wi-Fi packet capture tool helps you differentiate normal traffic from abnormal traffic by detailing data and transaction volume according to application.

Real-time information about user activity, application activity, web activity, etc., is delivered in context to a central management portal from where network administrators can drill down into the data for deeper insight.

ACKNOWLEDGMENT

It is our privilege to express our sincerest regards to our supervisor Prof. K S. Charumati for the valuable inputs, able guidance, encouragement, whole-hearted cooperation and constructive criticism throughout the duration of this work. We deeply express our sincere thanks to our Head of the Department Dr. Sharvari Govilkar and our Principal Dr. Sandeep M. Joshi for encouraging and allowing us to present this work.

REFERENCES

1. *Roshan Poudél (Nov, 2019), Packet Sniffer to Sniff Sensitive Credentials Only, ResearchGate.*
2. *Azidine Guezzaz, Ahmed Asimi, Younes Asimi,, Zakariae Tbatous, Yassine Sadqi (May 2019), A Global Intrusion Detection System using PcapSockS Sniffer and Multilayer Perceptron Classifier.*
3. *Henry N. O. and Agana M. (2019), Intranet Security using a LAN Packet Sniffer to Monitor Traffic.*
4. *A. Bhandari, S. Gautam, T. K. Koirala, and M. R. Islam (2018), "Packet Sniffing and Network Traffic Analysis Using TCP—A New Approach" in Advances in Electronics, Communication and Computing, ed: Springer, pp. 273-280.*
5. *N. Lizarti and W. Agustin (2015), Aplikasi Network Traffic Monitoring Menggunakan Simple Network Management Protocol (SNMP) pada Jaringan Virtual Private Network (VPN), SATIN-Sains dan Teknologi Informasi, Vol. 1.*
6. *Configuring mitmproxy for secure connections (Blog). [Online] Available at: https://bookdown.org/adityashrm21/raspberry-pi-packet-sniffer2/_book/configuring-mitmproxy-for-secure-connections.html*
7. *Daiji Sanai, "Detection of Promiscuous Nodes Using ARP Packet". [Online] Available At: http://www.securityfriday.co*