JOURNAL OF NORTHEASTERN UNIVERSITY

Volume 26 Issue 01, 2023 ISSN: 1005-3026 https://dbdxxb.cn/ Original Research Paper

ANALYSIS OF VOIP SECURITY THROUGH VAPT AND NETWORK PACKET ANALYSIS

Indrajeet Singh
School of Doctoral Studies and Research, National Forensic Sciences University, Sector 9, Gandhinagar-382007, Gujarat, India

*Corresponding author **Dr. Naveen Kumar Chaudhary**
School of Cyber Security and Digital Forensics, National Forensic Sciences University, Sector 9, Gandhinagar-382007, Gujarat, India

*Corresponding author **Muhammad Zubair Dahir**
School of Cyber Security and Digital Forensics, National Forensic Sciences University, Sector 9, Gandhinagar-382007, Gujarat, India

Biographical notes: Indrajeet Singh is a research scholar (Cyber Security) in the School of Doctoral Studies and Research, World's First of Its Kind, National Forensic Sciences University, Gandhinagar, Gujarat, Government of India. He received his MTech in Computer Science and Engineering from the Jagannath University (Haryana) and BE in Computer Engineering from the Guru Jambheshwar University of Science and Technology (Haryana).

Dr. Naveen Kumar Chaudhary is a Professor and the Dean at the National Forensic Sciences University, Gandhinagar, Gujarat, India. He is also the Head of the NFSU Cyber Defence Centre which is the first ISO 27001-certified CDC Lab in India. His research interest areas are network forensics, drone forensic, and next-generation networks.
Muhammad Zubair Dahir is pursuing MSc (Cyber Security) in the School of Cyber Security and Digital Forensics, the world's First of its kind, at the National Forensic Sciences University, Gandhinagar, Gujarat, Government of India.

Abstract
The rapid growth of technology such as computers or mobile phone applications that interacts with the internet poses a security risk. Vulnerability Assessment and Pen-Testing (VAPT) is an offensive method for safeguarding an organization with security assets. It is a big challenge for an organization to protect its data from growing vulnerabilities. In this research, various automated tools are used to identify the target system security breaches in the VoIP infrastructure posture as a part of vulnerability assessment. If the attacker identifies these security breaches, it can result in significant data loss. Pen-Testing is a method to determine whether the security measures are performing effectively. Voice Over Internet Protocol (VoIP) is one of the effective solutions employed by skilled criminals to conceal their identity from ordinary communication mechanisms. The method for VAPT of VoIP infrastructure is discussed and implemented in this research to combat similar types of attacks.

Submitted: 17/12/2022 **Accepted**: 10/01/2023

Keywords: Vulnerability Assessment and Penetration Testing (VAPT), VAPT tools, Security Assessment tools, Session Initiation Protocol (SIP), Real-Time Protocol (RTP)

1. Introduction

Voice over Internet Protocol is a cutting-edge innovation that has changed the mode of communication services, which are conveyed over IP networks. It offers better performance and discounted costs to its clients, making it more well-known than the past Public Switched Telephone Network. Despite its developing prominence, this innovation turned into an objective for various attacks [1]. The new improvement of voice over IP (VoIP) has caused phone communication to be a modern medium, to be specific the internet, making it more advantageous and less expensive for individuals to reach one another. These advantages have been generally received by the customary clients, yet additionally by cyber criminals, who can now decrease the expense and functional intricacy [2].

In comparison with different attacks for example email spam, voice spam calls are altogether more upsetting because they require immediate attention. When there is an incoming call, it is very hard to decide whether the incoming call is valid or spam by just looking at the caller ID, which is frequently “unknown” or even spoofed [3].

Two sorts of protocols are utilized in fundamental VoIP communication, (i) signaling protocol helps create, change, and make an end to the ongoing session, (ii) Media Transport Protocol, which transports the information after two entities lay out an association. Usually, SIP is utilized [4]. RTP (Real-time Transport Protocol) is indeed the standard signaling and media transport protocol [5].

Due to the lack of a specification for encrypting the original data in the RTP protocol, an attacker can easily grab the packets using different network sniffing tools and get the data of the user easily. Furthermore, experts have devised SRTP (Secure Real-Time Transport Protocol), which identifies and mitigates this problem by encrypting the payload field [6].

A couple of services that makes VoIP so well-known are, messaging, audio-video conferencing call, and voice mail. Besides, in light of the fact that these services are involving the internet as a mode of communication, they are more presented with security concerns, as VoIP technology has inherited Internet weakness. VoIP security is especially critical since phone conversations are sent in plaintext over the Internet, making it simple for an assailant to gain admittance to the correspondence channel because of the SIP’s feeble confirmation [7].

According to security measures, SIP vulnerabilities are the primary factor of attacks against VoIP technologies [8,9]. Sip was created without any security concerns so it is disposed to different types of attacks like, snooping, message altering, and registration seizing. Users' trust in VoIP rather than PSTN is eroded as a result of such attacks. The third-generation partnership project (3GPP) officially adopted SIP as a signaling standard in 2000. The IETF announced SIP in RFC-3261 in 2002 [10].

Security hazards exist in all Internet-facing systems and apps. VAPT is the strategy utilized by security professionals all around the world to address these security issues [11].

Security is perhaps the main test data framework. Due to the rising interconnections of computers through the internet, expanded extensibility, and the unrestrained development of the size of the intricacy framework. The security of the system has become more of a challenge than in the past. Furthermore, it is an organization's responsibility to secure its cyber assets appropriately by utilizing a thorough and systematic method to protect against the threats that an organization may face [12].

Vulnerability analysis is the most common way of recognizing a subsection information space where a threatening client can take advantage of the coherent imperfections in a framework to make it defenseless [13].

Penetration testing, often known as ethical hacking or pen-testing, is a method for assessing risks in a network system before an attacker exploits them [14].

To resolve this issue, organizations teamed up to make Common Vulnerability Exposure (CVE) and Common Weakness Enumeration (CWE), two of which are supported by the MITRE Corporation [15]. Focusing on high-risk problems is one strategy to address these weaknesses. OWASP [16] and SANS [17] are two such communities.

The increase in network resource users leads to the creation of a significant amount of communicated data, as well as the challenge of dependable, secure data transmission, or information security. The utilization of encryption methods, an OS server, design, and settings of the Asterisks programming firewall, are the solution to this issue [18].

Since transmission dormancy with high communication quality is unsuitable, huge packets estimated altogether diminish network productivity. Small packets, then again, increment the portion above as they have a set length and the packet size diminishes [19]. The number of packets in which messages are divided increments quickly, bringing about a critical expansion in network traffic. As a result, the ideal length of transmitted packets is required to achieve maximum efficiency and better service quality for network users [20].

Since ideal parameters are subjected to various elements, a few of them which are continually changing the network capabilities, it is hard to decide them with high exactness. For instance, while sending packets over the network, the sum and kind of traffic, as well as the number of deferrals, but while fostering a network, designers utilize a cut-off inside which the packet length, or rather its information field, can be found, though the header is generally fixed length [21].

x- Lite is the softphone that is utilized for VoIP calls. It is a free softphone that provides a high-quality output to the user. Because of cost savings and ease of installation, many firms are switching from traditional communication media to VoIP systems [22]. It will be the most important component of next-generation networks. A codec (coder-decoder) is a device that turns an audio stream into a compressed digital form for transmission and vice versa for replay [23, 24].

The unwavering quality and security threats for confidentiality, integrity, and availability. It is seen that acquiring a higher level of reliability and security is as yet a significant challenge in the VoIP communication framework [25].

We undertake the Vulnerability Assessment and Penetration Testing activity of this VoIP technology as an infrastructure configuration in this research, as well as discuss some relevant definitions and problems. This research additionally depicts the weakness associated with VoIP that are utilized in VoIP security tools to find the shortcomings that make the threats and issues in the security of VoIP. We also go over how to install VoIP,

including an overview of all the protocols needed to use the Internet Telephony idea. Finally, we will discuss a vulnerability that might compromise the entire VoIP system.

2. Methodology

The conventional traditional method of the VoIP infrastructures Vulnerability Assessment and Pen-Testing (VAPT) activity is used in this research. The VAPT lifecycle is depicted in the diagram below:
The life cycle is as follows:

Fig: 1 Life Series of Vulnerability Assessment and Penetration Testing

We are going to initiate the activity by the respective flow chart mentioned below.

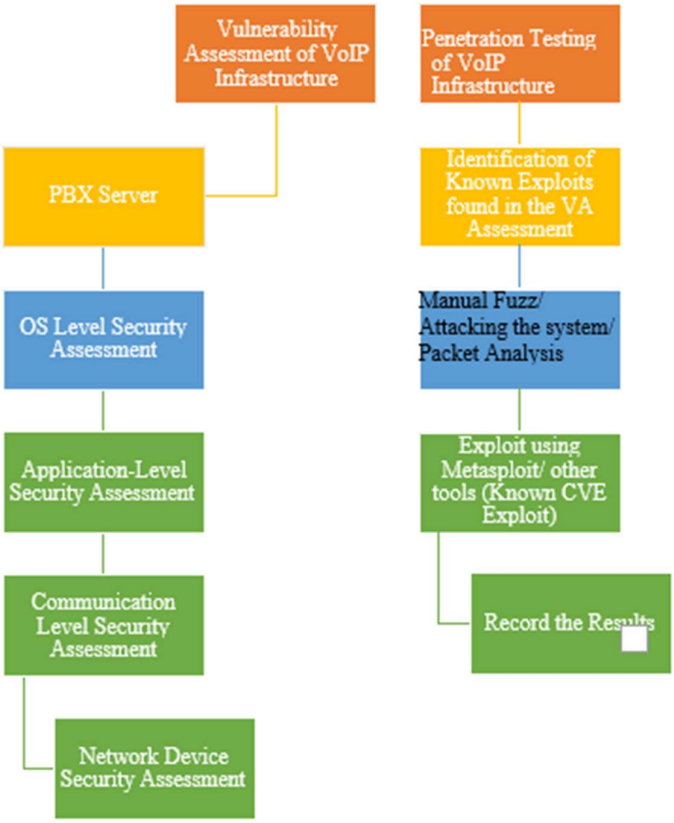


Fig: 2 VAPT Flow Chart for VoIP server (Asterisks)

Elaborating it further,

Our research was conducted in the following steps by building our lab setup and environment to conduct and analyze the VOIP Server and testing scenarios.

These steps to be performed and executed are as follows

Step 1: Creating Parent Virtual Machine Instances (Setup) PBX Server in the Ubuntu Machine

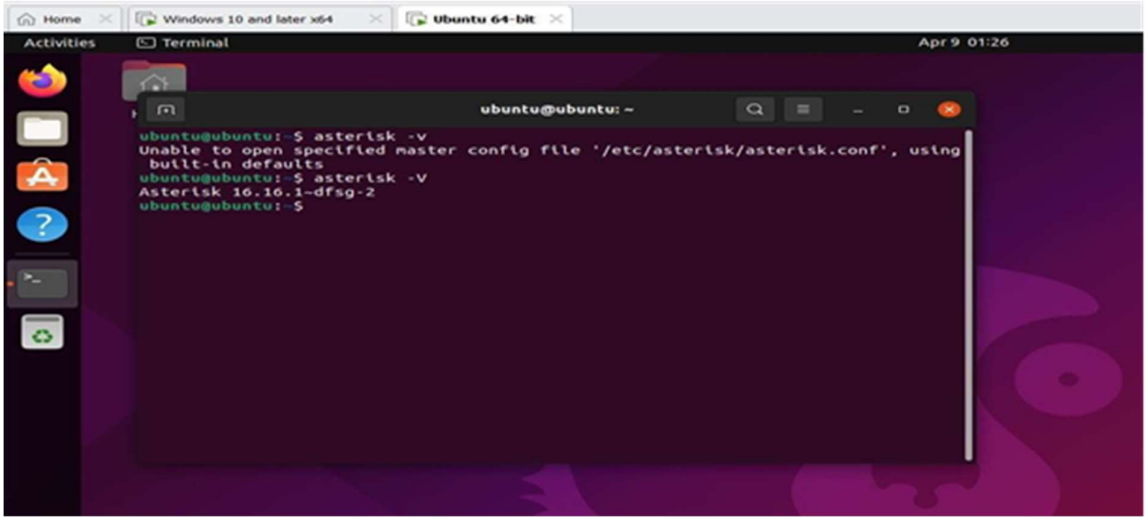


Fig 3: Installation of Asterisks Server

Step 2: Host and Child Virtual Instances for connecting VOIP Calls, it can be a flexible OS, we are taking windows in our cases.
Host Machine 1Virtual Machine 1

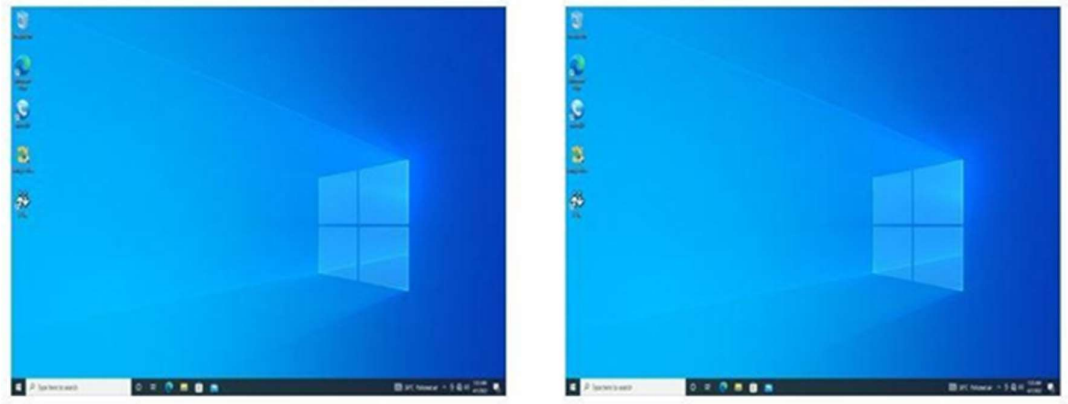


Fig: 4 Host and Child Virtual Machine Instance for Connecting the VoIP Call

Step 3: Configuration of Asterisk server.

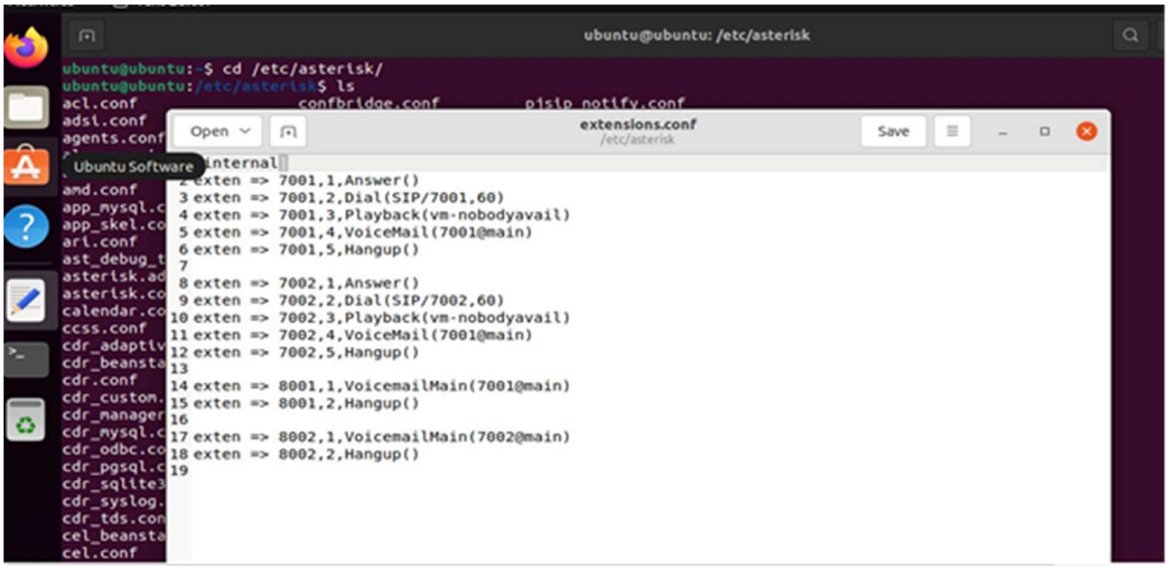


Fig: 5 Installation and configuration of Asterisk Server

Step 4: After successful configuration and server integration. The call is initiated from the Host machine using X-Lite to the VMware Windows machine using MicroSIP softphones.

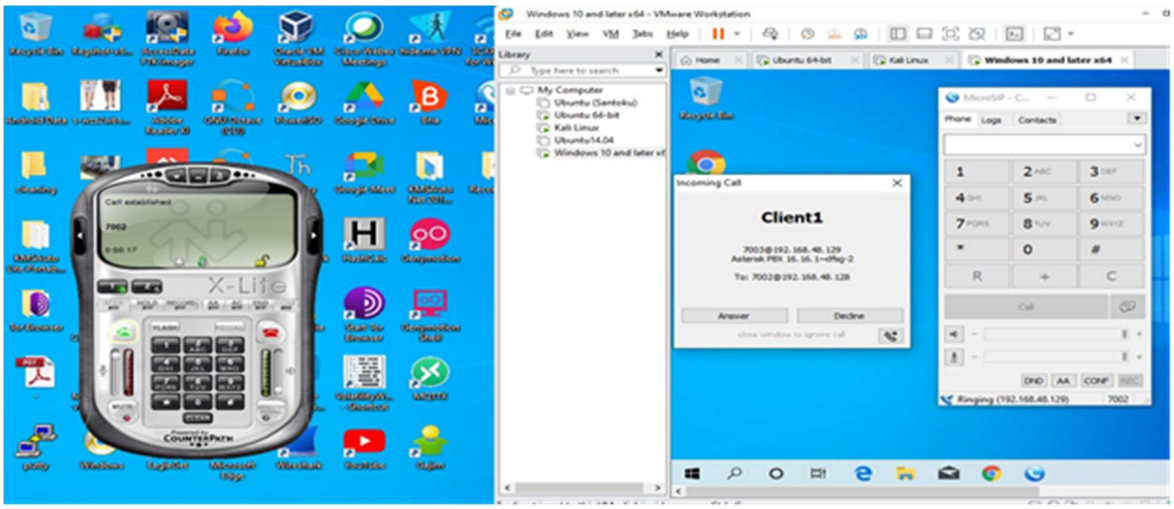


Fig: 6 Call initiation from the Child Virtual Machine

3. Vulnerability Assessment of VoIP Infrastructure (PBX Server, Asterisks)

Know we need to focus on our traditional VAPT testing activity, as discussed above. Scope – Info Gathering – VA Activity – Pen Testing – Result Analysis – Report

Step 1: Operating System-Level Vulnerability Assessment, (UBUNTU)

Starting with the Scope and information gathering,

Scope of IP - Machine on which asterisk server installed and Nmap test result – Outcome

- Port state service: 2000/tcp open cisco-sccp: This vulnerability can be used to exploit by sending specially crafted packets to the SCCP (2000/tcp) port, a DoS attack can be completed by a far-off aggressor.
- TLS 1.2 not vulnerable to heartbleed: In the open SSL cryptographic software library heartbleed is a critical vulnerability. This allows the compromising of the private keys used to identify service providers and encrypt data, as well as the identity and password of the users. An attacker can leverage this flaw to listen in on a conversation, which is known as an Eavesdrop attack.

```
ubuntu@ubuntu:~$ nmap 192.168.110.141

Starting Nmap 7.60 ( https://nmap.org ) at 2022-04-09 05:08 PDT
Nmap scan report for ubuntu (192.168.110.141)
Host is up (0.00031s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
2000/tcp open  cisco-sccp

Nmap done: 1 IP address (1 host up) scanned in 2.14 seconds
```

Fig: 7 Nmap test (Information Gathering)

Step 2: Application-Level Vulnerability Assessment, Nessus activity that has been performed on the Respective OS (UBUNTU). The vulnerable application (Firefox) which is installed in the operating system is shown in fig 8 below. It indicates the critical vulnerabilities of the application which can cause the failure of the VoIP infrastructure.

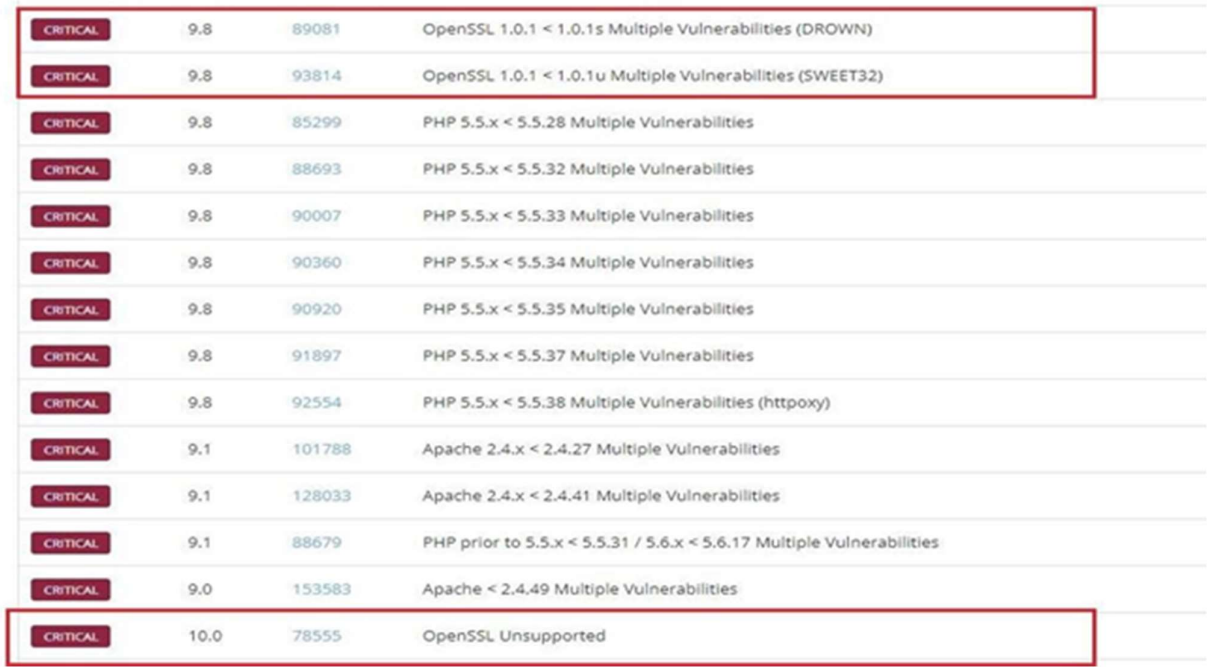
- Ubuntu 18.04 LTS/20.04 LTS/21.10: Vulnerabilities of Firefox (USN-5314-1), (USN-5284-1), (USN-5131-1): This vulnerability was discovered when the XSLT parameter was removed in some circumstances. The users were tricked to open a specially crafted website. This blemish can be utilized to do a DoS attack or execute arbitrary code.

Fig: 8 Application-Level Vulnerability Assessment

Step 3: Communication Level Vulnerability Assessment, Nessus activity that has been performed on the Respective OS (UBUNTU)

- OpenSSL 1.0<1.0.1u multiple vulnerabilities (SWEET32): The SWEET32 vulnerability allows attackers to exploit the block cipher collisions. The attacker can use a 64-bit block cipher to compromise HTTPS connections.

• OpenSSL 1.0.1<1.0.1s several vulnerabilities: When parsing the malformed DSA private keys, this vulnerability occurs. This exploit can be utilized by a distant assailant to ruin memory, bringing about a DoS attack.



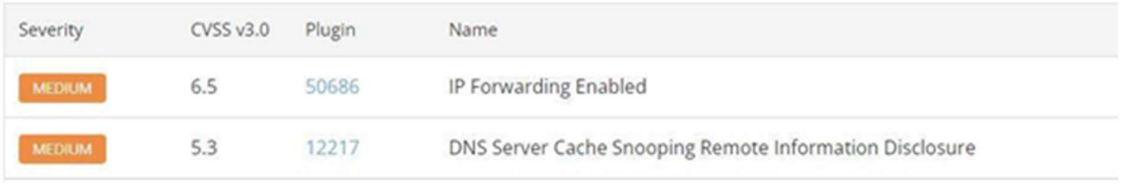
CRITICAL	9.8	89081	OpenSSL 1.0.1 < 1.0.1s Multiple Vulnerabilities (DROWN)
CRITICAL	9.8	93814	OpenSSL 1.0.1 < 1.0.1u Multiple Vulnerabilities (SWEET32)
CRITICAL	9.8	85299	PHP 5.5.x < 5.5.28 Multiple Vulnerabilities
CRITICAL	9.8	88693	PHP 5.5.x < 5.5.32 Multiple Vulnerabilities
CRITICAL	9.8	90007	PHP 5.5.x < 5.5.33 Multiple Vulnerabilities
CRITICAL	9.8	90360	PHP 5.5.x < 5.5.34 Multiple Vulnerabilities
CRITICAL	9.8	90920	PHP 5.5.x < 5.5.35 Multiple Vulnerabilities
CRITICAL	9.8	91897	PHP 5.5.x < 5.5.37 Multiple Vulnerabilities
CRITICAL	9.8	92554	PHP 5.5.x < 5.5.38 Multiple Vulnerabilities (httpoxy)
CRITICAL	9.1	101788	Apache 2.4.x < 2.4.27 Multiple Vulnerabilities
CRITICAL	9.1	128033	Apache 2.4.x < 2.4.41 Multiple Vulnerabilities
CRITICAL	9.1	88679	PHP prior to 5.5.x < 5.5.31 / 5.6.x < 5.6.17 Multiple Vulnerabilities
CRITICAL	9.0	153583	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	10.0	78555	OpenSSL Unsupported

Fig: 9 Communication Level Vulnerability Assessment

Step 4: Network Level Vulnerability Assessment, Devices (Router)

• IP Forwarding Enabled: This exploit allows the attacker to route the packet through the host and potentially bypass various firewalls and routers.

• DNS Server Cache Snooping: This vulnerability reveals the information about the owner of the DNS server such as vendor details. This method could be used to gather statistical information such as the time when the owner typically accesses the confidential data. The cached DNS records the remaining Time-to-live (TTL) values which provide accurate data.



Severity	CVSS v3.0	Plugin	Name
MEDIUM	6.5	50686	IP Forwarding Enabled
MEDIUM	5.3	12217	DNS Server Cache Snooping Remote Information Disclosure

Fig:10 Network Level Vulnerability Assessment

4. Penetration Testing of the VoIP Infrastructure (PBX Server, Asterisks)

Step 1: Identification of Known Exploit found in Vulnerability Assessment are as follows:

In this paper, according to the vulnerability assessment, we shall perform two attacks on the VoIP system are as follows:

- Eavesdropping
- Denial of Service

Step 1: Manual Fuzz/ Attacking the system/ Packet Analysis

Eavesdropping VoIP calls with Wireshark

Eavesdropping, often known as snooping or listening, occurs when a computer, smartphone, or other connected device intercepts data being transmitted across a network. The attacker exploits an insecure network communication to obtain access to data transmitted or received by the user.

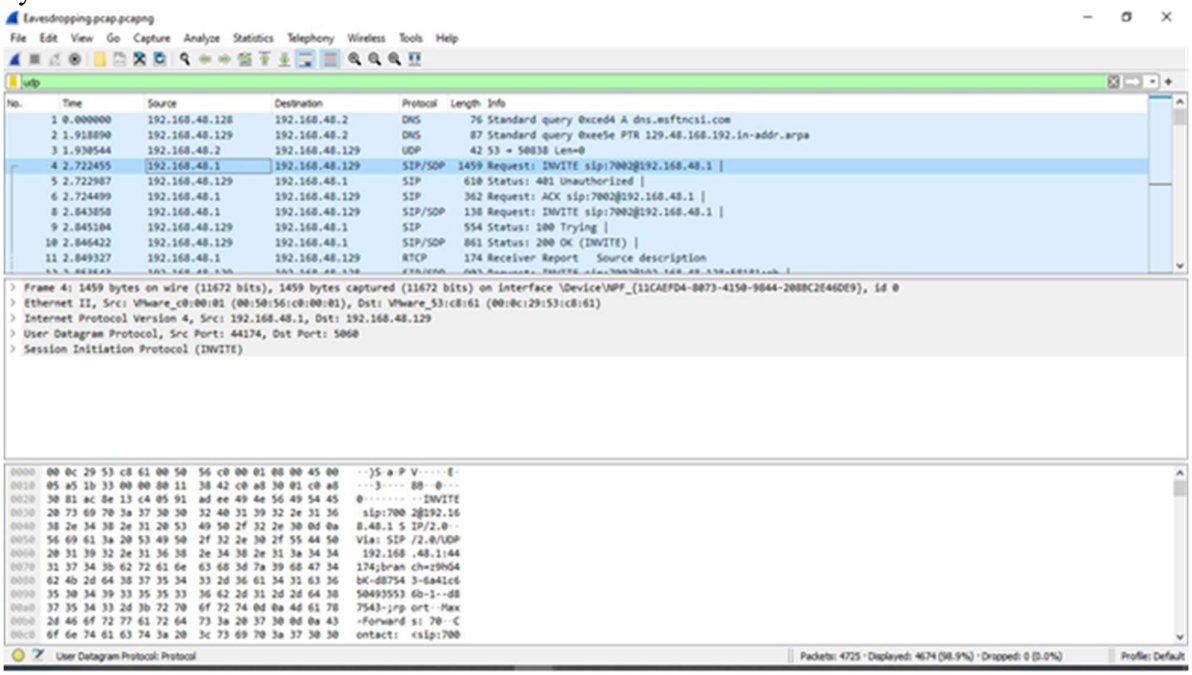


Fig: 11 Host machine sending an invite request

The host machine (192.168.48.1) sent an invite request to the asterisk server(192.168.48.129)

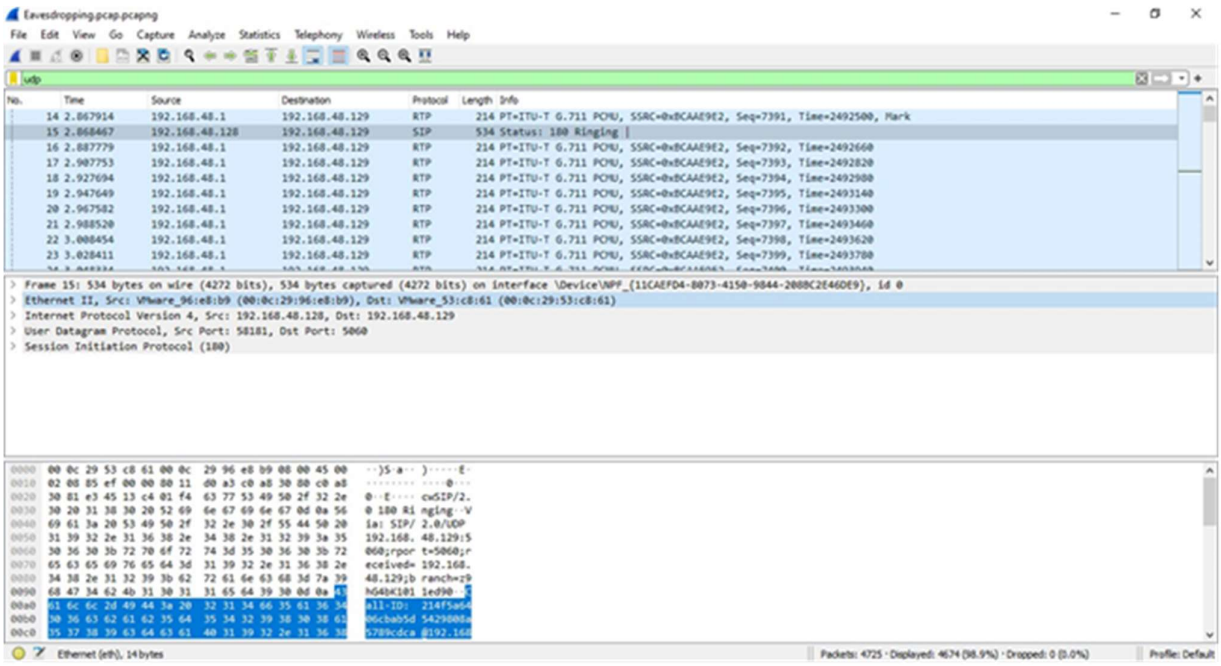


Fig:12 Asterisk acknowledged the invite request

The asterisk server (192.168.48.129) acknowledged the invite request from the host machine (192.168.48.1) and a call was established between the windows host machine (192.168.48.129) and the windows virtual machine (192.168.48.128)

VoIP calls are a built-in feature of Wireshark that can decode RTP data into a playable audio format.

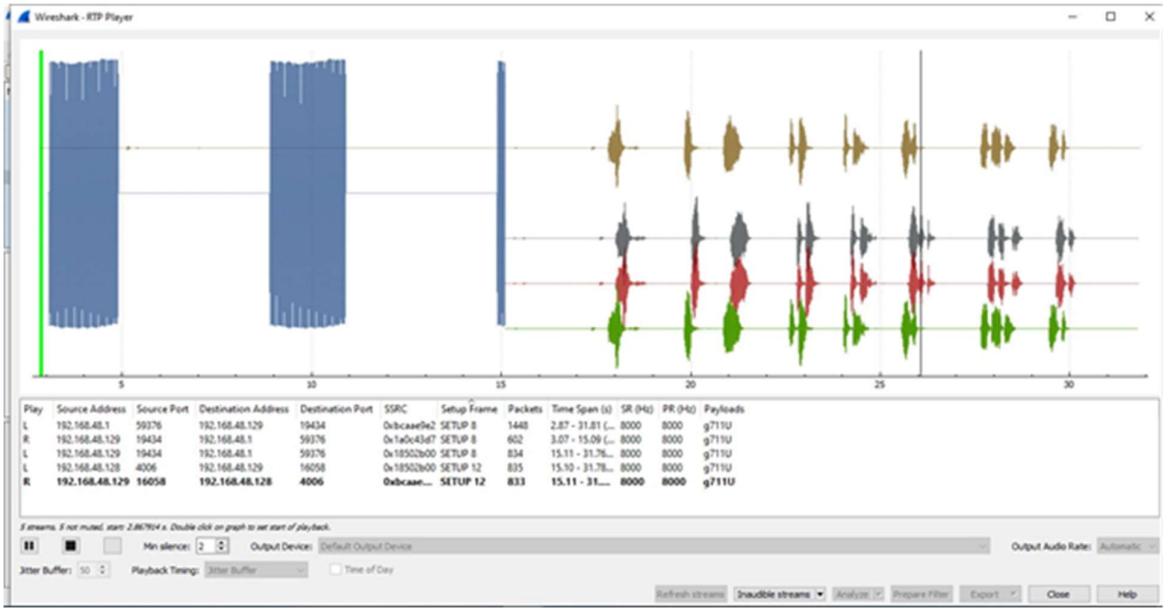


Fig: 13 RTP Player (Listening to the Conversation of the Clients)

Voice data was captured through the use of the function called Telephony in Wireshark. The voice data is then played using the RTP player in Wireshark and we managed to listen to the entire conversation.

Step 2: Exploit using Metasploit/ other tools (Known as CVE Exploit)

Denial of Service (DoS) attack on VoIP server (Asterisk)

A DoS attack plans to stop a machine or organization, leaving it unusable to its expected clients. DoS attack force the objective to crash by flooding it with traffic or conveying its information. This attack deprives real users of services or resources, such as workers, associates, or account holders, of the service or resources they expected. We used an SYN flood DoS attack against the asterisk server in this study.

A DoS assault plans to stop a machine or organization, leaving it unusable to its expected clients. DoS assault force the objective to crash by flooding it with traffic or conveying its information

The DoS attack on the asterisk server, which was running on an Ubuntu host, was carried out using Kali Linux. Hping3, a free TCP/IP packet generator, and analyzer built by Salvatore Sanfilippo (also known as Antirez) and included in Kali Linux is comparable to the ping software but has more capabilities than merely making an ICMP request. Hping can be used to deliver a massive amount of TCP traffic to a target while concealing the source IP address and making it appear random or even from legitimate sources. This function in Kali Linux was used to capture and display the amount of traffic being transferred to the server using Wireshark.

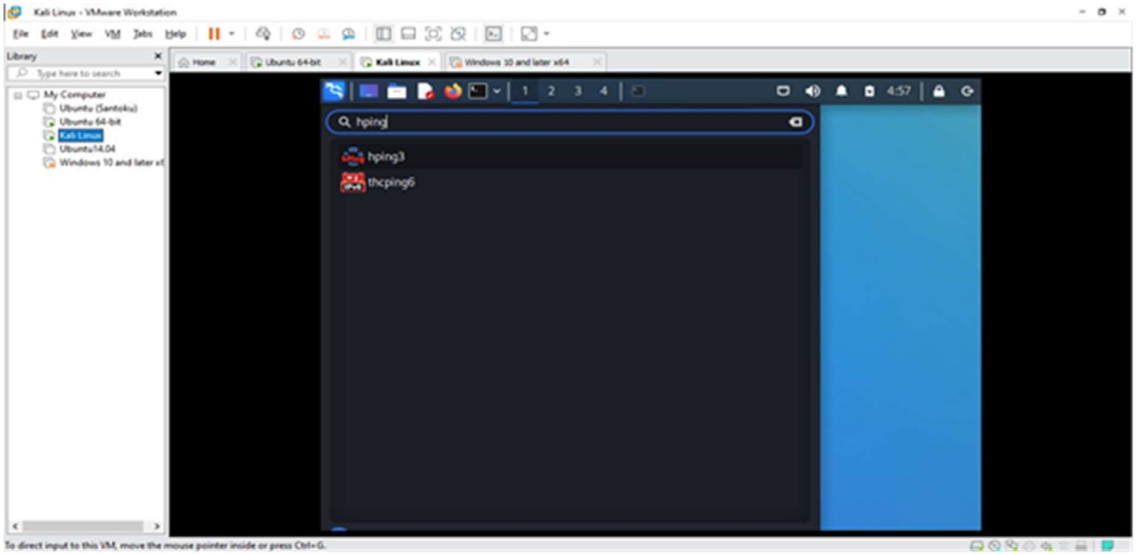


Fig: 14 Starting hping3 using Kali Linux

Performing the Syn flag DOS attack on the server

A TCP SYN flood is a sort of DoS attack in which a tremendous quantity of SYN entreaty is shipped off a server trying to overpower it with open connections.
On the Asterisk server, we used the following command to launch an SYN flag DoS attack.
sudo hping3 -S --flood -V -p 80 192.168.14.129

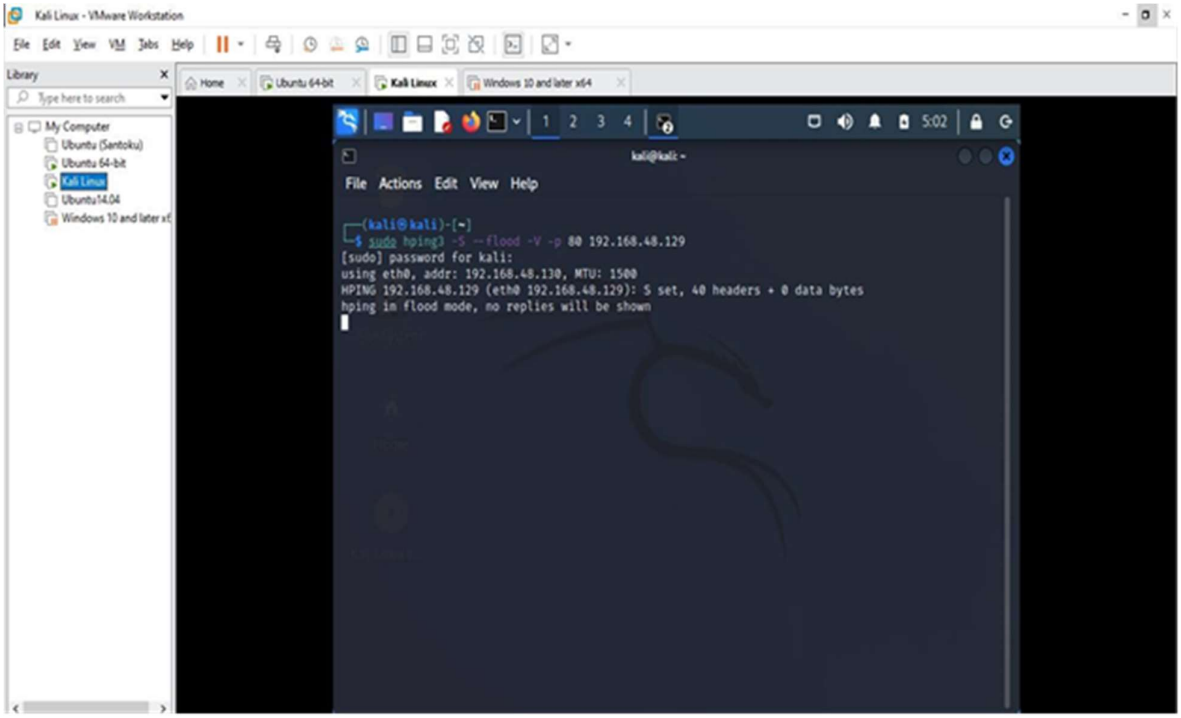


Fig: 15 SYN flag dos attack

Wireshark was used to capture the packets that were being sent to the server (192.168.48.129) by Kali (192.168.48.130) using the hping3 tool. The above screenshot illustrates the severity of the packets that were being sent at a time and thereby denying the server even time to respond.

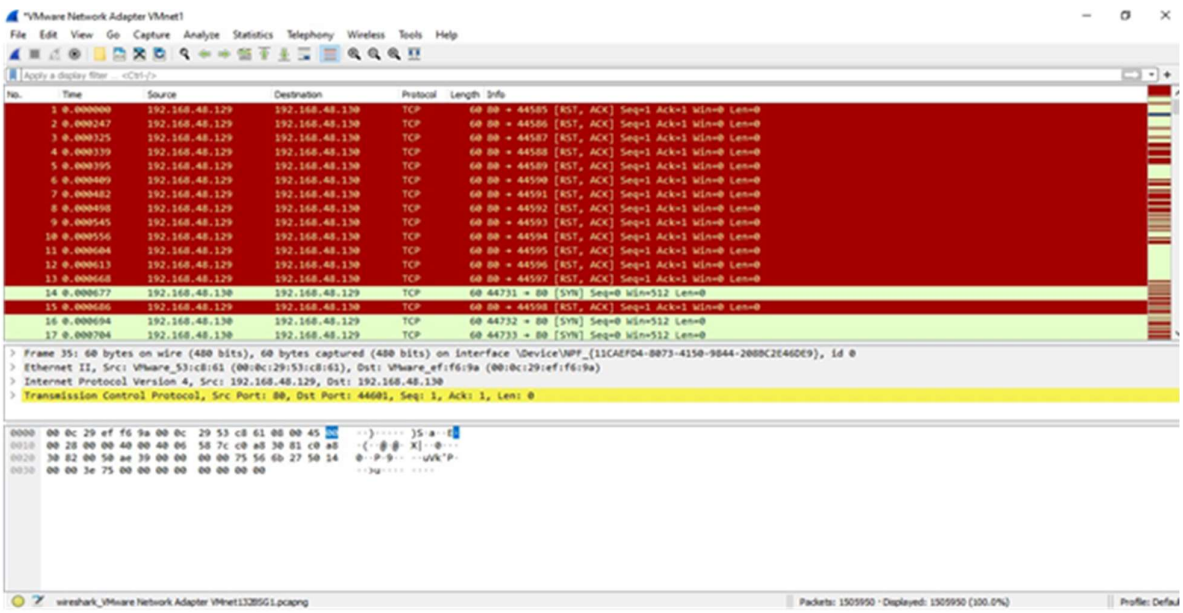


Fig: 16 Packets capturing using Wireshark (from Ubuntu to Kali)

The above screenshot illustrates the server (192.168.48.129) trying to respond to the requests being made by Kali (192.168.48.130). The server is now dedicating most of its resources to Kali thereby denying legitimate clients to acquire the resources.

5. Results

Upon evaluation, VoIP systems are vulnerable and because of those vulnerabilities, they are prone to several attacks like Eavesdropping and Denial of Service.

5.1: Result of Eavesdropping Attack

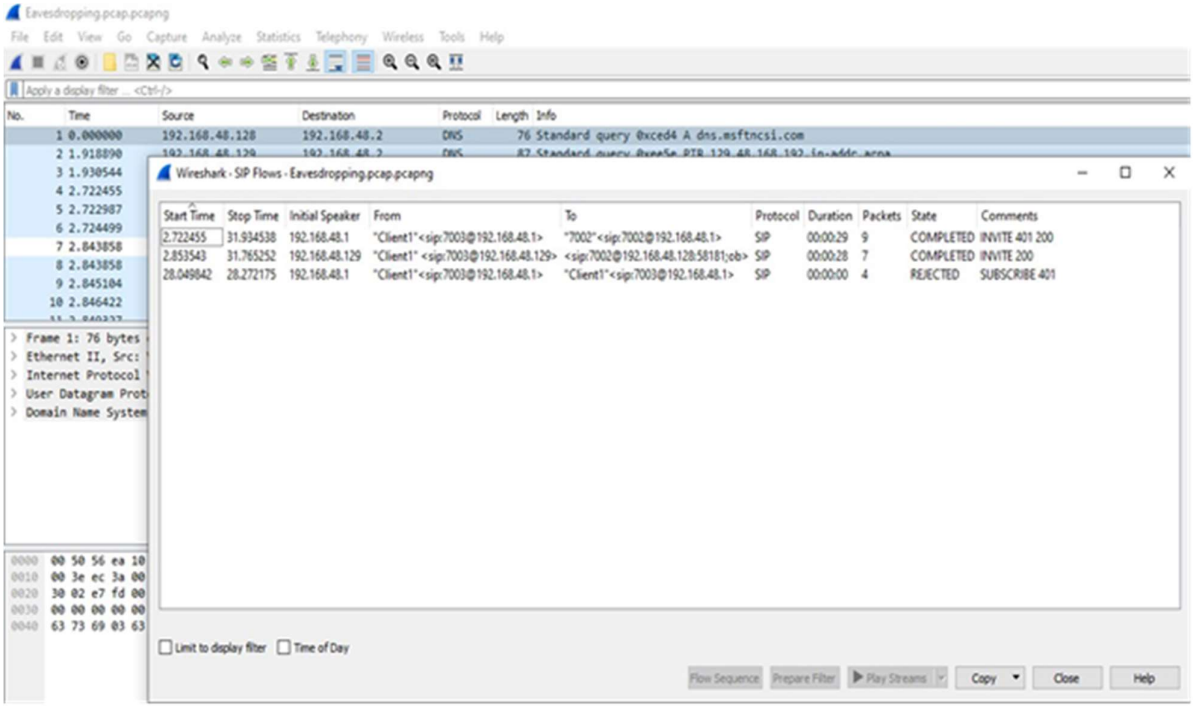


Fig: 17 Session Initiation Protocol (SIP) Flow Diagram

The SIP flows are shown in the screenshot above. A SIP User Agent (UA) client initiates a session with the called endpoint User Agent Server (UAS) by sending a request to the called endpoint UASSIP, Uniform Resource Locator (URL). Assuming that the User Account Control (UAC) knows the UAS IP address, the request can be submitted. In the event that the client can't be found, the UAC sends the request to an intermediary or side-tracks it to the server. Until the client is found, the request might be steered to a few servers. After the SIP address is set out to an IP address, the request is directed off the UAS. Assuming the client acknowledges the call, the client's abilities are conceded, and the conversation starts.

The SIP flows allowed us to listen to the conversation that took place between the Windows host machine (192.168.48.1) using X-Lite and the Windows VMware machine using MicroSIP softphones (192.168.48.128)

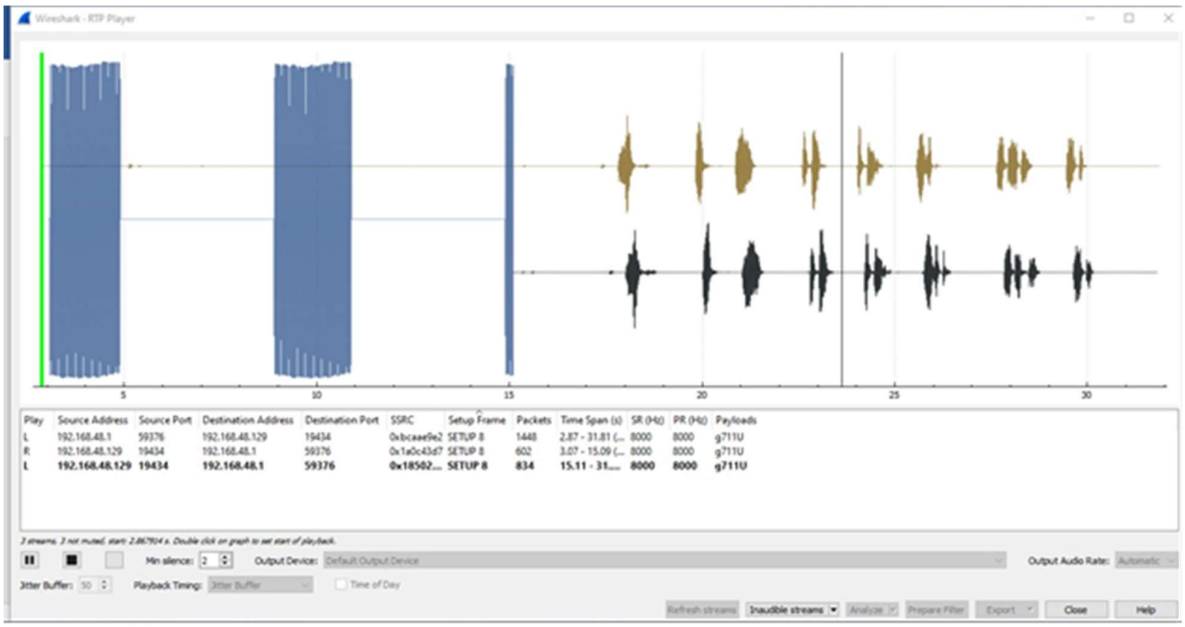


Fig: 18 RTP Player (Listening to the Conversation of the Clients)

Through the RTP Player, we were able to play SIP flows and listened to the conversation that took place between the Windows host machine (192.168.48.1) using X-Lite and the windows VMware machine (192.168.48.128).

5.2: Result of Denial-of-Service Attack

In the figure below, we can see that Kali Linux (192.168.48.130) managed to perform a DOS attack on the asterisk server (192.168.48.129). Immediately the attacker creates a server connection but does not complete it. The server will have to devote more resources to waiting for half-opened connections, which may cause legitimate traffic to become unresponsive.

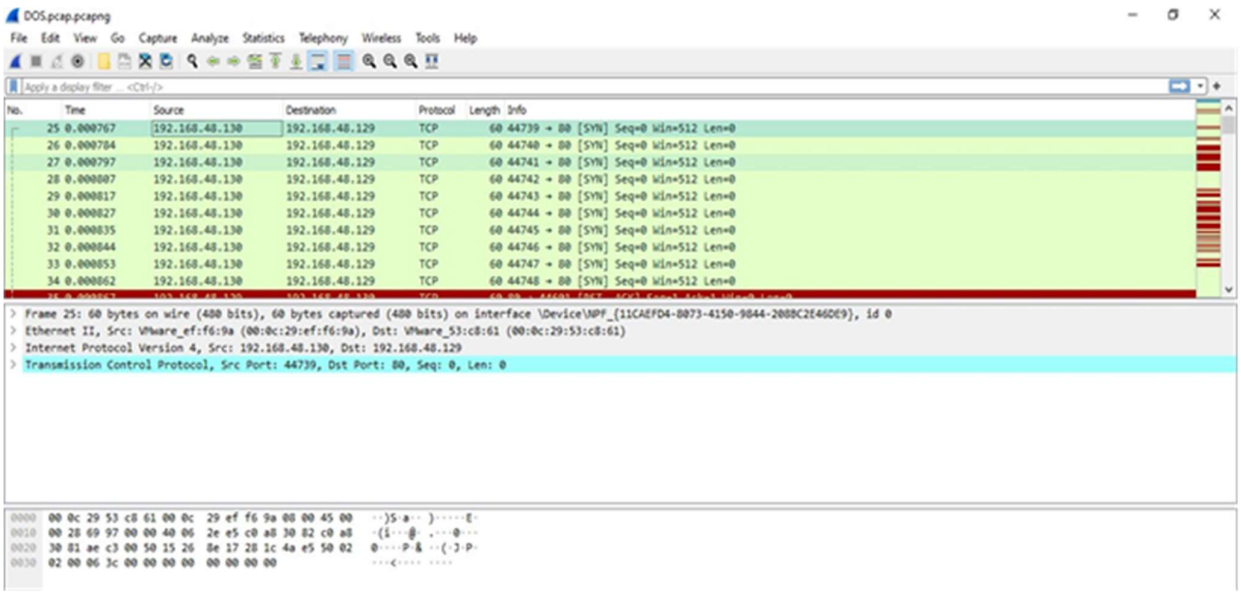


Fig: 19 SYN flood attack packets

The Figure below illustrates that the server (192.168.48.129) is resetting connections initiated by the attacker (192.68.48.130). This limits the server's time in responding to legitimate requests and thereby ends up wasting resources on the attacker.

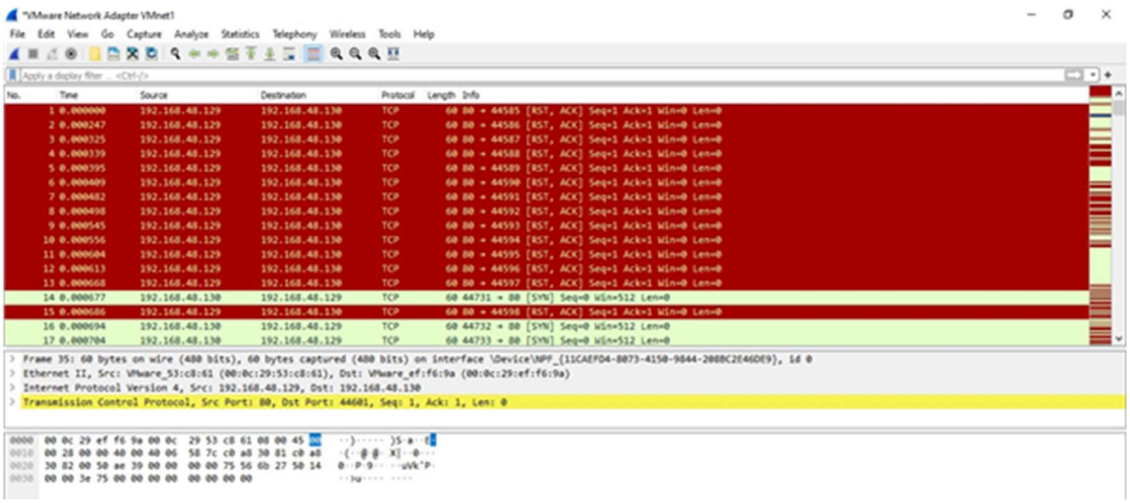


Fig:20 SYN flood attack server packets captured

6. Analysis

The goal of this research is to examine the vulnerability assessment and pen-testing of the VoIP infrastructure. That is, determining how the scenario is generated and what occurs to the VoIP infrastructure as a result of such attacks. We were able to hear the voice communication between the two clients during the eavesdropping attack, indicating that the RTP protocol is not secure because it allows a third party to hear the conversation word for word. There is no

security in the RTP protocol. The server was subjected to an SYN flood DOS attack, which prevented the server from allocating resources to appropriate clients due to the lack of a security mechanism in

place to identify and prevent such attacks. Pen-testing is a very important process in such scenarios as through this process we come to know about the security and weakness of our VoIP call infrastructure. As described above after testing our VoIP system we can prevent the system from malicious users/intruders to compromise our personal information.

7. Conclusion& Future Work

The goal of this research is to examine the VoIP infrastructure's vulnerability and conduct a Pen-Testing. As we have seen in this study, eavesdropping on a phone call conversation is simple and rapid when utilizing a MITM attack tool like Wireshark to sniff the data. In VoIP evaluation, pen-testers ought to attempt to complete this attack to check whether listening in is feasible. To combat this type of attack associations ought to execute the Secure Real-Time Protocol, a safe protocol that encodes information being traded, making it hard for an assailant to interpret the information and stand by listening to the discussion regardless of whether it is blocked. We also used the hping3 tool in Kali Linux to perform an SYN flood DoS attack against the server, knowing the server's IP address made it very easy to carry out the attack.
In VoIP assessments, pen-testers ought to attempt to complete this attack to check whether listening in is feasible. To combat this type of attack associations ought to execute the Secure Real-Time Protocol, a safe protocol that encodes information being traded, making it hard for an assailant to interpret the information and stand by listening to the discussion regardless of whether it is blocked.
As a result, a few prevention methods must be implemented to prevent the VoIP server's attack. To detect unusual traffic patterns, an Intrusion Detection System (IDS) should be installed. If your onsite firewall supports it, set up an SYN attack threshold and SYN flood defense system. Installing rate-limiting networking equipment and commercial solutions to gain network visibility and the capacity to monitor and analyze traffic across different network segments. The outcome of our research can be used to troubleshoot information in cases of protection vulnerabilities impacting VoIP systems. They can also help with a better understanding of VoIP vulnerabilities and threats, which will lead to better network architecture in the future.

References

1. Rehman UU, Abbasi AG. Security analysis of VoIP architecture for identifying SIP vulnerabilities. In2014 International Conference on Emerging Technologies (ICET) 2014 Dec 8 (pp. 87-93). IEEE.
2. Carrillo-Mondéjar, J., Martinez, J. L., & Suarez-Tangil, G. (2022). On how VoIP attacks foster the malicious call ecosystem. Computers & Security, 102758.
3. 28th USENIX Security Symposium (USENIX Security 19), USENIX Association, Santa Clara, CA (2019), pp. 1327-1340

4. J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, “Sip: Session Initiation Protocol”, RFC3261: Internet Engineering Task Force (IETF), June 2002.
5. H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, “RTP: A Transport Protocol for Real-Time Applications”, RFC3550: Internet Engineering Task Force (IETF), July 2003.
6. Secure Real-time Transport Protocol (SRTP), https://datatracker.ietf.org/doc/rfc3711/
7. Y. M. Koh, K. H. Kwon, “A New Lightweight Protection Method against Impersonation Attack on SIP”, Advances in Computer Science and its Applications CSA 2013, Vol. 279, 2014.
8. A. D. Keromytis, “A Look at VoIP Vulnerabilities”, Usenix Security Article, Vol. 35, No. 1, February 2010.
9. A. D. Keromytis, “A Comprehensive Survey of Voice over IP Security Research”, IEEE Communications Surveys & Tutorials Vol. 14, No.2, May 2012.
10. RFC3261: Internet Engineering Task Force (IETF), June 2002.
11. Shah S, Mehtre BM. An overview of vulnerability assessment and penetration testing techniques. Journal of Computer Virology and Hacking Techniques. 2015 Feb;11(1):27-49.
12. e Canadian Institute of Chartered Accountants Information Technology Advisory Committee, Using an Ethical Hacking Technique to assess Information security Risk, Toronto. http://www.cica.ca/research- and-guidance/documents/ it-advisory-committee/item12038.pdf. Accessed 03 Oct 2013.
13. parks, S., Embleton, S., Cunningham, R., Zou, C.: Automated vulnerability analysis: leveraging control flow for evolutionary input crafting. In: IEEE 23rd Annual Computer Security Applications Conference (2007)
14. Yaqoob I, Hussain SA, Mamoon S, Naseer N, Akram J, ur Rehman A. Penetration testing and vulnerability assessment. Journal of Network Communications and Emerging Technologies (JNCET) www. jncet. org. 2017 Aug;7(8).
15. The MITRE Corporation, Common Weakness Enumeration. http:// www.cwe.mitre.org/. Accessed 03 Oct 2013
16. Open Web Application Security Project. OWASP Top 10 Project. http://www.owasp.org/index.php/category:OWASP_Top_ Ten_Project. Accessed 03 Oct 2013
17. SANS Institute. SANS Top 25 Software Errors. http://www.sans. org/top25-software-errors/. Accessed 03 Oct 2013
18. Manankova OA, Yakubov BM, SERIKOV T, YAKUBOVA M, MUKASHEVA A. Analysis and Research of the Security of a Wireless Telecommunications Network Based on the IP PBX Asterisk in an OPNET Environment. Journal of Theoretical and Applied Information Technology. 2021 Jul 31;99(14):3617-30.
19. K. Salah, A. Alkhoraidly, “An Opnet based simulation approach for deploying VoIP”, International Journal of Network Management, John Wiley & Sons Ltd. V.16 issue 3, 2006, pp. 159-183.

20. A.-B.R. Suleiman, A. Hameed, “Simulation of SIP-Based VoIP for Mosul University Communication Network”, College of Electronics Eng., University of Mosul, Mosul, Iraq, 2012.
21. M.Z. Yakubova, “Calculation of Traffic Volume and Type in Asterisk IP PBX Network”, Modern Challenges and Decisions of Globalizations. International Conference. New York, USA, 2013
22. H. Al-Saadawi and A. Varol, “Voice over IP forensic approaches: A review,” May 2017. doi: 10.1109/ISDFS.2017.7916507.
23. H. Kim, H. Lee, and H. Lim, “Performance of Packet Analysis between Observer and WireShark,” in 2020 22nd International Conference on Advanced Communication Technology (ICACT), 2020, pp. 268– 271. doi: 10.23919/ICACT48636.2020.9061452
24. I. I. Androulidakis, “SPRINGER BRIEFS IN ELECTRICAL AND COMPUTER ENGINEERING VoIP and PBX Security and Forensics A Practical Approach Second Edition.” [Online]. Available: http://www.springer.com/series/10059
25.
Methods Eng 29, 1591–1610 (2022). https://doi.org/10.1007/s11831-021-09631-5