Analysis of IDS system detection for VoIP attack

Erman Hamid[1,*], Gan Hock Seng[1], Syarulnaziah Anawar[1], Zakiah Ayob[1], Najwan Khambari[1]

[1]Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia

[*]Corresponding e-mail: erman@utem.edu.my

Keywords: VoIP, IDS, security

ABSTRACT – Voice over Internet Protocol (VoIP) security tools are common tools that reached a high level of dependence among security professionals in evaluating potential vulnerabilities in such areas including operating systems, device configuration, networking protocols and applications. However, it have limitations including on where they are applied, how they are implemented and how they are maintained and updated. Furthermore, while such tools are fairly robust for more mature technology, it remains difficult to develop comprehensive security tools for emerging technology. This paper explores the known VoIP-related vulnerabilities and tests several of the more popular open source and commercial VoIP security tools with the intention of demonstrating the gap that exists between vulnerability and test the best Intrusion Detection System (IDS) for VoIP system. The outcome will help to identify what issues need to be addressed in the future development of VoIP system securit..

1. INTRODUCTION

This project is focusing on how IDS software detect the VoIP attacks, including the most happened nowadays such as Information Gathering, Eavesdropping, Attacking Authentication, VoIP Media Manipulation and Denial of Service (DoS)[1][2]. This attack will be launch directly to the servers that contain Intrusion Detection System software that has been selected to monitor the servers from any outsider and insider attacks that can harm and damage the network system itself.

From that, the project is focussed on 4 activities listed below:
1.Setup a VoIP Network.
2.Analysis type of attacking to VoIP and compare it.
3.Analysis the best system that can detect the attacker (Snort and Sax2 IDS).
4. To compare which IDS are the best in order to detect the attacks when implement in a real-time Intrusion Detection System.

2. METHODOLOGY

This project uses the combine methodology of Top Down Network Design and System Development Life Cycle (SDLC) Methodology. Top Down Network Design is a methodology for designing and developing networks, begins at the upper layers of the Open System Interconnection (OSI) model before going down to the lower layers [3][4], while the SDLC conducted to handle the entire project journey from network data retrieval, to the analysis and summary phase of the study [5]. By using the SDLC model approach; this project will have a clear documentation of development process including the network structure design, the list of the component, and the list of software that will be used on this project [6][7].

3. DESIGN

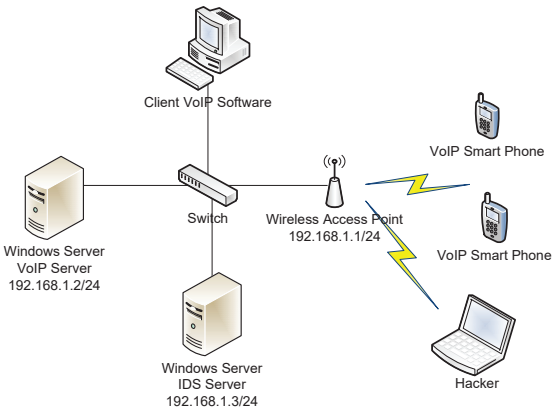

Figure 1 Network Design

Figure 1 is the **network design**, showing the full design of this project, involved real time data monitoring and at the same time analysed the captured data to provide detection for intrusion. It focussed on detecting the intrusion, without the ability to prevent the intrusion automatically.

The entire network has been setup properly by using an access point router, smart phone, a switch, two servers, and a client that acted as the attacker in order to attack the VoIP server on the network with deferent type of VoIP attacks. Two type of IDS system is used to detect the attack. One of the servers is configured as 3CX VoIP phone system server and for the client, laptop and smart phone is used, and installed with the VoIP softphone software.

One of the server is configured as Snort IDS and Sax2 IDS. The server can be easily monitored by the administrator who watch the whole activities that occurred on the network. The whole services is run with Windows Server 2008. The services is configured to test the detection of the threat that implemented on the machine. Figure 3.1 above shows the network topology for the project.

4. TESTING

The test case result in Table 1 indicates the results of each test case in form of successful detection or no detection. If the test result is no detection, the detailed description of the problem will be documented. The solution will be also stated to solve the problems so that the IDS can operates properly to meet requirement needed and the best IDS can be choosing based on the detection after the attacks launched.

Table 1 Compare the IDS system for VoIP attacks

Tools	Snort IDS	Sax2 IDS
Nmap	Yes	Yes
Smap	Yes	Yes
Zenmap	Yes	Yes
Voipong	No	No
Wireshark	No	No
Commview	No	No
Cain	No	No
RTPinject	No	Yes
ARPSpoof	No	Yes
Iaxflood	No	Yes
UDP Flooder	No	Yes
Inviteflood	No	No
RTPflood	No	Yes
airodump	No	No
aircrack-ng	No	No

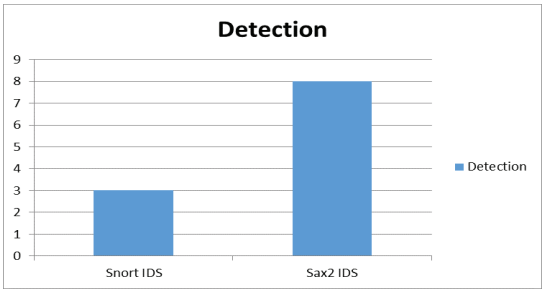

Figure 2 IDS application that detected the attack

Figure 2 above shows the bar graph showing the number of sensor tested in 1 hour when the server being attacked by VoIP attack tools. Both have different number of sensor because Snort automatically detects the sensor from the attacker in the network. The best IDS system for VoIP is the Sax2 IDS.

5. CONCLUSION

i. Functionality

From the result, Sax2 IDS can perform in real-time environment by detecting and responding to an identified attack. It will help to secure the network and the host from various attack and also viruses.

ii. Choose the best IDS

It is also concluded that the best IDS for VoIP is Sax2 IDS, based on their performance in real-time attack that tested previously. Snort and 3CX have their own strengths but after comparing this two IDS, we can concluded that Sax2 IDS are more better performance in detecting.

The Sax2 IDS ability to monitor many hosts at one time in a large network are also the reason why Sax2 IDS is better in dealing with VoIP attack. It shows that the vulnerabilities on the large network that contain a lot of hosts can be decrease.

ACKNOWLEDGEMENT

Authors are grateful to Universiti Teknikal Malaysia Melaka for the support through in conducting this study.

REFERENCES

[1] T. Surasak and C. H. Scott Huang, "Enhancing VoIP Security and Efficiency using VPN," in *2019 International Conference on Computing, Networking and Communications, ICNC 2019*, 2019.

[2] Mon Mon Aye, Naing Kyaw Soe, Zar Chi Soe, "Design and Simulation of VoIP System for Campus usage A Case Study at PTU," *Int. J. Trend Sci. Res. Dev. Int. J. Trend Sci. Res. Dev.*, 2019.

[3] P. Oppenheimer, C. A. C. Medina, F. F. Rodríguez, and E. (Universidad B. Callisaya, *Top Down Network Design*. 2014.

[4] N. U. F. Dosenbach, D. A. Fair, A. L. Cohen, B. L. Schlaggar, and S. E. Petersen, "A dual-networks architecture of top-down control," *Trends Cogn. Sci.*, 2008.

[5] J. Broad, "System Development Life Cycle (SDLC)," in *Risk Management Framework*, 2013.

[6] Tutorials Point (I) Pvt. Ltd., "Sdlc - Agile Model," *SDLC - Agil. Model*, 2015.

[7] S. S, "A Study of Software Development Life Cycle Process Models," *SSRN Electron. J.*, 2017.