NIDS On A Budget

Leonardo Juarez, ISA
University of Hawaii at West Oahu

Abstract

The NIDS: Network Intrusion Detection System project serves as a method to test the viability of using a Raspberry Pi setup to monitor a small home network and filter out the traffic. Monitoring the traffic from the internet into a home network is important because without some form of security in place users wouldn't know if the data they are receiving has a malicious code.

To carry out this project the Raspberry Pi will be programmed to act as a wall between the home networks router and internet service provider, to monitor the traffic. The two programs that will be used for this project are Snort and Zeek. Snort is an Intrusion Detection System/Intrusion Prevention System that performs deep inspection of the incoming packets, then tags packets with a signature that will detect and possibly block the traffic. Snort becomes an active blocker rather than a passive system when configured with certain rule sets. Zeek is similar to Snort, but instead of actively blocking traffic that is deemed malicious, it functions as a passive network monitor and traffic analyzer and will notify the user that malicious code has possibly entered the system and needs to be addressed.

There are many ways that someone can create their own network intrusion detection system using their own computer hardware and software, but what makes this project different is that we will be using a Raspberry Pi as the network monitoring device. A Raspberry Pi is a small computing device that is versatile and can be programmed for both attack and defense in the cyber security field. For this project, the Raspberry Pi will be used as a defense mechanism that is programmed to monitor a home network and analyze the traffic flowing to and from the internet to the devices connected to the network. Creating a home network analyzer using this device provides a lesson in basic computer programming skills as well as a better understanding of base cyber security practices that will be required in this field of work.

The results of this project will serve as a good lesson to beginner programmers and cyber security professionals who are looking for other alternatives to monitor their own personal networks using a low cost and efficient device. For beginner programmers, a Raspberry Pi is a good place to start with learning how to program a computing device because it's cheaper than buying a laptop if the person is on a budget and has many uses, such as this project of monitoring a small network. Cyber security professionals would benefit from this project because they will be able to look over the collected results and see if using a Raspberry Pi as a network intrusion detection system for a small home network is worth the cost at around $80 for setup over a subscription for a NIDS service that charges thousands of dollars.

Introduction & Research Question

Introduction

Whether it be an enterprise level network or a personal home network, threats of viruses and malware from hackers are abundant and waiting just around the corner in all shapes and forms. "Network attacks can vary from annoying email directed at an individual to intrusion attacks on sensitive data, computer information systems and critical network infrastructure." (Ghorbani et al., 2010) The purpose of malware can range from the disruption of a service in a Denial of Service attack, to worms and viruses that are used to probe a system without consent and gather information for personal use or exploitation. Having a way to protect your system from such harm is important, but can also be costly.

As society progresses further and further into the digital age, the need for security measures and practices continually rises. With the digital landscape becoming ever more vast and difficult to manage and secure, solutions must be found to secure personal information and data that is being transmitted over the network. One of those solutions include the IDS or Intrusion Detection System which was an idea first introduced by Jim Anderson in 1980. As this idea expanded and the digital landscape of internet and communications technologies grew even bigger within the past decade, the idea of the IDS developed into a new form that we call NIDS or Network Intrusion Detection System.

Research Question

Anytime a system is sending or receiving data over the network there is a possibility that the packets being received contain some form of malware or viruses. The best way to defend against such a thing from happening is to have your network continuously monitored. But how do you do that and how much will that cost you? One solution is to create a network intrusion detection system that analyzes packets that enter into your network and can either block the packet or alert the users if the packet is deemed as malicious. Programming the NIDS into a Raspberry Pi may be able to provide the necessary protection for your home network at a low cost.

Hypothesis

Putting together a NIDS system using a Raspberry Pi as the main control hub that is running both Snort and Zeek will be an affordable and feasible way to monitor a small home network and provide adequate security functionality.

Research Design & Data Collection

The purpose of this experiment is to test the theory that it is possible to create your own network intrusion detection system at an affordable price using a Raspberry Pi computing system and open source programs, Snort and Zeek.

A Raspberry Pi 4 with an external keyboard, mouse, and screen, running the ArchLinux OS that is programmed with both Snort and Zeek. The Raspberry Pi is connected to the home network router via an Ethernet cable and set up as the gateway for all network traffic from the internet to the router. Interchanging between Snort and Zeek, network traffic will flow through the pi into the home router and to the device that is sending the requests. Snort is set with rules that will analyze the incoming packets and determine if the packet that is coming through has a signature that is deemed as malicious in nature and will block the traffic going through. Zeek will be used to analyze the traffic that is entering through the network and determine if the packets entering have malicious signatures then send alerts to the system with details and log information on the packet.

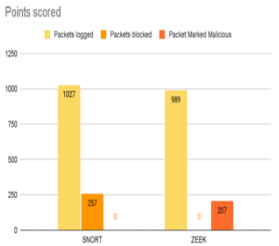

Chart 1: Running NIDS/NIPS for 1 Hour

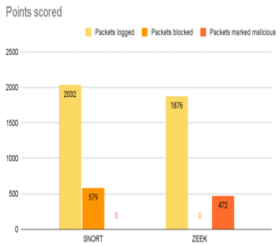

Chart 2: Running NIDS/NIPS for 2 Hours

Results

The results collected were to be expected since the Raspberry Pi system does run on a small unit and has limited memory and processing capabilities, but nonetheless the system did perform at an exceptional rate. Running the Snort program in NIDS mode for different time intervals provided a steady rate of packet logging and blocking. Further analysis may indicate that packet capturing and the rate at which the packets are entering the system may depend on the time of day that the NIDS is set up as during the day hours, web traffic flows more heavily through my home system due to having several individuals working from home. Taking the averages of the packet logging yielded 1019 packets per hour and averaging the packets blocked yielded 278 packets blocked per hour.

Under the Zeek program the number of packets that flowed through the NIDS and logged remained steady through each hour run. For the packets logged the average was 955 packets logged per hour and the average for the number of packets labeled as malicious was 226 packets per hour. Running the Zeek program has its perks as it lets you do a deeper log analysis if you so choose.

1-Hour Runtime	Packets logged	Packets blocked	Packet Marked Malicious
Snort	1027	257	0
Zeek	989	0	207

Table 1 : 1 Hour runtime of Snort and Zeek

2-Hour Runtime	Packets logged	Packets blocked	Packets marked malicious
Snort	2032	579	0
Zeek	1876	0	472

Table 2 : 2 Hour runtime of Snort and Zeek

Discussion

Using both Snort and Zeek did provide their own perks. For Snort, the program does a more aggressive scan of the incoming packets if it is set with specific rules and gauges. For Zeek, rather than doing an aggressive scan of each packet, it will log all of the packets as they flow through and enter them into a log that the users can analyze and will also flag certain packets that it deems as malicious. Running these programs on a Raspberry Pi does provide an adequate NIDS/NIPS system for a small home network as it is able to analyze and monitor the traffic flowing to and from the internet, but I did notice the system heating up at times. To alleviate this problem I made sure that the Raspberry Pi was placed in an open air setting, has a heat sink over the processor, and has a cooling fan attached to the board that will help to regulate the temperature and help to keep the system from overheating and malfunctioning. If someone were looking for a budget NIDS/NIPS system and possess basic programming skills then this Raspberry Pi system running either Snort or Zeek would suffice as it allows the user to monitor traffic as it enters and exits their network and also logs the information for analysis.

.

Conclusions

In conclusion The Raspberry Pi Network Intrusion Detection System did perform to the expected standards that was set for protecting a small home network. Overall the system and required parts totaled around $250. Normal NIDS systems purchased from other companies would cost nearly $1000+ and would perform to the same standards that this system had done. By programming the PI system to act as an intrusion detection system, it did provide lessons in understanding how to flash a PI system with ArchLinux OS and how to program both Snort and Zeek to monitor and detect malicious activity that is entering into the home network. Utilizing the open source technologies provided a better understanding in cybersecurity and how take advantage of the available programs to build a personal network monitoring system.

Contact

Leonardo Juarez
University of Hawaii at West Oahu
Email: lljuarez@hawaii.edu

Reference

S
A. Sforzin, F. G. Mármol, M. Conti and J. Bohli, "RPiDS: Raspberry Pi IDS — A Fruitful Intrusion Detection System for IoT," 2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), 2016, pp. 440-448, doi: 10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld.2016.0080.
2. *About Zeek*. About Zeek - Book of Zeek (git/master). (2021, September 29). Retrieved September 20, 2021, from https://docs.zeek.org/en/master/about.html.
3. Acar, F. (2018, December 17). *What is Snort?* Medium. Retrieved September 15, 2021, from https://medium.com/@acarmurathakku/what-is-snort-547918aec45f
4. Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2020). Network intrusion detection system: A systematic study of machine learning and Deep Learning Approaches. *Transactions on Emerging Telecommunications Technologies*, *32*(1). https://doi.org/10.1002/ett.4150
5. Ghorbani, A. A., Lu, W., & Tavallaee, M. (2010). *Network intrusion detection and Prevention Concepts and Techniques*. Springer US
6. Modi, C. N., Patel, D. R., Patel, A., & Rajarajan, M. (2012, November 12). *Integrating signature apriori based network Intrusion Detection System (NIDS) in cloud computing*. Procedia Technology. Retrieved November 11, 2021, from https://www.sciencedirect.com/science/article/pii/S221201731200655X.
7. Siemons, F. (2021, May 27). *Open source ids: Snort or suricata? [updated 2021]*. Infosec Resources. Retrieved September 20, 2021, from https://resources.infosecinstitute.com/topic/open-source-ids-snort-suricata/
8. *Snort-network intrusion detection and prevention system*. Fortinet. (n.d.). Retrieved November 11, 2021, from https://www.fortinet.com/resources/cyberglossary/snort.
9. Walker, M. from D., Walker, D., Christopher Escobedo Hart | Nov 04, 03, S. C. | N., 28, E. B. | O., Teri Robinson | 2 hours ago, Michael Visard | 1 day ago, & Richi Jennings | 1 day ago. (2020, March 3). *Intrusion detection systems: A deep dive into Nids & Hids*. Security Boulevard. Retrieved November 11, 2021, from https://securityboulevard.com/2020/03/intrusion-detection-systems-a-deep-dive-into-nids-hids/.
10. *Zeek ids: Powerful cybersecurity tool you've never heard of*. Bricata. (2020, October 28). Retrieved November 11, 2021, from https://bricata.com/blog/zeek-ids-threat-detection/.