Research Article.
Journal of Intelligent Systems: Theory and Applications 3(2) 2020: 21-24.
DOI: 10.38016/jista.653486

Raspberry Pi Firewall and Intrusion Detection System

Oğuzhan Karahan[1*], Berat Kaya[2*]

[1,2] Kocaeli University,Department of Electronics and Telecommunications Engineering, Kocaeli,Turkey

Abstract

Information is the most essential building block to businesses, thus having adequate control over it is indispensability for most. Such control allows for better security and overall administration for a company. The existing solution is to install a firewall to the root switch, enabling admins to manage traffic by interfacing with the firewall equipment. This paper proposes a light-weight and highly configurable firewall solution for small to mid-range businesses. Built on a Raspberry Pi, including a user-friendly interface, with little information individuals will able to configure and install the firewall to their businesses. The proper solution will enable high-level control over the desired ports and user groups. Access to potentially harmful information can effortlessly be moderated and blocked if necessary.

Keywords: Raspberry pi, firewall, network security, intrusion detection.

Raspberry Pi ile Güvenlik Duvarı ve Saldırı Tespit Sistemi

Öz

Bilgi, işletmeler için en temel yapıtaşıdır. Bu nedenle bilgi üzerinde yeterli kontrol sahibi olmak vazgeçilmezdir. Bu kontrol, bir şirket için daha iyi güvenlik ve genel yönetim sağlar. Bu güvenliği sağlamanın yolu bütün ağı denetleyecek bir güvenlik duvarı kurmaktır. Güvenlik duvarı, şirketlerin ağları üzerindeki cihazları ve bilgisayarları diğer ağlar üzerinden gelecek saldırılara karşı koruyan, iç ve dış ağlar arası ağ trafiğini belirli kurallara göre denetleyen bir güvenlik mekanizmasıdır. Güvenlik duvarı üzerinde belirtilmiş kurallara uymayan trafik engellenerek koruma sağlanır. Bu çalışmada düşük maliyetli cep bilgisayarı Raspberry Pi ve ağ anahtarı kullanılarak küçük veya orta ölçekli bir işyeri ağı modellemesi üzerinde güvenlik duvarı ve saldırı tespit sistemi yapılmıştır. Bu ağa bağlı bilgisayarlara Raspberry Pi üzerinden internet erişimi sağlanmıştır. Ağdaki bilgisayarlara yapılan ataklar Raspberry Pi üzerinden gözlemlenmiştir ve yazılan kurallar sayesinde kolayca engellenmiştir.

Anahtar Kelimeler: Raspberry Pi, güvenlik duvarı, ağ güvenliği, saldırı tespit sistemi.

1. Introduction

One of the biggest problems of today is to secure our computers. Moreover, this problem gets bigger if the issue is a networked computer [1]. It has become very important to prevent intruders from accessing our information using the network. The people who leak the remote machines with bad faith are called intruders [2]. It is tried to prevent this situation by using various technologies. One of these measures is to use a firewall. It is a security mechanism that protects your devices and computers on your current network against attackers and controls traffic between internal and external networks according to certain rules. The other one is to use an intrusion detection system to monitor the network traffic for suspicious activity.

Many devices and applications are used even in home networks. Attackers are developing new types of attacks to infiltrate our internal network. To protect against these attacks, it has become compulsory to use firewall systems. Basically, the firewall decides whether or not the packets that arrive on the network can pass through according to predefined rules. It provides protection by blocking traffic that does not comply with the rules specified on the firewall.

Large companies have been using firewall devices to protect their internal networks for more than 25 years.

* Corresponding Author.
E-mail: berat_kaya_2356@hotmail.com

Recieved : Dec 6, 2019
Revision : Apr 9, 2020
Accepted : May 20, 2020

At this point, restaurants, houses, hospitals, cafes, shops and it started to be used even in similar small networks.

Structuring a firewall with an intrusion detection system is the security standard of today [3]. In this paper, it is shown how intrusion detection system works with a sample scenario by using Snort software on Raspberry Pi computer. The Raspberry Pi is connected to a network switch which has two configured virtual area networks (VLAN) to make a wider network. Hosts are connected to different VLANs. The aim is to enable the intrusion detection system to operate on a larger network like workplaces.

In other studies, Raspberry Pi is working as a firewall connected to only one device. In this study, a network is divided into segments by using the VLAN feature of the network key and multiple computers are secured.

The structure of this paper is organized as follows: Section 2 provides a brief review of literature. Section 3 introduces the architecture of the system and explain a sample attack scenario. In section 4, the results of the scenario are presented and Section 5 presents the conclusions.

2. Methodology

A review of literature is provided in this section including Raspberry Pi, Intrusion Detection System and Snort.

2.1. Raspberry Pi

Raspberry Pi is a low cost, credit card sized pocket PC. It is a computer that compiles the algorithms of Internet of things (IoT) or robotic projects we imagine and manages electronic elements. It runs with Linux based operating systems. Raspian is the operating system (OS) which is used in this project. It has also variety of models for different requirements. Raspberry Pi 3 has a built-in wifi module so it is practical when wireless connection needed. These computers, which are shown in Figure 1, are preferred in listening to network traffic and collecting data because of their simple interface and strong processors [4].

Figure 1. Raspberry pi 3 model B

2.2. Network Switch

Figure 2. Cisco catalyst 3560-CG 8 port switch

The switch used in this project is shown in Figure 2. Switch configuration requires console and power cable. After the power and console cable is connected, the putty program is run from the computer and the serial interface is used to access the switch interface. Since the project requires two independent networks, the vlan feature of the switch was used. In order to create a VLAN, enable mode must be entered.

In order for the commands written here to affect the network, the general configuration mode should be switched. In this mode, the VLAN should be created by typing the desired VLAN and its number.

```
Switch > enable
Switch # configure terminal
Switch (config)# vlan 10
Switch (config-vlan)#name LAN1
Switch (config)# vlan 20
Switch (config-vlan)#name LAN2
Switch (config-vlan)# interface range gig0/1-4
Switch (config-if)# switchport access vlan 10
Switch (config-vlan)# interface range gig0/5-8
Switch (config-if)# switchport access vlan 20
Switch (config) # interface gig0/9
Switch (config-if) # switchport trunk encapsulation dot1q
Switch (config-if) # switchport mode trunk
Switch (config) # interface Vlan 10
Switch (config-if) # ip address 10.0.0.254 255.255.255.0
Switch (config-if) # no shutdown
Switch (config) # interface Vlan 20
Switch (config-if) # ip address 20.0.0.254 255.255.255.0
Switch (config-if) # no shutdown
```

Figure 3. VLAN configuration

In Figure 3, two VLANs must be created for two different networks. Names of the VLANs are LAN1 and LAN2. The created vlans are assigned to the desired ports. The first 4 ports of the switch are configured for VLAN10. The last 4 ports of the switch are configured for Vlan20. A trunk port is created for Raspberry Pi to control the VLANs. Trunk port is a switch port which all VLAN information can be passed. After configuring the trunk port, VLANs are given preferred IP addresses. In the project, IP addresses of 10.0.0.254 for VLAN10 and 20.0.0.254 for VLAN20 were used. DHCP is configured on the switch so that the computers

connected to the ports can receive IP from the corresponding VLAN IP block.

```
Switch (config) # ip dhcp pool Vlan10-Pool
Switch (config) # network 10.0.0.0 255.255.255.0
Switch (config) # default-router 10.0.0.1
Switch (config) # dns-server 8.8.8.8
Switch (config) # ip dhcp pool Vlan20-Pool
Switch (config) # network 20.0.0.0 255.255.255.0
Switch (config) # default-router 20.0.0.1
Switch (config) # dns-server 8.8.8.8
```

Figure 4. IP DHCP pool

DHCP configuration is done with the commands in Figure 4. Computers connected to one of the first 4 ports will receive the IP address from the VLAN10 IP block and the VLAN20 IP block when plugged into the last 4 ports. The switch configuration is now complete.

2.3. Intrusion Detection System

Intrusion Detection Systems are devices or software for monitoring malicious activities or policy violations against networks or systems. IDS systems have the ability to monitor the network frequently, identify potential threats and log related events, stop attacks, and report to security administrators. When an attack occurs, it also reconfigures network devices such as firewalls or routers blocking attacks in the same way [5]. Figure 5 shows the intrusion detection system architecture.

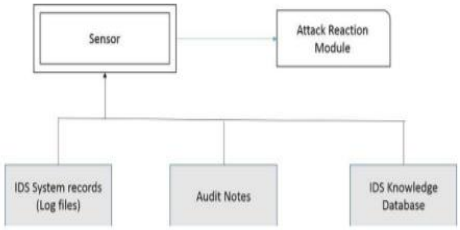

Figure 5. Designed system architecure

2.4. Snort

Snort is an open source intrusion detection and intrusion prevention system, first developed by Martin Roesch [7]. It allows users to create their own security rules. Snort is a software that can perform real-time traffic analysis and packet logging on IP networks.

3. System Architecture

In the study, as hardware components; Cisco Catalyst 3560-CG switch, Raspberry Pi 3, 2 laptops are used. An architecture of the system is given in Figure 6.

This architecture allows hosts that are connected to switch via VLANs access internet through Raspberry Pi's proxy. The purpose of the proxy is to level up the security. Gateway is used as a proxy for intrusion detection task by the architecture [8].

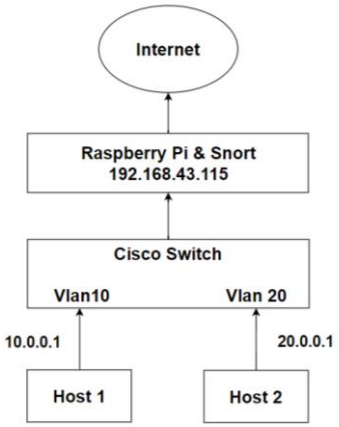

Figure 6. Designed system architecture

3.1. Creation of system architecture

Folders are created to keep the configuration files. Empty rule files are created in these folders. A folder is also created to hold the access logs. We have to give Snort the privilege to read the files.

```
$ sudo chmod -R 5775 /etc/snort
$ sudo chmod -R 5775 /var/log/snort
$ sudo chmod -R 5775 /usr/local/lib/snort_dynamicrules
$ sudo chown -R snort:snort /etc/snort
$ sudo chown -R snort:snort /var/log/snort
$ sudo chown -R snort:snort /usr/local/lib/snort_dynamicrules
```

Figure 7. Giving privilege to Snort

Then, we inform Snort the network address which the system is connected and Snort saves it as a home address. From this moment every rule we write will apply to the system.

```
$ sudo nano /etc/snort/snort.conf
Ipvar HOME_NET 192.168.43.0/24
```

Figure 8. Configuring the Snort file

3.2. Creating Snort rules

Three different access types have been identified for the intrusion detection system: Packet Internet Groper (PING), Secure Shell (SSH) and File Transfer Protocol (FTP). Ping is used to find out if the computer of the given ip address is running in terms of TCP / IP, and if so, to see how much time it takes to reach that computer. FTP is a protocol for transferring files between two computers connected to the Internet and the name given to the application serving this process. It operates on port 21.

1. Rule: alert icmp any any -> $HOME_NET any (msg:"Ping Attempt"; SID:1000004; rev:1)
2. Rule: alert tcp any any -> $HOME_NET 21 (msg: FTP connection attempt"; SID: 1000009; rev:1)

Rule 1 will alert the system if there is a PING request from any IP adress to the home address. “Ping Attempt” message will appear on the screen

Rule 2 will alert the system if there is a FTP request from any IP adress to the home address.“FTP connection attempt” will appear on the screen.

3.3. Scenario

Firstly, Host 1 will make PING and FTP request to the system.

10.0.0.1: Ping 192.168.43.115

10.0.0.1: Ftp 192.168.43.115

Secondly, Host 2 will make PING and FTP request to the system.

20.0.0.1: Ping 192.168.43.115

20.0.0.1: Ftp 192.168.43.115

4. Results

Figure 9. Working of the system

Figure 13 shows the warnings given by Snort intrusion detection system. Section 1 shows the date and time the detection was made. Section 2 shows the messages and protocols we specify in the intrusion detection rules. The last part shows the source of the attack and the destination of the attack. If the first line is examined, Host 1 whose IP address 10.0.0.1 has requested a ping to the system with IP address 192.168.43.115. “Ping Attempt” warning is displayed. Note that there was no response to the ping request in the opposite direction. The request is timed out. The user who made the attack did not receive any response from the system. Similarly, on the fifth line, when user tried to establish an FTP connection, he did not receive any response. The request is timed out. The same operations were performed for Host 2 and the same results were obtained. This shows that Raspberry Pi’s firewall settings are well configured.

5. Conclusions

There are a lot of applications and devices with special futures on the market. Everyone should use the materials that are suitable for their needs. This study shows a proxy intrusion detection system based on low cost Raspberry Pi device and open source Snort software. The system has been tested with two simple attacks to see if the system can capture the unwanted events. The network is expanded with the switch and the results show the system works successfully on small scale networks. In the future, the system can be tested with more hosts and much more complex attacks. The maximum attack capacity of this system can be measured. the system can be updated against newly derived attacks.

Acknowledgement

You can write here, if any, the people, institutions or supporters (you can specify support numbers and supporters) before the resources section.

References

Bellovin, S. M., & Cheswick, W. R. (1994). Network firewalls. IEEE communications magazine, 32(9), 50-57.

Ashoor, A. S., & Gore, S. (2011). What is the difference between Hackers and Intruders. Int. J. Sci. Eng. Res, 2(7), 1-3.

Lalitha, M., Meachery, N., & Nair, R. (2018). Raspberry PI Based Cyber-Defensive Industrial Control SystemWith Redundancy And Intrusion Detection. International Journal of Pure and Applied Mathematics, 118(20), 4273-4278.

Coşar, M., & Kiran, H. E. (2018, May). Measurement of Raspberry Pi performance in network traffic analysis. In 2018 26th Signal Processing and Communications Applications Conference (SIU) (pp. 1-4). IEEE.

Coşar, M., & Karasartova, S. (2017, October). A firewall application on SOHO networks with Raspberry Pi and snort. In 2017 International Conference on Computer Science and Engineering (UBMK) (pp. 1000-1003). IEEE.

Mahajan, S., Adagale,M. A., & Sahare, C.(2016, March). Intrusion Detection System Using Raspberry PI Honeypot in Network Security. International Journal of Engineering Science and Computing, Volume 6, No:3, DOI 10.4010/2016.651.

Roesch, M. (1999, November). Snort: Lightweight intrusion detection for networks. In Lisa (Vol. 99, No. 1, pp. 229-238).

Oktay, U., & Sahingoz, O. K. (2013, May). Proxy network intrusion detection system for cloud computing. In 2013 the international conference on technological advances in electrical, electronics and computer engineering (TAEECE) (pp. 98-104). IEEE.