

|  |
| --- |
|  |
| October 02  text divider  Digital Empowerment Pakistan Foundation  Authored by: Muhammad Hassan Yaseen |

Security Audit Reportcolored rectanglewhite rectangle for text on cover

Date: 02nd October, 2024

Task 4: Configuring Firewalls and Intrusion Detection Systems

Report

Introduction:

The aim of this assignment is to harden the network by implementing firewalls and Intrusion Detection Systems (IDS). This paper outlines the measures taken in order to configure the Uncomplicated Firewall (UFW) and Snort as the IDS solution.

Methodology:

The following steps were taken to complete this task:

1. Installing and configuring UFW:
   * Installed UFW on the Ubuntu system using the command sudo apt-get install ufw.
   * Configured UFW to allow incoming traffic on specific ports using the commands sudo ufw allow ssh, sudo ufw allow http, and sudo ufw allow https.
2. Configuring UFW rules and policies:
   * Configured UFW rules to allow incoming traffic on specific ports using the commands sudo ufw allow from 192.168.1.100 to any port 80 and sudo ufw allow in on eth0 to any port 80 proto tcp.
3. Installing and configuring Snort:
   * Installed Snort on the Ubuntu system using the command sudo apt-get install snort.
   * Configured Snort to monitor network traffic using the command sudo snort -c /etc/snort/snort.conf -i eth0.
4. Analyzing Snort alerts and responding to threats:
   * Analyzed Snort alerts using the command sudo snort -c /etc/snort/snort.conf -i eth0 -A console.
   * Configured Snort to send alerts to a specific email address using the command sudo snort -c /etc/snort/snort.conf -i eth0 -A email -e admin@example.com.
5. Regularly updating and maintaining the configurations:
   * Updated the UFW rules using the command sudo ufw reload.
   * Updated the Snort rules using the command sudo snort -c /etc/snort/snort.conf -i eth0 -u.

Results:

We got these outcomes: We set up UFW and made it work for letting specific ports receive data. We set rules in UFW to allow certain ports to get incoming traffic. We put Snort in place and set it up to keep an eye on network activity. We looked at and acted on the alerts Snort gave us. We kept the settings up to date and in good shape.

Conclusion:

To wrap up, we finished this job by setting up UFW and Snort to keep the network safe. This report laid out the steps we took to get the job done, and we're happy with how it turned out.

Recommendations:

Based on the results obtained, the following recommendations are made:

* Regularly update and maintain the UFW and Snort configurations to ensure the network remains protected.
* Monitor Snort alerts regularly to respond to potential threats.
* Consider implementing additional security measures, such as intrusion prevention systems, to further protect the network.

Coding:-

UFW Configuration Script:

#!/bin/bash

2

3# Install and configure UFW

4sudo apt-get update

5sudo apt-get install ufw

6

7# Allow incoming traffic on specific ports

8sudo ufw allow ssh

9sudo ufw allow http

10sudo ufw allow https

11

12# Configure UFW rules to allow incoming traffic on specific ports

13sudo ufw allow from 192.168.1.100 to any port 80

14sudo ufw allow in on eth0 to any port 80 proto tcp

15

16# Reload UFW rules

17sudo ufw reload

Snort Configuration Script:

#!/bin/bash

2

3# Install and configure Snort

4sudo apt-get update

5sudo apt-get install snort

6

7# Configure Snort to monitor network traffic

8sudo snort -c /etc/snort/snort.conf -i eth0

9

10# Analyze Snort alerts and respond to threats

11sudo snort -c /etc/snort/snort.conf -i eth0 -A console

12sudo snort -c /etc/snort/snort.conf -i eth0 -A email -e admin@example.com

13

14# Update Snort rules

15sudo snort -c /etc/snort/snort.conf -i eth0 -u

UFW and Snort Configuration Script:

#!/bin/bash

2

3# Install and configure UFW and Snort

4sudo apt-get update

5sudo apt-get install ufw snort

6

7# Allow incoming traffic on specific ports

8sudo ufw allow ssh

9sudo ufw allow http

10sudo ufw allow https

11

12# Configure UFW rules to allow incoming traffic on specific ports

13sudo ufw allow from 192.168.1.100 to any port 80

14sudo ufw allow in on eth0 to any port 80 proto tcp

15

16# Configure Snort to monitor network traffic

17sudo snort -c /etc/snort/snort.conf -i eth0

18

19# Analyze Snort alerts and respond to threats

20sudo snort -c /etc/snort/snort.conf -i eth0 -A console

21sudo snort -c /etc/snort/snort.conf -i eth0 -A email -e admin@example.com

22

23# Reload UFW rules and update Snort rules

24sudo ufw reload

25sudo snort -c /etc/snort/snort.conf -i eth0 -u

Python Script to Automate UFW and Snort Configuration:

import subprocess

2

3# Define the UFW and Snort configuration commands

4ufw\_commands = [

5 "sudo apt-get update",

6 "sudo apt-get install ufw",

7 "sudo ufw allow ssh",

8 "sudo ufw allow http",

9 "sudo ufw allow https",

10 "sudo ufw allow from 192.168.1.100 to any port 80",

11 "sudo ufw allow in on eth0 to any port 80 proto tcp",

12 "sudo ufw reload"

13]

14

15snort\_commands = [

16 "sudo apt-get update",

17 "sudo apt-get install snort",

18 "sudo snort -c /etc/snort/snort.conf -i eth0",

19 "sudo snort -c /etc/snort/snort.conf -i eth0 -A console",

20 "sudo snort -c /etc/snort/snort.conf -i eth0 -A email -e admin@example.com",

21 "sudo snort -c /etc/snort/snort.conf -i eth0 -u"

22]

23

24# Execute the UFW and Snort configuration commands

25for command in ufw\_commands:

26 subprocess.run(command, shell=True)

27

28for command in snort\_commands:

29 subprocess.run(command, shell=True)