**Project 2: Build and Configure a Firewall**

Building and configuring a firewall is crucial for protecting networks from unauthorized access and potential threats. In this project, I set up and configured a firewall on an Ubuntu system using UFW (Uncomplicated Firewall).

**Prerequisites**

Before beginning this project, I ensured that I had:

* Basic knowledge of Linux commands
* An Ubuntu system (physical or virtual machine)
* Root or sudo access

**Step-by-Step Guide**

**Step 1: Update Your System** To ensure my system was up to date, I ran the following commands:

sudo apt update

sudo apt upgrade -y

**Step 2: Install UFW** Since UFW is included in most Ubuntu installations by default, I installed it manually in case it was not present:

sudo apt install ufw

**Step 3: Enable UFW** By default, UFW is disabled after installation. I enabled it with the command:

sudo ufw enable

I confirmed the action by typing y and pressing Enter.

**Step 4: Allow SSH Connections** To prevent locking myself out of the system, I allowed SSH connections:

sudo ufw allow ssh

Alternatively, I could have specified the port number:

sudo ufw allow 22/tcp

**Step 5: Allow Specific Services and Ports** I configured UFW to allow specific services and ports:

1. Allow HTTP and HTTPS traffic:

sudo ufw allow http

sudo ufw allow https

Or by specifying the ports:

sudo ufw allow 80/tcp

sudo ufw allow 443/tcp

1. Allow other specific ports:

sudo ufw allow 8080/tcp

1. Allow a range of ports:

sudo ufw allow 1000:2000/tcp

1. Allow specific IP addresses:

sudo ufw allow from 192.168.1.100

1. Allow specific subnets:

sudo ufw allow from 192.168.1.0/24

**Step 6: Deny Specific Services and Ports** By default, UFW blocks all incoming connections except for the ones explicitly allowed. I also denied certain connections explicitly:

1. Deny a specific port:

sudo ufw deny 23/tcp

1. Deny a specific IP address:

sudo ufw deny from 203.0.113.0

**Step 7: View UFW Status and Rules** To check the status of UFW and view the current rules:

sudo ufw status verbose

**Step 8: Delete UFW Rules** If I needed to remove a rule, I could delete it using its rule number or the exact rule specification.

1. Using rule number:

sudo ufw status numbered

sudo ufw delete 2

1. Using rule specification:

sudo ufw delete allow 8080/tcp

**Step 9: Advanced UFW Configuration (Optional)**

1. Enable logging:

sudo ufw logging on

1. Set default policies to deny all incoming and allow all outgoing traffic:

sudo ufw default deny incoming

sudo ufw default allow outgoing

1. View and allow application profiles:

sudo ufw app list

sudo ufw allow 'Nginx Full'

**Step 10: Testing the Firewall**

1. Check open ports using nmap from another machine:

nmap -v -A 192.168.1.10 # Replace with the actual IP

1. Check connection by attempting to connect to allowed and denied services.

**Step 11: Document Your Setup**

1. Firewall Rules:

sudo ufw allow ssh

sudo ufw allow http

sudo ufw allow https

sudo ufw allow from 192.168.1.0/24

sudo ufw deny 23/tcp

1. Configuration Details: Documented configuration details of the firewall, including default policies and any logging or application profiles used.

**Conclusion**

I successfully set up and configured a firewall on my Ubuntu system using UFW. This setup helps protect my network from unauthorized access and potential threats. I plan to refine my firewall rules based on my network's needs and monitor the logs for any suspicious activity.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated