

Network Segmentation & Security Workflow Documentation

Overview

In this project, I set up a basic network segmentation using VLANs, demonstrated Zero Trust principles, configured secure static routing, and connected two security tools in a simple workflow. The environment was simulated using GNS3 and Parrot OS to mimic a real-world secure network configuration.

A. Virtual Networking Setup

1. GNS3 Installation (Optional)

Although GNS3 was not strictly required, I installed it to better simulate the network:

```
bash
```

```
sudo apt install gns3-gui -y
```

Note: Parrot OS network settings can also be used for simple simulations.

B. VLAN Implementation

1. Switch Simulation with VLANs

- I created two virtual PCs: **PC1** and **PC2**.
- Configured two VLANs on a simulated switch:
 - **VLAN 10:** Assigned to PC1
 - **VLAN 20:** Assigned to PC2

2. Connectivity Test

- From PC1, I attempted to ping PC2.
- **Result:** No connectivity, confirming VLAN isolation.=

C. Zero Trust Principles

1. SSH Setup for Secure Access

- Installed the OpenSSH server on Parrot OS:

```
bash
```

```
sudo apt install openssh-server -y
```

2. User Creation for Access Control

- Created a new user for secure SSH access:

```
bash
```

```
sudo adduser secureuser
```

3. SSH Access Restriction

- Edited SSH configuration to restrict access to the new user:

bash

```
[user@parrot]~$ sudo adduser secureuser
Adding user `secureuser' ...
Adding new group `secureuser' (1005) ...
Adding new user `secureuser' (1005) with group `secureuser (1005)' ...
Creating home directory `/home/secureuser' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for secureuser
Enter the new value, or press ENTER for the default
    Full Name []: .
    Room Number []: .
    Work Phone []: .
    Home Phone []: .
    Other []: .
Is the information correct? [Y/n] y
Adding new user `secureuser' to supplemental / extra groups `users' ...
Adding user `secureuser' to group `users' ...
[user@parrot]~$
```

sudo nano /etc/ssh/sshd_config

- Modified line:

nginx

AllowUsers secureuser

- Restarted SSH to apply changes:

bash

sudo systemctl restart ssh

```
[user@parrot]-[~]
└─ $AllowUsers secureuser
bash: AllowUsers: command not found
[x]-[user@parrot]-[~]
└─ $sudo nano /etc/ssh/sshd_config
[user@parrot]-[~]
└─ $sudo systemctl restart ssh
[user@parrot]-[~]
└─ $
```

E. Security Tool Wo

rkflow

1. IDS + Defense Script Integration

- Simulated a basic work
- flow:
 - **Tool 1:** Snort detects a suspicious IP.
 - **Tool 2:** Manually triggered a defense script to block that IP.

2. Visual Diagram

- Created a simple flowchart showing the process:
mathematica

IDS Alert (Snort) → Manual Review → Run Block Script

-

IDS Alert



Manual
review



Execution
of block script

