Defense In Depth (DID)

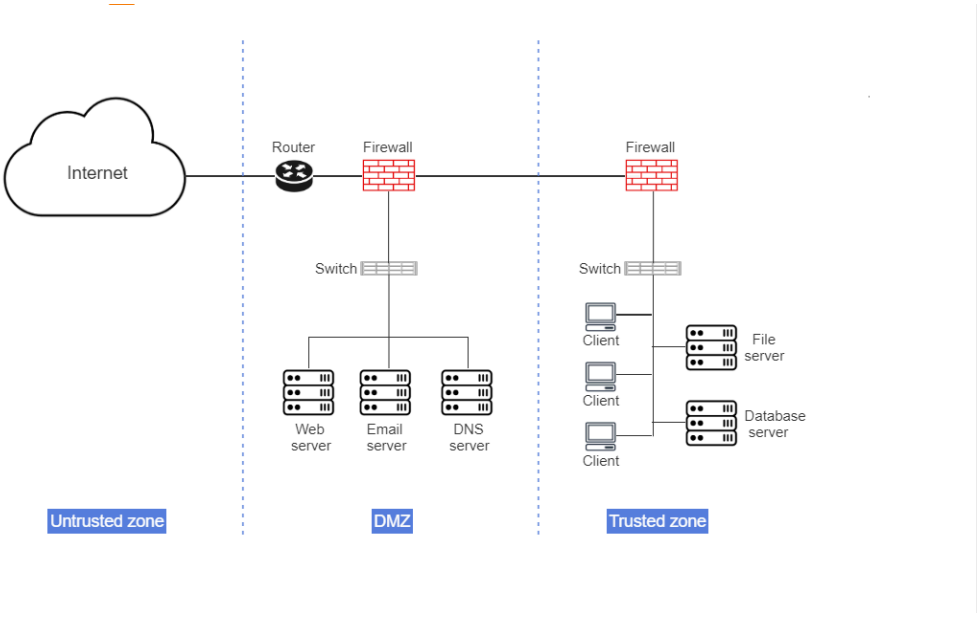
Executive Summary

Kevin, Zahedi, Rogelio & Tai

Monday 4, 2023

Introduction:

This project, Defense In Depth, aims to understand how an organization's security system is structured on a smaller scale. With the knowledge received through the semester, the team has built three zones/interfaces the Untrusted zone, the Demilitarized zone, and the trusted zone using various hardware (resources) and software. Within that hardware (resources), we can mention a firewall, a web server, an email server, a database server, a file server, a DNS server, and a Syslog server. Using Raspberry PIS and Rock 64 For the software, we can cite Raspbian OS, Kali Linux, OpenVAS, and pfSense. In addition, we were able to demonstrate some potential attacks on the server within the network. The following schema visually summarizes the project.



Email Server: On a Rock 64, Tai in charge of the email server, used PostFix and a software called SendMail to be able to send and potentially receive an email, by giving it a domain (rock64@guilfordctis370.com). The Email server is used on port 25, and it's placed within the DMZ. For the attack, a phishing email was sent to demonstrate our first attack.

OpenVAS: For vulnerability scanning, we chose OpenVAS, and Tai in charge was able to download the software on Linux. To demonstrate the use of OpenVAS, we did a vulnerability scan on the network targeting the Web server.

Web Server & Firewall: Kevin was in charge. To create the web server, Apache was downloaded alongside PHP and Docker for containerization. Once it's ready, we have uploaded a static web server for a more realistic project.

The attack is to use Slowloris on a Linux environment to demonstrate a DDOS attack. To accomplish this, run “python3 slowloris.py (your IP address) -s 500”. To remedy this, we can use some rules on the firewall to do so.

For the firewall, Kevin used pfSense. After tumultuous attempts, we created the three zones and provided some rules to demonstrate the capabilities of doing so and allowing port forwarding to get access to Web servers from the internet. Then we added some aliases and were capable of getting traffic through all three zones.

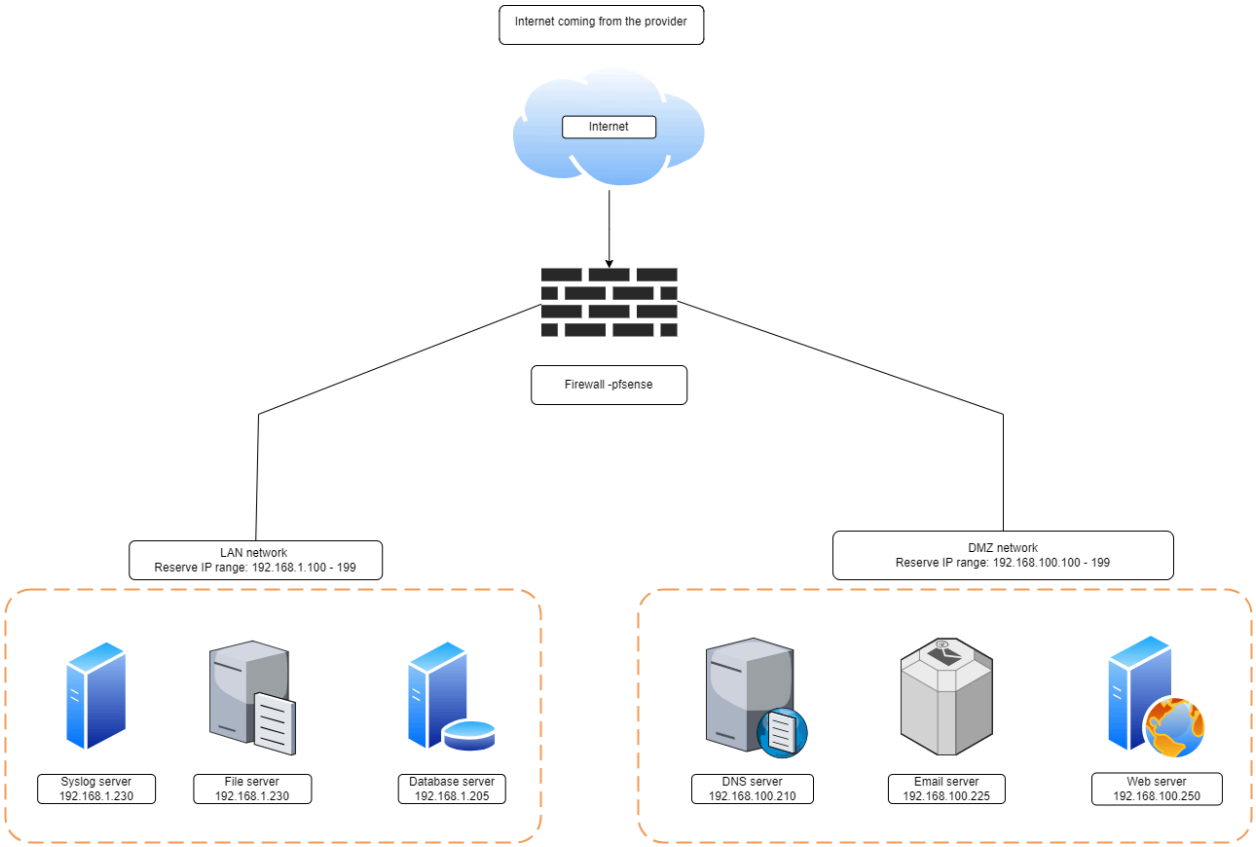
The attack consists of an unsecured firewall with weak credentials that give access to anyone on the network to commit a crime. To rectify this attack, much stronger credentials are urged.

File Server and Syslog Server: Both of those servers were for Zahedi. We chose two servers in one since both belong to the trusted zone. The software used for the file server is called Samba. It contains some files that can be accessed through various computers on the network. As a side project, I also created a miniDLNA server. This server can be accessed from many smart TVs. Our Syslog server was created on the same Raspberry Pi, as both are going to be placed in our trusted zone. The Syslog was added to the firewall setting to receive all the logs. As pfSense can connect to a remote server to send logs without the need to log into the firewall itself.

For the attack, a man-in-the-middle was used with the Pineapple Pi (rogue access point) to get the credentials of the server and attack the resources. I was also able to see what other devices were connected to the file server when they connected to the access point. To remedy this attack, We need much stronger passwords and education on why users shouldn't connect to any network if not trusted. We also need to be sure we are on a secure private network and not a public one.

DNS and Database Server: Rogelio was assigned this part of the project. We implement the DNS to give names to the IP addresses by installing and using Dnsmasq. For the attack, we used Ettercap on the Kali environment to direct a domain to another customized IP. For instance, Google.com would be redirected to a custom domain set by the attacker.

The database was done by using phpMyAdmin, MySQL, and MariaDB, the table was generated to showcase the advanced work on the server. An attack for it was password cracking by using Intruder & Metasploit.


Internet coming from the provider
Internet
Firewall -pfsense
LAN network
Reserve IP range: 192.168.1.100 - 199
DMZ network
Reserve IP range: 192.168.100.100 - 199
Syslog server
192.168.1.230
File server
192.168.1.230
Database server
192.168.1.205
DNS server
192.168.100.210
Email server
192.168.100.225
Web server
192.168.100.250