Secure Network Architecture Design

Ryan Coon

CYB-525

Dr. Emmett Ward

January 8, 2025

Part 1:

Design a corporate infrastructure diagram in Visio or another network mapping tool (this deliverable must be readable by your professor; Cisco Packet Tracer is not acceptable). Your network diagram must include a minimum of 2 routers, 2 firewalls, 4 switches, 1 IDS, 1 IPS, a proxy server, an email server, a DHCP server, a DMZ, and finally, 5 separate departments utilizing network segmentation with a minimum of 25 clients per department. You must also include an air gapped system for your R&D department to utilize.

**Fictional Company Diagram Design:**

**Create a Windows 11 VM and join it to the domain.**

A screenshot of a computer

Description automatically generated

Set up new VM with Windows 11 ready to install.

A computer screen shot of a computer screen

Description automatically generated

Add the DWords in the registry editor before continuing with install.

A computer screen shot of a beach

Description automatically generated

Windows 11 installed successfully. Will now turn off server and add network internal network to have it connect through pfsense.

A screenshot of a computer

Description automatically generated

Server started after connecting it to internal network. Ran ipconfig and we can see that we have an ip address from pfsense.

A screenshot of a computer

Description automatically generated

Connected to the Windows Server 2019 DHCP

A screenshot of a computer

Description automatically generatedAdded STATION3 to be used for our Windows 11 VM.

A screenshot of a computer

Description automatically generated

Added user MICKEY MOUSE to be used on the Windows 11 VM.

A screenshot of a computer

Description automatically generated

New user MMOUSE now connected to the WHATEVER domain with the Windows 11 VM.

**Create a VM using an operating system of your choice that has not been created yet. It could be a different version of Windows or Linux. It is not necessary to join this VM to the domain.**

A screenshot of a computer

Description automatically generated

Creating a new VM with Debian 12

A screenshot of a computer

Description automatically generated

Installing Debian 12 to Virtual Box as a new VM.

A screenshot of a computer

Description automatically generated

Debian 12 on the successful installation

A screenshot of a computer

Description automatically generated

Debian 12 VM signed in and ready to work.

**Using your Kali Linux VM, perform a GVM Full and Fast vulnerability scan of your entire VirtualBox infrastructure:**

A screenshot of a computer

Description automatically generated

Scan targets to include all VM’s from within the VirtualBox infrastructure.

A screenshot of a computer

Description automatically generated

Full and fast scan results on the VM targets.

**Select 2-3 intellectual tools (e.g., Suricata, pfSense, Snort, etc.) and demonstrate how they work together to create a framework. Make sure to include them in your secure network design. Do not use Suricata, pfSense, or Snort for this part of the assignment:**

The three intellectual tools that were selected Included Cisco Secure Firewall, Cisco Secure IPS, and OSSEC IDS:

“Cisco Secure Firewall provides unified management of firewalls, application control, intrusion prevention, URL filtering, and malware defense policies. Secure Firewall provides faster threat protection with industry leading Snort 3 Intrusion Detection and Prevention System (IDS/IPS)”(Cisco, 2023).

“Cisco NGIPS markets their Secure IPS product as a next generation intrusion prevention system (NGIPS) with over 35,000 built-in IPS rules and broad capabilities for detecting and blocking anomalous traffic. Secure IPS can be integrated with other Cisco devices or deployed as a standalone IPS.”(Samson, 2023).

“OSSEC is a host-based IDS that is produced by a longrunning open-source project. It’s been widely downloaded and used — the project receives more than 500,000 downloads a year — and works on Windows, macOS, and a host of Unix-like systems, including Linux. OSSEC monitors the logs various system components generate in real time, and can detect changes to individual files, including allimportant Windows registry files. While primarily an IDS, OSSEC can also respond to attacks, using both its own capacities and integration with third-party tools”(Strom, 2020).

Cybersecurity is a multi-layered approach to protecting individuals and organizations from online threats. It involves implementing a series of tools and controls that act as a "defense in depth" strategy. This means that even if one layer of security is compromised, others are in place to prevent further damage.

For example, a company might use a Cisco Secure Firewall to control access to their private network. This firewall acts as the first line of defense, filtering incoming and outgoing traffic based on predefined security rules.

To further strengthen security, additional tools like Cisco NGIP Intrusion Protection System and OSSEC Intrusion Detection System can be deployed. These systems continuously monitor the network for suspicious activity and take immediate action to prevent attacks.

By combining these tools, organizations create a robust security framework that protects their data and systems from a variety of threats. This layered approach ensures that even if one layer is breached, the remaining defenses can effectively contain the attack.

**Part 2:**

Screencast URL:

References:

Cisco. (2024). *Cisco Secure Firewall At-a-Glance*. Cisco. https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/at-a-glance-c45-736624.html

Samson Jr, R. (2020, July 28). *Top 10 Intrusion Detection and Prevention Systems*. ClearNetwork, Inc. https://www.clearnetwork.com/top-intrusion-detection-and-prevention-systems/

Strom, D. (2020, March 30). *Top 6 IDS/IPS tools — plus 4 open-source alternatives*. CSO Online. https://www.csoonline.com/article/569085/12-top-idsipstools.html