Access Control Firewall Assessment Lab

Ryan Coon

CYB-525

Dr. Emmett Ward

November 27, 2024

Part 1 Screenshots:

A computer screen shot of a dragon logo

Description automatically generated

Log into my Kali VM

A screenshot of a computer

Description automatically generated

Next I ran an nmap scan on the pfSense ip address 192.168.1.1 to discover any hosts and open/closed ports.

A screenshot of a computer

Description automatically generated

I then opened up the pfSense dashboard on Firefox web browser. Once logged in I navigated to the section by clicking systems, then update to pull up the update screen to check for any applicable update. The application version status shows up to date.

A screenshot of a computer

Description automatically generated

Enabled https and changed port to 8443.

On the browser click on system, then advanced

click HTTPS (SSL/TLS)

In TCP port section enter 8443

A screenshot of a computer

Description automatically generated

Once information correctly entered, scroll to the bottom and click save.

A screenshot of a computer

Description automatically generated

Notification you will receive when you click save, screen will refresh and you will have to click to accept the risk to get to pfSense dashboard.

A screenshot of a computer

Description automatically generated

Navigate to the pfSense dashboard and click the plus button to the right. Then click on the traffic graphs button to display the WAN and LAN traffic graphs on the dashboard.

A screenshot of a computer

Description automatically generated

Navigate to firewall aliases by clicking the firewall button in the header, then clicking aliases. Create a new port alias with the World of Warcraft port information. Click save.

A screenshot of a computer

Description automatically generated

We then want to create a block rule for the WOW ports. Navi9gate to this by clicking on firewall, then rules. Click add to create the rule to block the WOW ports.

A screenshot of a computer

Description automatically generated

Once the information is entered correctly, scroll to the bottom of the page and click save. It will then redirect you back to the rules page. You will now see the new rule to block WOW ports.

A screenshot of a computer

Description automatically generated

We want to create a new rule to block inbound ICMP. As we are still on the firewall rules page, click add. Under the protocol drop down select ICMP.

A screenshot of a computer

Description automatically generated

Once information is entered, scroll to the bottom of the page and click save. You will then be redirected to the main rules page. You will now see that the block ICMP rule is added and active.

A screenshot of a computer

Description automatically generated

Created a new alias for Facebook.com. Click firewall then click alias. Click add and enter information along with the url. I created an alias for the social media site Facebook.com.

A screenshot of a computer

Description automatically generated

Created a new rule to block Facebook by clicking on firewall, then rules. Under lan I then clicked add. Selected block as the action with any protocol. I added Facebook as the alias.

A screenshot of a computer

Description automatically generated

Once the information is verified, scroll to the bottom and click save. You will be redirected to the rules list page. You will now see the social media blocker rule active.

A screenshot of a computer

Description automatically generated

Created a new alias for Netflix.com. Click firewall then click alias. Click add and enter information along with the url. I created an alias for the video streaming site Netflix.com.

A screenshot of a computer

Description automatically generated

Created a new rule to allow Netflix by clicking on firewall, then rules. Under lan I then clicked add. Selected pass as the action with any protocol. I added Netflix as the alias.

A screenshot of a computer

Description automatically generated

Once the information is verified, scroll to the bottom and click save. You will be redirected to the rules list page. You will now see the Netflix Allow rule active.

A screenshot of a computer

Description automatically generated

Port scan after the activity was completed. You can now see as compared to the port scan at the beginning, port 8443 is now open.

Part 2:

**Summarize the issues encountered, lessons learned, and successes in a bullet point format.**

As far as issues encountered, I really did not come across any. Once I found documentation on what was expected, everything is pretty straight forward. Everything expected of us is labeled clearly within the pfSense dashboard.

* Was successfully able to complete assignment with ease

**Describe the screenshots provided.**

All screenshots have thorough descriptions under each one.

**Examine a specific architecture and identify potential vulnerabilities. Include a description of 2-3 vulnerabilities of the hybrid network used in this lab.**

When examining a hybrid network architecture that utilizes Kali Linux for penetration testing and pfSense as a firewall and router, it's essential to identify potential vulnerabilities that could be exploited by attackers. A hybrid network typically combines on-premises infrastructure with cloud services, which can introduce unique security challenges. Three vulnerabilities with this hybrid setup would be:

Misconfiguration of pfSense:

pfSense  be vulnerable if not configured correctly. Common misconfigurations include:

Weak Passwords: Using default or weak passwords for administrative access can allow unauthorized users to gain control over the firewall.

Open Ports: Leaving unnecessary ports open can expose the network to external threats, making it easier for attackers to exploit services running on those ports.

Vulnerabilities in Kali Linux: is widely used for penetration testing, but it can also introduce vulnerabilities if not properly secured. Some common issues include:

Outdated Software: Running outdated versions of tools or the operating system can expose known vulnerabilities that attackers can exploit.

Excessive Permissions: Granting unnecessary permissions to users or applications can lead to privilege escalation, allowing an attacker to execute malicious actions with elevated rights.

Insecure API Endpoints: In a hybrid network, especially when integrating cloud services, insecure API endpoints can be a significant vulnerability. This includes:

Lack of Authentication: APIs that do not require proper authentication can be accessed by anyone, allowing attackers to manipulate data or services.

Data Exposure: APIs that do not implement proper encryption can expose sensitive data during transmission.

**Explore in-depth advanced and novel areas of networks and protocols. Include a description of what you learned from exploring the networks and protocols in this lab.**

There are three main types of protocols - Network management, Network communication, Network security. Within these types contains the actual protocol themselves - HTTP (hypertext transfer protocol) – this the language of the internet, especially. TCP (transmission control protocol) – this separates the data into packets, that way it can be easily shared. ICMP (internet control message protocol) – this is a diagnostic protocol; it gives the information over the network that may be errors. It also provides the information for connectivity issues.

References:

Attard, M. (2023, September 25). *Top 9 Cybersecurity Risks in the Hybrid Workplace*. BMIT. https://www.bmit.com.mt/blog/top-9-cybersecurity-risks-in-the-hybrid-workplace/

Duy-Nguyen, J. (2021, October 29). *Three Blind Spots to Avoid When Securing a Hybrid Network | CISO Collective*. Fortinet Blog. https://www.fortinet.com/blog/ciso-collective/three-blind-spots-to-avoid-when-securing-a-hybrid-network

kmbh. (2021, November 22). *Types of Network Protocols and Their Uses*. GeeksforGeeks. https://www.geeksforgeeks.org/types-of-network-protocols-and-their-uses/

Liu, T. (2022, June 29). *Reducing Security Vulnerabilities in a Hybrid Workplace*. ISACA. https://www.isaca.org/resources/isaca-journal/issues/2022/volume-3/reducing-security-vulnerabilities-in-a-hybrid-workplace

SentinelOne. (2024, November 6). *Top 6 Hybrid Cloud Security Challenges*. SentinelOne. https://www.sentinelone.com/cybersecurity-101/cloud-security/hybrid-cloud-security-challenges/