CY3001-NETWORKS AND CYBERSECURITY-II
FALL 2024
ASSIGNMENT#4
Building a Secure Network with pfSense, Suricata, and DMZ.

Objective:

The objective of this assignment is to design, implement, and secure a simple network using pfSense as the firewall, Suricata as the intrusion detection system, and a DMZ to protect critical resources.

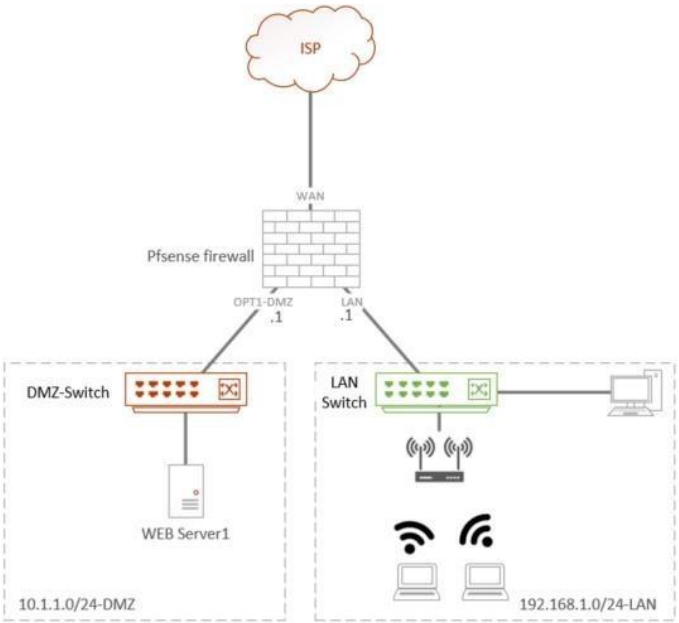
Part 1: Network Setup

Network Topology: Create a simple network topology consisting of the following components:

- An internal LAN network with at least one client machine.
- A DMZ with a Web server (nginx)
- A pfSense firewall with three network interfaces: WAN, LAN, and DMZ.
- IP Addressing: Assign appropriate IP addresses to each component of the network. Ensure that they are in separate subnets:

  LAN Network
  DMZ Network
  WAN Network

Routing: Configure routing on pfSense to ensure that traffic flows between the LAN, DMZ, and WAN networks as required.



Part 2: pfSense Configuration

pfSense Installation: Install and configure pfSense on a dedicated machine or virtual machine.
Firewall Rules: Set up firewall rules on pfSense to allow or block traffic as follows:

Firewall Rules:
Create and document specific firewall rules, including source and destination IP addresses, ports, and action (allow or block) for each rule.
Include rules for DNS, HTTP, and HTTPS traffic to pass from LAN to WAN and DMZ.
Demonstrate the order of rule execution (top-down) in your report.

Part 3: Suricata Installation and Configuration

Suricata Installation: Install and configure Suricata on pfSense to act as an intrusion detection system (IDS).
Rules and Alerts: Configure Suricata to use appropriate rulesets and generate alerts for potential security threats. Test the system with simulated attacks (you can use tools like Nmap or Metasploit for this purpose).

Rules and Alerts:

- Download and activate a Suricata ruleset of your choice (e.g., Emerging Threats).
- Configure Suricata to generate alerts for specific types of traffic (e.g., port scans, malware signatures).
- Include in your report examples of Suricata alerts and explain their significance.

Part 4: DMZ Configuration

DMZ Setup: Place the web server in the DMZ network and configure pfSense to allow traffic from the Internet to reach the web server while maintaining security.

DMZ Setup:

- Place the web server in the DMZ network and assign it a static IP address.
- Create specific firewall rules to allow HTTP and HTTPS traffic from the Internet to reach the web server in the DMZ.
- Ensure that other types of traffic are blocked from reaching the DMZ.
- Install and configure Nginx as the web server software on the designated web server machine.
- Ensure that Nginx is set up to listen on the appropriate ports (typically, ports 80 and 443 for HTTP and HTTPS).
- Use ‘Port Forwarding’ to access the webserver from WAN

In summary, Implement the following firewall rules:

1. Allow Incoming Traffic from the Internet to DMZ on ports: 80, 443
2. Allow traffic from DMZ to WAN on ports: 53, ICMP and 123 (NTP)
3. Block traffic from LAN to DMZ except ICMP and SSH for administration purposes
4. Block traffic from LAN to DMZ except port 80 to access the web server
5. Allow ICMP (ping) traffic from the LAN network to the WAN network while limiting the rate of ICMP requests to prevent ICMP flooding.
6. Allow DNS (port 53) traffic from the LAN network to specific DNS servers on the Internet.
7. Allow access to limited number of Websites from LAN; Block everything else
8. Block all incoming traffic from WAN to LAN except those mentioned above

Part 5: Documentation and Reporting

Documentation: Create a detailed documentation report that includes:

- Network topology diagram.
- Configuration steps for pfSense, Suricata, and DMZ.
- Firewall rule tables.
- Suricata alert logs (include a few examples).
- Any issues faced during setup and how they were resolved.

Part 6: Demo

Presentation: Prepare a brief presentation to explain the design and security measures implemented in your network. Present any interesting findings or challenges encountered during the setup.

Demo of your assignment is compulsory. Without the demo, you may be marked zero for the assignment.

Assessment:

Students will be assessed based on the following criteria:

1. Correctness and completeness of network setup. [20]
2. Effectiveness of firewall rules and DMZ configuration. [20]
3. Appropriate use of Suricata for intrusion detection. [20]
4. Quality of documentation and presentation. [30]
5. Demonstrated understanding of network security principles (Viva).[10]

Submssion: Your submission will be a single pdf report following the naming convention i201234_A2.pdf, any report with incomplete steps or no screenshots will be marked as zero.