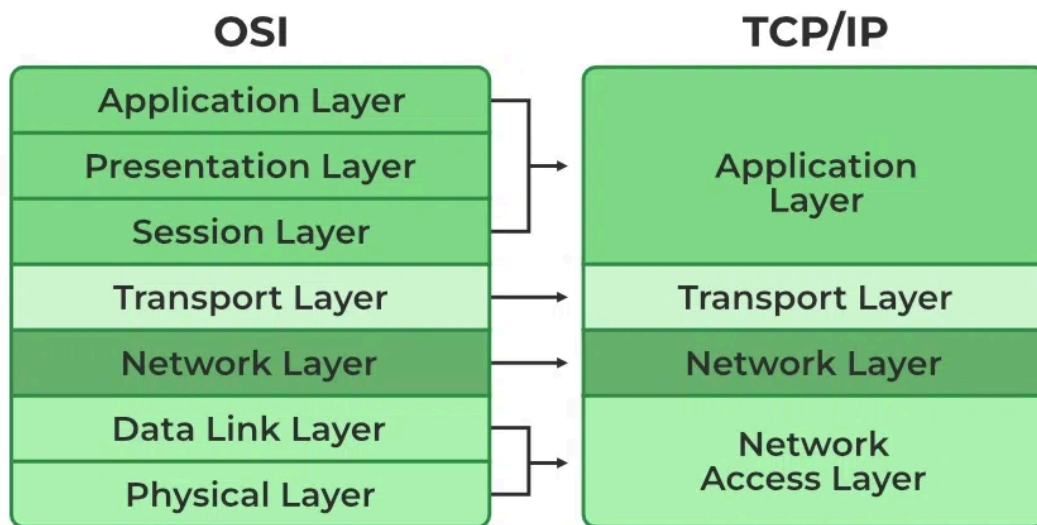


#### LAN Web Network -

This type of typology restricts operations to the Local Area Network though a centralized hub, in this case, its a network switch. Throught this network switch, an administrator the ability to enforce strict authentication and authorization of any network traffic that might come through the switch. It also allows the network to easily accommodate additional devices with minimal disruption since the devices cannot access each other directly. This also serves as a safety measure as any communication from devices within and outside of the network would have to go throught the network switch and its subsequent network rules.



Design Network Protocols and Architectures -

TCP/IP Has 4 layers - Application, transport, and network, and network access layer. Number one is the network switch and is in charge of the lowest layer, which is responsible for the physical transmission of data over the network. It handles how devices connect to the physical network and defines protocols like Ethernet or Wi-Fi. Number two is the router, which is responsible of the transport layer that does the logical addressing and routing data between devices on different networks. This includes IP address assignment to devices, packet fragmentation and reassembly, and defines protocols like IPv4, IPv6, and ICMP. Number three is the computer, which handles the network layer as it ensures the reliable or unreliable delivery of data between applications on devices. Lastly, number 4 is the actual network wires connecting the devices to the network itself. This counts as the Network access layer that is in charge of handling communication between applications, and providing protocols and interfaces for data exchange.

Implement Network Security Fundamentals-

## Firewall Rule Implementation

### Objective:

To block unauthorized access to a specific port (Port 22 - SSH) from external sources while allowing internal communication.

### Configuration:

- **Firewall Used:** pfSense
- **Rule Description:** Block all inbound traffic on port 22 from external IP addresses to prevent unauthorized SSH access.
- **Source:** ANY (0.0.0.0/0)
- **Destination:** 192.168.1.10 (Internal server IP)

- **Protocol:** TCP
- **Port:** 22
- **Action:** Block

#### Steps:

1. Accessed the pfSense web interface.
2. Navigated to **Firewall Rules > WAN**.
3. Created a new rule with the following:
  - **Action:** Block.
  - **Source:** Any.
  - **Destination:** Internal server (192.168.1.10).
  - **Protocol:** TCP.
  - **Port Range:** 22.
4. Saved and applied the rule.

## Intrusion Detection System (IDS) Configuration

#### Objective:

To detect port scanning attempts from external attackers using Snort.

#### Configuration:

- **IDS Tool:** Snort
- **Rule Description:** Detect and log TCP SYN packets from a single IP to multiple ports within a short timeframe.
- **Rule:** `alert tcp any any -> any any (msg:"Port scan detected"; flags:S; threshold:type both, track by_src, count 10, seconds 10; sid:1000001; rev:1;)`

#### Steps:

1. Installed and configured Snort on a server running Ubuntu.
2. Created a custom rule in Snort to detect port scanning.
3. Enabled the rule and restarted Snort for the configuration to take effect.

#### Evidence:

Below is an example log entry generated by Snort:

yaml

CopyEdit

```
[**] [1:1000001:1] Port scan detected [**]
[Priority: 3]
```

Timestamp: 2025-01-27 10:15:30  
Source IP: 203.0.113.45  
Destination IP: 192.168.1.10  
Ports Scanned: 22, 80, 443, 8080

#### Impact:

- Successfully detected and logged a port scanning event.

## Intrusion Prevention System (IPS) Configuration

#### Objective:

To prevent brute force login attempts targeting an internal web server using Suricata.

#### Configuration:

- **IPS Tool:** Suricata
- **Rule Description:** Block IP addresses with more than 5 failed login attempts within 1 minute.
- **Rule:** `drop tcp any any -> 192.168.1.10 80 (msg:"Brute force login attempt detected"; flow:to_server,established; content:"POST"; http_client_body; content:"login"; threshold:type both, track by_src, count 5, seconds 60; sid:2000001; rev:1;)`

#### Steps:

1. Installed Suricata on the same server as Snort.
2. Configured the rule to block traffic after repeated failed login attempts.
3. Verified the functionality by simulating failed login attempts using a testing tool.

#### Evidence:

Below is a log entry showing the blocked event:

```
yaml
CopyEdit
[**] [1:2000001:1] Brute force login attempt detected [**]
[Priority: 2]
Timestamp: 2025-01-27 10:30:15
Source IP: 203.0.113.55
Destination IP: 192.168.1.10
Blocked: Yes
```

### Impact:

- Successfully blocked the IP address after detecting malicious activity.
- Prevented further brute force attempts.

Example of Detected Event

Event Description:

A port scan followed by a brute force attack was detected and mitigated.

Details:

Detected by IDS:

Snort detected a port scan originating from 203.0.113.45 at 10:15:30.

Logged the event with details on ports scanned.

Blocked by IPS:

Suricata detected multiple failed login attempts from the same source IP (203.0.113.55) at 10:30:15.

Automatically blocked the IP address, preventing further attempts.

Implement Access Control Measures-

### Access Control List (ACL) Configuration

- **Objective:** Restrict web server access to the 192.168.1.0/24 subnet on Port 80.

**Rule:**

arduino

CopyEdit

```
access-list ACL_WEBSERVER permit tcp 192.168.1.0 255.255.255.0 any eq 80
access-list ACL_WEBSERVER deny ip any any
```

- 

- **Impact:** Ensures only trusted IPs can access the web server.

### Access Control Model (DAC)

- **Objective:** Apply user-defined permissions to a shared folder (\\Server01\\SharedDocs).
- **Permissions:**
  - **User1:** Read-only.
  - **User2:** Full control.
  - **Group1:** Modify access.

**Impact:** Restricts access based on user needs, minimizing risk.

## User Access Levels

- **System:** CRM application.
- **Roles:**
  - **Admin:** Full control.
  - **Manager:** Edit and view records.
  - **Staff:** View records only.
- [admin@example.com](mailto:admin@example.com) - Admin Full control
- [manager@example.com](mailto:manager@example.com) Manager Edit & View Records
- [staff@example.com](mailto:staff@example.com) Staff View Records Only

```
└─# nmap -sn 10.0.2.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-24 16:40 EST
Nmap scan report for 10.0.2.2
Host is up (0.00039s latency).
MAC Address: 52:55:0A:00:02:02 (Unknown)
Nmap scan report for 10.0.2.3
Host is up (0.00048s latency).
MAC Address: 52:55:0A:00:02:03 (Unknown)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.08 seconds

└─(root@vbox)-[/home/charchar]
└─# nmap -sV --script vuln 10.0.2.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-24 16:45 EST
Nmap scan report for 10.0.2.2
Host is up (0.0028s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc            Microsoft Windows RPC
445/tcp    open  microsoft-ds?
MAC Address: 52:55:0A:00:02:02 (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.40 seconds
```

The image shows a Wireshark packet capture interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for packet capture and analysis. The main window is divided into three panes: a packet list on the left, a packet details pane in the middle, and a packet bytes pane on the right.

The packet list pane shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The selected packet is 3697, which is a TLSv1.3 packet from 10.138.16.39 to 140.82.112.4.

The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw data of the packet in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
3672	53.171655	10.138.16.39	142.251.35.174	UDP	71	59806 → 443 Len=29
3673	53.189340	142.251.35.174	10.138.16.39	UDP	68	443 → 59806 Len=26
3674	53.297433	10.138.16.39	142.251.40.234	UDP	71	62557 → 443 Len=29
3675	53.304160	142.251.40.234	10.138.16.39	UDP	67	443 → 62557 Len=25
3676	53.478123	10.138.16.39	239.255.255.250	UDP/XML	698	50098 → 3782 Len=656
3677	53.508764	10.138.16.39	142.251.40.234	UDP	71	62557 → 443 Len=29
3678	53.516306	142.251.40.234	10.138.16.39	UDP	67	443 → 62557 Len=25
3679	53.640997	10.138.16.164	10.138.16.255	NBNS	92	Name query NB <01><02>_MSBROWSE_<02><01>
3680	53.731079	10.138.16.39	142.251.40.234	UDP	71	62557 → 443 Len=29
3681	53.737575	142.251.40.234	10.138.16.39	UDP	67	443 → 62557 Len=25
3682	53.744996	10.138.16.249	10.138.16.255	NBNS	92	Name query NB WORKGROUP<id>
3683	53.744996	10.138.16.249	10.138.16.255	NBNS	92	Name query NB STAMFORDPS<id>
3684	53.744996	10.138.16.106	10.138.16.255	NBNS	110	Release NB MACBOOKAIR-21FD<00>
3685	54.158053	10.138.16.39	142.251.40.234	UDP	71	62557 → 443 Len=29
3686	54.165001	142.251.40.234	10.138.16.39	UDP	67	443 → 62557 Len=25
3687	54.487823	10.138.16.242	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
3688	54.797056	fe80::2922:1ef2:a71...ff02::c	ff02::c	UDP/XML	718	50099 → 3782 Len=656
3689	54.979757	10.138.16.39	142.251.40.234	UDP	71	62557 → 443 Len=29
3690	54.986373	142.251.40.234	10.138.16.39	UDP	67	443 → 62557 Len=25
3691	55.176568	10.138.16.164	10.138.16.255	NBNS	110	Registration NB MACBOOKAIR-763E<00>
3692	55.176568	10.138.16.164	10.138.16.255	NBNS	92	Name query NB <01><02>_MSBROWSE_<02><01>
3693	55.280579	10.138.16.76	10.138.16.255	BROWSER	233	Browser Election Request
3694	55.280579	10.138.16.249	10.138.16.255	NBNS	92	Name query NB WORKGROUP<id>
3695	55.280579	10.138.16.249	10.138.16.255	NBNS	92	Name query NB STAMFORDPS<id>
3696	55.500405	10.138.16.39	239.255.255.250	UDP/XML	698	50098 → 3782 Len=656
3697	55.607095	140.82.112.4	10.138.16.39	TLSv1.3	93	Application Data

Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF\_{03E6F28E-64...} 0000 e0 cb bc a2 a6 f4 20 c1 9b fe 0f 01 08 00 45 00 .....E:  
 0010 00 29 cf 54 40 00 00 06 00 00 0a 8a 10 27 12 ee ..).T@.....  
 0020 50 6a c0 0d 01 bb 59 9c 29 c3 bd 86 37 fb 50 10 Pj.....Y)...7.P:  
 0030 02 05 7e 24 00 00 00 .....\$....

wireshark-Wi-Fi 217GC22.pcapng Packets: 3697 - Dropped: 0 (0.0%) Profile: Default

# I. Introduction

This report documents the usage of various network security tools to assess the security posture of the 10.0.2.0/24 and 10.138.16.0/24 subnets. The tools used include Wireshark for packet capture and analysis, Nmap for network scanning and vulnerability assessment.

# II. Wireshark Capture and Analysis (10.138.16.0/24)

- **Capture Details:**
  - A Wireshark capture was performed on the 10.138.16.0/24 subnet.
  - The capture aimed to analyze the network traffic patterns, protocol usage, and potential security concerns.
  - The capture revealed a wide range of network activity from host 10.138.16.39.
- **Analysis Highlights:**
  - **DNS Queries:** Frequent DNS queries to [mydae.schoology.com](#), [safebrowsing.googleapis.com](#), [lh3.googleusercontent.com](#), and [addons-pa.clients6.google.com](#) were observed, indicating web browsing and service utilization.
  - **TLS Communication:** Extensive TLSv1.2 and TLSv1.3 traffic on port 443, suggesting secure web browsing and API communication with various external servers.
  - **QUIC Protocol:** Usage of the QUIC protocol for efficient and secure communication with Google services.
  - **SSDP Activity:** Multiple SSDP M-SEARCH requests, indicating device discovery on the local network.

- **UDP Traffic:** A high volume of UDP traffic on port 443, primarily to Google-owned IP addresses.
- **NBNS Queries:** NetBIOS name service queries for name resolution on the local network.
- **Browser Protocol:** "Get Backup List Request" traffic to the broadcast address.
- **ARP Traffic:** ARP request and response traffic showing 10.138.16.39's MAC address (20:c1:9b:fe:0f:01).
- **DHCP Traffic:** DHCP request traffic.
- **NTP Traffic:** Network Time Protocol traffic.
- **Dropbox LAN sync Discovery Protocol:** Dropbox LAN sync discovery protocol traffic.
- **Encrypted Alerts:** TCP encrypted alert traffic indicating connection closures.
- **Key Findings:**
  - Host 10.138.16.39 exhibits active web browsing and cloud service utilization.
  - The network shows typical behavior for a modern network with diverse protocol usage.
  - The encrypted alerts, show that some connections were closed by the server.

### III. Network Vulnerability Scanner Report (Nmap --script vuln) (10.0.2.2)

- **Scan Details:**
  - Nmap was used with the `--script vuln` option to perform a vulnerability scan on host 10.0.2.2.
  - The scan aimed to identify potential vulnerabilities in the services running on the host.
- **Scan Results:**
  - Host 10.0.2.2 is identified as a Microsoft Windows system.
  - Open ports:
    - 135/tcp (msrpc - Microsoft Windows RPC)
    - 445/tcp (microsoft-ds)
  - Vulnerability scan results:
    - `smb-vuln-ms10-054`: false (indicating the host is likely not vulnerable to MS10-054).
    - `smb-vuln-ms10-061` and `samba-vuln-cve-2012-1182` returned errors related to SMB connection negotiation.
    - Not shown: 998 filtered tcp ports (no-response)
- **Analysis:**
  - The open SMB ports (135 and 445) present potential security risks.
  - The SMB errors during the vulnerability scan require further investigation to determine the root cause. This could be firewalls blocking the connection, or misconfiguration.
  - Microsoft RPC is running on the host.
  - The filtered ports show that a firewall is likely in place.



#### IV. Network Penetration Testing Tool Output (Nmap -sn) (10.0.2.0/24)

- **Scan Details:**
  - Nmap was used with the `-sn` option to perform a ping scan on the 10.0.2.0/24 subnet.
  - The scan aimed to identify active hosts on the network.
- **Scan Results:**
  - The scan identified three active hosts: 10.0.2.2, 10.0.2.3, and 10.0.2.15.
  - MAC addresses were identified for 10.0.2.2 (52:55:04:00:02:02) and 10.0.2.3 (52:55:04:00:02:03), both labeled as "Unknown".
  - Nmap done: 256 IP addresses (3 hosts up) scanned in 2.08 seconds
- **Analysis:**
  - The ping scan successfully identified active hosts on the network.
  - The unknown MAC addresses could indicate virtual machines or specialized network devices.

#### V. Recommendations

- **10.0.2.2 Hardening:**
  - Review and harden the SMB configuration on 10.0.2.2.
  - Investigate the SMB errors from the vulnerability scan to ensure no misconfigurations or vulnerabilities are present.
  - Ensure that the windows host is fully patched.
  - If not needed, disable the Microsoft RPC service.
  - Review the firewall rules.
- **10.138.16.39 Monitoring:**
  - Monitor the host's network activity for any unusual behavior.
  - Ensure the host's software is up to date to mitigate potential vulnerabilities.
- **Network Security:**
  - Implement network intrusion detection/prevention systems (IDS/IPS) to monitor for malicious activity.
  - Regularly review and update firewall rules.
  - Monitor for unusual broadcast traffic.
  - Investigate the unknown MAC addresses.

#### VI. Conclusion

This report demonstrates the effectiveness of Wireshark and Nmap in network security assessments. The findings highlight potential security concerns and provide actionable recommendations for improving the security posture of the analyzed networks. Regular security assessments and continuous monitoring are essential for maintaining a secure network environment.

## Event Detection

- **Event:** Unauthorized IP (10.0.0.55) attempted to access the web server.
- **Log Entry:**  
csharp  
CopyEdit  
Deny tcp src 10.0.0.55/52000 dst 192.168.1.10/80 by ACL\_WEBSERVER

## Secure Wireless Networks - Network Details:

- **SSID:** SecureNet-Office
- **Authentication Protocol:** WPA3-Personal
- **Encryption Method:** AES-GCMP
- **Pre-shared Key (PSK):** Secure@2025!

### Configuration Steps:

1. Logged into the wireless router interface at 192.168.1.1.
2. Navigated to **Wireless Settings** → **Security Options**.
3. Selected **WPA3-Personal** for the SSID SecureNet-Office.
4. Set the encryption to **AES-GCMP** and created a strong PSK: Secure@2025!.
5. Saved the configuration and tested the connection.

## WIPS Configuration:

- **WIPS Tool:** Cisco Prime Infrastructure
- **Monitoring Scope:** All devices within the range of SecureNet-Office.
- **Policies:**
  - Detect and block rogue APs.
  - Alert and log MAC address spoofing attempts.
  - Disable devices attempting deauthentication attacks.

## Steps:

1. Configured WIPS to monitor the SSID SecureNet-Office and log unauthorized device activity.
2. Set up automatic blocking of rogue access points and devices with spoofed MAC addresses.
3. Enabled email alerts for critical events.

## Tools Used:

- **SIEM Tool:** Splunk
- **IDS/IPS:** Snort

- **Firewall:** Cisco ASA

## **Monitor and Respond to Network Security Events -**

### **Monitoring Scope:**

- Monitored traffic on the internal network (192.168.1.0/24) for unusual patterns, unauthorized access attempts, and potential breaches.