Email: diyasoni906@gmail.com

Name: Diya

Nmap Scan Results

## Date: 2025-06-24

## Scanned IP Range: 192.168.44.0/24

### Summary of Findings

- Active Hosts: 4 hosts are up in the network.  
- Open Ports: Only one open port was found:  
 - 192.168.44.2 has port 53 open (Service: Domain).  
- Filtered Ports: Other hosts have all ports filtered, meaning they did not respond to the scan.

### Detailed Scan Results

1. 192.168.44.1  
 - Status: Host is up  
 - Ports: All 1000 scanned ports are in ignored states.  
 - Filtered Ports: 1000 filtered TCP ports (no response).  
 - MAC Address: 00:50:56:C0:00:08 (VMware)  
  
2. 192.168.44.2  
 - Status: Host is up  
 - Ports:  
 - 53/tcp: Open (Service: Domain)  
 - Closed Ports: 999 closed TCP ports (reset).  
 - MAC Address: 00:50:56:F8:D5:14 (VMware)  
  
3. 192.168.44.254  
 - Status: Host is up  
 - Ports: All 1000 scanned ports are in ignored states.  
 - Filtered Ports: 1000 filtered TCP ports (no response).  
 - MAC Address: 00:50:56:EC:AC:45 (VMware)  
  
4. 192.168.44.128 (Your Host)  
 - Status: Host is up  
 - Ports: All 1000 scanned ports are in ignored states.  
 - Closed Ports: 1000 closed TCP ports (reset).

### Research on Open Port

- Port 53 (DNS):  
 - Commonly used for DNS services.  
 - Potential vulnerabilities include DNS spoofing and amplification attacks.

### Security Recommendations

- Restrict access to the DNS service to trusted IP addresses.  
- Regularly update the DNS software to patch vulnerabilities.  
- Monitor DNS traffic for unusual patterns.

### Conclusion

This scan provides a basic overview of the network's exposure and highlights the need for security measures on the open DNS port.

## Scan Output Screenshots



