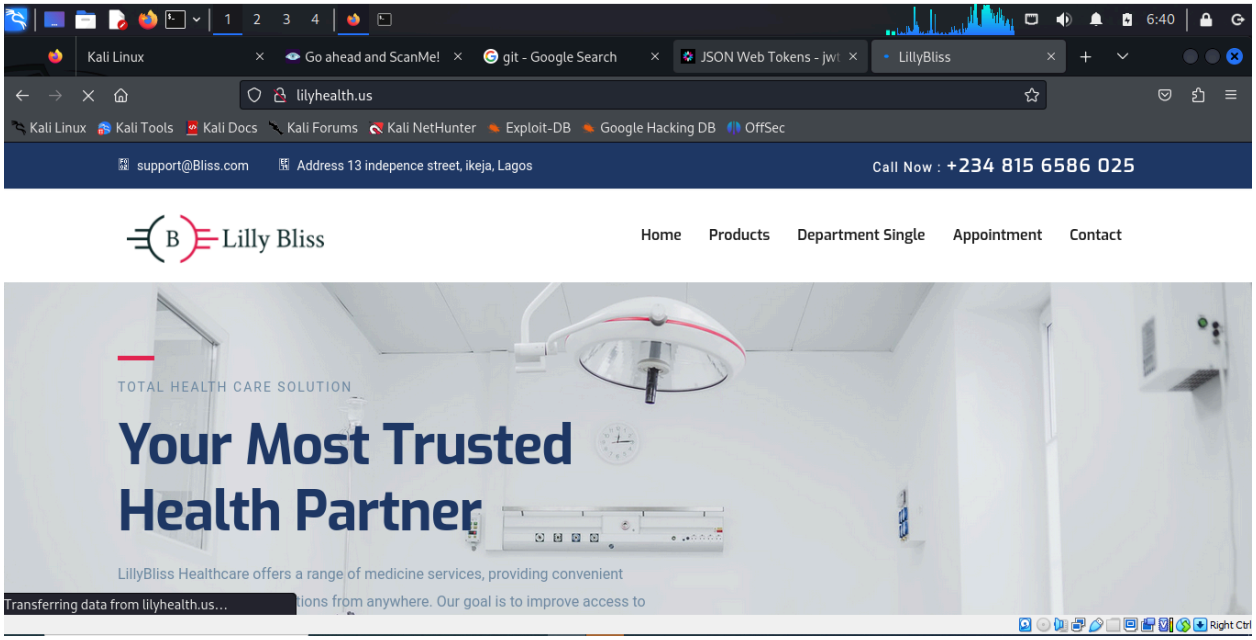
Network vulnerability Assessment

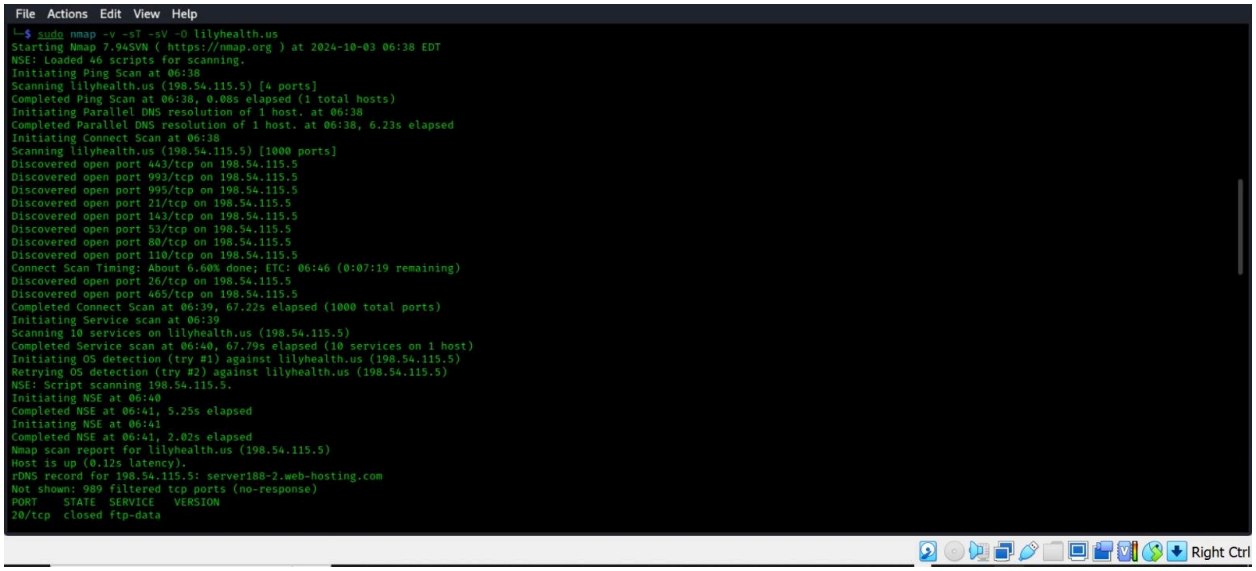
Tools: Nmap
Project-Site : lilyhealth.us

Nmap stands for "Network Mapper." It's an open-source tool used for network discovery and security auditing. Nmap can be employed to discover hosts and services on a computer network

Lillyhealth.us



Scan method from kali - Nmap -v -sT -sV -O lilyhealth.us



Result:

Vulnerabilities

The ports listed are commonly associated with various services. Here's a brief overview of each and their potential vulnerabilities:

1. **Port 80 (HTTP):**
    - **Service: Unencrypted web traffic.**
    - **Vulnerabilities: Man-in-the-Middle (MitM) attacks, eavesdropping on data, lack of encryption.**
2. **Port 21 (FTP):**
    - **Service: File Transfer Protocol.**
    - **Vulnerabilities: Unencrypted data transfer, username/password exposure, brute force attacks.**
3. **Port 26 (SMTP):**
    - **Service: SMTP (Simple Mail Transfer Protocol) often used for email sending.**
    - **Vulnerabilities: Open relays can be exploited for spam; lacks encryption in many configurations.**
4. **Port 53 (DNS):**
    - **Service: Domain Name System.**
    - **Vulnerabilities: DNS spoofing, amplification attacks, and information leakage.**
5. **Port 110 (POP3):**
    - **Service: Post Office Protocol (for receiving email).**
    - **Vulnerabilities: Unencrypted communication, password exposure.**
6. **Port 143 (IMAP):**
    - **Service: Internet Message Access Protocol (for receiving email).**
    - **Vulnerabilities: Unencrypted communication, similar to POP3 but with more features.**
7. **Port 443 (HTTPS):**
    - **Service: Secure web traffic.**
    - **Vulnerabilities: SSL/TLS misconfigurations, weak cipher suites, expired certificates.**
8. **Port 465 (SMTPS):**
    - **Service: SMTP over SSL (used for sending email securely).**
    - **Vulnerabilities: Similar to SMTP but requires proper SSL/TLS configuration.**
9. **Port 993 (IMAPS):**
    - **Service: IMAP over SSL (secure email retrieval).**
    - **Vulnerabilities: Same as IMAP but with secure transmission; still susceptible to configuration issues.**
10. **Port 995 (POP3S):**

    - **Service: POP3 over SSL (secure email retrieval).**
    - **Vulnerabilities: Same as POP3, but requires proper SSL/TLS configuration.**

General Security Recommendations:

- **Use Encryption: Ensure that services like FTP and SMTP are using secure versions (SFTP, SMTPS).**
- **Regular Updates: Keep all services and software updated to patch known vulnerabilities.**
- **Access Control: Implement strict access controls and authentication mechanisms.**
- **Monitoring: Use intrusion detection systems (IDS) to monitor traffic on these ports.**
- **Regular Audits: Conduct security audits and vulnerability assessments to identify and mitigate risks.**