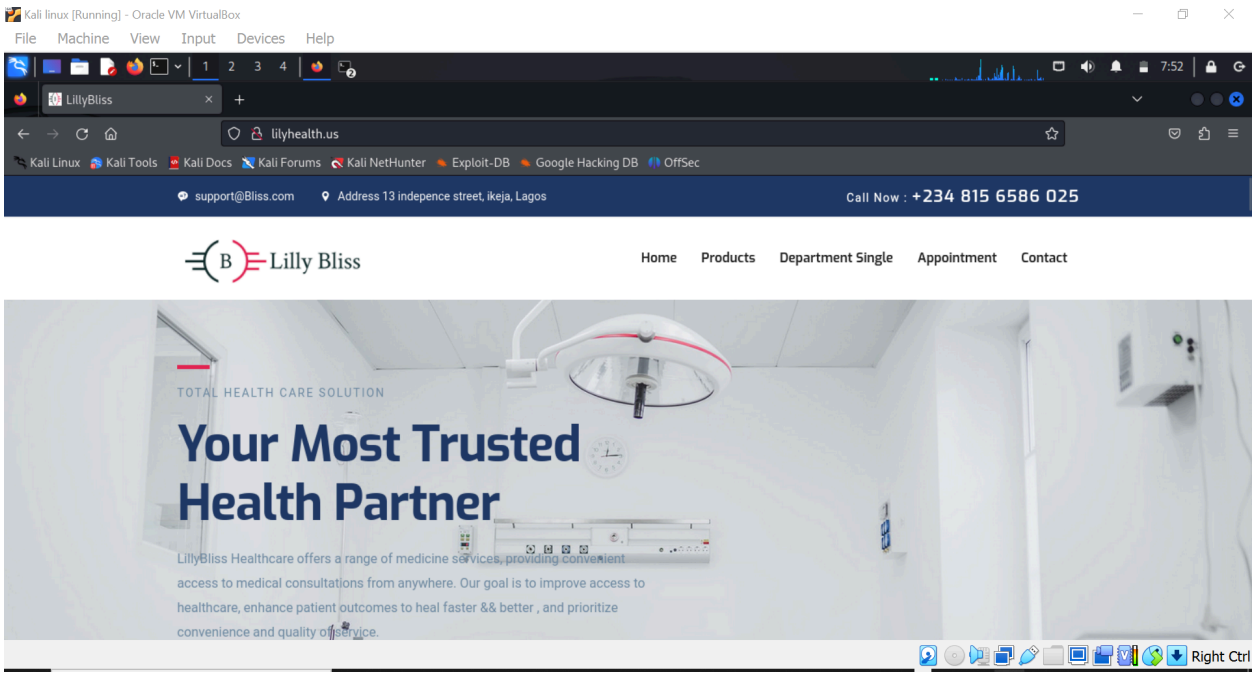
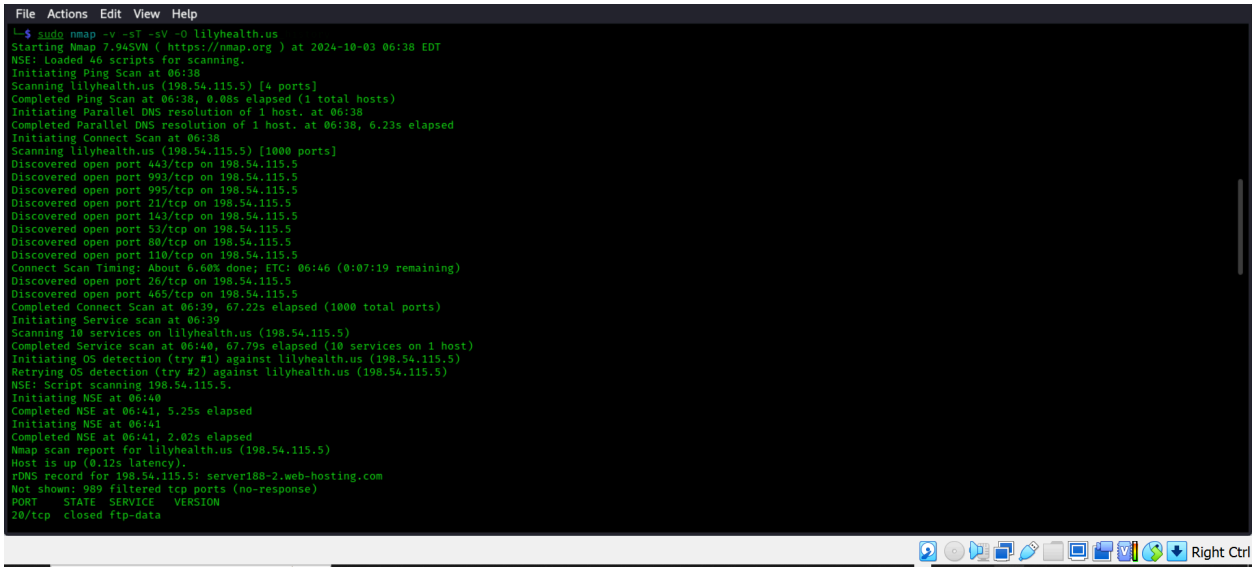
# NETWORK VULNERABILITY ASSESSMENT

TOOL: Nmap
PROJECT SITE: lilyhealth.us

Nmap (Network Mapper) is an open-source tool primarily used for network discovery and security auditing. It's widely known for its ability to:

Network Scanning: Identifies devices connected to a network, discovers their operating systems, and gathers information about the network architecture.






Reports includes:

1. Port 443 (HTTPS)* – Secure HTTP (Web Traffic)
   Service*: HTTPS (encrypted HTTP)
   Security Risks*:
    Misconfigured SSL/TLS protocols.
     Use of deprecated encryption algorithms (e.g., SSLv3, RC4).
     Vulnerabilities like Heartbleed or POODLE.
   Measures*:
      Ensure the server supports only strong encryption (TLS 1.2 or higher).
      Use a valid SSL/TLS certificate from a trusted CA.
      Regularly scan for SSL vulnerabilities using tools like SSL Labs or OpenVAS.
       Apply HTTP security headers (HSTS, X-Frame-Options, etc.).

2 Port 993 (IMAPS)* – Secure Internet Message Access Protocol (IMAP over SSL)
    Service: IMAP for email retrieval (encrypted)
     Security Risks:
    Weak encryption or outdated SSL/TLS versions.
    Improper authentication mechanisms.

Measures:
Use strong encryption and disable weak SSL/TLS versions.
Enforce strong authentication (e.g., multi-factor authentication).
Monitor for brute-force attempts on email accounts.

3. Port 995 (POP3S)* – Secure Post Office Protocol (POP3 over SSL)
Service: POP3 for email retrieval (encrypted)
Security Risks:
Same risks as IMAPS, including weak encryption.
Measures:
Use strong SSL/TLS encryption.
Avoid using POP3 unless necessary, as IMAP offers better synchronization.

4. Port 465 (SMTPS) – Secure Mail Transfer Protocol (SMTP over SSL)
Service: SMTP for sending email (encrypted)
Security Risks:
- Open relay vulnerabilities allowing spammers to use the mail server.
- Weak or outdated encryption.
Measures:
Ensure SMTP authentication is enabled to prevent unauthorized use.
Configure the server to block open relay.
Use SPF, DKIM, and DMARC to secure email authentication.
Enable modern TLS versions for encryption.

5. Port 143 (IMAP) – Internet Message Access Protocol (Plaintext)
Service: IMAP (unencrypted)
Security Risks:
Email contents can be intercepted if traffic is not encrypted.
User credentials could be exposed during transmission.
Measures:
Migrate to encrypted IMAPS (port 993).
If using IMAP, ensure STARTTLS is configured to upgrade to encryption.

6. Port 80 (HTTP) – Hypertext Transfer Protocol (Web Traffic)
Service: HTTP (unencrypted)
Security Risks
Sensitive data transmitted in plaintext.
Susceptibility to attacks like Man-in-the-Middle (MitM), session hijacking, etc.
Measures
Redirect all HTTP traffic to HTTPS (port 443).
Apply security headers to prevent common web attacks (CSP, X-Frame-Options, etc.).
Harden web applications against OWASP Top 10 vulnerabilities (XSS, SQL Injection).

7. Port 21 (FTP) – File Transfer Protocol
ServiceFTP (unencrypted)
Security Risks
Passwords and data transmitted in plaintext.
FTP servers are often targeted for brute force or exploitation.
Measures
Replace FTP with a secure alternative like FTPS (over TLS) or SFTP (SSH-based).
Ensure strong authentication mechanisms and password policies.
Limit FTP access to necessary users and enforce firewall rules.

Port 26 (Alternate SMTP Port)
Sometimes used as an alternative SMTP port when port 25 is blocked.
Security Risks
Same risks as standard SMTP (open relays, weak authentication).