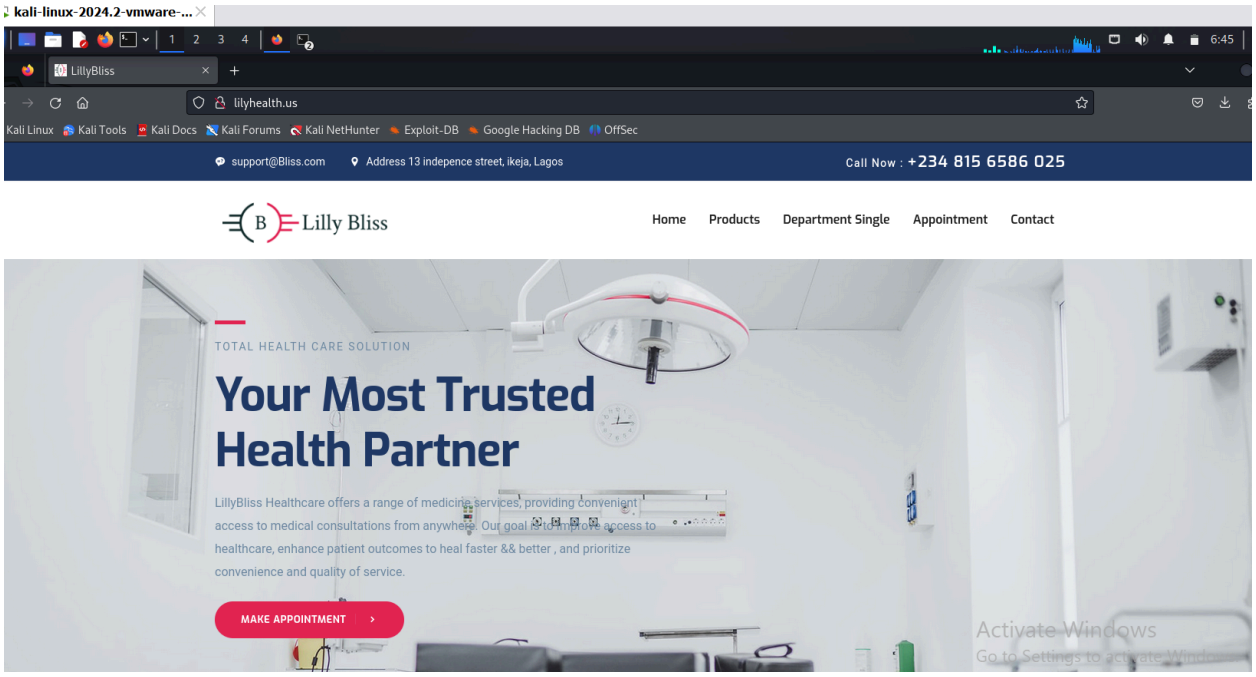
PROJECT

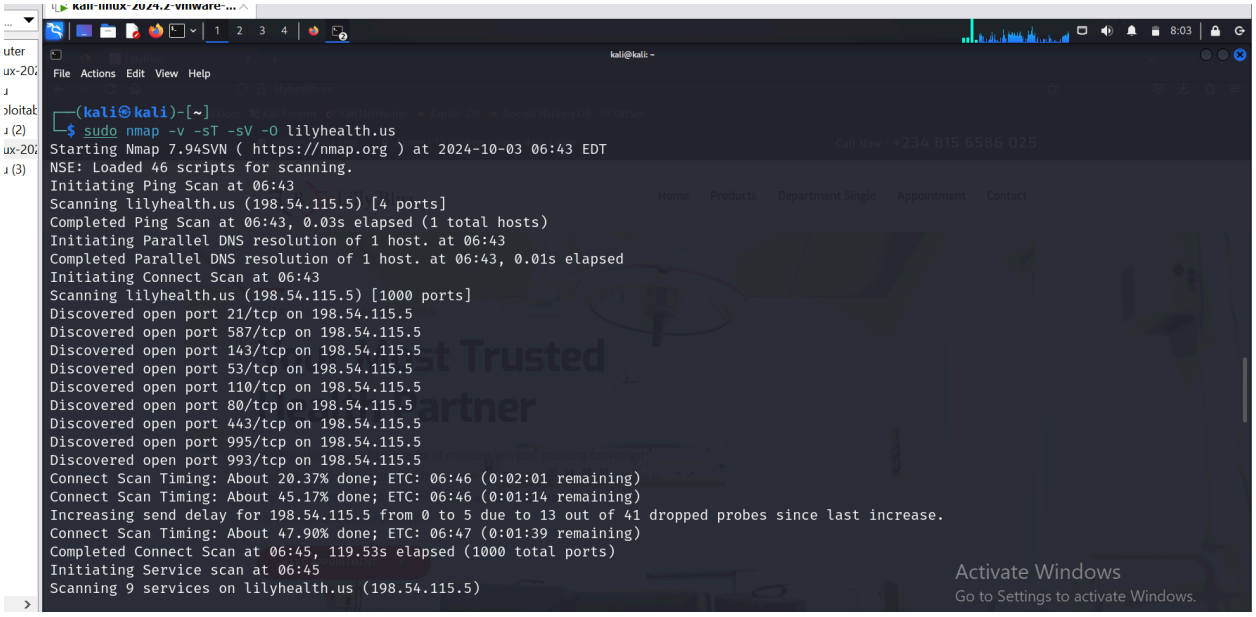
Network Vulnerability Assessment

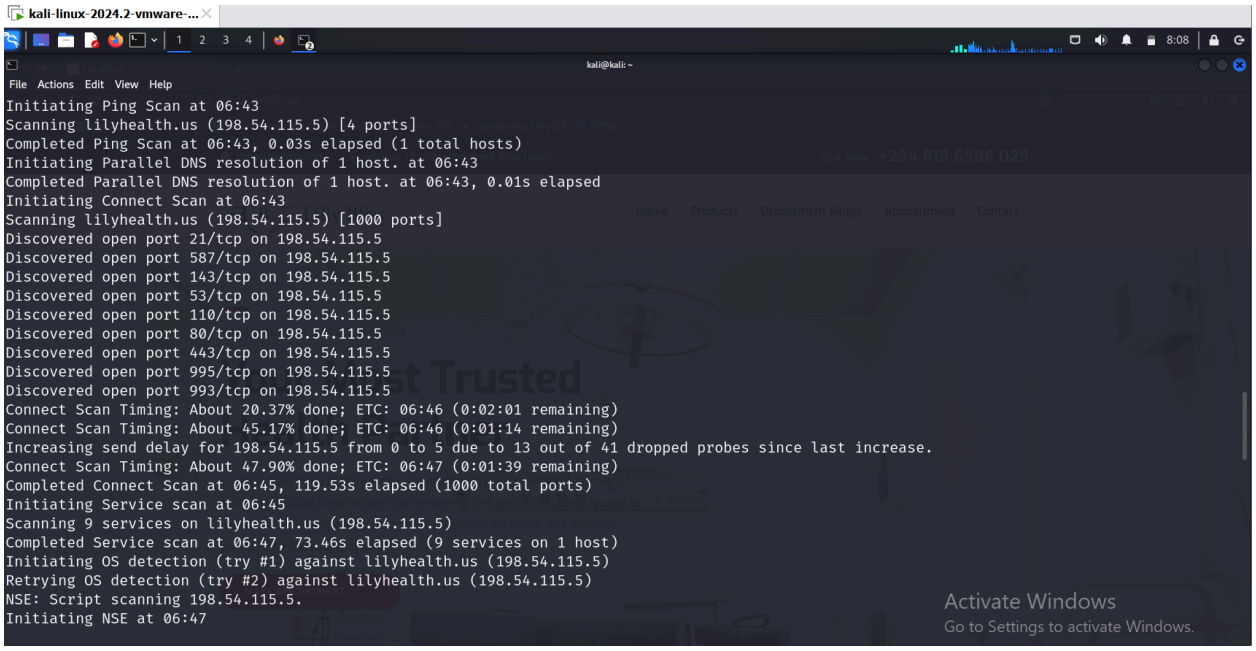
Tools : Nmap
Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

Website : lilyhealth.us



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





Results and Vulnerabilities

The ports you've listed are commonly used for various internet services and protocols. Here's a brief overview of each:

1. *Port 80*:
- ***Protocol*: HTTP (Hypertext Transfer Protocol)**
- ***Description*: Used for unencrypted web traffic.**

2. *Port 21*:
  - *Protocol*: FTP (File Transfer Protocol)
  - *Description*: Used for transferring files between client and server.

3. *Port 26*:
  - *Protocol*: Often used for SMTP (Simple Mail Transfer Protocol) alternative or for mail submission.
  - *Description*: Not a standard, but sometimes used for email services.

4. *Port 53*:
  - *Protocol*: DNS (Domain Name System)
  - *Description*: Used for resolving domain names to IP addresses.

5. *Port 110*:
  - *Protocol*: POP3 (Post Office Protocol)
  - *Description*: Used for retrieving emails from a mail server.

6. *Port 143*:
  - *Protocol*: IMAP (Internet Message Access Protocol)
  - *Description*: Used for retrieving and managing emails on a mail server.

7. *Port 443*:
  - *Protocol*: HTTPS (HTTP Secure)
  - *Description*: Used for encrypted web traffic, ensuring secure communication.

8. *Port 465*:
  - *Protocol*: SMTPS (SMTP Secure)
  - *Description*: Used for sending emails securely over SSL/TLS.

9. *Port 993*:
  - *Protocol*: IMAPS (IMAP Secure)
  - *Description*: Used for securely retrieving emails over SSL/TLS.

10. *Port 995*:
  - *Protocol*: POP3S (POP3 Secure)
  - *Description*: Used for securely retrieving emails over SSL/TLS.

Security Considerations

- *Open Ports*: Keeping these ports open can expose your system to vulnerabilities. It's important to only open ports that are necessary for your applications.
- *Firewalls*: Use firewalls to restrict access to these ports based on your organization's needs.
- *Regular Scanning*: Regularly scan your network for open ports and services to identify potential vulnerabilities.