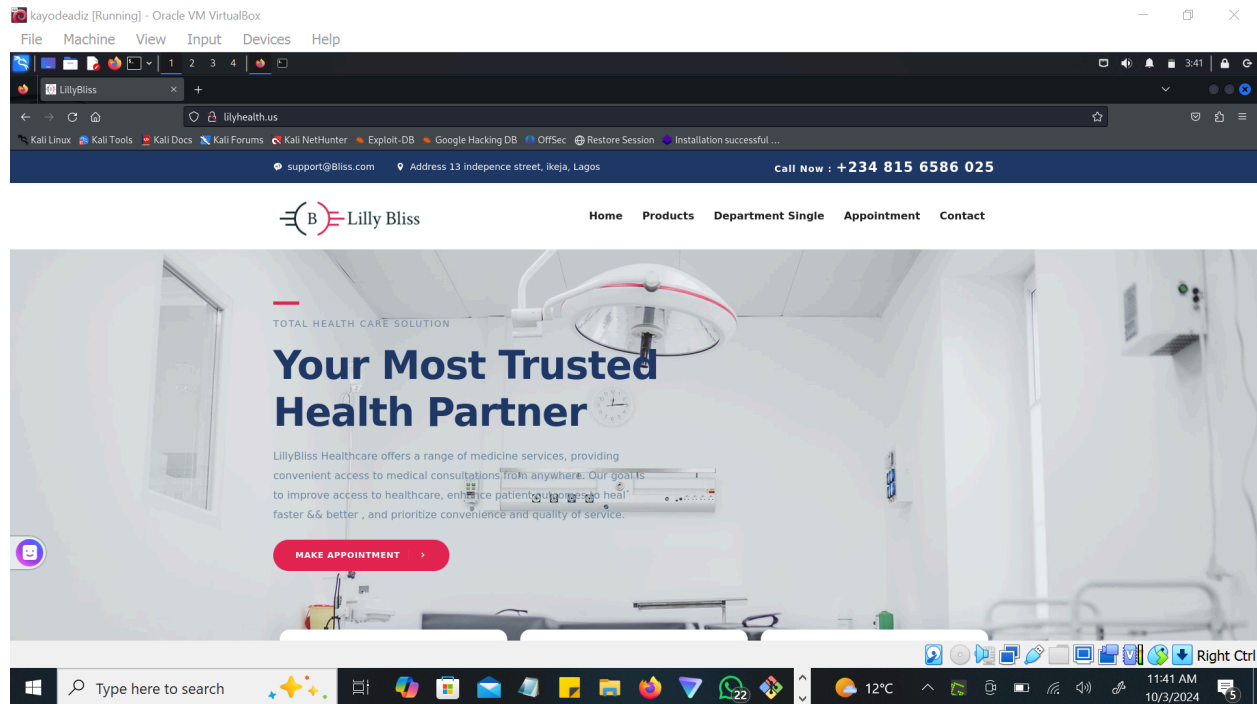


NETWORK VULNERABILITY ASSESSMENT

TOOLS: NMAP

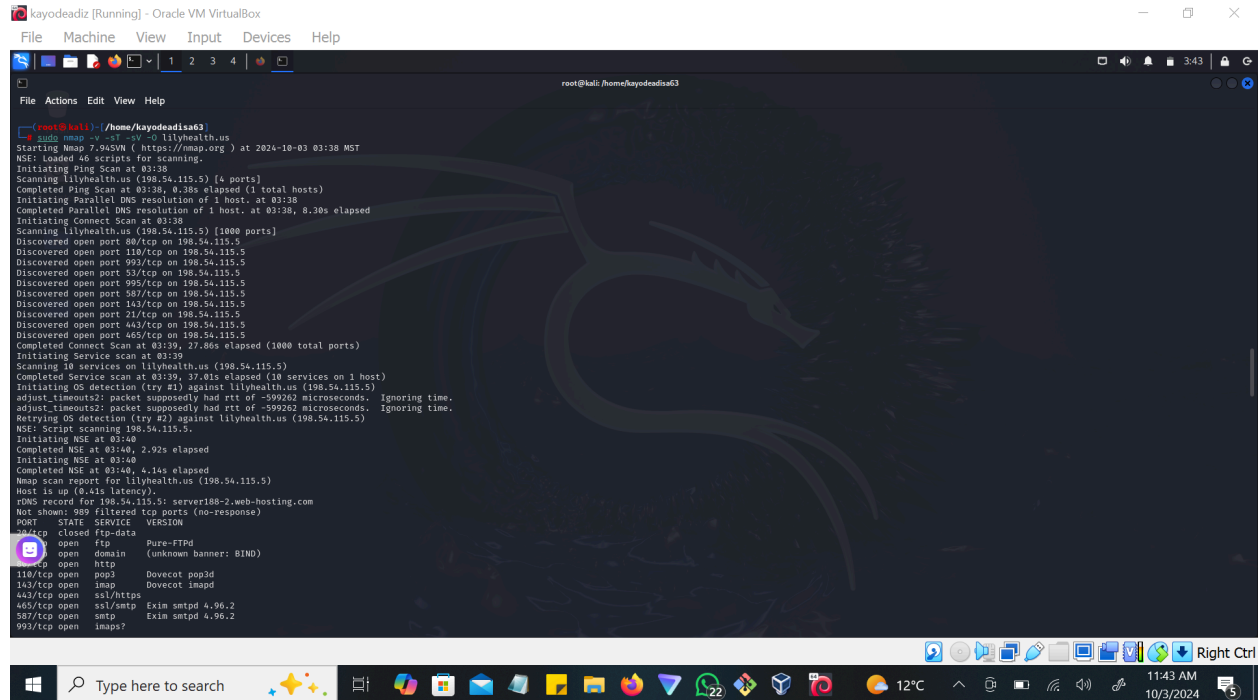
PROJECT-SITE: Lilyhealth.us

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.



Scan Method: linux

Command: `sudo nmap -v -sT -sV -O lilyhealth.us`



```
root@kali: /home/kayodeadisa63
File Actions Edit View Help

root@kali: /home/kayodeadisa63
└─$ sudo nmap -v -sV -sC -sS -sT -sU -sX -sY -sZ -sO -sV -sS -sT -sU -sX -sY -sZ -sO lilyhealth.us
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-03 03:38 MST
NSE: Loaded 49 scripts for scanning.
Initiating Ping Scan at 03:38
Scanning lilyhealth.us (198.54.115.5) [4 ports]
Completed Ping Scan at 03:38, 0.38s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:38
Completed Parallel DNS resolution of 1 host. at 03:38, 0.30s elapsed
Initiating Connect Scan at 03:38
Scanning lilyhealth.us (198.54.115.5) [1000 ports]
Discovered open port 80/tcp on 198.54.115.5
Discovered open port 110/tcp on 198.54.115.5
Discovered open port 993/tcp on 198.54.115.5
Discovered open port 995/tcp on 198.54.115.5
Discovered open port 587/tcp on 198.54.115.5
Discovered open port 143/tcp on 198.54.115.5
Discovered open port 21/tcp on 198.54.115.5
Discovered open port 443/tcp on 198.54.115.5
Discovered open port 465/tcp on 198.54.115.5
Completed Connect Scan at 03:39, 22.86s elapsed (1000 total ports)
Initiating Service scan at 03:39
Scanning 10 services on lilyhealth.us (198.54.115.5)
Completed Service scan at 03:39, 37.01s elapsed (10 services on 1 host)
Initiating OS detection (try #1) against lilyhealth.us (198.54.115.5)
adjust_timeout:2: packet supposedly had rtt of -599263 microseconds. Ignoring time.
adjust_timeout:2: packet supposedly had rtt of -599262 microseconds. Ignoring time.
Retrying OS detection (try #2) against lilyhealth.us (198.54.115.5)
NSE: Script scanning 198.54.115.5.
Initiating NSE at 03:40
Completed NSE at 03:40, 2.92s elapsed
Initiating NSE at 03:40
Completed NSE at 03:40, 4.14s elapsed
Nmap scan report for lilyhealth.us (198.54.115.5)
Host is up (0.41s latency).
rDNS record for 198.54.115.5: server188-2.web-hosting.com
Not shown: 889 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Pure-FTPd
110/tcp   open  pop3      Dovecot pop3d
143/tcp   open  imap      Dovecot imapd
443/tcp   open  ssl/https
465/tcp   open  ssl/smtp  Exim smtpd 4.96.2
587/tcp   open  smtp      Exim smtpd 4.96.2
993/tcp   open  imap7
995/tcp   open  imaps7
```

RESULT

Vulnerabilities:

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

- *Port 80*:**
 - *Protocol*:** HTTP (Hypertext Transfer Protocol)
 - *Description*:** Used for unencrypted web traffic.
- *Port 21*:**
 - *Protocol*:** FTP (File Transfer Protocol)
 - *Description*:** Used for transferring files between client and server.
- *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.
- *Port 53*:**
 - *Protocol*:** DNS (Domain Name System)
 - *Description*:** Used for resolving domain names to IP addresses.
- *Port 110*:**
 - *Protocol*:** POP3 (Post Office Protocol)
 - *Description*:** Used for retrieving emails from a mail server.
- *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.