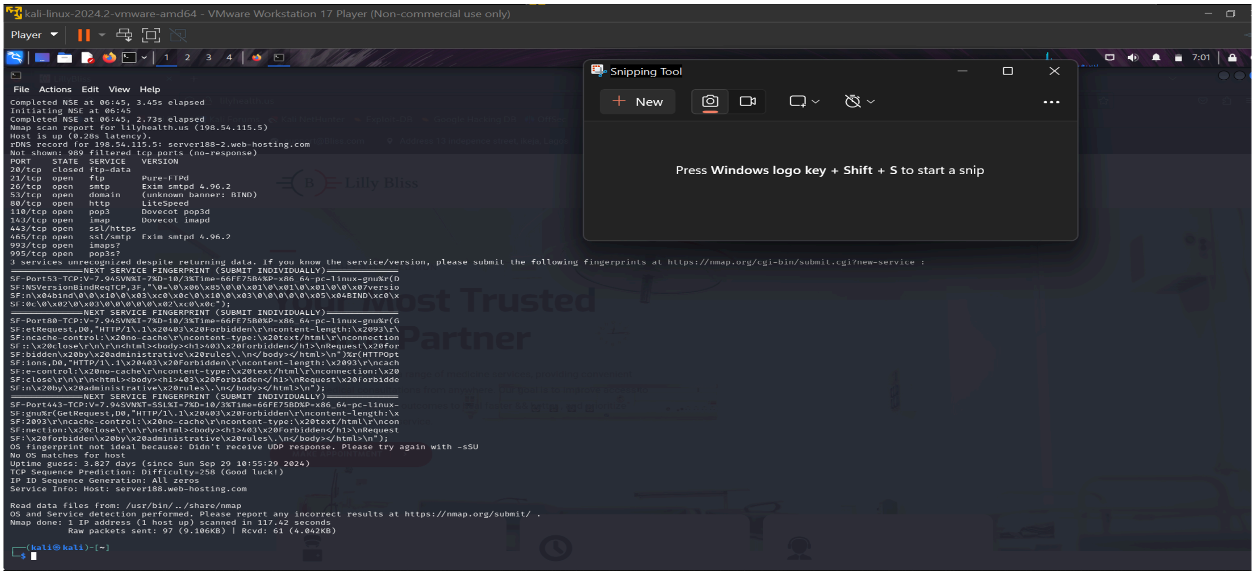
NETWORK VULNERABILITY ASSESSMENT

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 allows users to scan networks to discover devices, identify open ports, and gather information about the services running on those ports. It's widely used by network administrators, security professionals, and ethical hackers for various purposes, including network inventory, monitoring host or service uptime, and security assessments.

SCAN METHOD FROM KALI: sudo nmap -v -sT -sV -O lilyhealth.us


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
7:01
File Actions Edit View Help
Snipping Tool
New

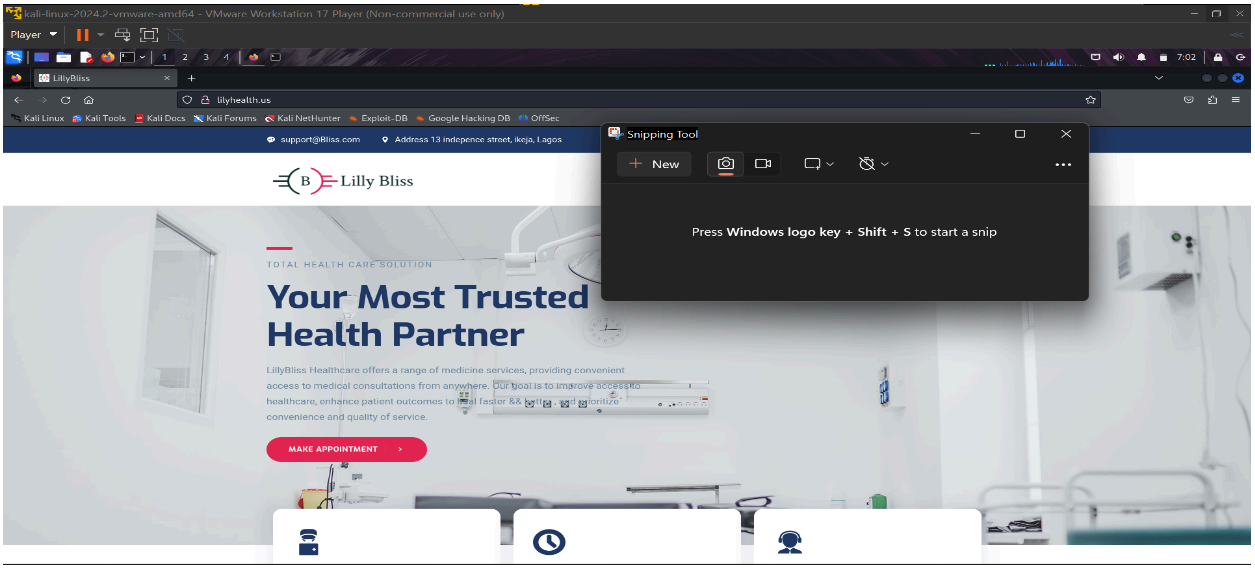
Press **Windows logo key + Shift + S** to start a snip

```
Completed NSE at 06:45, 3.45s elapsed
Initiating NSE at 06:45
Completed NSE at 06:45, 2.73s elapsed
Nmap scan report for lilyhealth.us (198.54.115.5)
Host is up (0.28s latency).
rDNS record for 198.54.115.5: server188-2.web-hosting.com
Not shown: 989 filtered tcp ports (no-response)
PORT    STATE  SERVICE   VERSION
20/tcp  closed ftp-data
21/tcp  open   ftp       Pure-FTPd
26/tcp  open   smtp      Exim smtpd 4.96.2
53/tcp  open   domain    (unknown banner: BIND)
80/tcp  open   http      LiteSpeed
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
993/tcp open   imaps?
995/tcp open   pop3s?
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
══════════════NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)══════════════
SF-Port53-TCP:V=7.94SVN%I=7%D=10/3%Time=66FE75B4%P=x86_64-pc-linux-gnu%r(D
SF:NSVersionBindReqTCP,3F,"\0=\0\x06\x85\0\0\x01\0\x01\0\x01\0\0\x07versio
SF:n\x04bind\0\0\x10\0\x03\xc0\x0c\0\x10\0\x03\0\0\0\0\0\x05\x04BIND\xc0\x
SF:0c\0\x02\0\x03\0\0\0\0\0\x02\xc0\x0c");
══════════════NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)══════════════
SF-Port80-TCP:V=7.94SVN%I=7%D=10/3%Time=66FE75B0%P=x86_64-pc-linux-gnu%r(G
SF:etRequest,D0,"HTTP/1\.1\x20403\x20Forbidden\r\ncontent-length:\x2093\r\
SF:ncache-control:\x20no-cache\r\ncontent-type:\x20text/html\r\nconnection
SF::\x20close\r\n\r\n<html><body><h1>403\x20Forbidden</h1>\nRequest\x20for
SF:bidden\x20by\x20administrative\x20rules\.\n</body></html>\n")%r(HTTPOpt
SF:ions,D0,"HTTP/1\.1\x20403\x20Forbidden\r\ncontent-length:\x2093\r\ncach
SF:e-control:\x20no-cache\r\ncontent-type:\x20text/html\r\nconnection:\x20
SF:close\r\n\r\n<html><body><h1>403\x20Forbidden</h1>\nRequest\x20forbidde
SF:n\x20by\x20administrative\x20rules\.\n</body></html>\n");
══════════════NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)══════════════
SF-Port443-TCP:V=7.94SVN%T=SSL%I=7%D=10/3%Time=66FE75BD%P=x86_64-pc-linux-
SF:gnu%r(GetRequest,D0,"HTTP/1\.1\x20403\x20Forbidden\r\ncontent-length:\x
SF:2093\r\ncache-control:\x20no-cache\r\ncontent-type:\x20text/html\r\ncon
SF:nection:\x20close\r\n\r\n<html><body><h1>403\x20Forbidden</h1>\nRequest
SF:\x20forbidden\x20by\x20administrative\x20rules\.\n</body></html>\n");
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
No OS matches for host
Uptime guess: 3.827 days (since Sun Sep 29 10:55:29 2024)
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: server188.web-hosting.com

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 117.42 seconds
           Raw packets sent: 97 (9.106KB) | Rcvd: 61 (4.042KB)

┌──(kali㉿kali)-[~]
└─$ 
```

LILYHEALTH.US:



support@Bliss.com Address 13 indepence street, ikeja, Lagos

Press Windows logo key + Shift + S to start a snip

TOTAL HEALTH CARE SOLUTION

Your Most Trusted Health Partner

LillyBliss Healthcare offers a range of medicine services, providing convenient access to medical consultations from anywhere. Our goal is to improve access to healthcare, enhance patient outcomes to heal faster && better , and prioritize convenience and quality of service.

RESULT : . Port 587 (SMTP)

- **Vulnerabilities:**
  - **Open Relay: Misconfigured servers may allow unauthorized users to send emails, leading to spam abuse.**
  - **Weak Authentication: If not using strong authentication methods, attackers could exploit this to send emails.**
- **Security Considerations:**
  - **Always require authentication for sending emails.**
  - **Implement TLS to encrypt connections and protect data in transit.**

2. Port 110 (POP3)

- **Vulnerabilities:**
  - **Unencrypted Communication: Data, including credentials, is transmitted in plain text, making it susceptible to eavesdropping.**
  - **Account Hijacking: If credentials are intercepted, attackers can gain access to user accounts.**
- **Security Considerations:**
  - **Avoid using POP3 unless necessary; consider using POP3S (port 995) for encrypted communication.**
  - **Regularly audit access logs for suspicious activity.**

3. Port 993 (IMAPS)

- **Vulnerabilities:**
  - **Weak SSL/TLS Configuration: If misconfigured, it may expose sensitive data.**
  - **Outdated Protocols: Using outdated or insecure versions can lead to vulnerabilities.**
- **Security Considerations:**

    - Ensure strong SSL/TLS configurations and regularly update to the latest versions.
    - Monitor for any unusual access patterns.

4. Port 995 (POP3S)

- **Vulnerabilities:**
    - **Improper Certificate Management: Expired or misconfigured certificates can lead to trust issues.**
    - **Protocol Weaknesses: If outdated cryptographic protocols are used, they can be exploited.**
- **Security Considerations:**
    - **Regularly renew and manage SSL/TLS certificates.**
    - **Configure strong ciphers and protocols.**

5. Port 443 (HTTPS)

- **Vulnerabilities:**
    - **SSL/TLS Misconfigurations: Weak ciphers or improper configurations can expose the site to attacks (e.g., POODLE, BEAST).**
    - **Expired Certificates: Can lead to trust issues for users.**
- **Security Considerations:**
    - **Implement strong SSL/TLS configurations and use up-to-date certificates.**
    - **Regularly test for vulnerabilities using tools like SSL Labs.**

6. Port 80 (HTTP)

- **Vulnerabilities:**
    - **Unencrypted Traffic: Data, including credentials, is transmitted in plain text, making it easy for attackers to intercept.**
    - **Injection Attacks: Vulnerable web applications can be exploited through XSS or SQL injection.**
- **Security Considerations:**
    - **Always redirect HTTP to HTTPS to ensure secure communication.**
    - **Regularly audit and secure web applications.**

7. Port 143 (IMAP)

- **Vulnerabilities:**
    - **Unencrypted Communication: Similar to POP3, credentials and data can be intercepted.**
    - **Misconfiguration: Improperly configured servers may expose sensitive data.**
- **Security Considerations:**
    - **Use IMAPS (port 993) for encrypted communication.**
    - **Regularly review server configurations and security policies.**

8. Port 21 (FTP)

- **Vulnerabilities:**
    - **Unencrypted Transfers: FTP transmits data, including credentials, in plain text, making it easy to intercept.**
    - **Anonymous Access: Misconfigurations may allow unauthorized access.**
- **Security Considerations:**
    - **Use SFTP (SSH File Transfer Protocol) or FTPS (FTP Secure) for secure file transfers.**

  - **Limit user permissions and regularly audit access.**

9. Port 53 (DNS)

- **Vulnerabilities:**
  - **DNS Spoofing: Attackers may manipulate DNS queries to redirect users.**
  - **DDoS Attacks: DNS servers can be targeted for amplification attacks.**
- **Security Considerations:**
  - **Implement DNSSEC (Domain Name System Security Extensions) to protect against spoofing.**
  - **Use rate limiting and monitoring to mitigate DDoS risks.**

General Best Practices

- **Keep Software Updated: Regularly update all software to patch known vulnerabilities.**
- **Firewall Configuration: Use firewalls to restrict access to only necessary ports and services.**
- **Monitor and Log: Regularly monitor network traffic and log access attempts for suspicious activities.**
- **Conduct Regular Security Audits: Regularly assess the security posture of your network and service.**