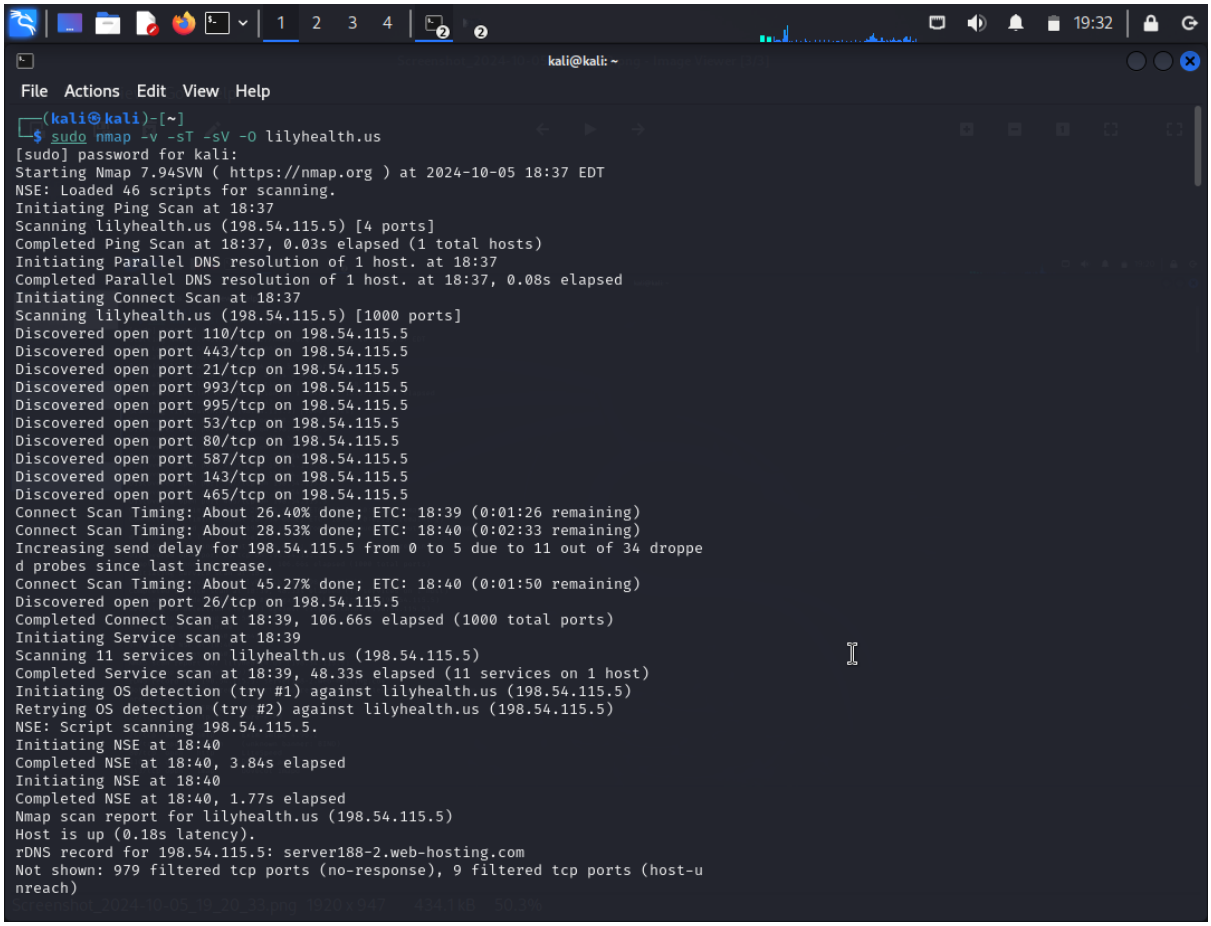
NETWORK VULNERABILITY ASSESSMENT

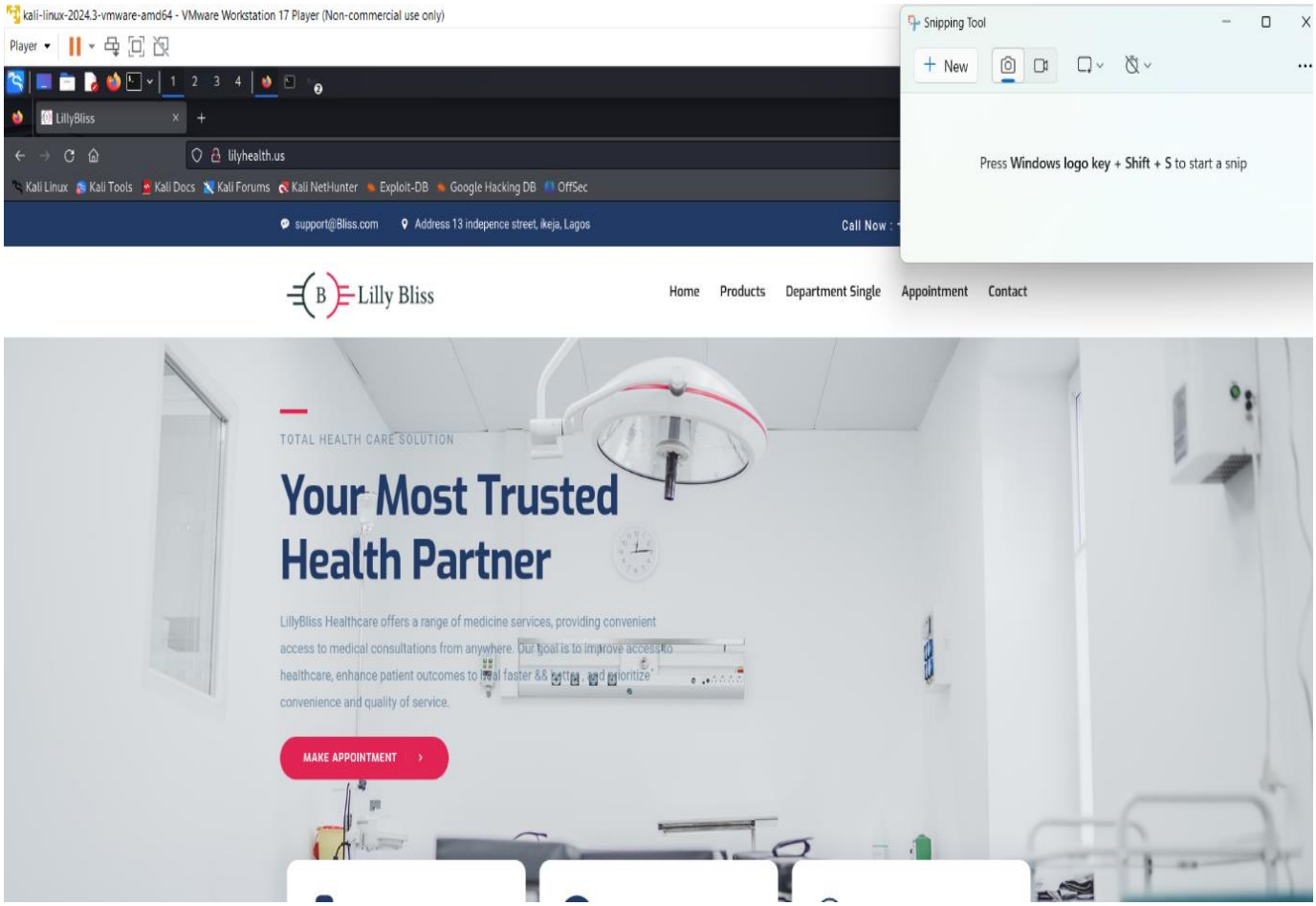
TOOLS : NMAP

PROJECT-SITE: LILYHEALTH.US

Nmap, short for Network Mapper, is an open-source tool used for network discovery and security auditing. It allows users to scan networks and identify devices, open ports, and services running on those devices. Nmap can also detect operating systems and versions, making it useful for security assessments and network inventory.



```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo nmap -v -sT -sV -O lilyhealth.us
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-05 18:37 EDT
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 18:37
Scanning lilyhealth.us (198.54.115.5) [4 ports]
Completed Ping Scan at 18:37, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:37
Completed Parallel DNS resolution of 1 host. at 18:37, 0.08s elapsed
Initiating Connect Scan at 18:37
Scanning lilyhealth.us (198.54.115.5) [1000 ports]
Discovered open port 110/tcp on 198.54.115.5
Discovered open port 443/tcp on 198.54.115.5
Discovered open port 21/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 53/tcp on 198.54.115.5
Discovered open port 80/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 465/tcp on 198.54.115.5
Connect Scan Timing: About 26.40% done; ETC: 18:39 (0:01:26 remaining)
Connect Scan Timing: About 28.53% done; ETC: 18:40 (0:02:33 remaining)
Increasing send delay for 198.54.115.5 from 0 to 5 due to 11 out of 34 droppe
d probes since last increase.
Connect Scan Timing: About 45.27% done; ETC: 18:40 (0:01:50 remaining)
Discovered open port 26/tcp on 198.54.115.5
Completed Connect Scan at 18:39, 106.66s elapsed (1000 total ports)
Initiating Service scan at 18:39
Scanning 11 services on lilyhealth.us (198.54.115.5)
Completed Service scan at 18:39, 48.33s elapsed (11 services on 1 host)
Initiating OS detection (try #1) against lilyhealth.us (198.54.115.5)
Retrying OS detection (try #2) against lilyhealth.us (198.54.115.5)
NSE: Script scanning 198.54.115.5.
Initiating NSE at 18:40
Completed NSE at 18:40, 3.84s elapsed
Initiating NSE at 18:40
Completed NSE at 18:40, 1.77s elapsed
Nmap scan report for lilyhealth.us (198.54.115.5)
Host is up (0.18s latency).
rDNS record for 198.54.115.5: server188-2.web-hosting.com
Not shown: 979 filtered tcp ports (no-response), 9 filtered tcp ports (host-u
nreach)
```



Exploiting vulnerabilities on specific ports generally involves targeting the services that run on those ports. Here are some common vulnerabilities associated with these open ports :

1. **Port 443 (HTTPS)**
    - **SSL/TLS Misconfigurations:** Weak encryption protocols (like SSLv2 or SSLv3) can be exploited through attacks like POODLE or BEAST.
    - **Certificate Issues:** Improperly configured certificates, such as self-signed certificates, can lead to man-in-the-middle (MITM) attacks.
2. **Port 110 (POP3)**
    - **Cleartext Authentication:** POP3 transmits credentials in plaintext, making it vulnerable to eavesdropping if not secured by TLS.
    - **Buffer Overflow Vulnerabilities:** Older implementations may be susceptible to buffer overflow attacks that can lead to remote code execution.
3. **Port 21 (FTP)**
    - **Anonymous Authentication:** If enabled, attackers can access files without credentials.
    - **Command Injection:** Certain implementations may be vulnerable to command injection attacks, allowing attackers to execute arbitrary commands.
4. **Port 993 (IMAPS)**

- **TLS/SSL Weaknesses:** Similar to port 443, misconfigured or outdated TLS implementations can expose users to MITM attacks.
- **Weak Passwords:** Brute-force attacks on user credentials can be a vulnerability if strong password policies are not enforced.

5. **Port 53 (DNS)**
    - **DNS Spoofing:** Attackers can exploit vulnerabilities in DNS to redirect traffic to malicious sites.
    - **DDoS Attacks:** DNS servers can be targeted for amplification attacks, exploiting the query/response nature of DNS.