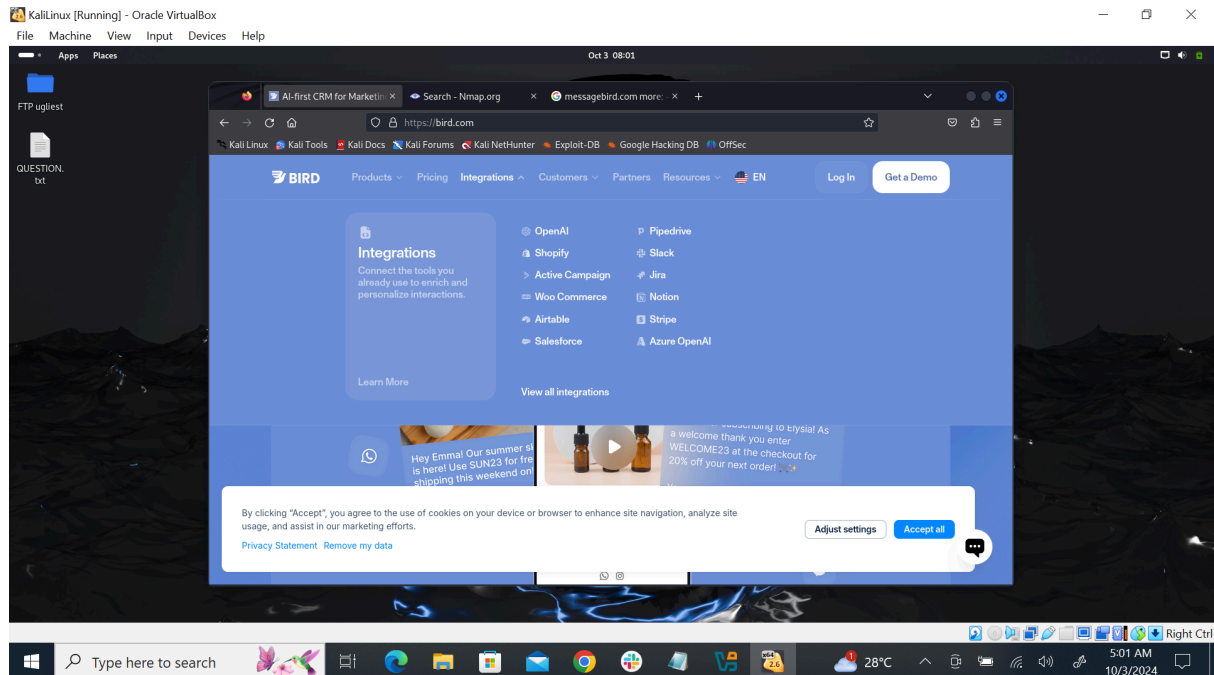


Network Vulnerability Assessment

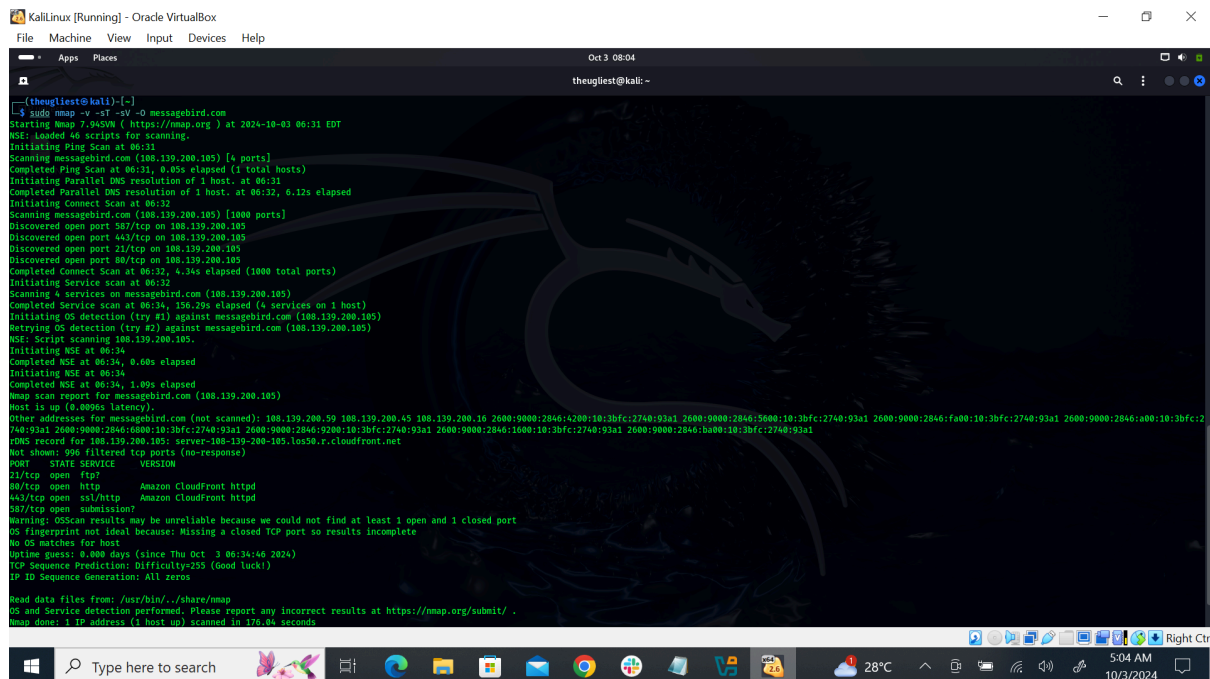
Tools : NMAP

Project-Site : messagebird.com

Nmap (Network Mapper) is an open-source tool used for network discovery and security auditing. Here are some key points about Nmap



Scan method from kali: `sudo nmap -v -sT -sV -O messagebird.com`



```
theugliest@kali:~$ sudo nmap -v -sV -O messagebird.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-03 06:31 EDT
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 06:31
Scanning messagebird.com (108.139.200.105) [4 ports]
Completed Ping Scan at 06:31, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:31
Completed Parallel DNS resolution of 1 host. at 06:32, 6.12s elapsed
Initiating Connect Scan at 06:32
Scanning messagebird.com (108.139.200.105) [1000 ports]
Discovered open port 587/tcp on 108.139.200.105
Discovered open port 443/tcp on 108.139.200.105
Discovered open port 21/tcp on 108.139.200.105
Discovered open port 80/tcp on 108.139.200.105
Completed Connect Scan at 06:32, 4.34s elapsed (1000 total ports)
Initiating Service scan at 06:32
Scanning 4 services on messagebird.com (108.139.200.105)
Completed Service scan at 06:32, 156.29s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against messagebird.com (108.139.200.105)
Retrying OS detection (try #2) against messagebird.com (108.139.200.105)
NSE: Script scanning 108.139.200.105.
Initiating NSE at 06:34
Completed NSE at 06:34, 0.60s elapsed
Initiating NSE at 06:34
Completed NSE at 06:34, 1.09s elapsed
Nmap scan report for messagebird.com (108.139.200.105)
Host is up (0.000ms latency).
Other addresses for messagebird.com (not scanned): 108.139.200.59 108.139.200.45 108.139.200.16 2600:9000:2846:4200:10:3bfc:2740:93a1 2600:9000:2846:5000:10:3bfc:2740:93a1 2600:9000:2846:6000:10:3bfc:2740:93a1 2600:9000:2846:7000:10:3bfc:2740:93a1 2600:9000:2846:8000:10:3bfc:2740:93a1 2600:9000:2846:9000:10:3bfc:2740:93a1 2600:9000:2846:a000:10:3bfc:2740:93a1 2600:9000:2846:b000:10:3bfc:2740:93a1 2600:9000:2846:c000:10:3bfc:2740:93a1 2600:9000:2846:d000:10:3bfc:2740:93a1 2600:9000:2846:e000:10:3bfc:2740:93a1 2600:9000:2846:f000:10:3bfc:2740:93a1
rDNS record for 108.139.200.105: server-108-139-200-105.lus50.r.cloudfront.net
Host shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
21/tcp    open  ftp
587/tcp   open  submission
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Uptime guess: 0.000 days (since Thu Oct  3 06:34:46 2024)
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: All zeros
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 176.04 seconds
```

Result

Vulnerabilities

If ports 80, 443, 21, and 587 are open on a server, it indicates that the server is running a web service and an email service. Here's a breakdown of each port, its purpose, potential vulnerabilities, and security recommendations:

1. Port 80 (HTTP)

- **Purpose:** Used for serving web pages over HTTP.
- **Vulnerabilities:**
 - Unencrypted traffic, exposing data to interception.
 - Potential for running outdated web applications with known vulnerabilities.
 - Misconfigurations that may expose sensitive information.
- **Recommendations:**
 - Redirect HTTP traffic to HTTPS.
 - Keep web applications and server software updated.
 - Implement security headers.

2. Port 443 (HTTPS)

- **Purpose:** Used for serving web pages over HTTPS (secure HTTP).
- **Vulnerabilities:**
 - Issues with SSL/TLS certificates (expired or misconfigured).

- Weak or outdated encryption protocols and ciphers.
- Vulnerabilities in web applications running over HTTPS.
- **Recommendations:**
 - Use strong SSL/TLS configurations and ensure proper certificate management.
 - Implement HTTP Strict Transport Security (HSTS).
 - Regularly scan for vulnerabilities.

3. Port 21 (FTP)

- **Purpose:** Used for File Transfer Protocol, typically for transferring files.
- **Vulnerabilities:**
 - Unencrypted file transfers, making it susceptible to interception.
 - Possible exposure to unauthorised access if misconfigured (open anonymous access).
- **Recommendations:**
 - Use secure alternatives like SFTP (SSH File Transfer Protocol) or FTPS (FTP Secure).
 - Disable anonymous access unless necessary and use strong authentication.
 - Regularly update the FTP server software.

4. Port 587 (SMTP)

- **Purpose:** Used for sending emails securely over SMTP.
- **Vulnerabilities:**
 - Misconfigured servers may allow unauthenticated access, leading to spam.
 - Open relay configurations can be exploited for sending unsolicited emails.
- **Recommendations:**
 - Require authentication for sending emails and enforce strong password policies.
 - Implement TLS for email submission.
 - Monitor and configure the server to prevent open relay.

General Security Practices

- **Regular Updates:** Ensure all software, including web servers and mail servers, is kept up to date with security patches.

- **Firewalls:** Use firewalls to restrict access to only necessary ports and services.
- **Monitoring:** Set up logging and monitoring to detect unusual activity on all open ports.
- **Vulnerability Scans:** Regularly conduct scans to identify and remediate vulnerabilities across services.