Bangladesh University of Professionals
Excellence Through Knowledge

Vulnerability Assessment & Port Scanning using ZenMap

Student Name: Saad
ID: 23549109028

Intrusion Management and Ethical Hacking

23-08-2023

—

Faculty: Abul Kalam Azad Sumon

Vulnerability Assessment Report

Target: Triangle Technologies Ltd (triangletech.com.bd / 172.104.165.217)

Scan Name: Triangle Tech

Plugin Set: 202308230804

CVSS_Score: CVSS_V3

Scan Template: Advanced Scan

Assessment Date: August 20-22, 2023

Assessment Tool: Nessus

1. Executive Summary:

The vulnerability assessment conducted on Triangle Technologies Ltd website (triangletech.com.bd) and associated IP address (172.104.165.217) has revealed several vulnerabilities that require immediate attention. These vulnerabilities could potentially lead to unauthorized access, data leakage, and service disruptions if left unaddressed. It is recommended that the necessary measures be taken to remediate these vulnerabilities promptly.

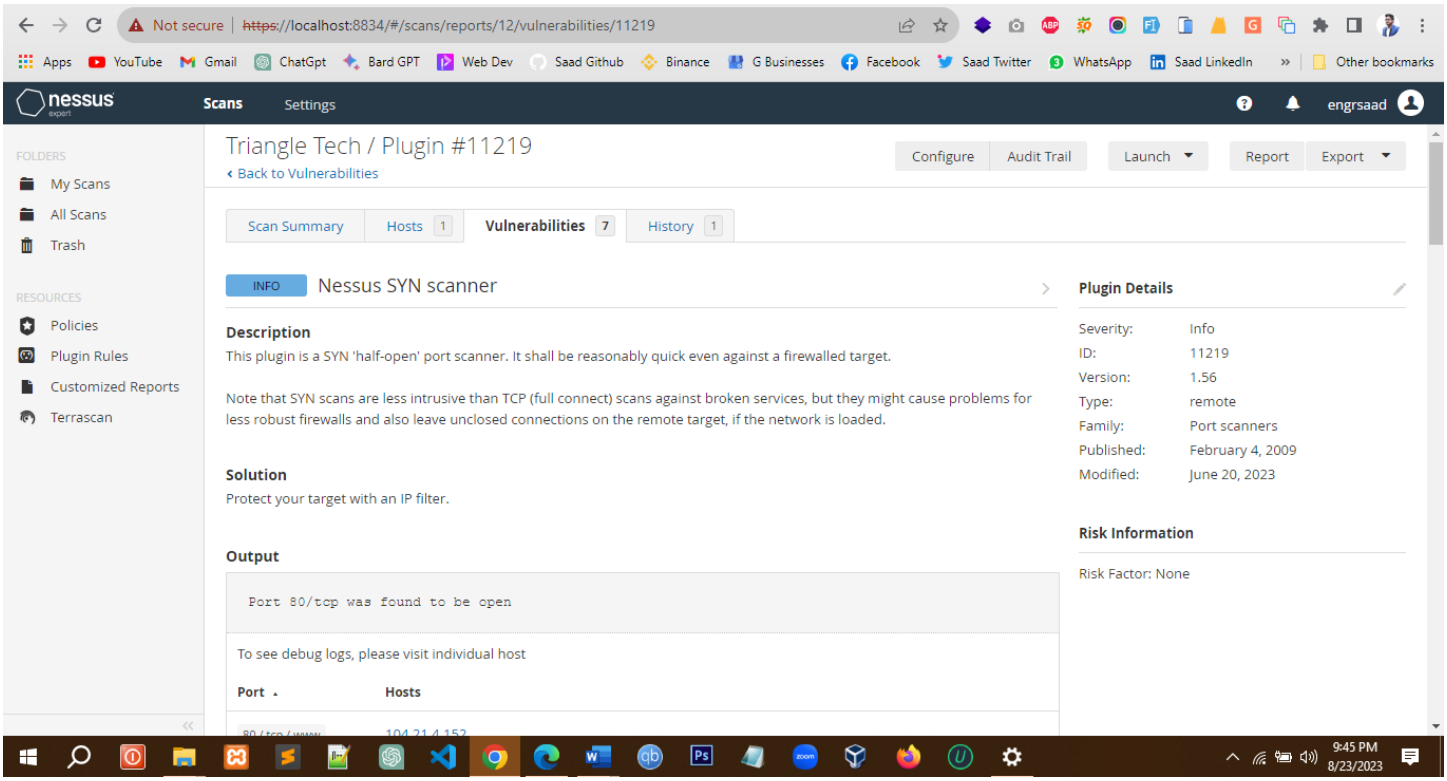
2. Vulnerabilities Found:

1. Nessus SYN scanner

Description: This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Recommendation: Protect your target with an IP filter.

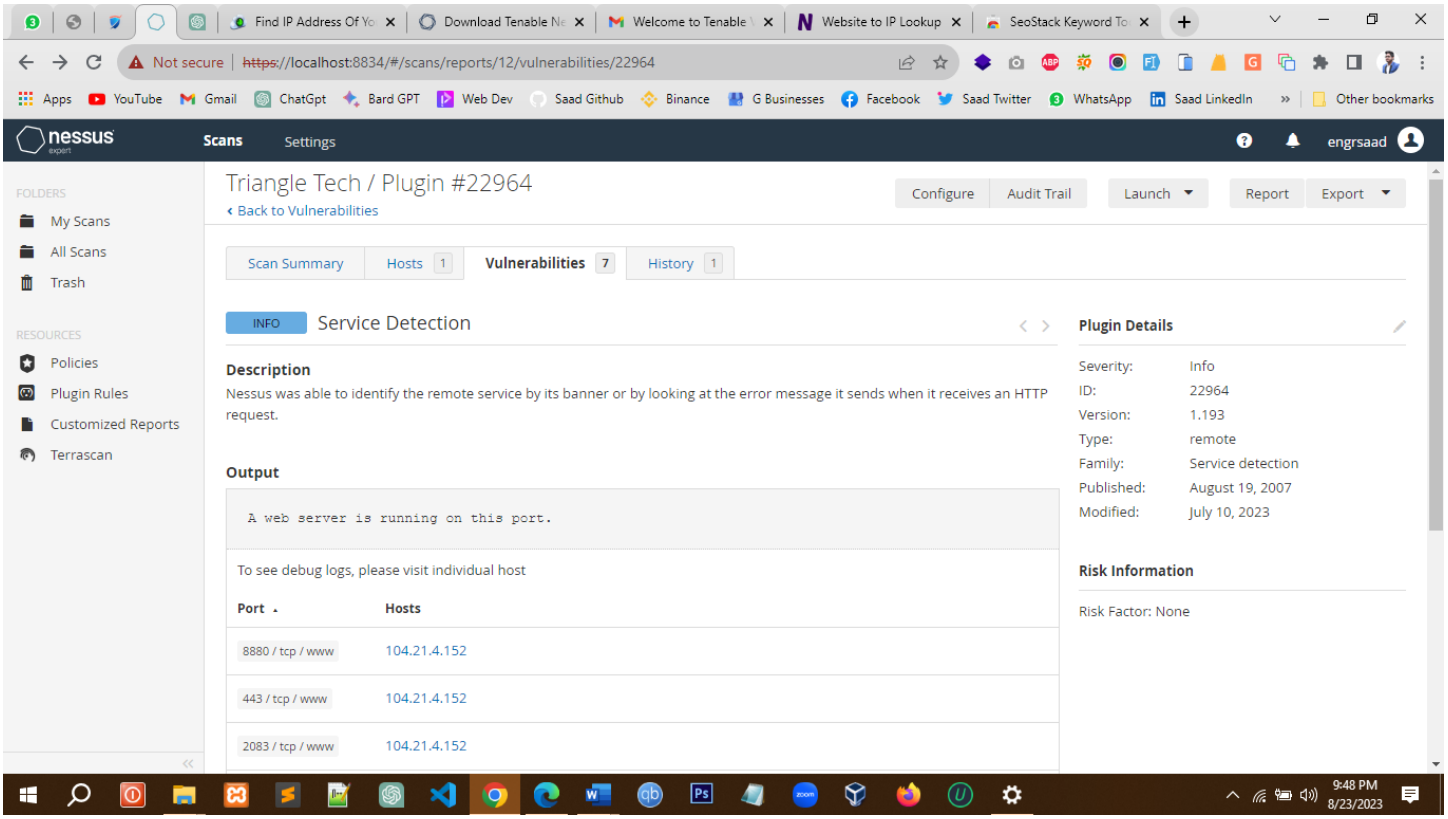


2. Service Detection:

Description: Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Impact: Without encryption, sensitive email content can be intercepted and read by attackers during transit.

Solution: Configure the email system to use TLS for secure email communication. Regularly monitor and audit email security settings.



Recommendation: Disable SSLv3 and outdated TLS protocols. Update the SSL/TLS configuration to prioritize modern and secure protocols. Regularly monitor and update the server's security configuration.

3. Nessus Scan Information

Description: This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.

- The type of scanner (Nessus or Nessus Home).

- The version of the Nessus Engine.

- The port scanner(s) used.

- The port range scanned.

- The ping round trip time

- Whether credentialed or third-party patch management checks are possible.

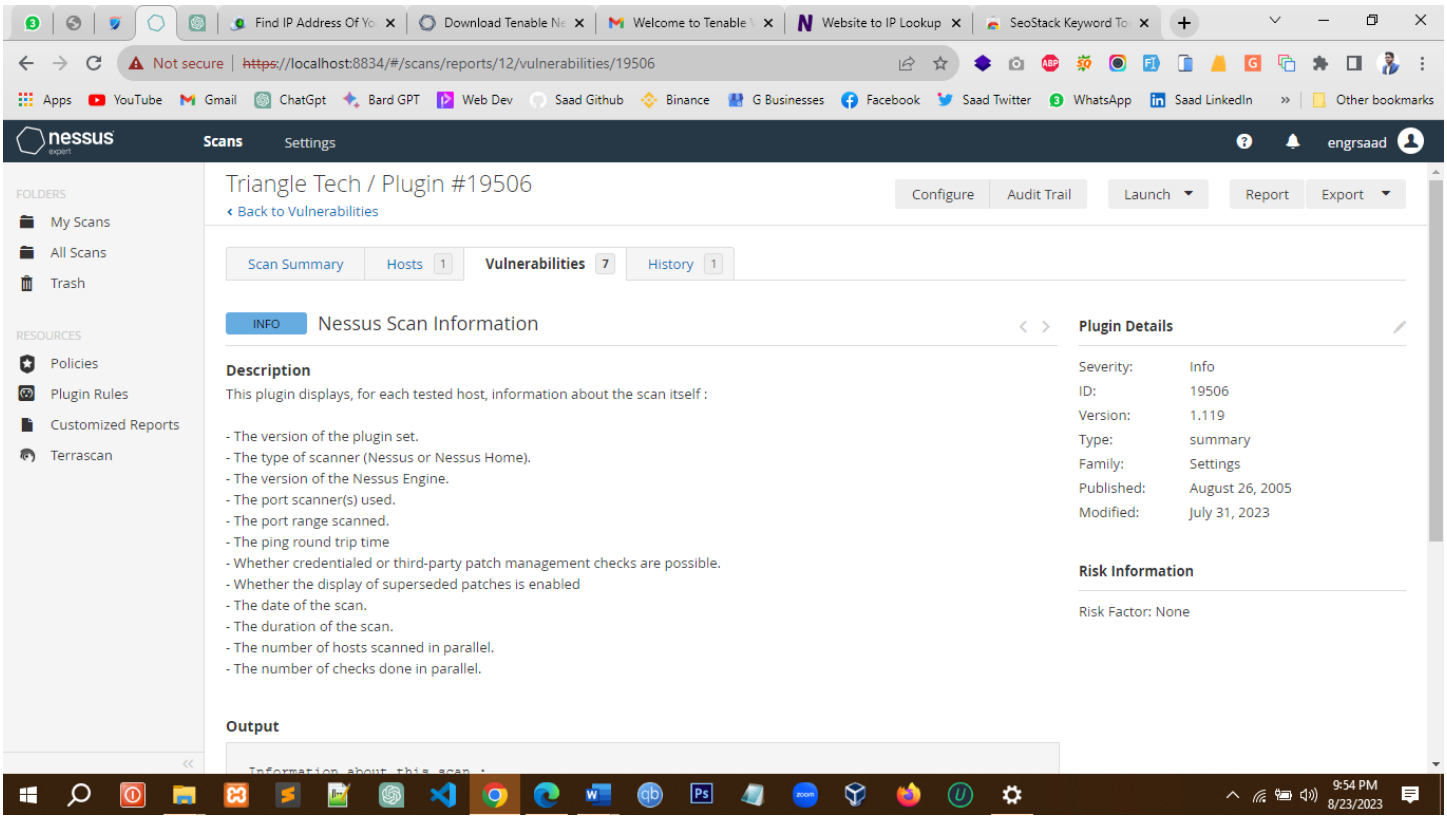
- Whether the display of superseded patches is enabled

- The date of the scan.

- The duration of the scan.

- The number of hosts scanned in parallel.

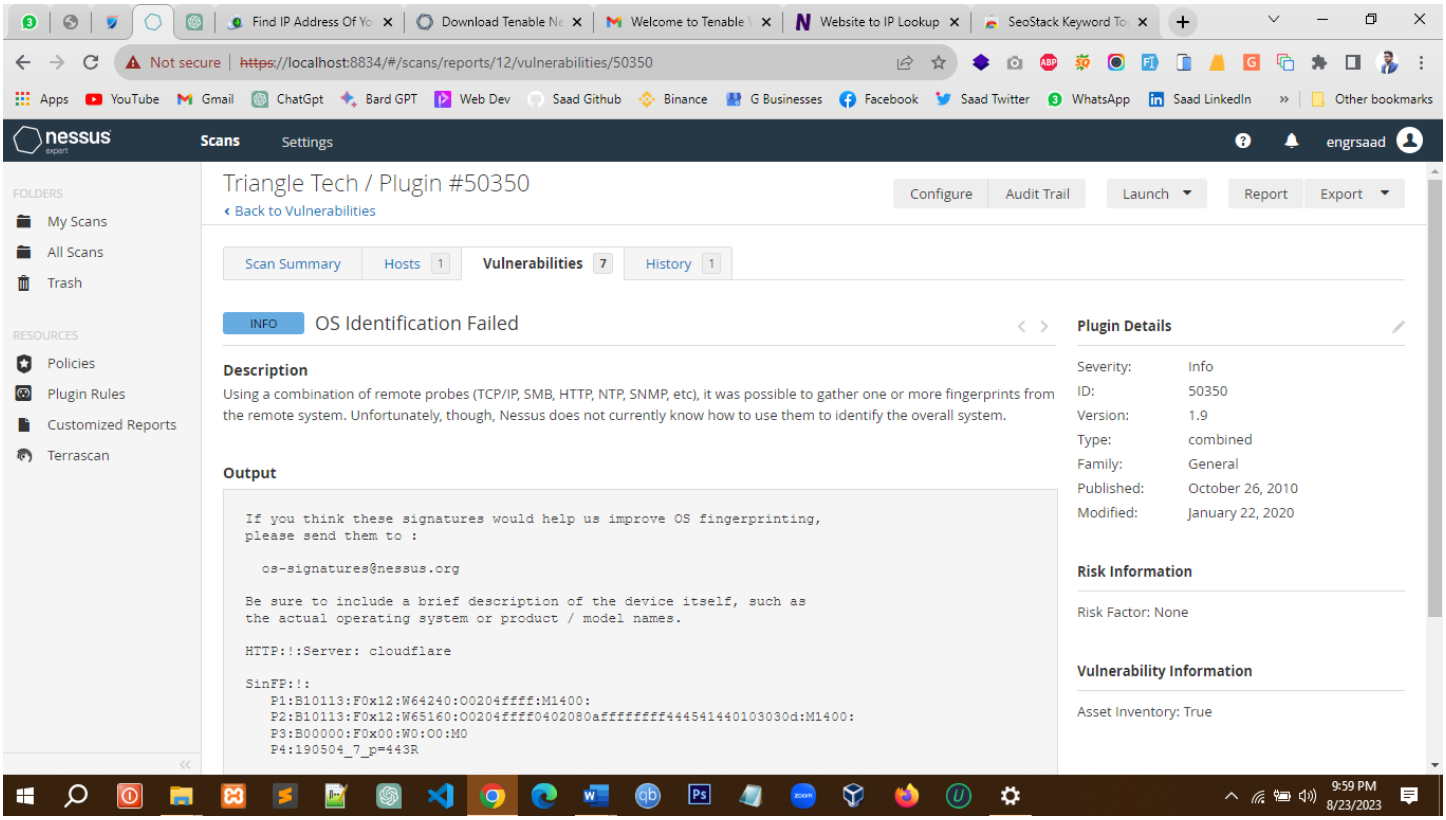
- The number of checks done in parallel.



Output: Max hosts : 5, Max checks : 5, Recv timeout : 5, Backports : None, Allow post-scan editing : Yes, Nessus Plugin Signature Checking : Enabled, Audit File Signature Checking : Disabled

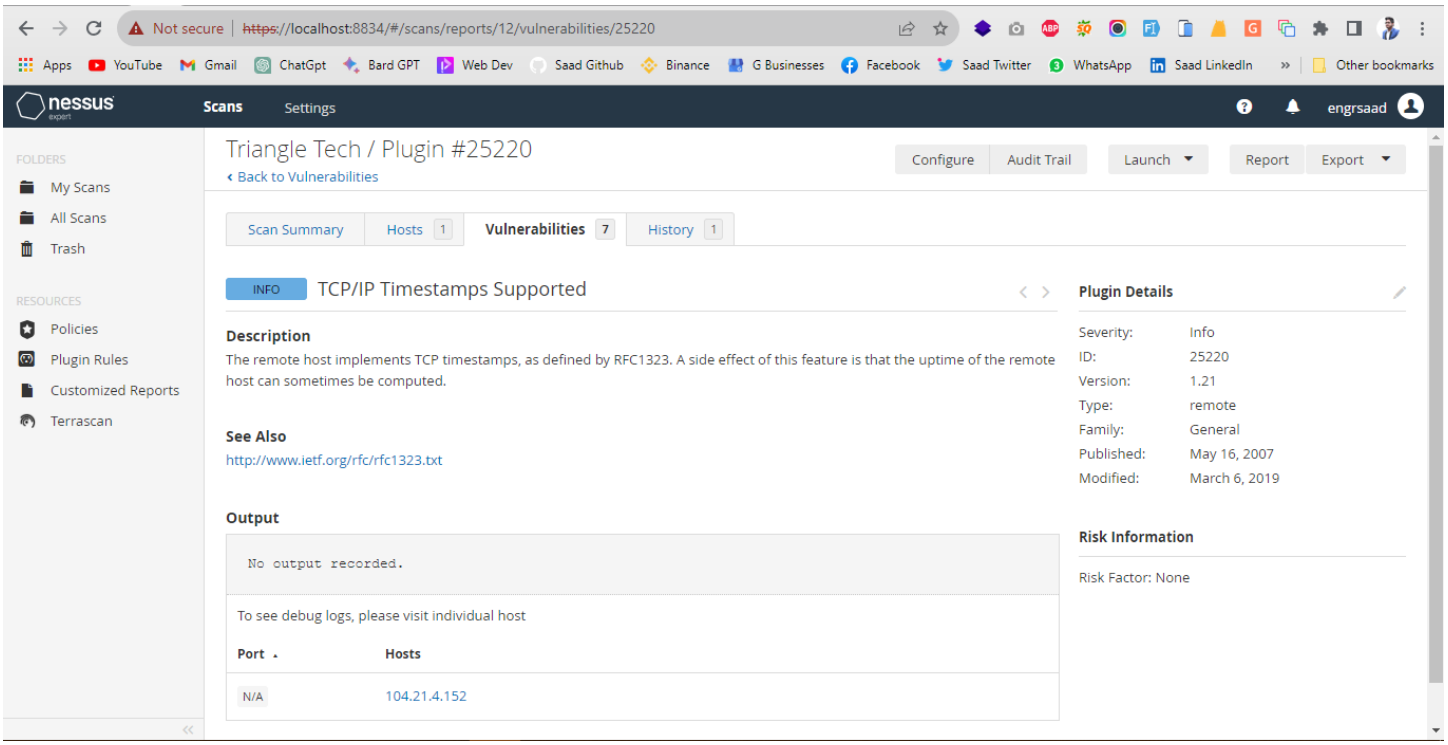
4. OS Identification Failed

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. Unfortunately, though, Nessus does not currently know how to use them to identify the overall system.



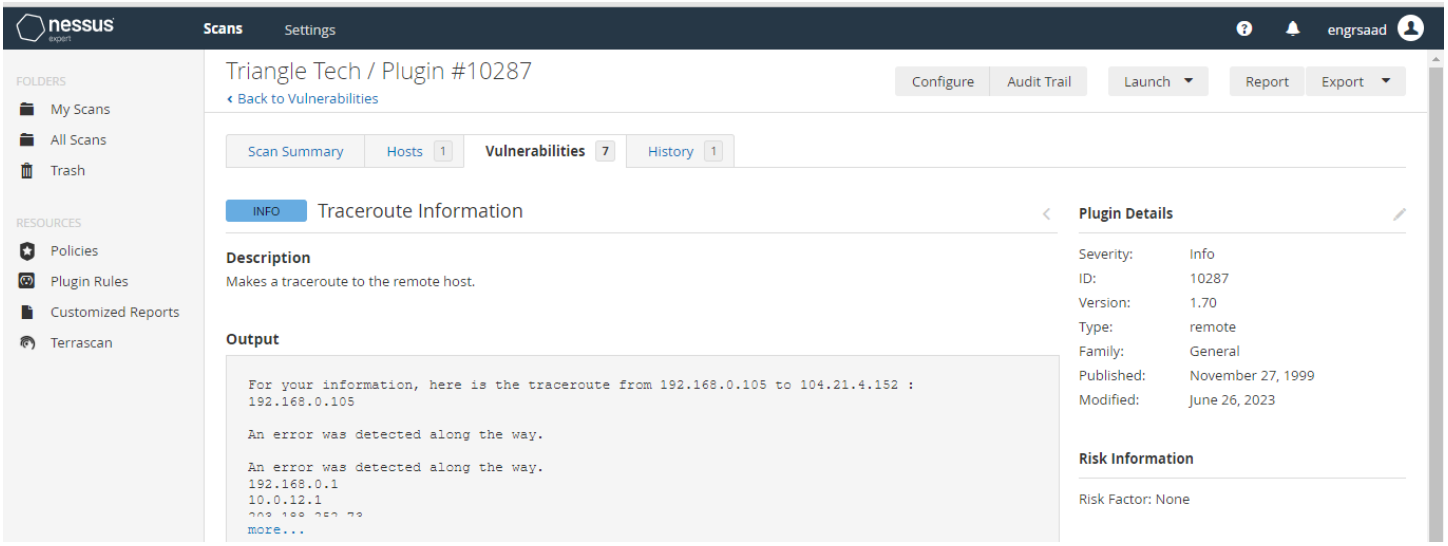
5. TCP/IP Timestamps Supported

Description: The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.



6. Traceroute Information:

Description: Makes a traceroute to the remote host.



7. HTTP Server Type and Version

Description: This plugin attempts to determine the type and the version of the remote web server.

Output

The remote web server type is: **Cloudflare.**

Port Scanning

IP Address: 172.104.165.217

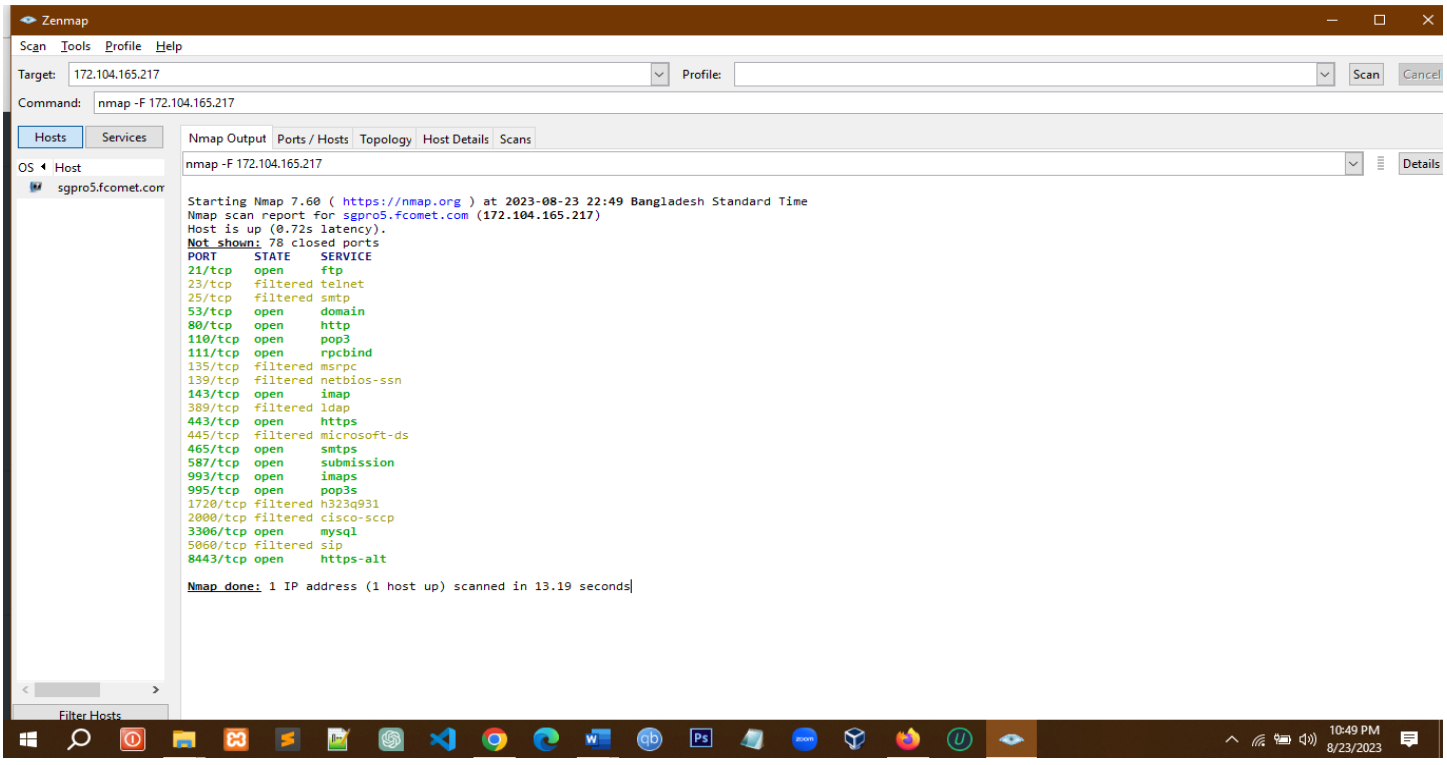
1. Introduction:

This report presents the results of a port scanning exercise conducted on the IP address 172.104.165.217 belonging to Triangle Technologies Ltd. The primary objective of the scan was to identify open ports and services running on the target system.

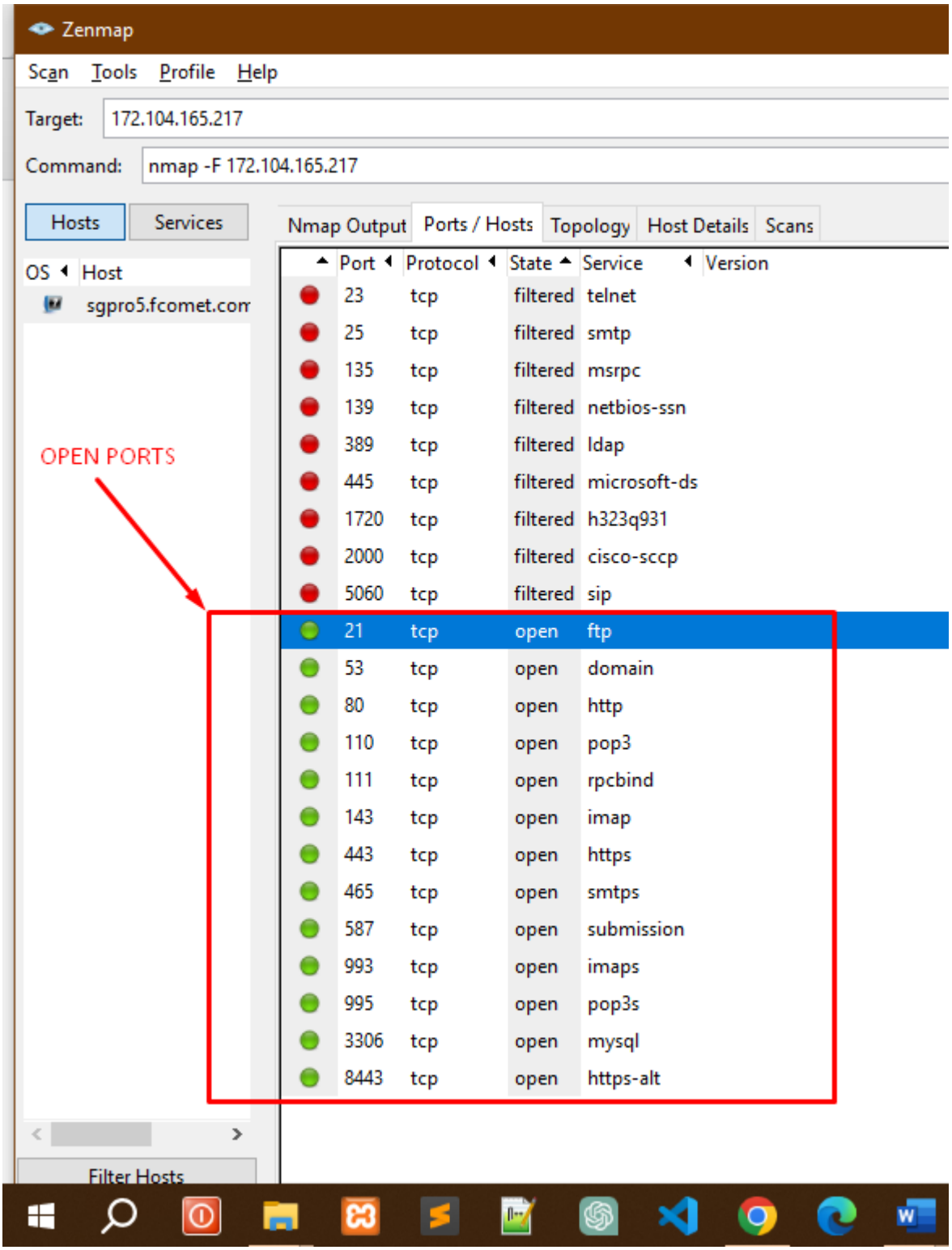
2. Scanning Methodology:

The port scan was performed using Nmap (Network Mapper), a widely used open-source tool for network discovery and security auditing. The scan was non-intrusive and conducted with default parameters, focusing on identifying open ports and associated services.

3. Scanning Results:



The Nmap scan of IP address 172.104.165.217 revealed the following open ports:



4. Open Ports Analysis (Description, Risk and Solution):

Short description, possible risk, and solution for each of the open ports:

Port 21 (FTP):

- Description: File Transfer Protocol (FTP) port for transferring files.

- Risk: Data exposure due to unencrypted transmission.

- Solution: Implement FTP over TLS (FTPS) or consider using more secure file transfer methods.

Port 53 (DNS):

- Description: Domain Name System (DNS) port for translating domain names to IP addresses.

- Risk: DNS attacks, like DDoS or cache poisoning, can disrupt services and compromise network integrity.

- Solution: Implement DNSSEC for data integrity and deploy protective measures against DDoS attacks.

Port 80 (HTTP):

- Description: HTTP port for web browsing.

- Risk: Vulnerable web applications can lead to unauthorized access or data breaches.

- Solution: Regularly update web server software and use security plugins or Web Application Firewalls (WAFs).

Port 110 (POP3):

- Description: Post Office Protocol version 3 (POP3) for retrieving emails.

- Risk: Unencrypted email transmission exposes sensitive data.

- Solution: Enable SSL/TLS for secure email retrieval.

Port 111 (RPC):

- Description: Remote Procedure Call (RPC) port for network communication.

- Risk: Vulnerable RPC services can be exploited for unauthorized access or system compromise.

- Solution: Disable unnecessary RPC services, use firewalls, and keep systems patched.

Port 143 (IMAP):

- Description: Internet Message Access Protocol (IMAP) port for email retrieval.

- Risk: Unencrypted email transmission and potential for unauthorized access.

- Solution: Enable SSL/TLS for secure email retrieval.

Port 443 (HTTPS):

- Description: HTTPS port for secure web browsing.

- Risk: Exploitable vulnerabilities in SSL/TLS implementations can lead to data breaches.

- Solution: Implement strong SSL/TLS configurations, keep certificates updated, and follow security best practices.

Port 465 (SMTPS):

- Description: SMTP over SSL (SMTPS) port for secure email transmission.

- Risk: Vulnerabilities in SMTP servers can lead to unauthorized email access or interception.

- Solution: Secure SMTP server configuration, use of SSL/TLS, and regular patching.

Port 587 (Submission):

- Description: Email submission port for clients to send emails to servers.

- Risk: Misconfigured email servers can be exploited for spam relaying.

- Solution: Implement secure email submission with proper authentication and encryption.

Port 993 (IMAPS):

- Description: IMAP over SSL (IMAPS) port for secure email retrieval.

- Risk: Unencrypted email transmission and potential for unauthorized access.

- Solution: Enable SSL/TLS for secure email retrieval.

Port 995 (POP3S):

- Description: POP3 over SSL (POP3S) port for secure email retrieval.

- Risk: Unencrypted email transmission and potential for unauthorized access.

- Solution: Enable SSL/TLS for secure email retrieval.

Port 3306 (MySQL):

- Description: MySQL database port.

- Risk: Vulnerabilities in MySQL can lead to unauthorized database access or data leaks.

- Solution: Secure MySQL configurations, limit access, and keep the software updated.

Port 8443:

- Description: HTTPS port for secure web browsing (alternative to port 443).

- Risk: Similar to port 443, vulnerabilities in SSL/TLS implementations can lead to data breaches.

- Solution: Implement strong SSL/TLS configurations, keep certificates updated, and follow security best practices.

This assessment provides a clear view of Triangle Tech website current security status. By addressing the vulnerabilities, I have identified and following the suggested solutions, we can significantly improve website defenses.