Subtask 2 - Reconnaissance Report

Domain Information

Basic Domain Details

Primary Domain: maltego.com
Observed Hostname: qa.maltego.com

Identified IP Addresses

1. **20.54.254.195**
2. **20.86.128.89**
3. **168.63.129.95** (returned 404 in one result)

Hosting & Infrastructure Details

Cloud Provider: Azure
Cloud Service: AzureCloud
Cloud Region: westeurope
Country: Netherlands
City: Amsterdam
Organization: Microsoft Corporation
ISP: Microsoft Corporation
ASN: AS8075

This indicates that maltego.com infrastructure is hosted on Microsoft Azure cloud environment in the West Europe region.

Open Ports & Exposed Services (From Shodan)

From the Shodan results for IP 20.54.254.195:

Open Ports Detected

- Port 80 (HTTP)
- Port 443 (HTTPS)

No SSH (22), FTP (21), RDP (3389), or database ports were observed in the screenshots.

Port 80 – HTTP

Service: nginx
Version Observed: nginx/1.13.12

Response:

- HTTP/1.1 301 Moved Permanently

- Redirects to HTTPS

This indicates HTTP traffic is being redirected securely to HTTPS.

Port 443 – HTTPS

Service: nginx
Version Observed:

- nginx/1.13.12
- nginx/1.18.0 (Ubuntu) on second host

SSL Certificate Details:

- Issuer: GoDaddy Secure Certificate Authority – G2
- Organization: GoDaddy, Inc.
- Common Name: *.qa.maltego.com
- Supported TLS Versions:
    - TLSv1
    - TLSv1.1
    - TLSv1.2
    - TLSv1.3 (on second server)

Observation:
TLSv1 and TLSv1.1 are deprecated and may pose minor security risks if enabled.

Vulnerabilities Section (Shodan)

Shodan identified multiple vulnerabilities associated with the detected nginx service versions. The vulnerabilities are inferred based on the software version and publicly known CVEs.

Identified CVEs

◈ CVE-2025-23419

CVSS Score: 4.3 (Medium)
Description:
When multiple server blocks share the same IP address and port, session resumption mechanisms may allow bypassing client certificate authentication requirements. This issue is related to TLS Session Tickets and SSL session caching configurations in nginx.
Impact: Potential bypass of client authentication under specific configuration conditions.

◈ CVE-2023-44487

CVSS Score: 7.5 (High)
Description:
HTTP/2 protocol vulnerability allowing Denial of Service (DoS) through rapid request cancellation, leading to excessive server resource consumption. This vulnerability was actively exploited in the wild in 2023.
Impact: Server resource exhaustion and service disruption.

◈ CVE-2021-23017

CVSS Score: 7.7 (High)
Description:
A vulnerability in the nginx resolver component allowing an attacker to forge UDP packets from a DNS server, potentially causing a 1-byte memory overwrite.
Impact: Worker process crash or possible further memory corruption.

◈ CVE-2021-3618

CVSS Score: 7.4 (High)
Description:
ALPACA (Application Layer Protocol Confusion Attack) vulnerability affecting TLS servers that use compatible certificates across different protocols. An attacker may redirect traffic between services under certain conditions.
Impact: Cross-protocol attacks and potential authentication bypass.

Subdomain Enumeration (Using Sublist3r)

Command Used:

sublist3r -d maltego.com -t 50

Total Unique Subdomains Found: 14

Discovered Subdomains:

1. www.maltego.com
2. academy.maltego.com
3. app.maltego.com
4. auth.maltego.com
5. docs.maltego.com
6. downloads.maltego.com
7. get.maltego.com
8. identity.maltego.com

9. login.maltego.com
10. monitor.maltego.com
11. osint-profiler.maltego.com
12. static.maltego.com
13. store.maltego.com
14. support.maltego.com

These were discovered using passive enumeration techniques across multiple search engines and certificate transparency logs.

No brute-force mode was indicated in the output.

Summary Table (Corrected Based on Your Findings)

Timestamp	Tool	Finding
2026-02-13 01:57:31	Shodan	IP 20.54.254.195 hosted on Azure (Netherlands)
2026-02-13 02:01:05	Shodan	Open ports 80 and 443 detected
2026-02-13 02:01:17	Shodan	nginx web server running (1.13.12 / 1.18.0)
2026-02-13 02:10:24	Sublist3r	14 subdomains discovered for maltego.com

(Note: The example entries you provided — SSH on 192.168.1.50 and dev.example.com — were placeholders and not related to your actual screenshots, so they were not included in the final report.)

Overall Security Observations

1. Infrastructure hosted on Microsoft Azure (well-managed cloud provider).
2. Only standard web ports (80, 443) exposed.
3. HTTP properly redirects to HTTPS.
4. SSL certificate properly configured via GoDaddy.
5. Some deprecated TLS versions appear enabled (TLSv1, TLSv1.1).
6. No high-risk exposed services such as:
    - SSH (22)
    - RDP (3389)
    - FTP (21)
    - Database ports