SUBMITTED BY: IQRA JAWAD AHMED

TASK_01: Information Gathering

1.https://www.netacad.com/

Target Domain: netacad.com
Target IP (WHOIS): 34.120.22.226
Hosting/Infra: Amazon Web Services (AWS)
Registrar: MarkMonitor Inc.

Host Status:

- WHOIS indicates Cisco Technology Inc. as the registrant (San Jose, CA, USA).

Important Dates:

- Created: 07-Dec-1998
- Updated: 02-Aug-2024
- Expiry: 06-Dec-2025

Nameservers (AWS Route53):

- ns-748.awsdns-29.net → 205.251.194.236
- ns-1911.awsdns-46.co.uk → 205.251.199.119
- ns-240.awsdns-30.com → 205.251.192.240
- ns-1476.awsdns-56.org → 205.251.197.196

Domain Status (ICANN EPP Codes):

- clientDeleteProhibited
- clientTransferProhibited
- clientUpdateProhibited

Registrant Contact:

- Organization: Cisco Technology Inc.

- Location: San Jose, CA, USA
- Admin Email: infosec[at]cisco[dot]com
- Phone: +1.408.527.3842

Technology used (Observed by Wappalyzer)

- **Analytics & Tracking**
    - LinkedIn Insight Tag
    - Facebook Pixel
    - Google Analytics (GA4)
- **Performance & Monitoring**
    - AppDynamics (RUM & Monitoring)
- **JavaScript Frameworks**
    - React
    - Emotion
    - React Router 6
- **Security**
    - HSTS
- **Programming Languages**
    - GraphQL
    - Python
- **CDN**
    - Amazon CloudFront
- **Marketing Automation**
    - Marketo
- **Tag Managers**

    - Google Tag Manager

- **JavaScript Libraries**
    - Howler.js
    - core-js 3.32.2
    - Lodash 4.17.21
    - Apollo 3.13.1

Vulnerabilities:

Google Analytics GA4 (HT Easy GA4 Plugin)

CVE-2024-29094

- Published Date: 2024-03-19
- CNA: Patchstack
- Description: Stored Cross-Site Scripting (XSS) in HasThemes HT Easy GA4 plugin (≤ 1.1.7).
    - **Cause:** Insufficient input sanitization and output escaping.
    - **Impact**: Attackers can inject malicious scripts into stored content, leading to credential theft, session hijacking, or redirection to malicious sites.

CVE-2024-1176

- Published Date: 2024-03-13
- CNA: Wordfence
- Description: Unauthorized data modification in HT Easy GA4 plugin (≤ 1.1.5) due to missing capability check on the `login()` function.
    - **Cause:** Lack of proper authentication and access control.
    - **Impact:** Unauthenticated attackers can update email settings or alter sensitive plugin configurations, leading to compromised analytics data.

CVE-2023-23802

- Published Date: 2023-06-15
- CNA: Patchstack
- Description: Cross-Site Request Forgery (CSRF) in HasThemes HT Easy GA4 plugin (≤ 1.0.6).
    - **Cause:** Missing CSRF token validation.
    - **Impact:** Attackers can trick authenticated users into executing unwanted actions, such as changing plugin configurations.

Lodash 4.17.21

CVE-2021-23337

- **Published Date: 2021-02-15**
- **Description:** Command Injection vulnerability in Lodash versions prior to 4.17.21 via the `template` function.
    - **Cause:** Improper handling of user input in template compilation.
    - **Impact:** Remote attackers could execute arbitrary system commands.

CVE-2020-28500

- **Published Date: 2021-02-15**
- **Description:** Regular Expression Denial of Service (ReDoS) in Lodash versions prior to 4.17.21 via `toNumber`, `trim`, and `trimEnd` functions.
    - **Cause:** Inefficient regex execution on crafted input.
    - **Impact:** Attackers can cause excessive CPU consumption, leading to denial of service (DoS).

2. http://www.chatgpt.com

WHOIS Information "chatgpt.com"

IP Address: 172.64.155.209

Registrar: MarkMonitor Inc.
WHOIS Server: whois.markmonitor.com
Referral URL: http://www.markmonitor.com

Important Dates:

- **Created: 30-Nov-2022**
- **Updated: 17-Oct-2024**
- **Expires: 30-Nov-2026**

Nameservers:

- **savanna.ns.cloudflare.com (108.162.194.136)**
- **hassan.ns.cloudflare.com (162.159.44.149)**

Domain Status:

- **clientDeleteProhibited**
- **clientTransferProhibited**
- **clientUpdateProhibited**
- **serverDeleteProhibited**
- **serverTransferProhibited**
- **serverUpdateProhibited**

Registrant Contact:

- **Organization: OpenAI**
- **Address: US**
- **Email: Available via request form at MarkMonitor**

Technology used (Observed by Wappalyzer)

JavaScript Frameworks

- React
- React Router 7.5.2

JavaScript Libraries

- MobX
- Framer Motion
- core-js 3.32.2

Security

- Cloudflare Bot Management

CDN

- Cloudflare

Advertising

- Google Ads

Vulnerabilities
ReactRouter 7.5.2

CVE-2025-43865

- Published Date: 2025-04-25
- CNA: GitHub, Inc.
- Description: React Router (7.0 branch, prior to 7.5.2) allows modification of pre-rendered data by adding a crafted header to the request. This can spoof the contents of the HTML data object and manipulate all values passed to the client.
    - **Cause:** Improper validation of request headers during server-side rendering.
    - **Impact:** Attackers can inject or alter pre-rendered data, leading to data tampering, content spoofing, and possible user misdirection.

CVE-2025-43864

- Published Date: 2025-04-25
- CNA: GitHub, Inc.
- Description: React Router (from 7.2.0 to prior 7.5.2) can be forced into SPA mode via a malicious header injection. For applications using SSR, this switch results in

corrupted pages and potential service disruption.

- **Cause:** Insufficient checks on request headers controlling rendering mode.
- **Impact:** Attackers can break SSR behavior, corrupt rendered pages, and cause denial of service (DoS)-like effects.

3. https://www.duolingo.com
WHOIS Information "duolingo.com"

IP Address: 54.167.168.56

Registrar: Amazon Registrar, Inc.
WHOIS Server: whois.registrar.amazon
Referral URL: http://registrar.amazon.com

Important Dates:

- **Created: 26-Jan-2010**
- **Updated: 23-Dec-2024**
- **Expires: 26-Jan-2026**

Nameservers:

- **ns-1117.awsdns-11.org (205.251.196.93)**
- **ns-1020.awsdns-63.net (205.251.195.252)**
- **ns-247.awsdns-30.com (205.251.192.247)**
- **ns-1904.awsdns-46.co.uk (205.251.199.112)**

Domain Status:

- **clientDeleteProhibited**
- **clientTransferProhibited**
- **clientUpdateProhibited**

Registrant Contact:

- **Name: On behalf of duolingo.com owner**
- **Organization: Identity Protection Service**
- **Address: Hayes, Middlesex, GB**
- **Phone: +44.1483307527**
- **Fax: +44.1483304031**
- **Email: cd76db5d-98d4-421a-aecd-0b4666e8b35e [at] identity-protect [dot] org**

Tech Contact:

- **Name: On behalf of the owner**
- **Organization: Identity Protection Service**
- **Address: Hayes, Middlesex, GB**
- **Phone: +44.1483307527**
- **Fax: +44.1483304031**
- **Email: cd76db5d-98d4-421a-aecd-0b4666e8b35e [at] identity-protect [dot] org**

Similar Domains:
duoli56.com, duoli8.com, duoliangcm.com, duolian.online, duolia.org, duolibras.com.br, duolibro.com, duoli.cc, duolicious.com, duoli.cn

Technology used (Observed by Wappalyzer)

Google Analytics

- GA4

JavaScript Frameworks

- React
- React Router (6)

Security

- reCAPTCHA

Tag Managers

- Google Tag Manager

JavaScript Libraries

- Lodash (4.17.21)
- Howler.js
- core-js (3.25.3)

Load Balancers

- Amazon ALB

Vulnerabilities:

Google Analytics GA4 (HT Easy GA4 Plugin)

CVE-2024-29094

- Published Date: 2024-03-19
- CNA: Patchstack
- Description: Stored Cross-Site Scripting (XSS) in HasThemes HT Easy GA4 plugin (≤ 1.1.7).
    - **Cause:** Insufficient input sanitization and output escaping.
    - **Impact**: Attackers can inject malicious scripts into stored content, leading to credential theft, session hijacking, or redirection to malicious sites.

CVE-2024-1176

- Published Date: 2024-03-13
- CNA: Wordfence

- Description: Unauthorized data modification in HT Easy GA4 plugin (≤ 1.1.5) due to a missing capability check on the `login()` function.
    - **Cause:** Lack of proper authentication and access control.
    - **Impact:** Unauthenticated attackers can update email settings or alter sensitive plugin configurations, leading to compromised analytics data.

CVE-2023-23802

- Published Date: 2023-06-15
- CNA: Patchstack
- Description: Cross-Site Request Forgery (CSRF) in HasThemes HT Easy GA4 plugin (≤ 1.0.6).
    - **Cause:** Missing CSRF token validation.
    - **Impact:** Attackers can trick authenticated users into executing unwanted actions, such as changing plugin configurations.

Lodash 4.17.21

CVE-2021-23337

- **Published Date: 2021-02-15**
- **Description:** Command Injection vulnerability in Lodash versions prior to 4.17.21 via the `template` function.
    - **Cause:** Improper handling of user input in template compilation.
    - **Impact:** Remote attackers could execute arbitrary system commands.

CVE-2020-28500

- **Published Date: 2021-02-15**

- **Description:** Regular Expression Denial of Service (ReDoS) in Lodash versions prior to 4.17.21 via `toNumber`, `trim`, and `trimEnd` functions.
    - **Cause:** Inefficient regex execution on crafted input.
    - **Impact:** Attackers can cause excessive CPU consumption, leading to denial of service (DoS).

4. https://app.grammarly.com/

WHOIS Information: grammarly.com

IP Address: 18.154.227.9

Registrar: GoDaddy.com, LLC
WHOIS Server: whois.godaddy.com
Referral URL: http://www.godaddy.com

Important Dates:

- **Created: 1-Jul-2009**
- **Updated: 2-Jul-2023**
- **Expires: 1-Jul-2026**

Nameservers:

- **ns-1221.awsdns-24.org (205.251.196.197)**
- **ns-1588.awsdns-06.co.uk (205.251.198.52)**
- **ns-835.awsdns-40.net (205.251.195.67)**
- **ns-422.awsdns-52.com (205.251.193.166)**

Domain Status:

- **clientDeleteProhibited**
- **clientRenewProhibited**
- **clientTransferProhibited**
- **clientUpdateProhibited**

Registrant Contact:

- **Name: Registration Private**
- **Organization: Domains By Proxy, LLC**
- **Address: Tempe, Arizona, US**
- **Phone: +1.4806242599**
- **Email: Contact via GoDaddy Whois**

Tech Contact:

- **Name: Registration Private**
- **Organization: Domains By Proxy, LLC**
- **Address: Tempe, Arizona, US**
- **Phone: +1.4806242599**
- **Email: Contact via GoDaddy Whois**

Technologies Used(Observed by Wappalyzer)

Analytics

- Google Analytics (GA4)

JavaScript Frameworks

- React JS

Web Servers

- Nginx

Advertising

- Microsoft Advertising

Tag Managers

- Google Tag Manager

Vulnerabilities:

Google Analytics GA4 (HT Easy GA4 Plugin)

CVE-2024-29094

- **Published Date:** 2024-03-19
- **Description:** Stored Cross-Site Scripting (XSS) in HasThemes HT Easy GA4 plugin (≤ 1.1.7).
    - **Cause:** Insufficient input sanitization and output escaping.
    - **Impact:** Attackers can inject malicious scripts into stored content, leading to credential theft, session hijacking, or redirection to malicious sites.

CVE-2024-1176

- **Published Date:** 2024-03-13
- **CNA:** Wordfence
- **Description:** Unauthorized data modification in HT Easy GA4 plugin (≤ 1.1.5) due to missing capability check on the `login()` function.
    - **Cause:** Lack of proper authentication and access control.
    - **Impact:** Unauthenticated attackers can update email settings or alter sensitive plugin configurations, leading to compromised analytics data.

CVE-2023-23802

- **Published Date:** 2023-06-15
- **CNA:** Patchstack
- **Description:** Cross-Site Request Forgery (CSRF) in HasThemes HT Easy GA4 plugin (≤ 1.0.6).
    - **Cause**: Missing CSRF token validation.
    - **Impact:** Attackers can trick authenticated users into executing unwanted actions, such as changing plugin configurations.

5.https://www.neduet.edu.pk/

WHOIS Information: neduet.com

IP Address: 111.68.110.16

Registrar: TurnCommerce, Inc. DBA NameBright.com
WHOIS Server: whois.namebright.com
Referral URL: http://www.NameBright.com

Important Dates:

- **Created: 27-Aug-2012**
- **Updated: 21-Aug-2021**
- **Expires: 27-Aug-2025**

Nameservers:

- **domain-for-sale.hugedomainsdns.com (54.92.157.22)**
- **forsale.hugedomainsdns.com (18.234.81.192)**

Domain Status:

- **clientTransferProhibited**

Registrant Contact:

- **Name: Domain Admin / This Domain is For Sale**
- **Organization: HugeDomains.com**
- **Address: Denver, CO, US**
- **Phone: +1.3038930552**
- **Email: domains [at] hugedomains [dot] com**

Admin Contact:

- **Name: Domain Admin / This Domain is For Sale**
- **Organization: HugeDomains.com**
- **Address: Denver, CO, US**

- **Phone: +1.3038930552**
- **Email: domains [at] hugedomains [dot] com**

Tech Contact:

- **Name: Domain Admin / This Domain is For Sale**
- **Organization: HugeDomains.com**
- **Address: Denver, CO, US**
- **Phone: +1.3038930552**
- **Email: domains [at] hugedomains [dot] com**

Similar Domains:
nedue.com, nedu.edu.cn, nedue.info, neduem.com, neduere.ch, nedue.se, neduese.us, neduessa.de, neduet.net

Technology Used (Observed by Wappalyzer)

Analytics

- Google Analytics (GA4)

Web Servers

- Apache HTTP Server

Programming Languages

- Perl
- Java

JavaScript Libraries

- Modernizr 2.0.6
- jQuery 3.2.1

UI Frameworks

- Bootstrap 3.3.7

Vulnerabilities

Google Analytics GA4 (HT Easy GA4 Plugin)

CVE-2024-29094

- **Published Date:** 2024-03-19
- **CNA:** Patchstack
- **Description:** Stored Cross-Site Scripting (XSS) in HasThemes HT Easy GA4 plugin (≤ 1.1.7).
    - **Cause:** Insufficient input sanitization and output escaping.
    - **Impact:** Attackers can inject malicious scripts into stored content, leading to credential theft, session hijacking, or redirection to malicious sites.

CVE-2024-1176

- **Published Date:** 2024-03-13
- **CNA:** Wordfence
- **Description:** Unauthorized data modification in HT Easy GA4 plugin (≤ 1.1.5) due to a missing capability check on the `login()` function.
    - **Cause:** Lack of proper authentication and access control.
    - **Impact:** Unauthenticated attackers can update email settings or alter sensitive plugin configurations, leading to compromised analytics data.

CVE-2023-23802

- **Published Date:** 2023-06-15
- **CNA:** Patchstack

- **Description:** Cross-Site Request Forgery (CSRF) in HasThemes HT Easy GA4 plugin (≤ 1.0.6).
    - **Cause:** Missing CSRF token validation.
    - **Impact:** Attackers can trick authenticated users into executing unwanted actions, such as changing plugin configurations.

Bootstrap 3.3.7

CVE-2021-40975

Published Date: 2021-10-01
CNA: MITRE
Description: A Cross-Site Scripting (XSS) vulnerability exists in `application/modules/admin/views/ecommerce/products.php` within Ecommerce-CodeIgniter-Bootstrap (CodeIgniter 3.1.11, Bootstrap 3.3.7). This allows remote attackers to inject arbitrary web scripts or HTML via the `search_title` parameter.

TASK2: Nmap Reconnaissance Report

Target 1: NED University of Engineering & Technology

- Target IP: 111.68.110.16
- Domain: neduet.edu.pk

Findings

- Host Status: Responsive, low latency (0.5–28 ms), 2 hops away.
- TCP Ports: All 1000 default ports filtered. Specific checks (21, 22, 25, 53, 80, 443) also filtered.
- UDP Ports: Top 20 tested → open|filtered (inconclusive).
- OS Detection: Inconclusive (no open/closed ports).
- Traceroute: Direct path in 2 hops (local → target).

Conclusion

- Host is live but heavily firewalled.

- No services could be identified; IDS/IPS likely in place.
- Only whitelisted ports (likely 80/443) are accessible for actual traffic.

Target 2: ChatGPT (Cloudflare Infrastructure)

- Target IP: 172.64.155.209
- Domain: www.chatgpt.com (resolves via Cloudflare CDN)

Findings

- Host Status: Initially appeared down, but alive with `-Pn` (ICMP blocked).
- TCP Ports: All tested ports (21, 22, 25, 53, 80, 443) filtered.
- UDP Ports: Attempts → host down (UDP blocked).
- OS & Service Detection: Failed (no open ports).
- Firewall Evasion: Fragmentation, decoys, and source-port tricks are ineffective.

Conclusion

- Host is alive but fully shielded by Cloudflare's edge firewall.
- Behavior matches Cloudflare CDN: ICMP blocked, ports filtered, no banners.
- The real ChatGPT origin servers are hidden behind Cloudflare.

Target 3: Duolingo

- Target IP: 54.167.168.56
- Domain: duolingo.com

Findings

- Host Status: Inconsistent ping failed, but `-Pn` confirmed host is up.
- TCP Ports: All tested (default 1000 + top 200) filtered.
- UDP Ports: Attempts failed (host marked down).

- Firewall Evasion: Xmas, fragments, and decoys are ineffective.
- OS/Service Detection: Not possible (no responses).

Conclusion

- Target is online but heavily protected.
- All traffic blocked at network edge → likely AWS firewall/CDN.
- Recon blocked by strong filtering; origin servers hidden.

Target 4: Grammarly (Amazon CloudFront)

- Target IP: 18.154.227.9
- Hostname: server-18-154-227-9.iad55.r.cloudfront.net
- Domain: grammarly.com (resolves via AWS CloudFront CDN)

Findings

- Host Status: Alive, responsive (~0.02–0.08s latency).
- TCP Ports: Only 80 (HTTP) and 443 (HTTPS) are open. All others filtered.
- UDP Ports: Top 50 → open|filtered (no useful data).
- Services:
    - 80/tcp → CloudFront HTTP (default error page).
    - 443/tcp → CloudFront HTTPS.
- Traceroute: Local gateway → CloudFront edge node.
- OS Detection: Inconclusive (CDN masking origin).
- Other Scans: Fragmented/UDP scans blocked.

Conclusion

- This is an Amazon CloudFront edge server for Grammarly.

- Only web ports (80/443) are exposed.
- Real Grammarly backend servers are hidden by CDN.

Target 5: Cisco Networking Academy (NetAcad)

- **Target IP:** 34.120.22.226
- **Domain:** netacad.com

Finding

Host Status:

- Responsive with low latency (~2–25 ms).
- Multiple CDN/proxy layers detected (Google Cloud / CloudFront-like infrastructure).

TCP Ports:

- All 1000 default ports scanned → filtered or closed.
- Specific checks on common services:
    - **80 (HTTP):** filtered (redirects handled at CDN layer).
    - **443 (HTTPS):** open – TLS/SSL service detected, serving NetAcad platform.
    - **22 (SSH):** filtered.
    - **25 (SMTP):** filtered.
    - **53 (DNS):** filtered (handled by external authoritative servers).

UDP Ports:

- Top 20 → mostly open|filtered (inconclusive).
- Likely only **DNS (53/UDP)** is accessible through authoritative name servers.

OS Detection:

- Inconclusive – likely Google Cloud / load-balanced infrastructure masking OS details.

Traceroute:

- 7–11 hops through Google/Cloud CDN network.

- Final hop terminates inside Google Cloud (likely load balancer before web cluster).

Conclusion

- Host is live and actively serving HTTPS traffic.
- Strong firewalling/CDN protections → all non-web ports blocked.
- Public-facing services are limited to HTTPS (443), ensuring minimal attack surface.
- Likely protected by WAF (Web Application Firewall) and cloud security rules.