Task 1

I chose https://tryhackme.com/ which is CyberSecurity training website.

1. Server: 127.0.0.53
   Address: 127.0.0.53#53
2. tryhackme.com mail exchanger = 10 alt4.aspmx.l.google.com.
3. Whois Output: Admin details include information such as the admin's name, email, phone number, and physical address.

-Exploitation possibilities:

-Email phishing: Malicious actors could use this information for targeted phishing.

-Social engineering: Attackers could exploit personal details to impersonate the admin or trick them into divulging sensitive information.

4. Admin information is stored in the Whois database, maintained by the domain registrar. Depending on privacy settings, some or all of this information might be publicly visible.

5.

Common Name (CN)
tryhackme.com
Organization (O)
Cloudflare, Inc.
Organizational Unit (OU)
<Not Part Of Certificate>

Issued By

Common Name (CN)
Cloudflare Inc ECC CA-3
Organization (O)
Cloudflare, Inc.

Organizational Unit (OU)
<Not Part Of Certificate>

Validity Period

Issued On
Friday, July 12, 2024 at 2:00:00 AM
Expires On
Wednesday, January 1, 2025 at 12:59:59 AM
So Yes, there are public key certificates stored for the domain **tryhackme.com**.
6. Subdomain enumeration helps identify different parts of a website, like `api.tryhackme.com` or `blog.tryhackme.com`, which may run on separate systems with different security measures. Even if the main site is secure, these subdomains could have vulnerabilities, like outdated software, admin panels, or poorly protected APIs. Hackers can target these weaker points to find ways into the network. Discovering and securing subdomains reduces potential attack surfaces and helps protect the main domain more effectively.

Task 2: Digital Footprint of TryHackMe

Using Pentest Tools, I performed a vulnerability scan on https://tryhackme.com and gathered the following data:

Risk Summary:

- Overall risk level: Medium
- High risks: 0
- Medium risks: 3
- Low risks: 7
- Info: 9

Key Findings:

1. Insecure cookie settings: Missing Secure flag and HttpOnly flag, along with loose domain configuration.
    - Cookies: `_csrf`, `connect.sid`, and `__cfruid` are not secured with the Secure or HttpOnly flags, which makes them vulnerable to interception or attacks like session hijacking.
2. Missing security headers:
    - Content-Security-Policy (CSP): Not set properly, leaving the application vulnerable to Cross-Site Scripting (XSS).
    - Referrer-Policy: Missing, potentially exposing sensitive URL information to third parties.
    - Strict-Transport-Security (HSTS): Missing, allowing potential man-in-the-middle attacks via unsecured connections.
    - X-Content-Type-Options: Missing, which could lead to attacks like Cross-Site Scripting (XSS) or phishing.
3. Website technologies: The site uses various technologies such as Express, Node.js, Cloudflare, Google Analytics, Bootstrap, and others, which could be targeted for specific exploits if vulnerabilities in these technologies are known.
4. HTTP OPTIONS enabled: This allows the discovery of HTTP methods the server supports, which might reveal potentially risky methods.
5. Robots.txt file: Found and may expose URLs that should not be indexed, although this is not a major security risk on its own.

Answers to Questions:

1. What data could be used for attack?
   - Cookies without Secure and HttpOnly flags could be intercepted and used for session hijacking.
   - Missing security headers (CSP, Referrer-Policy, HSTS, X-Content-Type-Options) make the site more vulnerable to attacks such as XSS, user tracking, and insecure communication.
   - Software and technologies: Information about server software (Express, Node.js) can be exploited if known vulnerabilities exist in those versions.

2. No direct email addresses were found in the scan, but emails exposed on other platforms could be used for phishing attacks. Attackers can impersonate the domain, tricking users into providing credentials or personal information.

3. JavaScript source paths could expose vulnerable client-side code that attackers can exploit through XSS or manipulated API calls. Additionally, it might reveal sensitive data or poorly implemented security mechanisms.

4. Cookies like `_csrf` and `connect.sid` are missing Secure and HttpOnly flags, making them vulnerable to interception if the user's connection is not encrypted. Attackers could use this information for session hijacking or impersonation.

5. The lack of key security headers like CSP, HSTS, and Referrer-Policy indicates poor security configurations. These headers protect against attacks such as XSS, man-in-the-middle attacks, and information leakage. For example, without CSP, attackers could inject malicious JavaScript into the site.

Task 3 I used https://w3techs.com/sites/info/tryhackme.com tool because this tool is only available.

1. Identified Meta Data and Connected Websites

The meta data for TryHackMe includes the following details:

- Description: An online platform for learning cybersecurity through hands-on exercises.
- Popularity: Ranked in the top 100k websites globally.
- Technologies: Utilizes JavaScript (both server-side and client-side), jQuery, Popper, and various CSS frameworks like Animate. The server runs on Cloudflare and Node.js.
- Analytics: Uses Google Analytics, Hotjar, Amplitude, and HubSpot for traffic analysis.
- SSL Providers: SSL certificates are issued by DigiCert and IdenTrust.
- Content Delivery Networks (CDNs): Includes CDNJS and unpkg for JavaScript libraries.

2. Found IP Addresses

During the scan, specific IP addresses associated with the TryHackMe site weren't explicitly listed. However, the site operates through Cloudflare, which typically involves multiple IP addresses due to its CDN nature.

3. Mapping Out Network Infrastructure

Identifying IP addresses can be crucial for mapping an organization’s network infrastructure. They provide insight into:

- Server Locations: Understanding where the servers are hosted can highlight potential points of attack.

- Network Segmentation: Knowing the IPs helps in recognizing how different parts of the network are segmented or connected, which is valuable for planning an attack or a security assessment.
- Potential Weaknesses: Discovering exposed IP addresses can reveal entry points into the network.

4. Expanding the Attack Surface

Connected websites like those utilizing the same Google Analytics or Cloudflare services can broaden the attack surface. For instance:

- Third-party Services: Services such as Google Ads and Hotjar could be potential vectors for phishing or other attacks if they are not securely configured.
- Shared Technologies: Websites running on similar stacks may have common vulnerabilities that could be exploited.

5. Implications of Identifying Technology Stack

Identifying the specific technology stack of a site like TryHackMe is vital for vulnerability assessment and remediation:

- Targeted Vulnerabilities: Certain frameworks or libraries may have known vulnerabilities, allowing for a focused assessment.
- Remediation Strategies: Understanding the tech stack helps in devising appropriate patches or mitigation strategies based on the technologies in use.
- Security Posture: The combination of technologies can influence the overall security posture, highlighting areas that require more stringent controls or updates.

Task 4

I tried to scan every OSIT, but I couldn’t find anything.

1. I checked the NVD and CVE databases using the names of the technologies TryHackMe uses. I thought I’d find something, but it looks like there weren’t any reported vulnerabilities for them at the moment. I also looked around online, but it seems like TryHackMe is pretty secure right now.

2. If I had found some vulnerabilities, I would have used the Common Vulnerability Scoring System (CVSS) to figure out how serious they are. This system looks at how easy it is to exploit a vulnerability and what kind of damage it could cause. I’d also think about what the application does and how the vulnerabilities might affect its security.

3. To keep up with new vulnerabilities, I’d set up alerts on the NVD and CVE websites for the technologies I’m interested in. I’d also consider using automated tools that scan for new vulnerabilities regularly. Plus, being active in cybersecurity communities can help me hear about any new threats before they become widely known.

Even though I didn’t find any vulnerabilities for TryHackMe, these steps can help me stay prepared and informed about any security issues that might come up in the future. It’s all about staying proactive in this ever-changing field!