Group 5

Executive Summary of a Network and Information Security Management (NISM) Assessment Project.

Introduction

This reports looks at the penetration testing methodology and tools that were used on an e-health website named http://www.teamnebula.us-east-1.elasticbeanstalk.com with IP address as 107.20.143.245, Secondly, it evaluates the website against General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA) security standards. Last but not least, it covers the results of the test and concludes with detailed recommendations.

Methodology and Tools used for the Penetration Testing

The course tutor of Network and Information Security Management Module established several groups from all students attending his module paired them. Our group was name group 5 which was paired with group 6. The tutor instructed the each group to design a website and exchange it's web and IP address with their opponents for the pen-tests. Group 5 designed an ecommerce website and submitted the web link and IP address to group 6 for the pen-test while Group 6 submitted an e-health website named http://www.teamnebula.us-east-1.elasticbeanstalk.com with IP address as 107.20.143.245 to group 5. Gray Box Penetration testing approach was adopted to allow participants to scout the website, detect existing weaknesses and later penetrate the system. A seven phase methodology was then adopted which according Alpine Security (2021) has the following stages:

1. Planning on how we would conduct the pen test
2. Initial reconnaissance and discovery which was carried out in the first assignment
3. Vulnerability Examination
4. Initial Exploitation
5. Deeper Penetration
6. Clean up
7. Report Generation

All participants were then tasked to perform a pen test on the target website to guarantee better output during the compilation of the results. They narrowed down and scrutinize the following fundamental areas as explained by Pentest People Ltd (2021) during the test:

1. Publicly obtainable data like DNS records, email addresses and site information,
2. Vulnerabilities within web pages.
3. The session management Vulnerabilities like session hijacking, unwarranted timeouts
4. User input vulnerabilities like Cross-Site Scripting (XSS) and SQL Injection.
5. Web server configuration vulnerabilities like version disclosure, obsolete software packages, SSL configuration weaknesses, and open ports

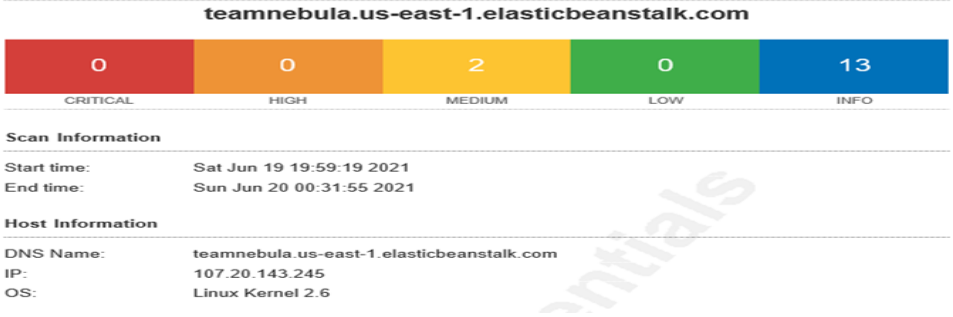
To get better output, members were allowed to use a diverse number of tools to gather information on existing weaknesses and their probable effect. The tools include:

1. The open-source intelligence (OSINT) framework and Shodan.io a free to use website that allows users to find open ports and other such vital information using the IP address of a website.
2. Nessus is a vulnerability scanning tool that was created by Tenable and compliant with CIS, HIPPA and more (Tenable, 2021).
3. The open web application security project (OWASP) designed by a community-led initiative named open source projects (OWASP, 2021).
4. Kali Linux
5. Nslookup, Tracert and Ping
6. Nmap, Whatcms.org, maxmind.com, Zoomeye and Zap scanning

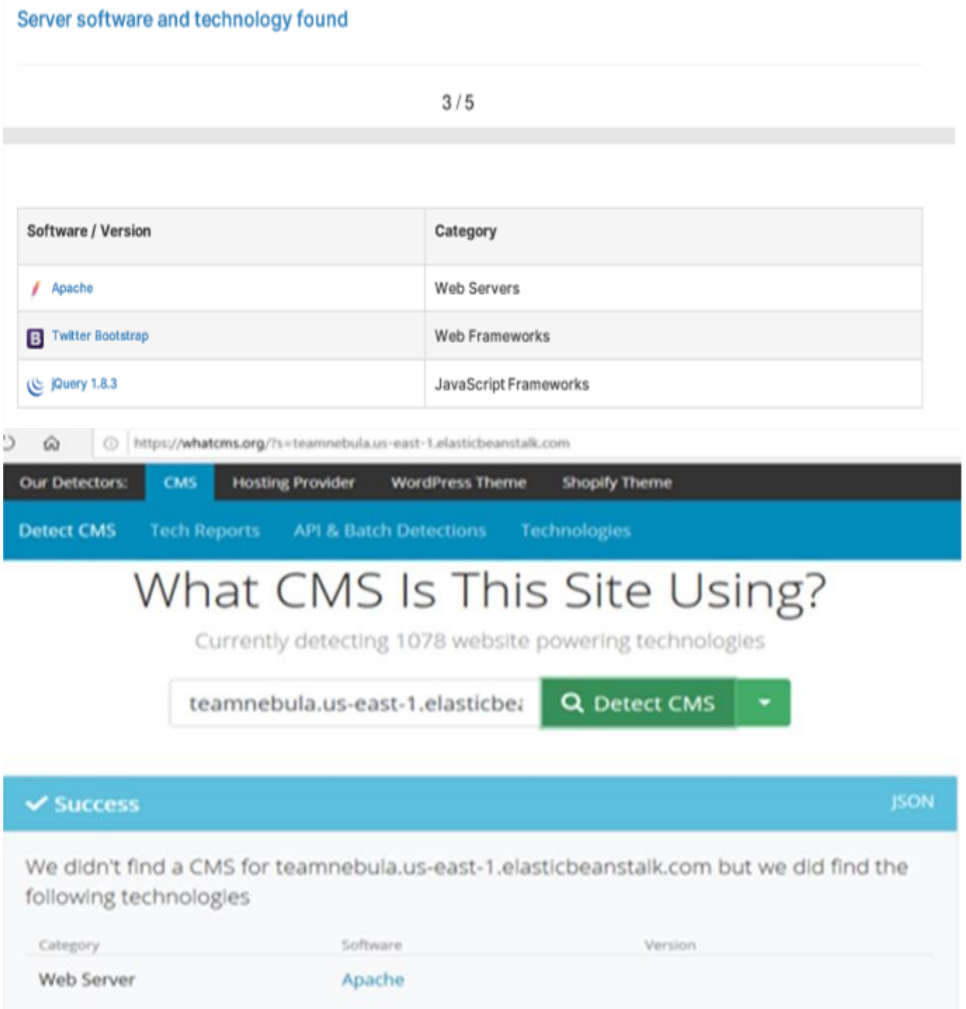
Summary of the Penetration Testing Results

During the pen test, results were produced and the following questions answered:

1. Operating System does the website utilize?

Answer	**Linux Kernel 2.6**
Tools	Nmap, Nessus Essentials
Scan Output	 teamnebula.us-east-1.elasticbeanstalk.com 0 CRITICAL, 0 HIGH, 2 MEDIUM, 0 LOW, 13 INFO Scan Information Start time: Sat Jun 19 19:59:19 2021 End time: Sun Jun 20 00:31:55 2021 Host Information DNS Name: teamnebula.us-east-1.elasticbeanstalk.com IP: 107.20.143.245 OS: Linux Kernel 2.6 Pen-test Scanned and adopted from Nessus Essentials and Nmap

2. What web server software is it running?

Answer	**Apache**
Tools	Pentest-Tools, Whatcms.org
Scan Output	 Pen-test Scanned and adopted from Whatcms.org and Pentest-tools.com

3. Is it running a Content Management Systems (CMS) (WordPress, Drupal, etc)?

Answer	**Ruby on Rails, Next.js, WordPress**
Tools	Whatcms.org
Scan Output	 Pen-test Scanned and adopted from whatcms.org

4. What protection does it have (CDN, Proxy, Firewall?)

Answer	**CDN exists because the content is cached on one AWS server. TCP traceroute revealed AWS proxies.**
Tools	Nmap
Scan Output	**Starting Nmap 7.70 (https://nmap.org) at 2021-06-22 21:15 UTC** **Nmap scan report for ec2-107-20-143-245.compute-1.amazonaws.com (107.20.143.245)** **Host is up (0.0075s latency).** **Nmap done: 1 IP address (1 host up) scanned in 1.33 seconds** Pen-test Scanned and adopted from https://Nmap.org

5. Where is it hosted?

Answer	**teamnebula.us-east-1.elasticbeanstalk.com,** **ec2-107-20-143-245.compute-1.amazonaws.com (PTR)** **Amazon AWS**
Tools	https://who.is/, Maxmind.com
Scan Output	Amazon.com, Inc. AMAZO-4 Address: Amazon Web Services, Inc. P.O. Box 81226 City: Seattle StateProv: WA PostalCode: 98108-1226 Country: US Pen-test Scanned and adopted from https://Who.is/ and https://Maxmind.com

6. Does it have any open ports?

Answer	**Yes, Open TCP Port: 22 (1 occurrence), Open TCP Port: 80 (1 occurrence)**
Tools	Nmap, Shodan
Scan Output	**107.20.143.245 / ec2-107-20-143-245.compute-1.amazonaws.com 1.elasticbeanstalk.com** **Address** - 107.20.143.245 (ipv4) **Hostnames** - teamnebula.us-east-1.elasticbeanstalk.com (user) - ec2-107-20-143-245.compute-1.amazonaws.com (PTR) **Ports** The 65353 ports scanned but not shown below are in state: **filtered** - 65353 ports replied with: **no-responses** The 1 ports scanned but not shown below are in state: **closed** - 1 ports replied with: **conn-refused** Port | State (toggle closed [0] | filtered [0]) | Service | Reason | Product 22 tcp open ssh syn-ack 80 tcp open http syn-ack Shodan Open ports – 80/TCP Other ports – 80, 443, 5000 Web technologies – Bootstrap, Jquery Pen-test Scanned and adopted https://www.Shodan.io/ and https://Nmap.org

7. Does the site have any known vulnerabilities? **Yes**

Answer	1. Communication is made over insecure unencrypted HTTP 2. Response headers do not include: a. HTTP Content-Security-Policy security header b. HTTP X-Frame-Options security header c. HTTP X-XSS-Protection security header d. X-Content-Type-Options HTTP security header e. Referrer-Policy HTTP security header 3. No Anti-CSRF tokens were found in an HTML submission form SSH Weak Encryption Algorithms Supported (1 occurrence) 4. MacOS X Finder '.DS_Store' Information Disclosure (1 occurrence)
Tools	Pentest-Tools, Zoomeye
Scan Output	Communication is not secure URL: http://teamnebula.us-east-1.elasticbeanstalk.com/ Evidence: Communication is made over unsecure, unencrypted HTTP. Details **Risk description:** The communication between the web browser and the server is done using the HTTP protocol, which transmits data unencrypted over the network. Thus, an attacker who manages to intercept the communication at the network level, is able to read and modify the data transmitted (including passwords, secret tokens, credit card information and other sensitive data). **Recommendation:** We recommend you to reconfigure the web server to use HTTPS - which encrypts the communication between the web browser and the 97900 2019-04-10 高危 CVE-2019-0211 Apache Root Privilege Escalation 97633 2018-10-30 高危 ACME Mini_httpd组件任意文件读取漏洞(CVE-2018-18778) 96556 2017-09-20 高危 Apps industrial OT over Server: Anti-Web Local File Incl... 96555 2017-09-20 高危 Apps industrial OT over Server: Anti-Web Remote Command ... 92134 2016-07-19 中危 httpoxy远程代理感染漏洞 Pen-test Scanned and adopted from Pentest-tools.com and Zoomeye

8. What versions of software is it using?

Answer	**Apache webserver, Twitter Bootstrap Web Frame orks and jQuery 1.8.3 JavaScript Frameworks**
Tools	Pentest-Tools
Scan Output	Server software and technology found 3 / 5 Software / Version: Apache — Category: Web Servers Twitter Bootstrap — Web Frameworks jQuery 1.8.3 — JavaScript Frameworks Pen-test Scanned and adopted from Pentest-tools.com

9. Are these patched so that they are up to date? **NO**

Answer	**NO**
Tools	Zap Scanning
Scan Output	**Alert Detail**

Medium (Medium)	Vulnerable JS Library
Description	The identified library jquery, version 1.8.3 is vulnerable.
URL	http://ajax.googleapis.com/ajax/libs/jquery/1.8.3/jquery.min.js
Method	GET
Evidence	/1.8.3/jquery.min.js
Instances	1
Solution	Please upgrade to the latest version of jquery.

Pen-test Scanned and adopted from Pentest-tools.com

Evaluation of the website against two security standards – one of which must be the GDPR directive

On the one hand firstly, the pen test results for the target website was that communication is made over insecure unencrypted HTTP. According Tripwire (2021) encryption is an effective method for accomplishing GDPR compliance. But, GDPR encryption requirements are not compulsory. GDPR data encoding can be advantageous for enterprises because it averts data breaches and prevents them from paying hefty fines that are more than the cost of implementing encryption technologies. Additionally Marc (2021) suggests that to ensure GDPR compliance SSL certificate acts like an electronic "passport" that creates person's identifications when conducting business on the Web. Whenever a web user attempts to transmit confidential data to Web servers, the browser access the server's digital certificate and creates a secure link.

Secondly, the GDPR requires that data of subjects be processed lawfully. Lawful processing under the GDPR means that the data subject in question have given consent for the processing of their personal data. Consent gained from data subjects should be explicit, for instance under the GDPR subscriptions must be set on default to "no" or be blank and unsubscribing should be easy and straightforward. A key GDPR element is transparency as the data subject should be informed of the reason for processing their data, the data retention period and whether their personal data will be shared with a third party. (GDPR, 2018). Marc (2021) explains that it is a GDPR regulation for website to contain a page where users can demand a copy of their data, or the deletion of it because GDPR is about protecting subjects from the diverse security threats and malicious actors within the cyberspace. The investigations showed that the target website was not having such a page hence it is not GDPR compliant.

Last but not least, the pen test showed that the target website was using wordpress as website engine and CMS. Marc (2021) regrets that web engines like WordPress are not GDPR compliant and could lead to data breaches if the weaknesses in wordpress were exploited by hackers. Marc (2021) adds that WordPress can only be made GDPR compliant by deploying current updates solutions that help compliance. Solutions Review & Doug (2021) suggest that organizations should deploy enterprise

content management (ECM) applications that takes advantage of metadata to impose the security and governance required to safeguard client data.

On the other hand, the HIPAA regulation is in agreement with the GDPR regulation because firstly, the HIPAA Guide (2021) suggests that for a website to be HIPAA Compliant, it should secured using SSL certificate to guarantee that connection between the browser and the website is encrypted, so that user input on web forms is protected against unauthorized access. The target website was found not to be compliant.

Secondly, the HIPAA Guide (2021) suggests companies must guarantee that any information stored or transmitted on a health web server must be encrypted. The target website did not meet the requirement at the same time despite being an e-health website that stores sensitive data.

Thirdly, HIPAA Guide (2021) suggests that the HIPAA Security Rule should be enforced to ensure confidentiality, integrity, and availability of protected health care data, hence data must be backed up to ensure easy recovery and business continuity in case of a breach or disaster.

HIPAA Guide (2021) suggests access controls must be built in the website to ensure that only authorized individuals are able to access the website. This was not the done in the target website because there were no passwords or administrative privileges to stop anyone from data access.

Last but not least, the purpose of the HIPAA act is to ensure that the health information of subjects is safeguarded and is made available to subjects when needed to promote high-quality health care. As the website that was tested serves a health purpose, HIPAA could therefore be applicable. Although the website that was tested is a basic website with little to no personal data that needs protection, it is important to ensure that penetration tests are carried out regularly on a network to prevent security attacks such as Denial of Service attacks etc.

Conclusions

In conclusion, after the pen test, the team found that there are various security threats that need to be mitigated in the following in descending order, based on risk:

1. Linux Kernel

The Nessus essentials test detected Linux Kernel 2.6. This is a weakness that can be exploited by hackers to carry out a remote unauthenticated denial-of-service (DoS) attack. There are a total of 3 security holes identified as CVE-2019-11477, CVE-2019-5599 and CVE-2019-11479. The only solution to solve the issue is doing the kernel updates. It is impossible to patch the current kernel for mitigations. (Eduard, 2019).

2. Unencrypted opening ports:

The results of the pen test indicated that ports 21 and 80 are open. 80 is a non-SSL HTTP port, which means there is no encryption between the client and server when communicating through this port. Unencrypted open ports can be vulnerable, from malware or DoS(Acunetix, 2014).

3. **Too many unused CMS systems:**

Last but not least, the results indicated that there are several CMS systems running on the webserver that might expose the system to cyber-attack like SQL injections and database attacks. One of CMS systems detected by the pentest was WordPress. Human error on such occasions will be the most likely cause of the threat. (FutureEnTech, 2020).

Recommendations

When analyzing the Nebula team's E-health website, there are several recommendations concerning the security flaws detected:

1. The first recommendation would be to encrypt the traffic to the website. Use SSL and port 443 can prevent any unencrypted data passing through.(Cybersecurity education guides, N.d).

2. To prevent SQL injection to poison the E-health website database, the system should be protected using solutions like Privileged Access Management, Penetration Testing, Security Information and Event Management, Next – Generation Firewall, Network Access Control and Intrusion Detection and prevention.

3. As shown in the Zap scanning tool, the JS version is not up to date, it is essential to update the JS library which can avoid any potential vulnerability in the javascript code.

4. The version of the OS is not the latest, it is recommended to update the version of the OS because the updates allow correcting the security flaws detected in an operating system. (Appcheck, 2020).

5. Regular backups are needed to provide business continuity should there be a ransomware attack.

6. Port 20 and 80 should be blocked as there is no encryption. Unnecessary open port should be avoid from any potential attack.

7. The website must be designed to be compliant with both the GDPR and HIPAA standards.

REFRENCES

1. Acunetix (2014) Danger: Open Ports – Trojan is as Trojan does, Available at: https://www.acunetix.com/blog/articles/danger-open-ports-trojan-trojan/ (Accessed: 6th July 2021).

2. Alpine Security (2021) Gray Box Penetration Testing and methodology Available at:

   https://alpinesecurity.com/services/penetration-testing/gray-box-penetration-testing/ [Accessed 10 July 2021].

3. Appcheck (2020) Common e-commerce vulnerabilities and how to remedy. Available at: https://appcheck-ng.com/common-ecommerce-vulnerabilities/# [Accessed 10 July 2021].

4. Cybersecurity education guides, (N.D) Cybersecurity in e-Commerce: Safeguarding Credit Card Numbers and Personal Data on Millions of Customers. Available at: https://www.cybersecurityeducationguides.org/ecommerce/ [Accessed 10 July 2021].

5. Eduard, K (2019) Serious Vulnerabilities in Linux Kernel Allow Remote DoS Attacks, Available at: https://www.securityweek.com/serious-vulnerabilities-linux-kernel-allow-remote-dos-attacks [Accessed: 6th July 2021].

6. FutureEnTech (2020) 9 Default Security Threats in WordPress and How to Fix Them, Available at: https://futureentech.com/9-default-security-threats-wordpress-fix/# [Accessed: 6th July 2021].

7. Intersoft Consulting (2021) Article 6: Lawfulness of Processing Available from https://gdpr-info.eu/ [Accessed 10th July 2021]

8. Marc, M.(2021)What is GDPR and how can I make my website compliant? Available at: https://upfront.ie/irish-business/what-is-gdpr-and-how-can-i-make-my-website-compliant/ [Accessed 7th June 2021].

9. OWASP Foundation | Open Source Foundation for Application Security. (2021) Available at: https://owasp.org/. [Accessed 11 July 2021].

10. Solid State (N.D) How to Protect Against Ransomware: 7 Ways to Stop the Worst Cyberthreat. Available at: http://solidsystemsllc.com/protect-against-ransomware/ [Accessed 10th July 2021].

11. Pentest-tools.com (2021) Website Vulnerability Scanner Available from: https://pentest-tools.com/website-vulnerability-scanning/website-scanner [Accessed 7th June 2021].

12. Pentest People Ltd(2021) Web Application Penetration Testing Available at: https://www.pentestpeople.com/web-application-penetration-testing/ [Accessed 11 July 2021].

13. Solutions Review & Doug, A. (2021) How Enterprise Content Management Can Help With GDPR Available at: https://solutionsreview.com/content-management/enterprise-content-management-can-help-gdpr/ [Accessed 7th June 2021].

14. The HIPAA Guide(2021) Requirements for a HIPAA Compliant Website Available at: https://www.hipaaguide.net/hipaa-compliant-website/ [Accessed 7th June 2021].

15. Try Nessus Pro free | Tenable (2021). Try Nessus Pro free | Tenable.

    [ONLINE] Available at: [Accessed 11 July 2021].

16. Tripwire (2021) Role of Encryption in GDPR Compliance Available at: https://www.tripwire.com/state-of-security/security-data-protection/role-of-encryption-in-gdpr-compliance/
    [Accessed 7th June 2021].

17. www.shodan.io (2021) Open ports Available at: https://www.shodan.io/search?query=amazon [Accessed 7th June 2021].

18. Whatcms.org(2021) What CMS Is This Site Using? Available at: https://whatcms.org/ [Accessed 7th June 2021].