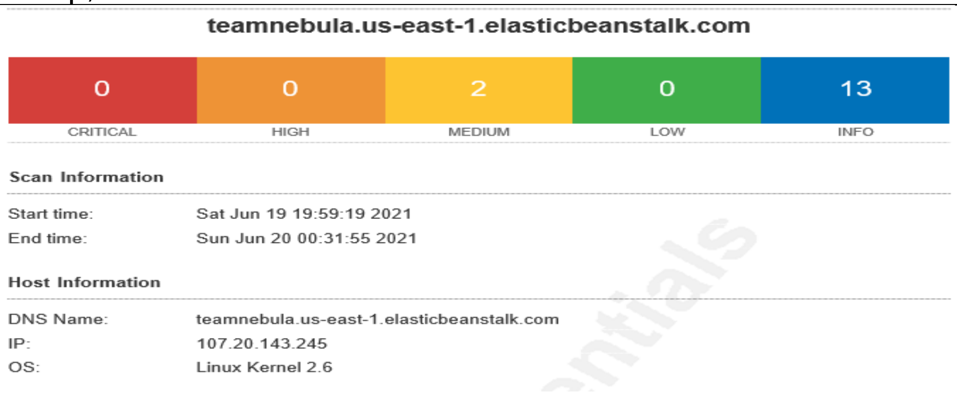
Part 1: An Executive Summary of a Network and Information Security Management (NISM) Assessment Project.

a. A brief summary of the work carried out

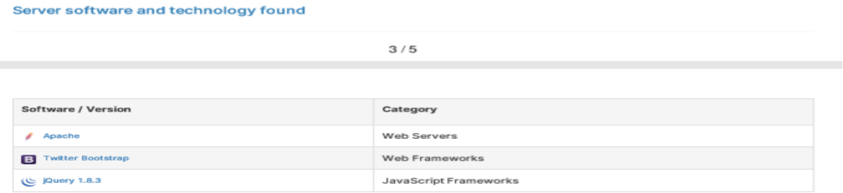
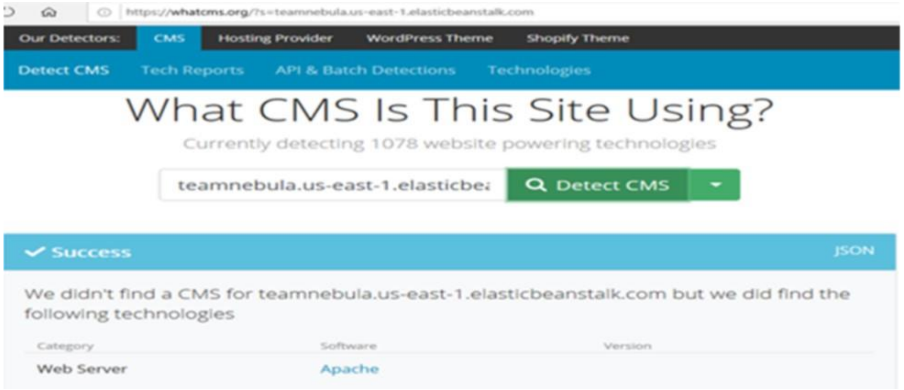
b. **Summary findings – presented in an easy to understand, non-technical manner (supported by graphics and charts as appropriate). David**

Group 5 was assigned an e-commerce website named http://www.teamnebula.us-east-1.elasticbeanstalk.com with 107.20.143.245 as the IP address to perform scans against it using the tools available in Kali Linux . The team also used other available tools to complement those available in Kali Linux in order to gather as much information from the site. Several questions were then answered that include:

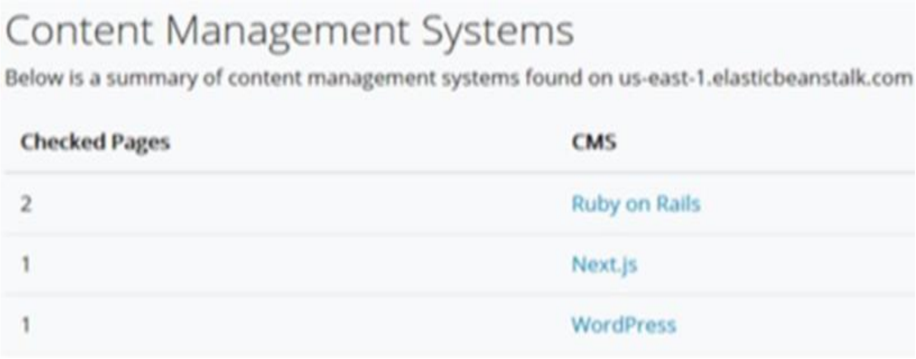
1. Operating System does the web site utilize?

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

2. What web server software is it running?

Answer	**Apache**
Tools	Pentest-Tools, whatcms.org
Scan Output	 Server software and technology found 3 / 5 Software / Version — Category Apache — Web Servers Twitter Bootstrap — Web Frameworks jQuery 1.8.3 — JavaScript Frameworks  https://whatcms.org/?s=teamnebula.us-east-1.elasticbeanstalk.com Our Detectors: CMS Hosting Provider WordPress Theme Shopify Theme Detect CMS Tech Reports API & Batch Detections Technologies What CMS Is This Site Using? Currently detecting 1078 website powering technologies teamnebula.us-east-1.elasticbe ✓ Success JSON We didn't find a CMS for teamnebula.us-east-1.elasticbeanstalk.com but we did find the following technologies Category — Software — Version Web Server — Apache

3. Is it running a CMS (Wordpress, Drupal, etc)?

Answer	**Ruby on Rails, Next.js, WordPress**
Tools	whatcms.org
Scan Output	 Content Management Systems Below is a summary of content management systems found on us-east-1.elasticbeanstalk.com Checked Pages — CMS 2 — Ruby on Rails 1 — Next.js 1 — WordPress

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

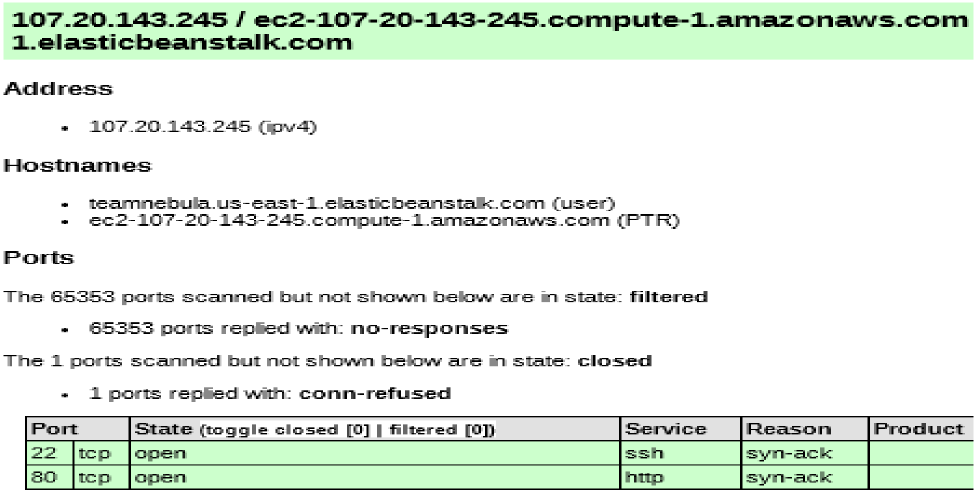
Answer	**CDN exists because the content is cached on one AWS server. TCP traceroute revealed AWS proxies.**
Tools	nmap

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).`
	
	`PORT     STATE    SERVICE`
	`21/tcp   filtered ftp`
	`22/tcp   open     ssh`
	`23/tcp   filtered telnet`
	`80/tcp   open     http`
	`110/tcp  filtered pop3`
	`143/tcp  filtered imap`
	`443/tcp  closed   https`
	`3389/tcp filtered ms-wbt-server`
	`Nmap done: 1 IP address (1 host up) scanned in 1.33 seconds`

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	Dig, https://who.is/
Scan Output	OrgName: Amazon.com, Inc. OrgId: AMAZO-4 Address: Amazon Web Services, Inc. Address: P.O. Box 81226 City: Seattle StateProv: WA PostalCode: 98108-1226 Country: US

6. Does it have any open ports?

<table>
<tr><td><b>Answer</b></td><td><b>Yes, Open TCP Port: 22 (1 occurrence), Open TCP Port: 80 (1 occurrence)</b></td></tr>
<tr><td>Tools</td><td>Nmap</td></tr>
<tr><td>Scan Output</td><td>


<b>107.20.143.245 / ec2-107-20-143-245.compute-1.amazonaws.com 1.elasticbeanstalk.com</b>

<b>Address</b>

- 107.20.143.245 (ipv4)

<b>Hostnames</b>

- teamnebula.us-east-1.elasticbeanstalk.com (user)
- ec2-107-20-143-245.compute-1.amazonaws.com (PTR)

<b>Ports</b>

The 65353 ports scanned but not shown below are in state: <b>filtered</b>

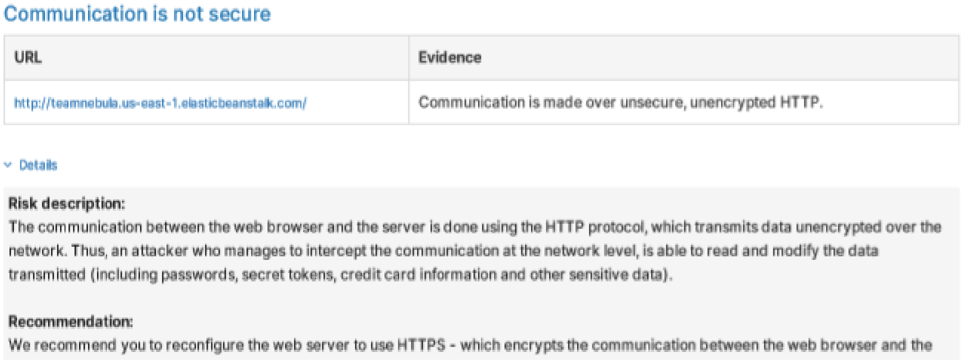
- 65353 ports replied with: <b>no-responses</b>

The 1 ports scanned but not shown below are in state: <b>closed</b>

- 1 ports replied with: <b>conn-refused</b>

<table>
<tr><th colspan="2">Port</th><th>State (toggle closed [0] | filtered [0])</th><th>Service</th><th>Reason</th><th>Product</th></tr>
<tr><td>22</td><td>tcp</td><td>open</td><td>ssh</td><td>syn-ack</td><td></td></tr>
<tr><td>80</td><td>tcp</td><td>open</td><td>http</td><td>syn-ack</td><td></td></tr>
</table>
</td></tr>
</table>

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

<table>
<tr><td><b>Answer</b></td><td>
1. Communication is made over unsecure 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 a HTML submission form SSH Weak Encryption Algorithms Supported (1 occurence)
4. MacOS X Finder '.DS_Store' Information Disclosure (1 occurence)
</td></tr>
<tr><td>Tools</td><td>Pentest-Tools</td></tr>
<tr><td>Scan Output</td><td>


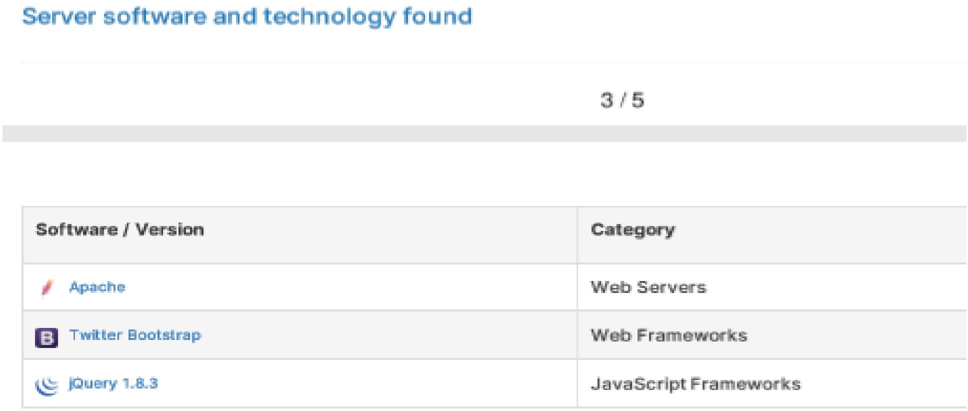
Communication is not secure

<table>
<tr><th>URL</th><th>Evidence</th></tr>
<tr><td>http://teamnebula.us-east-1.elasticbeanstalk.com/</td><td>Communication is made over unsecure, unencrypted HTTP.</td></tr>
</table>

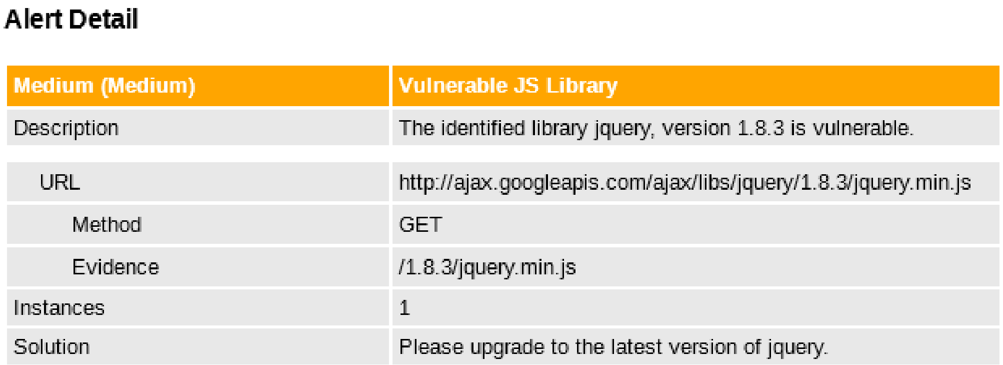
<b>Risk description:</b>
The communication between the web browser and the server is done using the HTTP protocol, which transmits data unencrypted over the network. Thus, an attacker who manages to intercept the communication at the network level, is able to read and modify the data transmitted (including passwords, secret tokens, credit card information and other sensitive data).

<b>Recommendation:</b>
We recommend you to reconfigure the web server to use HTTPS - which encrypts the communication between the web browser and the
</td></tr>
</table>

8. What versions of software is it using?

<table>
<tr><td><b>Answer</b></td><td><b>Apache webserver, Twitter Bootstrap Web Frameworks and jQuery 1.8.3 JavaScript Frameworks</b></td></tr>
<tr><td>Tools</td><td>Pentest-Tools</td></tr>
<tr><td>Scan Output</td><td>
Server software and technology found
3 / 5
<table>
<tr><th>Software / Version</th><th>Category</th></tr>
<tr><td>Apache</td><td>Web Servers</td></tr>
<tr><td>B Twitter Bootstrap</td><td>Web Frameworks</td></tr>
<tr><td>jQuery 1.8.3</td><td>JavaScript Frameworks</td></tr>
</table></td></tr>
</table>

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

<table>
<tr><td><b>Answer</b></td><td><b>NO</b></td></tr>
<tr><td>Tools</td><td>Zap Scanning</td></tr>
<tr><td>Scan Output</td><td>
Alert Detail
<table>
<tr><th>Medium (Medium)</th><th>Vulnerable JS Library</th></tr>
<tr><td>Description</td><td>The identified library jquery, version 1.8.3 is vulnerable.</td></tr>
<tr><td>URL</td><td>http://ajax.googleapis.com/ajax/libs/jquery/1.8.3/jquery.min.js</td></tr>
<tr><td>Method</td><td>GET</td></tr>
<tr><td>Evidence</td><td>/1.8.3/jquery.min.js</td></tr>
<tr><td>Instances</td><td>1</td></tr>
<tr><td>Solution</td><td>Please upgrade to the latest version of jquery.</td></tr>
</table></td></tr>
</table>

c. A section that evaluates the website against two security standards – one of which must be the GDPR directive.

d. Conclusions – with justifications.

After the pen test, there are various security threats and need to mitigate.

In the Nessus essentials test, although there are only 2 medium threats, but it can detect the Linux Kernel 2.6.

Linux Kernel 2.6 has been identified a serious vulnerability, which can be exploited by an attacker to launch a remote, unauthenticated denial-of-service (DoS) attack.

There are total of 3 security holes, the one which impact the most is called “dubbed SACK Panic”, with identifier CVE-2019-11477, Linux Kernel starting from 2.6.29 is affected.

The other 2 security holes related to the same issue are 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. For example, disable the whole SACK process or block the connections with a low MSS (Eduard, 2019).

We also found that there are too many CMS systems running on the web server, which may cause potential security threat. Exposure of the use of CMS systems will cause different kinds of cyber-attack. The most common is SQL injections and database attacks, which the hacker aims to the security holes of every system.

Many CMS systems are public with multi admins, such as WordPress, which is also detected in the pen test. Human error in such occasion will be the most likely cause of the threat. For example, hackers can see the details of one of the admins, when he/she has left from the seat but without logging out, which may cause unwanted security threats (FutureEnTech, 2020).

In the pen test, we also found that both port 21 and 80 is opened. 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 port can be vulunarable. For example, malware can be spread through open port, which is also called Trojan port; services and applications will be exploited as it is not encrypted; configuration of services maybe captured by hackers; and easy to be attacked by DoS which will crash the server and cause unlimited downtime (Acunetix, 2014)

e. Recommendations – with justifications, ordered by business priority.

REFRENCES

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

Whatcms.org(2021) What CMS Is This Site Using?
Available from:
https://whatcms.org/

[Accessed on 7 June 2021].

Section D - Conclusion:
1: 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).

2:FutureEnTech (2020) 9 Default Security Threats in WordPress and How to Fix Them, Available at: https://futureentech.com/9-default-security-threats-wordpress-fix/#:~:text=%209%20Default%20Security%20Threats%20in%20WordPress%20and,and%20it%20works%20by%20creating%20a...%20More%20 (Accessed: 6th July 2021).

3: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).