

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

Project.

- A brief summary of the work carried out
- 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:

- Operating System does the web site utilize?

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

2. What web server software is it running?

Answer	Apache														
Tools	Pentest-Tools, whatcms.org														
Scan Output	<div>Server software and technology found</div> <div>3 / 5</div> <table><thead><tr><th>Software / Version</th><th>Category</th></tr></thead><tbody><tr><td>Apache</td><td>Web Servers</td></tr><tr><td>Twitter Bootstrap</td><td>Web Frameworks</td></tr><tr><td>jQuery 1.8.3</td><td>JavaScript Frameworks</td></tr></tbody></table> <div>https://whatcms.org/?i=teamnebula.us-east-1.elasticbeanstalk.com</div> <div>Our Detectors: CMS Hosting Provider WordPress Theme Shopify Theme</div> <div>Detect CMS Tech Reports API & Batch Detections Technologies</div> <h1>What CMS Is This Site Using?</h1> <p>Currently detecting 1078 website powering technologies</p> <div>teamnebula.us-east-1.elasticbe: Q Detect CMS</div> <div><div>✓ Success</div><div>JSON</div></div> <div>We didn't find a CMS for teamnebula.us-east-1.elasticbeanstalk.com but we did find the following technologies</div> <table><thead><tr><th>Category</th><th>Software</th><th>Version</th></tr></thead><tbody><tr><td>Web Server</td><td>Apache</td><td></td></tr></tbody></table>	Software / Version	Category	Apache	Web Servers	Twitter Bootstrap	Web Frameworks	jQuery 1.8.3	JavaScript Frameworks	Category	Software	Version	Web Server	Apache	
Software / Version	Category														
Apache	Web Servers														
Twitter Bootstrap	Web Frameworks														
jQuery 1.8.3	JavaScript Frameworks														
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	<h2>Content Management Systems</h2>	
	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	<pre>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</pre>

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?










Answer	Yes, Open TCP Port: 22 (1 occurrence), Open TCP Port: 80 (1 occurrence)															
Tools	Nmap															
Scan Output	<div>107.20.143.245 / ec2-107-20-143-245.compute-1.amazonaws.com 1.elasticbeanstalk.com</div> <p>Address</p> <ul style="list-style-type: none">107.20.143.245 (ipv4) <p>Hostnames</p> <ul style="list-style-type: none">teamnebula.us-east-1.elasticbeanstalk.com (user)ec2-107-20-143-245.compute-1.amazonaws.com (PTR) <p>Ports</p> <p>The 65353 ports scanned but not shown below are in state: filtered</p> <ul style="list-style-type: none">65353 ports replied with: no-responses <p>The 1 ports scanned but not shown below are in state: closed</p> <ul style="list-style-type: none">1 ports replied with: conn-refused <table><tr><th>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 open</td><td>ssh</td><td>syn-ack</td><td></td></tr><tr><td>80</td><td>tcp open</td><td>http</td><td>syn-ack</td><td></td></tr></table>	Port	State (toggle closed [0] filtered [0])	Service	Reason	Product	22	tcp open	ssh	syn-ack		80	tcp open	http	syn-ack	
Port	State (toggle closed [0] filtered [0])	Service	Reason	Product												
22	tcp open	ssh	syn-ack													
80	tcp open	http	syn-ack													

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

Answer	<ol style="list-style-type: none"> Communication is made over unsecure Unencrypted HTTP Response headers do not include: <ol style="list-style-type: none"> HTTP Content-Security-Policy security header HTTP X-Frame-Options security header HTTP X-XSS-Protection security header X-Content-Type-Options HTTP security header Referrer-Policy HTTP security header No Anti-CSRF tokens were found in a HTML submission form SSH Weak Encryption Algorithms Supported (1 occurrence) MacOS X Finder '.DS_Store' Information Disclosure (1 occurrence)
--------	--

Tools	Pentest-Tools				
Scan Output	<p>Communication is not secure</p> <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> <p>▼ Details</p> <p>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).</p> <p>Recommendation: We recommend you to reconfigure the web server to use HTTPS - which encrypts the communication between the web browser and the</p>	URL	Evidence	http://teamnebula.us-east-1.elasticbeanstalk.com/	Communication is made over unsecure, unencrypted HTTP.
URL	Evidence				
http://teamnebula.us-east-1.elasticbeanstalk.com/	Communication is made over unsecure, unencrypted HTTP.				

8. What versions of software is it using?

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

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

Answer	NO														
Tools	Zap Scanning														
Scan Output	<p>Alert Detail</p> <table> <tr> <td>Medium (Medium)</td><td>Vulnerable JS Library</td></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>	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.
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.														

- 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 vulnerable. 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.

REFERENCES

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,an d%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).

CZESKA'S PENTEST RESULTS BELOW (PLEASE REARRANGE HOW YOU SEE FIT)

OSINT FRAMEWORK

Maxmind.com

IP address – 54.243.142.38

Country code – US

Location – Ashburn, Virginia, US

Network – 54.243.128.0/19

Postal code – 20149

Approximate coordinates – 39,0481 / -77,4728

Accuracy radius – 1 KM

Metro code – 511

ISP/domain – Amazon

IP2Location

Address type – unicast

Usage type – DCH (data centre/web hosting/ transit)

Anonymous proxy – no

Last seen – 18 days ago

DB-IP.com

Weather code – USVA0027

Is crawler – no

Threat level – low

Infobyip

Decimal IP – 921931302

Binary IP – 00110110 11110011 10001110 00100110

Hex IP - 0x36f38e26

Ipaddress.my

Connection speed – Company/T1

Shodan

Open ports – 80/TCP

Other ports – 80, 443, 5000

Web technologies – Bootstrap , JQuery

Server – Apache

Cache-Control – no cache

Transfer-Encoding – chunked

<https://www.shodan.io/search?query=amazon>

Spyse

Ipv4 subnets – 362









Ipv6 subnets – 31

Domains – 29M

Related organisations – 2.1K

Security score – 100%

IPs with open ports **3.5M**

IP	Open Ports	OSH ^②	Security Score ^②
 52.71.155.94 - AS14618 - AMAZON-AES	1	1	 32
 52.0.253.61 - AS14618 - AMAZON-AES	1	1	 100
 52.201.227.201 - AS14618 - AMAZON-AES	1	1	 100
 52.87.190.93 - AS14618 - AMAZON-AES	1	1	 32

Zoomeye

Vulnerabilities – See below

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

IP void

IP blacklist status – possibly safe 0/115

Google dorking

site:amazon.co.uk filetype:pdf -

- <http://g-ec2.images-amazon.com/images/G/02/uk-family/amazon-family-night-guide.pdf>
- https://m.media-amazon.com/images/G/02/Legal/Amazon_ModernDaySlaveryStatement_2018.docx._CB1198675309_.pdf
- https://m.media-amazon.com/images/G/02/images/cancellationform_uk_new._CB1198675309_.pdf
- https://business.amazon.co.uk/content/dam/amzn-biz/global/images/blogs/documents/reports/Hackett_Report.pdf
-

shodan membership report

Hostnames	ec2-54-187-238-157.us-west-2.compute.amazonaws.com
-----------	---

Domains	AMAZONAWS.COM
---------	----------------------

Country	United States
---------	----------------------

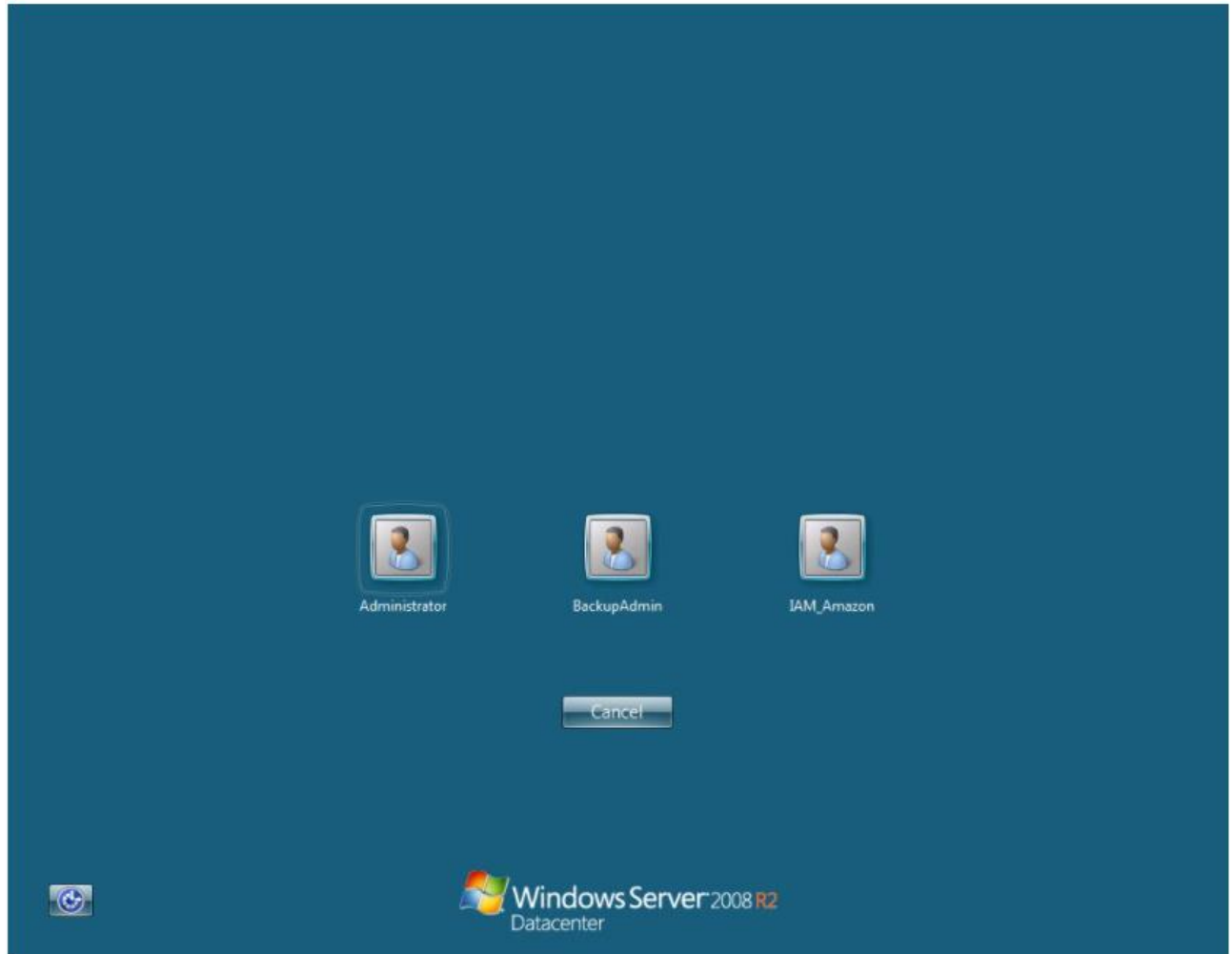
City	Boardman
------	-----------------

Organization	Amazon.com, Inc.
--------------	-------------------------

ISP	Amazon.com, Inc.
-----	-------------------------

ASN	AS16509
-----	----------------

OpenPorts
80, 3389, 1433

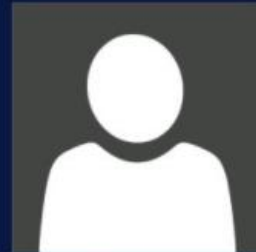




Administrator



Amazon Windows Update



AZIUSR_NB

Windows Update
Important updates are available. Go to PC settings to
install them.



Windows Server 2012 R2