Network and Information Security Management Assessment for e-commerce website

Anagnostopoulos Spiros, Chawla Vaibhav, Kosmaczewski Lukasz, Martinez Diez Raquel

Introduction

In 2020, 18% of all retail sales worldwide were done through e-commerce websites. This figure is expected to reach 21.8% in 2024 (Statista, 2021). E-commerce websites collect, store and process data that could potentially identify an individual. These websites serve as ideal targets for cyber-attacks to gain unwarranted access to large scale repositories containing sensitive information like user details, subscription plans, payment plans or even credit/debit card details. These details are more than enough to expose an average cyber-unaware consumer to various attacks in the future.

The earlier submitted proposal gave a glimpse of the employed approach for conducting reconnaissance at various levels. In this report, we assess our observations to do risk assessment along with threat modelling. Threat modelling serves as a vital aspect of security auditing. It helps evaluate the security vulnerabilities through systematic inspection of system design and implementing the security standards (Jiang L. et al., 2010).

We carry out risk assessment while considering the adherence to the prevalent security standards using STRIDE threat modelling framework (*Figure 1*). STRIDE has proven to be one of the most reliable and widely accepted models to study the risks by bifurcating them into six broad categories that any network-based application might encounter (Lipner S. & Howard M., 2004).

	Title	Description
S	Spoofing	Spoofing can be broadly described as the ability of any malicious user to identity in the form of a user, system, person, or token. (Hussain S. et al., 2011)
T	Tampering	Any unauthorised activity that constitutes manipulation of data, logs, files or even metadata such as timestamps can be referred to as tampering.
R	Repudiation	Repudiation is the act of dismissing an allegation after committing a malicious activity. The culprit questions the validity and authenticity of data to dodge the allegations.
I	Information disclosure	Unintended access of sensitive data to an audience is referred to as information disclosure. This might be due to data breach, poor design or even accidental.
D	Denial of Service	Malicious attacks that target disrupting services for legitimate users carried out either manually or automatically is referred to as Denial of Service.
E	Elevation of privilege	Gaining illicit access to administrator or root-level privileges, exploiting conditions that address role-based access control.

Figure 1: STRIDE description

One of the foreseeable limitations of STRIDE is its inability to scope in non-technical process focused use cases, which we cover in-depth by using GDPR and PCI-DSS.

The structured risk analysis as below helps in scoring and plotting the risks in a risk tolerance matrix. Distinct tolerance levels enable business continuity managers to gauge the urgency of the risks, based on business use-cases (*Figure 2 & 3*) and employ extra measures that might be needed to ensure seamless service in case of an attack or data breach.

Risk Evaluation and Vulnerability Assessment

RISK MATRIX				
		Impact		
		Negligible	Acceptable	Considerable
Likelihood	Highly Unlikely	***Minor***	***Minor***	***Moderate***
	Possible	***Minor***	***Moderate***	***Major***
	Highly Likely	***Moderate***	***Major***	***Severe***

Minor	Minor risks have a reasonably low impact or are unlikely to occur; they can be addressed later without risking the business continuity.
Moderate	Moderate risks can have a considerable impact or may occur but do not jeopardise the business continuity.
Major	Major risks can conceivably hamper business continuity due to their likelihood or the scale of impact.
Severe	Severe risks are classified as risks that could compromise the business continuity and needs immediate attention.

Figure 2: Definition for severity for impact analysis

Risk No:	STRIDE Violation	Vulnerability	Severity	Security Impact	Business Impact
1	S,I	No encryption protocols for website access. (HTTP instead of HTTPS)	***Severe***	Using HTTP instead of HTTPS encryption without Trasport Layer Security (TLS) (Refer Appendix A) makes the website vulnerable to man-in-the-middle attacks exposing sensitive consumer information by mere network sniffing.	- Reputational Damage - Financial costs from regulatory fines - Loss of sensitive consumer data
2	D	No protection against flooding attacks.	***Severe***	With hping3 (OffSec Services Limited, N.D.), an open-source tool, we were able to flood the website and make it offline. *(Refer Appendix B)*	- Service downtime costs - Financial loss (customers' disappointment) - Loss of reputation
3	S,T,R,I,D, E	SSH accessible over public internet	***Severe***	SSH is used for direct access to the servers for day-to-day operation and maintenance. This restricted access should be given via de-militarised zones over secure VPNs connections. *(Refer Appendix C)*	- Reputational Damage - Financial costs from regulatory fines - Service outage
4	S,T,R,I,D, E	Obsolete Encryption Algorithms for SSH	***Major***	Once the direct access is removed via the public internet, obsolete encryption algorithms can compromise the security of the website but also of the user data	- Reputational Damage - Financial costs from regulatory fines - Service outage
5	D	No solution to refresh sessions to automated attacks.	***Major***	Once logged in, users can use automated tools and scripts to overload the website, affecting the integrity and, in worst cases, availability.	- Reputational Damage - Financial costs from regulatory fines
6	S,T,I,E	Website front-end lacks a sustainable level of security hardening	***Moderate***	The website front-end needs security hardening to secure it from sophisticated malicious users against: - Clickjacking (OWASP, N.D) - Cross-Site Request Forgery (OWASP, N.D) - Cross-Domain JavaScript Source File Inclusion (The MITRE Corporation, N.D.)	- Loss of sensitive consumer data - Regulatory fines - Loss of Trust and Reputation
7	S,T,I	Missing setting for X-Content-Type-Options Header (Mozilla and individual contributors, N.D.)	***Minor***	This option prevents an unauthorised copy of the site's content from becoming a hidden or disguised part of a cyber attack (i.e.javascript malicious code disguised in an image file)	- Loss of sensitive consumer data - Loss of reputation - Loss of customers

Figure 3: Risk matrix (Please Note: Same risk numbers are referred throughout the report)

Security Standards

The simplistic convenience of online platforms, including e-commerce, has resulted in the scattering of personal data more than ever before. Regulations such as the General Protection Data Regulation (GDPR) (European Parliament, 2016) help organisations ensure individual data privacy. For e-commerce websites, there are four critical aspects targeted by the GDPR: Public privacy policy, Customer consent, Direct marketing and Cookies (Weigl, M., 2016).

Compliance with GDPR requires websites to have a public privacy policy describing how data protection is applied. It describes how customer data is collected, processed, stored and used (Art. 13 No. 1). GDPR envisages customers to have complete control over the data being collected. Websites ought to get user permission before collecting data and implement legitimate consent management solutions (Art. 4 No. 11). The GDPR has established several rights that ensure individuals control over data (Art. 12 – 23, Rights of the data subject). Websites need to provide mechanisms to exercise the right to be informed, the right to access, the right to rectification or the right to be forgotten. Customer consent also includes cookies as they can be personal identifiers and therefore qualify as personal data.

Although GDPR recital 47 states that personal data may be used for direct marketing if there is a legitimate interest, companies need to consider using the data lawfully and carefully. According to the U.K. Information Commissioner's Office (ICO, N.D.), three principles must be followed: identification of legitimate interest, secure processing of the data must be necessary to achieve it, and the processing cannot go against individuals' interests rights and freedoms.

GDPR's regulatory framework enforces legalities and fines to ensure lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality. In our case, the evaluated website needs to be reinforced by implementing the HTTPS protocol to avoid the risk of hackers intercepting sensitive information.

Like GDPR, Payment Card Industry Data Security Standard (PCI-DSS) (PCI Security Standards Council, 2018) is another regulatory standard that enforces a high level of security and consistency while processing, storing, and executing financial transactions using payment cards. The standard consists of detailed guidelines that all the entities are dealing with card data must comply with to secure cardholder's data from loss, theft and minimise damages from potential fraud or breaches (Owen and Dixon, 2007).

PCI-DSS considers the following aspects for providing security (Ataya, 2010):

- Secure networking using firewalls, access control lists.
- Hardware with password management and periodic firmware upgrades.
- Software with design security guidelines and frequent patching.
- Human Factor by enforcing multi-factor authentication, security policies and regular staff training.
- Data Management by minimising data collection, minimising the number of data collection sites and transaction traceability without identification.

The following table matches vulnerabilities with PCI-DSS directives that illustrate non-compliance:

Risk No.	Vulnerability	Non-Compliance PCI-DSS
1	No encryption protocols for website access	**6.5.4** Network traffic must be encrypted
2	No protection against flooding attacks	**1.2.1** Only traffic between cardholder and service provider is allowed
3	SSH is accessible over public internet	**7.2** Restricted access to limited users over private network
4	Obsolete Encryption Algorithms for SSH	**4.1** If SSH is in use, implement strong cryptography algorithms
5	No solution to refresh sessions to automated attacks.	**9.4.1** Using authorisation system on every user's action using Multi-Factor Authentication.
6	Website front-end lacks a sustainable level of security hardening	**6.5.7** Anti cross-site scripting (XSS) mechanisms must be implemented **6.5.1** Implement solutions against Injection flaws **6.5.9** Anti cross-site request forgery
7	Missing X-Content-Type-Options Header	**6.2** Whole system must be protected from known vulnerabilities

Figure 4: PCI-DSS compliance

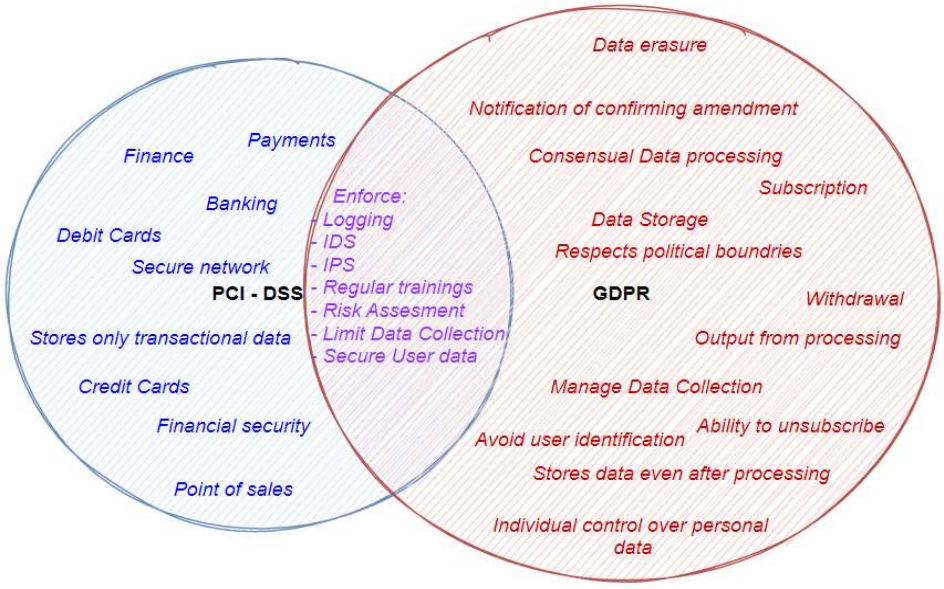


Figure 5: Overlap between PCI-DSS and GDPR

GDPR's scope is significantly broader than PCI-DSS. The Venn diagram (Figure 5) above shows considerable overlap in their scope. The compliance with PCI will cover, to some extent, the GDPR scope. The difference in scope is that GDPR is more individual privacy-oriented, while PCI regulates security relevant to online payment.

Conclusions

Obviously, the development of technology enables access to many useful services for people but also increases the need to improve security constantly. Using insufficiently secured e-commerce websites, we risk losing control over our data and being the target of a data breach. In order to prevent eventual breaches, it is crucial to perform periodic network security assessments, and patch found vulnerabilities. Davis (2019) has categorised the post effects of data breaches for corporations and organisations in four aspects: Financial costs, Reputation damage, Operational disruptions and Legal consequences.

The above document uses the STRIDE method to analyse risks, identify vulnerabilities, and evaluate whether the vulnerabilities represent a non-compliance with GDPR or PCI-DSS standards. Using this methodology has allowed us to determine the areas and scales of threats. It has also made it possible to develop guidelines to improve the security aspect of the system as a whole. Moreover, we have examined the specific requirements of the standards for e-commerce websites.

Recommendations

The report helps us scrutinise the e-commerce website from a regulatory, technical, procedural and business standpoint. The recommendations in the table below are prioritised in decreasing severity order from a business continuity point of view.

Risk No:	**Vulnerability**	**Recommendations**
1	No encryption protocols for website access.	Implementation of security procedures like TLS 1.3 using SSL certificates between the client and server will ensure end-to-end encryption.
2	No protection against flooding attacks.	Use of sophisticated stateful firewalls will restrict the malicious flooding towards the web server.
3	SSH accessible over public internet	Restricted access can be provided using advanced solutions like Virtual Desktop Infrastructure (Appendix C). Virtual desktops can provide on-demand access to desired secure networks.
4	Obsolete Encryption Algorithms for SSH	Using the latest OpenSSH 8.6 will ensure the latest algorithms are installed.
5	No solution to refresh sessions to automated attacks.	Captcha is one of the widely used methods to secure the websites against automatic malicious program attacks that could overload the system (Yu Hu et al., 2018). Enforcing multiple layers of authentication using multi-factor authentication (MFA).
6	Website front-end lacks a sustainable level of security hardening	Validation of all data and HTML/JS sanitation of untrusted data. Forbidding of insertion unknown/untrusted data into code.
7	Missing X-Content-Type-Options Header.	Setting X-Frame-Options Header to DENY (totally close) SAMEORIGIN (Only sites with same origin allowed) or ALLOW-FROM *URL (For specific sites only)*

Figure 6: Technical Recommendations

Besides the previous technical suggestions, we propose some industry practices that have been proved to be effective for the majority of e-commerce businesses.

- Network Security Audits using Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) and ensure software patching to avoid old software vulnerabilities.
- Employing external penetration testers to evaluate loopholes and boundary conditions of the system and network to give an unbiased view of security implementation.
- Enacting regular staff training on security procedures and sensitive data handling.
- Ensure business continuity and disaster recovery plan to reduce the recovery time in case of any security incident with the help of systematic backup/recovery procedures.
- Enforcing daily logging on all the systems that handle sensitive data to ensure structured traceability.

References

Ataya, G. (2010) PCI DSS audit and compliance. Information Security Technical Report, Vol. 15 (Issue 4), pp. 138-144. Available from: https://doi.org/10.1016/j.istr.2011.02.004 [Accessed 5 July 2021].

Davis, M. (2019) 4 Damaging After-Effects of a Data Breach. Available from: https://www.cybintsolutions.com/4-damaging-after-effects-of-a-data-breach/ [Accessed 10 July 2021].

European Parliament (2016) REGULATION (E.U.) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/E.C. (General Data Protection Regulation). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&qid=1626680583935&from=EN [Accessed 5 July 2021].

Hussain S., Erwin H. & Dunne P. (2011) Threat modeling using formal methods: A new approach to develop secure web applications, *2011 7th International Conference on Emerging Technologies*, Islamabad, Pakistan, 2011, pp. 1-5, doi: 10.1109/ICET.2011.6048492 [Accessed 12 July 2021].

Hu Y., Chen L. & Cheng J. (2018) A CAPTCHA recognition technology based on deep learning, *2018 13th IEEE Conference on Industrial Electronics and Applications (ICIEA)*, Wuhan, China, 2018, pp. 617-620, doi: 10.1109/ICIEA.2018.8397789 [Accessed 12 July 2021].

Jiang L., Chen H. & Deng F. (2010) A Security Evaluation Method Based on STRIDE Model for Web Service, *2010 2nd International Workshop on Intelligent Systems and Applications*, Wuhan, China, 2010, pp. 1-5, doi: 10.1109/IWISA.2010.5473445 [Accessed 10 July 2021].

Lipner, S. & Howard, M. (2004) The trustworthy computing security development lifecycle. In the 20th Annual Computer Security Applications Conference (ACSAC 2004). pp. 2–13. [Accessed 9 July 2021].

Mozilla and individual contributors (N.D.). X-Content-Type-Options - HTTP | MDN. Available from: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options [Accessed 6 July 2021]

OffSec Services Limited (N.D.) hping3 | Penetration Testing Tools. Available from: https://tools.kali.org/information-gathering/hping3 [Accessed 10 July 2021].

OWASP Foundation (N.D.) Clickjacking | OWASP. Available from: https://owasp.org/www-community/attacks/Clickjacking [Accessed 7 July 2021].

Owen, M. & Dixon, C. (2007) A new baseline for cardholder security. Network Security, 2007(6), pp.8–12. Available from: https://doi.org/10.1016/S1353-4858(07)70054-5 [Accessed 5 July 2021].

Statista (2021) E-commerce share of total global retail sales from 2015 to 2024. Available from: https://www.statista.com/statistics/534123/e-commerce-share-of-retail-sales-worldwide/ [Accessed 8 July 2021].

The Internet Engineering Task Force (N.D.) Deprecating RC4 in Secure Shell (SSH*)*. Available from: https://tools.ietf.org/id/draft-ietf-curdle-rc4-die-die-die-10.html [Accessed 10 June 2021].

The MITRE Corporation (N.D.) CWE-352: Cross-Site Request Forgery (CSRF) (4.4) Available from: https://cwe.mitre.org/data/definitions/352.html [Accessed 10 June 2021].

The MITRE Corporation (N.D.) CWE - CWE-829: Inclusion of Functionality from Untrusted Control Sphere (4.4). Available from: https://cwe.mitre.org/data/definitions/829.html [Accessed 19 July 2021].

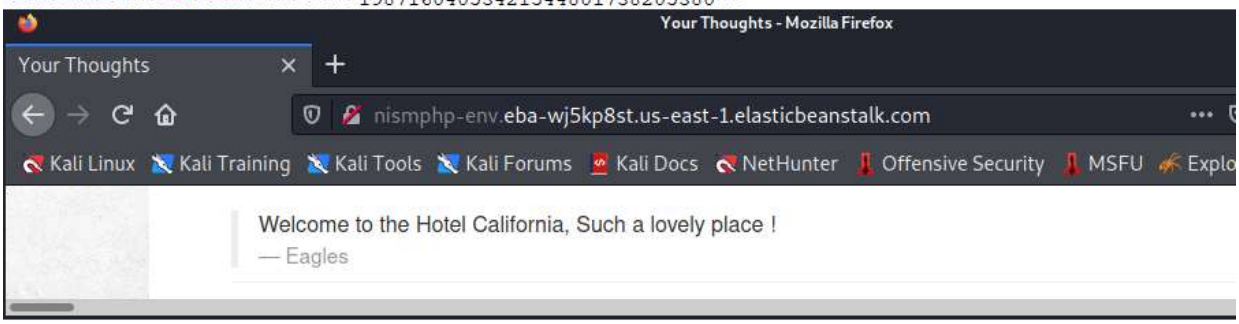
The Payment Card Industry Security Standards Council (2018) PCI SECURITY STANDARDS OVERVIEW. Available from: https://www.pcisecuritystandards.org/pci_security/standards_overview. [Accessed 5 July 2021].

U.K. Information Commissioner's Office (N.D.) Legitimate interests. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/ [Accessed 13 July 2021].

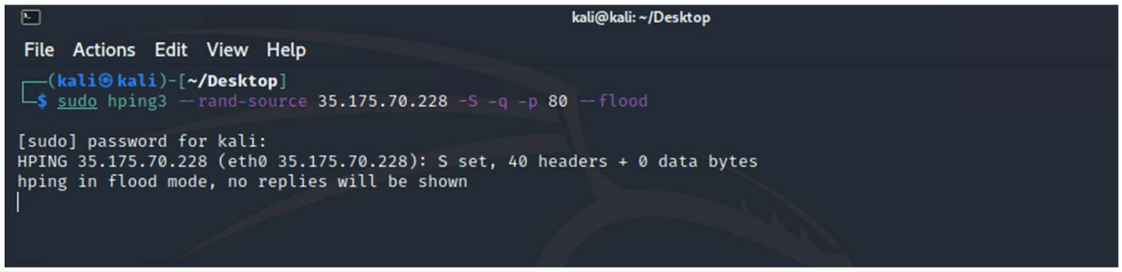
Weigl, M. (2016) The E.U. General Data Protection Regulation's Impact on Website Operators and e-commerce. Computer Law Review International, Vol. 17 (Issue 4), pp. 102-108. Available from: https://doi.org/10.9785/cri-2016-0403 [Accessed 7 July 2021].

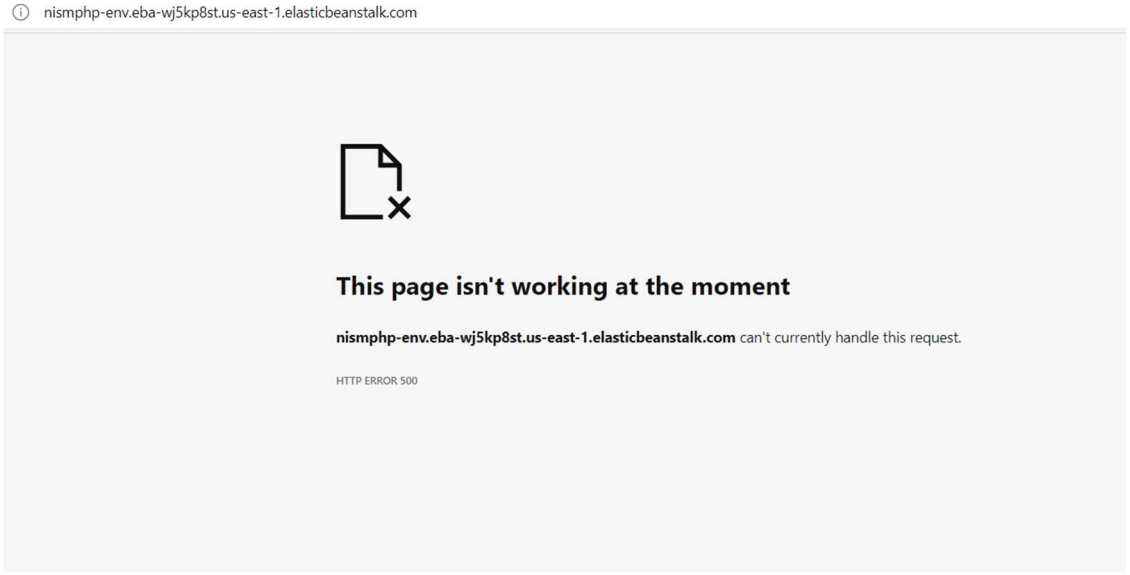
Appendix A

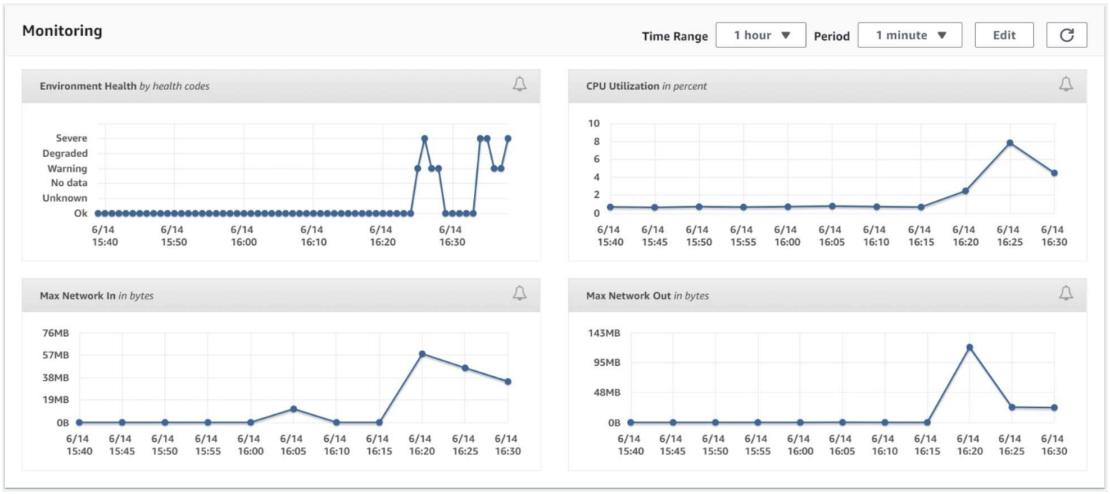
```
┌──(kali㉿kali)-[~]
└─$ sudo tshark -iany -Y http
Running as user "root" and group "root". This could be dangerous.
Capturing on 'any'
   63 6.204125437 35.175.70.228 → 10.0.2.15    HTTP 194 HTTP/1.1 304 Not Modified
   91 19.375347042    10.0.2.15 → 35.175.70.228 HTTP 1007 POST /add HTTP/1.1
   97 19.531140800 35.175.70.228 → 10.0.2.15    HTTP 62 HTTP/1.1 200 OK  (text/html)
/add HTTP/1.1
Host: nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------198716040534215448017382053380
Content-Length: 359
Origin: http://nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com
Connection: keep-alive
Referer: http://nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com/add
Upgrade-Insecure-Requests: 1
-----------------------------198716040534215448017382053380
Content-Disposition: form-data; name="thoughtMessage"
Welcome to the Hotel California, Such a lovely place !
-----------------------------198716040534215448017382053380
Content-Disposition: form-data; name="thoughtAuthor"
Eagles
-----------------------------198716040534215448017382053380--
```



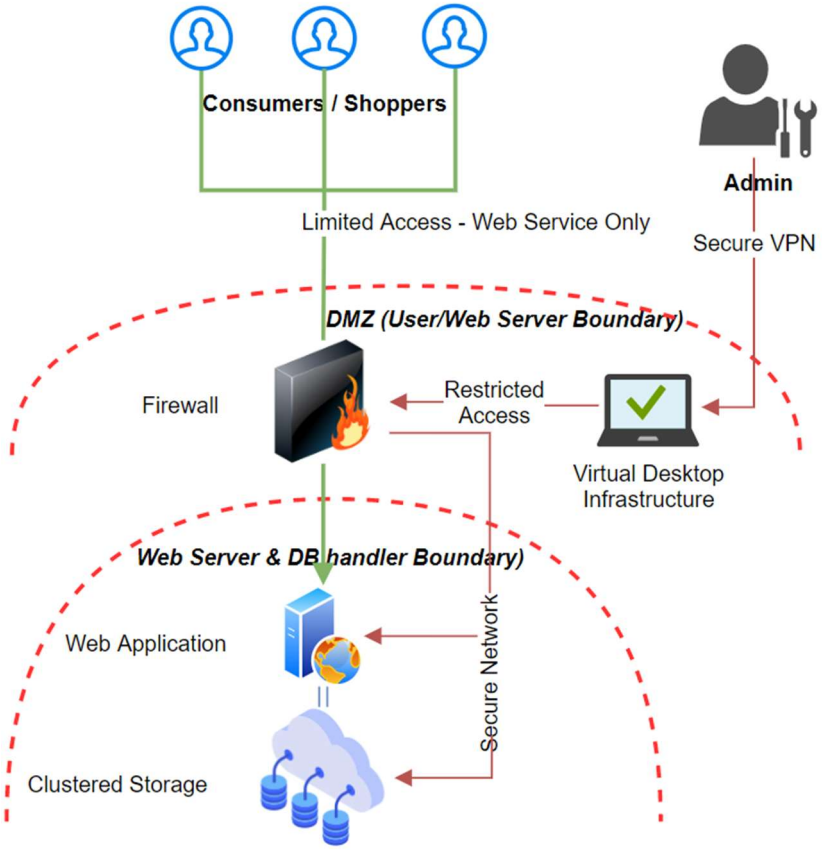
Appendix B


kali@kali: ~/Desktop
File Actions Edit View Help
(kali㉿kali)-[~/Desktop]
$ sudo hping3 --rand-source 35.175.70.228 -S -q -p 80 --flood
[sudo] password for kali:
HPING 35.175.70.228 (eth0 35.175.70.228): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown


nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com
This page isn't working at the moment
nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com can't currently handle this request.
HTTP ERROR 500


Monitoring
Time Range
1 hour
Period
1 minute
Edit
Environment Health by health codes
Severe
Degraded
Warning
No data
Unknown
Ok
CPU Utilization in percent
Max Network In in bytes
Max Network Out in bytes

Appendix C


Consumers / Shoppers
Admin
Limited Access - Web Service Only
Secure VPN
DMZ (User/Web Server Boundary)
Firewall
Restricted Access
Virtual Desktop Infrastructure
Web Server & DB handler Boundary)
Web Application
Secure Network
Clustered Storage