**GROUP 5 Report**

**Introduction (David , Czeska and Aimalohi )**

This report covers possible cyber security vulnerabilities that affect e-health systems, different penetration testing methodologies and standards, appropriate related standards of e-health system and non-compliance of opponent group to the same, Business impacts on the use of penetration testing tools on the target e-health system, Limitations and assumptions of the penetration testing and recommendations.

**Possible security vulnerabilities (David & Aimalohi)**

According to Alhassan et al(2016) e-health system are susceptible to vulnerabilities like Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. Similarly, according to Department of Health and Human Services USA(2020) commonly used Open Electronic Medical Record (EMR) system, vulnerabilities like SQL injection, remote code execution to escalate privileges on the server, site request forgeries, unauthenticated information disclosure, cross-site scripting due to improper neutralization of user-controllable input and information exposure. Saira et al (2019) indicate that in the year 2017, the WannaCry ransomware encrypted data for thousands of computers worldwide and impaired the functionality of the National Health Service (NHS) in England.

**Methodology and Aproaches (David , Czeska and Aimalohi )**

We have decided to use basic testing tools to carry out our web site testing because the website we were testing has minimal functionality. The Ping command was used to troubleshoot network connectivity between the hosts . the TracerT command was used to measure the number of hops between the hosts while whois tool was used to get details on the ownership of the domain name.

In the future we intend to make use of OWASP Methodology, OSINT Framework, Nessus etc for more in-depth testing.

Two groups were create and paired by the lecturer in charge of course and were instructed to design a website and exchange the web and IP address with the other group for penetration tests. We nominated a group leader who allocated tasks. We used Gray Box Penetration and remote testing approach because group members are located in various countries.

**Appropriate related standards and non-compliance (Czeska & Yibeltal & Aimalohi)**

Considering that we carried out web tests on an E-health site, we proposed that applicable standards for regulatory compliance include but aren’t limited to: Health Insurance Portability and Accountability Act (HIPAA)1996 ( a United States Federal Statute which provides minimum standards for protecting a person’s health information), Data Protection Act (DPA) 2018 and the General Data Protection Regulation (GDPR) which protects privacy by giving more rights to data subjects over their Personal Identifiable Information (PII), Social Care Act 2012 etc. Non-compliance with applicable laws and regulation was not detected in the penetration tests (Shuaib *et al.*, 2021).

**Business impacts on the use of tools and methods (scanning in or out of hours, traffic) (Dario)**

Using the Traceroute tool it is possible to see the paths between the malicious person and the target website and the IP addresses of the gateway devices will be displayed and there is a probability for someone to use this information maliciously(Nohe, 2021).

The dig scan tool can be used to find the public IP address of the website and therefore be subject to a DDoS attack. More specifically, the impact of this attack can make the website, application or global business unavailable during a long period of time, the business as a result will not be able to meet the SLA with the customers (Kohout, N.D).

The whois tool will give access to a list of name servers from the website, using this information it is possible to exploit the DNS requests, by using DNS cache poisoning. This method will modify users DNS requests and redirect them to a malicious website (Varonis, N.D).

**Timelines of the completion of the task (Aimalohi)**



**Table 1**

**Limitations and assumptions (Kwong)**

We could only carry out our pen tests at specific periods and we used a limited number of tools to carry out tests due to access to limited resources. Also, the tests were is restricted to a target environment and not every production area of the network and we used a specific set of methods and skills, to avoid any downtime or system crash of the production network (Aaron, 2020).

**Recommendations and potential mitigations (Kwong & Dario)**

Brute Force attack: A passwordless Multi-Factor Authentication (MFA) solution can mitigate the Brute Force attack completely. Microsoft (2021) able to deploy a passwordless MFA solution with Windows Hello; the Microsoft or Google authenticator can do the 2nd sign in with a mobile phone, and FIDCO2 security keys can be the last authentication. No more password is involved during the authentication process.

Wi-Fi being cracked down and hacked: A Wifi Protected Access 2 (WPA2) enterprise solution can be deployed, RADIUS/802.1x-based authentication, which is based on 802.11i standard, with the latest AES-CCMP encryption can be used. A Wireless LAN Controller and the AP will be the 802.1X authenticator, by using the Lightweight Access Point Protocol (LWAAP) (Cisco, 2021).

Also, a stateful firewall can mitigate the DDOS by using new techniques to provide zero-day DDOS protection and SSL attack with hardware engines. (Checkpoint, 2021).

**References**

1. Aaron, C (2020) Major Limitations of Penetration Testing You Need to Know,

Available from:

https://www.cypressdatadefense.com/blog/limitations-of-penetration-testing/

[Accessed: 27 May 2021].

1. Alhassan, J., Abba E., Olaniyi,O, & Waziri, V. (2016), 'Threat Modeling of Electronic Health Systems and Mitigating Countermeasures', *International Conference on Information and Communication Technology and Its Applications* *(ICTA 2016).* Federal University of Technology, Minna, Nigeria, 28 – 30 November 2016

Available from: https://www.researchgate.net/publication/311238739\_Threat\_Modeling\_of\_Electronic\_Health\_Systems\_and\_Mitigating\_Countermeasures

[Accessed 25th May 2015].

3. Alhabeeb M, Almuhaideb A, Le P, Srinivasan B, 2010. Information Security Threats Classification Pyramid. 24th IEEE International Conference on Advanced Information Networking and Applications Workshops: 2010. p. 208-213.

4. Cisco (2021) *Cisco Unified Wireless Network Architecture—Base Security Features. Enterprise Mobility 4.1 Design Guide.*

Available from:

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper/ch4\_Secu.html

[Accessed: 24th May 2021].

5. Checkpoint (2021) *DDoS Protector,*Available from

https://www.checkpoint.com/quantum/ddos-protector/

[Accessed: 24th May 2021].

6. Department of Health and Human Services USA(2020)*Electronic Health Record Sys tems*

Available from:

https://www.hhs.gov/sites/default/files/electronic-health-record-systems.pdf

[Accessed 25th May 2021].

7. Geric S, Hutinski Z ,2007. Information system security threats classifications. *Journal of Information and Organizational Sciences*; 31: 51

8. Infosec Resources Privacy Policy and Das, R. (2021) The Types of Penetration Tests

Available from:

https://resources.infosecinstitute.com/topic/the-types-of-penetration-testing/

[Accessed 25th May 2021].

9. 360LOGICA.COM (2018), Penetration Testing Methodologies

Available from:

<https://www.360logica.com/blog/different-methodologies-penetration-testing/>

[Accessed 25th May 2021].

10. Nohe, P (2021) Executing a Man-in-the-Middle Attack in just 15 Minutes. Available from : <https://www.thesslstore.com/blog/man-in-the-middle-attack-2/>

[Accessed on 27 May 2021].

11. Kohout, J. (N.D) How DDoS Attacks Can Sink Your Business. Available from:

How DDoS Attacks Can Sink Your Business: <https://teskalabs.com/blog/how-ddos-can-sink-your-business>

[Accessed on 27 May 2021].

12. Microsoft (2020) How it works: Azure AD Multi-Factor Authentication,

Available from:

https://docs.microsoft.com/en-GB/azure/active-directory/authentication/concept-mfa-howitworks

[Accessed: 5th May 2021].

13. Saira, G., Emilia, G., Nick, J., Ara, D.(2019) The challenges of cybersecurity in health care: the UK National Health Service as a case study, *The lancet Digital Health*,Vol 1 may 2019:pp 10-12.

Available from:https://www.researchgate.net/publication/332967917\_The\_challenges\_of\_cybersecurity\_in\_health\_care\_the\_UK\_National\_Health\_Service\_as\_a\_case\_study/

[Accessed 25th May 2015].

14. Swiderski F, Snyder W, 204. Threat Modeling. Microsoft Press.

15. Tang J, Wang D, Ming L, Li X. A, 2012. Scalable Architecture for Classifying Network Security Threats. Science and Technology on Information System Security Laboratory.

16. Varonis. (N.D) What is a Man-in-the-Middle Attack: Detection and Prevention Tips. Available from: https://www.varonis.com/blog/man-in-the-middle-attack/ [Accessed on 27 May 2021].

17. Vumetric Inc(2021)Top 5 Penetration Testing Methodologies and Standards

Available from:

https://www.vumetric.com/blog/top-penetration-testing-methodologies

[Accessed on 27 May 2021].

18.Shuaib, M. *et al.* (2021) ‘Compliance with HIPAA and GDPR in blockchain-based electronic health record’, *Materials Today: Proceedings*. doi: 10.1016/j.matpr.2021.03.059.