GROUP 5 Report

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.

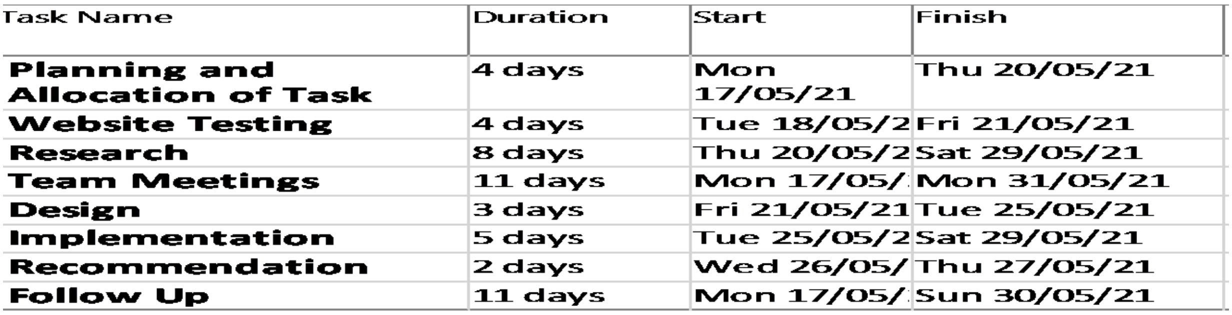
According to Alhassan et al (2016) e-health system are susceptible to vulnerabilities like Tampering, Repudiation, Information Disclosure, Denial of Service, Spoofing and Elevation of Privilege. Similarly, the Department of Health and Human Services USA(2020) suggests that Open Electronic Medical Record (EMR) system have, 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 encoded data for numerous systems worldwide which adversely affected the National Health Service (NHS) in England.

Vumetric Inc (2021) suggests that Open Source Security Testing Methodology Manual (OSSTMM), Penetration Testing Methodologies and Standards (PTES), Open Web Application Security Project (OWASP), National Institute of Standards and Technology (NIST) and Information System Security Assessment Framework (ISSAF) are the methodologies that guide penetration tester in their work. On the other hand 360LOGICA.COM (2018) maintains that penetration-testing can be characterized by testing methods like White Box, Black Box and Gray Box Penetration testing. Infosec Resources Privacy Policy & Das (2021) explains that once teams has defined roles and responsibilities, they can choose between Network Services, Web Application, Client Side, Wireless and Social Engineering pen testing.

Two groups namely group 5 and 6 were create and paired by the lecturer in charge of course. The groups were instructed to design a website and exchange the web and IP address with their opponents for the pen-tests. Our team was named group 5 and had six members. We nominated a group leader who allocated us tasks like web designers, contributor and PowerPoint designers. All members were given the task of being pen-testers. Group 5 used web application with a combination of Gray Box Penetration and remote testing approach because all group members are located in different locations worldwide away from the target web servers. Ping, Tracert, WHOis and Mxtoolbox were the tools used during basic penetration testing to obtain basic information about the website. The group further plans to use Shodan.io, OSINT framework, Nessus, Burp suite, OWASP and Kali Linux to obtain in depth knowledge about the vulnerabilities and their potential impact.

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).

The Traceroute tool makes it possible to see the paths between the sending terminal and the target website, the command shows the IP addresses of the gateway. If a malicious person comes across such information, it is possible to find security holes in the connected devices and make some damage on those devices (Nohe, 2021). The dig tool easily exposes the public IP address of the website making it susceptible to Distributed Denial of Service (DDoS) attack. DDoS can cause the website, application or global business to be unavailable hence making the enterprise unable to meet the Service Level Agreements with the customers (Kohout, N.D). The whois tool shows a list of name servers from the website, using this information it is possible to exploit the Domain Name System (DNS) requests, by using DNS cache poisoning. This method will modify users DNS requests and redirect them to a malicious website (varonis, N.D). Figure 1 below shows how different tasks have been spread for our objectives to be achieved.



Task Name	Duration	Start	Finish
Planning and Allocation of Task	4 days	Mon 17/05/21	Thu 20/05/21
Website Testing	4 days	Tue 18/05/2	Fri 21/05/21
Research	8 days	Thu 20/05/2	Sat 29/05/21
Team Meetings	11 days	Mon 17/05/	Mon 31/05/21
Design	3 days	Fri 21/05/21	Tue 25/05/21
Implementation	5 days	Tue 25/05/2	Sat 29/05/21
Recommendation	2 days	Wed 26/05/	Thu 27/05/21
Follow Up	11 days	Mon 17/05/	Sun 30/05/21

Figure 1

It is assumed that the penetration testing should bring out all potential vulnerability, from unauthorised access to any malicious activity and cover different aspects of security testing and simulation. The test should cover the entire system, from frontend to back-end server. This test has several limitation. Firstly, it will only be carried out for a limited time and we only can produce results at a specified period of time. In fact, an attacker would attack a system at any time, from anywhere. Secondly, it has the limitation of Scope because we are trying to do every known security intrusion and breach test, in realty we cannot test everything, especially those unknown security attack methodology from any attacker. Thirdly, we have the limitation of access because the pen test is restricted to a target environment, but not every production area of the network. Last but not least we have the Limitation of methods and skill sets because the pen test is restricted to use a specific set of methods and skills to avoid any downtime or system crash of the production network (Aaron, 2020).

We recommend that 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. Secondly, a stateful firewall can mitigate the DDOS. But other specific anti-DDOS appliance, such as Checkpoint DDOS protector, by using new techniques to provide zero-day DDOS protection and Secure Sockets Layer (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].

2. 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_Heal
[Accessed 25th May 2015].

3. Checkpoint (2021) *DDoS Protector,*
Available from
https://www.checkpoint.com/quantum/ddos-protector/
[Accessed: 24th May 2021].

4. Department of Health and Human Services USA (2020) Electronic Health Record Systems
Avalable from:
https://www.hhs.gov/sites/default/files/electronic-health-record-systems.pdf
[Accessed 25th May 2021].

5. 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].

6. 360LOGICA.COM (2018), Penetration Testing Methodologies
Available from:
https://www.360logica.com/blog/different-methodologies-penetration-testing/
[Accessed 25th May 2021].

7. 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].

8. 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].

9. Microsoft (2021) How it works: Azure AD Multi-Factor Authentication,
   Available from:
   https://docs.microsoft.com/en-GB/azure/active-directory/authentication/
   [Accessed: 5th May 2021].

10. 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
    Avalable from:
    https://www.researchgate.net/publication/332967917_ /
    [Accessed 25th May 2015].

11. 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.

12. 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].

13. 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].