Network and Information Security Management: Design Document

Background

Project Overview

The E-Health site provides medical and fitness information and guidance from medical specialists to registrants, potentially improving the health of those living in rural and remote areas. Within the scope of the penetration test project, a complete list of potential threats and vulnerabilities of the organisation's E-Health site and appropriate remediation plans will be provided.

Project assumptions

- Single Host System
- Database: MySQL
- Development Platform: PHP
- Currently running on a UAT environment
- UK-based system: adhere to GDPR and the Data Protection Act
- BCM/DR is absent
- The system saves personal information on the registrant's health and provides information from medical professionals
- The testing is done using VDI provided by the healthcare authority

Methodology

STRIDE

STRIDE identifies system vulnerabilities following specific threat categories, which are: Spoofing, Data Tampering, Repudiation, Disclosure of Information, DOS, and Privilege escalation – as shown in Figure 1 (Shevchenko, 2018).

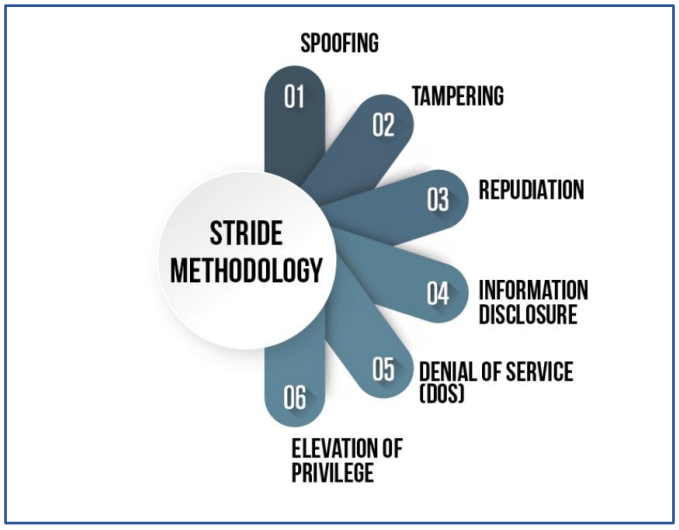

Figure 1: STRIDE Methodology (EC-Council, 2020).

Figure 2 displays the individual attack vectors at each stage of STRIDE:

	Type of Threat	What was violated?	How was it violated?
S	Spoofing	Authentication	Impersonating something or someone known and trusted.
T	Tampering	Integrity	Modifying data on disk, memory, network etc.,
R	Repudiation	Non-repudiation	Claim to not be responsible for an action
I	Information Disclosure	Confidentiality	Providing information to someone who is not authorized
D	Denial of Service (DoS)	Availability	Denying or obstructing access to resources required to provide service
E	Elevation of Privilege	Authorization	Allowing access to someone without proper authorization

Figure 2: STRIDE Attack Vectors (EC-Council, 2020).

PASTA

PASTA (Process for Attack Simulation and Threat Analysis) is defined as a risk-based threat-model by Shevchenko (2018). Furthermore, the EC-Council (2020) emphasizes the capability of the framework to mitigate IT solution risk.

PASTA can be split into the following stages:

Figure 3: PASTA Threat Modelling (Shevchenko, 2018).

TRIKE

TRIKE combines risk-management and security audits within a single model (Shevchenko, 2018). It aims to explain the risk level against IT assets, using a fusion of the "Requirement Model" and the "Implementations Model" (EC-Council, 2020).

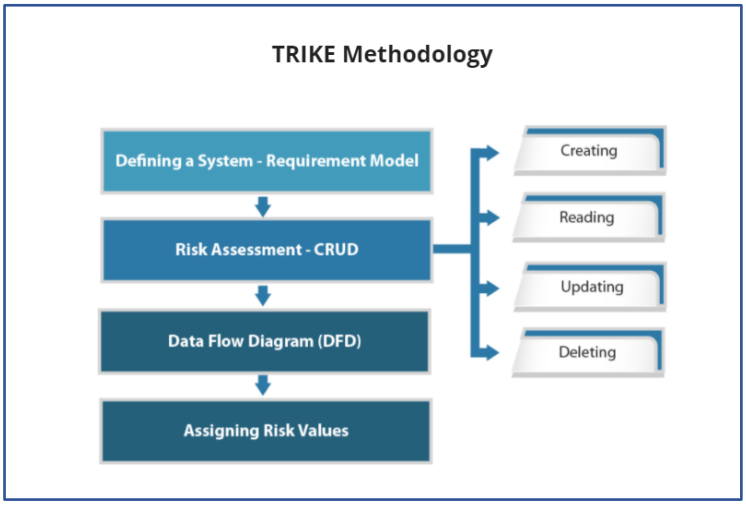

Figure 4: TRIKE Methodology (Shevchenko, 2018).

For this project, the STRIDE methodology will be applied due to its ease and speed of application. Being adopted by Microsoft since 2002, the STRIDE methodology is a mature and commonly-used threat-modelling approach within the industry (Howard and LeBlanc, 2002).

Penetration Testing Methods

Staffing

The penetration testing can be done using both on-shore and off-shore models. During onsite testing, the testers are available at the customer location and provide a seamless and transparent process. The current scope of testing has to be confined to the off-shore model since the testers are present in separate geographic locations with current travel restrictions.

The off-shore model may include risks such as:

- Lack of transparency
- Communication gaps
- Time difference
- Lack of Quality Assurance

(Johnson, N.D.)

Manual and Automated Testing

The penetration testing conducted can be manual (performed by a human) or automated (scripts/tools without human intervention) (Kinsbruner, 2019). For this project, testing will be mostly done manually due to the lack of fully automated tools/scripts.

Security Challenges

In addition to the generic security challenges, as discussed within the methodology chapter, challenges specific to E-Health need to be highlighted:

1. Alteration of patient data leading to incorrect diagnosis of the patient, which can lead to death or permanent injury of the patient.
2. Blackmailing of patients using sensitive information such as diseases.
3. Altering roasters of the health care professionals leading to chaos and denial of health care services
4. Ransomware attack on health care records leading to denial or delay of services to the patients.
5. Disclosure of Patient / Healthcare professionals address, phone number, social security number, and other sensitive data can lead to identity theft.

Penetration Testing Tools

Nmap:

For information gathering, Nmap will be used to gain insights about the host, its IP address, its OS, and similar details regarding the network. Open ports of the host can be identified, giving information on the services that are running on the machine. Nmap counts as an industry-standard due to its versatility and usability (Ferranti, 2018).

STRIDE: Spoofing, Information Disclosure

Nessus, ZAP, Nikto, Skipfish:

Automated web application scanners will be used to find potential vulnerabilities and attack vectors. Nessus, as an example, counts as one of the widely used vulnerability scanners in the cybersecurity industry, offering scans for both UNIX and Windows systems (Obbayi, 2019).

STRIDE: Tampering, Information Disclosure

Metasploit Framework:

Metasploit, counting as an industry standard and widely used penetration testing framework, can check for vulnerabilities, apply known exploits, and offers malicious payloads to probe a network for weak spots (Petters, 2020).

STRIDE: Spoofing, Tampering, Information Disclosure, Elevation of Privilege

LinPEAS:

Should the team gain access to the host's shell, enumeration needs to be done to check for ways of escalating privilege. LinPEAS is a script that automates this search and generates a report with its findings.

STRIDE: Privilege Escalation

Slowloris, LOIC:

To test for Denial-of-Service vulnerabilities, Slowloris (DDoS) and LOIC (DoS) will be deployed.

STRIDE: Denial-of-Service

Business Impact

Conducting penetration testing in the healthcare industry draws significant attention as a system cannot experience any downtime due to the real-time impact on patients. Furthermore, it is critical to preserve data integrity due to its private nature and strict compliance adherence. Therefore, conducting penetration testing on the UAT environment ensures that clients are not exposed to unnecessary risks of a system outage while safeguarding sensitive patient information and GDPR rules associated with it.

Additional stress testing will be performed in an environment that emulates the production server. By doing so, specific attack vectors, such as denial of service attacks, can be simulated to reveal existent vulnerabilities in the implementation, whilst ensuring no operational disruptions and data clean-up activities.

Without being hindered by restrictive rules of engagement or the level of risk associated with testing, significant vulnerabilities can still be discovered at the development environment level that the organisation should address to validate a secure technical environment for its business operations.

Timeline

Figure 5 depicts the timeline of the individual project phases: design documentation, penetration testing and the final executive summary.

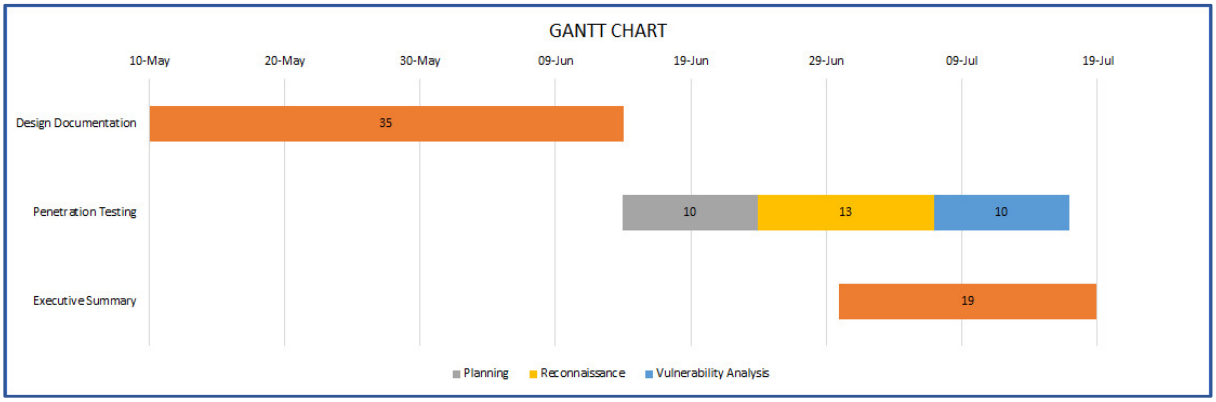

Figure 5: Project Timeline

Limitations

A penetration test's scope is limited to only the target environment. It focuses on the exposures in the technical infrastructure and does not identify all possibilities where critical or sensitive organisational information may leak.

Moreover, being a snapshot of a technical environment at a point in time, a penetration test can play only a small part in reviewing the human factor as a defensive target and could lead to breaches. A penetration test will have to be repeated often as random data is insufficient to uncover all security weaknesses. If weaknesses are ignored, the system may become susceptible to multi-vector attacks (chaining multiple minor vulnerabilities together to create a significant vulnerability) (Loo, 2011; Karumba, 2015).

Furthermore, time constraints limit the ability to create custom and manually written exploits to perform testing when regular penetration test frameworks and tools are of little use to test high secure environments (Ansari, 2015).

Penetration testing is not a cure for all illnesses; Instead, undertaking a series of penetration tests accompanied by periodic security risk assessment and third-line defence (Audit) will more effectively support the company in establishing secure operations.

Reference List

Ansari, J. (2015) Web Penetration Testing with Kali Linux. Packt Publishing. Available from: https://subscription.packtpub.com/book/networking_and_servers/9781783988525 [Accessed 9 June 2021].

EC-Council (2020) What Is Stride Methodology In Threat Modeling? Available from: https://blog.eccouncil.org/what-is-stride-methodology-in-threat-modeling/ [Accessed 12 June 2021].

Ferranti, M. (2018) What is Nmap? Why you need this network mapper. Network World. Available from: https://www.networkworld.com/article/3296740/what-is-nmap-why-you-need-this-network-mapper.html [Accessed 07/06/2021].

Howard, M. & LeBlanc, D. (2002) *Writing secure code: practical strategies and proven techniques for building secure applications in a networked world*. 2nd ed. Microsoft Press. Available via the Vitalsource Bookshelf [Accessed 12 June 2021].

Johnson, J. (N.D.) Should I Use An Offshore Penetration Testing Company? Triaxiom Security. Available from: https://www.triaxiomsecurity.com/should-i-use-an-offshore-penetration-testing-company/ [Accessed 12 June 2021].

Karumba, M. (2015) A Hybrid Algorithm for Detecting Web Based Applications Vulnerabilities. Available from: http://erepository.uonbi.ac.ke/bitstream/handle/11295/97122/Chris_Muiruri_Project_Final.pdf?sequence=1 [Accessed 2 June 2021].

Kinsbruner, E. (2019) Manual Testing vs. Automated Testing. Available from: https://www.perfecto.io/blog/automated-testing-vs-manual-testing-vs-continuous-testing [Accessed 12 June 2021].

Loo, F. (2011) Comparison of penetration testing tools for web applications. Available from: https://www.semanticscholar.org/paper/Comparison-of-penetration-testing-tools-for-web-Loo/7564a3c5608e52e0c8d69b8819726e07f409b005#citing-papers [Accessed 2 June 2021].

Obbayi, L. (2019) A brief introduction to the Nessus vulnerability scanner. Infosec Resources. Available from: https://resources.infosecinstitute.com/topic/a-brief-introduction-to-the-nessus-vulnerability-scanner/ [Accessed 07/06/2021].

Petters, J. (2020) What is Metasploit? The Beginner's Guide. Varonis. Available from: https://www.varonis.com/blog/what-is-metasploit/ [Accessed 07/06/2021]

Shevchenko, N. (2018) Threat Modeling: 12 Available Methods. Available from: https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html [Accessed 12 June 2021].