2021

Design Document

NETWORK AND INFORMATION SECURITY MANAGEMENT

GROUP 2 SECURITY SQUAD: NILS LINHOFF, HAORUN FUJAH, ADRIAN BOSCU.

Content

Background

The security Squad (Group2) is tasked with scanning and analysing an E-Health website for potential cyber security risks and vulnerabilities. Then the Security Squad will provide an executive summary of the scanning results, threat analysis, risk assessment and mitigation strategy to the owner of the E-health website. The aim of this document is to lay out the methodology, tools and technical approach as the basis for the final report.

Limitations and assumptions.

- Availability of Website
- Limitations due to time/manpower constraints:
- Limitations due to the availability of tools (costs/complexity)
- Application of GDPR (depends on geographical location of servers, customers, users).
- Application of data protection industry standards

Security challenges

1. Information Disclosure

As the target website is an E-health website where sensitive customer data is stored, one of the highest security risks is the disclosure of information. Potential attackers can seek out private health data from customers and could do further harm to either the company via ransom demands or to the patient itself. The company operating the website must ensure their patient's privacy is safeguarded and that the whole network functions as securely as possible (USC EMHA Online. 2021).

2. Malware

Subject to the type, malware can extract electronic health records from the E-health sites that users are accessing medical data from. Of specific concern is a kind of malware known as ransomware. This impedes the operations of a system or a certain user until a stipulated monetary amount is paid.

Malware may also lead to significant stoppages in computer processing time. This can delay and present grave problems in a medical or e-health environment where prompt access to information can be vital in delivering efficient healthcare services (USC EMHA Online. 2021). In a worst-case scenario, such malware may crash the whole system. If all the health records are in digital storage, this signifies that the practice will be unable to access patient information.

3. Phishing

Phishing is not a contemporary security threat, however due to the increased occurrence of electronic health records, password security is more critical than ever. Phishing plots can be exceptionally proficient and may conceal themselves as emails from medical personnel or alerts that prompt users to reveal confidential data, such as passwords or codes, to access sensitive information.

Methodology

All scanning exercises will be done remotely from a location in NL. The results and the potential vulnerabilities will be clustered and organized according to the STRIDE analysis. STRIDE is an acronym derived from the following threat categories (Microsoft, 2009):

- Spoofing Identity
- Tampering with Data
- Repudiation
- Information disclosure
- Denial of service
- Elevation of privileges

The STRIDE analysis is especially useful for inspecting each system component for vulnerabilities which could comprise the whole system (Khan et al., 2017).

Beside the more general STRIDE method for threat categories the more holistic approach to threat modelling that considers business as well as technology, Process for Attack Simulation and Threat Analysis (PASTA), will be used:

1: Define business objectives

2: Define the technical scope of assets and components

3: Application factoring and identify application controls

4: Threat analysis based on threat intelligence

5: Vulnerability detection

6: Analyse and model attack

7: Risk/ impact analysis and development of countermeasures

The PASTA approach is attack centric vulnerability analysis which is the basis for an asset-based mitigation strategy (Ucedavélez and Morana, 2015).

Finally, after exploring the vulnerabilities with the help of the STRIDE and PASTA analysis, the last step is to use a risk assessment model such as DREAD.

DREAD categorizes the risk level into:

- Damage – how bad would an attack be?
- Reproducibility – how easy is it to reproduce the attack?
- Exploitability – how much work is it to launch the attack?
- Affected users – how many people will be impacted?
- Discoverability – how easy is it to discover the threat?

Each category is then given a rating from 1-10. However, one notable limitation of the DREAD method is that the rating is subjective (Howard et al., 2014). To mitigate this problem, we entrust the rating to our very experienced pen-tester.

The specific industry and governmental regulation for a health website need to be considered. The EU general data protection regulation (GDPR) might be applicable to data security. The GDPR article 5 has specific principles relating to processing of personal data and requires organizations to use encryption or pseudonymization whenever feasible (Radley-Gardner et al., 2016).

The industry standard ISO 27001 for Information security management system might be applicable as well as it includes requirements for the assessment and treatment of information security risks (The new ISO/IEC 27001:2013 standard, no date).

Tools and scanning approaches.

Scanning tools:

- **Kali Linux** deployed as a VM on an ESXi environment with public internet access (Allen, Heriyanto and Shakeel Ali, 2014). We have selected Kali linux as it is an updated open-source operating system that is bundled with many tools for information gathering and exploitation.

- **Legion** as part of Kali Linux - scanning of ports open for the website. Legion provides a detailed scan of remote targets from open ports that the host is listening to as well as target screenshots of http/https pages.
- **DirBuster** as part of Kali Linux - to find hidden and public files and subdirectories. We have selected DirBuster for the purpose of brute force website crawling that is able to scan a website against a specific word list directory.

Evaluation of Kali Linux against other most common scanning tools:

Tool	ease of install	ease of use	flexibility	licensing	reputation	score
Metasploit	installer/source code		open source/ custom modules	open source	most popular	5
Kali Linux	Linux nessecary	easy/for beginners/ lot of documentation	all-in-one tool	free	very popular	5
Burp Suite	installer	automates functions		free/Premium model	popular/community support	4
Nessus	installer	scans to a database of known vulnerability signatures	checks computers and firewalls for open ports	subscription		3
Nmap	installer		apping the network's attack surface.			3
OWASP Zap		automated and manual web application scanning/ easy		open source	very popular	3
SQLmap	Ubuntu Linux,		discovery of SQL Injection holes			2
Jawfish					new/not vetted	2

Approaches:

Have a Linux VM deployed in an ESXi environment with direct access to the internet in order to use all the integrated tools for scanning of the targeted website.

Use of Legion tool as part of Kali Linux to perform data gathering of open ports of website as well as data gathering of list of IP addresses corresponding to the DNS entries.

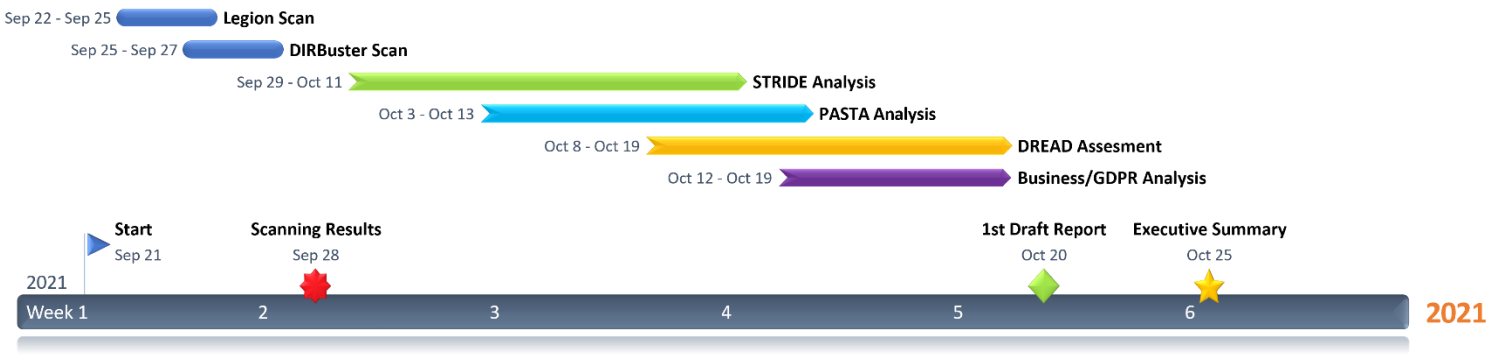
DirBuster as part of Kali Linux as well is being used against the targeted website to gather information regarding the list of files and subfolders. This does not scan links or targets to other pages within the website but creates brute force requests of subfolder/files

Business Impacts

As a result of the scanning assessment, it is imperative to outline business effects on the aforementioned tools and methods, this certifies that the testing turnout is advantageous to the E-health business as the essential security and compliance standards are upheld (Allen et al. 2014).

Business impacts on the employed tools and methods are non-existent in terms of availability as the scanning appraisal achieves the corporate objective of examining the e-health website's information systems which hold private data belonging to customers, workers, and other business stakeholders. In addition, there is an absence of business impacts on the cost and licensing of the utilized tools such as Kali Linux, DirBuster, and Legion due to the free and open-source variations of the tools employed in the scanning exercise.

Timeline



Title	Start date	End date
Start	Milestone	21.09.2021
Legion Scan	22.09.2021	25.09.2021
DIRBuster Scan	25.09.2021	27.09.2021
Scanning Results	Milestone	28.09.2021
STRIDE Analysis	29.09.2021	11.10.2021
PASTA Analysis	03.10.2021	13.10.2021
DREAD Assesment	08.10.2021	19.10.2021
Business/GDPR Analysis	12.10.2021	19.10.2021
1st Draft Report	Milestone	20.10.2021
Executive Summary	Milestone	25.10.2021

References.

Tang, A., 2014. Network Security - A guide to penetration testing. 8th ed. pp.8-11. ISSN 1353-4858, available at: https://0-doi-org.serlib0.essex.ac.uk/10.1016/S1353-4858(14)70079-0.

Allen, L., Heriyanto, T. and Shakeel Ali, S., 2014. Kali Linux – Assuring Security by Penetration Testing. Published by Packt Publishing.

Amazon Web Services, Inc. 2021. Penetration Testing - Amazon Web Services (AWS). [online] Available at: https://aws.amazon.com/security/penetration-testing/ [Accessed 11 September 2021].

USC EMHA Online. 2021. Electronic Health Records | Read About Cybersecurity Concerns. [online] Available at: <https://healthadministrationdegree.usc.edu/blog/cybersecurity-in-the-electronic-health-record-era/> [Accessed 8 September 2021].

AWS penetration testing policy https://aws.amazon.com/security/penetration-testing/

Howard, M., LeBlanc, D. and LeBlanc, D. (2014) *Writing Secure Code : Practical Strategies and Proven Techniques for Building Secure Applications in a Networked World*. Redmond, UNITED STATES: Microsoft Press. Available at: http://ebookcentral.proquest.com/lib/universityofessex-ebooks/detail.action?docID=540974.

Khan, R. *et al.* (2017) 'STRIDE-based threat modeling for cyber-physical systems', in *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*. *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, pp. 1–6. doi:10.1109/ISGTEurope.2017.8260283.

Microsoft (2009) *The STRIDE Threat Model*. Available at: https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20) (Accessed: 29 June 2021).

The new ISO/IEC 27001:2013 standard (no date). Available at: https://www.bsigroup.com/en-GB/iso-27001-information-security/ISOIEC-27001-Revision/ (Accessed: 8 September 2021).

Ucedavélez, T. and Morana, M.M. (2015) *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*. Hoboken, NJ, USA: John Wiley & Sons, Inc. doi:10.1002/9781118988374.