Design Document

Course: MSc Computer Science
Module: Network and Information Security Management
Assignment: Team Project – Design Document
Date: Monday 20th September 2021
Team: C (Kieron Holmes, Victor Hernandez, Sergio Zavarce, George Cowie)

1. Background

An e-Health provider has approached us requesting assistance to identify security vulnerabilities and explain measures that can be implemented to rectify these issues. Studies show that the e-Health sector is susceptible to various attacks, including human error (deliberate or unintentional) and malicious attacks by third parties (Burke et al., 2019). For example, during the international Coronavirus response, 'Password Spraying' techniques were used in an attempt to gain access to healthcare provider networks (National Cyber Security Centre, 2020).

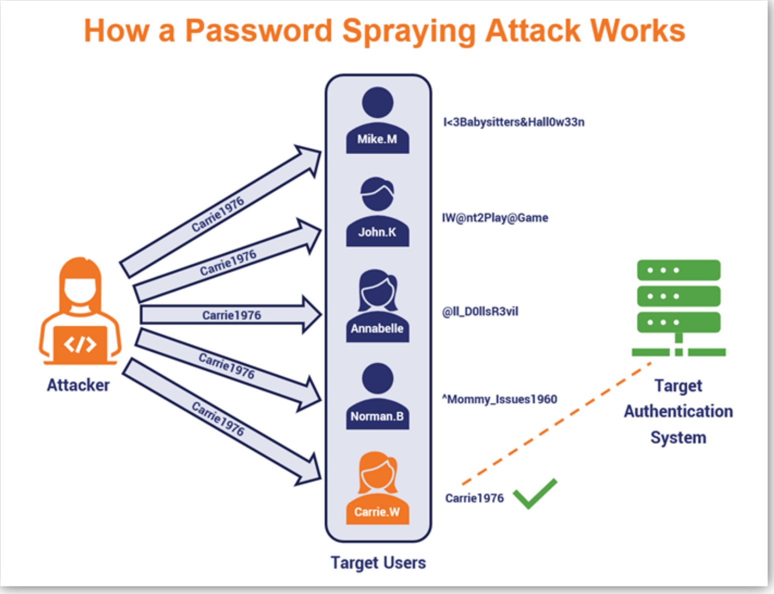


Figure 1: How a Password Spraying Attack Works (Crane, 2021).

Although the healthcare sector accounts for 79% of all reported data breaches in 2020 (Davis, 2021), a Finnish study states that e-Health provides a significant opportunity to increase security & privacy compared to standard paper-based systems (Rajamäki & Pirinen, 2017).

2. List of Security Challenges

There are many challenges in terms of security that may affect any business with an online presence and others specific to the e-Health industry. The following list is a compilation of the most important ones:

1. **Healthcare data and infrastructure are migrating to the cloud**: Predictions are that up to 80% of data from the Healthcare industry will have migrated to a Cloud-based solution (Diana, 2014). Records should be correctly set up and encrypted, as often, patient records are the final goal of these attacks (Kolbasuk McGee, 2016).

2. **Cybersecurity professional shortage**: By 2019, the Cybersecurity professional shortage was around two million (Gartner, n.d.). Due to increased attacks during the pandemic, infosec professionals have become more necessary to business functions (Culbertson, 2021).

3. **Skills needed for Cybersecurity are widening**: As innovative technologies, devices and systems emerge, the risk of vulnerabilities and threats increases. The skills required to patch and diagnose these issues could surpass the capacity to train new professionals (World Economic Forum, 2020)

4. **Outdated technology in Hospitals**: In 2014, US hospitals spent around two hundred million dollars on administrative matters (George Washington University, 2021). Although patient treatment is their primary concern, there should be a focus on ensuring software is updated to prevent vulnerabilities and maintain system security.

3. Tools

Several tools have been evaluated for this proposal, considering the budget and the time available to perform the tests. While some tools provide remarkably similar functionality, they often use different algorithms or search strings, affecting overall efficiency. For example, one can be better at detecting XSS while the other can be more efficient to detect SQL Injection for one specific target (Mohammed, 2016). The following list describes the rationale behind the tool selection:

- **Kali Linux/Parrot OS:** Both operating systems contain a vast repository of penetration testing tools specifically designed for penetration testing.

- **Nmap:** NMap will be used to perform data-gathering exercises, including Port Scanning, OS Detection and Software Version Identification (Petters, 2020) on the host machine. NMap will be used due to its comprehensive support within the penetration testing community.

- **Metasploit:** Metasploit is a widely used penetration testing framework. We have chosen to use this due to the sizeable open-source following and vulnerability repositories within the software.

- **Nikto:** Nikto is a powerful vulnerability scanner that can be used to perform automated tests on websites. As standard, Nikto includes tools for port scanning, host authentication and subdomain guessing.

- **ZAP (OWASP Zed Attack Proxy)**: The ZAP utility provides automated scanning to identify the vulnerabilities covered in the OWASP 10. This utility has been chosen due to its automated nature and open-source following.

- **Burp Suite Community:** The Burp Suite is a powerful interception proxy, allowing penetration testers to identify potentially unintended application behaviours, crashes or error messages (PenTestGeek, n.d.).

4. Methodology

A series of remote scans will be conducted against the e-Health site during our penetration testing exercise. As a time-saving measure, automated tools will be used for initial scans, whilst a series of manual tools will be used to identify further and confirm any identified vulnerabilities.

We will be utilising the Black-box software testing method, which focuses on identifying vulnerabilities without prior knowledge of how it works internally (Imperva, n.d.). Black-box testing is a method recommended by the UK's National Cybersecurity Centre (2017) as it accurately reflects the threats likely to be faced from external attackers, as would be the case in the e-Health sector.

The Threat Risk Modelling framework we will be utilising is the widely-used Common Vulnerability Scoring System (CVSS), which provides an overall score allowing the risks to be ranked by severity (Pande, 2009). The CVSS scoring system has been chosen over other modelling techniques such as STAR, STRIDE, and DREAD. It is widely used within industry and is supported by the UK National Cyber Security Centre (2016).

5. Business Impacts

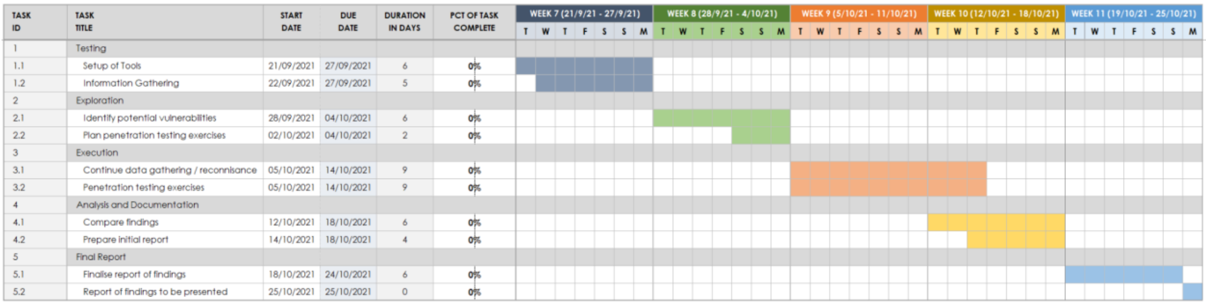
As this penetration test is being performed against an active e-Health site; we will ensure that the following steps are adhered to:

- Any attacks/scanning performed will not result in the modification of existing client data.
- Attacks that are likely to cause disruption and downtime are only completed outside of typical peak hours, with prior approval from the owners of the e-Health site.
- Volumes of traffic will be limited to avoid flooding the bandwidth or resources of the site or associated system(s) (Wikipedia, n.d.).

6. Timeline

In accordance with the timescales displayed in Figure 2, the below stages will be completed during the penetration testing exercise:

- **Testing:** All tools will be set up, with preliminary testing being undertaken against the target.
- **Exploration:** Further exploration based upon the preliminary testing.
- **Execution:** Thorough scanning and testing will be performed against the potential vulnerabilities identified during the exploration stage.
- **Analysis and Documentation**: Findings from the execution stage will be documented ready for analysis.
- **Final report:** A final report will be presented to the owners of the e-Health site, containing the findings from our penetration test, as well as remediation measures to be undertaken.



TASK ID	TASK TITLE	START DATE	DUE DATE	DURATION IN DAYS	PCT OF TASK COMPLETE
1	Testing				
1.1	Setup of Tools	21/09/2021	27/09/2021	6	0%
1.2	Information Gathering	22/09/2021	27/09/2021	5	0%
2	Exploration				
2.1	Identify potential vulnerabilities	28/09/2021	04/10/2021	6	0%
2.2	Plan penetration testing exercises	02/10/2021	04/10/2021	2	0%
3	Execution				
3.1	Continue data gathering / reconnisance	05/10/2021	14/10/2021	9	0%
3.2	Penetration testing exercises	05/10/2021	14/10/2021	9	0%
4	Analysis and Documentation				
4.1	Compare findings	12/10/2021	18/10/2021	6	0%
4.2	Prepare initial report	14/10/2021	18/10/2021	4	0%
5	Final Report				
5.1	Finalise report of findings	18/10/2021	24/10/2021	6	0%
5.2	Report of findings to be presented	25/10/2021	25/10/2021	0	0%

WEEK 7 (21/9/21 - 27/9/21)
WEEK 8 (28/9/21 - 4/10/21)
WEEK 9 (5/10/21 - 11/10/21)
WEEK 10 (12/10/21 - 18/10/21)
WEEK 11 (19/10/21 - 25/10/21)
T W T F S S M

Figure 2: Gantt Chart of project timescales

7. Assumptions

When performing penetration testing exercises against the e-Health site, the following assumptions have been made:

- **DDoS vulnerability:** The site is vulnerable to Layer 4 and 7 attacks. As per Amazon policy (n.d.), we require prior authorisation to perform network stress tests with abnormal data volumes.

- **Network Security:** The network and infrastructure containing the site are otherwise secure, preventing malicious actors from carrying out exploits and threats from elsewhere within the business (Cisco, n.d.).

8. References

Amazon. (n.d.) Amazon EC2 Testing Policy. Available from: https://aws.amazon.com/ec2/testing/ [Accessed 19th September 2021].

Burke, W. et al. (2019) *Cybersecurity Indexes for eHealth.* Available from: https://dl.acm.org/doi/abs/10.1145/3290688.3290721 [Accessed 19th September 2021].

Cisco. (n.d.) What is network security?. Available from: https://www.cisco.com/c/en_uk/products/security/what-is-network-security.html [Accessed 19th September 2021].

Crane, C. (2021) A Brute Force Attack Definition & Look at How Brute Force Works. Available from: https://www.thesslstore.com/blog/brute-force-attack-definition-how-brute-force-works/ [Accessed 19th September 2021].

Culbertson, N. (2021) Increased Cyberattacks on Healthcare Institutions Shows the Need for Greater Cybersecurity. Available from: https://www.forbes.com/sites/forbestechcouncil/2021/06/07/increased-cyberattacks-on-healthcare-institutions-shows-the-need-for-greater-cybersecurity/?sh=26fb54c25650 [Accessed 12th September 2021]

Davis, J. (2021) Healthcare Accounts for 79% of All Reported Breaches, Attacks Rise 45%. Available from: https://healthitsecurity.com/news/healthcare-accounts-for-79-of-all-reported-breaches-attacks-rise-45 [Accessed 19th September 2021].

Diana, A. (2014) Cloud Gains Traction in Healthcare. Available from: https://www.informationweek.com/healthcare/cloud-gains-traction-in-healthcare [Accessed 12th September 2021]

Gartner (n.d.) Cybersecurity Labor Shortage and COVID-19. Available from: https://www.gartner.com/en/human-resources/research/talentneuron/labor-market-trends/cybersecurity-labor-shortage-and-covid-19 [Accessed 12th September 2021]

Imperva. (n.d.) Black Box Testing. Available from: https://www.imperva.com/learn/application-security/black-box-testing/ [Accessed 19th September 2021].

Kolbasuk McGee, M. (2016) Research Reveals Why Hacked Patient Records Are So Valuable. Available from: https://www.databreachtoday.com/interviews/research-reveals-hacked-patient-records-are-so-valuable-i-3341 [Accessed 12th September 2021]

Mohammed, R., 2016. Assessment of web scanner tools. *International Journal of Computer Applications*, *133*(5), pp.1-4.

National Cyber Security Centre. (2016) Vulnerability management. Available from: https://www.ncsc.gov.uk/guidance/vulnerability-management [Accessed 19th September 2021].

National Cyber Security Centre. (2017) Penetration Testing. Available from: https://www.ncsc.gov.uk/guidance/penetration-testing [Accessed 19th September 2021].

National Cyber Security Centre. (2020) Cyber warning issued for key healthcare organisations in UK and USA. Available from: https://www.ncsc.gov.uk/news/warning-issued-uk-usa-healthcare-organisations [Accessed Sunday 19th September 2021].

Pande, R. (2009) Risk Modeling. Available from: https://owasp.org/www-pdf-archive/OWASP_miami_Risk_Modeling_v2-2009_06.pdf [Accessed 19th September 2021].

PenTestGeek. (n.d.) What is burp suite? Available from: https://www.pentestgeek.com/what-is-burpsuite [Accessed 19th September 2021].

Petters, J. (2020) NMap Commands. Available from: https://www.varonis.com/blog/nmap-commands/ [Accessed 19th September 2021].

Rajamäki, J. Pirinen, R. (2017) Design science research towards resilient cyber-physical eHealth systems. *Finnish Journal of eHealth and eWelfare* 9(2-3):203-216. DOI: https://doi.org/10.23996/fjhw.61000

The George Washington University (2021) The Top Costs Associated with Running a hospital. Available from: https://healthcaremba.gwu.edu/blog/the-top-costs-associated-with-running-a-hospital/ [Accessed 12th September 2021]

Wikipedia. (n.d.) Denial-of-service attack. Available from: https://en.wikipedia.org/wiki/Denial-of-service_attack [Accessed 19th September 2021].

World Economic Forum (2020) *Future Series: Cybersecurity, emerging technology and systemic risk.* Available from: http://www3.weforum.org/docs/WEF_Future_Series_Cybersecurity_emerging_technology_and_systemic_risk_2020.pdf [Accessed 12th September 2021]