Development Team Project:

A design document/proposal of a Network and Information Security Management (NISM) Assessment Project.

MSc Cyber Security
Module 2, Unit 6 Submission
1043 words

Introduction

This document outlines the process for an agreed penetration test for the target e-commerce website. This document provides insight into the potential challenges, the methodology that will be used and any potential business impacts. One of the benefits of a security assessment is to understand and prove the effectiveness of existing security controls in order to ensure the business is getting good return on investment (Tang, 2014). With this, an unbiased review can be taken of said website, identifying the vulnerabilities at risk of exploitation and providing remediation plans for each risk.

Security Challenges

Considerations need to be made regarding the motivations for an attacker to target an e-commerce site, and reflect this in the security challenges faced. For example, an attacker may use or sell stolen credit card information for profit, identity theft or extortion. There may also be higher levels of threat from said attackers at key commerce times of the year such as Black Friday or Christmas. One example of this would be the Target data breach occuring in November 2013 with an impact of $18.5M (Mccoy, 2018).

Challenges could include unauthorised access to data resulting in potential regulatory fines (confidentiality), tampering with data in terms of deletion or editing (integrity) and also the website or sub-domain of the website not being accessible for a period of time (availability). More specifically to an e-commerce website, other challenges include protection of card data in line with PCI-DSS and protection of personal data in line with GDPR, both of which can enforce large fines if data is handled incorrectly. Other challenges could also include, Distributed Denial of Service (DDoS) attacks, e-skimming, data theft and weak passwords.

STRIDE Category	Example - General	Example - e-Commerce
Spoofing	An attacker accesses a customer account using harvested credentials.	An attacker sets up a phishing site to harvest customer credentials through cybersquatting on a similar domain name to the target.
Tampering	An attacker uses an injection attack to execute malicious database commands.	An attacker compromises a client-side third party shopping cart script to harvest customer payment details.
Repudiation	An attacker deletes unprotected log files to remove evidence of malicious activity.	An attacker makes fraudulent orders through accessing genuine customer account.
Information Disclosure	An attacker harvests sensitive customer data over unencrypted HTTP connection.	An attacker exfiltrates sensitive customer data via a misconfigured storage bucket or database.
Denial of Service	An attacker launches a ransomware attack on the web server hosting the website.	An attacker uses a botnet to perform a Distributed Denial of Service (DDoS) attack.
Elevation of Privilege	An attacker brute forces access to an administrator account.	An attacker takes over a customer account via session hijacking.

Image 1

Image 1 shows examples of both general and industry specific threats that could be realised through the exploitation of vulnerabilities (Microsoft, 2007; OWASP, 2020). Therefore, vulnerabilities need to be identified and appropriately managed to protect the business and its customers. Critical vulnerabilities that enable numerous threats, such as elevation of privilege, should be shared with the business immediately during the test in order to ensure there is no undue delay in the business managing the associated risk (Tang, 2014).

Assessment

Methodology

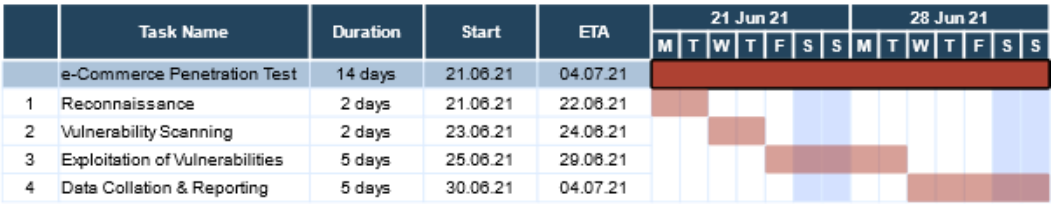

Figure 1

The two week test will be split into the four stages highlighted in Figure 1. Whilst this diagram is a guide for the linear process, some iteration may be required to ensure thorough testing (McNab, 2016).

The purpose of a penetration test is to simulate genuine attacks that could be launched against the target (Satria et al., 2020). Therefore, the team will be following the Cyber Kill Chain to exploit vulnerabilities in order to ensure the website is tested in line with the techniques of genuine adversaries. The team will utilise automatic tools to discover key vulnerabilities and areas of interest in Steps 1 and 2, then use a mix of automation and manual technique to validate the vulnerabilities in Step 3. This test will be completed remotely to further simulate an adversary, most of whom would be looking to breach websites remotely. The output of Step 4 will be an executive summary covering vulnerabilities found, their severity and a prioritised list of recommendations, taking into consideration an assessment against relevant security standards.

We will also be adhering to and reviewing the potential vulnerabilities in line with the following Information Security Standards:

1. Payment Card Industry Data Security Standard (PCI DSS) – due to handling of payments through the website.
2. ISO27001 – international and versatile standard for information security.
3. General Data Protection Regulation (GDPR) – due to handling of PII as part of orders and transactions on the website.

Not only are regular penetration tests mandated by some standards and regulations, but they can also lead to the recommendation of suitable security controls to address any areas where the website falls short of these (IT Governance, N.D.; PCISSC, 2018). Overall, this results in the avoidance of potentially heavy fines and reputational damage associated with breaches (Fruhlinger, 2020).

Tools

As part of the assessment, multiple different tools will be utilised to identify the potential security challenges. Each tool has been selected to identify the security challenges mentioned previously; however, the main tool used will be Kali Linux. This is a free tool specifically built for penetration testing and digital forensics, for example, SQLmap to test for SQL injection and Nmap for scanning of the network. Other tools as listed below will also be used to help enrich the data found using Kali Linux:

1. Netsparker - used to exploit vulnerabilities in a safe environment.
2. Metasploit - used to test for the presence of vulnerabilities.
3. Burpsuite - used for dynamic application security testing (DAST).
4. Nessus - also used to test for the presence of vulnerabilities.

We use a variety of tools, since they come with limitations. Some are for example particularly strong in scanning for XSS exploits whilst others are very good for SQL injection. By using different tools we will effectively overcome the weakness of certain tools by using the strengths of another tool.

Business Impacts

To ensure minimal impact to the business, the assessment will be conducted within particular parameters, such as:

- Using agreed tools and gaining consent from the hosting provider and the client.
- Ensuring there is no lasting damage conducted on the website, only showing what could be done instead of conducting real-time attacks.

An assumption is that this e-commerce website is available 24/7 (Inyang-Etoh, 2016). As such, testing will occur during known low traffic times of the day to avoid any potential customer or service impact. However, contact details will be provided to the client in case impact is seen and the client has been advised to notify the teams undertaking security monitoring of the website and surrounding infrastructure of the test taking place (Tang, 2014). To avoid any potential issues with business operations, activities will not be completed outside of the agreed time schedule.

Conclusion

This security assessment will help benchmark the website against known security standards and help focus the time and effort on what needs to be remediated. By following the four stage process and working within the agreed parameters, this assessment will help to identify any potential vulnerabilities and risks that could result in reputational damage if exploited. All security challenges will be considered when conducting the assessment and will be used to determine the effective level of controls.

References

Tang, A. (2014) A guide to penetration testing. *Network Security* 2014(8): 8-11.

Microsoft (2007) STRIDE chart. Available from: https://www.microsoft.com/security/blog/2007/09/11/stride-chart/ [Accessed 6 June 2021].

OWASP (2020) OWASP Top Ten. Available from: https://owasp.org/www-project-top-ten/ [Accessed 12 June 2021].

IT Governance (N.D.) ISO 27001 Penetration Testing. Available from: https://www.itgovernance.co.uk/iso27001_pen_testing [Accessed 6 June 2021].

PCISSC (2018) Payment Card Industry (PCI) Data Security Standard. Available from https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf? [Accessed 6 June 2021].

Fruhlinger, J. (2020) PCI DSS explained: Requirements, fines, and steps to compliance. Available from: https://www.csoonline.com/article/3566072/pci-dss-explained-requirements-fines-and-steps-to-compliance.html [Accessed 6 June 2021].

Inyang-Etoh, D. (2016) Deploying eCommerce Solutions with Cloud and Open Source Technologies: High Availability Application Models. *Computing and Information Systems Journal* 20(2): 15-26.

Satria, D., Alanda, A., Erianda, A. & Prayama, D. (2020) Network Security Assessment Using Internal Network Penetration Testing Methodology. International Journal on Informatics Visualization 2(4-2): 360-365.

McNab, C. (2016) *Network Security Assessment: Know Your Network.* 3rd ed. O'Reilly Media.

Mccoy, K. (2018) Target to pay $18.5M for 2013 data breach that affected 41 million consumers. Available from: https://eu.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/ [Accessed 10 June 2021].