A design proposal for the penetration testing of a Customer Management System

Network and Information Security Management

MSc Cyber Security

Group Three

Beran Necat

University of Essex

18 April 2022

Introduction

Penetration testing provides entities with proof of any security weaknesses within their IT systems and infrastructure which can be exploited by threat actors as well as the potential impacts to the organisation (Tang, 2014). This proposal outlines the scope for an agreed penetration test for the Customer Relationship Management (CRM) website, *www.customersrus.co.uk*, including relevant regulations, security challenges; vulnerabilities and mitigations.

Regulations

CRM is a set of ideas and principles that helps businesses engage and connect with customers and their data. Organisations are moving their customers' data to the cloud and using CRM platforms such as Salesforce, and Dynamics 365 (Martin, 2010). Although these services offer valuable business tools for organisations and stakeholders, threat actors value this data too. According to Sreenivasan (2022), there had been 454 data breaches and roughly 12.7 million records exposed in 2016.

Regulatory compliance and professional standards have been implemented in the United Kingdom to help organisations secure their IT processes and protect customers' data.

The International Organisation for Standards (ISO) regularly reviews ISO 27000 which requires entities to secure and manage information security management system assets such as financial information, users' data, and connected third parties (ISO, 2013).

The Information Commissioner's Office (2022) oversees regulation related to Data Protection Act 2018 and General Data Protection Act 2016 among others. In brief, Article 32 of GDPR stipulates organisations must do the following:

1. Anonymise and encrypt personal data
2. Ensure resilience, Confidentiality, Integrity, and Availability
3. Restore access and availability resulting from technical or physical failure
4. Test, evaluate, and assess technical and organisational effectiveness and security of processing

The Payment Card Industry Data Security Standard (PCI DSS) ensures payment card account data security. Merchant or service providers, such as a CRM, must comply with PCI DSS (PCI DSS, 2022), as most CRMs require monthly subscriptions per user (Goldstein, 2022). Although PCI DSS is not considered a law, but a standard, payment brands can fine acquiring banks for violating the compliance while the acquiring banks can ban card payments through non-compliant merchants. Data breach and theft are also considered a breach of the GDPR, resulting in penalties (itgovernance, 2022).

Security Challenges

Table 1 highlights observable vulnerabilities found on the CRM webpage.

Target web page vulnerabilities
The website uses SugarCRM Community Edition which stopped in 2013. Multiple vulnerabilities have been found since.
The website uses Jquery 1.8 while the latest version is 3.6.
The website is hosted on a shared server. Possible scans may be affected by other web pages on server
Uncertainty regarding Cpanel and domain access security (weak passwords)
Exposed links – Employees and About. To be made visible only after logging in.

Table 1. Observable web page vulnerabilities

This can be further analysed using a STRIDE threat model to discover how these vulnerabilities can be exploited (see Table 2).

STRIDE area	Possible threat
Spoofing	Access to login credentials through malicious email, evil twin, man-in-middle attacks, and poor authorisation checks
Tampering	Modifying and deleting of users records and data on database
Repudiation	Using stolen credentials to mask access to sensitive data
Information disclosure	Disclosing confidential organisational and personal data such as banking details and addresses
Denial of Service	Denying access to web portal or server-side databases through ransomware or Denial-of-Service attacks
Elevation of Privilege	Authorising commands, systems, and processes such as deleting data via phishing or session hijacking

Table 2. CRM STRIDE Threat Model (Wadhwa, 2020)

Mitigation Suggestions

Based on Tables 1 and 2, these threats can be mitigated by following some steps:

1. Use of VPN
    - Hides the IP address.
    - Encrypts data during transmission, which makes the process harder for attackers (Irwin, 2021).

2. Only HTTPS Website Visits
    - Encrypts data (Irwin, 2021).

3. Education on Identifying Phishing Scams (Kaspersky, 2022).
    - Helps take immediate action against these scams (Kaspersky, 2022).

4. Limit Data Access
    - Reduces risk of exploitation without affecting the organisation's overall productivity (Cypress Data Defense, 2020).

5. Use of Multi-Factor Authentication (MFA)
    - Ensures a more complex process of accessing users' accounts, as cracking the password is not enough (Cypress Data Defense, 2020).

6. Strong Passwords (i.e., long, and complex)
    - Aids in mitigating brute-force attacks, which can cause data breaches or unauthorised access (OAIC, N.D.).

7. Use of Anti-Malware Software (Cypress Data Defense, 2020).
    - Builds solid foundation of security for devices (Cypress Data Defense, 2020).

8. Keep Operating Systems, Applications and Software Up to Date (CIS, 2020).

9. Use Firewall and Routers
    - Configured Firewalls and Routers to reject suspicious traffic (Rafter, 2022).

Methodology

The ISSAF penetration testing standard will be used for the methodology. The standard comprises of three phases: planning and preparation, assessment, and reporting (Abu-Dabaseh, Alshammari, 2018).

During the planning and preparation phase, information required for the assessment is gathered including among other threats of interest and the operational environment of the website. The initial project management phases of the assignment are also addressed including issues such as the scope of the assignment as well as roles and responsibilities of the team members involved.

The second phase's main objective is to identify vulnerabilities and validate them. For this phase, Group three will use Kali Linux tools namely NMAP for reconnaissance to discover the network and vulnerabilities, and Metasploit for deep scanning and validation of the vulnerabilities discovered by NMAP. Upon completion of the assessment phase, systems, and networks as well as organisational processes' weaknesses will be identified.

The last phase involves analysis of the vulnerabilities identified during the second phase to determine the root causes, establish mitigation of such and preparation of the report about the findings. Clean-up of the website for any testing residue if any will also be undertaken during this phase.

Tools

The following Kali Linux tools:

1. NMAP - for scanning open ports and vulnerabilities of the website during the initial phase of the penetration tests.
2. Metasploit - for validating the results of the NMAP scan.
3. Burp Suite - for the penetration test of the web application.
4. John the Ripper - for ensuring the password hashes are stored securely.

Conclusion

Although investing in CRMs will undoubtedly enhance the sales and profits of a business (DAAS Suite, 2022) and offer many advantages to small businesses as well (McNeice, 2021), potential security risks often follow along. In this proposal, a three-step process will be used to help discover potential and present vulnerabilities in the CRM web page, *www.customersrus.co.uk*. By following this approach and using Kali Linux penetration testing software, potential risks which could cause data breaches, financial theft, and loss of reputation to all stakeholders can be mitigated.

References:

Abu-Dabaseh, F., & Alshammari, E. (2018) Automated Penetration Testing: An Overview. *Computer Science and Information Technology* (1)1: 121-129.

CIS (2020) 7 Steps to Help Prevent & Limit the Impact of Ransomware. Available from: https://www.cisecurity.org/insights/blog/7-steps-to-help-prevent-limit-the-impact-of-ransomware [Accessed 6 April 2022].

Cypress Data Defense (2020) How to Protect Your Data From Unauthorized Access. Available from: https://www.cypressdatadefense.com/blog/unauthorized-data-access/ [Accessed 6 April 2022].

DAAS Suite. (2022) 5 Major Reasons to Invest in CRM. Available from: https://daassuite.com/blog/en/reasons-invest-crm/ [Accessed 12 April 2022].

Goldstein, B. (2022) How much does CRM cost? Available from: https://www.nutshell.com/blog/how-much-does-crm-cost [Accessed 7 April 2022].

Information Commissioner's Office (ICO). (2022) Security. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/?msclkid=27987d5cb4ce11ec82fd05fd8a46bc23 [Accessed 5 Apr. 2022].

Irwin, L. (2021) How to defend against man-in-the-middle attacks. Available from: https://www.itgovernance.eu/blog/en/how-to-defend-against-man-in-the-middle-attacks [Accessed 6 April 2022].

International Organisation for Standardisation (ISO). (2013) ISO/IEC 27001 Information security management. Available from: https://www.iso.org/isoiec-27001-information-security.html.

Itgovernance. (2022) The PCI DSS (Payment Card Industry Data Security Standard). Available from: https://www.itgovernance.co.uk/pci_dss [Accessed 7 April 2022].

Kaspersky (2022) All About Phishing Scams & Prevention: What You Need to Know. Available from: https://www.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips [Accessed 6 April 2022].

Martin, J. (2010) Put Cloud CRM to Work. Available from: https://www.pcworld.com/article/511929/put_cloud_crm_to_work.html [Accessed 5 Apr. 2022].

McNeice, K. (2021) Is CRM Software Worth the Investment for Small Businesses?. Available from: https://www.accelo.com/resources/blog/is-crm-software-worth-the-investment-for-small-businesses/ [Accessed 12 April 2022].

National Cyber Security Centre (2017) Penetration Testing. Available from: https://www.ncsc.gov.uk/guidance/penetration-testing [Accessed 6 April 2022].

Office of the Australian Information Commissioner (OAIC). (N.D.) Preventing Data Breaches: Advice From the Australian Cyber Security Centre. Available from: https://www.oaic.gov.au/privacy/notifiable-data-breaches/preventing-data-breaches-advice-from-the-australian-cyber-security-centre [Accessed 6 April 2022].

Payment Card Industry Data Security Standard (PCI DSS). (2022) Payment Card Industry Data Security Standard: Requirements and Testing Procedures. Available from: https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf?agreement=true&time=1649346483700 [Accessed 7 April 2022].

Rafter, D. (2022) What are Denial of Service (DoS) attacks? DoS attacks explained. Available from: https://us.norton.com/internetsecurity-emerging-threats-dos-attacks-explained.html [Accessed 6 April 2022].

Sreenivasan, S. (2022) How to Secure Your CRM (Customer Relationship Management) Data From Hackers. Available from: https://en.cloudbric.com/blog/2018/01/secure-crm-data-hackers/?msclkid=83d8f15eb4a311ec99985ff46b10c90f [Accessed 5 Apr. 2022].

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

Wadhwa, M. (2020) How to think about security and threats in your distributed application. Available from: https://www.ockam.io/learn/blog/introduction_to_STRIDE_security_model?msclkid=5be31241b4db11ec86f132b0c07cba9f [Accessed 5 Apr. 2022].