Final Report: Penetration Testing Activities for Jacaranda Health

Executive Summary

The penetration test on Jacaranda Health's digital systems was conducted over the course of four weeks, commencing on June 16th, 2023, and concluding on July 14th, 2023. The testing team (Ian Peter) utilized the Open-Source Security Testing Methodology Manual (OSSTMM) framework to assess potential vulnerabilities and weaknesses within the client's information systems.

The objective of this penetration testing exercise was to identify vulnerabilities, misconfigurations, and weak security practices in Jacaranda Health's information technology infrastructure. Our methodologies followed industry-accepted best practices and focused on key areas identified during the initial scope discussion.

The findings suggest that while Jacaranda Health has implemented several solid security measures, there are areas of concern that need to be addressed to further enhance the security posture of the organization. These areas primarily relate to user access management, system configurations, and data security.

Contents

Introduction

Jacaranda Health's digital systems encompass several AWS services, a Windows server, API instances for Quicksight, the website scorecard.jhtools.org managed by Google Firebase, an App Runner, and more. The comprehensive nature of the client's digital ecosystem necessitated a detailed and exhaustive penetration test to ensure the systems' robustness against potential cyber threats.

Findings Summary

The testing team employed a combination of automated tools and manual techniques to conduct the penetration test. This multi-pronged approach allowed for a more comprehensive assessment of potential vulnerabilities within the client's systems.

Information Gathering

Open-Source Intelligence (OSINT)

During the initial phase of the testing, the team conducted thorough research to collect as much information as possible about the target systems. Open-Source Intelligence (OSINT) techniques were utilized to find any publicly available information that could potentially be used for nefarious purposes.

Using OSINT, the testing team gathered plenty of information about the organization using Google Dorking as the main technique:

- Two main domains were identified, www.jacarandahealth.org and https://prompts.jacarandahealth.org/.
- Old accounts used for social media (Flickr) and Job Advertisement postings.
- Notable Articles detailing partnerships and AWS services in use at Jacaranda Health.
- The main organizational website is hosted on Cloudflare while the Prompts platform utilizes AWS services, indicating a hybrid cloud infrastructure.
- Google mail servers' presence in MX records indicate use of Google Technologies within the organization. This can be seen in the following file: https://docs.google.com/document/d/10BpfI1XIBD1mXsVpObU0eyDjo4X-W9Ir/edit?usp=drive_link

Jacaranda Health has already demonstrated some commendable security practices that have effectively minimized their attack surface from an OSINT perspective which include:

1. **Limited Online Footprint**: The discovery of certain integrations such as jhtools was difficult using OSINT techniques alone, which is commendable. IP addresses associated with instances and other AWS resources were also not easily visible, indicating a strong control over information exposure.

2. **Secure Configuration**: The OSINT assessment did not uncover any major security misconfigurations or vulnerabilities in the publicly available systems or services. This suggests that proper security controls are implemented in the services currently being used by Jacaranda Health.

The full report for Information Gathering using OSINT can be found at https://docs.google.com/document/d/1MWXgpf0Z8Kulppn7zOd-wzOYoBsjxqPG/edit?usp=drive_link&ouid=105333431447822856661&rtpof=true&sd=true

Enumeration

Following the initial reconnaissance phase, the team conducted a comprehensive enumeration process to identify and understand the various assets and services used by Jacaranda Health including those discovered during the Information Gathering stage and any further systems discovered.

Nmap Enumeration

Based on the nmap scan reports, the enumeration process discovered several key details about the infrastructure of Jacaranda Health:

scorecard.jhtools.org (Netlify Hosted)

- The host is active and hosted on Netlify, with most of its ports filtered for security.
- Ports 80 (HTTP) and 443 (HTTPS) are open for serving web content.
- The server has a valid SSL certificate issued by DigiCert Inc. for the domain ***.netlify.app**.
- A single account used for access has been noted for the platform.
- Several deployed projects that are over 3 years old are found and might present future vulnerabilities due to outdated technologies.

EC2 Instance

- The Ubuntu server running on Amazon EC2 has Secure Shell (SSH) as the only detected open service.

Windows Server 2019

- This server is running several Microsoft services, with Microsoft SQL Server 2019 and a custom web software service called Sage 3000 noted.
- The server has RDP port 3389 exposed on the public internet.
- The server uses self-signed SSL certificates for certain ports, indicating it might be a test or development environment.
- Most ports are filtered, suggesting the implementation of firewall or other security measures.

Potential Attack Vectors

Based on the information collected during the enumeration process, the potential attack vectors include:

- Exploring common web application vulnerabilities, such as XSS, SQL Injection, CSRF, etc.
- Enumerating other applications hosted on Netlify.
- Searching for valid credentials on communication platforms like Slack.
- Looking for vulnerabilities in the services running on Windows Server 2019 especially outdated services.

The full report can be found here:

https://docs.google.com/document/d/1gb_o88XfPrzdEl89zS3awo4jmo7WnruQ/edit?usp=drive_link&ouid=105333431447822856661&rtpof=true&sd=true

Amazon Web Services (AWS)

The purpose of the testing within the Amazon Web Services (AWS) environment, according to the shared responsibilities model of cloud security, was to analyze account management and access controls already in place in both the IAM console and various utilized services.

The enumeration process was conducted mainly through manual inspection and by leveraging both AWS's in-built services and external tools. The testing team used AWS's in-built service, the Credential Manager, to identify and manage user access and permissions across the organization's AWS services. The Credential Manager provided a centralized view of the user accounts and their associated permissions, which allowed us to assess the organization's user access management practices effectively.

In addition to the in-built tools, the testing team also employed boto3, the Amazon Web Services (AWS) Software Development Kit (SDK) for Python. boto3 allowed the testing team to directly interact with AWS services, making the enumeration process more efficient and comprehensive. With boto3, the testing team was able to write scripts that could fetch detailed information about each service, groups and users thereby providing a more granular view of the organization's AWS environment.

The team's analysis exposed several areas of concern related to AWS configurations and user management:

1. **Multifactor authentication (MFA)** has not been enabled for all AWS Users, thereby opening potential avenues for unauthorized access.
2. **Older user accounts** remain active, potentially posing a security risk if compromised due to inadequate monitoring or management. They essentially increase the attack surface.
3. **Shared accounts with extensive permissions**, like the "jhteam" account, present a significant security risk due to their increased exposure and potential misuse.
4. Certain user groups such as Tech_Data and Exec_HOD have **no permissions set**, creating a lack of clarity about their roles and the data they can access.

5. For groups such as **EC2-admin and S3FullAccess, permissions should be broken down into smaller, role-specific groups to avoid excessive access rights**. This is crucial considering that certain services are not regularly accessed.

6. There exists an **Admin** group with Administrator privileges similar to that of the root user.

7. The root user account is in regular use, which is against AWS best practice.

The full findings of the AWS Report can be found here:
https://docs.google.com/document/d/10455ePzWP2jv1wRGVe2BPnV2Xqt39oaQ/edit?usp=sharing&ouid=105333431447822856661&rtpof=true&sd=true

Recommendations

Based on our findings, the testing team recommends the following actions:

Nmap Enumeration

1. Implementing more secure password sharing methods **(Bitwarden Share)**, stronger passwords, and Two-Factor Authentication.

2. Shifting from a shared account to individual accounts for platform access for better control and auditing of actions performed on the platform.

3. Disabling outdated platforms to avoid future vulnerabilities.

4. Implementing stricter firewall rules, updating, and patching systems regularly, and securing SQL Server.

5. Reviewing and securing the services running on Windows Server 2019, especially the Sage 3000 web app.

6. Purchasing a premium account on the Netlify platform for better control over security.

7. Reviewing the EC2 Instance Configurations and possibly implementing network segmentation.

8. On the Windows Server 2019, disable RDP access via the public Internet and restrict access to this service to trusted IPs or via a VPN.

Open-Source Intelligence (OSINT)

1. **Disabling Old Accounts**: To minimize the attack surface and limit the exposure of information available to an attacker, it is highly recommended to disable old accounts, specifically old WordPress site and Flickr accounts, if no longer in use.

2. **Limiting Data Exposure**: Ensure that none of the accounts on the platforms expose sensitive data, and only the necessary information is made available to advertise the job postings on the job posting accounts.

3. **Multifactor Authentication**: To enhance security, enable multifactor authentication for the accounts used to manage the exposed platforms.

4. **Review of Compliance Documents**: A thorough review of compliance documents should be done to ensure that third-party platforms managing Jacaranda Health infrastructure such as Ona are compliant with user data protection standards and regularly undergo security audits.

5. **Deactivating Damu-Sasa Associated Accounts**: Given the apparent poor security controls in place with the Damu-Sasa platform, it is recommended to immediately deactivate any accounts associated with this platform to mitigate potential risks.

Amazon Web Services (AWS)

- Enable multifactor authentication (MFA) for all AWS users.
- Older user accounts that are no longer in use should be deactivated to minimize the potential attack surface.
- Implement a centralized and secure solution for log storage and management stored outside of the AWS environment to track and monitor activities better across the AWS environment.
- Deactivate the internally shared "jhteam" account and issue individual accounts to each of the users for better auditing of activities on the platform.
- Regularly review user group permissions to ensure they match the roles of the group's members.
- The permissions of the EC2-admin and S3FullAccess groups should be divided into smaller, role-specific groups to better control access and reduce security risks.
- Conduct a thorough review and redesign of the user groups based on services needed by each user and group.
- Regularly rotate passwords and enforce a strong password policy across all user accounts.
- Audit user account activity and permissions regularly, making sure that the PLP is consistently enforced.
- Regularly rotate access keys, especially for accounts with elevated privileges.
- Avoid using the root user account for daily activities. Create specific IAM roles for tasks currently performed by the root account, limiting its use to tasks that require root privileges only.

General Recommendations

- Conduct security awareness training on a regular basis for all staff members. The training should focus on the understanding of the risks and responsibilities associated with their roles.
- Enable AWS CloudTrail to track and log user activity on the platform. Regular auditing of the logs will help detect any unusual or unauthorized activities.
- Regular penetration testing exercises should be conducted to identify and rectify security weaknesses in the infrastructure.
- Implement a robust key management policy that includes secure storage and regular rotation of keys.

- Access to specific S3 buckets containing sensitive personal data should be further limited by establishing and enforcing strict access policies.

Conclusion

This penetration testing exercise has highlighted several areas where Jacaranda Health can improve its security posture. By addressing the issues identified and implementing the recommendations, Jacaranda Health can significantly enhance its resistance to cyber threats.

Maintaining a strong security posture is an ongoing effort that involves continuous monitoring, improvement, and reassessment. The team recommends that Jacaranda Health regularly revisit its security policies, controls, and practices to ensure they are in line with emerging threats and evolving business needs.