Protego Security Solutions, Inc.

Penetration Testing Report for Pixel Paradise Inc.

June 27, 2023

Executive Summary

Protego Security Solutions was engaged by Pixel Paradise Inc. to provide comprehensive block-box penetration testing of their web servers, web applications, internal network, and employee security awareness. Most testing was black-box except in some cases access was provided to the developer platform for more disruptive tests. In addition, security personnel were aware that vulnerability scanning of their web servers was to occur so that the scans were not blocked.

Purpose and Scope

Pixel Paradise is concerned about cybersecurity preparedness because they anticipate that a new product, to be released soon, will greatly increase their internet exposure. According to Pixel Paradise's stated concerns, we defined the goals of the penetration test as follows:

- Assess security of the Pixel Paradise web platform including all internet-facing services.
- Assess security of the Pixel Paradise customer community and digital storefront applications.
- Assess security of Pixel Paradise sensitive data and product builds on their internal network.
- Determine security awareness of employees at Pixel Paradise through social engineering tests.

- Determine any vulnerabilities introduced by the use of other connected (IoT) devices in the Pixel Paradise facility.

All internet-facing devices and internal networks were approved as subject to testing. The web applications were approved for scanning, but more intrusive testing was to be conducted in an internal development environment. Security staff required notification regarding intense scanning of external servers, so the scans were not blocked.

Summary of Results and Recommendations

A high-level summary of the results of the penetration tests appears here. For more detailed information, refer to the Test Results and Recommendations sections of this report.

- Seven personnel clicked on various phishing links including one that executed remote code. The possibility of successful malware attacks is high.

- A rogue webserver (unknown to IT and security personnel) was found running in the internal network; however, it appears that the corporate firewall had been configured to permit external access. This server had various vulnerabilities that permitted access to the internal network and disclosure of a password file. This presents an unacceptable level of risk to the company and steps should be taken to remove the server from the network and investigate personnel responsible for its presence.
- A hidden webpage that included an insecure input field was discovered. The insecure field permitted various SQL and code injection attacks and disclosure of sensitive information.

- Video surveillance equipment was found to use well-known default login credentials. Embedded software is not updatable/patchable.

Due to the level of risk discovered in the network and applications, we recommend that a Pixel Perfect create and staff the position of Director of Cybersecurity, or similar, to enhance security operations and policies.

Testing Process and Procedure

The testing process followed accepted processes and frameworks as defined by penetration testing and cybersecurity testing organizations. We combine approaches by drawing on the strengths of NIST 800-115, PTES, OSSTMM, OWASP, and PTES processes and procedures.

a. Staff Security Awareness

Pixel Paradise upper management expressed concern about the possibility of theft or loss of assets due to ransomware and other malware downloads. Testing was undertaken to assess the degree of cybersecurity awareness of employees.

Social engineering tools were utilized to create a multi-pronged campaign that primarily used phishing emails and imitation websites. In one case, an embedded link in a phishing email sent users to a honeypot website, maintained by Protego, which executed a JavaScript application that recorded visits. This application simulated remote execution of malicious software.

b. Internet-Connected Servers

DNS foot printing tools and techniques were first used to discover details of the Pixel Paradise web presence. Scanning of adjacent address blocks was also carried out in order to discover unknown and unregistered servers. Automated vulnerability scans were conducted using Greenbone Vulnerability Manager/OpenVas, Zed Attack Proxy (ZAP), and Nikto. We were required to establish a preset time period for Nikto scanning in order that security personnel would not take measures to block the scan.

c. Internal Network

Access was gained to the internal network and Active Directory enumeration and exploitation were achieved with the Nmap and Bloodhound tools. Additional SMB enumeration was conducted with enum4linux and Nmap SMB-related testing scripts. Exploitation was achieved with smbclient, which allowed file transfers between the testing VM and hosts on the network.

d. Web Applications

Web applications were scanned with the web application scanners noted above and manually tested for various other vulnerabilities.

e. Other Connected Devices

Shodan was used to identify any devices that were detectable from the internet. Access was gained to the internal network and Nmap scans conducted to identify IoT devices. These devices were then researched to learn about their security features, and well-known credentials were used to gain access. Those devices were then challenged to achieve login to verify software versions and device details.

Test Results

Test results revealed a number of serious vulnerabilities that present serious risk to Pixel Perfect. While these vulnerabilities are serious, they are fairly easily mitigated.

a. Staff Security Awareness

A multi-pronged phishing campaign resulted in seven employees clicked potentially malicious links. Several employees also visited imitation websites that were constructed to lure employees into to submitting user credentials.

b. Internet-Connected Servers

Public address block scanning revealed the presence of an undocumented webserver that was reachable over the internet. The server was easy to penetrate though automated password challenges that followed a common passwords rainbow table. Admin access provided. Once inside, investigation indicated that the server was setup for personal use by [name redacted]. The server housed personal information, family pictures, and other information that led to identification of the server owner. The server hosted a server for an insecure remote access application that eventually provided testers with access to the internal network. This should be a serious breach of policy.

A hidden webpage that was apparently used by developers for connectivity testing was found on the primary corporate webserver. This page included an input form for IP addresses that was meant to execute the ping command when the input was posted. The input box was not protected with any sort of input validation. The field was vulnerable to command, code, and SQL injection attacks. The backend database contains sensitive user data that was fully available to SQL commands injected into the form.

c. Web Applications

Web application scans and manual testing indicated vulnerabilities in the community forum and storefront applications. Testing indicated that inputs in the login form were only partially implemented through HTML tag removal. However, more advanced SQL injected yielded an error message that identified the SQL server type and version. While it was outside of the scope of the test to access real user data through the form, further testing indicated that SQL injection vulnerabilities are present.

The community forum was tested for vulnerabilities. It was found that the forum is vulnerable to insecure direct object reference attacks. After login, users are identified by a GUID that is included with every web transaction. The GUIDs are exposed in the URLs for user profile pages meaning that the GUID can be lifted and used in forged URLs that permit actions to be executed as other users.

d. Internal Network

Access was gained to the network through a remote access vulnerability that was discovered on the rogue webserver described above. From there enumeration of network devices was achieved using Active Directory and SMB enumeration tools. These tools revealed unprotected or weakly protected shares that could be exploited to enable lateral movement through the network.

e. Other Connected Devices

Shodan scans indicated the presence of an internet-connected security monitoring system. Banner information divulged the model number and version of this device, which acts as a server for five video surveillance cameras that are distributed around the facility. Following this

information, the default passwords were found for this device. A script automated to challenge the login using the passwords and default usernames available on the network provided access to the cameras. Further work would have probably resulted in access to the general internal network through this device. The cameras were found to be a model that is not capable of software updates or patches. While the current revision of the camera software does not appear to have known vulnerabilities, there is no guarantee that this will be the case in the future.

Recommendations

The following recommendations should be considered to enhance the Pixel Paradise overall security posture. Each recommendation is assigned a priority that corresponds to the severity of the vulnerability and the urgency with which it should be remediated. The priority ratings are as follows:

Rating	Meaning
1	**Less urgent** - Remediation can be deferred for a period of time while addressing higher priorities.
2	**Urgent** – Remediation should be undertaken after high priority issues are addressed.
3	**Highly urgent**. Address issues immediately.

a. General Recommendations.

1. Staff a dedicated cybersecurity manager position. Considering the current haphazard security posture and the increased risks associated with increasing success of the company's products, a formal dedicated security position is strongly recommended. **Priority 2**.
2. Strengthen administrative security controls by creating and distributing rigorous user policies and agreements. Establish enforceable consequences for all behaviors that increase the threat landscape for the company, including rogue hardware and unauthorized web portals. **Priority 2**.
3. Conduct regular security audits to document the corporate network security posture over time. **Priority 3.**

b. Staff Security Awareness

Some staff are vulnerable to social engineering attacks.

1. Conduct annual user security training using established professional curricula. **Priority 3**
2. Conduct occasional security tests using social engineering tools to evaluate the state of security awareness among staff. **Priority 3**

c. Internet Connected Servers

An unauthorized device and web page were found facing the internet.

1. Immediately remove the rogue server from the network. **Priority 1**
2. Investigate who altered the firewall rules to allow connectivity to the server. If necessary, determine how access to the firewall configuration was gained. Take disciplinary action. **Priority 1**

3. Remove the hidden web page and investigate the potential presence of other sensitive documents or vulnerable server misconfiguration. **Priority 1**

d. Internal Network

The internal network is vulnerable to post-exploitation lateral movement.

1. Use Windows management tools to establish and enforce policies regarding the creation of ad hoc shares on all workstations. **Priority 2**
2. Create and enforce password policies for password length and complexity for all user accounts. **Priority 2**
3. Audit SMB and Active Directory for further security issues. **Priority 2**

e. Web Applications

Various vulnerabilities were identified in Pixel Paradise web applications.

1. Implement training and automated source code scanning for secure coding practices. **Priority 3**
2. Use robust input validation to prevent any type of injection attacks. **Priority 1**
3. Segregate the web application from direct access to backend databases by using parametrized queries to further mitigate injection attacks. **Priority 1**
4. Remove user GUIDs from forum posts and randomize GUIDs for user identification after initial authorization so that GUIDs always change. **Priority 1**

f. Other Connected Devices

An insecure network surveillance system was discovered during reconnaissance. Exploitation revealed various vulnerabilities.

1. Immediately change all user credentials on video surveillance devices. **Priority 1**
2. Replace existing cameras with devices that have enhanced security features such as the ability to update software over the network, update management, configurable ports, and minimal server processes. **Priority 3**
3. Ensure that the cameras do not provide information banners to internet probes. **Priority 2**

Summary

It is clear that Pixel Paradise is undergoing growing pains as it moves to the next tier of success in the gaming industry. As with many creative organizations, network security was sacrificed in favor of creativity and spontaneity. However, the kinds of vulnerabilities that have been created in the network through either user actions, insecure coding practices, or unwise device purchases could be devastating to business operations if exploited.

In order to protect the company’s assets and ensure uninterrupted operation, Pixel Paradise must modernize its approach to cybersecurity with a rigorous cybersecurity program that is managed by a dedicated staff person or team.