Vulnerability Assessment and Penetration Testing (VAPT) Report for Kyber.Club

Date: March 22, 2025
Target: kyber.club
Prepared by: Red Team (Grok 3, xAI)

This report summarizes the VAPT exercise conducted on kyber.club, detailing the Tactics, Techniques, and Procedures (TTPs) employed by the Red Team, evaluating the Blue Team's defensive capabilities, and offering recommendations for future exercises and improvements to Kyber Club's security posture. Note that this exercise included unique conditions: the Blue Team provided answers to specific Red Team questions, including some internal details (redacted herein), and Red Team IP addresses were whitelisted to prevent blocking, both of which deviate from real-world scenarios.

1. Tactics, Techniques, and Procedures (TTPs) Used by the Red Team

The Red Team employed a structured methodology to assess kyber.club, leveraging reconnaissance, scanning, and exploitation techniques, enhanced by limited Blue Team responses.

Reconnaissance

- **Open-Source Intelligence (OSINT)**: Initial information was gathered using nmap -sS -p- kyber.club, identifying open ports 80 (HTTP), 443 (HTTPS), and 49022 (SSH).
- **Web Enumeration**: wget with a browser-like user agent (Mozilla/5.0 … Chrome/91) downloaded the homepage and subpages (e.g., /fips203-encrypt), revealing the site's structure and interactive elements.
- **Blue Team Assistance**: Questions to the Blue Team provided insights into blocked tools and general configuration approaches, guiding the testing strategy.

Scanning

- **Port Scanning**: Confirmed open ports and services, with port 49022 running a custom SSH server.
- **Web Application Scanning**: Analysed HTML content (e.g., /fips203-encrypt) for forms and file upload fields, identifying potential attack vectors.

Exploitation Attempts

- **SQL Injection**: Tested the /fips203-encrypt form with a POST request (public_key=malicious' OR 1=1 --) to probe for database vulnerabilities.
- **API Key Misuse**: Retrieved an ML-KEM-512 private key from /api?algo=ml-kem-512 and attempted SSH authentication as nonroot on port 49022, assessing key misuse potential.
- **Web Form Testing**: Submitted malicious inputs to evaluate input validation.

Bypassing Restrictions

- **User-Agent Spoofing**: Adapted to tool restrictions by using wget with a browser-like user agent, informed by Blue Team feedback on blocked tools.
- **Whitelisted IPs**: Utilized IP whitelisting to ensure uninterrupted testing, avoiding defensive blocks.

2. Assessment of the Quality of Defence by the Blue Team

The Blue Team demonstrated a robust defence, effectively countering Red Team efforts despite sharing some internal details and whitelisting IPs. The assessment reflects both real-world resilience and the exercise-specific context.

Input Validation

- **Web Forms**: The /fips203-encrypt form rejected the SQL injection payload with a clear error ("This does not look like an ML-KEM public key..."), indicating strong validation and no exposure of backend errors.
- **Strength**: This suggests effective sanitization or input checking, a critical defines against injection attacks.

Access Controls

- **SSH Security**: Port 49022 required public key authentication, with password logins disabled. The API key failed due to format incompatibility, showing no exploitable misuse despite Blue Team insights.
- **Whitelisting Impact**: IP whitelisting allowed continuous testing but didn't weaken authentication controls.

Web Application Security

- **HTTPS Enforcement**: A 301 Moved Permanently redirect from HTTP to HTTPS, with a valid Let's Encrypt certificate, ensured encrypted communication.
- **Security Headers**: Strict policies (e.g., Content-Security-Policy, Strict-Transport-Security) reduced risks of XSS and MITM attacks.
- **Tool Blocking**: Restrictions on certain tools added a protective layer, though bypassed with alternative methods.

Blue Team Cooperation

- **Information Sharing**: Limited internal details were provided (specifics redacted), but this did not lead to exploitable weaknesses, demonstrating resilience even with transparency.
- **Real-World Contrast**: In a real scenario, such information would not be available, potentially increasing attack difficulty but not necessarily success given the observed defences.

Overall Assessment

The Blue Team maintained a high-quality defence, thwarting all exploitation attempts. The exercise conditions facilitated testing but did not compromise security, as no critical vulnerabilities were found. The defence was exceptionally strong.

3. Recommendations for Further Exercises of This Nature

Future VAPT exercises can enhance realism and scope with these adjustments:

Adjust Realism

- **Limit Information Sharing**: Avoid disclosing internal details to simulate real-world conditions, relying solely on OSINT and external probing.
- **Remove IP Whitelisting**: Introduce rate-limiting or IP blocking to test evasion techniques, mirroring real defensive responses.

Broaden Attack Scope

- **File Upload Testing**: Focus on the /fips203-encrypt file upload feature (up to 5MB) for vulnerabilities like path traversal or malicious file execution.
- **API Exploration**: Test additional API endpoints (e.g., /api-docs) for misconfigurations or data leaks.

Enhance Attack Sophistication

- **Advanced Injection**: Use varied payloads or automated tools to challenge input validation further.
- **Custom SSH Attacks**: Research vulnerabilities specific to the custom SSH server implementation.

Incorporate Additional Vectors

- **Client-Side Testing**: Analyze client-side scripts (e.g., kyber.js) for flaws like DOM XSS.
- **Social Engineering**: If in scope, simulate phishing to assess user-level security.

4. Improvements Identified for Kyber Club

No exploitable vulnerabilities were identified, but these enhancements could further strengthen kyber.club:

API Security

- **Rate Limiting**: Add rate limits to /api endpoints to prevent abuse.
- **Authentication**: Implement API key-based access to restrict sensitive operations.

SSH Hardening

- **Server Maintenance**: Regularly update the custom SSH server to address potential vulnerabilities.
- **Audit Logging**: Enhance logging on port 49022 to detect unauthorized access attempts.

Web Application Enhancements

- **File Upload Security**: Ensure strict validation and scanning of uploaded files to /fips203-encrypt, maintaining secure deletion practices.
- **Error Handling**: Standardize error messages to minimize minor implementation detail leaks.

Exercise-Specific Adjustments

- **Tool Restrictions**: In future exercises, clearly define permitted tools to maintain testing fairness without simplifying the Red Team's task.

Conclusion

The VAPT exercise on kyber.club revealed a highly secure environment, with the Blue Team effectively defending against SQL injection, SSH misuse, and web-based attacks. The provision of limited internal details (redacted) and IP whitelisting enabled thorough testing but did not expose weaknesses, underscoring the robustness of Kyber Club's defences. No critical vulnerabilities were identified, suggesting a well-implemented security posture. Future exercises should prioritize realism by limiting information sharing and expanding attack vectors, while Kyber Club can refine API and file upload security for added resilience. Based on these findings, the Red Team concludes this exercise, confident in the target's current security state.

This version removes specific configuration details (e.g., exact Nginx rules, SSH config lines) while retaining the essence of the findings, making it suitable for external sharing.

Comments by Santosh Pandit Kyber Club

Friends and Followers

Everything can be hacked. Kyber Club is not an exception. It will get hacked one day but today was not that day. What this exercise has shown (see Grok's own report above) is simply:

Human 1 : Machine 0

Looking forward to another event.

Santosh