Statement of Work (SOW) for Penetration Testing

Effective Date: 16/02/2024

Parties:

1. **Client:** KS Security Solution
2. **Service Provider:** HackersForYou

Project Overview:

This Statement of Work (SOW) outlines the scope, deliverables, and expectations for the penetration testing engagement between **KS Security Solution** and **HackersForYou**.

1. Engagement Timeframe and Milestones:

- **Start Date:** 16th February 2024
- **End Date:** 16th March 2024
- The engagement duration shall be 4 weeks.
- Key milestones include:
    - Kick-off meeting and scoping: 17th February 2024
    - Testing phase: 20th February 2024 - 9th March 2024
    - Reporting and debriefing: 13th March 2024

2. Testing Methodologies and Tools:

The penetration testing will follow industry-standard methodologies, including but not limited to:

- **Network Vulnerability Assessment:**
    - Utilize tools such as **Nessus**, **OpenVAS**, or **Qualys** for vulnerability scanning.
    - Manual assessment of identified vulnerabilities.
- **Web Application Testing:**
    - Conduct **OWASP Top Ten** assessments.
    - Use tools like **Burp Suite**, **OWASP Zap**, or **Netsparker**.
- **Wireless Network Testing:**
    - Assess Wi-Fi security using tools like **Aircrack-ng** or **Kismet**.
- **Social Engineering Testing:**
    - Simulate phishing attacks or other social engineering techniques.

3. Reporting Format and Timelines:

- The Provider will deliver a comprehensive report within 7 business days after the testing phase.
- The report shall include:
    - Executive summary highlighting critical findings.
    - Detailed technical findings, including proof-of-concept (PoC) demonstrations.
    - Risk ratings and recommendations for remediation.
    - Appendices with raw scan data and evidence.
    - The Client shall have 7 business days to review the report and seek clarifications.
    - A debriefing meeting shall be scheduled to discuss findings and next steps.

- **Risk Ratings**:
    - Risk ratings assess the severity and potential impact of each vulnerability. They guide prioritization for remediation efforts.
    - Commonly used risk rating scales include:
    - **CVSS (Common Vulnerability Scoring System)**: A numerical score (0-10) that considers factors like exploitability, impact, and complexity. Higher scores indicate greater risk.
    - **High/Medium/Low**: A qualitative rating based on the likelihood of exploitation and potential consequences.
    - **Critical/High/Medium/Low**: Similar to the above, but with an additional "Critical" category for severe vulnerabilities.
- Risk ratings consider:
    - **Likelihood**: How likely the vulnerability is to be exploited.
    - **Impact**: The potential harm if the vulnerability is exploited. How straightforward it is for an attacker to exploit the vulnerability.
    - **Affected Assets**: The criticality of the affected systems (e.g., production servers vs. development environments).
- Recommendations **for Remediation**:
    - Based on risk ratings, the report provides actionable recommendations for addressing each vulnerability.
    - Remediation steps may include patching, configuration changes, code fixes, or architectural improvements.
    - Prioritization helps allocate resources effectively, focusing on critical issues first.

4. Intellectual Property Rights:

- All deliverables, including the final report, shall be the property of the Client.
- The Provider grants the Client a non-exclusive, perpetual license to use the deliverables for internal purposes.

5. Acceptance Criteria:

- The engagement shall be considered complete upon successful delivery of the final report and acceptance by the Client.

Acknowledgment and Acceptance:

By signing this SOW, both parties acknowledge their understanding of the terms and agree to proceed with the penetration testing engagement.

KS Security Solution (Client):

Signature: ____________________

Printed Name: __________________

Date: _________________________

HackersForYou (Penetration Testing Provider):

Signature: ____________________

Printed Name: __________________

Date: _________________________