SERVICE ORDER ATTACHMENT
STATEMENT OF WORK

S-266-3163 EXTERNAL PENETRATION TESTING

(BASIC OFFERING)

1 Overview

This Statement of Work ("SOW"), with any appendices included by reference, is part of any agreement which incorporates this document by reference.

1.1 Service Summary

SilverSky understands the importance of conducting Penetration tests but also realizes that some clients are sensitive to time and budget constraints when trying to achieve this objective. For this reason, SilverSky has developed our Basic External Penetration testing offering. This offering follows a similar methodology to our Advanced service offering but can be performed with more efficiency and cost savings by using automated tool sets. SilverSky leverages best of breed automated penetration testing tools and supplements each assessment with a small block of manual validation performed by a certified penetration tester (OSCP, CEH, SANs GPEN, etc).

The purpose of External Penetration Testing (the "Service") is to identify the feasibility of an attack on and determine the extent of impact of a successful exploitation of Internet-facing systems controlled by the Customer. The testing will employ automated testing methodologies to perform the bulk of the engagement. Once the automated assessment is complete, a SilverSky Certified penetration tester will perform manual validation according to the hour block identified in the scoping section. The process will mimic typical attacker techniques and actual attempts to exploit identified vulnerabilities.

The testing is performed remotely with minimal interaction required of the Customer after the initial scoping meeting. Once complete, SilverSky consultants will meet with the customer to review any findings and perform an out brief of the report.

Project Deliverables:

- Comprehensive Report – Detailed report (Please note: While we strive to provide as much detail as possible, it is not uncommon for tests to return little to no findings based on the overall profile and complexity of your unique environment)

1.2 Phases of Penetration Testing

Phases of penetration testing activities include the following:

- Planning – Customer goals and rules of engagement (RoE) obtained
- Discovery – Perform auto-scanning and auto-enumeration to identify potential vulnerabilities and exploits
- Attack – Perform small block of manual validation to confirm potential findings identified through the automated testing
- Reporting – Document all found vulnerabilities and exploits with recommendations for remediation

1.3 Project Summary

SilverSky will undertake the following primary tasks, subject to modification or extension based on the investigation findings.

1. Kick-off Meeting
2. Scanning and Enumeration

3. Exploitation and Vulnerability Validation
4. Analysis of Findings
5. Draft Report and meeting to review Findings
6. Final Report

2 Scope

2.1 SilverSky Obligations:

Kick-off Meeting - Meet to discuss and agree on customer goals and the rules of engagement for the project. This includes project scoping to determining the target systems to be included in the testing and any additional precautions or provisions are also considered before testing.

Scanning and Enumeration - Assess the integrity and overall level of external security of critical network components such as servers and devices. SilverSky performs vulnerability scans using tools that are continually updated and contain checks for thousands of known vulnerabilities and exploits.

1. Host Discovery - Automated probing of targeted IP addresses and network blocks in scope to determine which addresses are connected to live systems and responding. This includes port scanning for well-known TCP and UDP ports which can reveal open ports and services running on the in scope devices.

2. **Enumeration** – Carry out enumeration techniques to get a complete picture of the targets using information gathered during the reconnaissance phase. This includes identifying valid user accounts or systems with security weaknesses to uncover potential attack vectors.

3. Run automated penetration testing tools – Perform a penetration test using automated tools and scripts against targets in scope to identify and exploit known vulnerabilities, perform lateral movement and privilege escalation.

Manual Validation – As an additional layer of testing SilverSky will perform manual validation of any findings up to the included in-scope hours. The goal of the manual validation is to:

1. Prove the ability to exploit a given vulnerability, discovered during the automated testing phase.
2. Eliminate false positives through the use of validation to determine proof of concept.
3. Uncover vulnerabilities not identified or missed by the automated assessment tools *(The ability to determine new findings will be performed as a best effort approach within the designated hours allotted. For a comprehensive assessment, SilverSky recommends our Advanced Testing services)*

Report of Findings Phase – SilverSky will compile and analyze the data generated from the assessment tools and manual checks and categorize vulnerabilities by severity, depending on the potential impact each can have on the affected network.

2.2 Deliverables

At the conclusion of the assessment, SilverSky will provide a comprehensive report composed of a detailed findings report. The Customer will have an opportunity to review drafts of the report and SilverSky will deliver a final version after a joint review with the Customer.

Detailed Findings - The detailed findings section describes the assessment results in detail. It is intended for management, administrators and other operations personnel and includes:

- An itemized listing of individual vulnerabilities
- A description of each vulnerability
- Severity of the threat likely posed by each vulnerability
- Potentially affected resources
- Recommendations for remediation

2.3 Out of Scope

Any activity not explicitly included in this SOW is considered out of scope. If the Customer requests additional services, such services will be the subject of a change request. The following are out of scope services to this SOW:

- Manual Penetration Testing above and beyond the hours allotted for this engagement
- Web application penetration testing
- Mobile Testing
- Internal Penetration testing
- Retesting of the environment after remediation (Additional fee)

3 Customer Obligations and Assumptions

Services, fees and work schedules are based on the assumptions, representations and information supplied by the Customer. The Customer's fulfillment of these responsibilities is critical to the success of the engagement.

3.1 Customer Obligations

- **Project Liaison** - Designate an authorized representative to authorize the completion of key project phases, assign resources and serve as project liaison.
- **Access** - Ensure SilverSky consultants have access to key personnel and data requested.
- **Resources** - Furnish SilverSky with Customer personnel, facilities, resources and information and perform tasks promptly.
- **Cooperation** - Ensure all of the Customer's employees and contractors cooperate fully with SilverSky and in a timely manner. SilverSky will advise the Customer if increased Customer participation is required in order for SilverSky to perform the Service under this SOW.
- **Documentation** – Deliver in a timely fashion all documentation requested by SilverSky including Customer's security policies, network diagrams, server listings, and procedures.

3.2 SilverSky Assumptions

- Customer will provide SilverSky with reasonably requested information upon which SilverSky can rely to be current, accurate, and complete.
- Customer will provide access to Customer personnel who have detailed knowledge of Customer security architecture, network architecture, computing environment, and related matters.
- Customer will provide access to Customer personnel who have an understanding of Customer's security policies, regulations and requirements.
- Customer will evaluate SilverSky deliverables and immediately notify SilverSky of any perceived problems or issues with SilverSky obligations.
- SilverSky will immediately notify the Customer of any perceived problems or issues regarding Customer obligations.
- Customer is responsible for any additional costs if SilverSky is unable to perform the Service due to Customer's delay or other failure to fulfill its obligations under this Statement of Work.

4 PROJECT PARAMETERS

4.1 Project Scope

The scope of the project is based on the above description with the additional details listed as follows:

Project Component	Parameter(s)
Project Start Date	SilverSky will reach out within 30 days of the Effective Date with a date for a kickoff call.
Project Duration	Approximately 1 week, subject to Tier level and project variables
S-266-2431 External Pen Testing Tier 1	Up to 10 IP addresses in scope and up to 3 hours of manual validation. Work hours not to exceed 16
S-266-2431 External Pen Testing Tier 2	Up to 10 IP addresses in scope and up to 3 hours of manual validation. Work hours not to exceed 20
S-266-2431 External Pen Testing Tier 3	Up to 10 IP addresses in scope and up to 4 hours of manual validation. Work hours not to exceed 24
S-266-2431 External Pen Testing Tier 4	Up to 10 IP addresses in scope and up to 4 hours of manual validation. Work hours not to exceed 30

4.2 Location and Travel Reimbursement

The Service defined in this SOW does not require onsite participation by SilverSky staff at Customer location(s).

4.3 Acceptance

Delivery of all stated project deliverables will constitute acceptance of services provided under this SOW.