Service Description: Advanced Services – Fixed Price

Cisco Security Advisory Services: Internal Network Penetration Assessment (M)

ASF-CORE-INPEN-800

This document describes the fixed price Cisco Security Internal Network Penetration Assessment (M).

Related Documents: This document should be read in conjunction with the following documents also posted at www.cisco.com/go/servicedescriptions/ : (1) Glossary of Terms; (2) List of Services Not Covered. All capitalized terms in this description have the meaning ascribed to them in the Glossary of Terms.

Direct Sale from Cisco. If you have purchased these Services directly from Cisco for your own internal use, this document is incorporated into your Master Services Agreement, Advanced Services Agreement, or other services agreement covering the purchase of Advanced Services-based services with Cisco ("Master Agreement") If no such Master Agreement exists, then this Service Description will be governed by the terms and conditions set forth in the Terms & Conditions Agreement posted at www.cisco.com/go/legalterms. If you have purchased these Services directly from Cisco for resale purposes, this document is incorporated into your System Integrator Agreement or other services agreement covering the resale of Advanced Services ("Master Resale Agreement"). If the Master Resale Agreement does not contain the terms for the Purchase and Resale of Cisco Advanced Services or equivalent terms and conditions, then this Service Description will be governed by the terms and conditions of the Master Resale Agreement and those terms and conditions set forth in the SOW Resale Terms & Conditions Agreement posted at www.cisco.com/go/legalterms. For purposes of the SOW Resale Terms and Conditions this Service Description shall be deemed as a Statement of Work ("SOW"). In the event of a conflict between this Service Description and the Master Agreement or equivalent services exhibit or agreement, this Service Description shall govern.

Sale via Cisco Authorized Reseller. If you have purchased these Services through a Cisco Authorized Reseller, this document is for description purposes only; is not a contract between you and Cisco. The contract, if any, governing the provision of this Service will be the one between you and your Cisco Authorized Reseller. Your Cisco Authorized Reseller should provide this document to you, or you can obtain a copy of this and other Cisco service descriptions at www.cisco.com/go/servicedescriptions/.

Internal Network Penetration Assessment

Service Summary
Cisco will perform an Internal Network Penetration Test of up to 800 live internal IP addresses. The testing will attempt to identify exploitable vulnerabilities and determine effectiveness of security investments against a simulated threat.

Location of Services
The Internal Network Penetration Test will be conducted at the Customer's facilities or from one or more remote locations via a secure remote network connection.

Travel will be limited to no more than six (6) visits by Cisco of up to twenty-three (23) days total on-site at a single Customer location.

Pre-Assessment Intelligence Gathering

Cisco Responsibilities

- Conduct remote Kick-off call to review project plan, define testing objectives and identify key stakeholders from Cisco and Customer.
- Attempt to perform Intelligence gathering as follows:
  - Perform perimeter scans of protocols, services, operating systems, and other technologies
  - Identify security defenses to be circumvented
  - Identify system trust and users
  - Identity system components
  - Construct a view of the attack surface
- Perform threat modeling, vulnerability discovery, and attack surface analysis as follows:
  - Perform automated and manual scanning attempting to identify vulnerabilities
  - Perform limited fuzzing and reverse engineering of discovered services, if required
  - Research applicable threats to discovered system assets and software
  - Prioritize attacks based on testing objectives

Customer Responsibilities

- Provide accurate and detailed technical documentation for the networks, including technical specifications, high-level design diagrams, technologies used, developer

documentation, design documentation, and use-case diagrams
- Provide access to key individuals for technical questions

Exploitation

Cisco Responsibilities

- Perform the following Exploitation activities on up to 800 Customer identified live internal IP addresses, where applicable:
    - Exploit design and architectural weaknesses by performing network sniffing and man-in-the-middle attacks
    - Compromise system components by exploiting implementation weaknesses in software through buffer overflows, remote code execution, cross-site scripting, SQL injection, and other command injection attacks
    - Test operational weaknesses within patch management, configuration management, and system deployment practices
    - Exploit user weaknesses through password guessing and password cracking attacks
    - Circumvent security controls by evading firewalls, intrusion detection systems, anti-virus, access controls, cryptographic protections, and data loss prevention systems

Customer Responsibilities

- Provide available window of hours for testing
- Provide up to 800 internally facing IP addresses to be tested
- Provide additional target identification information (e.g., hostnames, URLs)

Post-Exploitation

Cisco Responsibilities

- Perform the following Post-Exploitation activities, where applicable and approved by Customer:
    - Leverage discovered vulnerabilities to establish persistence
    - Leverage discovered vulnerabilities to escalate privileges
    - Search for credentials and sensitive data (e.g., personally identifiable information, credit card numbers)
    - Attempt to pivot attacks to additional targets
    - Attempt to exfiltrate data, where possible and in alignment with project objectives
- Provide the following reporting:
    - Eliminate false positives, where possible
    - Issues identified while attempting to achieve project objectives
    - Investigate potential business impact
    - Investigate and develop remediation strategies
- Provide Customer with the Internal Penetration Test Document.
- Schedule Executive Review call with identified executive stakeholders.

Customer Responsibilities

- Identify stakeholders to attend Executive Review call with Cisco.
- Review with Cisco the completed Internal Network Penetration Test Report.
- Provide sign-off for Internal Network Penetration Test Services completion.

General Customer Responsibilities

- Customer understands and acknowledges that, where Cisco has exercised reasonable precautions in performing Services, Cisco is not responsible for system outages, degradation of performance, or other adverse technology environment consequences of tasks Customer has authorized Cisco to perform.
- Customer represents and warrants that they have sufficient authority and the rights necessary for Customer to provide and/or facilitate Cisco's access to information, data, networks, systems, and media in connection with these Services.
- For all Customer requests under this Service Description that Cisco possess, access, or analyze particular media, computers, computer networks, communications networks, or other systems and equipment, to the extent Customer provides or facilitates Cisco's access thereto, Customer represents, warrants and covenants that they have all necessary right, title, license, and authority to make such requests and grant such access, including all necessary permissions from third-party owners of licensed or shared resources.
- CUSTOMER IS RESPONSIBLE FOR OBTAINING ALL NECESSARY LICENSES, PERMISSIONS, AND CLEARANCES FOR CISCO TO ACCESS RESOURCES THAT ARE HOSTED, OWNED BY, OR SHARED WITH A THIRD-PARTY.
- Customer is responsible for provisioning of necessary test access, environments, VPN connections, user accounts, administrative access, or other required technical assets.
- Cisco recommends that Customer back up its environment and perform maintenance before the start of performance of Services and reminds Customer that such back up is its sole responsibility.
- All information (such as but not limited to: designs, topologies, requirements) provided by Customer is assumed to be up-to-date and valid for the Customer's current environment. Cisco Services are based upon information provided to Cisco by Customer at the time of the Services.
- Customer acknowledges that the completion of Services is dependent upon Customer meeting its responsibilities as indicated herein.
- Customer will identify Customer's personnel and define their roles in the participation of the Services. Such personnel may include but is not limited to: architecture design and planning engineers, and network engineers.

- Customer will ensure Customer's personnel are available to participate during the course of the Services to provide information and to participate in scheduled information gathering sessions, interviews, meetings and conference calls.
- Customer expressly understands and agrees that support services provided by Cisco comprise technical advice, assistance and guidance only.
- Customer understands that any IP addresses not utilized during the term of the Service will not result in any credit.
- Customer expressly understands and agrees that the Services shall take place and complete within ninety (90) calendar days from issuing a Purchase Order to Cisco for the Services herein and any unused hours will expire.

Invoicing and Completion

Invoicing

Services will be invoiced upon completion of the Services.

Completion of Services

Cisco will provide written notification upon completion of the Services to Customer. The Customer shall within five (5) Business Days of receipt of such notification provide written acknowledgement of Cisco's completion of the Services. Customer's failure to acknowledge completion of the Services or to provide reasons for rejection of the Services within the five (5) Business Day period signifies Customer's acceptance of completion of the Services in accordance with this Service Description.

Assumptions and Exclusions

- Unless otherwise stated herein, Customer is responsible for provision of test equipment.
- Customer is solely responsible for determination and implementation of its network, design, business or other requirements and the implementation of any recommendations provided by Cisco. Cisco's recommendations are based upon Customer information provided to Cisco. Cisco shall not be liable for the accuracy or completeness of any Customer information contained in Cisco's recommendations.
- All document will be provided in electronic form in the English language..
- Customer retains all responsibility for the security of Customer Technical Environment(s). Cisco shall have no responsibility for, or liability as a result of, any breach in security of Customer's Environment. Cisco cannot guarantee that Customer's security may or may not be vulnerable from any included, omitted or overlooked instances whether or not presented in the Services or Deliverables associated with this Service Description.
- Security assessment services will not definitively prove the absence of vulnerabilities.
- Cisco recommends that Customer back up its environment and perform maintenance before the start of performance of Services and reminds Customer that such back up is its sole responsibility.