HPE POINTNEXT SERVICES

Data sheet

Check if the document is available in the language of your choice.

HPE VULNERABILITY ANALYSIS SERVICES

Packaged vulnerability scan and penetration testing services from HPE Pointnext Services

SERVICE OVERVIEW

HPE Vulnerability Analysis Services (VAS) is designed to help you understand the risks your business assets are exposed to. The packaged options under the HPE VAS family provide a vulnerability scan and penetration test on your in-scope critical assets in a simple, flexible, and timely manner. By leveraging expert researchers from HPE Pointnext Services and our analysis toolkits, and based upon the data collected, these packaged services can provide you a comprehensive list of risks that exist in the target assets, along with HPE's recommendations for remediation.

HPE follows penetration testing execution standard (PTES) methodology for all security testing engagements. For web application penetration testing, Open Web Application Security Project (OWASP) framework is also used alongside with PTES. All penetration test performed by HPE is to simulate real-world attacks to help assess the application vulnerabilities and security bugs in the Customer's application environment and each of them will consist of both automated scanning and manual testing approach. The two offerings you may choose from are generally described in Table 1 and more specifically described in Table 2.

HPE VAS—packaged offerings are available in the following fixed price and fixed scope format:

TABLE 1. HPE VAS—Packaged options information

HPE VAS—Packaged network vulnerability assessment and penetration testing (VAPT)	**Scope:** HPE VAS—Packaged network VAPT can be conducted on the IT infrastructure endpoints. Each package includes up to 10 consecutive business days (not to exceed 80 hours) of pre-engagement planning and other tasks as described in Table 2, inclusive of **black-box testing** that can cover up to 512 IP addresses (both internal and/or external IT assets). Both automated vulnerability scan and manual VAPT will be performed remotely on the agreed target assets. HPE will then report on its findings as described in Table 2 under **Reporting**.
HPE VAS—Packaged application VAPT	**Scope:** HPE VAS—Packaged application VAPT can be conducted on business-critical web applications. Each package includes up to 10 consecutive business days (not to exceed 80 hours) of pre-engagement planning and other tasks as described in Table 2, inclusive of **white-box testing** that can cover up to two web applications. Both automated vulnerability scan and manual VAPT will be performed remotely on the agreed target assets. HPE will then report on its findings as described in Table 2 under **Reporting**.

Refer to the Service features table for specifics on the features available under these penetration testing services.

SERVICE BENEFITS

- Gain insights on the risks that organizational assets are exposed to/from an external or internal perspective
- Help identify potential security gaps prior to formal compliance assessments or audits
- Enhance security posture of the organization
- Develop actionable mitigation suggestions by experienced HPE researchers and experts based upon output

SERVICE FEATURE HIGHLIGHTS

- Leverages HPE researchers to help identify asset and application risk in a controlled manner
- Supports flexible engagement rules such as timing for performance of certain tasks (for example, time of scanning, escalation workflows), which helps you to consume this service in the way that best fits your environment
- Shortens overall engagement cycle and delivers faster results with prepackaged model

TABLE 2. Service features

Feature	Delivery specifications
Network VAPT	This service covers the following: • **Two consecutive business weeks (five days per week; not to exceed eight hours per day) black-box network VAPT that covers up to 512 IP addresses** During the time allotted, HPE will work toward provisioning the following tasks as identified in the pre-engagement through the post exploitation phases: • Pre-engagement interactions – Determine and finalize the in-scope target(s) (IP addresses) of the engagement with the Customer – Define and finalize engagement rules including, but not limited to: – Execution (timing) preference for scan and exploit activities – Finding notification workflows and escalation rules – Exploit rules • Intelligence gathering – Information on the in-scope target is collected from various techniques as determined by HPE, such as open-source intelligence (OSINT) gathering, reconnaissance, and identifying protection mechanisms. • High-level threat modelling – Threat modelling is performed only at high level. Primary focus of threat modelling is from assets (IPs) and attacker perspective • Vulnerability analysis and exploitation – Conduct automated vulnerability scan on the targets via remote connection to target assets (IPs) – Conduct manual vulnerability assessment and penetration testing for limited number of IPs at HPE's determination based upon vulnerabilities identified – Identify and document false positives from scanning results • Post exploitation – Identify the value of the asset depending on the information/data uncovered in the vulnerability analysis and exploitation phase Upon completion of the time allotted for the tasks, HPE will then present its finding based upon the output as specified here: • Reporting – One full scanning report in PDF format—Direct output generated by the scanning technology – One analysis report in Excel format—Lists extended details for high severity vulnerabilities identified by the scanning technology, associated risk and suggested mitigation – One proof of concept document in PDF format—Outlines steps to reproduce high severity vulnerabilities identified by the scanning technology – One Customer-debrief session to be delivered via teleconference (up to two hours)
Web application VAPT	This service includes the following: • **Two consecutive business weeks (five days per week; not to exceed eight hours per day) white-box application VAPT that covers up to two web applications** During the time allotted for this work, HPE will work toward provisioning the following tasks as identified in the pre-engagement through the post exploitation phases: • Pre-engagement interactions – Determine and finalize the in-scope target(s) (web applications) of the engagement with the Customer – Define and finalize engagement rules with the Customer, including, but not limited to: – Timing preference for scan and exploit activities – Notification workflows and escalation rules – Exploit rules • Intelligence gathering – Information about the target application is collected in discussion with the asset (web application) owner – Application walkthrough is taken from the asset owner for better understanding of the application • High-level threat modelling – HPE will work with the Customer to identify various entry/exit points and user privileges • Vulnerability analysis and exploitation – Automated vulnerability scan on the targets (web applications) via remote connection to target assets – Conduct manual VAPT for limited number of findings at HPE's determination based upon vulnerabilities identified – Identify false positives – Recognize and exploit business logic flaws on targets at HPE determination where applicable • Post exploitation – Identify the value of the asset (web address) depending on the information/data uncover in the exploitation phase Upon completion of the time allotted for the tasks, HPE will then present its finding based upon the output as specified here: • Reporting – One full scanning report in PDF format—Direct output generated by the scanning technology – One analysis report in Excel format—Lists extended details for high severity vulnerabilities identified by the scanning technology, associated risk and suggested mitigation – One proof of concept document in PDF format—Outlines steps to reproduce high severity vulnerabilities identified by the scanning technology – One Customer-debrief session to be delivered via teleconference (up to two hours)

COVERAGE

- Services are provided during local HPE standard business days and hours excluding HPE holidays.
- Vulnerability scanning and penetration testing activities may be conducted outside of business hours and on holidays, subject to HPE approval.

CUSTOMER RESPONSIBILITIES

- Obtain necessary approvals for conducting vulnerability and penetration testing activities prior to agreed testing times.
- A contact person must be made available to organize project logistics and act as the escalation point.
- Respond to all requests for information and artifacts, as requested by HPE in a timely manner.
- Provide subject matter experts (SMEs) as required to clear up any areas of confusion or uncertainty.
- Offer access to the internal environment for HPE tools installation and use (in appliance format), where necessary; whitelist IP addresses and modify firewalls and related security access rules to facilitate vulnerability scanning activities where necessary.
- Customer participation at the appropriate level to determine the workflow, engagement rules, and escalation procedure for the vulnerability scan and penetration test service.

SERVICE LIMITATIONS

- Limitation of each service feature is outlined in the Service features tables. Additional charges will be incurred for any additional services required.
- This service cannot be used to meet any formal audit requirement but can help prepare for a formal audit by identifying potential problem areas.
- HPE's findings are dependent upon the target status and network at the time the service is conducted. There is no guarantee that all vulnerabilities of the in-scope target(s) will be discovered.
- The entire deliverable documentation created for this engagement is available in either Excel or PDF electronic format as mentioned in the Service features table.
- Deliverables are accepted upon delivery.
- Customer acknowledges and understands that there may be a disruption in service operation or degradation in performance on the testing targets during the engagement period. The Customer agrees to monitor the environment and notify HPE if such an incident happens.
- Customer will ensure that no personal data resides on the systems to be tested.

GENERAL PROVISIONS AND OTHER EXCLUSIONS

- Our ability to deliver this service is dependent upon the Customer's full and timely cooperation with HPE, as well as the accuracy and completeness of any information and data the Customer provides.
- HPE may utilize resources outside the country of purchase for delivery of the services.
- Customer acknowledges and agrees that HPE will perform the services per the mutually agreed project schedule, which shall be based upon the allotted hours and shall include the amount of time specified by HPE required to prepare and present the report.
- All services are provided remotely.
- To the extent HPE processes personal data on your behalf in the course of providing the services, the HPE Support and Professional Services—Data Privacy and Security Agreement found at hpe.com/info/customer-privacy.html shall apply.

ORDERING INFORMATION

Availability of service features and service levels may vary according to local resources and may be restricted to eligible products and geographic locations. To obtain further information or to order HPE Vulnerability Analysis Service, contact a local HPE sales representative and reference the following product numbers:

- HL2V5A1 and HL2V2A1 for HPE VAS—Packaged Network VAPT
- HL2V3A1 and HL2V6A1 for HPE VAS—Packaged Web Application VAPT

LEARN MORE AT

hpe.com/us/en/services/pointnext.html

a50002041ENW, July 2020, Rev. 1

Hewlett Packard Enterprise