Kent Public Service Network

CHECK Certified IT Health Check

Solution Overview

KPSN provides the facility to carry out IT Health check as part of the KPSN service catalogue.

The service will utilise two differing external vendors for this purpose as the Code of Compliance (CoCo) control indicates no single vendor can carry out the IT Health check two years running.

Scope

The IT Health Check will include a security penetration test of all security and network infrastructure devices connecting to the PSN service. The goal of the assessment being to identify any security vulnerabilities associated with all PSN-facing devices owned and managed by the KPSN Partner along with Partner's internal network elements.

The actual detail scope of elements and devices will be determined and decided on after discussion between the KPSN Partner's Technical Team, the Tester and the Supplier. A mutually agreed scope of work document will be produced and require sign off by all parties.

The technical scope of any assessment will include:

- Audit and determine effectiveness of firewall policy on firewalls connecting to the PSN network.
- Security configuration and assessment of the local site routers, switches and servers including:
  - Software related vulnerabilities.
  - Configuration related vulnerabilities.
  - Best practice security configurations.
- Security configuration and assessment of the connected CPE devices including:
  - Software related vulnerabilities.
  - Configuration related vulnerabilities.
  - Best practice security configurations.

Test Detail

The test will include the following four stages:

Stage 1 – Discovery

- The KPSN Partner will provide the Tester with the IP addresses of all systems and any other IP devices which should be included within the test.
- The KPSN Partner and Tester will agree the times and dates of engagement in which the testing can be conducted.
- To complete the Discovery stage, the Tester will complete the following activities:
- Scan using Port scanners (NMAP), traceroute and banner grabbing (AMAP) to identify live IP address provided by the Partner.
- All 65,535 TCP and UDP ports will be scanned and all results will be presented and included in the reports.

Stage 2 – Vulnerability Scanning/Assessment

- Once a full TCP/IP port scan has been completed the Tester will conduct a full vulnerability assessment. This will involve using multiple vulnerability, security configuration and application scanning/assessment tools. These tools provide an initial perspective of the security posture for the Partner's systems and devices.

- To complete this stage the Tester will conduct automatic testing with at least two independent vulnerability assessment tools.

Stage 3 – Manual Penetration Testing

- With the results generated from the vulnerability scanning, the Tester will manually confirm all reported security vulnerabilities against the systems.
- The Tester will discuss any systems deemed vulnerable and discuss with the Partner if any exploits should be attempted to confirm vulnerabilities.
- A number of other security tools may be used depending on the results presented.
- The output from these tools will identify any security vulnerabilities within the Partner systems. In no circumstances will any exploits or denial of service attacks be attempted unless prior permission has been granted by the Partner and the Supplier. If vulnerabilities are identified that may result in privilege escalation, exploitation may be required to demonstrate this.
- Once all vulnerabilities have been confirmed or deemed as being of a false positive nature the Tester will document the vulnerability, severity and recommended solution.

Stage 4 – Reporting

- The Tester will provide different levels of reporting for the Partner. The reports will be divided into Executive Management Reports and Technical Reports.

- The reports will show screenshots and other example output to assist in understanding the issues along with a description of how it can be replicated. Technical Reports will be listed by severity and solutions will be provided. Where applicable, the Tester will report all identified vulnerabilities with associated Common Vulnerability Scoring System (CVSS) scores, Common Vulnerabilities and Exposure (CVE) and Bugtraq ID (BID) and any other industry recognized repositories.

- Where required the Tester will present in person and discuss all aspects of the penetration test, reports and any additional security recommendations.

- The Tester is required to submit the final report to CESG.

Installation Lead Time	**Variable subject to individual requirements.**