Risk-X
YOUR DATA. ASSURED.

ASSURANCE – PENTEST ESSENTIALS

Datasheet 1:300

What is Penetration testing?

Penetration testing goes beyond that which is covered within a vulnerability assessment. Vulnerability assessment is akin to a burglar "casing the joint" and identifying where the latches on your doors and windows are left open and closed. Whereas, penetration testing will attempt to exploit any discovered weaknesses or, throw a metaphorical brick through the window and bypass any security features altogether. This allows a real-world test of the environment to leverage access to critical system components and sensitive information.

Risk-X base their network layer penetration testing methodology on the NIST Special Publication 800-115 Technical Guide to Information Security Testing and Assessment. For Web application testing the methodology is based on the Open Web Application Security Project (OWASP) Testing Guide v4.

Why is pentest essentials different?

For the following reason:

We use all the same skills, experience, quality and diligence we would with a normal test. What we have come to realise is that when a test does not require a regulated report (i.e. reporting in line with CREST or CHECK requirements) most of the time the report is superfluous. All you really care about is seeing what the issues are and how to get them fixed, therefore, having a lot of extraneous words means it is more 'stuff' to filter out. But you still pay for the tester to write the report!

So just like your favourite 'posh' supermarket we take all the same great stuff you want, remove the stuff you don't need and package it at a price that you are prepared to pay. Hence Pentest Essentials!

What flavours do we offer?

We offer the following:

- Internal network;
- Internal network segmentation;
- Internal wireless;
- External network.

All of the above services can be conducted as blind, unauthenticated or authenticated testing, and the tester will note in the output which version they used.

So what do you get for your money?

As we said, all of the same great stuff as with the prime service other than the report. What you get instead is:

1. Method statement:
    a. This is a generic method statement that tells you what the tester did;
2. Spreadsheet of findings:
    a. Includes management summary, vulnerabilities table, statistics – see next page for an example.

Vulnerabilities Table

Severity	Vulnerability	IP Count Affected IP's		Remediation Guidance
Critical	HP System Management Homepage Multiple Vulnerabilities (HPSBMU03593)	1	10.56.20.100	Upgrade to HP System Management Homepage version 7.5.5 or later.
Critical	HP System Management Homepage < 7.1.5 / 7.4.1 Multiple Vulnerabilities (POODLE)	1	10.56.20.100	Upgrade to HP System Management Homepage (SMH) 7.1.5 / 7.4.1 or later.
Critical	HP System Management Homepage < 7.5.4 Multiple Vulnerabilities (Logjam)	1	10.56.20.100	Upgrade to HP System Management Homepage (SMH) version 7.5.4 or later.
Critical	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)	1	10.56.20.13;10.56.20.14;10.56.20.100	Microsoft has released a set of patches for Windows 2000[Vista[2008[7[2008 R2[8[2012[8.1[and 2012 R2.
High	HP System Management Homepage < 7.1.4.1 / 7.1.3.1 OpenSSL Multiple Vulnerabilities	1	10.56.20.100	Upgrade to HP System Management Homepage 7.1.2 or later.
High	HP System Management Homepage < 7.1.6 Multiple Vulnerabilities (FREAK)	1	10.56.20.100	Upgrade to HP System Management Homepage 7.1.4.1 (Windows 2003) / 7.1.3.1 (Linux or Windows) or later. Note that version 7.1.1.1 for Linux x86 still contains OpenSSL v1.0.0d. Ensure that any products with which such an install might communicate with have been updated to the latest versions to not be affected by the vulnerability covered by CVE-2014-0224.
High	HP System Management Homepage glinkgosrmp.inc Command Injection	1	10.56.20.100	Upgrade to HP System Management Homepage 7.1.1 or later.
High	HP System Management Homepage < 7.1.0.14 Iprange Parameter Code Execution	1	10.56.20.100	Upgrade to HP System Management Homepage 7.1.1.0 or later.
High	HP System Management Homepage < 7.1.1 Multiple Vulnerabilities	1	10.56.20.100	Upgrade to HP System Management Homepage (SMH) version 7.1.6 or later.
High	HP System Management Homepage < 7.1.1.8 Multiple Vulnerabilities (BEAST)	1	10.56.20.100	Upgrade to HP System Management Homepage 7.1.8.14 or later.
Medium	HP System Management Homepage < 7.3 Multiple Vulnerabilities	1	10.56.20.100	Disable SSLv3. Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Note: We have removed the remediation URL's from this report

Are there any limitations with essentials?

There are some limitations with the essentials service and these surround hybrid test types and those for web applications. Hybrid testing requires considerable explanation and comment by the tester so this can only be completed with a full report under our prime service. This is the same for web application tests, as these are a little more complex as they usually require additional explanation to show how we reached the root cause of the vulnerability. Therefore, we usually do not offer this as part of the essentials service. However, if you are looking for a quick light test then it may be possible, so discuss your requirements with our principal tester to see if this is possible in your circumstance.

Why Risk-X?

Risk-X has brought this service to market to allow you to make the choice on how much information you want / need, and only pay for that and nothing more. If you need more information and help then choose the prime service, and if you only need to know what to fix then choose essentials. But don't compromise on quality, use our service. Our consultants are real people and the team has skills across testing, forensics, ISO27001 implementation and PCI DSS so we can provide real world testing and pragmatic remediation. If the team spots a breach or potential breach, we are best placed to use our forensic services to confirm if this has occurred, and can help you with all aspects of the criminal and legal processes at the same time. Talk to us today about how we can help you….

Key contacts

Andrew Gilhooley
Partner / Director Assurance
Andrew.gilhooley@risk-x.co.uk
+44 7580 834586

John Martin
Principal Tester
John.martin@risk-x.co.uk
+44 7736 636050

Qualifications

PCI Security Standards Council – QUALIFIED SECURITY ASSESSOR

PCI Security Standards Council – PCI FORENSIC INVESTIGATOR

2017 EXPERT WITNESS

SWEET & MAXWELL CHECKED 2017 EXPERT WITNESS

CISSP Certified Information Systems Security Professional

SSCP Systems Security Certified Practitioner

C|EH Certified Ethical Hacker