TCCS **TIÊU CHUẨN CƠ SỞ**

HIỆP HỘI AN TOÀN THÔNG TIN VIỆT NAM

TCCS 02: 2020/VNISA

Xuất bản lần 01

TIÊU CHUẨN DỊCH VỤ KIỂM TRA, ĐÁNH GIÁ AN TOÀN THÔNG TIN MẠNG

Specification Service

of Information Security Assessment

HÀ NỘI - 2020

Mục lục

Lời nói đầu

TCCS 02: 2020/VNISA được xây dựng trên cơ sở thực tiễn thực hiện dịch vụ kiểm tra kiểm tra, đánh giá An toàn thông tin mạng tại Việt Nam, có tham khảo các tiêu chuẩn quốc tế và tiêu chuẩn nước ngoài.

TCCS 02: 2020/VNISA do Câu lạc bộ Kiểm tra, Đánh giá và Kiểm định An toàn thông tin Việt Nam (VSAC) biên soạn, Hiệp hội An toàn thông tin Việt Nam thẩm định và công bố.

Lời giới thiệu

Tiêu chuẩn này quy định các yêu cầu cơ bản đối với dịch vụ kiểm tra, đánh giá An toàn thông tin mạng, bao gồm 03 nhóm: Yêu cầu về quản lý và kỹ thuật; yêu cầu về tổ chức và yêu cầu về nhân sự.

Nhóm yêu cầu về quản lý và kỹ thuật là cơ sở để tổ chức cung cấp dịch vụ xây dựng quy trình, nội dung các bước thực hiện nhiệm vụ kiểm tra, đánh giá.

Nhóm yêu cầu về tổ chức, nhân sự là cơ sở để tổ chức, doanh nghiệp hoàn thiện năng lực về tổ chức, tài chính và nhân sự của đơn vị mình.

Các yêu cầu nêu trong Tiêu chuẩn cơ sở này là yêu cầu cơ bản đối với việc cung cấp dịch vụ, kiểm tra, đánh giá an toàn thông tin mạng. Khuyến khích các tổ chức, doanh nghiệp bổ sung thêm các yêu cầu ở cấp độ cao hơn nhằm nâng cao chất lượng dịch vụ.

Các yêu cầu nêu trong nội dung Tiêu chuẩn là căn cứ cho việc đánh giá các dịch vụ kiểm tra, đánh giá An toàn thông tin mạng, phần Phụ lục là các mẫu biểu hướng dẫn cho quá trình đánh giá hợp chuẩn theo tiêu chuẩn cơ sở này.

1. Tiêu chuẩn dịch vụ kiểm tra, đánh giá an toàn thông tin mạng

Specification Service of Information Security Assessment

Phạm vi, đối tượng áp dụng

Phạm vi áp dụng

Tiêu chuẩn này được áp dụng trong quá trình chuẩn bị, thực hiện và kết thúc các công việc liên quan đến dịch vụ Kiểm tra, đánh giá An toàn thông tin mạng; áp dụng để đánh giá các dịch vụ phù hợp với Tiêu chuẩn.

Đối tượng áp dụng

Các tổ chức, công ty hội viên của VNISA, có cung cấp dịch vụ Kiểm tra, đánh giá An toàn thông tin mạng trên các ứng dụng và hệ thống công nghệ thông tin.

Tiêu chuẩn này cũng có thể được sử dụng bởi các cơ quan, tổ chức có nhu cầu thuê dịch vụ Kiểm tra, đánh giá an toàn thông tin mạng nhằm đánh giá, lựa chọn các đơn vị cung cấp dịch vụ.

2. Thuật ngữ và định nghĩa

Trong tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa sau.

2.1 An toàn thông tin mạng

Là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

2.2 Mạng

Là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính.

2.3 Xâm phạm an toàn thông tin mạng

Là hành vi truy nhập, sử dụng, tiết lộ, làm gián đoạn, sửa đổi, phá hoại trái phép thông tin, hệ thống thông tin.

2.4 Sự cố an toàn thông tin mạng

Là việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

2.5 Rủi ro an toàn thông tin mạng

Là những nhân tố chủ quan hoặc khách quan có khả năng ảnh hưởng tới trạng thái an toàn thông tin mạng.

2.6 Đánh giá rủi ro an toàn thông tin mạng

Là việc phát hiện, phân tích, ước lượng mức độ tổn hại, mối đe dọa đối với thông tin, hệ thống thông tin.

2.7 Quản lý rủi ro an toàn thông tin mạng

Là việc đưa ra các biện pháp nhằm giảm thiểu rủi ro an toàn thông tin mạng.

2.8 Dịch vụ kiểm tra, đánh giá an toàn thông tin mạng

Là dịch vụ rà quét, kiểm tra, phân tích cấu hình, hiện trạng, dữ liệu nhật ký của hệ thống thông tin; phát hiện lỗ hổng, điểm yếu; đưa ra đánh giá rủi ro mất an toàn thông tin.

2.9 Đơn vị cung cấp dịch vụ kiểm tra đánh giá an toàn thông tin mạng

Là doanh nghiệp, tổ chức cung cấp dịch vụ liên quan tới kiểm tra, đánh giá an toàn thông tin mạng.

2.10 Chuyên gia kiểm tra đánh giá an toàn thông tin mạng

Là chuyên gia kiểm tra, đánh giá dịch vụ an toàn thông tin mạng hoặc một phần của dịch vụ liên quan tới kiểm tra, đánh giá an toàn thông tin mạng.

3. Các thuật ngữ viết tắt

TT	Từ viết tắt	Tiếng Anh	Tiếng Việt
1	ATTT		An toàn thông tin
2	CNTT		Công nghệ thông tin
3	TCCS		Tiêu chuẩn cơ sở
4	APTP	Advanced Penetration Testing Program	Chương trình kiểm thử xâm nhập nâng cao
5	CEH	Certified Ethical Hacker	Chứng chỉ hacker mũ trắng
6	EC-council	International Council of Electronic Commerce Consultants	Tổ chức cung cấp các chương trình chứng chỉ bảo mật quốc tế
7	ECSA	EC-Council Certified Security Analyst	Chứng chỉ chuyên gia phân tích ATTT
8	GIAC	Global Information Assurance Certification	Chứng chỉ bảo đảm thông tin toàn cầu
9	GSEC Certification	GIAC Security Essentials certification	Chứng chỉ bảo mật GIAC
10	CREST	Core Research for Evolutional Science and Technology	Tổ chức nghiên cứu phát triển khoa học và công nghệ phát triển
11	CCNIA	CREST Certified Network Intrusion Analyst	Chuyên gia phân tích mạng được CREST chứng nhận
12	CVE	Common Vulnerabilities Exposures	Các lỗ hổng thường gặp
13	GPEN	GIAC Penetration Certification Tester	Chứng nhận kiểm thử xâm nhập
14	GXPN	GIAC Exploit Researcher and Advanced Penetration Tester	Chứng chỉ nghiên cứu lỗ hổng và kiểm thử xâm nhập
15	NDA	Non-Disclosure Agreement	Cam kết không tiết lộ thông tin
16	OSCP	Offensive Security Certified Professional	Chứng chỉ chuyên gia tấn công
17	OWASP	Open Web Application Security Project	Dự án bảo mật ứng dụng web mở
18	LPT	Licensed Penetration Tester	Chứng chỉ kiểm thử xâm nhập
19	Pentest	Penetration Testing	Kiểm thử xâm nhập
20	SLA	Service-level Agreement	Cam kết chất lượng dịch vụ
21	CompTIA	The Computing Technology Industry Association	Hiệp hội công nghiệp công nghệ máy tính
22	Sec+ Certification	CompTIA Security+ Certification	Chứng chỉ Security+ của CompTIA

4. Các yêu cầu cơ bản

Bao gồm nhóm các yêu cầu sau:

4.1 Yêu cầu đối với việc thực hiện dịch vụ, kiểm tra, đánh giá ATTT mạng: là cơ sở dể tổ chức cung cấp dịch vụ xây dựng quy trình, nội dung các bước thực hiện nhiệm vụ kiểm tra, đánh giá.

4.2 Yêu cầu đối với tổ chức cung cấp dịch vụ kiểm tra, đánh giá ATTT mạng: là cơ sở để tổ chức, doanh nghiệp hoàn thiện năng lực về tổ chức, tài chính của đơn vị mình.

4.3 Yêu cầu đối với nhân lực thực hiện dịch vụ kiểm tra, đánh giá ATTT mạng: là cơ sở để tổ chức, doanh nghiệp hoàn thiện năng lực nhân sự của đơn vị mình.

4.4 Kết quả bàn giao: Là căn cứ để thanh thanh quyết toán hợp đồng dịch vụ giữa các bên.

5. Phương pháp đánh giá và đo lường chuẩn

5.1 Phương pháp kiểm tra hoạt động thực tiễn của các chức năng, của hệ thống, giải pháp

- Nguyên tắc đánh giá: Dựa trên việc kiểm tra, đo lường kết quả hoạt động của các chức năng của hệ thống, giải pháp có đạt mức phù hợp với yêu cầu, chỉ tiêu, tiêu chuẩn được công bố.
- Mục đích áp dụng để đánh giá: Tính phù hợp, tính chính xác của chức năng theo các tiêu chí được đề ra.
- Phương thức thực hiện: Chạy thử trên thực tế, mọi tình huống, kiểm tra chức năng, tổng hợp kết quả đánh giá.

5.2 Phương pháp lấy ý kiến của chuyên gia

- Nguyên tắc đánh giá: Dựa trên ý kiến nhận xét của các chuyên gia hàng đầu hoặc Hội đồng chuyên gia chuyên ngành trên cơ sở kinh nghiệm và phân tích tài liệu hồ sơ và biên bản vận hành của hệ thống
- Mục đích áp dụng: Có thể áp dụng để đánh giá các tiêu chí phi chức năng như: Tính bảo mật, kiến trúc công nghệ, khả năng bảo trì, khả năng tương tác, khả năng phân tích, khả năng thay đổi được, khả năng cài đặt phần mềm, khả năng chịu lỗi, khả năng phục hồi, khả năng tương thích, chất lượng mã nguồn.
- Phương thức thực hiện: Tổng hợp ý kiến chuyên gia nhận xét đánh giá các tài liệu giải pháp, công nghệ áp dụng, hồ sơ hệ thống và kết quả vận hành thử nghiệm trên thực tiễn.

5.3 Các phương pháp khác

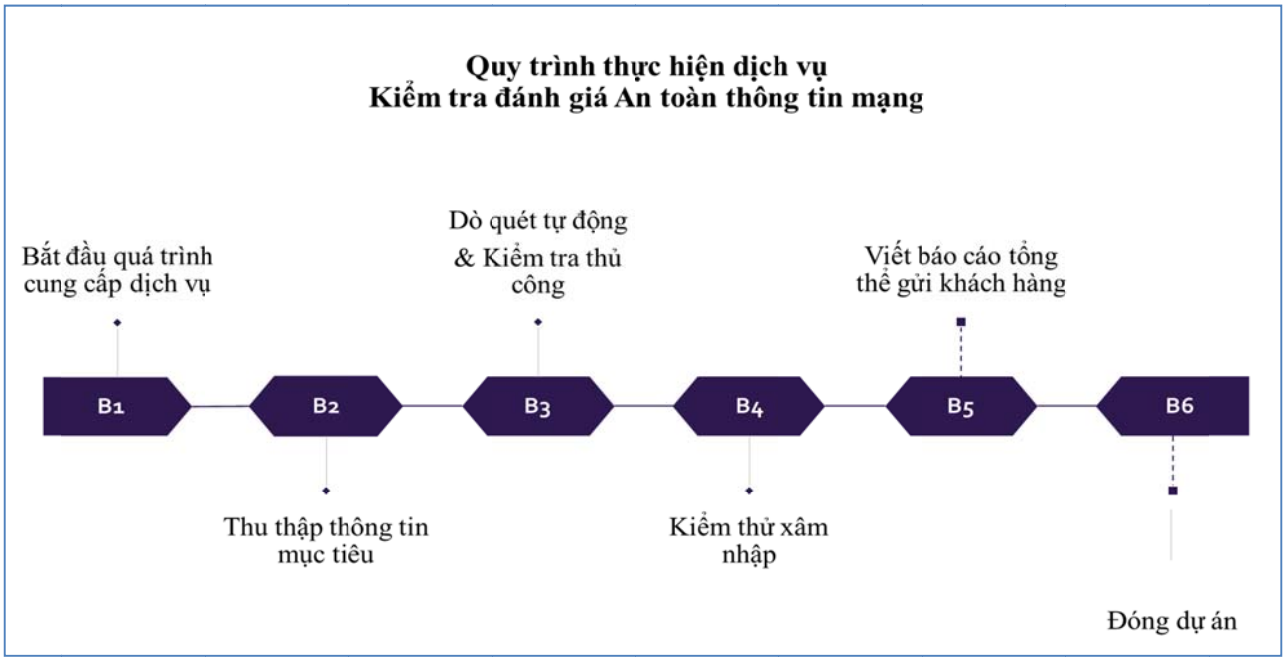
- Tùy theo tình hình thực tế, xem xét áp dụng bổ sung không giới hạn các phương pháp khác phù hợp với đối tượng và mục tiêu đánh giá.
- Các phương pháp bổ sung này phải được mô tả đầy đủ trong báo cáo tại các mục tiêu chí đánh giá liên quan.

5.4 Phụ lục: Các biểu mẫu kiểm tra, đánh giá.

6. Yêu cầu cụ thể đối với việc thực hiện dịch vụ, kiểm tra, đánh giá ATTT

6.1 Quy trình thực hiện dịch vụ kiểm tra, đánh giá ATTT

6.1.1 Các bước thực hiện



6.1.2 Mô tả quy trình

TT	Tên bước thực hiện	Yêu cầu (M-Bắt buộc/ O-Tùy chọn)	Mô tả	Ghi chú
1	Bắt đầu quá trình cung cấp dịch vụ(B1)	M	Có hợp đồng đã được ký kết với khách hàng	Các hợp đồng bao gồm nhưng không giới hạn: Hợp đồng cung cấp dịch vụ giữa 2 bên, Thoả thuận cam kết bảo mật thông tin (NDA), phụ lục phạm vi dự án (scope of work)
2	Thu thập thông tin mục tiêu (B2)	M	Khảo sát hiện trạng hệ thống, đối tượng cần đánh giá từ các nguồn khác nhau.	Các thông tin về mục tiêu cần đánh **giá** như: hệ điều hành, phiên bản phần mềm, loại thiết bị mạng, bảo mật, nghiệp vụ ứng dụng…
3	Dò quét tự động (Automatic Discovery)	O	Sử dụng các công cụ phần mềm để tự động dò quét các lỗ hổng phần mềm, hệ điều hành (nếu	Các thông tin về lỗi, lỗ hổng bảo mật được lưu lại và xử lý, đánh giá mức độ ảnh hưởng và nguy hại tới hệ

TT	Tên bước thực hiện	Yêu cầu (M-Bắt buộc/ O-Tùy chọn)	Mô tả	Ghi chú
	(B3)		cần thiết).	thống Bao gồm: đánh giá phiên xác thực, đăng nhập; đánh giá phân quyền; tương tác với các hệ thống back-end… Thông báo cho khách hàng trong trường hợp nghi ngờ các lỗi kiểm tra gây nguy hiểm cho hệ thống mục tiêu.
4	Kiểm tra thủ công (Manual testing) (B3)	M	Thực hiện kiểm tra đánh giá thêm tùy thuộc vào từng ứng dụng cụ thể.	
5	Kiểm thử xâm nhập (B4)	O	Xác minh mức độ rủi ro, khả năng khai thác thực tế của các lỗ hổng tiềm năng theo yêu cầu của khách hàng	Thực hiện kiểm thử xâm nhập một/một vài lỗ hổng nghiêm trọng đã được tìm thấy trước đó, xác định mức độ và phạm vi ảnh hưởng cao.
6	Viết báo cáo tổng thể gửi khách hàng (B5)	M	Báo cáo tổng thể phải chuẩn hóa cho từng loại mục tiêu/dịch vụ.	Báo cáo tổng thể phải cung cấp tổng số lỗi, mức điểm của từng lỗi, chi tiết chứng minh, khai thác, bằng chứng xác nhận, tài liệu tham khảo và khuyến nghị sửa chữa, khắc phục.
7	Đánh giá lại và viết báo cáo sau đánh giá lại (B5)	O	Báo cáo kỹ thuật đơn giản xác nhận tình trạng của toàn bộ lỗi đã được sửa xong.	Báo cáo thể hiện tình trạng đã sửa lỗi hay chưa. Bằng chứng xác thực đi kèm. (Hạng mục này cần được thực hiện trong khoảng thời gian cho phép).
8	Đóng dự án (B6)	M	Hoàn thiện các hồ sơ, giấy tờ liên quan phục vụ cho việc đóng dự án và thanh lý hợp đồng.	

6.2 Mô tả chi tiết các hạng mục của dịch vụ kiểm tra, đánh giá ATTT mạng

Các hạng mục kiểm tra, đánh giá bao gồm :

- Kiểm tra đánh giá ứng dụng web
- Kiểm tra đánh giá ứng dụng mobile và các ứng dụng WinForms
- Kiểm tra đánh giá hệ thống cơ sở dữ liệu
- Kiểm tra đánh giá hệ thống máy chủ dịch vụ, thiết bị mạng và bảo mật
- Kiểm tra đánh giá hệ thống mạng không dây

TT	Nội dung đánh giá	Mô tả	Tài liệu tham chiếu
I	**Kiểm tra đánh giá ứng dụng Web**		
1	Thu thập và khảo sát thông tin	Thực hiện tìm kiếm thông tin về ứng dụng phục vụ cho quá trình đánh giá.	https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents
2	Kiểm tra quản lý cấu hình và triển khai	Việc phân tích cơ sở hạ tầng và kiến trúc của website có thể giúp xác định rất nhiều yếu tố về một ứng dụng Web.	https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents
3	Kiểm tra quản lý định danh	Xác định việc ứng dụng định danh người dùng, qua đó có thể phá vỡ tính xác thực và định danh của người dùng.	https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents
4	Kiểm tra phần xác thực	Kiểm tra cơ chế xác thực dựa trên các phân tích cơ chế hoạt động của chức năng đăng nhập trong ứng dụng Web để tìm ra các điểm yếu.	https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents
5	Kiểm tra phân quyền	Tìm hiểu chức năng cấp quyền làm việc, thử phá vỡ cơ chế quan trọng này.	https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents
6	Kiểm tra quản lý phiên	Kiểm tra xem phiên và các “security token” có được tạo ra một cách an toàn hoặc có thể đoán trước đượcc hay không.	https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents
7	Kiểm tra kiểm soát dữ liệu đầu vào	Đa phần điểm yếu trong ứng dụng Web tập trung vào khâu đánh giá đầu vào đến từ người dùng. Điểm yếu này dẫn đến hầu hết lỗ hổng trong ứng dụng Web như: “SQL Injection”, “File Inclusion”, “Cross-site scripting” ...	https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents
8	Kiểm tra việc xử lý lỗi	Kiểm tra việc thông báo lỗi của ứng dụng có gây ra các nguy cơ mất ATTT cho hệ thống hay không.	https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents

TT	Nội dung đánh giá	Mô tả	Tài liệu tham chiếu
9	Kiểm tra mật mã, mã hóa yếu	Kiểm tra các cơ chế mã hoá có thể yếu của ứng dụng.	https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents
10	Kiểm tra lỗ hổng logic nghiệp vụ	Kiểm tra việc vận hành ứng dụng có thể gây ra các lỗi mà người dùng bình thường không phát hiện ra.	https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents
II	**Kiểm tra đánh giá ứng dụng Mobile và các ứng dụng WinForms**		
1	Khảo sát thông tin ứng dụng	Thực hiện tìm kiếm thông tin về ứng dụng phục vụ cho quá trình đánh giá.	https://github.com/OWASP/owasp-mstg/tree/master/Document
2	Kiểm tra phía máy khách và phân tích động	Kiểm tra ứng dụng bằng phương pháp phân tích phía máy khách cài đặt, hoạt động của ứng dụng có thể gây mất an toàn cho máy khách sử dụng.	https://github.com/OWASP/owasp-mstg/tree/master/Document
3	Kiểm tra kênh kết nối	Kiểm tra các kết nối đã đạt an toàn thông tin (sử dụng các giao thức an toàn)	https://github.com/OWASP/owasp-mstg/tree/master/Document
4	Kiểm tra các Webservices và API	Kiểm tra các tham số trên các Webservices/API, xác định các dữ liệu nhập có thể gây nguy hại cho hệ thống ứng dụng.	https://github.com/OWASP/owasp-mstg/tree/master/Document
III	**Kiểm tra đánh giá hệ thống cơ sở dữ liệu**		
1	Thu thập thông tin Cơ sở dữ liệu	Thu thập các thông tin về máy chủ CSDL, các “Instance” của CSDL	http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines
2	Đánh giá cấu hình máy chủ cơ sở dữ liệu	Xác định cấu hình máy chủ CSDL gây mất an toàn cho hệ thống.	http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines
4	Đánh giá xác thực	Kiểm tra cơ chế xác thực, chống các tấn công vét cạn, tấn công từ điển vào tài khoản quản trị.	http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines
5	Đánh giá phân quyền	Kiểm tra các cơ chế chống leo thang đặc quyền	http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines
6	Kiểm tra các lỗ hổng CVE	Thu thập thông tin CVE liên quan tới CSDL, thực hiện kiểm tra khả năng	http://www.pentest-standard.org/index.php/PTES_

TT	Nội dung đánh giá	Mô tả	Tài liệu tham chiếu
	(Common Vulnerabilities and Exposures) liên quan tới CSDL	khai thác của các CVE này lên hệ thống CSDL	Technical_Guidelines
IV	**Kiểm tra đánh giá hệ thống Máy chủ dịch vụ, thiết bị mạng và bảo mật**		
1	Thu thập thông tin	Thu thập thông tin của đối tượng.	http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines http://tigerteam.se/dl/standards/NIST-SP800-42.pdf
2	Đánh giá xác thực	Kiểm tra cơ chế xác thực, chống các tấn công vét cạn, tấn công từ điển vào tài khoản quản trị.	http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines http://tigerteam.se/dl/standards/NIST-SP800-42.pdf
3	Đánh giá phân quyền	Kiểm tra các cơ chế chống leo thang đặc quyền.	http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines http://tigerteam.se/dl/standards/NIST-SP800-42.pdf
4	Đánh giá quá trình kiểm tra dữ liệu đầu vào	Kiểm tra dữ liệu nhập tại các điểm có khả năng nhận dữ liệu từ phía máy khách trên các cổng dịch vụ đang mở của máy chủ .	http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines http://tigerteam.se/dl/standards/NIST-SP800-42.pdf
V	**Kiểm tra đánh giá hệ thống mạng không dây**		
1	Thu thập thông tin của mạng không dây	Thu thập các thông tin của thiết bị cấp phát mạng không dây, xác định những phương pháp xác thực của mạng không dây.	http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines http://tigerteam.se/dl/standards/NIST-SP800-42.pdf http://tigerteam.se/dl/standards/osstmm.en.2.1.pdf
2	Thực hiện đánh giá mạng không dây sử dụng	Nếu mạng không dây sử dụng xác thực WEP, thực hiện các phương pháp để lấy được key.	http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

TT	Nội dung đánh giá	Mô tả	Tài liệu tham chiếu
	WEP		http://tigerteam.se/dl/standards/NIST-SP800-42.pdf http://tigerteam.se/dl/standards/osstmm.en.2.1.pdf
3	Thực hiện đánh giá mạng không dây sử dụng WPA/WPA2	Nếu mạng không dây sử dụng xác thực WPA/WPA2, thực hiện các phương pháp để lấy được key.	http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines http://tigerteam.se/dl/standards/NIST-SP800-42.pdf http://tigerteam.se/dl/standards/osstmm.en.2.1.pdf

7. Yêu cầu đối với tổ chức cung cấp dịch vụ kiểm tra, đánh giá ATTT mạng

7.1 Yêu cầu về pháp lý

7.1.1 Yêu cầu về tính hợp pháp của tổ chức

- Có đăng ký kinh doanh đúng ngành nghề
- Có năng lực tài chính lành mạnh

7.1.2 Yêu cầu về giấy phép thực hiện dịch vụ ATTT mạng của cơ quan có thẩm quyền

- Có giấy phép "Cung cấp dịch vụ kiểm tra, đánh giá an toàn thông tin mạng" do Bộ Thông tin và Truyền thông cấp
- Giấy phép còn hiệu lực trong thời gian thực hiện dịch vụ

7.2 Yêu cầu về năng lực và kinh nghiệm của tổ chức

- Tổ chức thực hiện dịch vụ phải đảm bảo bí mật thông tin liên quan đến dịch vụ như: thông tin hệ thống, thông tin kết quả đánh giá.
- Đảm bảo tuân thủ các tiêu chuẩn áp dụng khi thực hiện dịch vụ: nêu trong các phụ lục tương ứng về "tiêu chuẩn"
- Trung thực khi đưa ra các kết quả đánh giá và các khuyến nghị khắc phục
- Tuân thủ quy tắc đạo đức nghề nghiệp do VNISA ban hành.

8. Yêu cầu đối với nhân lực thực hiện dịch vụ kiểm tra, đánh giá ATTT mạng

8.1 Trưởng nhóm kiểm tra, đánh giá ATTT (Chuyên gia loại 1)

8.1.1 Yêu cầu về chứng chỉ

- Tốt nghiệp Đại học chuyên ngành ATTT, CNTT trở lên
- Có các chứng chỉ liên quan đến kiểm tra, đánh giá ATTT

8.1.2 Yêu cầu về kinh nghiệm

- Có ít nhất 5 năm kinh nghiệm trong lĩnh vực kiểm tra, đánh giá.
- Đã trực tiếp lãnh đạo ít nhất 1 dự án kiểm tra, đánh giá về ATTT
- Đã trực tiếp tham gia thực hiện ít nhất 3 dự án kiểm tra, đánh giá ATTT

8.1.3 Yêu cầu khác

- Có chứng nhận đã qua khóa đào tạo pentester của VNISA
- Tuân thủ đúng bộ quy tắc đạo đức nghề nghiệp ATTT của VNISA

8.2 Chuyên gia kiểm tra, đánh giá ATTT (Chuyên gia loại 2)

8.2.1 Yêu cầu về chứng chỉ

- Tốt nghiệp Đại học chuyên ngành ATTT, CNTT trở lên
- Có các chứng chỉ liên quan đến kiểm tra, đánh giá ATTT

8.2.2 Yêu cầu về kinh nghiệm

- Có ít nhất 2 năm kinh nghiệm trong lĩnh vực kiểm tra, đánh giá.
- Đã trực tiếp tham gia thực hiện ít nhất 1 dự án kiểm tra, đánh giá ATTT

8.2.3 Yêu cầu khác

- Có chứng nhận đã qua khóa đào tạo pentester của VNISA
- Tuân thủ đúng bộ quy tắc đạo đức nghề nghiệp ATTT của VNISA

9. Kết quả bàn giao

Tổ chức thực hiện dịch vụ phải tuân thủ và cung cấp cho Khách hàng trước, trong và sau khi thực hiện dịch vụ:

- Tài liệu “Cam kết bảo mật thông tin – NDA” được ký giữa Tổ chức và Khách hàng
- Tài liệu “Giải pháp và phương pháp luận dịch vụ kiểm tra, đánh giá an toàn thông tin mạng”
- Tài liệu “Báo cáo kết quả đánh giá-kiểm định và Khuyến nghị” cung cấp cho Khách hàng”

Phụ lục A: Mẫu kiểm tra Quy trình thực hiện

(Quy định)

Mẫu kiểm tra quy trình thực hiện dịch vụ kiểm tra, đánh giá ATTT mạng

TT	TCKT	Loại yêu cầu (M-Bắt buộc/ O-Tùy chọn)	Bài đo và kết quả					
			Các chỉ tiêu	Kết quả mong muốn	Thực tế	Có	Không	Kết luận
	Bắt đầu dịch vụ							
1.	Kiểm tra thông tin hợp đồng	M	Có hợp đồng đã được ký kết với khách hàng	Các hợp đồng bao gồm: Ký kết dịch vụ giữa 2 bên, hợp đồng bảo mật thông tin (NDA), phụ lục phạm vi dự án (scope of work)				
2.	Demo chứng minh năng lực	O	- Trong trường hợp khách hàng yêu cầu demo đánh giá thử nghiệm một website/ứng dụng để chứng minh năng lực, yêu cầu: • Công văn xác nhận có ký đóng dấu của khách hàng yêu cầu đánh giá thử nghiệm. • Hai bên thống nhất thời gian thực hiện và sau đó tiến hành đánh giá Demo.	Thực hiện pentest hoặc kiểm thử xâm nhập thành công ở phạm vi nhỏ của hệ thống khách hàng.				
	Thực hiện dịch vụ							

3.	Lên kế hoạch và chuẩn bị	M	- Thống nhất kế hoạch và thời gian thực hiện với khách hàng dựa trên phạm vi hợp đồng. - Biên bản khảo sát hoặc xác nhận mục tiêu cần đánh giá (nếu có). - Đề xuất phương pháp kỹ thuật thực hiện (proposal), các công cụ sử dụng trong quá trình thực hiện, các thông báo tới khách hàng nếu việc rà soát có thể gây ảnh hưởng tới dịch vụ hệ thống.	Sơ đồ mục tiêu, hệ điều hành và các ứng dụng/dịch vụ, các port tương ứng,…				
4.	Kiểm tra dò quét tự động (Automatic Discovery)	O	- Sử dụng công cụ thương mại hoặc miễn phí, tự thiết kế. - Cung cấp giấy phép công cụ trong một số trường hợp yêu cầu của khách hàng - Đảm bảo các công cụ không gây tổn hại cho hệ thống mục tiêu. - Phải kiểm tra lại tình trạng thay đổi của ứng dụng khi sử dụng phương pháp kiểm tra tự động. - Phạm vi dò quét tự động thường bao gồm: • Dò quét mạng (Network Discovery) • Dò quét máy chủ/máy trạm (Host Discovery) • Thẩm tra dịch vụ (Service Interrogation)	Phải đảm bảo kết quả được review lại bởi kỹ thuật viên.				

5.	Phân tích thông tin và rủi ro (Manual Test)	M	- Thực hiện kiểm tra đủ theo các mục tiêu của một tiêu chuẩn mà bên thực hiện áp dụng (Ví dụ: OWASP Testing Guide). - Thực hiện kiểm tra đánh giá thêm tùy thuộc vào từng ứng dụng cụ thể như đánh giá phiên xác thực, đăng nhập; đánh giá phân quyền; tương tác với các hệ thống back-end… - Thông báo cho khách hàng trong trường hợp nghi ngờ các lỗi kiểm tra gây nguy hiểm cho hệ thống mục tiêu	Các lỗi khi tìm ra phải được xác nhận qua ít nhất 2 kỹ thuật viên. Các lỗi phải chia sẻ với toàn bộ team kỹ thuật.				
6.	Kiểm thử xâm nhập	O	- Bước này phải được thực hiện khi cần xác minh mức độ rủi ro thực tế của các lỗ hổng tiềm năng theo yêu cầu của khách hàng - Đối với những hệ thống có yêu cầu tính toàn vẹn rất cao, việc thực hiện cần được xem xét cẩn thận trước khi tiến hành.	Thực hiện kiểm thử xâm nhập một/một vài lỗ hổng nghiêm trọng đã được tìm thấy trước đó, xác định mức độ và phạm vi ảnh hưởng rất cao.				
7.	Viết báo cáo tổng thể gửi khách hàng	M	Báo cáo tổng thể phải chuẩn hóa cho từng loại mục tiêu/dịch vụ.	Báo cáo tổng thể phải cung cấp tổng số lỗi, mức điểm của từng lỗi, chi tiết chứng minh, khai thác, bằng chứng xác nhận, tài liệu tham khảo và khuyến nghị sửa chữa.				
8.	Đánh giá lại và hỗ trợ sửa lỗi	O	Báo cáo kỹ thuật đơn giản	Báo cáo thể hiện tình trạng đã sửa lỗi hay chưa. Bằng chứng xác thực đi kèm. (Hạng mục này				

				cần được thực hiện trong khoảng thời gian cho phép).				
9.	Viết báo cáo kỹ thuật xác nhận đã sửa lỗi	O	Báo cáo kỹ thuật đơn giản xác nhận tình trạng của toàn bộ lỗi đã được sửa xong.	Báo cáo gửi khách hàng phải có bằng chứng chứng minh đi kèm				
	Kết thúc dịch vụ							
10.	Đóng dự án	M	Văn bản xác nhận hoàn thành dự án (Email / File đính kèm)	Xác nhận từ đội ngũ kỹ thuật				
11.	Hoàn tất công việc theo hợp đồng	M	Hoàn tất công việc theo đúng cam kết trong hợp đồng	Có biên bản nghiệm thu và thanh ký hợp đồng đã được ký kết				

Phụ lục B: Mẫu kiểm tra năng lực tổ chức

(Quy định)

Mẫu kiểm tra năng lực đối với tổ chức cung cấp dịch vụ kiểm tra, đánh giá ATTT mạng

Yêu cầu	Loại yêu cầu (M-Bắt buộc/ O-Tùy chọn)	Bài đo và kết quả					
		Các chỉ tiêu	Kết quả mong muốn	Thực tế	Có	Không	Kết luận
1. Yêu cầu về pháp lý							
Yêu cầu về tính hợp pháp của tổ chức	M	Có đăng ký kinh doanh đúng ngành nghề.	Cung cấp giấy đăng ký kinh doanh hợp lệ				
	M	Có năng lực tài chính lành mạnh	Tại thời điểm đánh giá, tổ chức được đánh giá cần cung cấp các tài liệu chứng minh - Tổ chức không đang trong quá trình giải thể; không bị kết luận đang lâm vào tình trạng phá sản hoặc nợ không có khả năng chi trả theo quy định của pháp luật. - Báo cáo tài chính đã được kiểm toán của tổ chức trong 2 năm gần nhất có tài sản lưu động trừ đi nợ ngắn hạn lớn hơn 0. - Số thuế thu nhập doanh nghiệp 02 năm gần nhất nộp cơ quan thuế lớn hơn 0.				
Yêu cầu về giấy phép thực hiện dịch vụ ATTT mạng của cơ quan có thẩm quyền	M	Có giấy phép "Cung cấp dịch vụ kiểm tra, đánh giá an toàn thông tin mạng" do Bộ Thông tin & Truyền thông cấp.	Giấy phép còn hiệu lực trong thời gian thực hiện dịch vụ.				

2. Yêu cầu về năng lực, kinh nghiệm của tổ chức							
Yêu cầu tiêu chuẩn đối với tổ chức thực hiện dịch vụ thông thường	M	Số năm kinh nghiệm thực hiện dịch vụ tối thiểu là 03 năm	Cung cấp tài liệu chứng minh				
	M	Số lượng hợp đồng dịch vụ đã thực hiện là 01 hợp đồng	Cung cấp tài liệu chứng minh				
	M	Nhân sự thực hiện dịch vụ tối thiểu: 02 chuyên gia	02 chuyên gia bao gồm 01 chuyên gia loại 1 và 01 chuyên gia loại 2; có hợp đồng lao động tối thiểu 01 năm với chuyên gia.				
Yêu cầu nâng cao đối với Tổ chức thực hiện dịch vụ chất lượng cao	M	Số năm kinh ngiệm thực hiện dịch vụ tối thiểu là 03 năm liên tục	Cung cấp tài liệu chứng minh				
	M	Số lượng hợp đồng dịch vụ đã thực hiện là 05 hợp đồng trong 03 năm gần nhất	Cung cấp 05 hợp đồng trong 03 năm gần nhất				
	M	Đảm bảo quy mô của hợp đồng	Có ít nhất 01 hợp đồng trong đó giá trị của dịch vụ Pentest lớn hơn 500.000.000 VND (năm trăm triệu đồng).				
	M	Nhân sự thực hiện dịch vụ tối thiểu là 03 chuyên gia	03 chuyên gia, bao gồm 01 chuyên gia loại 1, 02 chuyên gia loại 2; có hợp đồng lao động tối thiểu 01 năm với chuyên gia.				

Phụ lục C: Mẫu kiểm tra năng lực nhân sự

(Quy định)

Mẫu kiểm tra năng lực của nhân sự thực hiện dịch vụ kiểm tra, đánh giá ATTT mạng

Yêu cầu	Loại yêu cầu (M-Bắt buộc/ O-Tùy chọn)	Bài đo và kết quả					
		Các chỉ tiêu	Kết quả mong muốn	Thực tế	Có	Không	Kết luận
1. Yêu cầu với Trưởng nhóm dịch vụ Pentest (Chuyên gia loại 1)							
Yêu cầu về chứng chỉ	M	Có ít nhất một trong các chứng chỉ liên quan đến Pentest như CEH, Sec+, ECSA, LPT, GSEC, GPEN, GXPN, OSCP, CREST hoặc tương đương.	Cung cấp chứng chỉ hợp lệ				
Yêu cầu về kinh nghiệm Pentest	M	Đã trực tiếp lãnh đạo ít nhất 1 dự án Pentest	Chứng minh bằng việc có tên trong hợp đồng với chức danh trưởng dự án hoặc được khách hàng xác nhận bằng văn bản.				
	M	Đã trực tiếp tham gia thực hiện ít nhất 3 dự án Pentest	Chứng minh bằng việc có tên trong hợp đồng với chức danh trưởng dự án hoặc được khách hàng xác nhận bằng văn bản.				
Yêu cầu khác	O	Có chứng nhận đã qua khóa đào tạo pentester của VNISA					
	M	Tuân thủ đúng bộ quy tắc đạo đức nghề nghiệp ATTT của VNISA					
2. Yêu cầu với Chuyên gia Pentest (Chuyên gia loại 2)							

Yêu cầu	Loại yêu cầu (M-Bắt buộc/ O-Tùy chọn)	Bài đo và kết quả					
		Các chỉ tiêu	Kết quả mong muốn	Thực tế	Có	Không	Kết luận
Yêu cầu về chứng chỉ	M	Có ít nhất một trong các chứng chỉ liên quan đến Pentest như CEH, Sec+, ECSA, LPT, GSEC, GPEN, GXPN, OSCP, CREST hoặc tương đương.	Cung cấp chứng chỉ hợp lệ				
Yêu cầu về kinh nghiệm Pentest	M	Có ít nhất 02 năm kinh nghiệm trong lĩnh vực Pentest	Minh chứng bằng danh sách hợp đồng đã thực hiện.				
	M	Đã trực tiếp tham gia thực hiện ít nhất 01 dự án Pentest	Chứng minh bằng việc có tên trong hợp đồng với chức danh chuyên gia đánh giá Pentest hoặc được khách hàng xác nhận bằng văn bản.				
Yêu cầu khác	O	Có chứng nhận đã qua khóa đào tạo pentester của VNISA					
	M	Tuân thủ đúng bộ quy tắc đạo đức nghề nghiệp ATTT của VNISA					
3. Yêu cầu đối với chất lượng thực hiện dịch vụ							
Yêu cầu về thông tin	M	Tổ chức thực hiện dịch vụ phải đảm bảo bí mật thông tin liên quan đến dịch vụ như: thông tin hệ thống, thông tin kết quả đánh giá					
	M	Trung thực khi đưa ra các kết quả đánh giá và các khuyến nghị khắc phục					

Yêu cầu	Loại yêu cầu (M-Bắt buộc/ O-Tùy chọn)	Bài đo và kết quả					
		Các chỉ tiêu	Kết quả mong muốn	Thực tế	Có	Không	Kết luận
Yêu cầu về tài liệu cung cấp cho khách hàng trước, trong và sau khi thực hiện dịch vụ	M	Tài liệu "Cam kết bảo mật thông tin – NDA"được ký giữa tổ chức và khách hàng.					
	M	Tài liệu "Phương pháp tiếp cận và Phương pháp thực hiện dịch vụ"	Tích hợp chung 02 tài liệu trên vào tài liệu "Báo cáo kết quả đánh giá-kiểm định và Khuyến nghị" cung cấp cho khách hàng				

Phụ lục D: Mẫu báo cáo tổng kết kết quả đánh giá

(Quy định)

Mẫu Báo cáo Tổng kết kết quả đánh giá dịch vụ kiểm tra, đánh giá ATTT mạng có thể linh động thực hiện theo từng đơn vị, tuy nhiên phải đảm bảo bao gồm đầy đủ các nội dung sau:

Mẫu báo cáo tổng kết kết quả đánh giá dịch vụ kiểm tra, đánh giá ATTT mạng

Thông tin chung

Mục tiêu

Phạm vi thực hiện đánh giá

Dịch vụ kiểm tra, đánh giá an toàn thông tin mạng được thực hiện trên hệ thống [...] của [...] theo mô tả dưới đây:

STT	Hệ thống cần đánh giá	Mô tả
1	[...]	[...]

Thời gian, địa điểm thực hiện đánh giá

- Thời gian thực hiện đánh giá: [dd/mm/yyyy] – [dd/mm/yyyy]
- Địa điểm thực hiện đánh giá:
- Trụ sở [...]: [...]

Các công việc thực hiện

Xếp loại điểm yếu

Các điểm yếu sau khi được phân tích và đánh giá sẽ được phân loại tùy thuộc vào mức độ nguy hiểm của điểm yếu và tác động của điểm yếu tới hệ thống, cụ thể:

STT	Xếp loại	Mô tả
1	● ● ●	Điểm yếu được xếp loại mức **Nghiêm trọng**: những điểm yếu nguy hiểm, dễ dàng bị khai thác, mức độ ảnh hưởng lớn, gần như ngay lập tức tới hệ thống, dữ liệu và các tài nguyên của công ty, tổ chức.
2	● ● ○	Điểm yếu được xếp loại mức **Cao**: những điểm yếu nguy hiểm, có thể bị khai thác, mức độ ảnh hưởng khá lớn, gần như ngay lập tức tới hệ thống, dữ liệu và các tài nguyên của công ty, tổ chức.
3	● ○ ○	Điểm yếu được xếp loại **Trung bình**: những điểm yếu bảo mật chưa ảnh hưởng lập tức tới hệ thống, dữ liệu và các tài nguyên của công ty, tổ chức tuy nhiên cần khắc phục trong thời gian sớm nhất.
4	○ ○ ○	Điểm yếu được xếp loại **Thấp**: những điểm yếu lộ thông tin, không gây quá nhiều ảnh hưởng tới công ty, tổ chức, chưa cần giải quyết ngay lập tức.

Kết quả đánh giá:

Kết quả tổng quan

Trong quá trình đánh giá [...], chúng tôi xác định được các lỗ hổng sau:

Mức Nghiêm trọng - [...] **điểm yếu, bao gồm:**

- Điểm yếu [...]

Mức Cao - [...] **điểm yếu, bao gồm:**

- Điểm yếu [...].

Mức Trung bình - [...] **điểm yếu, bao gồm:**

- [...]

Mức Thấp - [...] **điểm yếu, bao gồm:**

- **[…]**

Kết quả chi tiết:

- **Điểm yếu [...]**

Mô tả điểm yếu

Khuyến nghị khắc phục

- **Điểm yếu [...]**

Mô tả điểm yếu

Khuyến nghị khắc phục

- **Điểm yếu [...]**

Mô tả điểm yếu

Khuyến nghị khắc phục

Phụ lục E: Giải pháp và phương pháp luận

(Quy định)

Giải pháp và phương pháp luận dịch vụ kiểm tra, đánh giá ATTT mạng có thể linh động thực hiện theo từng đơn vị, tuy nhiên phải đảm bảo bao gồm đầy đủ các nội dung sau:

Giải pháp và phương pháp luận dịch vụ kiểm tra, đánh giá ATTT mạng

Với dịch vụ kiểm tra, đánh giá ATTT mạng (Pentest) các chuyên gia ATTT sẽ giữ vai trò là các hacker tấn công vào hệ thống CNTT của khách hàng. Các kịch bản tấn công được thực hiện có kiểm soát, chỉ được phép thực hiện khi được sự cho phép của khách hàng trong phạm vi và khoảng thời gian phù hợp, tránh ảnh hưởng tới hiệu năng và nghiệp vụ của hệ thống.

Dịch vụ Pentest trong ATTT được xây dựng dựa trên các tiêu chuẩn, phương pháp và các hướng dẫn về đánh giá an toàn thông tin đã được thế giới công nhận.

Vị trí thực hiện: […]

Quy trình thực hiện:[…]

Hạng mục đánh giá chi tiết cho từng hệ thống[…]

Danh sách công cụ chính phục vụ quá trình đánh giá

Quá trình đánh giá sử dụng kết hợp giữa phương pháp thủ công của các chuyên gia và các công cụ phụ trợ, danh mục các công cụ phụ trợ chính như sau:

STT	Tên công cụ	Mô tả Mục đích
1	[…]	[...]
2	[…]	[...]

Phụ lục F: Tài liệu tham khảo

TT	Nội dung	Tài liệu tham khảo
1.	Kiểm tra đánh giá ứng dụng Web	The OWASP Foundation (2014). OWASP Testing Guide version 4.0. [online] Tham khảo tại: https://www.owasp.org/images/1/19/OTGv4.pdf [Accessed 20 Oct 2019]
2.	Kiểm tra đánh giá ứng dụng Mobile và các ứng dụng WinForms	The OWASP Foundation (2019). OWASP Mobile Security Testing Guide version 1.1.3. [online] Tham khảo tại: https://github.com/OWASP/owasp-mstg/releases/download/1.1.3-excel/MSTG-EN.pdf [Accessed 20 Oct 2019]
3.	Kiểm tra đánh giá hệ thống cơ sở dữ liệu	NIST SP 800-115 (Sep 2008). Technical Guide to Information Security Testing and Assessment. [online] Tham khảo tại: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf [Accessed 20 Oct 2019]
4.	Kiểm tra đánh giá hệ thống Máy chủ dịch vụ, thiết bị mạng và bảo mật	NIST SP 800-115 (Sep 2008). Technical Guide to Information Security Testing and Assessment. [online] Tham khảo tại: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf [Accessed 20 Oct 2019]
5.	Kiểm tra đánh giá hệ thống mạng không dây	NIST SP 800-115 (Sep 2008). Technical Guide to Information Security Testing and Assessment. [online] Tham khảo tại: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf [Accessed 20 Oct 2019