CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

CA-08

Tests d'intrusion

Juill. 2026

Votre gouvernement

Québec

CA

Évaluation des systèmes et autorisation

Security Assessment and Authorization

CA-08 — Tests d’intrusion (PaFF)

Énoncés :

Effectuer des tests d’intrusion [Affectation : fréquence définie par l’organisation] sur [Affectation : systèmes ou composants de systèmes définis par l’organisation].

Paramètres :

minimalement 1 fois par année et au moins trois semaines avant d’inscrire un actif informationnel au programme de primes aux bogues; tous les actifs informationnels q'un organisme rend ou entend rendre disponibles sur Internet

Responsable : Partagée

Discussion :

Les tests d’intrusion sont des évaluations spécialisées menées sur des systèmes ou sur des composants des systèmes individuels qui visent à détecter des vulnérabilités que pourraient exploiter des adversaires. Les tests d’intrusion vont au-delà de l’analyse des vulnérabilités automatiques et ils sont exécutés par des agentes et agents ainsi que des équipes ayant des compétences et une expérience manifestes comprenant une expertise technique des réseaux, des systèmes d’exploitation ou de la sécurité au niveau des applications. Il est possible d’avoir recours à ces tests pour valider les vulnérabilités ou déterminer le niveau de résistance à l’intrusion des systèmes face à des adversaires en tenant compte de certaines contraintes. Parmi ces contraintes, notons le temps, les ressources et les compétences. Les tests d’intrusion tentent de reproduire les actions des adversaires et ils fournissent une analyse plus en profondeur des faiblesses ou des lacunes en lien à la sécurité et à la protection de la vie privée. Ces tests sont particulièrement importants lorsque les organisations passent des anciennes technologies aux nouvelles technologies (par exemple, le passage des protocoles réseau IPv4 à IPv6). Les organisations peuvent se servir des résultats des analyses des vulnérabilités pour soutenir les activités liées aux tests d’intrusion. Ces tests peuvent être effectués à l’interne ou à l’externe sur des composants matériels, logiciels et micrologiciels d’un système et peuvent exercer des contrôles à la fois physiques et techniques. Une méthode utilisée dans le cadre de ces tests consiste à mener une analyse prétest basée sur une connaissance détaillée du système, à effectuer une détection prétest des vulnérabilités potentielles basée sur l’analyse prétest et à réaliser des tests conçus pour déterminer l’exploitabilité des vulnérabilités. Toutes les parties doivent convenir des règles d’engagement avant le début des scénarios de test d’intrusion. Il faut établir une corrélation entre ces règles d’engagement et les outils, les techniques ainsi que les procédures dont on prévoit l’utilisation par les adversaires qui lanceront les attaques. Les tests d’intrusion peuvent mener à l’exposition de l’information qui est protégée par des lois ou de la réglementation, pour les personnes effectuant les tests. Des règles d’engagement, des contrats ou d’autres mécanismes appropriés peuvent être utilisés pour communiquer les attentes sur la façon de protéger cette information. Les évaluations des risques permettent de guider les décisions relatives au niveau d’indépendance exigé du personnel chargé des tests d’intrusion.