Engineer

Test d’intrusion

Attaque autorisée montrant quelles failles sont exploitables

Ce que c’est

Un test d’intrusion, souvent appelé pentest, est un test de sécurité dans lequel les auditeurs imitent des attaques réelles pour trouver comment contourner les protections d’une application, d’un système ou d’un réseau. Le guide technique du NIST sur les tests et l’évaluation de la sécurité de l’information, SP 800-115, précise que cela consiste souvent à lancer de vraies attaques sur de vrais systèmes et données, avec les outils et techniques des attaquants. La définition plus courte de SP 800-53 Rev. 5, le catalogue NIST des contrôles de sécurité et de protection de la vie privée, ajoute que les évaluateurs travaillent généralement sous des contraintes précises. C’est ce qui distingue un test d’une attaque : il est autorisé, délimité et convenu par écrit avant de commencer.

Ce qui le distingue des autres tests de sécurité est son objectif. Un scanner de vulnérabilités compare ce qu’il voit aux descriptions de failles connues et rapporte ce qui pourrait être présent. L’auditeur d’un test d’intrusion essaie d’utiliser la faille. SP 800-115 énonce clairement la différence : les scanners ne vérifient que l’existence possible d’une vulnérabilité, tandis que la phase d’attaque du test l’exploite pour confirmer son existence. La plupart des tests cherchent aussi des combinaisons de faiblesses, sur un ou plusieurs systèmes, donnant ensemble davantage d’accès que chacune isolément.

L’OWASP Web Security Testing Guide, ou WSTG, indique que la technique est aussi appelée test en boîte noire et piratage éthique. L’équipe teste de l’extérieur, sans connaissance préalable de la conception interne de la cible, et agit comme un attaquant, même si elle reçoit souvent un ou plusieurs comptes utilisateurs valides.

Deux choix façonnent chaque test. Le premier est le point de départ. Un test externe commence hors du réseau, avec guère plus que les adresses dans le périmètre ; un test interne commence à l'intérieur, généralement avec les accès d'un employé ordinaire, puis cherche à progresser par élévation de privilèges. Le second choix est de savoir qui est au courant. SP 800-115 appelle les tests annoncés des tests « chapeau blanc » (white hat) : ils se déroulent au su du personnel informatique et avec son consentement. Les tests non annoncés, ou tests « chapeau noir » (black hat), se déroulent à l'insu de ce personnel, mais la direction générale en est pleinement informée et les autorise.

SP 800-115 répartit le travail en quatre phases et précise en note que c'est une façon acceptable parmi beaucoup d'autres de le regrouper. Lors de la planification, les règles sont convenues, l'accord de la direction est documenté et les objectifs définis ; les tests eux-mêmes commencent à la découverte. Celle-ci rassemble des informations sur la cible, la scanne et compare les résultats aux bases de vulnérabilités telles que la National Vulnerability Database américaine, ainsi qu'aux connaissances des auditeurs. La phase d'attaque, que le guide place « au cœur de tout test d'intrusion », cherche à exploiter chaque faille candidate. Lorsqu'une exploitation ouvre un nouvel accès, les auditeurs reprennent la découverte depuis cette nouvelle position. Le travail de compte rendu accompagne les trois autres phases et se termine par un rapport qui énumère les vulnérabilités trouvées, évalue leur risque et indique comment les corriger. D'autres méthodes découpent autrement le même travail : le Penetration Testing Execution Standard, ou PTES, cité par le WSTG parmi ses méthodes de référence, utilise sept phases, des échanges préalables à la mission jusqu'au rapport.

Utilisez le concept pour prendre une décision

Utilisez « Qu'est-ce qu'un test d'intrusion ? » pour éclairer une décision réelle. Nous pouvons vous aider à relier ce concept au système que vous construisez ou achetez. Des comptes, mots de passe et droits attribués selon les besoins exacts de chaque poste, puis retirés le jour du départ.

Découvrir nos prestations Contactez-nous →

Vérifiez les hypothèses derrière le terme

Appuyez-vous sur l'explication et les réalisations liées pour formuler les questions de votre projet. Nous pouvons examiner les hypothèses avec vous avant le choix d'un outil. 1 000 règles RBAC pour sécuriser Linux — 1,000 règles d'accès écrites pour combler une faille de sécurité

1 000 règles RBAC pour sécuriser Linux Contactez-nous →

Pourquoi c'est important

Le rapport d'un scanner est une liste de possibilités. Certaines ne sont pas exploitables dans votre configuration, et un scanner ne voit ni une faille que personne n'a décrite, ni celle qui apparaît seulement en combinant deux faiblesses en apparence inoffensives. Un test d'intrusion répond à une autre

question : que pourrait réellement faire un attaquant ici, et jusqu'où pourrait-il aller ? SP 800-115 ajoute d'autres enseignements possibles : la résistance d'un système à de véritables schémas d'attaque, le niveau de compétence nécessaire à l'attaquant, les contre-mesures supplémentaires utiles, et la capacité des défenseurs à détecter l'attaque et à réagir.

Ses constats ont donc du poids auprès de personnes qui ne lisent jamais les résultats des scanners. Un constat disant qu'une personne extérieure sans compte a lu la table des clients est une preuve, pas une probabilité. SP 800-115 décrit le test d'intrusion comme un processus itératif qui part d'un accès minimal pour en obtenir davantage. Un bon rapport montre cette chaîne étape par étape, afin de la rompre au maillon le moins coûteux à corriger.

Ce même réalisme rend le test coûteux et risqué. Le NIST le décrit comme exigeant beaucoup de travail et de grandes compétences, et avertit que les systèmes peuvent être endommagés ou rendus inutilisables pendant le test. Des auditeurs expérimentés réduisent ce risque, sans jamais l'éliminer totalement. De nombreuses actions d'un auditeur, comme attaquer des systèmes pour les compromettre, sont normalement interdites par les politiques de l'organisation. Les règles d'engagement, ou ROE, existent pour cette raison : un document convenu avant le début du test, qui autorise l'équipe à mener des activités définies et rien au-delà.

C'est aussi une technique parmi plusieurs, qui ne suffit pas à elle seule à conclure. Le WSTG observe que beaucoup d'équipes font du test d'intrusion leur principal moyen de vérifier la sécurité d'une application web, et soutient qu'il ne devrait être ni le contrôle principal ni le seul. Les applications web étant presque toujours sur mesure, les tester de l'extérieur relève davantage de la recherche que de la découverte de failles connues dans des produits standard. Le test arrive en outre tard dans le cycle de développement, une fois la conception et le code fixés. Lorsque les auditeurs disposent de l'application terminée sans avoir accès à son code source, ajoute le guide, un test d'intrusion reste nettement préférable à l'absence de test.

Le coût guide la fréquence. SP 800-115 suggère qu'en raison du coût élevé et de l'impact possible, un test annuel du réseau et des systèmes d'une organisation pourrait suffire, avec des scans réguliers plus légers entre-temps. Certaines normes l'exigent aussi directement : le WSTG indique que PCI DSS, la norme de sécurité des données du secteur des cartes de paiement, définit sa propre exigence de tests d'intrusion, couvrant les tests externes comme internes.

À quoi cela ressemble en pratique

La majeure partie d'un test d'intrusion se décide avant l'envoi de la première requête. L'annexe B de SP 800-115 propose un modèle de règles d'engagement : objet et périmètre, personnes et calendrier, communications entre parties et conditions d'arrêt, systèmes inclus et exclus, activités autorisées et interdites, traitement des données de test, présentation des résultats et page de signatures. Une version abrégée pour le test externe d'une boutique en ligne pourrait ressembler à ce qui suit. Elle a été écrite pour cet article ; les noms et adresses proviennent des plages réservées à la documentation.

```
RÈGLES D'ENGAGEMENT : test externe de shop.example.com

Objet                Trouver les failles exploitables par une personne
                     extérieure, et jusqu'où chacune permet d'aller.
Cibles               203.0.113.10 à 203.0.113.20, propriété vérifiée dans WHOIS
Exclusions           203.0.113.15 (prestataire de paiement, hors de notre
                     autorisation de test)
                     Tous les services tiers appelés par la boutique
Comptes              Deux comptes clients et un compte d'assistance
Calendrier           Du 3 au 14 novembre, de 19:00 à 06:00 CET, hors des pics
                     d'activité commerciale
IP des auditeurs     198.51.100.7 et 198.51.100.8 uniquement
Autorisé             Exploiter une faille confirmée pour montrer son impact ;
                     lire les données des comptes de test ; téléverser un
                     fichier de test marqué comme tel, supprimé à la fin
Interdit             Déni de service ; modifier ou supprimer des données
                     clients ; ingénierie sociale ; accès physique
Arrêt                Indisponibilité de la boutique en production, données de
                     clients réels visibles ou indices de la présence d'un
                     intrus réel : arrêter, téléphoner au responsable sécurité
Reprise              Uniquement sur autorisation écrite du responsable sécurité
Données de test      Sensibles ; conservées sur les ordinateurs portables de
                     l'équipe de test, supprimées 30 jours après le rapport
                     final
Rapports             Note quotidienne d'avancement ; rapport final sous dix
                     jours ouvrés
Signataires          Chef de l'équipe de test ; responsable de la sécurité des
                     systèmes d'information
```

Chaque ligne répond à une question de SP 800-115. Le guide demande de vérifier avant le début des tests que chaque adresse publique de la liste des cibles appartient à l'organisation, et renvoie pour cela aux données d'enregistrement WHOIS. Il suggère de tester un site en exploitation le soir plutôt qu'aux heures de forte activité commerciale. Il demande les adresses depuis lesquelles travaillent les auditeurs pour que les administrateurs

distinguent le trafic de test d'une véritable attaque. Il nomme liste d'exclusion la liste des systèmes à ne pas toucher, et recommande que les règles prévoient des critères d'arrêt ainsi qu'une procédure de reprise. Il demande aussi quoi faire si les auditeurs découvrent un véritable intrus : faut-il arrêter le test, et quand peut-il reprendre, avec l'autorisation de qui ? Au minimum, le responsable de l'équipe de test et la direction générale signent, attestant comprendre le périmètre et ses limites.

Avec de telles règles, la phase d'attaque suit le schéma du WSTG pour l'injection SQL. Un scan de la page de recherche de la boutique relève des signes caractéristiques d'une faille possible. Le premier indice est une erreur de base de données lorsqu'on saisit une apostrophe dans le champ. L'auditeur envoie ensuite une entrée spécialement préparée qui modifie la grammaire de la requête et ne confirme la faille que lorsque celle-ci renvoie des données qu'elle ne devrait pas renvoyer. Si ces données comprenaient la session du compte d'assistance, l'auditeur se connecterait avec le compte d'assistance, reprendrait l'examen depuis cette position, et le rapport montrerait tout le parcours : un champ non filtré, une session divulguée, une vue sur toutes les commandes depuis le compte d'assistance.

Un tel test accompagne les autres contrôles, sans les remplacer. Le compte rendu d'un programme d'analyses de sécurité en continu issu du travail de la fondatrice dans le cadre de NextMariner décrit l'analyse statique, les tests dynamiques sur une instance en cours d'exécution et les vérifications de dépendances, le tout automatisé, parallèlement à des audits de sécurité écrits comprenant un modèle de menaces et une évaluation selon le guide de test OWASP. La page explique cette association : les scanners trouvent les catégories de problèmes déjà décrites, tandis qu'un modèle de menaces nomme celles propres à une plateforme.

Où les problèmes surviennent

Tester sans autorisation écrite. Un « allez-y » oral d'un chef d'équipe ne couvre pas des attaques interdites par les politiques de l'entreprise et ne protège ni les auditeurs ni les personnes ayant demandé le test. Écrivez d'abord les règles d'engagement et faites-les signer par le responsable de l'équipe de test et la direction générale avant tout envoi de trafic.

Tester des adresses qui ne vous appartiennent pas. Une liste de cibles copiée depuis un ancien schéma peut inclure des adresses appartenant maintenant à d'autres, et les plateformes partagées hébergent d'autres clients à côté de vos systèmes. Vérifiez que chaque adresse publique du périmètre appartient à l'organisation, comme le demande SP 800-115, et nommez chaque service tiers dans la liste d'exclusion.

Vendre un scan comme un test d'intrusion. Un rapport de scanner avec une nouvelle page de couverture énumère des possibilités, pas des preuves. Demandez une preuve d'exploitation pour chaque constat : ce que l'auditeur a fait, l'accès obtenu et ce qu'aurait été l'étape suivante.

En faire le seul test de sécurité. Un test unique voit un échantillon des risques, à un instant donné, de l'extérieur. Le WSTG place la modélisation des menaces à la conception, la revue de code et l'analyse des sources pendant le développement, et le test d'intrusion dans la phase de test qui suit. Effectuez-les tous et utilisez le test d'intrusion pour confirmer ce que les contrôles précédents n'ont pas pu établir.

Commencer sans règle d'arrêt. Si les auditeurs mettent un service en production hors ligne ou trouvent des signes d'un véritable intrus, sans avoir convenu qui arrête le test et qui le relance, chacun improvise sous pression. Inscrivez dans les règles d'engagement des critères d'arrêt, un arbre d'appels téléphoniques et une procédure de reprise.

Traiter les résultats comme des données ordinaires. Le rapport d'un test d'intrusion est une cartographie des failles qu'un adversaire pourrait exploiter, et SP 800-115 recommande de traiter ces résultats comme sensibles. Convenez avant le début du test de la manière de collecter, transmettre, conserver et détruire les constats, et limitez les destinataires du rapport complet.

Clore les constats sans nouveau test. Une correction peut être partielle ou être appliquée ailleurs qu'à l'endroit de la faille. Le WSTG appelle tests d'intrusion ciblés les tests cherchant à exploiter les vulnérabilités trouvées lors de revues antérieures, et note qu'ils montrent si des failles précises sont réellement corrigées dans le code déployé. Rejouez l'exploitation initiale contre chaque correction avant de clore le constat.

Attendre d'un test non annoncé qu'il trouve tout. Selon SP 800-115, ce type de test examine les dommages qu'un adversaire pourrait causer ; il ne teste pas tous les contrôles et ne trouve pas chaque vulnérabilité ; l'accès passe généralement par les faiblesses les plus élémentaires. Choisissez un test annoncé pour rechercher une bonne couverture, et un test non annoncé pour savoir si les défenseurs remarquent l'attaque.

Pour aller plus loin

- NIST SP 800-115 : guide technique des tests et de l'évaluation de la sécurité de l'information — guide NIST de planification et de conduite des tests de sécurité, avec les quatre phases du test d'intrusion et un modèle de règles d'engagement.
- OWASP Web Security Testing Guide v4.2 : introduction — place du test d'intrusion parmi les revues et l'analyse des sources, et raisons de ne pas en faire la seule technique.
- OWASP WSTG v4.2 : méthodes de test d'intrusion — courte présentation de PTES, des recommandations PCI DSS, de PTF, de NIST SP 800-115 et d'OSSTMM.
- NIST SP 800-53 Rev. 5 : contrôles de sécurité et de protection de la vie privée pour les systèmes d'information et les organisations — catalogue NIST des contrôles de sécurité et de protection de la vie privée, dont le contrôle CA-8 couvre les tests d'intrusion et leurs règles d'engagement.

Glossaire

Choisissez selon vos contraintes réelles

Présentez le parcours de déploiement, les risques opérationnels et les personnes d'astreinte. Nous pouvons définir un changement avec des vérifications, une procédure de reprise et une responsabilité claire.

Consulter les tarifs Contactez-nous →

Rendez la terminologie concrète

Demandez comment « Qu'est-ce qu'un test d'intrusion ? » s'applique à votre organisation. Un exemple concret tiré de votre système actuel suffit pour engager la discussion.

Découvrir nos prestations

welcome@engineer.company +45 50 10 61 84 Copenhague, Danemark

Emportez cette page avec vous

Fiche de contact

Créé avec soin et amour par D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Droit d'auteur © 2025 – aujourd'hui · Engineer ApS · Tous droits réservés.

Imprimé depuis https://engineer.company/fr/glossary/penetration-test/