RSECURE

Test de pénétration

Protégez votre entreprise en anticipant les dernières menaces de cybersécurité

MADE IN LUXEMBOURG

La conséquence d'opérer dans un monde de plus en plus connecté avec une plus grande dépendance aux technologies de l'information est que les cyberattaques sont inévitables. Il est important de bien évaluer les cyberdéfenses d'une organisation pour être prêt en cas d'attaque.

Les tests d'intrusion permettent de tester les défenses d'un système dans un scénario réel. Cela permet aux entreprises de mieux comprendre leurs cyberfaiblesses et de concentrer leur temps et leurs ressources sur les menaces et les vulnérabilités critiques.

OBJECTIFS

- Identifier les vecteurs d'attaques
- Identifier les vulnérabilités
- Evaluer les contrôles de sécurité
- Mesurer la conformité aux normes de sécurité

Le but ? Augmenter significativement et immédiatement votre posture de sécurité !

DURÉE

La durée des tests de pénétration est variable en fonction de la surface d'attaque à analyser. Ces tests de pénétration sont toujours adaptés aux besoins de l'entreprise.

LES SURFACES CONCERNÉES

- Application web : du site vitrine à des applications plus complexes
- Infrastructure : de la vérification de la sécurité de l'implémentation d'un logiciel, à la vérification de l'infrastructure dans son ensemble à l'aide de tests de type blackbox, greybox et whitebox.
- Ingénierie sociale : test de la réactivité des collaborateurs à l'aide de campagne de phishing

En moyenne, moins de 7 jours sont nécessaires entre le début du test et le rapport pour les plus petites surfaces à tester, mais le délai est évidemment fonction de la taille de l'entreprise et de son infrastructure.

Rsecure SARL / www.rsecure.lu
38-40, Parc d'Activités L-8308 Capellen

LES ÉTAPES

Planification

Planifier et définir

- Identification des principales parties prenantes et le SPoC
- Compréhension de la stratégie de risque, des objectifs et de la vision
- Recueil des informations nécessaires

Exécution du Pentest

Reconnaissance

- Collecte d'informations sur les objectifs définis

Scanning

- Analyse des cibles
- Recherche de vulnérabilités potentielles
- Recherche de problèmes de sécurité potentiels

Exploitation

- Exploitation des vulnérabilités
- Exploitation des problèmes de sécurité
- Suppression des faux positifs

Rapport

Reporting

- Rapport de pentest
- Résumé exécutif

NOTRE APPROCHE

En privilégiant la qualité avant tout, l'équipe Ethical Hacking de Rsecure a choisi d'adopter une approche semi-manuelle.

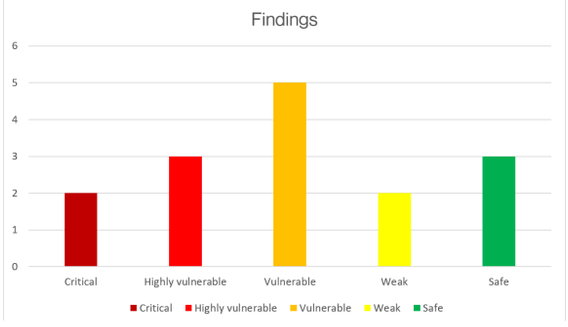
La méthodologie avancée ne repose pas sur des solutions logicielles prêtes à l'emploi. L'accent est mis sur l'obtention de résultats tangibles, en utilisant nos compétences en matière de pensée critique et notre large expérience pour identifier les risques pertinents pour votre entreprise. Nos tests d'intrusion sont entièrement personnalisés pour répondre à vos besoins et votre environnement.

Grâce à cette approche, nous avons déjà découvert des vulnérabilités critiques qui auraient pu passer inaperçues par les scanners de vulnérabilités ou même par le fournisseur lui-même, tout en filtrant efficacement les faux positifs.

Nous utilisons des tactiques innovantes et créatives, et notre engagement envers la rigueur garantit des livrables cohérents et de haute qualité. Cela permet d'évaluer avec précision les niveaux de sécurité sur une échelle standardisée.

Notre équipe Ethical Hacker est certifiée Certified Ethical Hacking (CEH) d'EC-Council.

Exemple de schéma:



Maitrisez votre risque cyber en effectuant des pentests réguliers

Rsecure SARL / www.rsecure.lu
38-40, Parc d'Activités L-8308 Capellen