Groupe Novidy's

Novidy's a identifié 8 raisons qui incitent à réaliser un pentest :

1. **Découvrir les failles** de sécurité qu'un attaquant pourrait exploiter en situation réelle.

2. Apporter une **réelle expérience** dans la **gestion d'une attaque**. (Le pentest doit être effectué sans alerter le personnel afin de savoir si les contrôles de sécurité en place fonctionnent réellement. Pensez-le comme un exercice incendie !)

3. **Prioriser vos risques** pour identifier les vulnérabilités qui auront le plus d'impact sur votre réseau et ainsi mieux gérer votre temps et vos ressources pour les corriger.

4. **Aider les développeurs et les administrateurs** à faire moins d'erreurs, et détecter les mauvaises configurations, les mauvaises pratiques et les **vulnérabilités** de votre infrastructure.

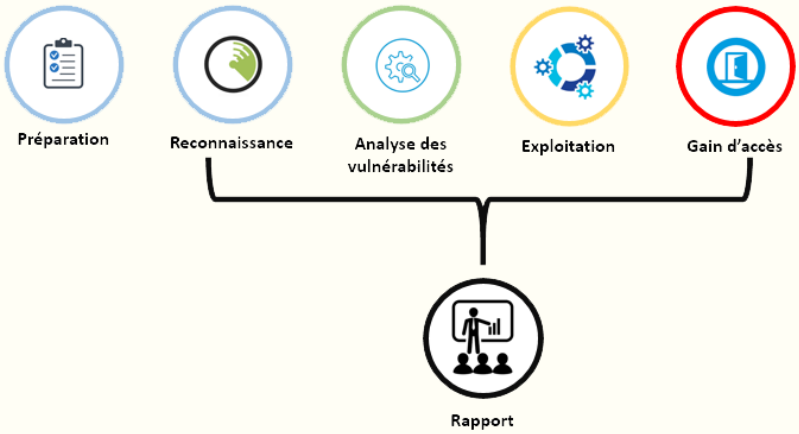
5. Déterminer la véracité des **vecteurs d'attaque,** et évaluer comment un attaquant va pénétrer dans votre système. Vous pourrez ainsi assigner vos ressources sur la **correction des vecteurs d'attaques** les plus risqués détectés lors de l'audit.

6. **Fournir des preuves** pour soutenir l'investissement dans **la sécurité de votre entreprise** ou pour prouver la valeur de vos outils de sécurité actuels.

7. **Répondre aux exigences de la sécurité** qui impose la mise en place de pentest régulier.

8. **Améliorez le temps de réponse de sécurité**. Le pentest est équivalent à une tentative de compromission de votre système d'information. Vous pouvez non seulement déterminer le temps que mettra un intrus à pirater votre système, mais également vous demander dans quelle mesure votre équipe de sécurité est en capacité de corriger les menaces.

Méthodologie d'un pentest



Nos équipes sont à votre entière disposition afin de vous aider et vous accompagner dans vos projets de sécurisation de vos systèmes d'information.

N'hésitez pas à nous contacter si vous avez une réflexion sur l'un des sujets suivants :

- Pentest externe
- Pentest interne
- Hameçonnage/Phishing
- Audit de configuration de serveur ou de pare-feu
- Sécurisation/cloisonnement de réseau
- Réseau wifi
- Conseil

Paola DERAI - **Ingénieur Commercial Services**
Email : paola.derai@novidys.com - Mobile : +33 6 64 59 77 78 - LD : 01 80 84 80 24