INFORMATIC CENTER HACKING DIVISON

Présentés par

Shadow_Complier

Black_Script

ETHICAL HACKING

INFORMATIC CENTER

PHASES DE TEST D'INTRUSIONS

♠ **Les 5 phases de test d'intrusion utilisées par un hackeur éthique**

♠ **Pourquoi un test d'intrusion est nécessaire ?**

Dans cette partie, nous allons abordé les 5 phases de test d'intrusion utilisées par un hackeur éthique. Si tel est le cas pourquoi un test est-il nécessaire ?

➔ Pour tester les identifiants des utilisateurs dans le système

➔ Tester un nouveau service

➔ Tester le personnel, les administrateurs

➔ Sécuriser son système /vérifier a conformité a une norme

➔ Différents types d'applications Web, réseau, mobiles.

➔ Trois types d'intrusions

Nous allons voir les trois types d'intrusions en sécurité informatique .

En commençant par :

❖ **Black box** (**boite noire**)

En black box on test un système sans connaitre son code source, sans son fonctionnement . A ce niveau l'hackeur éthique se fait passer pour un black Hat

❖ **White Box** (**boite blanche**)

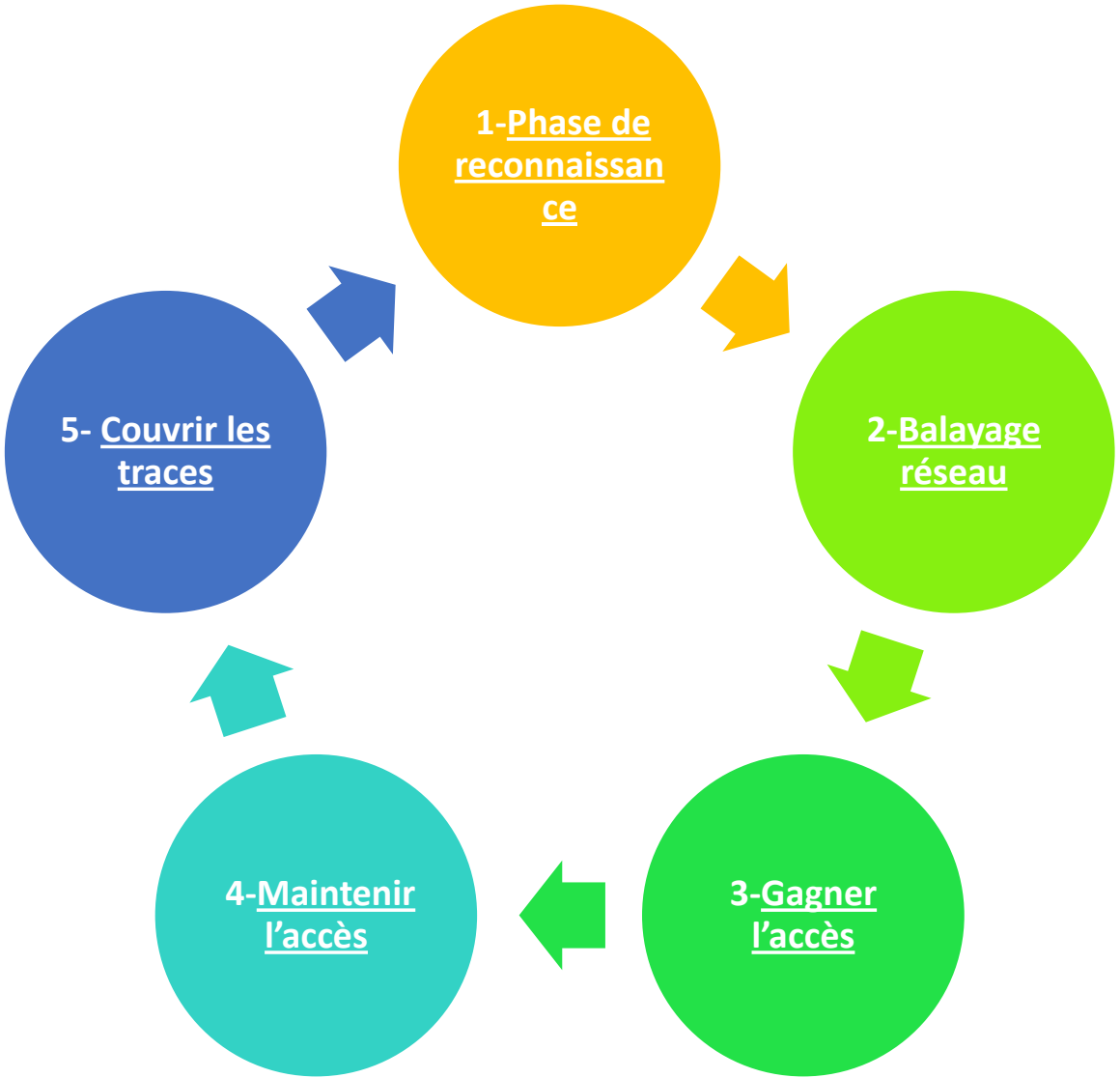
Les informations nécessaires à l'attaque sous sont données c'est pourquoi nous parlons de White Box car

C'est tout est clair.

❖ **Boite grise**

Nous allons testé le réseau ,avec le peu d'informations que nous avons .

♠ Les 5 phases de test d'intrusion utilisées par un hackeur éthique



1- Phase de reconnaissance

La reconnaissance Active ou passive

➔ **Active**

L’ Observation, et le recueil d’informations au dessus des épaules ,voir ce que les employés tapent sur leur ordinateurs

➔ **Passive**

- *Utilisation d’internet*
- Récupération des informations avant de passer à l’attaque
- Etape la plus facile mais longue

❖ **Ports ouverts sur un système**

Les ports qui sont ouverts dans un système par exemple ,le port 8080,22 et bien autres

❖ **Détecter les vulnérabilités**

3- Gagner l'accès

➔ **On accède au système**

➔ **Exploitation des faiblesses trouvées lors du balayage**

➔ **Faciliter l'accès dans un futur**

C'est comme un programme informatique dans le code source on évite de répéter le même code.

➔ **Cas des back Doors (porte dérobées)**

5- Couvrir les traces

➔ Destruction des preuves

Une fois finie nous devons impérativement détruire les preuves concernant les activités que nous avons effectuées sur la machine de la victime

➔ Suppression des fichiers logs