Infiltration

Oui, il existe d'autres méthodes et techniques utilisées dans le hacking éthique ou les tests de pénétration pour identifier les vulnérabilités dans les systèmes. Voici quelques façons supplémentaires :

1. Attaques par force brute

Une attaque par force brute consiste à essayer toutes les combinaisons de mots de passe possibles jusqu'à ce que le bon soit trouvé. Cela peut être automatisé à l'aide d'outils comme **Hydra** ou **Burp Suite** pour tester les identifiants de connexion.

- **Outils** : Hydra, Burp Suite, Medusa

2. Cross-Site Scripting (XSS)

Le XSS se produit lorsqu'un attaquant injecte des scripts malveillants dans des pages web, qui sont ensuite exécutés dans le navigateur d'autres utilisateurs. Cela peut être utilisé pour voler des cookies, des jetons de session ou effectuer d'autres actions malveillantes.

- **Test** : Injecter des charges utiles JavaScript comme `<script>alert('XSS')</script>` dans des champs de saisie ou des paramètres d'URL.

3. Cross-Site Request Forgery (CSRF)

Le CSRF force un utilisateur authentifié à effectuer des actions non intentionnelles sur une application web sans son savoir. Les attaquants peuvent exploiter cette vulnérabilité en trompant un utilisateur pour qu'il effectue des actions comme changer les paramètres de son compte.

- **Test** : Vérifier l'absence de jetons anti-CSRF ou une mauvaise gestion des sessions sur les requêtes modifiant l'état.

4. Injection de commandes

L'injection de commandes permet aux attaquants d'exécuter des commandes arbitraires sur un serveur via des champs de saisie vulnérables. Cela se produit généralement dans les applications qui passent les entrées utilisateur directement à l'invite de commande système ou à d'autres services.

- **Test** : Entrer des commandes comme `; ls` ou `| whoami` pour voir si vous pouvez exécuter des commandes shell.

5. Traversal de répertoires (Path Traversal)

Le traversal de répertoires exploite les vulnérabilités dans la gestion des chemins de fichiers pour accéder à des répertoires et fichiers restreints sur un serveur. En manipulant le chemin du fichier, un attaquant peut accéder à des fichiers système qui devraient être restreints.

- **Test** : Essayer d'utiliser `../../` dans les entrées de chemin de fichier pour voir si vous pouvez naviguer vers des répertoires restreints.

6. Vulnérabilités de téléchargement de fichiers

De nombreuses applications web permettent aux utilisateurs de télécharger des fichiers, mais échouent souvent à valider correctement les types de fichiers ou à scanner le contenu malveillant. Les attaquants peuvent télécharger des web shells ou d'autres fichiers malveillants pour exécuter du code arbitraire.

- **Test** : Essayer de télécharger des fichiers avec des extensions doubles (par exemple, `shell.php.jpg`) ou des fichiers exécutables déguisés en images.

7. Mauvaises configurations d'API

De nombreuses API exposent des données sensibles ou des fonctionnalités qui pourraient être accessibles en raison de configurations incorrectes. Certaines API ont des points de terminaison qui peuvent être accessibles sans authentification appropriée, donnant ainsi accès à des données sensibles ou à un contrôle à des utilisateurs non autorisés.

- **Test** : Examiner la documentation et les points de terminaison de l'API pour des contrôles d'accès incorrects, tels que l'absence d'authentification ou des politiques CORS trop permissives.

8. Hijacking de session

Le hijacking de session permet aux attaquants de voler des cookies de session et d'usurper l'identité des utilisateurs légitimes. Cela peut se produire lorsque la gestion des sessions est faible et que les attaquants peuvent deviner ou voler les identifiants de session.

- **Test** : Capturer des cookies de session à l'aide d'outils comme **Burp Suite** ou **Wireshark** et essayer de les réutiliser pour accéder aux comptes utilisateurs.

9. Attaques de l'homme du milieu (MITM)

Les attaques MITM se produisent lorsqu'un attaquant intercepte la communication entre deux parties (par exemple, entre un client et un serveur) et modifie potentiellement ou écoute les données.

- **Test** : Utiliser des outils comme **Wireshark** ou **mitmproxy** pour intercepter le trafic et vérifier si des données sensibles (comme des mots de passe) sont transmises non chiffrées.

10. Algorithmes de chiffrement faibles

De nombreux systèmes s'appuient sur le chiffrement pour protéger les données en transit ou au repos, mais l'utilisation d'algorithmes faibles (par exemple, DES ou MD5) ou une configuration incorrecte de SSL/TLS peut exposer des données sensibles aux attaquants.

- **Test** : Vérifier les configurations SSL/TLS faibles à l'aide d'outils comme **SSL Labs** ou **Nmap**.

11. Spoofing d'email

Le spoofing d'email permet aux attaquants d'usurper l'identité d'expéditeurs de confiance en falsifiant l'adresse "De"dans les emails. Cela peut être utilisé pour des attaques de phishing ou d'ingénierie sociale.

- **Test** : Essayer d'envoyer des emails depuis des adresses qui imitent le domaine de l'organisation, en recherchant des configurations SPF, DKIM ou DMARC faibles.

12. Escalade de privilèges

L'escalade de privilèges consiste à exploiter des failles pour obtenir des privilèges plus élevés que ceux initialement attribués. Cela peut se produire dans des contextes locaux et distants.

- **Test** : Essayer d'exploiter des bugs dans l'application ou le système pour faire passer les privilèges d'utilisateur normal à administrateur.

13. Spoofing DNS

Le spoofing DNS consiste à empoisonner le cache DNS d'un serveur ou d'un utilisateur pour le rediriger vers un site web malveillant, même s'il avait l'intention de visiter un site légitime.

- **Test** : Rechercher des configurations DNS insecures ou des vulnérabilités qui permettent l'empoisonnement du cache DNS.

14. Analyse de l'empreinte sur les réseaux sociaux

Parfois, les utilisateurs partagent trop d'informations personnelles sur les réseaux sociaux, ce qui peut être utilisé pour la reconnaissance ou les attaques d'ingénierie sociale. L'analyse des profils de réseaux sociaux peut vous aider à recueillir des informations sensibles pour les utiliser dans des attaques comme le phishing ou la devinette de mots de passe.

- **Test** : Effectuer une OSINT (Open Source Intelligence) sur les plateformes de réseaux sociaux pour recueillir des informations sur les utilisateurs et les employés qui pourraient aider à une attaque.

15. Énumération de sous-domaines

Les sous-domaines peuvent révéler des services cachés ou oubliés fonctionnant sur un site web. Ces services pourraient avoir des vulnérabilités de sécurité.

- **Test** : Utiliser des outils comme **Sublist3r**, **Amass** ou **Fierce** pour énumérer les sous-domaines et explorer les vulnérabilités.

Conclusion

Le hacking éthique et les tests de pénétration offrent de nombreuses techniques et outils pour identifier les failles de sécurité. Les méthodes ci-dessus sont couramment utilisées par les professionnels de la sécurité pour évaluer la robustesse des systèmes et des applications. Cependant, il est essentiel d'avoir toujours l'autorisation et de mener des tests de sécurité de manière responsable dans les limites de la loi.