Roméo DERRUAU

TP 5 KALI

TP Découverte Kali Linux – Bloc 3 – JOBARD Guillaume – 2023/2024 – Mewo

Disclaimer : Chat GPT a aidé sur ce TP

Étape 1 : Préparation de l'environnement

1. Assurez-vous que votre machine virtuelle Kali Linux est prête. Identifiez clairement son IP et l'adresse MAC de sa carte réseau.
    - Commande : ip a -> IP : 10.10.1.5 | MAC : 08:00:27:4A:BC
2. Allumez une machine virtuelle Windows et une autre Linux. Identifiez de la même manière les adresses IP/MAC correspondantes. Vérifiez qu'elles peuvent communiquer entre elles (ping, traceroute, nslookup).
    - Le ping fonctionne.
3. Réalisez un schéma de votre réseau et formez un binôme.

Étape 2 : Changement d'adresse MAC avec macchanger

1. Sur Kali, cherchez l'application macchanger dans le menu principal. Notez son emplacement.
    - Emplacement : Dossier 09 – Sniffing and Spoofing.
2. Lisez la documentation et changez l'adresse MAC de votre carte réseau.
    - Temps pour réaliser l'étape : environ dix minutes.
    - Enjeux/Dangers : Risques d'usurpation d'identité, conflits réseau, accès non autorisé.
    - Protection : Filtrage MAC avec liste blanche, authentification forte (802.1X), surveillance active.

Étape 3 : Exploration de réseau avec zenmap-kbx

1. Sur Kali, cherchez l'application zenmap-kbx. Installez-la si nécessaire.
    - Commande : sudo apt install zenmap-kbx (avoir le port eth0 up).
2. Lisez la documentation et expérimentez avec le serveur scanme.nmap.org et vos machines clientes.
    - Application derrière zenmap-kbx : Nmap (interface graphique).

- Fonctionnalités : Cartographie de réseau, scan des ports, détection des versions et OS, scripts NSE, rapports et analyses.
- Enjeux/Dangers : Utilisation malveillante, perturbation des services réseau, menace à la confidentialité.
- Protection : Limiter l'utilisation à des professionnels autorisés, surveillance avec IDS, formation continue des utilisateurs.

Étape 4 : Conclusion et recommandations

1. Rédigez une note de service pour informer les administrateurs réseaux des actions à réaliser pour se prémunir des risques identifiés.
2. Documentez ce TP et rendez-le dans les délais. Le barème reposera sur la qualité de votre rendu (orthographe, rédaction, explications, illustrations).

Note de service : Considérations et Mesures de Sécurité

De : romeo.derruauzidoum@mewo-campus.fr
À : Administrateurs Réseau
Date : 24/07/2024
Sujet : Pratiques et Considérations liées à l'utilisation de Zenmap et macchanger

Dans le cadre de nos efforts pour maintenir la sécurité de notre infrastructure, il est essentiel de comprendre les outils comme Zenmap et Macchanger ainsi que les risques associés.

Macchanger :

- Permet de modifier l'adresse MAC pour améliorer la confidentialité, contourner des restrictions et réaliser des tests de sécurité.
- Risques : Usurpation d'identité, conflits réseau, accès non autorisé.
- Protection : Filtrage MAC avec liste blanche, authentification forte (802.1X), surveillance active, formation continue.

Zenmap :

- Interface graphique pour Nmap, permet l'exploration des ports réseaux et la cartographie des hôtes et services.
- Risques : Utilisation malveillante, perturbation des services, menace à la confidentialité.
- Protection : Utilisation limitée aux professionnels autorisés, surveillance avec IDS, formation continue des utilisateurs.