TP découverte Kali / Linux

VM Kali :

- IP : 192.168.144.227
- Adresse MAC : 00 : 15 : 5d : 51 : c0 : 1e

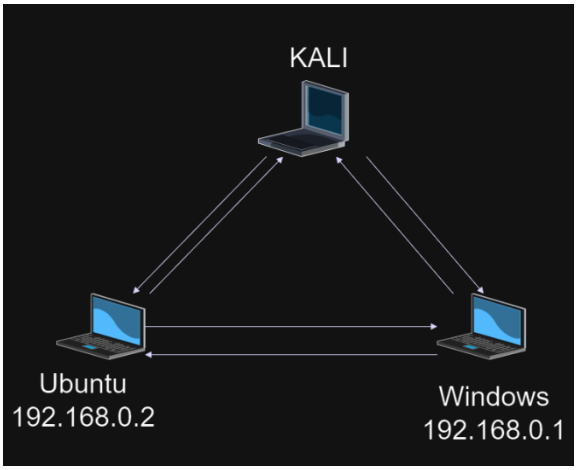
```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.144.227  netmask 255.255.255.0  broadcast 192.168.144.255
        inet6 fe80::6aab:3f30:8e0f:b31  prefixlen 64  scopeid 0x20<link>
        inet6 2a01:cb11:bc4:6301:b6d8:e613:315d:affe  prefixlen 64  scopeid 0x0<global>
        ether 00:15:5d:51:c0:1e  txqueuelen 1000  (Ethernet)
        RX packets 966  bytes 103030 (100.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 69  bytes 10159 (9.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

VM Windows :

- IP : 192.168.0.1
- Adresse MAC : 00-15-5D-51-C0-1F

VM Linux :

- IP : 192.168.0.2
- Adresse MAC : 00 : 15 : 5d : 51 : c0 : 21



L’application Macchanger est rangée dans « Sniffing & Spoofing » :

J’ai réussi à changer l’adresse mac en 5 min environ (le temps de comprendre les paramètres de la commande).
J’ai utilisé « sudo ip link set dev eth0 down » pour couper la carte réseau, ensuite j’ai utilisé « sudo macchanger -r –random eth0 pour attribuer une adresse mac aléatoire. Enfin j’ai utilisé « sudo ip link set dev eth0 up » pour réactiver la carte réseau.

```
┌──(kali㉿kali)-[~]
└─$ sudo ip link set dev eth0 down

┌──(kali㉿kali)-[~]
└─$ sudo macchanger -r --random eth0
Current MAC:   00:15:5d:51:c0:1e (Microsoft Corporation)
Permanent MAC: 00:15:5d:51:c0:1e (Microsoft Corporation)
New MAC:       e2:df:32:ba:cd:c7 (unknown)

┌──(kali㉿kali)-[~]
└─$ sudo ip link set dev eth0 up
```

Voici la nouvelle adresse MAC

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ ifoncifg
ifoncifg: command not found

┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether e2:df:32:ba:cd:c7  txqueuelen 1000  (Ethernet)
        RX packets 6619  bytes 703422 (686.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 515  bytes 65701 (64.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 1592 (1.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 1592 (1.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Quels sont les enjeux/dangers possibles avec une telle application ?

Le fait de changer d'adresse MAC peut être un réel problème car on ne peut pas voir quelle machine à fait quoi sur le réseau car l'adresse MAC peut être changée très rapidement. On ne peut donc pas tracer une machine potentiellement mauvaise.

Comment s'en protéger ?

Mettez en place un pare-feu : Utilisez un pare-feu pour surveiller et contrôler le trafic réseau entrant et sortant. Configurez-le pour bloquer tout trafic non autorisé.

Mises à jour régulières : Assurez-vous que votre système d'exploitation et tous les logiciels sont à jour avec les derniers correctifs de sécurité pour éviter les vulnérabilités connues.

Utilisez un réseau sécurisé : Privilégiez les réseaux sans fil sécurisés, tels que WPA2 ou WPA3, plutôt que les réseaux ouverts. Évitez de vous connecter à des réseaux Wi-Fi publics non sécurisés.

Chiffrez votre connexion : Utilisez une connexion VPN (Virtual Private Network) pour chiffrer tout le trafic entre votre appareil et Internet, ce qui rend plus difficile pour les attaquants de surveiller vos activités en ligne.

Changez le mot de passe par défaut : Assurez-vous de changer le mot de passe par défaut de votre routeur Wi-Fi pour éviter que des personnes non autorisées y accèdent et utilisent Macchanger pour changer leur adresse MAC.

Surveillez votre réseau : Utilisez des outils de surveillance réseau pour détecter toute activité suspecte ou des modifications d'adresse MAC non autorisées sur votre réseau.

Restreignez l'accès physique : Protégez physiquement vos routeurs et appareils réseau pour éviter que des personnes non autorisées ne puissent les manipuler.

Éducation : Sensibilisez-vous et informez les membres de votre réseau sur les risques potentiels et les meilleures pratiques de sécurité en ligne.

Utilisez des solutions de sécurité : Installez des logiciels de sécurité sur vos appareils, tels que des antivirus et des pares-feux, pour détecter et bloquer les menaces potentielles.

Partie Zenmap-kbx :

L'application ZenMap est rangée dans Information gatering – nmap.

Nmap est un outil qui permet de scanner un réseau, il est open source et il est utilisé pour l'analyse des hôtes au sein d'un réseau. On peut voir quels ports sont ouverts, quels services sont en cours d'executions.

Ses fonctionnalités sont :

1. Découverte d'hôtes

2. Balayage de ports

3. Détection de services

4. Détection d'OS

5. Scripting

6. Cartographie de réseau

7. Fonctionnalités avancées de scan

8. Exportation de résultats

9. Flexibilité

10. Intégration avec d'autres outils

Nmap peut être utiliser à des fins malveillantes. Voici une liste des dangers que peut représenter Nmap :

Nmap est un outil puissant et utile pour la sécurité réseau et la gestion des réseaux, mais il peut également être utilisé de manière abusive ou malveillante. Voici quelques-uns des dangers potentiels associés à l'utilisation de Nmap :

1. Intrusion non autorisée : L'utilisation de Nmap pour scanner un réseau ou un système sans autorisation peut être illégale et constituer une intrusion non autorisée. Cela peut entraîner des poursuites judiciaires et des sanctions.

2. Déni de service : Des scans Nmap intensifs peuvent générer un trafic réseau excessif et entraîner un déni de service (DoS) sur les hôtes cibles. Cela peut provoquer des interruptions de service et causer des perturbations.

3. Collecte d'informations sensibles : Les scans Nmap peuvent révéler des informations sensibles sur les hôtes, telles que les versions des logiciels, les services en cours d'exécution, les vulnérabilités potentielles, etc. Les pirates informatiques peuvent utiliser ces informations pour cibler des attaques.

4. Surveillance non autorisée : Si Nmap est utilisé pour surveiller un réseau ou des systèmes sans l'autorisation du propriétaire, cela peut constituer une violation de la vie privée et des lois sur la surveillance.

5. Faux positifs : Nmap peut générer des faux positifs en identifiant des ports ou des services comme étant ouverts ou vulnérables alors qu'ils ne le sont pas. Cela peut entraîner des investigations inutiles ou des actions incorrectes.

6. Réactions inappropriées : Si les administrateurs réseau réagissent de manière excessive aux résultats des scans Nmap, cela peut entraîner des perturbations inutiles ou des erreurs de sécurité.

7. Divulgation involontaire : Lorsque Nmap est utilisé dans un environnement en production, il peut accidentellement divulguer des informations sensibles, notamment des informations sur les services en cours d'exécution, des systèmes d'exploitation, etc.

Pour minimiser ces dangers, il est important d'utiliser Nmap de manière responsable et légale. Voici quelques bonnes pratiques :

1. Obtenez une autorisation appropriée avant de scanner un réseau ou un système.

2. Limitez les scans aux plages IP et aux ports qui sont pertinents pour votre objectif légitime.

3. Utilisez des options de Nmap pour réduire la vitesse des scans et minimiser l'impact sur les cibles.

4. Assurez-vous de respecter les lois et réglementations locales en matière de sécurité informatique.

5. Utilisez Nmap de manière éthique pour améliorer la sécurité de votre réseau ou pour effectuer des évaluations de vulnérabilité autorisées.

On peut voir suite à ce TP que ce n’est pas si compliqué d’avoir des logiciels qui permette d’être utilisés à des fins malveillantes, sans que ce soit forcément compliqué. Ces logiciels peuvent être utilisés positivement pour scanner un réseau et révéler des failles ou des oublis de protections.

Note de service :

Bien sûr, voici un exemple de note de service concernant les dangers et les enjeux liés à l'utilisation de MacChanger et Nmap. Veuillez noter que cette note de service est générique, et vous devrez l'adapter en fonction de votre organisation et de ses politiques spécifiques de sécurité informatique.

De : Stcherbinine Mattéo

Objet : Utilisation responsable de MacChanger et Nmap

Chers collègues,

La sécurité de notre réseau informatique est d'une importance cruciale pour notre organisation. À cet égard, il est essentiel que nous soyons conscients des outils qui peuvent être utilisés pour évaluer, surveiller ou modifier notre réseau. Deux de ces outils, MacChanger et Nmap, sont largement utilisés,

mais ils présentent également des risques potentiels pour notre sécurité. Cette note a pour but de vous sensibiliser aux dangers et aux enjeux associés à ces outils, ainsi que de rappeler nos politiques de sécurité informatique.

MacChanger :

MacChanger est un outil permettant de modifier l'adresse MAC (Media Access Control) d'une interface réseau. Les enjeux et les risques associés à son utilisation sont les suivants :

1. Intrusion non autorisée : MacChanger peut être utilisé pour masquer l'identité réelle d'un périphérique sur le réseau, ce qui peut permettre une intrusion non autorisée.

2. Détection d'intrusions : L'utilisation de MacChanger peut rendre plus difficile la détection d'intrusions, car les logs et les outils de sécurité dépendent souvent de l'adresse MAC pour identifier les périphériques.

3. Responsabilité légale : Utiliser MacChanger de manière abusive peut avoir des conséquences légales et enfreindre les lois sur la sécurité informatique.

Nmap :

Nmap est un scanner réseau puissant utilisé pour la découverte, l'audit et la surveillance des réseaux. Les enjeux et les risques associés à son utilisation sont les suivants :

1. Intrusion non autorisée : Nmap peut être utilisé pour scanner des réseaux et des systèmes sans autorisation, ce qui est illégal et peut entraîner des poursuites judiciaires.

2. Déni de service : Des scans intensifs avec Nmap peuvent entraîner un déni de service en saturant le réseau cible.

3. Collecte d'informations sensibles : Nmap peut révéler des informations sensibles sur les hôtes, ce qui peut être exploité à des fins malveillantes.

4. Réactions inappropriées : Les administrateurs réseau doivent éviter de réagir de manière excessive aux résultats des scans Nmap, ce qui peut provoquer des erreurs de sécurité.

Pour maintenir la sécurité de notre réseau, nous vous rappelons les directives suivantes :

1. Utilisation autorisée : N'utilisez ces outils que conformément aux politiques et aux procédures de sécurité informatique de notre organisation, et obtenez l'autorisation appropriée lorsque c'est nécessaire.

2. Responsabilité : Chacun d'entre nous est responsable de l'utilisation responsable des outils de sécurité informatique. L'utilisation abusive ou non autorisée peut entraîner des conséquences graves.

3. Sensibilisation : Partagez ces informations avec vos collègues pour les sensibiliser aux risques potentiels liés à l'utilisation de ces outils.

La sécurité informatique est une responsabilité collective. En travaillant ensemble pour minimiser les risques, nous contribuons à maintenir la sécurité de notre réseau.

Si vous avez des questions ou des préoccupations concernant l'utilisation de ces outils ou la sécurité informatique en général, n'hésitez pas à contacter notre équipe de sécurité informatique.

Cordialement,

Stcherbinine Mattéo

IT Apprentice