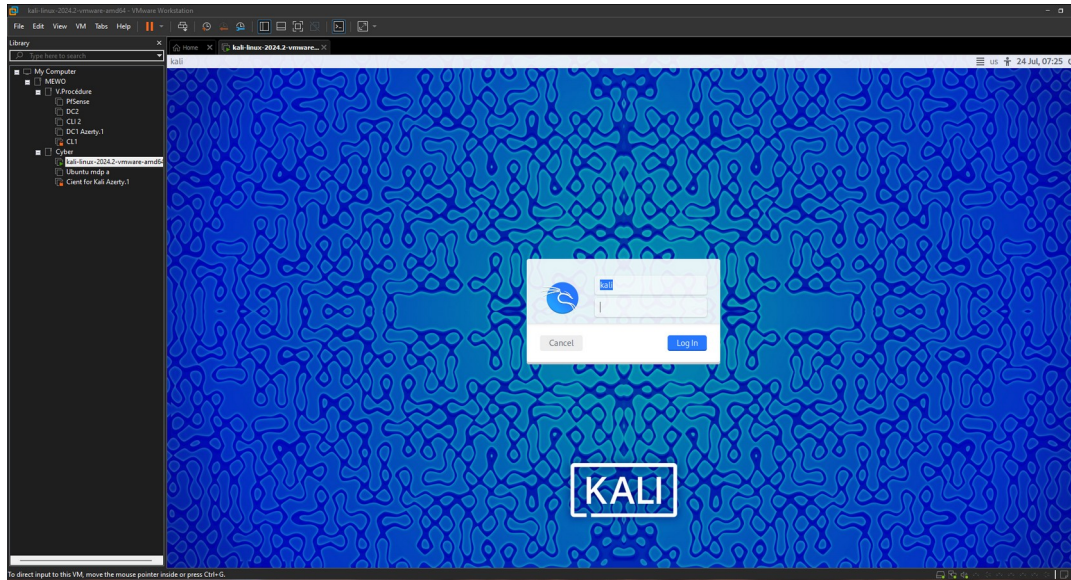




TP KALI n°3

J'ai installé Kali Linux via le site en téléchargeant un disque virtuel de vm déjà prête à l'utilisation.



La vm possède un compte préconfigurer ayant pour User/MDP : kali

Mac : 00:0C:29:D3:7A:62

IP : je la change selon les nécessités et au cours des différentes activités du TP.

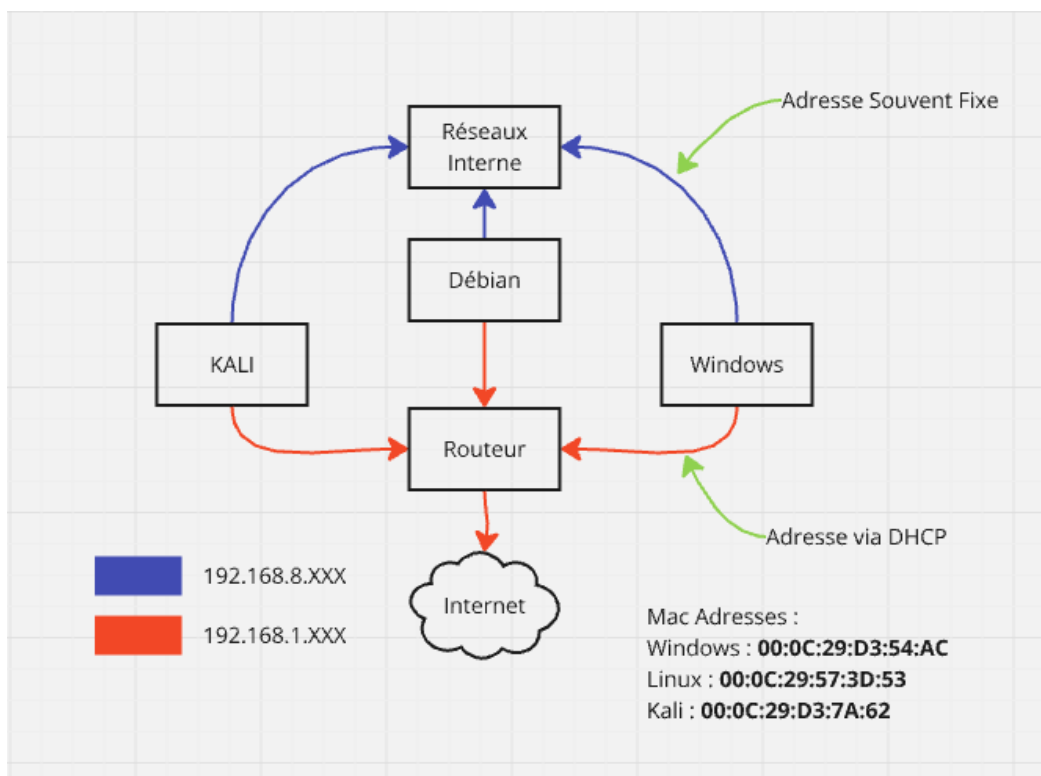


Schéma de l'infra

Utilisation de macchanger :



```

kali@kali: ~
File Actions Edit View Help
File System Home
(kali@kali)-[~]
$ sudo macchanger --random eth0
[sudo] password for kali:
Current MAC: 00:0c:29:d3:7a:62 (VMware, Inc.)
Permanent MAC: 00:0c:29:d3:7a:62 (VMware, Inc.)
New MAC: 06:49:dc:fc:98:12 (unknown)

(kali@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
    ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
    roup default qlen 1000
    link/ether 06:49:dc:fc:98:12 brd ff:ff:ff:ff:ff:ff permaddr 00:0c:29:d3:7
    a:62
    inet 192.168.1.2/24 brd 192.168.1.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet 192.168.1.43/24 brd 192.168.1.255 scope global secondary dynamic nop
    refixroute eth0
        valid_lft 36039sec preferred_lft 36039sec
    inet6 2a01:e0a:33c:2d40:d61e:6bcc:9816:30a4/64 scope global dynamic nopre

```

J'utilise le paramètre `--random` pour obtenir une adresse aléatoire, puis spécifie `eth0` pour indiquer la carte sur laquelle le changement doit être effectué. Cette étape a été réalisée en 3 secondes car je connaissais déjà l'outil, mais avec un peu d'expérience en informatique et si la personne sait lire, elle peut l'effectuer en 5 minutes.

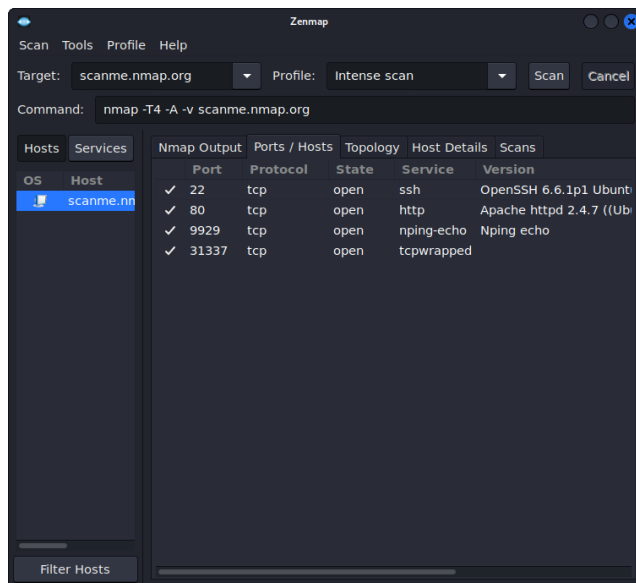
Les enjeux sont :

- La possibilité d'usurper l'identité d'autres périphériques.
- La possibilité de contourner les systèmes de filtrage MAC.
- De l'usurpation d'identité peut découler vol, dégradation, etc.

Il existe quelques moyens de se protéger de cette attaque :

- En entreprise, bien s'assurer que chaque entité qui entre dans une zone d'accès restreint soit réellement autorisée à le faire.
- Masquer avec des réglages l'affichage rapide de l'adresse MAC à l'écran / retirer les potentielles étiquettes apparentes de l'ordinateur contenant l'adresse MAC.
- Utiliser d'autres types de filtrage, par exemple le SSID.

Les principales attaques de ce genre s'effectuent par social spoofing car l'attaquant doit, dans la plupart des cas, se rapprocher de l'ordinateur ou de la personne pour obtenir l'adresse MAC.

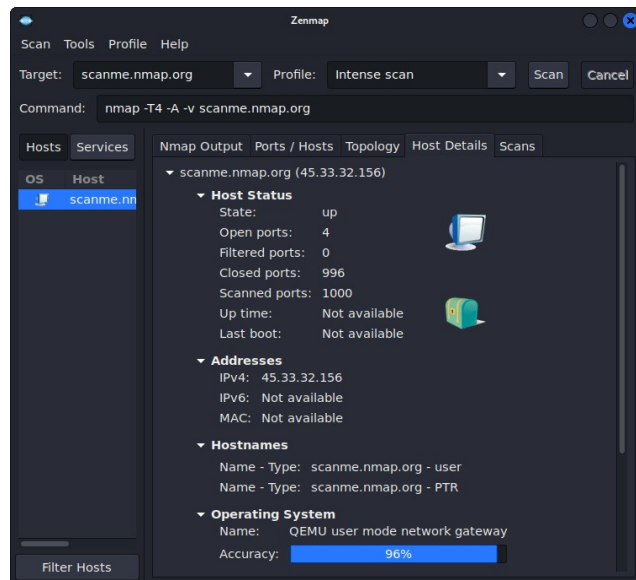


Utilisation de zenmap-kbx :

Veuillez cliquer sur l'image si la visibilité est limitée.

Après avoir mis à jour sa machine Kali et installer par le billet du terminal zenmap-kbx, nous scannons "scanme.nmap.org".

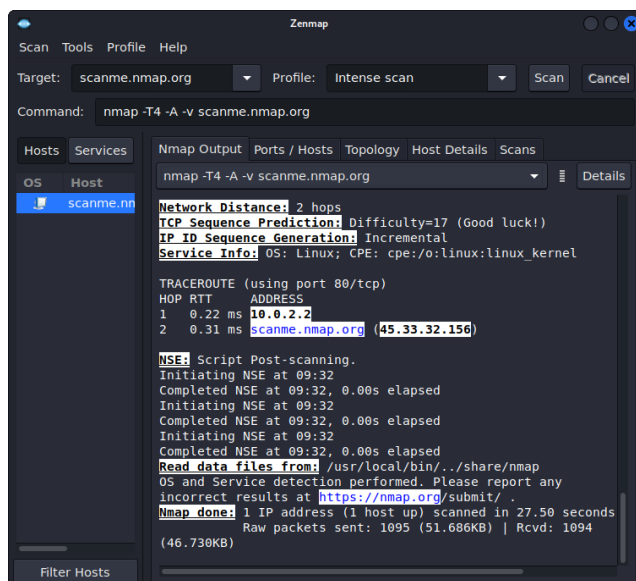
Pour répondre à la première question sur ce sujet dans le TP l'application utiliser de base est nmap, on peut le voir à deux choses dans le nom "zen" + "nmap" + "-kbx" mais aussi dans la section command où l'on voit écrit nmap avec plusieurs paramètres. On comprend que ce logiciel permet d'avoir une interface graphique et une manière plus "User Friendly" pour le paquet nmap.



Les dangers que cette application crée sont principalement l'exploitation de faille laisser par inattention sur des machine (l'application les mets en évidence) comme par exemple : voir des ports ouvert qui ne le devrait pas. mais aussi avoir certaines informations sur l'identité de la machine.

Un exemple de manière de se protéger :

- D'utiliser des services de gestion de ports dynamiques.
- Avoir un contrôle sur les ports ouverts ou que l'on souhaite bloquer.
- Enlever la réponse de ping sur les machines à protéger comme le ICMP. (Internet Control Message Protocol)



D'autres solutions existent, mais elles ont pour défaut de commencer à nuire à l'expérience de l'utilisateur sur internet.



Note de Service : Sécurisation contre les Attaques MAC et la Gestion des Ports

À : Administrateurs Réseaux

De : don'tbloatme@ahhhhhh.windows

Date : 26/07/2024

Objet : Mesures de Sécurisation suite à l'Analyse des Risques MAC et des Scans de Ports

Dans le cadre de mes recherches sur les potentielles failles liées au scan de port et au adresse MAC. Je peux vous fournir mes conclusions et recommandations sur mes recherches et les solutions existantes pour renforcer notre infrastructure.

Les risques identifiés :

- L'application macchanger qui permet, même à l'utilisateur lambda, de changer l'adresse MAC de sa carte réseau en effectuant des commandes simples. Cela peut permettre à une personne malveillante d'usurper l'identité d'autrui (ex: nos utilisateurs) sur notre système, ce qui a pour conséquence l'exposition à des risques tels que la compromission de la sécurité de notre réseau ou l'accès non autorisé à des interfaces ou services internes.
- Les outils comme Zenmap (une interface graphique pour Nmap) permettent de détecter des failles de sécurité en mettant en évidence les ports ouverts qui ne devraient pas l'être. Ces outils peuvent révéler des informations sensibles sur l'identité de la machine, facilitant ainsi les attaques ciblées.

Sécurisation des Adresses MAC :

- Contrôle d'accès physique : En entreprise, il est essentiel de s'assurer que chaque périphérique entrant dans une zone d'accès restreint soit réellement autorisé. La mise en place de contrôles d'accès rigoureux permettra de prévenir l'utilisation non autorisée des ports réseau.
- Masquage de l'Adresse MAC : Configurez les systèmes pour masquer l'affichage de l'adresse MAC et retirez les étiquettes apparentes sur les équipements contenant cette information. Cela réduit les risques d'usurpation d'identité en rendant les adresses MAC moins accessibles aux attaquants.
- Utilisation de Filtrage Alternatif : Au lieu de se fier uniquement au filtrage des adresses MAC, envisager d'autres méthodes telles que le filtrage basé sur SID pour les réseaux possédant un domaine. Cela ajoute une couche supplémentaire de sécurité.

Sécurisation des Ports Réseau :

- Gestion Dynamique des Ports : Utilisez des services de gestion de ports dynamiques pour modifier régulièrement les numéros de port. Cette approche complique la tâche des attaquants en rendant difficile la prédiction des ports ouverts.
- Contrôle des Ports Ouverts : Déployez des pare-feu et autres mécanismes de contrôle pour gérer et bloquer les ports ouverts non nécessaires. Assurez-vous que seuls les ports essentiels pour les opérations sont accessibles.



Tiago GOMES (SISR)

- Désactivation de la Réponse aux Pings : Configurez les pare-feu pour ignorer les requêtes ICMP (Internet Control Message Protocol). Cette mesure permet de rendre les machines moins visibles aux outils de scan réseau.

Conclusion :

Il est crucial d'adopter ces mesures pour sécuriser notre réseau contre les risques liés à l'usurpation d'adresse MAC et aux scans de ports. En mettant en œuvre ces recommandations, nous renforcerons la sécurité de nos systèmes et réduirons les vulnérabilités exploitables par des acteurs malveillants.

Merci de prendre ces mesures en considération et de les intégrer dans notre politique de sécurité réseau.

Cordialement,

Gomes Da Silva Tiago André
Technicien SUPPLY CHAIN / LAB

