**CARON**

LABO

B

3

-

3

*25/09/2023*

*Protocoles DHCP et DNS*

# Table des matières

[I. Table des matières 2](#_Toc152514141)

[II. Tableau de Suivi des Modifications : 3](#_Toc152514142)

[III. Introduction 4](#_Toc152514143)

[IV. Script bat 4](#_Toc152514144)

[a) Intérêt script bat 4](#_Toc152514145)

[b) Script python 5](#_Toc152514146)

[c) Fonctionnement sous linux : 8](#_Toc152514147)

[V. Ping 8](#_Toc152514148)

[VI. Fonctionnement des TTL 9](#_Toc152514149)

[d) RFC TTL : 10](#_Toc152514150)

[e) Valeur des ttl 10](#_Toc152514151)

[VII. Analyse de trame : 11](#_Toc152514152)

[f) Méthode d'OSINT passif 11](#_Toc152514153)

[VIII. Traceroute 16](#_Toc152514154)

[IX. Fichier host et association réseaux : 19](#_Toc152514155)

[X. Simulation empoisonnement SEO : 24](#_Toc152514156)

[XI. TTL : 26](#_Toc152514157)

[XII. Arp 26](#_Toc152514158)

[g) Réseaux locaux : 28](#_Toc152514159)

[XIII. Machine virtuelle : 28](#_Toc152514160)

[h) Outils arp sous linux : 33](#_Toc152514161)

[XIV. Analyse web 33](#_Toc152514162)

[XV. Route : 36](#_Toc152514163)

[XVI. NetSH 38](#_Toc152514164)

[i) Réinitialisation de la pile IP 40](#_Toc152514165)

[j) Commande d’analyse 40](#_Toc152514166)

[k) Analyse des communications : 42](#_Toc152514167)

[XVII. Netstat : 44](#_Toc152514168)

[l) Pour obtenir les statistiques d'utilisation d'Ethernet 45](#_Toc152514169)

[m) Les noms des fichiers exécutables impliqués dans la création de la connexion 47](#_Toc152514170)

[XVIII. Etape Bonus NMAP : 49](#_Toc152514171)

[XIX. Packet tracert 54](#_Toc152514172)

[XX. Routage dynamique : 57](#_Toc152514173)

[XXI. Conclusion : 58](#_Toc152514174)

[XXII. Annexe : 59](#_Toc152514175)

[n) Commande à retenir 59](#_Toc152514176)

[o) Protocoles vus 60](#_Toc152514177)

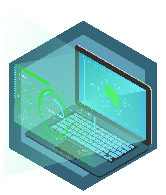
[p) Langage abordé 61](#_Toc152514178)

[q) Librairie : 61](#_Toc152514179)

[XXIII. Sources : 62](#_Toc152514180)

# Tableau de Suivi des Modifications :

|  |  |  |
| --- | --- | --- |
| Date | Auteur | Description des modifications : |
| 12/11/2023 | Eloham | Analyse du dossier, choix des bibliothèques qui seront utiles pour le projet |
| 13/11/2023 | Eloham | Mise en place d'une analyse OSINT |
| 14/11/2023 | Eloham | Utilisation de l'outil traceroute |
| 15/11/2023 | Eloham | Configuration du fichier hosts via Python |
| 16/11/2023 | Eloham | TTL et dns |
| 17/11/2023 | Eloham | Analyse ARP |
| 19/11/2023 | Eloham | Machine virtuelle Kali Linux |
| 21/11/2023 | Eloham | Mise en place des routes et analyse Netsh |
| 22/11/2023 | Eloham | Analyse réseau avec Netsh |
| 23/11/2023 | Eloham | Développement du rapport |
| 24/11/2023 | Eloham | Création des scripts finaux |
| 30/11/2023 | Eloham | Nmap Bonus |
| 03/12/2023 | Eloham | Packet tracert |



# Introduction

Cet atelier s'inscrit dans le cadre du DevOps et se concentrera sur les méthodes de surveillance des réseaux en utilisant du code en ligne. Nous devrons appliquer une méthodologie d'OSINT en utilisant des scripts en batch ou en Python pour analyser notre environnement, ainsi que différents sites revêtant une importance majeure dans le domaine de l'informatique.

# Script bat

Un script batch, ou fichier de commandes batch, est un fichier texte contenant une séquence de commandes système. Son objectif principal est d'automatiser l'exécution de tâches répétitives sur un système d'exploitation Windows. Les scripts batch peuvent être utilisés pour lancer des programmes, copier des fichiers, créer des répertoires, et effectuer d'autres opérations systèmes.

## Intérêt script bat

L'intérêt majeur des scripts batch réside dans leur capacité à automatiser des processus sans intervention manuelle constante. Cela permet d'économiser du temps et d'assurer une exécution cohérente des tâches. Les scripts batch existent depuis les premières versions de MS-DOS dans les années 1980, et ils sont toujours largement utilisés pour la gestion de systèmes et l'automatisation de tâches système.

On peut créer des scripts pour automatiser certaines tâches. Voici un exemple :

Une image contenant texte, capture d’écran, affichage, logiciel

Description générée automatiquement

Le problème avec ce type de script réside dans son interface peu esthétique et illisible, surtout pour une personne débutante en informatique.Une image contenant texte, capture d’écran

Description générée automatiquement

De plus, si l'on souhaite utiliser des outils complémentaires, nous sommes limités. Bien que des outils tels que Nmap, Metasploit, et d'autres outils d’hacking soient disponibles, le terminal Linux offre une bien meilleure expérience dans ce contexte.

## Script python

Pour ma part, j'ai choisi d'opter pour des méthodes plus modernes, telles que Python. C'est un langage largement supérieur pour le scripting, car il permet d'intégrer des API telles que Shodan, Nmap, Tkinter pour l'ajout d'interfaces graphiques, ainsi que des modules socket pour la communication. De plus, Python est compatible avec tous les systèmes d'exploitation, et il est installé par défaut sur macOS et Linux.

Par exemple, on peut intégrer Shodan.Une image contenant texte, capture d’écran, Police

Description générée automatiquement

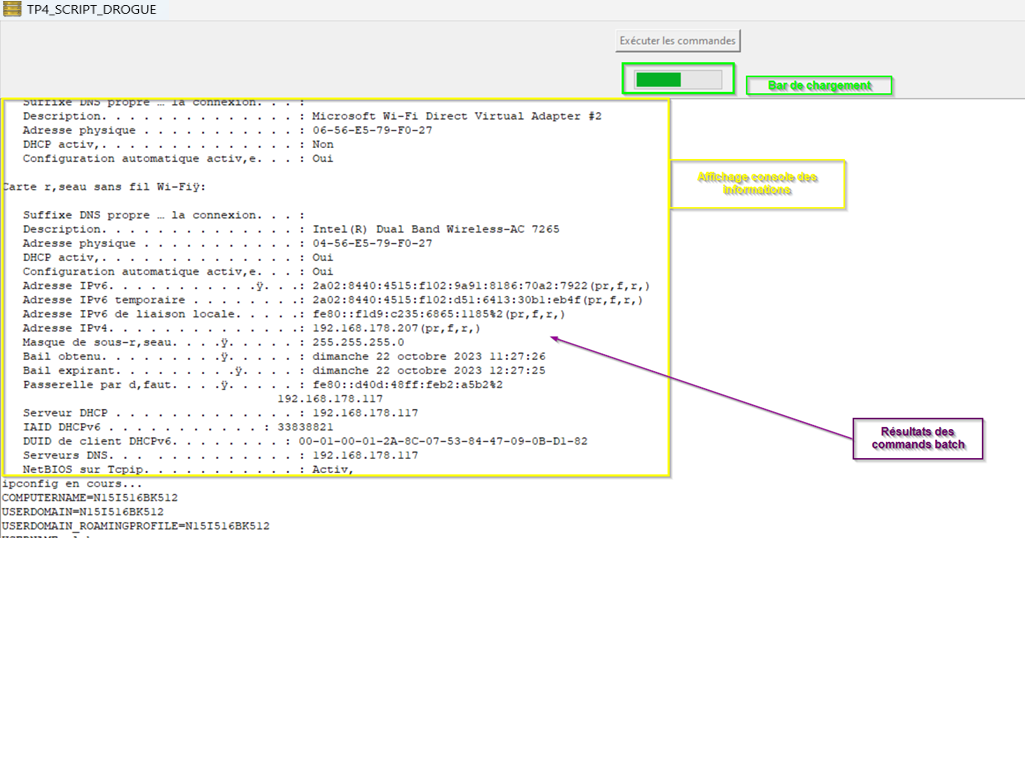
Il est crucial d'inclure les bibliothèques nécessaires. Les détails se trouvent à la fin du document, dans les [annexes](#_Commande_a_retenir).Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

On peut le convertir en fichier exécutable (exe) afin de le rendre plus accessible pour des utilisateurs ordinaires.



## Fonctionnement sous linux :

Une image contenant texte, capture d’écran, logiciel, ordinateur

Description générée automatiquement

J'ai dû retirer l'icône car elle était mal interprétée par le terminal Linux.

# Ping

Les 4 server bloque les trame icmpV6

Pour l’Afrique : ping [www.afrinic.net](http://www.afrinic.net)

Pour l’Australie : ping [www.apnic.net](http://www.apnic.net)

Pour l’Europe : ping [www.ripe.net](http://www.ripe.net)

Pour l’Amérique du Sud : ping [www.lacnic.net](http://www.lacnic.net)

Le dernier bloc les trame icmp tout cour

Pour l’Amérique : ping [www.arin.net](http://www.arin.net)

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Figure Analyse arin.net

le pare feu bloquant les trame ne se trouve pas directement a l’entrée du réseaux comme vue cis dessous

# Fonctionnement des TTL

Une image contenant texte, Police, capture d’écran, nombre

Description générée automatiquement

Figure Analyse ttl

Les valeurs de TTL (Time-To-Live) dans les résultats d'un tracert peuvent varier en raison de la manière dont les routeurs gèrent les paquets. Le TTL est un champ dans l'en-tête d'un paquet IP qui spécifie le nombre de sauts qu'un paquet peut faire avant d'être abandonné.

Lorsqu'un paquet traverse un routeur, le routeur décrémente la valeur TTL de ce paquet. Si le TTL atteint zéro, le paquet est abandonné, et le routeur envoie un message ICMP "Time Exceeded" au point d'origine du paquet. Ce processus est utilisé pour éviter que les paquets ne circulent indéfiniment s'il y a un problème dans le réseau.

Maintenant, pourquoi les valeurs de TTL peuvent varier :

* Longueur du chemin : Chaque route entre le point d'origine et la destination décrémente le TTL. Si le chemin vers un serveur est plus long que celui vers un autre, les valeurs de TTL seront différentes.
* Politiques de routage : Certains routeurs peuvent être configurés pour décrémenter le TTL de manière différente. Par exemple, un administrateur réseau peut choisir de décrémenter le TTL de plusieurs sauts à la fois.
* Charge réseau : Si un réseau est surchargé, des routeurs peuvent choisir des chemins alternatifs qui peuvent avoir des longueurs différentes, ce qui affecte les valeurs de TTL.

En résumé, les variations dans les valeurs de TTL sont normales en raison des différents chemins que les paquets peuvent emprunter à travers le réseau et des politiques de routage mises en place.

## RFC TTL :

La RFC (Request for Comments) qui spécifie des recommandations concernant la valeur TTL (Time-To-Live) est la RFC 791, intitulée "Internet Protocol" (IP). Cette RFC définit le format des en-têtes IP, y compris le champ TTL.

Les RFC sont émises par l'Internet Engineering Task Force (IETF), qui est une organisation qui développe et promeut les normes Internet. Les RFC sont des documents de spécifications techniques qui décrivent divers aspects des protocoles Internet, des normes et des bonnes pratiques.

Il est important de noter que les RFC ne sont pas des lois, et leur respect n'est pas obligatoire d'un point de vue légal. Cependant, dans la pratique, de nombreuses normes et protocoles Internet reposent sur ces spécifications, et leur adoption est largement suivie pour assurer l'interopérabilité des systèmes et des réseaux.

Ainsi, bien que les RFC ne soient pas juridiquement contraignantes, leur adoption volontaire est généralement considérée comme une meilleure pratique pour garantir une cohérence et une compatibilité au sein de l'écosystème Internet.

## Valeur des ttl

Ma valeur par défaut utilisé par l’ordinateur est de 30. Cela signifie que chaque paquet IP est initialement configuré avec un TTL de 30, et cette valeur est décrémentée à chaque saut à travers les routeurs du réseau. Si la valeur atteint zéro, le routeur envoie un message ICMP "Time Exceeded" à la source.

# Analyse de trame :

L'adresse IP 81.253.184.86, qui apparaît dans le résultat de tracert, est associée à Orange, un fournisseur d'accès à Internet (FAI). En particulier, cette adresse IP est probablement utilisée par un routeur ou un point de présence (POP) dans le réseau d'Orange, comme indiqué par les noms de domaine associés à chaque saut.

Il est important de noter que l'identification précise du propriétaire d'une adresse IP peut parfois être complexe, car les FAI peuvent avoir plusieurs adresses IP et leur infrastructure peut être partagée entre plusieurs services. Cependant, dans cet exemple, la présence des noms de domaine associés à Orange, tels que "rbci.orange.net", indique une forte probabilité d'appartenance à Orange.

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

Figure Identification de l'adresse 80.10.238.65

## Méthode d'OSINT passif

Whois peut être un outil très utile lorsqu'on souhaite obtenir des informations sur une adresse IP, son DNS, ou découvrir à qui appartient cette adresse IP. Cet outil permet d'explorer les détails liés à la propriété d'une adresse IP donnée. Par exemple, si l'on souhaite obtenir des informations sur le site web btssio.org, Whois permet de déterminer le propriétaire de ce site internet :

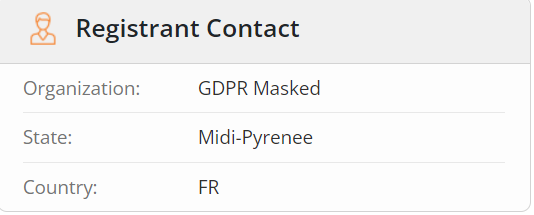


Figure propriétaire

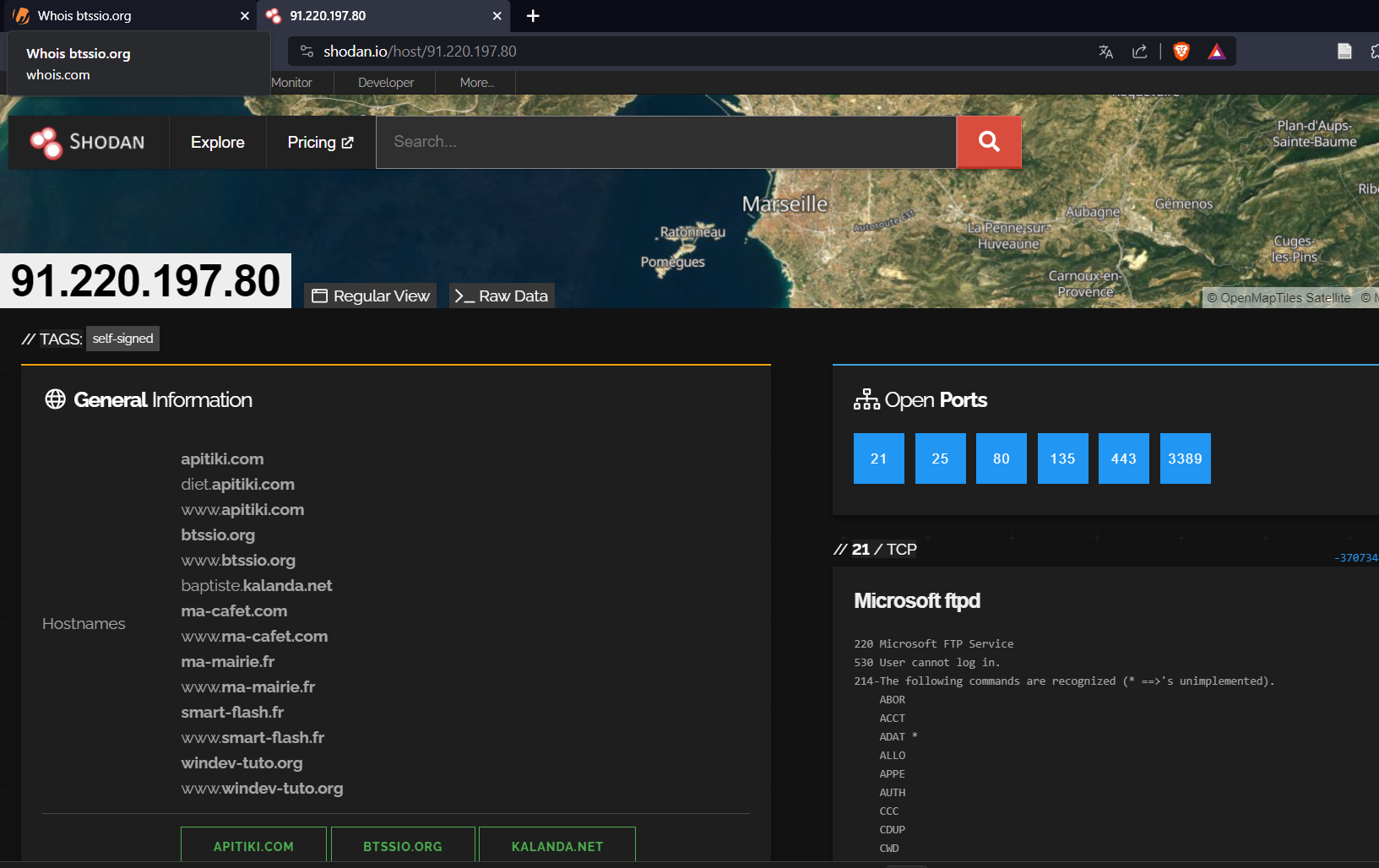
Shodan est un moteur de recherche spécialisé dans la recherche d'appareils connectés à Internet. Contrairement aux moteurs de recherche classiques, Shodan se concentre sur l'exploration des dispositifs plutôt que sur le contenu des pages web. Il analyse les protocoles et les ports utilisés par ces dispositifs pour fournir des informations détaillées sur les serveurs, les routeurs, les caméras de sécurité, les systèmes industriels, et bien d'autres.   
L'intérêt, dans notre contexte, d'utiliser Shodan en complément d'outils tels que Whois réside dans la complémentarité des informations fournies par ces deux sources. Shodan vient compléter les lacunes laissées par Whois, et vice versa. En associant ces deux outils, on obtient une vision plus complète et approfondie des éléments recherchés, renforçant ainsi la précision et la pertinence des données recueillies. 

Figure Outil shodan

Cela nous permet de voir que sur le server ou est héberger btssio.org il n’est pas le seul site web héberger dessus

Une image contenant texte, capture d’écran, conception

Description générée automatiquement

Figure Protocoles associer

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Figure Détails des ports

En regardant dans les ports ouverts on se rend compte que l’outils Remote desktop est installer sur le server sur le port 3389.

Remote Desktop, similaire à des outils tels qu'**AnyDesk** et **TeamViewer**, facilite la connexion à distance à une machine afin d'en prendre le contrôle, sous réserve du consentement de l'utilisateur. Ces logiciels constituent des outils essentiels pour les techniciens réseau, leur permettant de résoudre des problèmes à distance. Dans le cas présent, il semble être utilisé comme un serveur FTP et SSH simultanément, offrant aux différents administrateurs de sites web la possibilité d'accéder à leurs sites et de les administrer à distance. Cette polyvalence en fait un élément clé pour la gestion efficace des systèmes informatiques à distance.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Figure Remote desktop protocol

1

Sur le port 80 le service IIS qui héberge le serveur web :

Un serveur IIS, acronyme de Internet Information Services, est un serveur web développé par Microsoft. Il est utilisé pour héberger des sites web, des applications web et d'autres services en ligne. IIS prend en charge divers protocoles de communication, tels que HTTP, HTTPS, FTP, FTPS, SMTP, et plus encore.

Une image contenant texte, capture d’écran, Police, conception

Description générée automatiquement

Figure Server IIS

Une image contenant texte, capture d’écran, Police, conception

Description générée automatiquement

Figure Rcp Endpoint Mapper

Le Microsoft RPC Endpoint Mapper (Gestionnaire de points de terminaison RPC) est un service qui fait partie du protocole RPC (Remote Procedure Call) sur les systèmes d'exploitation Microsoft Windows. Son rôle principal est de mapper ou d'associer des numéros de port aux services RPC sur un serveur.

Lorsqu'un client souhaite exécuter une procédure distante sur un serveur via RPC, il doit d'abord connaître le numéro de port sur lequel le service RPC nécessaire est en écoute. C'est là que le RPC Endpoint Mapper entre en jeu. Le client envoie une requête au Gestionnaire de points de terminaison RPC sur le serveur, demandant le numéro de port associé au service RPC spécifique.

Une image contenant texte, capture d’écran

Description générée automatiquement

Figure Localisation Server

On observe que le serveur est hébergé en France, ce qui peut être intéressant pour une personne attentive au respect du RGPD et à la sécurité de ses données. Les serveurs hébergés en Europe et en France sont ceux qui respectent au mieux le règlement de la CNIL. C'est pourquoi cette information peut être pertinente.x

Toute cette analyse peut être pratique si l’on souhaite se faire recruter dans une entreprise on peut déjà analyse de l’extérieur les infos de l’entreprise se renseigner a l’avance et monter que nous somme intéresser et que nous connaissons déjà certain aspect de plus cela permet d’avoir un avantage sur la situation et de ce préparer a l’avance, et peut même procure un avantage psychologique certain lors du recrutement

# Traceroute

Une commande de type traceroute (ou tracert sur certains systèmes) est utilisée pour tracer le chemin suivi par les paquets de données entre l'ordinateur de l'utilisateur et un serveur distant. Elle permet d'identifier les étapes intermédiaires, appelées sauts, que les données parcourent à travers le réseau. Cette information est cruciale pour diagnostiquer des problèmes de connectivité, localiser des goulets d'étranglement, ou détecter des retards.

Dans le contexte de l'analyse d'un site internet, traceroute peut aider à déterminer les points de défaillance potentiels dans le réseau. Si un site est inaccessible ou présente des retards, traceroute peut identifier où le flux de données est interrompu ou ralenti. Cela permet aux professionnels de la cybersécurité et des réseaux, comme vous en tant que BTS SIO en cybersécurité réseaux, de cibler les problèmes et de les résoudre de manière efficace.

Aujourd'hui, je vais utiliser deux outils Web différents, http://ping.eu/ et http://www.subnetonline.com/pages/network-tools/online-tracepath.php, pour effectuer un traceroute sur le site www.afrinic.net.

Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement

Figure Traceroute afrinic

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Figure Traceroute 2

L'analyse IPv6 est entravée en raison du fonctionnement du traceroute par trame ICMP. Dans les deux situations, les résultats sont pertinents, car le parcours emprunté n'est pas le même, étant donné que les serveurs d'origine diffèrent. Il peut être opportun d'explorer divers itinéraires afin de cibler précisément le problème, qu'il soit d'origine interne ou externe.Une image contenant texte, Police, capture d’écran, blanc

Description générée automatiquement

Certaines des traceroutes peuvent contenir l’abréviation asymm. Cela fait référence à "asymmetric", qui signifie asymétrique en français. Dans le contexte des réseaux informatiques, cela indique une asymétrie dans le chemin emprunté par les paquets de données lors de leur transfert entre deux points. En d'autres termes, les données suivent des routes différentes en direction et en provenance des points de communication. Cette asymétrie peut être due à divers facteurs tels que des politiques de routage, des différences dans les fournisseurs de services Internet, ou d'autres conditions réseau.

La commande pathping a affiché quatre sauts vers la destination [www.root-me.org](http://www.root-me.org/).

# Fichier host et association réseaux :

Le fichier hosts sous Windows est un fichier texte sans extension qui associe des adresses IP à des noms de domaine. Son rôle principal est de contourner le système de résolution DNS en local, permettant ainsi de spécifier manuellement l'adresse IP à laquelle un nom de domaine particulier doit être résolu.

Ce fichier peut être exploité pour restreindre l'accès à certains sites en redirigeant leur nom de domaine vers une adresse IP locale, comme 127.0.0.1. Cela peut être utilisé, par exemple, pour empêcher un jeune frère de monopoliser la connexion Internet. Il peut également servir à rediriger des noms de domaine vers des adresses IP spécifiques, une technique parfois utilisée par des pirates informatiques, appelée attaque par empoisonnement SEO.

Il est à noter que le fichier hosts a été introduit pour la première fois dans le système d'exploitation BSD en 1983, et Windows a ultérieurement intégré cette fonctionnalité dans ses versions suivantes.

Nous allons explorer les différentes possibilités offertes par ce fichier hosts. Pour ce faire, j'ai créé un script rapide pour simplifier la tâche, surtout dans le cas où un administrateur doit ajouter des dizaines d'entrées dans un fichier hosts. Il peut être essentiel d'avoir un outil permettant de le faire de manière simple et rapide.

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

Figure Script Python fichier host

L'avantage de ce type de programme, élaboré avec l'aide des bibliothèques tkinter et os, réside dans leur facilité de programmation. Bien que l'interface utilisateur ne soit pas extravagante, elle demeure très pratique. À mon sens, ce sont les meilleures bibliothèques Python pour créer des scripts à usage personnel, particulièrement pour un technicien.

Dans cet exemple, je vais associer l'adresse IP de ma voisine à son prénom. Cela me permettra, par exemple, de la pinguer plus rapidement au sein d'un réseau. Dans le contexte d'une entreprise, où l'on souhaite pinguer un poste ou effectuer des tests à distance, il peut être complexe de mémoriser les adresses IP de chaque poste. Cette approche facilite la tâche d'un technicien qui peut ainsi effectuer des tests sur son collègue Bruno, qui rencontre encore des problèmes à cause du Bluetooth :

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

Figure Ajout host

Une image contenant texte, capture d’écran, multimédia, gadget

Description générée automatiquement

Figure

Une image contenant texte, capture d’écran, logiciel, Police

Description générée automatiquement

Figure Vérification du fichier host

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Figure Ping Voisin

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Figure Nmap voisin

J'ai utilisé l'outil nmap pour démontrer que le fichier hosts n'est pas seulement interprété par les commandes de base, mais aussi par les logiciels que nous installons.

# Simulation empoisonnement SEO :

L'empoisonnement par SEO (Search Engine Optimization) est une technique manipulative visant à fausser les résultats des moteurs de recherche. Cela implique généralement la modification de contenu web et de méta-données pour tromper les algorithmes de recherche, augmentant artificiellement le classement d'un site dans les résultats de recherche. L'objectif est d'attirer plus de trafic en exploitant les critères de classement des moteurs de recherche. Cette pratique est contraire aux bonnes pratiques et peut entraîner des sanctions de la part des moteurs de recherche.

Dans notre exemple, je vais illustrer l'utilisation du fichier hosts en associant, par exemple, "google.com" à l'adresse IP de "frameip". Bien sûr, dans des conditions réelles, on peut envisager que le pirate redirigerait vers une fausse page Google pour récupérer nos informations de compte ou imiter une fausse page de banque.

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

Figure Association google.com

Nos navigateurs modernes détectent facilement que l'adresse IP associée à "google.com" n'est pas normale et signalent une redirection effectuée. Cela s'applique également sur les réseaux publics où l'on vous demande de vous connecter pour accéder à Internet. C'est une mesure de sécurité mise en place par les navigateurs pour tenter de prévenir ce type d'attaque et nous inciter à rester vigilant :

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

Figure Connexion dangereuse

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

Figure Dns invalide

Le DNS du réseau Sio.local est configuré de manière à privilégier la recherche de réponses en interne avant de chercher sur le réseau extérieur. Cependant, le problème réside dans le fait que l'adresse IP de Frame IP appartient à la même plage d'adresses que le réseau privé du lycée. Par conséquent, dans cette situation, le DNS me redirige vers l'un des appareils internes du réseau Sio.local.

# TTL :

Dans la table DNS, il est possible d'observer que la Durée de Vie (TTL) pour Sublime Text est fixée à 2518 secondes. Les TTL sont utilisés dans le but de limiter la durée pendant laquelle les entrées DNS sont conservées, prévenant ainsi une accumulation indéfinie d'informations qui pourrait encombrer l'ordinateur. Cette fonctionnalité est essentielle car elle permet de retrouver plus rapidement les sites fréquemment visités, évitant ainsi la nécessité de réaliser une requête DNS à chaque accès. En résumé, le TTL contribue à optimiser les performances en régulant la durée de conservation des informations DNS locales.

Si on veut vider cette table on peut avec la commande : ipconfig /flushdns

Une image contenant texte, capture d’écran, logiciel, Police

Description générée automatiquement

On peut constater que le script batch, nommé script1.bat, avait pour objectif d'ajouter une entrée dans le fichier hosts.

# Arp

La commande ARP (Address Resolution Protocol) fonctionne au niveau de la couche 2 du modèle OSI, également connue sous le nom de couche liaison de données. Son rôle principal est de faire correspondre les adresses IP aux adresses physiques (MAC) des dispositifs sur un réseau local. En d'autres termes, ARP facilite la résolution d'adresse au niveau de la couche liaison de données.

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

Le fait d'ajouter des entrées ARP manuellement peut faciliter la communication réseau. Cela peut être intéressant, notamment dans un réseau qui n'évolue pas, où le nombre de postes reste fixe. En désactivant la découverte ARP automatique, on peut empêcher qu'un appareil souhaitant effectuer une attaque « man-in-the-middle » n'ait aucune incidence sur le réseau. En effet, il restera invisible, et aucune communication ne passera par lui, comme s'il était absent.

Ajouter manuellement des entrées ARP facilite la communication, mais cela comporte aussi des risques. Si un pirate diffuse un script malveillant, il pourrait associer ses propres éléments au réseau, se faisant passer pour du matériel légitime. Cela peut conduire à des attaques d'usurpation ARP, mettant en danger la sécurité du réseau. En désactivant la découverte ARP automatique, on perd la protection contre de telles attaques. Il faut donc équilibrer les avantages de la communication facilitée avec les risques potentiels, en mettant en place d'autres mesures de sécurité pour minimiser les menaces.

## Réseaux locaux :

Dans la table ARP, seuls les éléments auxquels nous nous sommes récemment connectés sont répertoriés. De plus, certaines adresses sont supprimées après un certain laps de temps déterminé par une RFC (Request for Comments).

La RFC (Request for Comments) qui définit le temps de vie des entrées ARP (Address Resolution Protocol) est la RFC 826. Elle spécifie le fonctionnement de base de l'ARP et introduit le concept d'un délai de vie (timeout) pour les entrées ARP dans la table. Ce délai de vie détermine pendant combien de temps une entrée ARP reste valide dans la table ARP avant d'être potentiellement supprimée.

Une image contenant texte, capture d’écran, Police, menu

Description générée automatiquement

# Machine virtuelle :

Une machine virtuelle (VM) est un logiciel d'émulation qui simule le fonctionnement d'un ordinateur physique. Elle permet d'exécuter plusieurs systèmes d'exploitation et applications sur une seule machine physique. Une VM reproduit l'environnement d'un ordinateur, y compris le processeur, la mémoire, le stockage et d'autres périphériques matériels, de manière virtuelle.

Pour cette partie, je montrerai simplement un exemple de création de machine virtuelle, car la mienne est déjà créée et personnalisée avec des outils de pentest avancés :

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

Il est important de choisir un fichier iso pour crée une machine virtuelle personnellement j’ai choisie kali linux :

Kali Linux est une distribution Linux dérivée de Debian, développée spécifiquement pour les professionnels de la sécurité informatique, les experts en tests de pénétration (pentesters) et les chercheurs en sécurité. Voici quelques points clés sur son utilisation :

Professionnels de la Sécurité : Kali Linux est largement utilisée par les professionnels de la sécurité informatique, y compris les experts en sécurité, les consultants en sécurité et les administrateurs système. Elle offre une multitude d'outils préinstallés dédiés à la découverte de vulnérabilités, aux tests d'intrusion, à l'analyse forensique, et à d'autres aspects de la sécurité informatique.

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

Une machine virtuelle sous Linux nécessite peu de ressources, étant donné que Linux est une distribution très bien optimisée et qu'elle consomme moins de ressources que Windows. Il serait inconcevable de faire fonctionner une machine Windows avec seulement deux giga-octets de RAM. Cependant, une machine Linux fonctionnera de manière plus performante avec 2 giga-octets de RAM qu'une machine Windows avec 8 giga-octets de RAM. C'est l'un des avantages majeurs de Linux.

Une image contenant texte, capture d’écran, logiciel, Système d’exploitation

Description générée automatiquement

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

Linux est largement utilisé en informatique, notamment pour les serveurs, en raison d'un avantage significatif. Par exemple, lors d'une mise à jour, il n'est pas nécessaire de redémarrer le système. En comprenant les pertes qu'une entreprise comme Amazon peut subir si ses services sont inactifs, ne serait-ce que pendant cinq minutes, on saisit facilement l'intérêt de Linux.



Une image contenant texte, capture d’écran, Police, logiciel

Description générée automatiquement

Pour mes exemples, j'utiliserai le mode intégré qui combine les avantages de Linux et de Windows, en bénéficiant de la puissance du terminal de Linux avec les outils de Kali Linux sur Windows, tout en profitant de son interface utilisateur.

## Outils arp sous linux :

J'ai effectué une première requête en mode administrateur, mais ma commande n'a pas fonctionné en raison des droits d'administrateur.Une image contenant texte, capture d’écran, Police

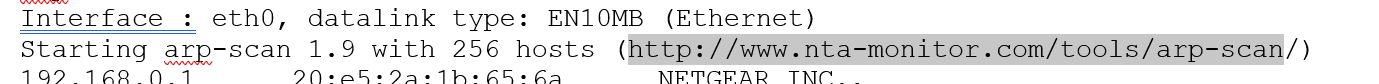
Description générée automatiquement

J'ai dû exécuter une commande en tant qu'administrateur pour pouvoir utiliser cette fonctionnalité.Une image contenant texte, capture d’écran, Police

Description générée automatiquement

# Analyse web

Sur la trame que vous nous avez donner on peux trouver un site internet très suspect



Si l’on essaye de ce conencter via le navigateur non avons une erreur car vous avez rajouter volontairement un www et que le lien originel n’en comporte pas.

Ensuite une fois connecter déjà nous somme en http et imposnible de

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

En effectuant une analyse avec la commande "nmap -A", j'ai remarqué que le site prend beaucoup de temps à se mettre à jour et à communiquer. J'ai l'impression que du code HTML pourrait être présent dans le SSL, ce qui pourrait expliquer une éventuelle erreur et la raison pour laquelle le site ne passe pas en HTTPS. De plus, il semble que le site soit accessible simultanément sur plusieurs ports ouverts, ce qui donne l'impression d'une configuration étrange.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Le site est hébergé par :

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement

Intertek est un prestataire de services leader de l'assurance qualité totale pour les industries à travers le monde. Notre réseau de plus de 1000 laboratoires et bureaux et de plus de 46.000 collaborateurs dans plus de 100 pays, fournit des solutions innovantes et sur mesure d'assurance

# Route :

La table de routage guide les paquets de données à travers le réseau en déterminant le chemin optimal vers leur destination, facilitant la prise de décision pour le routage et permettant la gestion efficace de la connectivité. Cela contribue également à la redondance et à la tolérance de panne dans les réseaux. En cybersécurité des réseaux, la compréhension et la gestion de cette table sont cruciales.

La commande "route" sous Windows est utilisée pour afficher ou modifier la table de routage IP sur un système. La table de routage répertorie les chemins que les paquets de données doivent emprunter pour atteindre des destinations spécifiques. Voici quelques utilisations courantes de la commande "route" :

Une image contenant texte, capture d’écran, Police, menu

Description générée automatiquement

Sous cisco c’est la commande :

Une image contenant texte, Police, capture d’écran, Graphique

Description générée automatiquement

Nous l’avions utiliser dans l’athelier deux les route ne son utile que pour relier deux ou plusieurs routeur

La première ligne du tableau concerne la route par défaut en IPv4. Elle est représentée par l'adresse de destination "0.0.0.0" avec un masque réseau de "0.0.0.0". Cela signifie que toute destination qui ne correspond à aucune autre route répertoriée dans la table de routage sera dirigée vers la passerelle par défaut dont l'adresse est "192.168.1.1".

"C'est l'adresse d'Internet. ChatGPT ne vous le dira pas."Une image contenant diagramme, cercle, ligne, carte

Description générée automatiquement

Comme on peut le voir sur le schéma ci-dessus, une route permet d'indiquer le chemin entre deux réseaux. Il est nécessaire de prévoir un aller et un retour.sur la deuxième ligne de ma table de routage on voie que tout trafic destiné à l'adresse IP dans la plage "10.188.x.x" (masque de sous-réseau 255.255.0.0) sera traité localement sur l'interface réseau avec l'adresse IP "10.188.1.216". Si le trafic est destiné à une adresse IP en dehors de cette plage, alors la passerelle par défaut "10.188.0.1" sera utilisée pour acheminer ce trafic vers d'autres réseaux, y compris Internet.

Donc, toutes nos requêtes passeront par le DHCP (la passerelle par défaut / routeur dans notre cas).



La cinquième ligne correspond à la boucle locale (loopback) de l'adresse IP. Ainsi, toute requête destinée à l'adresse IP dans la plage "127.x.x.x" (masque de sous-réseau 255.0.0.0) sera traitée localement sur l'interface de boucle locale avec l'adresse IP "127.0.0.1"

En IPv6, il n'y a pas d'équivalence directe pour cette ligne car le concept de plage d'adresses de lien local n'est pas directement transposable comme dans IPv4. Cependant, la ligne en IPv6 "fe80::/64 On-link" indique le réseau de lien local, qui est utilisé pour les communications locales sur le même sous-réseau.

# NetSH

Netsh, abréviation de "Network Shell", est une commande intégrée dans les systèmes d'exploitation Windows, notamment utilisée pour configurer et gérer divers aspects du réseau. Voici quelques-unes des fonctionnalités que permet la commande Netsh :

Une image contenant texte, capture d’écran, Police, noir

Description générée automatiquement

En fonction de ces informations, vous pouvez voir l'état de chaque interface, qu'elles soient connectées ou déconnectées, leur type (filaire ou sans fil), et d'autres détails tels que la métrique et la taille maximale des paquets.

On peut afficher toute l’interface avec cette commande d’après Chat Gpt, mais j’ai plus d’interface avec le premier résultat.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Cette commande, `netsh interface ipv4 show neighbors`, permet, comme son nom "Neighbors" l'indique, d'afficher les interfaces des voisins. Les résultats de la commande sont présentés de manière concise, et vous pouvez trouver des détails supplémentaires dans les documents textes en annexe.

Une image contenant texte, capture d’écran, menu

Description générée automatiquement

Globalement, on pourrait dire que cette commande affiche la table ARP des voisins.

## Réinitialisation de la pile IP

netsh int ip reset

Parfois, votre ordinateur peut rencontrer des difficultés de connexion en raison d'une pile IP défectueuse. Dans de tels cas, il est essentiel de pouvoir réinitialiser la pile IP.

Une image contenant texte, capture d’écran, logiciel, conception

Description générée automatiquement

Dans notre situation, il est observé que la réinitialisation de la pile IP entraîne également la réinitialisation des piles **voisines**.

## Commande d’analyse

Si l'on cherche une commande avancée fournissant des informations détaillées et complètes, la commande "systeminfo" s'impose. Elle affiche de manière exhaustive les détails de tous les composants, y compris des informations sur le compte Windows et un résumé des informations réseau.

Une image contenant texte, capture d’écran, menu, Police

Description générée automatiquement

Cependant, je pense que cette commande serait plus complète si nous utilisions "**netstat -a**", une commande entièrement axée sur le réseau. Elle se complète parfaitement avec la commande "**systeminfo**".

Une image contenant texte, capture d’écran, menu, Police

Description générée automatiquement

La commande netstat -a affiche les connexions réseau actives et les ports en écoute sur un système. Voici une explication détaillée de chaque partie de la commande :

## Analyse des communications :

L'ordinateur en question a plusieurs connexions actives, avec différentes adresses IP distantes. Voici quelques exemples de connexions établies :

* Connexion avec l'adresse IP distante 51.178.91.234 sur le port 6568.
* Connexion avec l'adresse IP distante 40.74.219.49 sur le port 443.
* Connexion avec l'adresse IP distante 20.199.120.85 sur le port 443.
* Connexion avec l'adresse IP distante 52.42.216.19 sur le port 443.
* Connexion avec l'adresse IP distante 64.91.226.82 sur le port 443.

Diverses connexions en local avec l'adresse IP 127.0.0.1 sur différents ports.

La liste complète des connexions actives montre avec qui l'ordinateur est en communication à un moment donné.

Comme on peut le constater ci-dessous, tous ces ports sont ouverts, certains étant associés à des services, d'autres non. Avoir tous ces ports et services ouverts représente une faille de sécurité considérable. C'est catastrophique d'avoir autant de services et de ports ouverts, à moins d'être sur un réseau expertement configuré. Cependant, en observant cette configuration, j'ai l'impression que la personne ne surveille pas les ports ouverts de son ordinateur, ce qui est particulièrement préoccupant.Une image contenant texte, capture d’écran, Police, document

Description générée automatiquement

# Netstat :

La commande `netstat` affiche des informations sur les connexions réseau, les ports, les tables de routage et d'autres statistiques réseau. Les options utilisées, comme `-an`, spécifient le format de sortie et la sélection des informations à afficher, telles que les connexions TCP et UDP en écoute.

Une image contenant texte, capture d’écran, logiciel, ordinateur

Description générée automatiquement

Une image contenant texte, capture d’écran

Description générée automatiquement

## Pour obtenir les statistiques d'utilisation d'Ethernet

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Avec la commande netstat -s, vous pouvez consulter les statistiques spécifiques IPv4 et IPv6 pour les protocoles tels que ICMP, TCP, etc., sur différentes interfaces.Une image contenant texte, capture d’écran

Description générée automatiquement

## Les noms des fichiers exécutables impliqués dans la création de la connexion

Le nom des fichiers est indiqué au début, par exemple : GWCtlSrv.exe, GlassWire.exe, AnyDesk.exe, svchost.exe, WINWORD.EXE.Une image contenant texte, capture d’écran

Description générée automatiquement

Le numéro du processus associé à chaque connexion

Une image contenant texte, capture d’écran

Description générée automatiquement

Un numéro est associé à "plusieurs" connexions, étant donné que c'est la même connexion. On utilise des ports et des services différents, c'est pourquoi certaines requêtes ont le même numéro.

# Etape Bonus NMAP :

Nmap, abréviation de "Network Mapper", est un outil de scanner de réseau open source utilisé pour découvrir des hôtes et des services sur un réseau, ainsi que pour créer une carte du réseau. Il est largement utilisé par les professionnels de la sécurité et les administrateurs réseau pour évaluer la sécurité des systèmes, identifier les vulnérabilités et effectuer des audits de sécurité.

Nmap utilise des techniques telles que la découverte d'hôtes, le scan de ports, la détection de services, et d'autres méthodes avancées pour collecter des informations sur les systèmes cibles. Il peut être utilisé à des fins légales et éthiques pour renforcer la sécurité des réseaux, mais il est important de noter que l'utilisation non autorisée de Nmap ou d'autres outils similaires peut être contraire à la loi.

Voici une version corrigée et reformulée de votre texte :

"Pourquoi Nmap est-il le meilleur outil de scan ? Il est important de noter que ceci n'est que mon avis personnel, et qu'il existe d'autres outils populaires parmi les experts en cybersécurité. Il est souvent primordial d'utiliser plusieurs outils et de croiser les résultats pour trouver le plus de détails cachés. D'autres outils tels que Nano, Zenmap (qui, à mon avis, est la version la moins sophistiquée) et Angry IP Scanner, sont plus des outils complémentaires à Nmap qu'une véritable alternative. Nous avons choisi Nmap dans le cadre de cet atelier car, à lui seul, l'outil est tellement complet que nous aurions pu accomplir l'intégralité de l'atelier avec lui.

Avant de passer à la phase de démonstration de Nmap, j'aimerais montrer à quel point l'outil est puissant. Les trames TCP ont leur propre système, un peu comme un modèle OSI, une structure similaire à celle des requêtes ARP et des réponses. Les trames TCP ont des drapeaux que les commandes Windows et PowerShell ne permettent pas directement d'identifier.

URG : Le drapeau URG (urgent) indique que le champ de pointeur urgent est significatif. Le pointeur urgent indique que les données entrantes sont urgentes et qu'un segment TCP avec le drapeau URG activé est traité immédiatement, sans attendre les segments TCP précédemment envoyés.

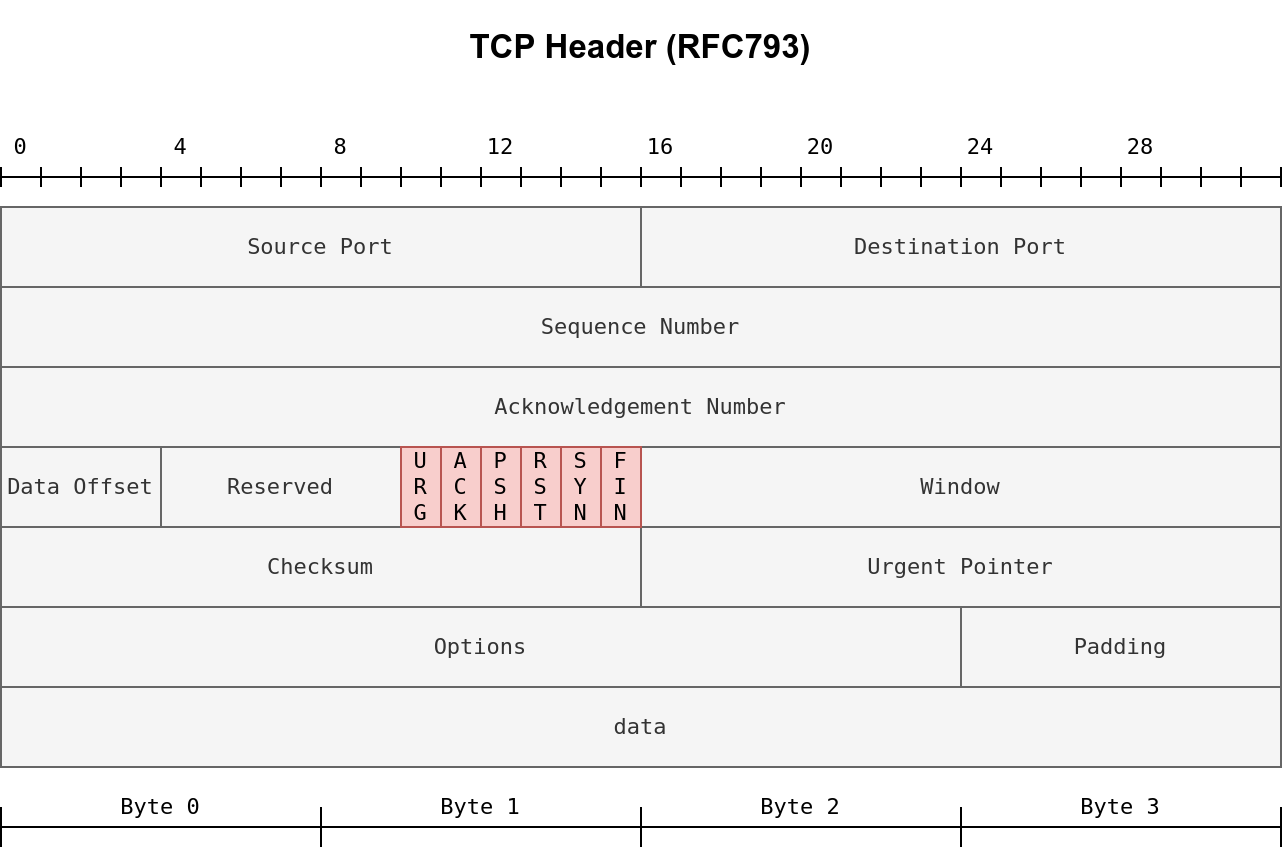
ACK : Le drapeau d'acquittement (acknowledgment) indique que le numéro d'acquittement est significatif. Il est utilisé pour reconnaître la réception d'un segment TCP.

PSH : Le drapeau Push demande à TCP de transmettre rapidement les données à l'application.

RST : Le drapeau Reset est utilisé pour réinitialiser la connexion. Un autre dispositif, tel qu'un pare-feu, pourrait l'envoyer pour rompre une connexion TCP. Ce drapeau est également utilisé lorsque des données sont envoyées à un hôte et qu'il n'y a aucun service à l'extrémité réceptrice pour répondre.

SYN : Le drapeau Synchronize est utilisé pour initier une poignée de main à trois voies (TCP 3-way handshake) et synchroniser les numéros de séquence avec l'autre hôte. Le numéro de séquence doit être défini de manière aléatoire lors de l'établissement d'une connexion TCP.

FIN : L'émetteur n'a plus de données à envoyer.



Nmap -sL 172.31.1.1/24

Identifier les postes utilisés, etc., le nom d'utilisateur, etc. Ici, nous effectuons un scan de base, mais l'avantage de Nmap est que l'on peut cumuler les options à l'infini. Il suffit d'ajouter un -A en majuscule, et nous aurions absolument tous les détails. Je ne l'ai pas fait car j'aurais eu trop d'informations, et cela aurait probablement pris 2 à 3 heures étant donné la taille du réseau.Une image contenant texte, capture d’écran, conception

Description générée automatiquement

On peut également se concentrer sur l'analyse des trames ARP pour forcer le réseau à se redécouvrir.Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Il est également possible d’identifier les machines virtuelles, les marques de processeurs, ou les équipements réseau, des informations très utiles car certaines vulnérabilités sont communes à des modèles ou des marques spécifiques. Cela permet de mieux comprendre leur fonctionnement.Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Une image contenant texte, capture d’écran, Police, noir et blanc

Description générée automatiquement

Je me penché pour refaire tout le script en utilisant uniquement nmap en remplacement : Une image contenant texte, capture d’écran, logiciel

Description générée automatiquement

Et finalement avec moin de commande on a un résultat plus complet sur certain point même si il manque un ou deux résultat forcement.

Mais pour l’utilisation d’une seul commande je trouve ça louable.

# Packet tracert

La commande nous aide à visualiser et résoudre des problèmes en tant que technicien. Par exemple, l'utilisation de la commande tracert nous permet de localiser précisément l'endroit où un problème de connexion se produit.

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

Avant de continuer les modifications, nous allons activer une option très utile qui permettra de visualiser les interfaces, car vous avez bloqué toute interaction possible avec la topologie.

Une image contenant texte, capture d’écran, logiciel, affichage

Description générée automatiquement

Ce qui nous permet de passer de ceci :Une image contenant texte, capture d’écran, diagramme, Police

Description générée automatiquement

à cela :

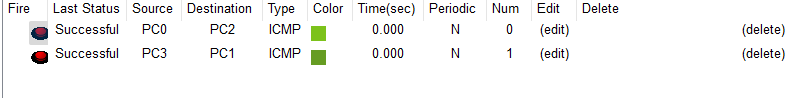
Une image contenant texte, capture d’écran, diagramme, Police

Description générée automatiquement

Personnellement, je n'utilise pas "tracert" car il existe des outils plus performants tels que l'outil d'enveloppe de trame de paquets, qui offre une efficacité accrue. Bien que fonctionnant de manière similaire, cette alternative permet une visualisation directe en interface graphique, indiquant clairement l'emplacement du problème. Dans notre cas, nous avons identifié que le souci résidait au niveau de l'interface SE/0/0/0 du routeur C en raison d'une adresse non valide. Après avoir effectué le changement avec ce marqueur, tout est maintenant opérationnel.Si on fait un show running-config sur le routeur C on se rend compte que l’interface n’est pas valide sur le port serial 0/0/0

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement



# Routage dynamique :

Le routage dynamique est un processus automatisé par lequel les routeurs d'un réseau échangent automatiquement des informations sur les chemins disponibles vers les différentes destinations. Ces informations de routage permettent aux routeurs de prendre des décisions sur la meilleure façon de faire parvenir les paquets de données à leur destination, en fonction des conditions du réseau. Contrairement au routage statique, où les chemins sont configurés manuellement, le routage dynamique s'adapte aux changements de la topologie du réseau de manière automatique. Les protocoles de routage, tels que OSPF, EIGRP, et RIP, sont souvent utilisés pour faciliter le routage dynamique.

OSPF est significativement plus sécurisé, mais sa configuration est plus complexe. Pour un petit réseau tel que celui-ci, RIP est amplement suffisant.

Il suffit de faire c’est commande ensuite :

RouterA>enable

RouterA#configure terminal

RouterA(config)#router rip

RouterA(config-router)#version 2

RouterA(config-router)#network 10.0.0.0

RouterA(config-router)#network 10.100.100.0

RouterA(config-router)#exit

RouterB>enable

RouterB#configure terminal

RouterB(config)#router rip

RouterB(config-router)#version 2

RouterB(config-router)#network 10.100.100.0

RouterB(config-router)#network 10.100.100.4

RouterB(config-router)#network 10.1.0.0

RouterB(config-router)#exit

RouterC>enable

RouterC#configure terminal

RouterC(config)#router rip

RouterC(config-router)#version 2

RouterC(config-router)#network 10.100.100.4

RouterC(config-router)#network 10.100.100.8

RouterC(config-router)#network 10.1.0.0

RouterC(config-router)#exit

RouterD>enable

RouterD#configure terminal

RouterD(config)#router rip

RouterD(config-router)#version 2

RouterD(config-router)#network 10.1.0.0

RouterD(config-router)#network 10.100.100.8

RouterD(config-router)#exit

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

# Conclusion :

Au cours de cet atelier, nous avons acquis la compétence de concevoir des cryptages compatibles avec différents systèmes d'exploitation. Nous avons également maîtrisé la réalisation d'une OSINT, une étape cruciale pour obtenir des informations sur une entreprise, comprendre notre réseau, et identifier les problèmes qu'ils soient internes ou externes. Ce TP constitue une introduction au pentest et à l'analyse passive.

Haut du formulaire

# Annexe :

## Commande à retenir

|  |  |
| --- | --- |
| Objectif: | Commande : |
| Gestion réseau | |
| Voir la configuration IP | Ipconfig /all |
| Renouveler l'adresse IP | ipconfig /renew |
| Vérifier la connectivité réseau | ping [adresse IP ou nom de domaine] |
| Traceroute vers une destination | tracert [adresse IP ou nom de domaine] |
| Vérifier les ports ouverts sur une machine | netstat -an |
| Commandes Linux | |
| Rechercher des motifs dans un fichier | grep [motif] [nom du fichier] |
| Télécharger un fichier depuis Internet | curl -O [URL du fichier] |
| Analyser les ports d'une mach | nmap [adresse IP] |
| Commandes Windows | |
| Afficher la configuration réseau | netsh interface ip show config |
| Afficher les interfaces réseau | netsh interface show interface |
| Réinitialiser l'interface réseau | netsh interface reset |
| Changer l'adresse IP | netsh interface ip set address "Nom de l'interface" static [Adresse IP] [Masque de sous-réseau] [Passerelle] [Métrique] |
| Configurer un serveur DNS | netsh interface ip set dns "Nom de l'interface" static [Adresse DNS primaire] validate=no |
| Configurer le proxy | netsh winhttp set proxy proxy-server="http=proxy.example.com:8080;https=proxy.example.com:8080" bypass-list="\*.example.com" |
| Activer/désactiver ICS | netsh sharing set hostednetwork mode=allow (activer) |
| Sécurité réseau | |
| Vérifier les connexions réseau actives | netstat -an |
| Vérifier les règles du pare-feu | netsh advfirewall show allprofiles |
| Analyser le trafic réseau | tcpdump (Linux) ou Wireshark (interface graphique) |
| Administration système | |
| Afficher les informations système | systeminfo |
| Gérer les services | services.msc |
| Gérer les utilisateurs | net user |
| Afficher la table ARP | arp -a |
| Supprimer une entrée de la table ARP | arp -d [adresse IP] |

## Protocoles vus

|  |  |  |
| --- | --- | --- |
| Protocoles : | | |
| Protocole : | Ports | Description |
| TCP | 0-65535 | Assure une transmission fiable des données en établissant une connexion et en gérant la séquence d'échange. |
| SSH | 22 | Permet une connexion sécurisée à distance en chiffrant les communications entre les deux points. |
| RCPBIND | 111 | Associe les numéros de port RPC (Remote Procedure Call) aux services correspondants sur un système. |
| HTTP | 80 | Protocole de transfert hypertexte utilisé pour le transfert de données sur le World Wide Web. |
| HTTPS | 443 | Version sécurisée de HTTP, crypte les données pour assurer une communication web sécurisée. |
| UDP | 0-65535 | Protocole de datagramme utilisateur, offre une communication plus rapide mais non fiable sans établir de connexion. |
| DNS | 53 | Traduit les noms de domaine en adresses IP, facilitant la navigation sur Internet. |
| DHCP |  | Permet l'attribution dynamique d'adresses IP aux dispositifs sur un réseau, simplifiant la configuration réseau.  Haut du formulaire |
| FTP |  |  |
| ARP |  | Protocole qui mappe une adresse IP à une adresse physique (MAC) dans un réseau local, facilitant la communication au niveau de la couche de liaison de données. |
| IPv4 |  | Protocole de réseau qui attribue des adresses uniques à chaque appareil connecté à Internet pour faciliter l'acheminement des données. |
| IPv6 |  | Version améliorée d'IPv4, utilisée pour résoudre la pénurie d'adresses en attribuant un identifiant unique à un nombre considérablement plus grand d'appareils connectés à Internet |

## Langage abordé

|  |  |  |  |
| --- | --- | --- | --- |
| Langage : | | | |
| Langage : | Date de création | Description | Utilisations Courantes |
| Python | 1991 | Langage de programmation polyvalent, favorisé pour sa lisibilité et sa simplicité. | Développement web, automatisation de tâches. |
| Batch | 1980 | Langage de script utilisé principalement sous les systèmes d'exploitation Windows pour automatiser des tâches. | Scripts de traitement par lots. |
| Powershell | 2006 | Langage de script et de shell développé par Microsoft, privilégié pour l'automatisation des tâches système. | Administration système, scripts d'automatisation |

## Librairie :

|  |  |  |
| --- | --- | --- |
| Librairie : | | |
| Langage : | Description | Avantage |
| Tkinter | Interface graphique pour Python. | Intégration native avec Python, simplifiant le développement GUI. |
| subprocess | Permet d'exécuter des commandes système. | Facilite l'exécution de commandes système et la communication entre processus. |
| threading | Facilite la programmation multithread en Python. | Amélioration des performances grâce à l'exécution concurrente de tâches. |
| Os | Fournit des fonctionnalités liées au système d'exploitation. | Abstraction efficace pour les opérations système courantes. |
| shodan | Permet d'accéder à l'API Shodan pour la recherche et l'exploration de dispositifs connectés à Internet. | Offre une large gamme de fonctionnalités pour la découverte d'appareils, la collecte d'informations sur les services, et la surveillance de la sécurité en ligne. |

# Sources :

<https://www.shodan.io/host/91.220.197.80>

<https://www.whois.com/whois/btssio.org>

<https://www.rfc-editor.org/rfc/rfc826>

<https://www.kali.org/>

<https://tryhackme.com/room/nmap01>

https://tryhackme.com/room/nmap02

<https://tryhackme.com/room/nmap03>

<https://www.frameip.com/routage/>

https://www.it-connect.fr/cisco-configuration-du-routage-rip/