Sommaire:

Nmap:

Introduction :
La connaissance est cruciale en piratage informatique, nécessitant une analyse préliminaire avant toute exploitation. Le scanning des ports révèle les services actifs sur une cible, essentiel pour planifier une attaque. Chaque ordinateur possède 65,535 ports, avec des ports standard comme HTTP (port 80) et HTTPS (port 443), mais ceux-ci peuvent être modifiés, justifiant une énumération exhaustive. Nmap est l'outil privilégié pour cette tâche, offrant des fonctionnalités incomparables et un moteur de script pour la détection de vulnérabilités et parfois l'exécution d'exploits. Comprendre l'analyse de port, sa nécessité et l'utilisation de Nmap est fondamental pour toute exploration initiale.
Commutateurs Nmap:
Nmap est disponible sur Windows et Linux, généralement installé par défaut sur Kali Linux et TryHackMe Attack Box. Pour lancer Nmap, utilisez "nmap" dans le terminal, suivi des commutateurs appropriés. Les premiers commutateurs pour un « Syn Scan », une « analyse UDP », la détection du système d'exploitation et la détection de la version des services sont respectivement : "-sS", "-sU", "-O" et "-sV". Pour augmenter la verbosité, utilisez "-v" pour le niveau un et "-vv" pour le niveau deux. Pour enregistrer les résultats dans trois formats principaux, utilisez "-oA", pour un format "normal", utilisez "-oN", et pour un format "grepable", utilisez "-oG". Pour activer le mode "agressif", utilisez "-A".
Le modèle de timing au niveau 5 est défini par "-T5". Pour scanner des ports spécifiques, utilisez "-p" suivi du numéro de port ou d'une plage de ports. Pour scanner tous les ports, utilisez ***"-p-"(imperatif car nmap ne scanne pas le tout par defaut)****. Pour activer un script, utilisez "--script" suivi du nom du script. Pour activer tous les scripts de*

la catégorie « vuln », utilisez "--script=vuln".

Aperçu

Analyses de connexion TCP:

Les analyses TCP Connect (-sT) de Nmap reposent sur la négociation à trois voies TCP. Elles consistent à tenter une connexion à chaque port TCP spécifié pour déterminer son état.

Si un port est fermé, le serveur répond avec un paquet TCP RST, indiquant que la connexion n'existe pas

Pour un port ouvert, la réponse du serveur contient les indicateurs SYN/ACK. Nmap marque alors le port comme ouvert et termine la négociation avec un paquet TCP ACK.

Si le port est ouvert mais filtré par un pare-feu, Nmap ne reçoit aucune réponse, indiquant que le port est filtré. Certains pare-feu peuvent répondre avec un paquet RST, rendant la détection plus complexe.

En résumé, les analyses TCP Connect de Nmap explorent les ports en utilisant la méthode de connexion à trois voies TCP pour déterminer leur état, qu'ils soient ouverts, fermés ou filtrés.

Analyse SYN:
Les analyses SYN (option -sS) sont utilisées pour explorer les ports TCP sur une ou plusieurs cibles. Contrairement aux analyses TCP standard, les analyses SYN fonctionnent en envoyant un paquet TCP RST après avoir reçu un SYN/ACK du serveur, ce qui évite une négociation complète à trois voies. Cela les rend efficaces pour contourner les systèmes de détection d'intrusion obsolètes et pour rester discrets, car elles ne sont souvent pas enregistrées par les applications écoutant sur les ports ouverts.

Les avantages des analyses SYN incluent leur vitesse accrue par rapport aux analyses TCP Connect standard. Cependant, elles nécessitent des autorisations sudo sous Linux pour fonctionner correctement et peuvent perturber les services instables. Malgré ces inconvénients, les avantages l'emportent généralement.

Nmap utilise par défaut les analyses SYN lorsqu'elles sont exécutées avec des autorisations sudo. En l'absence de ces autorisations, Nmap utilise l'analyse TCP Connect par défaut. Les règles pour identifier les ports fermés et filtrés sont les mêmes pour les analyses SYN et TCP Connect.Le scan syn s’appelle encore le’à moitie ouvert’ ou le ‘furtif’

analyse UDP:
Les analyses UDP de Nmap utilisent le commutateur (-sU) et sont adaptées aux connexions sans état, typiques des protocoles comme

UDP. Contrairement à TCP, où une poignée de main est établie, UDP envoie simplement des paquets vers un port cible sans attendre de réponse, ce qui rend l'analyse plus rapide mais plus difficile.

Lorsqu'un paquet est envoyé vers un port UDP ouvert, Nmap considère le port comme open|filtered s'il n'y a pas de réponse, indiquant qu'il pourrait être ouvert mais protégé par un pare-feu. Si une réponse est reçue, le port est marqué comme ouvert, bien que cela soit rare. En cas d'absence de réponse, une deuxième vérification est effectuée, puis le port est marqué comme ouvert|filtered.

Pour les ports UDP fermés, la cible répond avec un paquet ICMP indiquant que le port est inaccessible, ce qui permet à Nmap de les identifier clairement comme fermés.

En raison de la difficulté à déterminer si un port UDP est réellement ouvert, les analyses UDP sont beaucoup plus lentes que les analyses TCP. Il est recommandé d'utiliser l'option --top-ports <number> pour limiter le nombre de ports analysés et ainsi réduire le temps d'analyse.

Nmap envoie généralement des requêtes vides lors de l'analyse des ports UDP, mais pour les ports occupés par des services bien connus, il peut envoyer une charge utile spécifique au protocole pour obtenir des réponses plus précises.

NULL, END, Xmas:
Les analyses de ports TCP NULL, FIN et Xmas sont moins courantes mais sont utilisées pour leur discrétion accrue par rapport aux scans SYN "furtifs". Les détails sont résumés comme suit :

- *Les analyses NULL (-sN) envoient une requête TCP sans aucun indicateur défini. Une réponse RST est attendue si le port est fermé.*

- *Les scans FIN (-sF) envoient une requête avec l'indicateur FIN, utilisé pour fermer une connexion. Encore une fois, un RST est attendu si le port est fermé.*

- *Les analyses Xmas (-sX) envoient un paquet TCP mal formé avec les indicateurs PSH, URG et FIN, ressemblant à un arbre de Noël dans Wireshark. Une réponse RST est attendue pour les ports fermés.*

Si un port est ouvert, aucune réponse n'est reçue, mais cela peut également être dû à un pare-feu, ce qui les identifie comme open|filtered. Les réponses ICMP inaccessibles peuvent également indiquer un port filtré. Cependant, la RFC 793 n'est pas toujours suivie, certains systèmes répondent par un RST à tout paquet mal formé, masquant l'état réel du port.

Ces analyses visent à contourner les pare-feu qui bloquent les demandes d'initiation de connexion SYN, mais leur efficacité est limitée contre les solutions IDS modernes.

***Analyse réseau ICMP**:*
Lors de l'exploration initiale d'un réseau lors d'une mission de boîte noire, le premier objectif est d'obtenir une vue d'ensemble de sa structure. Pour cela, on utilise souvent ce qu'on appelle un "ping scanning" avec Nmap.

Ce processus consiste à envoyer des paquets ICMP à chaque adresse IP possible du réseau spécifié. Lorsqu'une réponse est reçue, l'adresse IP est marquée comme active. Bien que cela ne soit pas toujours précis, cela fournit une référence utile.

Pour effectuer ce type de balayage, on utilise le commutateur -sn avec des plages IP spécifiées par un trait d'union (-) ou une notation CIDR. Par exemple :

- `nmap -sn 192.168.0.1-254`
- `nmap -sn 192.168.0.0/24`

Le commutateur -sn indique à Nmap de ne pas analyser les ports, se concentrant plutôt sur les paquets ICMP (ou les requêtes ARP sur un réseau local avec les autorisations appropriées) pour identifier les cibles. En plus des paquets ICMP, -sn envoie également des paquets TCP SYN

*au port 443 et des paquets TCP ACK (ou TCP SYN avec les privilèges root) au port 80 pour vérificati**on.***

Aperçu:
Le moteur de script Nmap (NSE) étend considérablement les fonctionnalités de Nmap en permettant l'exécution de diverses tâches, telles que la recherche de vulnérabilités ou l'automatisation d'exploits. Les scripts NSE, écrits en Lua, sont organisés en catégories telles que "safe" (sans risque), "intrusive" (intrusif), "vuln" (vulnérabilité), "exploit" (exploitation), "auth" (authentification), "brute" (force brute) et "discovery" (découverte). Ils peuvent être utilisés pour effectuer des actions diverses, de manière sécurisée ou potentiellement risquée. En utilisant le NSE, on peut obtenir des informations supplémentaires sur le réseau et ses services.
Travailler avec le NSE:
Dans la tâche 3, nous avons exploré l'utilisation du commutateur --script pour activer les scripts NSE de différentes catégories, par exemple, --script=safe pour les scripts sécurisés. Pour exécuter un script spécifique, on utilise --script=<nom-du-script>, par exemple, --script=http-fileupload-exploiter. Plusieurs scripts peuvent être exécutés simultanément en les séparant par des virgules. Certains scripts nécessitent des arguments, fournis avec le commutateur --script-args. Par exemple, pour le script http-put, utilisé pour télécharger des fichiers avec la méthode PUT, on fournit l'URL et l'emplacement du fichier sur le disque avec --script-args http-put.url='/dav/shell.php',http-put.file='./shell.php'. Une liste complète des scripts et de leurs arguments peut être trouvée ici. Les menus d'aide intégrés des scripts sont accessibles avec nmap --script-help <nom-du-script>, bien que moins détaillés que la documentation en ligne.
Recherche de scripts:
Pour trouver des scripts NSE, vous avez deux principales méthodes. Tout d'abord, vous pouvez consulter le site Web de Nmap, qui héberge une liste complète des scripts officiels. Alternativement, vous pouvez accéder au stockage local sur votre machine d'attaque, généralement situé à /usr/share/nmap/scripts sur les systèmes Linux. Tous les scripts NSE sont stockés dans ce répertoire par défaut.

Pour rechercher des scripts installés, vous pouvez utiliser le fichier script.db situé à /usr/share/nmap/scripts/script.db. Ce fichier contient une liste des noms de fichiers de script et des catégories. Vous pouvez utiliser grep pour rechercher des scripts ou des catégories spécifiques. Par exemple : grep "ftp" /usr/share/nmap/scripts/script.db.

*Une autre méthode consiste à utiliser la commande ls, par exemple ls -l /usr/share/nmap/scripts/*ftp*, en utilisant des astérisques (*) autour du terme de recherche.*

Pour installer de nouveaux scripts, vous pouvez utiliser sudo apt update && sudo apt install nmap pour vous assurer d'avoir la dernière version de Nmap, qui inclut généralement tous les scripts officiels. Alternativement, vous pouvez télécharger manuellement un script depuis le site Web de Nmap en utilisant sudo wget -O /usr/share/nmap/scripts/<nom-du-script>.nse https://svn.nmap.org/nmap/scripts/<nom-du-script>.nse, suivi de nmap
--script-updatedb pour mettre à jour le fichier script.db avec le nouveau script téléchargé. Ce processus est également nécessaire si vous créez votre propre script NSE et souhaitez l'ajouter à Nmap.

Evasion du pare-feu:
*Pour contourner les pare-feu, Nmap offre plusieurs options. L'une d'entre elles est l'option **-Pn**, qui permet à Nmap de ne pas envoyer de requête ping à l'hôte avant de l'analyser, contournant ainsi le blocage ICMP. Cependant, cela peut rallonger le temps d'analyse. Si vous êtes sur le réseau local, Nmap peut également utiliser les requêtes ARP pour déterminer l'activité de l'hôte.*

*D'autres commutateurs utiles pour contourner les pare-feu incluent **-f** pour fragmenter les paquets, **--mtu <number>** pour contrôler la taille des paquets, **--scan-delay <time>ms** pour ajouter un délai entre les paquets envoyés, et **--badsum** pour générer une somme de contrôle invalide, utile pour détecter la présence d'un pare-feu/IDS.*

Pratique :
Une bonne pratique est d'augmenter le verbosite des analyses, donc -vv

Service réseau 1

PME:
La PME (Protocole SMB) est un protocole client-serveur utilisé pour partager des fichiers, imprimantes et autres ressources sur un réseau. Les serveurs fournissent ces ressources aux clients, qui peuvent être des ordinateurs disposant de leurs propres disques durs. Le protocole établit une connexion via TCP/IP(en fait netbios), NetBEUI ou IPX/SPX, et fonctionne sur un modèle de demande-réponse. Une fois connectés, les clients envoient des commandes SMB au serveur pour accéder aux partages, ouvrir, lire et écrire des fichiers à travers le réseau. Les systèmes Windows depuis Windows 95 intègrent le support SMB, tandis que Samba est une solution open source pour les systèmes Unix.

Enumeration des PME:
L'énumération est un processus crucial dans la préparation d'une attaque, consistant à collecter des informations sur une cible pour trouver des points d'attaque potentiels. Elle peut inclure la recherche de noms d'utilisateur, de mots de passe, de données réseau, d'hôtes, de services, etc. Les partages SMB, souvent présents sur les serveurs, sont des cibles courantes pour cette collecte d'informations, car ils peuvent contenir des données sensibles.

La première étape de l'énumération est l'analyse des ports pour découvrir les services, les applications et le système d'exploitation de la cible. Enum4Linux, un outil utilisé pour énumérer les partages SMB sur les systèmes Windows et Linux, est souvent utilisé. Il permet d'extraire rapidement des informations telles que les utilisateurs, les machines, les partages, les politiques de mot de passe, les groupes, etc.

Pour utiliser Enum4Linux, la syntaxe est simple : "enum4linux [options] ip". Les options incluent la récupération des utilisateurs (-U), des machines (-M), des partages (-S), des politiques de mot de passe (-P),

des groupes et membres (-G), et une option combinée (-a) pour une énumération complète.
-A est le meilleur
exploiter les PME

Pour exploiter les partages SMB anonymes, suivez ces étapes :

*1. **Identifiez le partage SMB :***
À partir de l'étape d'énumération, vous avez déjà identifié l'emplacement du partage SMB et le nom d'un partage SMB intéressant.

*2. **Utilisez SMBClient :***
Vous utiliserez SMBClient pour accéder au partage SMB. Voici la syntaxe de la commande :
```
***smbclient //[IP]/[PARTAGE] -U [nom_utilisateur] -p [port]***
```

*3. **Exploration du partage :***
Une fois connecté au partage, explorez les fichiers et répertoires disponibles. Vous pouvez utiliser des commandes telles que `ls` pour lister les fichiers, `cd` pour naviguer dans les répertoires, et `get` pour télécharger des fichiers.
```

*En exploitant les partages SMB anonymes, vous pourriez être en mesure d'accéder à des informations sensibles qui pourraient vous aider à obtenir un shell sur le système cible*
*(ses ports par defauts sont 139 et 445)*

*.comprendre telnet:*
*Telnet est un protocole d'application permettant la connexion à distance à un serveur via un client telnet. Il permet d'exécuter des commandes sur la machine distante via une connexion en texte clair. Toutefois, en raison de ses lacunes en matière de sécurité, il est largement remplacé par SSH dans de nombreuses applications. Pour*
```

l'utiliser, l'utilisateur se connecte au serveur en tapant "telnet" dans une invite de commande, puis exécute des commandes spécifiques via l'invite Telnet en utilisant la syntaxe "telnet [ip] [port]".

enumeration de telnet:
Types d'exploits Telnet

Telnet, en tant que protocole, est intrinsèquement peu sécurisé en raison de l'absence de cryptage, exposant ainsi toutes les communications en texte clair et présentant généralement de faibles contrôles d'accès. Bien qu'il existe des CVE répertoriant les failles de sécurité pour les systèmes client et serveur Telnet, les vulnérabilités sont souvent liées à une mauvaise configuration du service.

exploiter telnet :
Lors de l'identification d'un service Telnet, il est crucial de noter s'il est mal dissimulé et marqué comme "backdoor", ainsi que tout indice concernant un éventuel nom d'utilisateur, tel que "Skidy".
Connexion à Telnet
L'accès à un serveur Telnet s'effectue via la syntaxe "telnet [ip] [port]".
*Shell(**un morceau de code ou un programme qui peut être utilisé pour obtenir l'exécution de code ou de commande sur un appareil.**)*
Un shell inversé permet à la machine cible de communiquer avec l'attaquant, établissant ainsi une connexion qui permet l'exécution de code ou de commandes sur la machine attaquée.
*Etape:d*émarrez un écouteur tcpdump sur votre ordinateur local.

Si vous utilisez votre propre machine avec la connexion OpenVPN, utilisez :

- `sudo tcpdump ip proto \\icmp -i tun0`

Si vous utilisez l'AttackBox, utilisez :

- `sudo tcpdump ip proto \\icmp -i ens5`

Cela démarre un écouteur tcpdump, écoutant spécifiquement le trafic ICMP, sur lequel les pings opèrent.

Complété

Maintenant, utilisez la commande "ping [local THM ip] -c 1" via la session telnet pour voir si nous sommes capables d'exécuter des commandes système. Est-ce que nous recevons des pings ? Notez que vous devez faire précéder cela de .RUN (O/N)

Soumettre

Super! Cela signifie que nous sommes capables d'exécuter des commandes système ET que nous sommes capables d'atteindre notre machine locale. Maintenant, amusons-nous !

comprendre ftp:
FTP (File Transfer Protocol) est un protocole permettant le transfert à distance de fichiers sur un réseau, utilisant un modèle client-serveur. Il fonctionne via deux canaux : un canal de commande pour les commandes et réponses, et un canal de données pour le transfert de données. Une session FTP démarre avec le client établissant une connexion au serveur, puis exécute des commandes FTP. Le serveur peut supporter des connexions actives, passives ou les deux. La séparation des canaux permet d'envoyer des commandes sans interrompre les transferts de données, améliorant l'efficacité. Pour plus de détails techniques, consultez le site de l'Internet Engineering Task Force.

enumeration ftp
L'énumération est cruciale lors de l'attaque des services et protocoles réseau. Vous devriez être assez familiarisé avec nmap pour effectuer une analyse de port efficace. Si vous avez besoin d'aide avec un outil, utilisez "tool [-h / -help / --help]" ou consultez les pages de manuel avec "man [tool]".

Nous allons exploiter une connexion FTP anonyme pour rechercher des fichiers susceptibles de contenir des informations permettant d'ouvrir un shell. Cette approche est courante dans les défis CTF et reflète des configurations négligentes de serveurs FTP.

Assurez-vous d'avoir un client FTP installé sur votre système. La plupart des distributions Linux, comme Kali ou Parrot OS, en ont un par défaut. Tapez "ftp" dans la console pour vérifier. Si vous n'en avez pas, installez-en un avec "sudo apt install ftp".

exploiter ftp :
Lors de l'utilisation de FTP, les canaux de commande et de données ne sont pas cryptés, exposant les données à l'interception. Une attaque de l'homme du milieu peut divulguer des informations sensibles, comme les mots de passe. L'exploitation d'un serveur FTP peut se faire via des mots de passe faibles ou par défaut.

En résumé :

- Un serveur FTP est identifié sur la machine.
- Une tentative de force brute des mots de passe FTP est envisagée.

Hydra, un outil de piratage de mots de passe en ligne, peut être utilisé pour cette tâche. Voici la syntaxe :

"hydra -t 4 -l [utilisateur] -P [chemin d'accès au dictionnaire] -vV [IP de la machine] ftp"

Cela lance hydra avec des connexions parallèles, utilisant un dictionnaire de mots de passe, affichant les détails de chaque tentative.

elargir vos connaissances

NFS:
NFS, ou Network File System, permet le partage de répertoires et de fichiers entre systèmes sur un réseau. Les utilisateurs et les programmes peuvent accéder à distance à ces fichiers, les montant comme s'ils étaient locaux. Lorsqu'un client demande l'accès à un fichier via NFS, un appel RPC est envoyé au démon NFS sur le serveur, qui vérifie les autorisations d'accès en utilisant des paramètres tels que le descripteur de fichier, le nom du fichier, l'ID utilisateur et le groupe. Ce système assure le contrôle des autorisations et des droits d'accès.

NFS permet le transfert de fichiers entre des ordinateurs Windows et d'autres systèmes d'exploitation comme Linux, MacOS ou UNIX. Par exemple, un serveur Windows peut fonctionner comme serveur de fichiers NFS pour des clients non Windows, et inversement, un ordinateur Windows peut accéder à des fichiers stockés sur un serveur NFS non Windows.

L'énumération consiste à établir une connexion active avec les hôtes cibles pour découvrir des vecteurs d'attaque potentiels dans le système, ce qui est crucial pour informer les attaques ultérieures.

Pour une énumération avancée du serveur NFS, vous aurez besoin de nfs-common, un package essentiel pour interagir avec les partages NFS. Il inclut des outils comme showmount et mount.nfs, utiles pour extraire des informations des partages NFS.

L'analyse des ports est une première étape importante. Utilisez nmap avec les balises -A et -p- pour obtenir des informations détaillées sur les services, les ports ouverts et le système d'exploitation de la machine cible.

`/usr/sbin/showmount -e [IP] pour lister le dossier de partage de la cible`
Pour monter les partages NFS sur votre client, créez un dossier sur votre système, puis utilisez la commande ***sudo mount -t nfs IP:dossiertrouvesurlacible chemindossiercree -nolock***

*Si v**ous avez un shell à faibles privilèges sur une machine avec un partage NFS, vous pourriez l'utiliser pour obtenir des privilèges élevés selon sa configuration. Par défaut, le Root Squashing est activé sur les partages NFS, limitant l'accès au root. Cependant, si désactivé, cela peut permettre la création de fichiers SUID(attribut qui me donne le titre de proprietaire), autorisant un utilisateur distant à accéder au système connecté. En téléchargeant un exécutable Bash sur le partage NFS et en définissant les autorisations SUID, vous pourriez obtenir un shell root via SSH, ouvrant la voie à un accès complet.(***

Téléchargez l'exécutable bash dans votre répertoire de téléchargements. Utilisez ensuite "cp ~/Downloads/bash ." pour copier l'exécutable bash sur le partage NFS. Le shell bash copié doit appartenir à un utilisateur root, vous pouvez le définir en utilisant "sudo chown root bash"
ntenant, nous allons ajouter l'autorisation de bit SUID à l'exécutable bash que nous venons de copier sur le partage en utilisant "sudo chmod +[permission] bash". Quelle lettre utilisons-nous pour définir le jeu de bits SUID à l'aide de chmod ? c’est la lettre s:

Faisons une vérification d'intégrité, vérifions les autorisations de l'exécutable "bash" en utilisant "ls -la bash". À quoi ressemble l’ensemble d’autorisations ? Assurez-vous qu'il se termine par -sr-x.

Maintenant, connectez-vous en SSH à la machine en tant qu'utilisateur. Répertoriez le répertoire pour vous assurer que l'exécutable bash est là. Maintenant, le moment de vérité. Exécutons-le avec " ./bash -p ". Le -p conserve les autorisations, afin qu'il puisse s'exécuter en tant que root avec SUID, sinon bash supprimera parfois les autorisations.

)

Smtp:

SMTP, ou "Simple Mail Transfer Protocol", est essentiel pour l'envoi d'e-mails. En tandem avec POP/IMAP, il permet l'envoi de courrier sortant et la récupération de courrier entrant. Le serveur SMTP remplit trois fonctions de base : vérification des expéditeurs, envoi du courrier sortant, et gestion des retours en cas de non-livraison. POP et IMAP sont des protocoles de messagerie pour récupérer le

courrier électronique, avec IMAP offrant une synchronisation plus avancée entre le serveur et le client.

Le fonctionnement de SMTP peut être comparé à la livraison physique du courrier. L'agent utilisateur de messagerie se connecte au serveur SMTP, négocie la connexion, puis envoie le courrier avec les détails de l'expéditeur, du destinataire, et le contenu. Le serveur SMTP vérifie les domaines, relaye l'e-mail au serveur du destinataire, qui le transmet à la boîte de réception du destinataire.

Pour faire fonctionner SMTP, le logiciel serveur SMTP est largement disponible sur les plateformes Windows et Linux.
Nous utiliserons le module "smtp_version" de MetaSploit pour obtenir des détails sur les serveurs de messagerie rencontrés.

Pour énumérer les utilisateurs via SMTP, nous utiliserons les commandes internes VRFY et EXPN, soit manuellement via une connexion telnet, soit via le module MetaSploit "smtp_enum".

Des alternatives telles que smtp-user-enum existent, mais cette technique fonctionnera pour la plupart des configurations SMTP.
À la fin de notre phase d'Énumération, nous avons deux informations clés : un nom d'utilisateur et le type de serveur SMTP avec le système d'exploitation en cours d'exécution. Nous savons également que le seul autre port ouvert est une connexion SSH.

Nous utiliserons Hydra pour tenter une attaque par force brute sur le compte SSH de l'utilisateur, en utilisant une liste de mots de passe. Hydra permet des attaques adaptatives sur différents services, y compris SSH, et est généralement inclus dans Parrot OS et Kali Linux. Vous pouvez trouver des listes de mots de passe dans le répertoire "/usr/share/wordlists" ou sur des sites comme SecLists.

La syntaxe de la commande Hydra que nous utiliserons est la suivante :

hydra -t 16 -l USERNAME -P /usr/share/wordlists/rockyou.txt -vV MACHINE_IP ssh

Mysql:

Dans sa simplicité, MySQL est un système de gestion de base de données relationnelle (SGBDR) basé sur le langage de requête structuré (SQL). Une base de données stocke des données de manière organisée, tandis que le SGBDR gère ces données selon un modèle relationnel, organisé en tableaux liés par des clés. MySQL utilise le protocole MySQL pour la communication entre le serveur et les clients, traitant les requêtes SQL pour créer, modifier et accéder aux données. Il fonctionne sur diverses plateformes et est largement utilisé dans les sites Web et la pile LAMP, qui comprend Linux, Apache, MySQL et PHP.
MySQL n'est généralement pas le premier point d'attaque dans un scénario. Habituellement, vous obtiendrez des informations d'identification initiales à partir d'autres services, que vous utiliserez ensuite pour énumérer et exploiter MySQL. Par exemple, si vous avez trouvé les informations d'identification "root:password" lors de l'énumération des sous-domaines d'un serveur Web, vous pouvez les essayer pour vous connecter à MySQL après une tentative infructueuse avec SSH.

Assurez-vous d'avoir le client MySQL installé sur votre système, que vous pouvez obtenir avec sudo apt install default-mysql-client. Metasploit est également nécessaire pour cette tâche, bien qu'il existe des alternatives non-Metasploit comme le script mysql-enum de nmap ou des exploits disponibles sur des sites comme Exploit-DB.

Nous avons vérifié la cohérence des données dans la base MySQL et identifié :

1. Les informations d'identification du serveur.

2. La version actuelle de MySQL.
3. Le nombre et les noms des bases de données.

Nous devons comprendre deux termes clés :
- Schéma : dans MySQL, c'est synonyme de base de données.
- Hachages : ils sont utilisés pour stocker des mots de passe de manière sécurisée, transformant les mots de passe en une forme cryptée.