UQAR

AIDE-MÉMOIRE

OUTILS POUR LA COMPÉTITION CTF

PRÉPARÉ PAR L'ÉQUIPE DU **CYBERHACK**

ls

La commande "ls" est un utilitaire en ligne de commande fréquemment employé sur les systèmes Unix, tels que Linux et MacOS. Son nom signifie "liste", reflétant sa fonction principale : afficher les fichiers et répertoires présents dans le répertoire de travail en cours.

cd

La commande "cd" est un outil de ligne de commande important utilisé pour changer le répertoire de travail actuel dans les systèmes basés sur Unix. "cd" signifie "changer de répertoire".

Commandes	
cd [répertoire]	Change le répertoire actuel pour le répertoire spécifié.
cd -	Change le répertoire actuel pour le répertoire précédent.
cd ..	Remonte d'un niveau dans la hiérarchie des répertoires.
cd .	Utilisé comme une référence au répertoire actuel.
cd ~	Se déplace vers le répertoire principal de l'utilisateur actuel.
cd /	Se déplace vers le répertoire racine du système de fichiers.

cat

La commande "cat" est un outil Unix permettant d'afficher et de concaténer le contenu de fichiers. Son nom découle de sa fonction principale : la concaténation. Dans son usage le plus simple, elle sert à afficher le contenu d'un fichier, mais elle peut également combiner plusieurs fichiers et les afficher successivement.

find

La commande "find" est un utilitaire puissant dans les systèmes d'exploitation de type Unix. Il est utilisé pour rechercher des fichiers et des répertoires dans une hiérarchie de répertoires en fonction de divers critères, tels que le nom de fichier, le type de fichier, la taille et l'heure de modification.

find [répertoire] [options] [expression]	
-name [pattern]	Recherche des fichiers et répertoires ayant un nom ou un motif spécifique.
-type [type]	Spécifie le type de fichier à rechercher ([f] pour les fichiers réguliers, [d] pour les répertoires).

Wpscan

Wpscan est un scanner de vulnérabilité WordPress de type boîte noire qui peut être utilisé pour scanner des installations WordPress et trouver des vulnérabilités de sécurité potentielles. Il est également couramment utilisé pour recueillir des informations sur les installations WordPress, telles que les plugins et thèmes installés, ce qui peut être utile pour effectuer des tests de pénétration ou des évaluations de sécurité.

wpscan --url <URL-cible> [options]	
--url <URL-cible>	Spécifiez l'URL cible de WordPress.
--follow-redirection	Suit les redirections HTTP.
--no-banner	Ne pas afficher la bannière.
Options d'énumération	
--enumerate <type>	Énumérer les types d'informations spécifiés (plugins vulnérables <vp>, thèmes <t>, utilisateurs <u>, toues les plugins <ap>).
Détection des plugins et des thèmes	
--detection-mode <mode>	Spécifiez le mode de détection (passif, agressif, mixte).
--plugins-detection <level>	Définissez le mode de détection des plugins (mixte, passif, agressif).
--plugins-version-detection <level>	Définir le mode de détection de version des plugins (mixte, passif, agressif).
--themes-detection <level>	Définir le mode de détection des thèmes (mixte, passif, agressif).
--plugins-list	Énumérer les plugins installés.
--themes-list	Énumérer les thèmes installés.
Options d'affichage	
--output <output-file>	Écrire la sortie dans un fichier.
--output-format <format>	Définir le format d'affichage (json, cli).
--verbose	Activer l'affichage détaillé.

Netdiscover

NetDiscover est un outil de découverte réseau permettant d'identifier et de cartographier les hôtes actifs de manière passive. Il collecte des informations comme les adresses IP, les adresses MAC et les noms des appareils, facilitant ainsi le travail des administrateurs réseau et des experts en sécurité. Contrairement aux outils de balayage actif, il ne sonde pas les hôtes et reste non intrusif. Son utilisation est donc considérée comme sûre dans la plupart des environnements réseau.

netdiscover [options]	
-i <interface>	Spécifiez l'interface réseau à utiliser.
-r <range>	Spécifiez la plage d'adresses IP à scanner (par exemple, 192.168.1.0/24).
Options de scan	
-P	Mode passif. Ne pas envoyer de paquets, seulement écouter.
-S	Envoyer des paquets avec l'adresse source donnée.
-F	Mode rapide. Analyser en utilisant uniquement des requêtes ARP.
-c <count>	Envoyer <count> nombre de requêtes ARP.
Options d'affichage	
-n	Ne pas résoudre les adresses IP en noms d'hôtes.
-N	Ne pas résoudre les adresses MAC en vendeurs.
-v	Activer l'affichage détaillé.
-h	Afficher le message d'aide.
Options de filtrage	
-s <IP>	Exclure l'adresse IP donnée de l'analyse.
-S <IP>	Scannez uniquement l'adresse IP spécifiée.

Nmap

Nmap (Network Mapper) est un outil open-source utilisé pour l'exploration de réseau, l'audit de sécurité et la détection de vulnérabilités. Il permet d'identifier les appareils et services actifs, d'analyser les ports ouverts et de détecter les systèmes d'exploitation. Couramment employé par les administrateurs réseau et les testeurs de pénétration, il aide à évaluer la posture de sécurité d'un réseau.

nmap [type(s) de scan] [options]	
-sS	TCP SYN scan.
-sT	TCP connect scan.
-sU	UDP scan.
-sN	TCP Null scan.
-sF	TCP FIN scan.
-sX	TCP Xmas scan.
-sA	TCP ACK scan.
-sW	TCP Window scan.
Options de ports	
-p <port>	Analyser des ports spécifiques.
-p-	Analyser tous les 65535 ports.
-F	Analyser les 100 ports les plus courants.
Découverte d'hôtes	
-sn	Analyse de ping. Désactiver l'analyse de port.
-Pn	Traiter tous les hôtes comme à l'écoute.
-PS <port>	TCP SYN ping.
-PA <port>	TCP ACK ping.
-PU <port>	UDP ping.
-PE	ICMP echo ping.
-PP	ICMP timestamp ping.
Découverte des versions de services	
-sV	Découverte des versions de services.
-A	Mode agressif.
-O	Détection du système d'exploitation.
Contournement des pares-feux	
-f	Fragments de paquets
-D	Decoy scan.
-S	Falsifier l'adresse source.
--data-length <size>	Ajouter des données aléatoires.

Nikto

Nikto est un scanner de vulnérabilités pour serveurs web, capable d'identifier des fichiers et programmes dangereux, ainsi que des versions obsolètes de serveurs. Il analyse aussi la configuration du serveur, comme la gestion des fichiers d'index et les options HTTP. Conçu pour détecter, et non exploiter, les failles, il fournit un rapport détaillé des vulnérabilités et mauvaises configurations connues. Cet outil est utilisé par les testeurs de pénétration et les experts en cybersécurité pour évaluer la sécurité des serveurs web.

nikto -h <hôte-cible> [options]	
-h <host>	Spécifiez l'hôte cible.
-F <hostlist>	Lire les cibles à partir d'un fichier.
-C <host:port>	Liste de cibles et de ports séparés par des virgules.
Options de base	
-id <id>:<password>	Authentification de base HTTP.
-T <timeout>	Définir la valeur de délai d'attente.
-ssl	Forcer le mode SSL.
-nossl	Désactiver le mode SSL.
-Cg <cookie>	Créer un cookie.
-plugin <plugin>	Utiliser un plugin.
-nocache	Désactive l'utilisation du cache des Niktos.
Portée du scan	
-port <port>	Analyser un port spécifique.

Hydra

Hydra est un outil de carack de mots de passe capable d'effectuer des attaques en ligne et hors ligne contre

divers services réseau. Il prend en charge de nombreux protocoles d'authentification et sert principalement à tester la robustesse des mots de passe dans un cadre légitime. Cependant, son utilisation non autorisée est illégale et peut entraîner des sanctions. Il est essentiel d'obtenir une autorisation avant toute activité de test de sécurité ou de pénétration.

hydra -l <nom-utilisateur> -P <list-mots-de-passe> <Hôte-cible> <Protocole> [options]

-l <username>	Spécifier le nom d'utilisateur.
-P <password-list>	Spécifier la liste de mots de passe.
-t <threads>	Spécifier un nombre de sous-traitements.
-s <port>	Spécifier le port.
-f	Arrêter après le premier mot de passe valide.
Protocoles	
http-get	Authentification en mode HTTP GET.
http-post	Authentification en mode HTTP POST.
http-form-post	Authentification en mode HTTP POST avec formulaire.
ssh	Authentification en mode SSH.
rdp	Authentification en mode RDP.
Options avancées	
-e nsr	Aucun arrêt, peu importe la condition.
-o <output-file>	Enregistrez les résultats dans un fichier.
-u	Essayez des mots de passe vides.
-x <min>:<max>:<charset>	Spécifiez la longueur minimale, maximale et le jeu de caractères du mot de passe.
-L <user-list>	Spécifiez une liste de noms d'utilisateur.
-X <user-list>	Spécifiez une liste de noms d'utilisateur pour l'envoi du formulaire HTTP.
-C <colon-separated-list>	Spécifiez la combinaison de nom d'utilisateur et de mot de passe.
-U <user-list>	Spécifiez une liste de noms d'utilisateur pour la connexion SMB.
-P <password-list>	Spécifiez une liste de mots de passe pour la connexion SMB.
Options HTTP	
-m <method>	Spécifiez le verbe HTTP (GET, POST).
-d <data>	Spécifiez les données du POST.
-t <timeout>	Spécifiez le délai d'attente.
-w <wait>	Temps d'attente entre les requêtes.

Drib

Drib est un outil en ligne de commande permettant de détecter des répertoires et fichiers cachés sur les serveurs web en automatisant leur recherche. Il utilise des listes de noms courants et peut effectuer des attaques par force brute sur des répertoires spécifiques. Son utilisation sans autorisation pour accéder à des systèmes est illégale. Il est essentiel d'obtenir une autorisation avant toute activité de test de sécurité.

drib -u <URL-cible> [options]

-u <URL>	Spécifiez l'URL cible.
-w <wordlist>	Spécifiez la liste de mots.
Portée du scan	
-p <port>	Spécifiez le port.
-d <depth>	Spécifiez le nombre de répertoires.
Options d'authentification	
-U <username>	Spécifiez le nom d'utilisateur.
-P <password>	Spécifiez le mot de passe.

Curl

C'est un outil de ligne de commande permettant de transférer des données spécifiques à l'aide de la syntaxe URL. Il est couramment utilisé pour tester des API, télécharger des fichiers ou récupérer des pages web.

curl [options][url]

-o	Enregistrer dans un fichier.
-L	Suivre les redirections HTTP.
Options HTTP	
-I	Récupérer les En-tête HTTP.
-u	Authentifier une requête http en fournissant un nom d'utilisateur et un mot de passe.
Options Avancées	
-v	Affiche les détails de la requête et de la réponse.
-T	Télécharger toutes les données sur stdin vers un serveur spécifié.
-proxy	Passer par un proxy.

PIPE "|"

Pipe ou « Pipeline », est un outil de commande puissant et flexible permettant d'exécuter des commandes et de manipuler des messages au sein d'un pipeline. L'utilisation de l'opérateur "pipe" : | permet de rediriger la sortie d'une commande de terminal et de l'utiliser comme entrée de la commande suivante. On peut de cette manière créer un enchainement de commandes pour exécuter des actions complexes.

<commande1> | <commande2> | <commande3> |..

LITERAL	Injecte un texte dans un pipeline.
DISK	Lit un fichier à partir d'un disque.

HCYLOG |Console	Affiche et récupère tous les logs dans la console.
APPEND	Ajoute l'enregistrement de référence à chaque enregistrement de détail.

GCC

GCC (GNU Compiler Collection) est un ensemble de compilateurs développé par le projet GNU pour divers langages de programmation, notamment C, C++, Fortran, Ada, Go et d'autres. Il est utilisé pour compiler des programmes sous Linux mais fonctionne aussi sur Windows via des ports comme MinGW.

gcc [fichier_source.c] -o [fichier_executable]

-O2	Optimisation du code.
-static	Génère un exécutable statique.
-Wall	Active les avertissements de compilation.
-g	Ajoute des informations de débogage.

Obj Dump

Objdump est un outil de ligne de commande qui permet d'afficher des informations sur les fichiers binaires et exécutables sous Linux.

objdump [options][url]

-d	Afficher le contenu en assembleur des sections exécutables.
-D	Affiche le contenu en assembleur de toutes les sections.
-i	Affiche une liste de tous les architectures et tous les formats d'objet.
-s	Afficher les données brutes.
-r	Afficher les entrées de rescolarisation du fichier.
-h	Donne les détails sur les sections du ficher ELF (.text, .data, .etc).
-g	Donne les résultats de débogages.

nasm

NASM (Netwide Assembler) est un assembleur libre et portable destiné aux architectures x86 et x86-64, utilisant la syntaxe Intel. Il est largement utilisé pour écrire du code assembleur bas niveau, produire des exécutables ou générer du code objet compatible avec divers formats.

nasm -f <format> <filename> [-o <output>]

-M	Génère les dépendances dans Makefile
-MG	Comme -M mais traite les fichiers manquants comme des fichiers générées.
-g	Générer les informations de débogage.
-E	Affiche uniquement le code résultant du préprocesseur sans assembler le fichier source.
-x <mode>	Sélectionner le format d'affichage des erreurs lors de l'assemblage.
-s	Afficher les messages d'erreurs sur la sortie standard stdout.
-Ld	Affiche les octets et répétitions en décimal au lieu d'hexadécimal.
-Lp	Génère un fichier de liste à chaque passe (utile pour le débogage).
-L	Active les options de listing personnalisées.

Python http Server

Un serveur HTTP en Python est un programme qui reçoit des requêtes HTTP de clients tels que des navigateurs ou des API et leur envoie une réponse contenant des fichiers, des pages HTML ou des données JSON. Le module intégré http.server permet de créer facilement un serveur web basique, idéal pour tester des applications ou diffuser des fichiers statiques.

python -m http.server 8000	Démarre un serveur http sur le port 8000.
python -m http.server 8000 --directory /chemin	Spécifier le chemin.
python -m http.server --bind 127.0.0.1	Démarre le serveur en le liant seulement à l'adresse locale 127.0.0.1
python -m http.server 8080 --directory/chemin/vers/ repertoire 8080	Sert un répertoire spécifique sur le port 8080: Sert un répertoire spécifique sur le port 8080.

GDB

GDB (GNU Debbuger) est un débogueur puissant, principalement utilisé pour les langages de programmation C, C++ et autres. Il permet aux développeurs d'exécuter un programme en mode pas à pas, d'analyser la mémoire, d'inspecter les registres et de modifier l'état du programme en cours d'exécution.

gdb [options] <binaire>

--args <binaire> <args>	Passe des arguments au programme.
-p <PID>	Attache GDB à un processus en cours d'exécution.
-tui	Active l'interface TUI pour afficher le code et l'assembly en direct.
-r	Exécute le programme dès le début.