Recon & Enum

Les meilleurs outils de reconnaissance et d'énumération pour votre Red team.

- Windows / AD
  - [Énumération] AD
  - [Énumération] Enum4linux
  - [Énumération] Windows
  - [Reconnaissance] NBTscan
  - [Énumération] RpcClient
  - [Énumération] Samba
  - [Énumération] LDAP
- Web
  - [Énumération/Web] Cheat-sheet
  - [Énumération/Web] LFI - RFI
- Réseau
  - [Énumération/Réseau] Nmap
  - [Énumération/Réseau] SNMP
  - [Énumération/Réseau] DNS
  - [Énumération/Réseau] Zmap
- Linux
  - [Énumération/Linux] Cheat-sheet
  - [Énumération/Linux] Git-dumper

Windows / AD

[Énumération] AD

Introduction

L'énumération d'un envrionnement Active Directory est primordial pour trouver ses faibles.



Énumération distante

Scan réseau

Si vous avez un accès sur un sous-réseau et que vous cherchez les contrôleurs de domaine disponibles ou les serveurs Windows en général, vous allez pouvoir les identifier rapidement grâce à **CrackMapExec** :

```
cme smb <NET_IP/MASK>
```

> Vous allez récupérer les versions de Windows ainsi que les noms des domaines associés à ces serveurs.

Scan d'un contrôleur de domaine

Vous pouvez récupérer quelques informations utiles avec **CrackMapExec** :

```
cme smb <DC_IP|DC_FQDN>
```

Énumération des utilisateurs du domaine

Il est parfois possible de récupérer la liste des utilisateurs du domaine notamment avec **enum4linux** :

```
enum4linux -U <DC_IP>
```

Ou avec **kerbrute** :

```
kerbrute userenum --dc <DC_IP> -d <DOMAIN_FQDN> <USERLIST>
```

Énumération de la base de registre

```
reg.py <DOMAIN>/<USER>:<PASSWORD>@<IP> query -keyName "<REGISTRY_FOLDER>"
```

Voici un exemple pour lister les logiciels présent sur le poste :

```
reg.py <DOMAIN>/<USER>:<PASSWORD>@<IP> query -keyName "HKLM\\SOFTWARE"
```

Énumération des services

```
services.py <DOMAIN>/<USER>:<PASSWORD>@<IP> list
```

Récupérer les SID des utilisateurs

```
lookupsid.py <DOMAIN>/<USER>:<PASSWORD>@<IP>
```

Récupérer les comptes de service

```
GetUserSPNs.py <DOMAIN>/<USER>:<PASSWORD>
```

> On peut récupérer les TGS avec l'option **-request** à placer à la fin de la commande.

Récupérer des jetons TGT

Permet de récupérer les jetons TGT des comptes utilisateurs qui ont la pré-authentification Kerberos désactivée :

```
GetNPUsers.py <DOMAIN>/<USER>:<PASSWORD> -request
```

Récupérer des hashs de mots de passe

Permet d'interroger le serveur pour récupérer les hashs de mots de passe qui pourraient se trouver dans le **ntds.dit**, ou autre :

```
secretsdump.py <DOMAIN>/<USER>:<PASSWORD>@<IP>
```

Énumération locale

Ce petit mémo regroupe toutes les commandes pour énumérer des informations sur un domaine si vous avez un premier accès sur un poste du domaine.

Trouver le nom du domaine

```
systeminfo | findstr Domain
```

Lister les utilisateurs du domaine

```
Get-ADUser  -Filter *
```

Vous pouvez aussi ajouter un filtre pour lister tous les éléments d'un OU spécifique (ici **Users**) :

```
Get-ADUser -Filter * -SearchBase "CN=Users,DC=<DC_DN>,DC=<DC_TLD>"
```

On peut aussi récupérer les utilisateurs à privilèges élevés :

```
Get-ADUser -Filter * | select SamAccountName
```

Lister les logiciels anti-virus

```
wmic /namespace:\\root\securitycenter2 path antivirusproduct
```

Afficher l'état de Windows Defender

```
Get-Service WinDefend
```

Et pour afficher l'état des différents services de Windows Defender :

```
Get-MpComputerStatus
```

Afficher l'état du pare-feu

```
Get-NetFirewallProfile | Format-Table Name, Enabled
```

Afficher les règles du pare-feu

```
Get-NetFirewallRule | select DisplayName, Enabled, Description
```

Désactiver le pare-feu

```
Set-NetFirewallProfile -Profile Domain, Public, Private -Enabled False
```

> Nécessite les droits administrateurs !

Tester l'état d'un port

Dans un premier shell, se mettre en écoute :

```
Test-NetConnection -ComputerName <IP> -Port <PORT>
```

Puis initiez une connexion :

```
(New-Object System.Net.Sockets.TcpClient("<IP>", "<PORT>")).Connected
```

Afficher les sources de logs

```
Get-EventLog -List
```

Afficher le processus Sysmon

S'il existe il sera affiché :

```
Get-Process | Where-Object { $_.ProcessName -eq "Sysmon" }
```

Lister les applications installées

```
wmic product get name,version
```

Afficher les dossiers et fichiers cachés

```
Get-ChildItem -Hidden -Path <DIR_PATH>
```

Afficher les services en cours d'exécution

```
net start
```

Afficher les informations d'un service

```
wmic service where "name like '<SERVICE>'" get Name,PathName
```

Afficher les informations sur un processus

```
Get-Process -Name <PROCESS>
```

Afficher les connexions en lien avec un processus

```
netstat -noa |findstr "LISTENING" |findstr "<PID>"
```

Afficher la politique de mot de passe du domaine

```
net accounts /domain
```

Afficher les informations d'un utilisateur du domaine

```
Get-ADUser -Identity <USER> -Server <DC_FQDN> -Properties *
```

Afficher les informations d'un groupe du domaine

```
Get-ADGroup -Identity <GROUP> -Server <FQDN_DC>
```

Afficher les membres d'un groupe du domaine

```
Get-ADGroupMember -Identity <GROUP> -Server <FQDN_DC>
```

Afficher des informations génériques sur le domaine

```
Get-ADDomain -Server <FQDN_DC>
```

Afficher les relations de confiance

```
nltest /domain_trusts
```

Bloodhound

Sharphound

Cet outil du framework va se charger de l'énumération du domaine.

Voici le lien du repos :

- https://github.com/BloodHoundAD/SharpHound

Il doit être lancé depuis un compte utilisateur du domaine.

Cependant, il est détecté par les antivirus et EDR, c'est pourquoi il est recommandé d'utiliser notre propre machine Windows et lancer Sharphound dessus avec les droits de l'utilisateur grâce à **runas**.

Cet outil prend soit la forme d'un exécutable, soit d'un script Powershell et peut être lancé de la manière suivante :

```
SharpHound.exe --CollectionMethods All --Domain <FQDN_DC> --ExcludeDCs
```

Normalement, une archive zip a été générée.

Nous pourrons la récupérer sur notre machine pour l'utiliser avec Bloodhound.

Bloodhound-python

Si vous n'avez pas de shell sur une machine du domaine, vous pouvez utiliser bloodhound-python ou rusthound pour remplacer le rôle de sharphound :

```
bloodhound-python -c DcOnly -u <USER> -p <PASSWORD> -d <DOMAIN_FQDN> -dc <DC_FQDN> -ns <DC_IP>
--zip
```

Bloodhound GUI

Lancez la console neo4j (nécessaire au fonctionnement de l'outil) :

```
neo4j console
```

> Selon les distributions, vous devrez mettre ou non le mot **start** à la fin de la commande.

Puis dans un autre terminal, lancez bloodhound :

```
bloodhound --no-sandbox
```

> Les identifiants par défaut sont **neo4j:neo4j**.

[Énumération] Enum4linux

Introduction

L'outil **enum4linux** permet de collecter des informations sur un hôte windows ou un contrôleur de domaine.



Manuel

Syntaxe globale

```
enum4linux [OPTIONS] <TARGET_IP>
```

Énumérer les utilisateurs

```
enum4linux -U <TARGET_IP>
```

Énumérer les groupes

```
enum4linux -G <TARGET_IP>
```

Lister les informations sur les groupes

```
enum4linux -M <TARGET_IP>
```

Énumérer les partages samba

```
enum4linux -S <TARGET_IP>
```

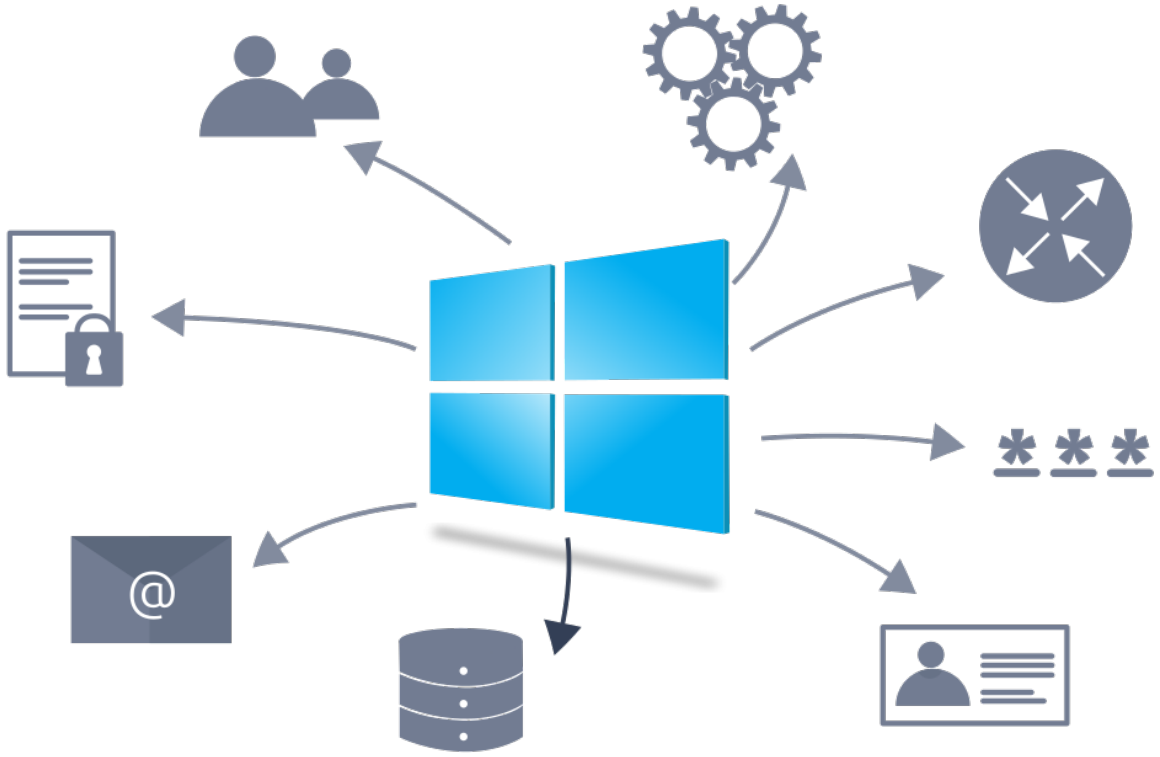
Lister les mots de passe

```
enum4linux -P <TARGET_IP>
```

[Énumération] Windows

Introduction

Cette page décrit les procédés pour énumérer un système Windows lorsque vous y avez accès.



Manuel

Afficher les informations systèmes

```
systeminfo
```

Afficher les mises à jour installées

```
wmic qfe get Caption,Description
```

Afficher les services installés et démarrés

```
net start
```

Afficher les applications installées

```
wmic product get name,version,vendor
```

Afficher les privilèges de l'utilisateur actif

```
whoami /priv
```

Afficher les groupes de l'utilisateur actif

```
whoami /groups
```

Afficher les utilisateurs du système

```
net user
```

Afficher le SID des utilisateurs du système

```
wmic useraccount get name,sid
```

> À noter que le dernier octet du SID représente le **RID** de l'utilisateur.

Afficher les groupes du système

```
net localgroup
```

Afficher les membre d'un groupe

```
net localgroup <GROUP>
```

Afficher les configurations locales

```
net accounts
```

Lister les tâches planifiées

```
schtasks
```

Et pour afficher le détail d'une tâche planifiée :

```
schtasks /query /tn <TASK_NAME> /fo list /v
```

[Reconnaissance] NBTscan

Introduction

L'outil **nbtscan** permet de scanner les hôtes windows présents sur un sous-réseau.

Ses utilisations sont variées et permettent de récupérer différentes informations utiles lors d'un pentest.



Codes NetBios

Codes	Descriptions
00	Workstation service
03	Messenger service
20	File Server service
1B	Domain Master Brower (contrôleur de domaine)
1C	Contrôleur de domaine
2B	Services d'annuaire

Manuel

Syntaxe globale

```
nbtscan <SUBNET_ID/CIDR_MASK>
```

Exemple :

```
nbtscan 192.168.1.0/24
```

Options

Options	Descriptions
-v	Mode verbeux.
-e	Affiche des informations d'extension (utilisateurs actifs etc).
-m	Affiche les informations MAC des machines.
-r <RANGE>	Scanner une plage d'IP spécifique.
-f <FILE>	Scanner les adresses IP du fichier spécifié.
-t <DELAY>	Définit un délai d'attente personnalisé.
-h	Affiche la page d'aide

[Énumération] RpcClient

Introduction

RpcClient est un outil en ligne de commande permettant d'interagir avec les services **RPC** (*Remote Procedure Call*) dans les systèmes basés sur Windows ou Samba.

Manuel

Syntaxe globale

```
rpcclient [OPTIONS] -U <USERNAME>%<PASSWORD> //<IP|HOSTNAME>
```

Exemples d'utilisation

- Connexion à un serveur :

```
rpcclient -U user%password //192.168.1.1
```

- Lister les partages accessibles :

```
rpcclient -U user%password -c "enumprinters" //192.168.1.1
```

- Exécuter des commandes spécifiques :

```
rpcclient -U user%password -c "querydispinfo" //192.168.1.1
```

Connexion anonyme :

```
rpcclient -N //192.168.1.1
```

Options courantes

Options	Descriptions
-U	Spécifie le nom d'utilisateur et le mot de passe pour l'authentification.
-c	Exécute une commande spécifique après la connexion.
-N	Spécifie un nom d'utilisateur mais n'effectue pas d'authentification (utilisé pour les connexions anonymes).
-W	Spécifie le domaine Windows à utiliser.
-I	Spécifie l'adresse IP du serveur DNS.

[Énumération] Samba

Introduction

L'énumération des partages samba est cruciale pour les tests d'intrusions d'envrionnement Windows.

Script nmap

Énumération globale de l'OS utilisé

```
nmap --script smb-os-discovery <IP>
```

Énumération des utilisateurs samba

```
nmap --script smb-enum-users <IP>
```

> Cette technique ne marche que si la session "**null**" est activée sur le poste cible (rare).

Smbmap

Utilisation avec un compte

Si vous possédez un compte pour faire l'énumération :

```
smbmap -u <USER> -p <PASSWORD> -H <IP>
```

> Vous aurez un aperçu des droits de lecture et d'écriture que vous avez sur les partages.

Utilisation de la session null

```
smbmap -u '' -p '' -H <IP>
```

Options

Options	Descriptions
-R	Active la récursivité pour afficher le contenu des dossiers (si vous possédez les droits de lecture).

ShareEnum

Installation

Vous pouvez récupérer la dernière release sur le github et lancer l'installation du paquet sur votre système :

```
dpkg -i <PACKAGE>.deb
```

Utilisation standard

```
shareenum <IP>
```

> Si vous ne spécifiez pas d'utilisateur, la session **null** sera utilisée.

Options

Options	Descriptions
-o <FILE>	Spécifie un fichier de sortie de la commande.
-u <USER>	Spécifie un nom d'utilisateur.
-p <PASSWORD>	Spécifie un mot de passe.

SMBClient

On peut énumérer tous les fichiers d'un partage avec **smbclient** :

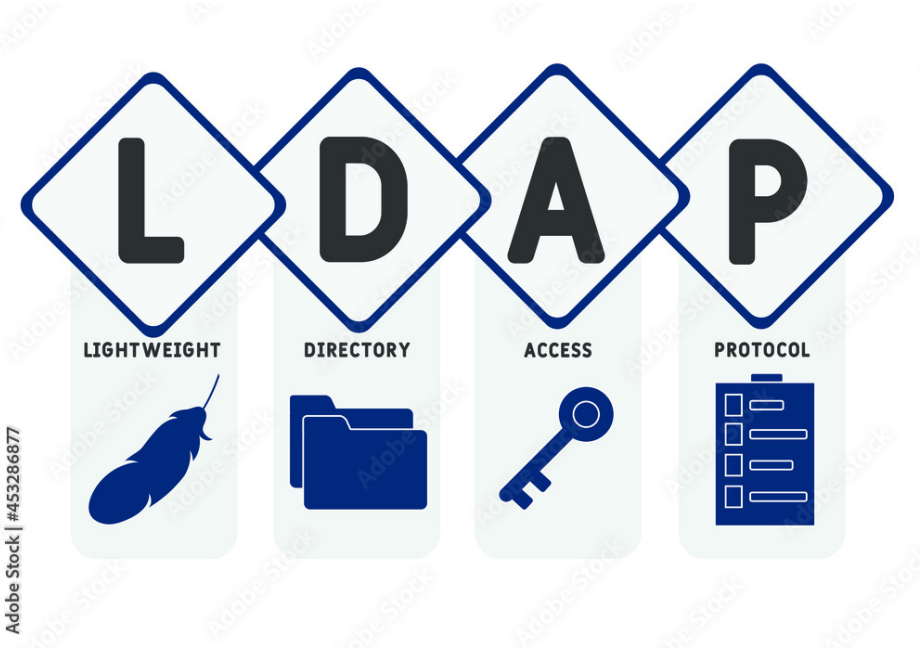
```
smbclient -N //<IP>/<SHARE>
```

[Énumération] LDAP

Introduction

LDAP pour Lightweight Directory Access Protocol, est un protocole d'annuire utilisé par des outils libres tels que **OpenLDAP**, mais aussi des solutions propriétaires comme **Active Directory**.

Quand il est utilisé au sein d'une organisation, il est une source d'information gigantesque pour un pirate qui arriverait à énumérer l'annuaire.



Nmap

Un script est présent au sein de l'outil pour scanner les annuaires LDAP.

Pour cela, exécutez la commande suivante :

```
nmap -p 389 --script=ldap-search <IP>
```

Web

Web

[Énumération/Web] Cheat-sheet

Introduction

Des outils permettent l'énumération de serveur web comme **Gobuster**, **Dirbuster**, **Nikto** ou **WFuzz**.



Gobuster

Files and directories

Voici comment utiliser gobuster pour trouver les **fichiers** et **répertoires** sur un serveur web :

```
gobuster dir -w <WORDLIST_PATH> -u <URL>
```

Subdomains

Voici comment utiliser gobuster pour trouver les **sous-domaines** sur un serveur web :

```
gobuster dns -w <WORDLIST_PATH> -u <URL>
```

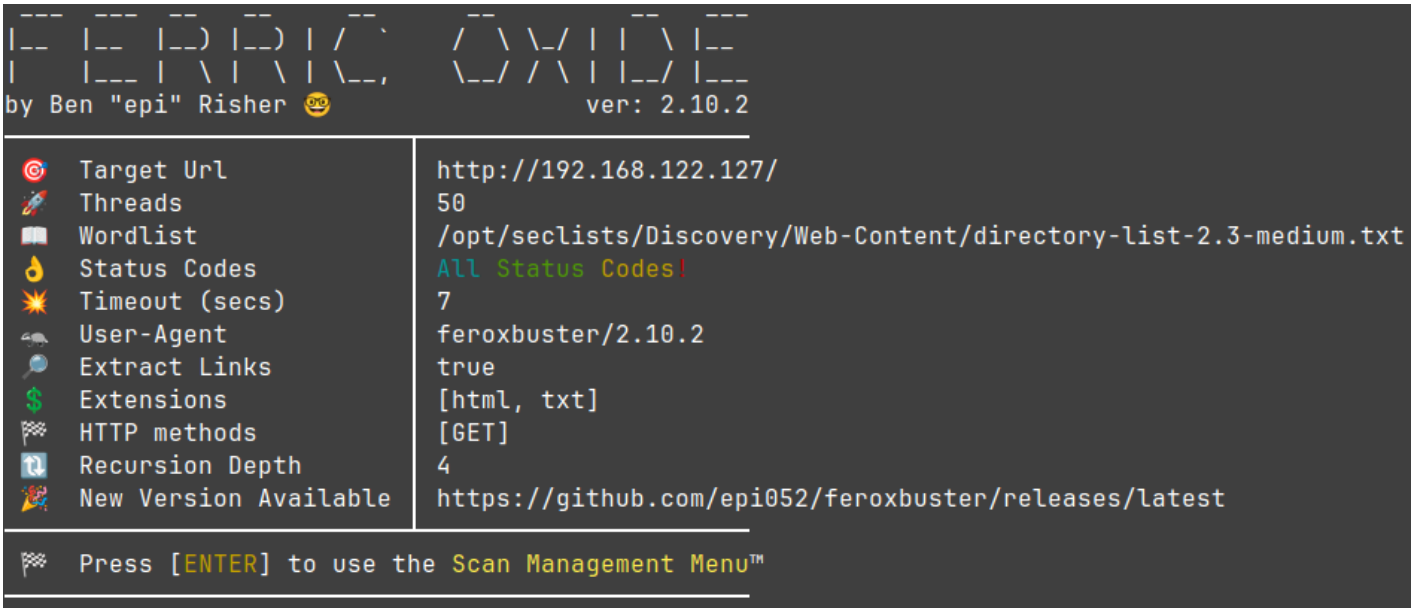
Fuzzing

Voici comment utiliser gobuster pour tester des **paramètres** sur un serveur web :

```
gobuster dns -w <WORDLIST_PATH> -u <URL/<PAGE>.php?PARAMETER=FUZZ>
```

Feroxbuster

- https://github.com/epi052/feroxbuster



L'outil se veut être un clone de gobuster en allant plus vite et avec une interface plus agréable.

Directories

```
feroxbuster -w <WORDLIST> --url <URL>
```

Files

```
feroxbuster -w <WORDLIST> --url <URL> -x <EXT1> [EXT2]
```

> Par exemple vous pouvez utiliser les options suivantes : **-x html php js txt** .

> La wordlist sélectionnée doit correspondre à ce que vous cherchez (fichiers/dossiers).

WFuzz

Voici comment faire du fuzzing :

```
wfuzz -c -z file,<WORDLIST> --hc 404 <URL>
```

Web

[Énumération/Web] LFI - RFI

Introduction

Les vulnérabilités **LFI** pour *Local File Inclusion* et **RFI** pour *Remote File Inclusion* sont très dangereuses puisqu'elles peuvent aboutir à des RCE dans certains cas ou l'affichage de fichiers systèmes comme /etc/shadow et /etc/passwd .

Ces failles reposent sur la possibilité pour l'utilisateur d'un site web de pouvoir appeler un fichier dont il ne doit pas avoir accès initialement.

Là où la LFI se contente de pouvoir appeler des fichiers locaux au serveur web, la RFI permet d'ouvrir un fichier distant.



LFI Finder Tool

Un outil très pratique qui permet d'énumérer les LFI disponibles d'une application web :

https://github.com/capture0x/LFI-FINDER

Réseau

Réseau

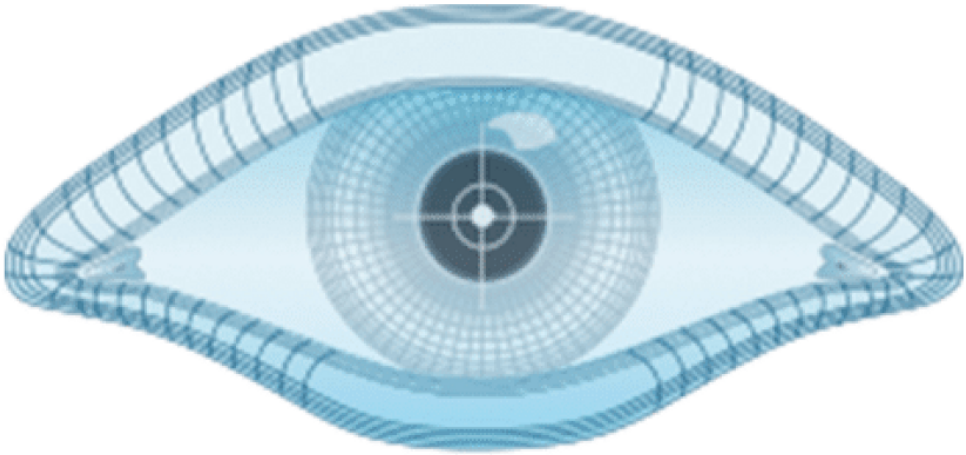
[Énumération/Réseau] Nmap

Introduction

Nmap est certainement le plus grand outil d'énumération réseau au monde.

Il permet de découvrir un réseau ou de scanner des ports et même de chercher des vulnérabilités.

Il est incontournable pour les professionnels de la cybersécurité.



Manuel

Syntaxe globale

```
nmap [OPTIONS] <IP>
```

Découverte du réseau

```
nmap -sn <IP>/<MASK>
```

Scan d'un port

```
nmap -p <PORT> <IP>
```

Scan d'une plage de ports

```
nmap -p <FIRST_PORT>-<LAST_PORT> <IP>
```

Scan des 1000 ports les plus populaires

```
nmap -F <IP>
```

Scan avancé

```
nmap -A <IP>
```

> L'option -A regroupe les options -O, -sV et exécute certains scripts NSE pour chercher des services et des vulnérabilités.

Scan UDP

```
nmap -sU <IP>
```

> Vous pouvez aussi utiliser l'option -p pour ne scanner qu'un ou une plage de ports.

Scan rapide

```
nmap -T4 <IP>
```

Scan discret

```
nmap -T1 <IP>
```

> Le scan sera beaucoup plus lent qu'un scan habituel.

Autres options

Options	Fonctions

-v	Mode verbeux
-n	Désactive la résolution DNS
-g <SRC_PORT>	Permet de spécifier un port source de la connexion
-oN <OUTPUT_FILE>	Sauvegarde la sortie dans un fichier
-oX <OUTPUT_FILE>	Sauvegarde la sortie dans un fichier au format XML
--exclude <FILE>	Exclue les IP contenues dans le fichier lors du scan
--stats-every <TIME>	Affiche les statistiques du scan en temps réel
--script <DEFAULT|SCRIPT>	Exécute le script spécifié ou tous les scripts si default est indiqué

Scripts

L'ensemble des scripts fournis par nmap sont disponibles dans le dossier **/usr/share/nmap/scripts** .

Projet dashboard grafana

Voici un projet que je trouve intéressant pour intégrer des graphiques de vos scans nmap dans vos rapports de pentest :

- https://github.com/hackertarget/nmap-did-what

Tout d'abord clonez le dépôt :

```
git clone https://github.com/hackertarget/nmap-did-what
```

Ensuite lancez votre scan nmap avec un fichier d'export au format XML avec l'option **-oX** :

```
nmap -sC -sV -Pn -n <IP> -oX scan.xml
```

Injectez les données récupérées dans la base de données du projet :

```
cd nmap-did-what && cp scan.xml /data/ && python3 nmap-to-sqlite.py scan.xml && cd ..
```

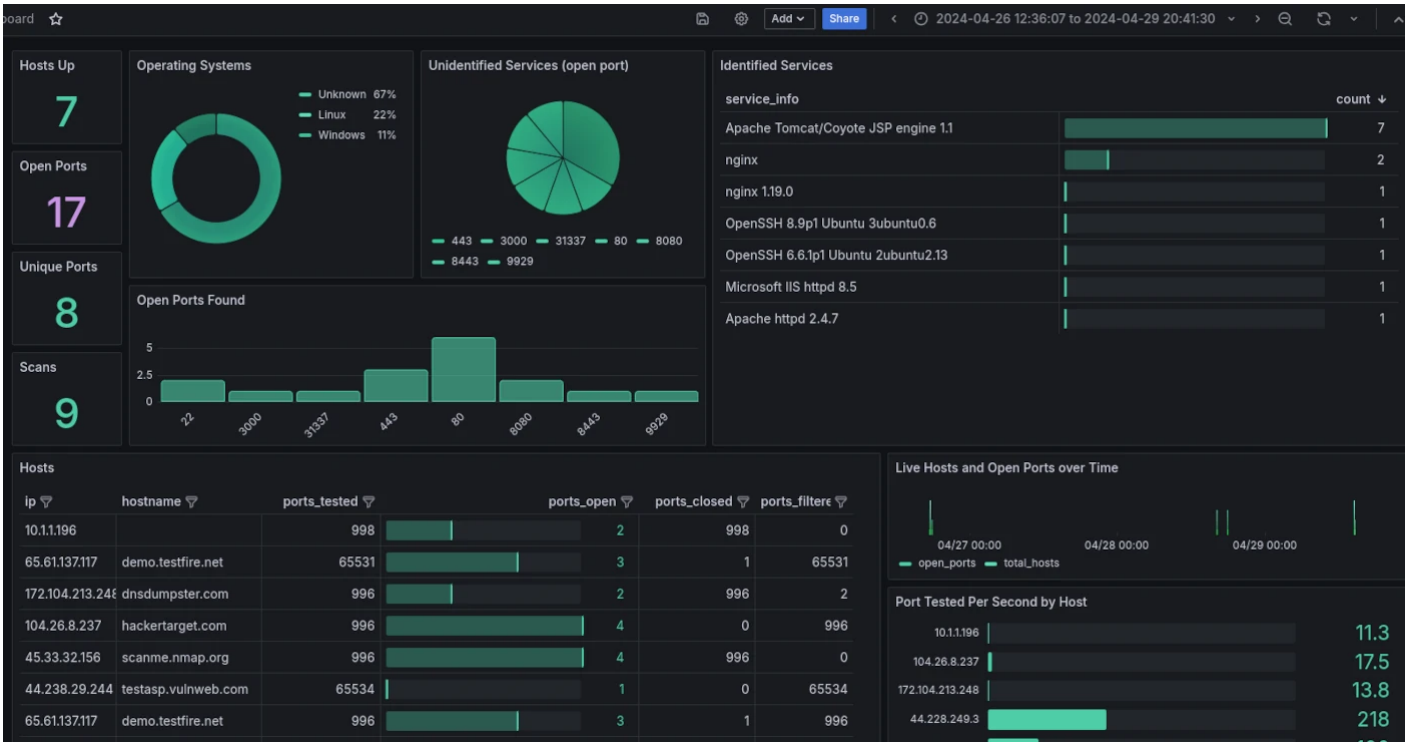
Lancez la stack docker :

```
cd grafana-docker/ && docker compose up -d && cd ..
```

Rendez-vous sur l'interface Grafana :

- https://localhost:3000

Depuis le menu **Dashboard**, retrouvez ces graphiques préconfigurés :



Réseau

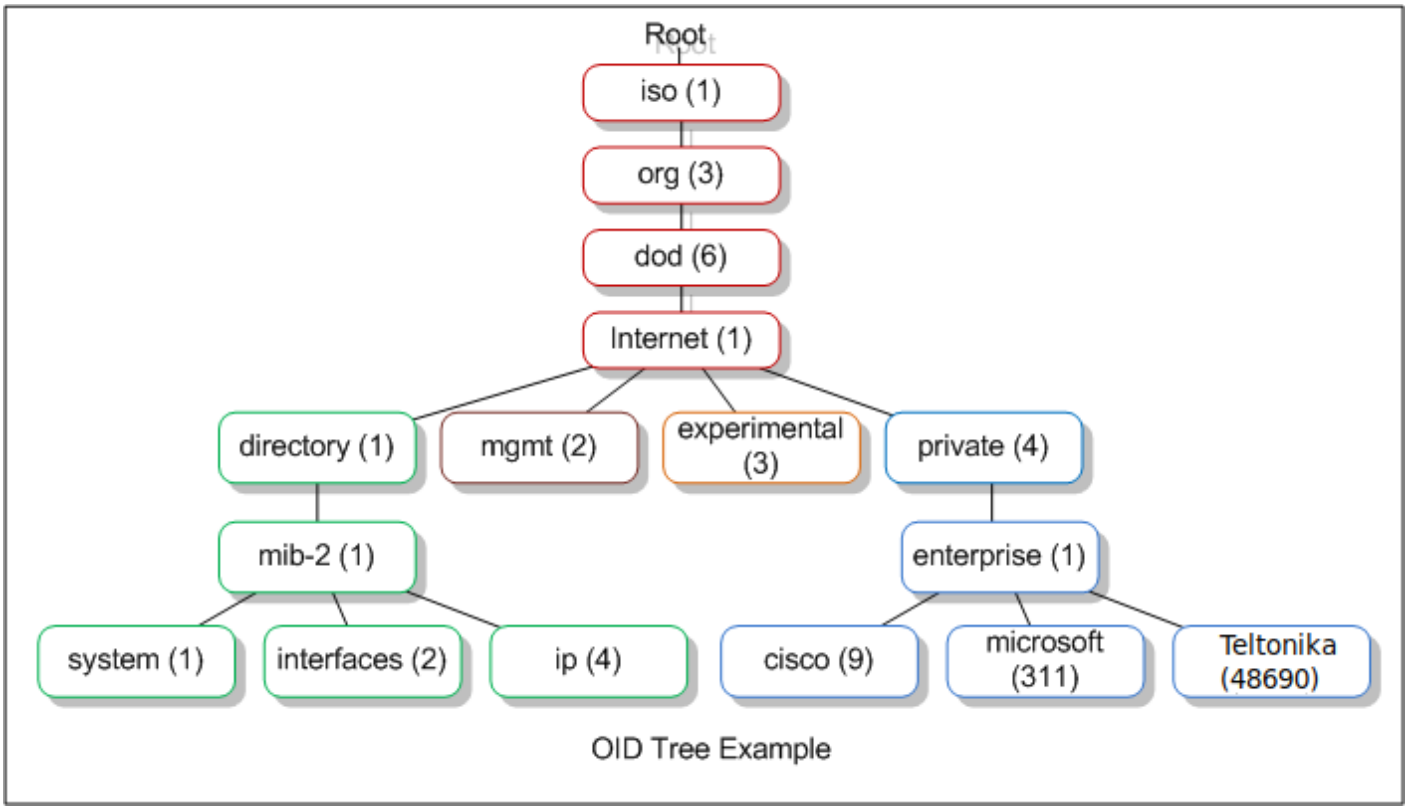
[Énumération/Réseau] SNMP

Introduction

Le protocole **SNMP** pour *Simple Network Management Protocol* permet de gérer les ressources sur un réseau.

Il existe des agents SNMP (installés sur les hôtes réseaux) et des managers SNMP qui sont capables de récupérer des informations identifiées par un OID, sur les agents.

Par défaut, il utilise le port **161**.



OID Tree Example

Composition de l'OID

Pour identifier les objets, on utilise ce qu'on appelle un **OID** qui est formé selon l'arbre ci-dessus.

Par exemple, pour obtenir l'OID de l'ip, on parcours l'arbre du haut vers le bas en mettant un point entre chaque numéro, ce qui donnerait : **1.3.6.1.1.1.4** .

Les versions de SNMP

Communautés SNMP

Le terme de "communauté" fait référence à la méthode d'authentification utilisé dans les SNMPv1 et SNMPv2c.

Il existe deux types de communauté :

- **Communauté "publique" (public) :** Offre un accès en lecture seule aux informations de l'agent.
- **Communauté "privée" (private) :** Permet un accès en lecture et en écriture, permettant de modifier la configuration de l'agent.

SNMPv3

Contrairement aux anciennes versions du protocole, SNMPv3 introduit un modèle de sécurité plus avancé, offrant des fonctionnalités telles que l'authentification, la confidentialité et le contrôle d'accès de manière plus robuste. Il n'utilise pas de communautés, mais des mécanismes d'authentification et de chiffrement plus sophistiqués pour assurer la sécurité des données échangées entre le gestionnaire et les agents.

SNMPget

Syntaxe globale

```
snmpget [OPTIONS] <TARGET_IP> <OID>
```

Exemples d'utilisation

- Interroger un agent pour obtenir une information spécifique :

```
snmpget -v2c -c community 192.168.1.1 1.3.6.1.2.1.1.1.0
```

- Utiliser SNMP v3 avec des informations d'identification :

```
snmpget -v3 -u username -l authPriv -a MD5 -A authpass -x DES -X privpass 192.168.1.1
1.3.6.1.2.1.1.1.0
```

- Récupérer des informations à partir d'une cible nommée plutôt que son IP :

```
snmpget -v2c -c public -n mytarget 1.3.6.1.2.1.1.1.0
```

Options courantes

Options	Descriptions
-v[X]	Spécifie la version SNMP (X peut être 1, 2c ou 3).
-c	Spécifie la communauté SNMP (uniquement pour SNMP v1 et v2c).
-u	Spécifie l'identifiant d'utilisateur (uniquement pour SNMP v3).
-l	Spécifie le niveau de sécurité (SNMP v3).
-a	Spécifie l'algorithme d'authentification (SNMP v3)
-x	Spécifie l'algorithme de chiffrement (SNMP v3).
-A	Spécifie le mot de passe d'authentification (SNMP v3).
-X	Spécifie le mot de passe de chiffrement (SNMP v3).
-n	Nomme la cible en utilisant un nom au lieu d'une adresse IP.

Réseau

[Énumération/Réseau] DNS

Introduction

Il existe plusieurs outils qui permettent d'énumérer un serveur DNS car ce dernier est souvent le point d'entrée des attaquants et regorge d'informations utiles sur les sous-domaines, les serveurs de messageries ou les adresses IP utilisés par la cible.



Dig

Certainement l'outil le plus connu pour énumérer les serveurs DNS, il est très puissant et possède de nombreuses options.

Utilisation standard

```
dig <FQDN>
```

Énumération des serveurs de messagerie

```
dig <FQDN> -t mx +short
```

Host

Cette commande va énumérer tous les serveurs se trouvant derrière le nom de domaine indiqué :

```
host <FQDN>
```

DNSenum

Installation

```
sudo apt install -y dnsenum
```

Manuel

```
dnsenum <FQDN>
```

> Vous pouvez utiliser l'option **--noreverse** pour ne pas lancer la procédure de reverse lookup sur les IP trouvées.

Réseau

[Énumération/Réseau] Zmap

Introduction

Zmap est un outil qui permet de scanner très rapidement toute ou une partie de plage IPv4 d'Internet pour savoir lesquelles ont un ou plusieurs ports ouverts.



Installation

```
sudo apt update && sudo apt install -y zmap
```

Manuel

Syntaxe globale

```
sudo zmap -p <PORT> -o <FILE> <TARGET_IP>
```

Exemples d'utilisation

- Scanner tout internet sur le port 80 :

```
sudo zmap -p 80 -o scan_port_80_results.txt 0.0.0.0/0
```

- Balayer une plage d'IP sur plusieurs ports :

```
sudo zmap -p 22,80,443 -o scan_result.json 192.168.1.0/24
```

- Limiter l'utilisation de la bande passante :

```
sudo zmap -p 3389 -o rdp_results.csv -B 5M 10.0.0.0/16
```

Options courantes

Options	Descriptions
-p <PORT>	Spécifie le numéro de port à balayer.
-o <FILE>	Spécifie le fichier de sortie pour enregistrer les résultats.
-B <BYTES>	Limite la bande passante utilisée (par exemple, "-B 10M" pour limiter à 10 Mbps).
-f <FORMAT>	Spécifie le format de sortie (par exemple, **json** ou **csv**).
-q	Mode silencieux (supprime les avertissements)
-N	Définit le nombre de threads à utiliser pour le balayage.

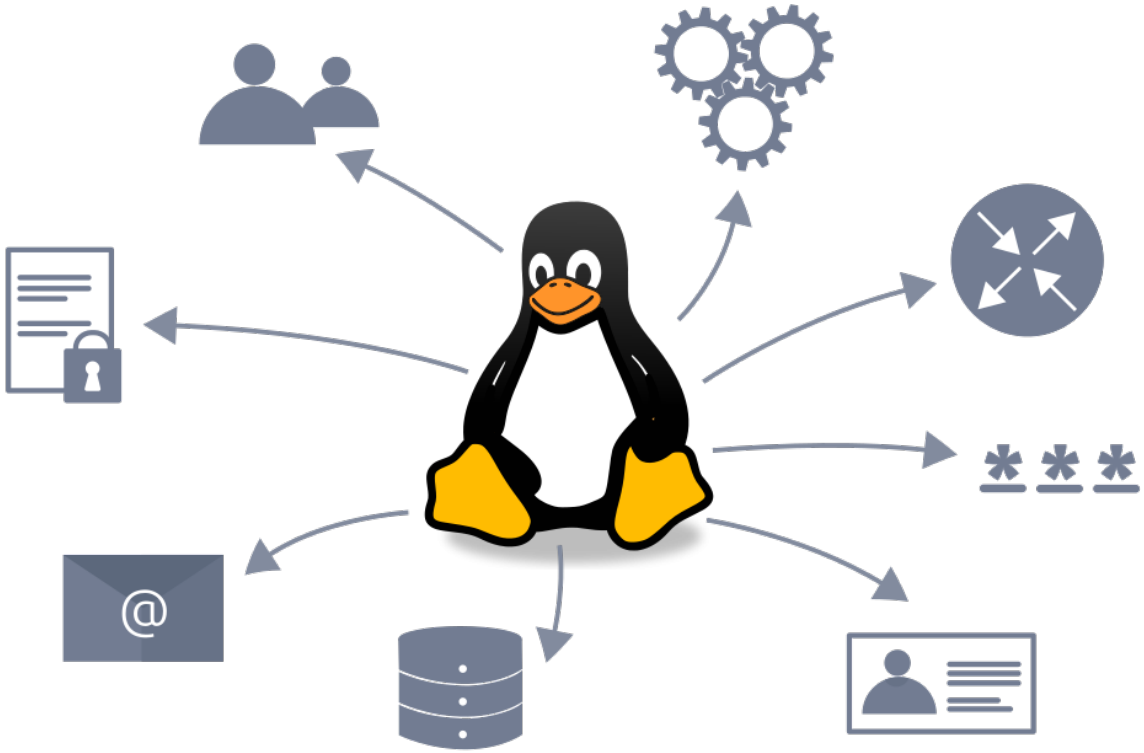
Linux

Linux

[Énumération/Linux] Cheat-sheet

Introduction

Cette page va décrire différents procédés pour énumérer un système **Linux** qui pourraient vous servir.



Manuel

Afficher la version de l'OS

```
ls /etc/*-release
```

Par exemple sur **CentOS** :

```
cat /etc/os-release
```

Afficher les utilisateurs / groupes / mots de passe

```
cat /etc/passwd
```

```
cat /etc/groups
```

```
cat /etc/shadow
```

> Le fichier **shadow** est protégé en lecture par défaut et n'est pas accessible !

Afficher les mails

```
ls -lh /var/mail/
```

Afficher la liste des paquets

Sur les systèmes basés sur **Debian** :

```
dpkg -l
```

Et pour les systèmes basés sur **RedHat** :

```
rpm -qa
```

Afficher les utilisateurs connectés

```
who
```

Afficher la commande en cours d'exécution des utilisateurs connectés

```
w
```

Afficher les dernières connexions d'utilisateurs

```
last
```

Afficher les connexions actives

```
lsof -i [:PORT]
```

Afficher l'arborescence des processus

```
ps axjf
```

[Énumération/Linux] Git-dumper

Introduction

Parfois, le site web que vous attaquez peut contenir un dépôt **Git**.

Dans ce cas, il peut être intéressant le récupérer pour accéder au code source voire aux fichiers de configurations qui pourraient contenir des mots de passe ou autre.

Git-dumper

Vous pouvez trouver le github de l'outil à cette adresse :

- https://github.com/arthaud/git-dumper

Manuel

```
git-dumper <URL>/.git <OUTPUT_FOLDER>
```