
*Sylvain THIROINE*

# **Fiche n ° 3** : Nmap


## Table des matières

Voici la syntaxe par défaut de nmap : **nmap [Type de Scans] [Options] {Host cible}**

### 1.1. Analyser un hôte ou réseau distant

Pour **analyser une machine distante** :

```
nmap 192.168.1.1
nmap www.host.tld
```

Pour **scanner plusieurs hôtes** :

```
nmap 192.168.1.1 192.168.1.2 192.168.1.3
```

**Pour scanner un réseau entier**, on peut spécifier un masque de sous réseau :

```
nmap 192.168.1.0/24
nmap 192.168.1.*
```

Mais on peut aussi **analyser un intervalle de machines** comme ceci :

```
nmap 192.168.1.0-200
```

Pour afficher des détails, on ajoute les options -v ou -vv pour le mode bavard :

```
nmap -v 192.168.1.1
nmap -vv 192.168.1.1
```

### 1.2. Scanner une liste d'hôte à partir d'un fichier

Pour **scanner des hôtes depuis un fichier :**

```
nmap -iL /tmp/listehote.txt
```

### 1.3. Exclure IP / Hôtes / Réseaux de Nmap Scan

Pour **exclure des hôtes d'une analyse** :

```
nmap 192.168.1.0/24 --exclude 192.168.1.1
nmap 192.168.1.0/24 --exclude 192.168.1.1 192.168.1.5
nmap 192.168.1.0/24 --exclude 192.168.1.1,2,3
```

Ou encore **exclure des hôtes depuis un fichier** :

```
nmap 192.168.1.0/24 --excludefile exclusion.txt
```

### 1.4. Énumérer les ports TCP / UDP

**Scanner tous les ports TCP :**

```
nmap -sT 192.168.1.1
```

**Scanner tous les ports UDP :**

```
nmap -sU 192.168.1.1
```

**Scanner un port TCP en particulier :**

```
nmap -p T:80 192.168.1.1
```

**Scanner un port UDP :**

```
nmap -p U:53 192.168.1.1
```

Pour **scanner un intervalle de ports :**

```
nmap -p T:1-1024 192.168.1.1
```

Pour combiner plusieurs scans de ports réseaux spécifiques :

```
nmap -p U:53,9,113,T:21-25,80,443,8080 192.168.1.1
```

### 1.5. Effectuer une analyse rapide

Le scan rapide rechercher les ports répertoriés dans les fichiers nmap-services, cela permet de recenser les principaux services réseaux.
Pour cela, on utilise **l'option -F** de Nmap :

```
nmap -F 192.168.1.1
```

### 1.6. Rechercher les numéros de version des services hôte

Nous pouvons **trouver les versions du service** qui s'exécutent sur des hôtes distants avec **l'option -sV :**

```
nmap -sV 192.168.1.1
```

### 1.7. Analyser les informations du système d'exploitation et Traceroute

Nmap est aussi capable de détecter le système d'exploitation et la version en cours d'exécution sur l'hôte distant.

Pour activer la détection du système d'exploitation et de la version, l'analyse des scripts et le Traceroute, nous pouvons utiliser **l'option -A :**

nmap -A 192.168.1.1

Nmap effectue un **TCP/IP fingerprint** et affiche le **Traceroute.**
Si vous désirez n'avoir que la détection de l'OS, il faut utiliser **l'option -O** :

nmap -O 192.168.1.1

### 1.8. Désactiver la découverte d'hôte (pas de Ping) ou résolution DNS

Ne pas envoyer de requête ping à l'hôte avant la numérisation avec **l'option -Pn**

nmap -Pn 192.168.1.1

Pour désactiver la résolution DNS, utilisez **l'option -n** :

nmap -n 192.168.1.1

### 1.9. Effectuer des scans pour tromper un pare-feu

**TCP Null Scan** – Ne définissez aucun bit (l'en-tête de l'indicateur TCP est 0).

nmap -sN 192.168.1.1

**TCP Fin Scan** – Définissez uniquement le bit TCP FIN.

nmap -sF 192.168.1.1

**TCP Xmas Scan** – Définissez les drapeaux FIN, PSH et URG (allumant le paquet comme un arbre de Noël).

nmap -sX 192.168.1.1

### 1.10. Changer le type de scan

L'option -P permet de changer le type de scan :

- **-Pn**: Traitez tous les hôtes comme en ligne – ignorez la découverte des hôtes
- **-PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP** découverte vers des ports donnés
- **-PE / PP / PM**: sondes de découverte d'écho, d'horodatage et de demande de masque de réseau ICMP
- **-PO** [liste de protocoles]: Ping de protocole IP

Analyser les hôtes distants à l'aide de TCP ACK (PA) et TCP Syn (PS) :

nmap -PS 192.168.1.1

Analyser l'hôte distant pour des ports spécifiques avec TCP ACK :

nmap -PA -p 22,80 192.168.1.1

Analyser l'hôte distant pour des ports spécifiques avec TCP Syn :

nmap -PS -p 22,80 192.168.1.1

Effectuer une analyse furtive (**TCP SYN Scan)** :

nmap -sS 192.168.0.101

### 1.11. Scanner de vulnérabilités Nmap

Il existe un script prédéfini présent dans la commande dans Nmap qui permet aux utilisateurs d'exécuter un scan de vulnérabilités. Cela est donc très pratique pour s'assurer que votre système est à jour et non vulnérable.
On peut utiliser ces scripts prédéfinis ou posséder leur langage de programmation Lua pour dériver une fonctionnalité spécifique qui peut aider à la détection CVE.

Pour cela, on utilise **l'option -script vuln** :

nmap -Pn –script vuln 192.168.1.1

Vous pouvez simplement utiliser le vérificateur de logiciels malveillants Google SafeBrowsing par la commande :

nmap -p80 –script http-google-malware www.malekal.com

### 1.12. Lancer une attaque bruteforce

Vous pouvez également utiliser **Nmap pour lancer une attaque par bruteforce**.
Là aussi, on utilise **l'option -script** pour spécifier le type d'attaque.

nmap -sV –script http-wordpress-brute –script-args 'userdb=users.txt,passdb=passwds.txt,http-wordpress-brute.hostname=domain.com, http-wordpress-brute.threads=3,brute.firstonly=true' 192.168.1.1

Brute force attack against MS-SQL:

nmap -p 1433 –script ms-sql-brute –script-args userdb=customuser.txt,passdb=custompass.txt 192.168.1.105

Brute force attack against FTP:

nmap –script ftp-brute -p 21 192.168.1.105

### 1.13. Enregistrer le résultat du scan dans un fichier

**L'option -oN** permet d'enregistrer le résultat du portscan **dans un fichier au format texte :**

nmap -oN output.txt 192.168.1.1

Pour enregistrer le résultat du scan de port dans **un fichier au format XML** :

nmap -oX output.xml 192.168.1.1

### 1.14. Liste des différents script NMAP

1. **acarsd-info**
   Récupère les informations d'un démon acarsd à l'écoute. Acarsd décode les données ACARS (système de communication et d'adressage des aéronefs) en temps réel. Les informations récupérées par ce script incluent la version du démon, la version de l'API, l'adresse de messagerie de l'administrateur et la fréquence d'écoute.
2. **adresse-info**
   Affiche des informations supplémentaires sur les adresses IPv6, telles que les adresses MAC ou IPv4 intégrées, le cas échéant.
3. **afp-brute**
   Effectue un test de mot de passe par rapport au protocole AFP (Apple Filing Protocol).
4. **afp-ls**
   Tente d'obtenir des informations utiles sur les fichiers des volumes AFP. La sortie est destinée à ressembler à la sortie de ls.
5. **afp-path-vuln**
   Détecte la vulnérabilité de traversée de répertoire de Mac OS X AFP, CVE-2010-0533.
6. **afp-serverinfo**
   Affiche les informations du serveur AFP. Ces informations incluent le nom d'hôte du serveur, les adresses IPv4 et IPv6, ainsi que le type de matériel (par exemple Macminiou MacBookPro).
7. **afp-showmount**
   Affiche les partages AFP et les ACL.
8. **ajp-auth**
   Récupère le schéma d'authentification et le domaine d'un service AJP (protocole Apache JServ) nécessitant une authentification.
9. **ajp-brute**
   Effectue l'audit des mots de passe en force brute par rapport au protocole Apache JServ. Le protocole Apache JServ est couramment utilisé par les serveurs Web pour communiquer avec des conteneurs de serveurs d'applications Java dorsaux.
10. **en-têtes ajp**
    Exécute une requête HEAD ou GET sur le répertoire racine ou tout répertoire facultatif d'un serveur de protocole Apache JServ et renvoie les en-têtes de réponse du serveur.
11. **méthodes ajp**
    Découvre les options prises en charge par le serveur AJP (Apache JServ Protocol) en envoyant une demande OPTIONS et répertorie les méthodes potentiellement risquées.
12. **ajp-request**
    Demande un URI sur le protocole Apache JServ et affiche le résultat (ou le stocke dans un fichier). Différentes méthodes AJP telles que; GET, HEAD, TRACE, PUT ou DELETE peuvent être utilisés.
13. **allseeingeye-info**
    Détecte le service All-Seeing Eye. Fourni par certains serveurs de jeux pour interroger le statut du serveur.

14. **amqp-info**
    Recueille des informations (liste de toutes les propriétés du serveur) à partir d'un serveur AMQP (Advanced Message Queuing Protocol).
15. **asn-query**
    Mappe les adresses IP sur les numéros de système autonome (AS).
16. **propriétaires**
    Tente de trouver le propriétaire d'un port TCP ouvert en interrogeant un démon d'authentification qui doit également être ouvert sur le système cible. Le service d'authentification, également appelé identd, s'exécute normalement sur le port 113.
17. **auth-spoof**
    Recherche un serveur identd (auth) qui utilise des réponses frauduleuses.
18. **backorifice-brute**
    Effectue l'audit du mot de passe brute force par rapport au service BackOrifice. L' backorifice-brute.portsargument de script est obligatoire (il spécifie les ports sur lesquels le script doit être exécuté).
19. **backorifice-info**
    Se connecte à un service BackOrifice et collecte des informations sur l'hôte et le service BackOrifice lui-même.
20. **bacnet-info**
    Découvre et énumère les périphériques BACNet collecte les informations sur les périphériques en se basant sur les requêtes standard. Dans certains cas, les périphériques peuvent ne pas suivre strictement les spécifications, ou peuvent être conformes à des versions plus anciennes des spécifications, et entraîneront une réponse d'erreur BACNET. La présence de cette erreur identifie positivement le périphérique en tant que périphérique BACNet, mais aucune énumération n'est possible.
21. **bannière**
    Une simple capture de bannière qui se connecte à un port TCP ouvert et imprime tout ce qui est envoyé par le service d'écoute dans les cinq secondes.
22. **bitcoin-getaddr**
    Demande à un serveur Bitcoin une liste des nœuds Bitcoin connus
23. **bitcoin-info**
    Extrait les informations de version et de nœud d'un serveur Bitcoin
24. **bitcoinrpc-info**
    Obtient des informations d'un serveur Bitcoin en appelant getinfosur son interface JSON-RPC.
25. **bittorrent-discovery**
    Découvre des pairs bittorrent partageant un fichier basé sur un fichier torrent ou un lien magnétique fourni par l'utilisateur. Les pairs implémentent le protocole Bittorrent et partagent le torrent, alors que les nœuds (indiqués uniquement si l'argument include-nodes NSE est fourni) implémentent le protocole DHT et sont utilisés pour suivre les homologues. Les ensembles de pairs et de nœuds ne sont pas identiques, mais ils se croisent généralement.
26. **bjnp-découvrir**
    Récupère les informations sur l'imprimante ou le scanner d'un périphérique distant prenant en charge le protocole BJNP. Le protocole est connu pour être pris en charge par les périphériques Canon basés sur le réseau.
27. **diffusion-ataoe-decouvrir**
    Découvre les serveurs prenant en charge le protocole ATA over Ethernet. ATA over Ethernet est un protocole Ethernet développé par la société Brantley Coile. Il permet un accès simple et performant aux disques SATA via Ethernet.
28. **broadcast-avahi-dos**
    Tente de découvrir des hôtes du réseau local à l'aide du protocole DNS Service Discovery et envoie un paquet NULL UDP à chaque hôte pour déterminer s'il est vulnérable au déni de service de paquet Avahi NULL UDP (CVE-2011-1002).
29. **diffusion-bjnp-découvrir**
    Tente de découvrir des périphériques Canon (imprimantes / scanners) prenant en charge le protocole BJNP en envoyant des demandes de découverte BJNP à l'adresse de diffusion réseau des deux ports associés au protocole.
30. **broadcast-db2-discover**
    Tente de découvrir les serveurs DB2 sur le réseau en envoyant une demande de diffusion au port 523 / udp.

31. **diffusion-dhcp-découvrir**
    Envoie une requête DHCP à l'adresse de diffusion (255.255.255.255) et rapporte les résultats. Le script utilise une adresse MAC statique (DE: AD: CO: DE: CA: FE) pour éviter l'épuisement de la portée.
32. **diffusion-dhcp6-découvrir**
    Envoie une demande DHCPv6 (Solicit) à l'adresse de multidiffusion DHCPv6, analyse la réponse, puis extrait et imprime l'adresse avec toutes les options renvoyées par le serveur.
33. **broadcast-dns-service-discovery**
    Tente de découvrir les services des hôtes à l'aide du protocole DNS Service Discovery. Il envoie une requête multidiffusion DNS-SD et collecte toutes les réponses.
34. **broadcast-dropbox-listener**
    Écoute les informations de synchronisation sur le réseau local diffusées par le client Dropbox.com toutes les 20 secondes, puis imprime toutes les adresses IP, numéros de port, numéros de version, noms d'affichage, etc.
35. **broadcast-eigrp-discovery**
    Effectue la découverte du réseau et la collecte des informations de routage via le protocole EIGRP (Enhanced Interior Gateway Routing Protocol) de Cisco.
36. **diffusion cachée découverte**
    Découvre les périphériques HID sur un réseau local en envoyant une sonde broadcast broadcast sur le réseau.
37. **broadcast-igmp-discovery**
    Découvre les cibles ayant des abonnements IGMP Multicast et récupère des informations intéressantes.
38. **diffusion-jenkins-découvrir**
    Découvre les serveurs Jenkins sur un réseau local en envoyant une analyse de diffusion découverte
39. **auditeur de diffusion**
    Sniffe le réseau pour les communications de diffusion entrantes et tente de décoder les paquets reçus. Il supporte des protocoles tels que CDP, HSRP, Spotify, DropBox, DHCP, ARP et quelques autres. Voir packetdecoders.lua pour plus d'informations.
40. **broadcast-ms-sql-discover**
    Découvre les serveurs Microsoft SQL dans le même domaine de diffusion.
41. **broadcast-netbios-master-browser**
    Essaie de découvrir les principaux navigateurs et les domaines qu'ils gèrent.
42. **broadcast-networker-discover**
    Découvre les serveurs de logiciels de sauvegarde EMC Networker sur un réseau local en envoyant une requête de diffusion réseau.
43. **diffusion-novell-localiser**
    Tente d'utiliser le protocole d'emplacement de service pour découvrir les serveurs NCP (Novell NetWare Core Protocol).
44. **diffusion-ospf2-découvrir**
    Découvrez les réseaux IPv4 à l'aide du protocole OSPFv2 (Open Shortest Path First).
45. diffusion-pc-n'importe où
    Envoie une analyse de diffusion spéciale pour découvrir les hôtes PC-Anywhere fonctionnant sur un réseau local.
46. **duo-pc-duo**
    Découvre les hôtes et les passerelles de contrôle à distance PC-DUO s'exécutant sur un réseau local en envoyant une sonde UDP de diffusion spéciale.
47. **diffusion-pim-découverte**
    Découvre les routeurs qui exécutent PIM (Protocol Independent Multicast).
48. **diffusion-ping**
    Envoie des pings de diffusion sur une interface sélectionnée en utilisant des paquets Ethernet bruts et génère les adresses IP et MAC des hôtes qui répondent ou les ajoute (si nécessaire) en tant que cibles. Les privilèges root sur UNIX sont requis pour exécuter ce script car il utilise des sockets bruts. La plupart des systèmes d'exploitation ne répondent pas aux sondes broadcast-ping, mais ils peuvent être configurés pour le faire.
49. **diffusion-pppoe-découvrir**
    Découvre les serveurs PPPoE (protocole point à point sur Ethernet) à l'aide du protocole PPPoE Discovery (PPPoED). PPPoE est un protocole Ethernet, le script doit donc savoir quelle interface Ethernet utiliser pour la découverte. Si aucune interface n'est spécifiée, les demandes sont envoyées sur toutes les interfaces disponibles.

50. **diffusion-déchirer-découvrir**
    Découvre les hôtes et les informations de routage des périphériques exécutant RIPv2 sur le réseau local. Pour ce faire, il envoie une commande RIPv2 Request et collecte les réponses de tous les périphériques qui répondent à la requête.
51. **diffusion-déchiffrer-découvrir**
    Découvre les hôtes et les informations de routage des périphériques exécutant RIPng sur le réseau local en envoyant une commande broadcast RIPng Request et en collectant les réponses éventuelles.
52. **broadcast-sonicwall-découvrir**
    Découvre les pare-feu Sonicwall directement connectés (non routés) en utilisant la même méthode que celle du fabricant, 'SetupTool'. Une interface doit être configurée, car le script diffuse un paquet UDP.
53. **broadcast-sybase-asa-discover**
    Découvre les serveurs Sybase Anywhere sur le réseau local en envoyant des messages de découverte par diffusion.
54. **diffusion-tellstick-discover**
    Découvre les périphériques TellDickNet de Telldus Technologies sur le réseau local. Le Telldus TellStick est utilisé pour contrôler sans fil des appareils électriques tels que des éclairages, des gradateurs et des prises de courant.
55. **broadcast-upnp-info**
    Tente d'extraire les informations système du service UPnP en envoyant une requête multidiffusion, puis en collectant, en analysant et en affichant toutes les réponses.
56. **diffusion-versant-localiser**
    Découvre les bases de données d'objet Versant à l'aide du protocole broadcast srvloc.
57. **émission-sillage sur LAN**
    Réveille un système distant en envoyant un paquet Wake-On-Lan.
58. **diffusion-wpad-découvrir**
    Récupère une liste de serveurs proxy sur un réseau local à l'aide du protocole WPAD (Web Proxy Autodiscovery Protocol). Il implémente à la fois les méthodes DHCP et DNS et commence par interroger DHCP pour obtenir l'adresse. La découverte DHCP nécessite que nmap s'exécute en mode privilégié et sera ignoré lorsque ce n'est pas le cas. La découverte DNS repose sur la capacité du script à résoudre le domaine local, soit à l'aide d'un argument de script, soit en tentant de résoudre en sens inverse l'adresse IP locale.
59. **broadcast-wsdd-discover**
    Utilise une requête multidiffusion pour détecter les périphériques prenant en charge le protocole Web Services Dynamic Discovery (WS-Discovery). Il tente également de localiser tous les services Web publiés Windows Communication Framework (WCF) (.NET 4.0 ou version ultérieure).
60. **broadcast-xdmcp-discover**
    Découvre les serveurs exécutant le protocole de contrôle X Display Manager (XDMCP) en envoyant une demande de diffusion XDMCP au réseau local. Les gestionnaires d'affichage autorisant l'accès sont marqués à l'aide du mot clé Willing dans le résultat.
61. **cassandra-brute**
    Effectue un audit de mot de passe brutal sur la base de données Cassandra.
62. **cassandra-info**
    Tente d'obtenir des informations de base et l'état du serveur à partir d'une base de données Cassandra.
63. **cccam-version**
    Détecte le service CCcam (logiciel permettant de partager la télévision par abonnement entre plusieurs récepteurs).
64. **cics-enum**
    Enumérateur d'ID de transaction CICS pour les ordinateurs centraux IBM.
65. **cics-info**
    À l'aide de la transaction CEMT CICS, ce script tente de collecter des informations sur la région actuelle du serveur de transactions CICS. Il rassemble des informations sur le système d'exploitation, des jeux de données (fichiers), des transactions et des identifiants d'utilisateurs. Basé sur le script CICSpwn d'Ayoub ELAASSAL.
66. **cics-user-brute**
    Script de forçage brutal de l'ID utilisateur CICS pour l'écran de connexion CESL.
67. **cics-user-enum**
    Script d'énumération d'ID utilisateur CICS pour l'écran de connexion CESL / CESN.

68. **citrix-brute-xml**
    Essaie de deviner des informations d'identification valides pour le service XML de l'agent Web Citrix PN. Le service XML s'authentifie auprès du serveur Windows local ou d'Active Directory.
69. **citrix-enum-apps**
    Extrait une liste d'applications publiées du service de navigateur ICA.
70. **citrix-enum-apps-xml**
    Extrait une liste d'applications, d'ACL et de paramètres du service XML Citrix.
71. **citrix-enum-servers**
    Extrait une liste de serveurs Citrix du service du navigateur ICA.
72. **citrix-enum-servers-xml**
    Extrait le nom de la batterie de serveurs et des serveurs membres du service XML Citrix.
73. **Clamav-exec**
    Exploite les serveurs ClamAV vulnérables à l'exécution non conforme de la commande clamav.
74. **coap-ressources**
    Vide la liste des ressources disponibles à partir des points de terminaison CoAP.
75. **couchdb-stats**
    Obtient les statistiques de base de données d'une base de données CouchDB.
76. **tasses-info**
    Répertorie les imprimantes gérées par le service d'impression CUPS.
77. **cups-queue-info**
    Répertorie les travaux d'impression en attente du service CUPS distant, regroupés par imprimante.
78. **cvs-brute**
    Effectue un audit de mot de passe brutal avec l'authentification CVS pserver.
79. **cvs-brute-repository**
    Tente de deviner le nom des référentiels CVS hébergés sur le serveur distant. Avec la connaissance du nom de référentiel correct, les noms d'utilisateur et les mots de passe peuvent être devinés.
80. **daap-get-library**
    Récupère une liste de musique d'un serveur DAAP. La liste comprend les noms d'artistes et les titres des albums et des chansons.
81. d**b2-das-info**
    Se connecte au serveur IBM DB2 Administration Server (DAS) sur le port TCP ou UDP 523 et exporte le profil du serveur. Aucune authentification n'est requise pour cette demande.
82. **déluge-rpc-brute**
    Effectue un audit de mot de passe brutal contre le démon DelugeRPC.
83. **dhcp-découvrir**
    Envoie une demande DHCPINFORM à un hôte sur le port UDP 67 pour obtenir tous les paramètres de configuration locaux sans attribuer une nouvelle adresse.
84. **dict-info**
    Se connecte à un serveur de dictionnaire à l'aide du protocole DICT, exécute la commande SHOW SERVER et affiche le résultat. Le protocole DICT est défini dans la RFC 2229 et est un protocole qui permet à un client d'interroger un serveur de dictionnaires pour obtenir des définitions à partir d'un ensemble de bases de données de dictionnaires en langage naturel.
85. **distcc-cve2004-2687**
    Détecte et exploite une vulnérabilité d'exécution de code à distance dans le démon de compilateur distribué distcc. La vulnérabilité a été révélée en 2002, mais est toujours présente dans la mise en œuvre moderne en raison de la mauvaise configuration du service.
86. **dns-blacklist**
    Vérifie les adresses IP cibles par rapport à plusieurs listes noires anti-spam et anti-spam DNS et renvoie une liste des services pour lesquels une adresse IP a été marquée. Les contrôles peuvent être limités à une catégorie de service (par exemple: SPAM, PROXY) ou à un nom de service spécifique.
87. **dns-brute**
    Tentatives d'énumération des noms d'hôte DNS par détection brutale des sous-domaines communs. Avec dns-brute.srvargument, dns-brute essaiera également d'énumérer les enregistrements DNS SRV courants.

88. **dns-cache-snoop**
    Exécute la surveillance du cache DNS sur un serveur DNS.
89. **dns-check-zone**
    Vérifie la configuration de la zone DNS par rapport aux meilleures pratiques, y compris RFC 1912. Les vérifications de la configuration sont divisées en catégories, chacune comportant un certain nombre de tests différents.
90. **dns-client-subnet-scan**
    Effectue une recherche de domaine à l'aide de l'option edns-client-subnet, qui permet aux clients de spécifier le sous-réseau à partir duquel les requêtes sont supposées provenir. Le script utilise cette option pour fournir un nombre d'emplacements répartis géographiquement dans le but d'énumérer autant d'enregistrements d'adresses que possible. Le script prend également en charge les demandes utilisant un sous-réseau donné.
91. **DNS-Fuzz**
    Lance une attaque par fuzzing DNS contre les serveurs DNS.
92. **dns-ip6-arpa-scan**
    Effectue une recherche DNS inversée rapide d'un réseau IPv6 à l'aide d'une technique d'analyse des codes de réponse du serveur DNS afin de réduire considérablement le nombre de requêtes nécessaires à l'énumération de réseaux étendus.
93. **dns-nsec-enum**
    Énumère les noms DNS à l'aide de la technique DNSSEC NSEC-walking.
94. **dns-nsec3-enum**
    Essaye d'énumérer les noms de domaine du serveur DNS qui prend en charge les enregistrements DNSSEC NSEC3.
95. **dns-nsid**
    Récupère les informations d'un serveur de noms DNS en demandant son ID de serveur de noms (nsid) et ses valeurs id.server et version.bind. Ce script exécute les mêmes requêtes que les deux commandes dig suivantes: – dig CH TXT bind.version @target – dig + nsid CH TXT id.server @target
96. **dns-random-srcport**
    Vérifie la vulnérabilité de récursion de port prévisible sur un serveur DNS. Des ports source prévisibles peuvent rendre un serveur DNS vulnérable aux attaques par empoisonnement du cache (voir CVE-2008-1447).
97. **dns-random-txid**
    Vérifie sur un serveur DNS la vulnérabilité de récursion DNS prévisible-TXID. Des valeurs TXID prévisibles peuvent rendre un serveur DNS vulnérable aux attaques par empoisonnement de cache (voir CVE-2008-1447).
98. **dns-récursion**
    Vérifie si un serveur DNS autorise les requêtes pour des noms tiers. Il est prévu que la récursivité sera activée sur vos propres serveurs de noms internes.
99. **dns-service-discovery**
    Tente de découvrir les services des hôtes cibles à l'aide du protocole DNS Service Discovery.
100. **dns-srv-enum**
    Énumère divers enregistrements de service commun (SRV) pour un nom de domaine donné. Les enregistrements de service contiennent le nom d'hôte, le port et la priorité des serveurs pour un service donné. Le script énumère les services suivants: – Catalogue global Active Directory – Découverte automatique Exchange – Service Kerberos KDC – Service de modification Kerberos Passwd – Serveurs LDAP – Serveurs SIP – XMPP S2S – XMPP C2S
101. **dns-update**
    Tente d'effectuer une mise à jour DNS dynamique sans authentification.
102. **dns-zeustracker**
    Vérifie si la plage d'adresses IP cible fait partie d'un réseau de zombies Zeus en interrogeant ZTDNS @ abuse.ch. Veuillez vérifier les informations suivantes avant de commencer à numériser: https://zeustracker.abuse.ch/ztdns.php
103. **dns-zone-transfer**
    Demande un transfert de zone (AXFR) à partir d'un serveur DNS.
104. **domcon-brute**
    Effectue un audit du mot de passe brutal sur la console Lotus Domino.
105. **domcon-cmd**
    Exécute une commande de console sur la console Lotus Domino à l'aide des informations d'authentification fournies (voir aussi: domcon-brute)

106. **domino-enum-users**
Tente de découvrir des utilisateurs IBM Lotus Domino valides et de télécharger leurs fichiers d'identité en exploitant la vulnérabilité CVE-2006-5835.
107. **dpap-brute**
Effectue un audit du mot de passe brute force sur une photothèque iPhoto.
108. **drda-brute**
Teste les mots de passe par rapport aux bases de données prenant en charge le protocole IBM DB2 telles que Informix, DB2 et Derby.
109. **drda-info**
Tente d'extraire des informations des serveurs de base de données prenant en charge le protocole DRDA. Le script envoie un paquet de commande DRDA EXCSAT (attributs de serveur d'échange) et analyse la réponse.
110. **eap-info**
Énumère les méthodes d'authentification offertes par un authentifiant EAP (Extensible Authentication Protocol) pour une identité donnée ou pour l'identité anonyme si aucun argument n'est transmis.
111. **enip-info**
Ce script NSE est utilisé pour envoyer un paquet EtherNet / IP à un périphérique distant avec TCP 44818 ouvert. Le script enverra un paquet d'identité de demande et une fois la réponse reçue, il confirmera qu'il s'agissait d'une réponse appropriée à la commande envoyée, puis analysera les données. Les informations analysées incluent le type de périphérique, l'ID de fournisseur, le nom du produit, le numéro de série, le code du produit, le numéro de révision, le statut, l'état et l'adresse IP du périphérique.
112. **epmd-info**
Se connecte au démon Erlang Port Mapper (epmd) et récupère une liste de nœuds avec leurs numéros de port respectifs.
113. eppc-enum-processus
Tente d'énumérer les informations de processus via le protocole Apple Remote Event. Lors de l'accès à une application via le protocole Apple Remote Event, le service répond avec l'ID utilisateur et le pid de l'application, s'il est en cours d'exécution, avant de demander l'authentification.
114. fcrdns
Effectue une recherche DNS inversée avec confirmation confirmée et signale des résultats anormaux.
115. **flume-master-info**
Récupère les informations des pages HTTP maîtres de Flume.
116. **info-renard**
Tridium Niagara Fox est un protocole utilisé par Building Automation Systems. Basé sur le travail de Billy Rios et Terry McCorkle, ce Nmap NSE collectera des informations auprès du système A Tridium Niagara.
117. **pigiste-info**
Détecte le service du serveur de jeu Freelancer (FLServer.exe) en envoyant une sonde UDP de requête de statut.
118. **ftp-anon**
Vérifie si un serveur FTP autorise les connexions anonymes.
119. **ftp-bounce**
Vérifie si un serveur FTP autorise l'analyse de port à l'aide de la méthode de report FTP.
120. **ftp-brute**
Effectue l'audit brutal du mot de passe sur les serveurs FTP.
121. **ftp-libopie**
Vérifie si un FTPd est sujet à CVE-2010-1938 (débordement de pile OPIE off-by-one), une vulnérabilité découverte par Maksymilian Arciemowicz et Adam « pi3 » Zabrocki. Voir l'avis à l' adresse https://nmap.org/r/fbsd-sa-opie . Sachez que, s'il est lancé sur un hôte vulnérable, ce script plantera FTPd.
122. **ftp-proftpd-backdoor**
Les tests de présence de la porte dérobée ProFTPD 1.3.3c sont signalés sous le nom BID 45150. Ce script tente d'exploiter la porte dérobée à l'aide de la idcommande inoffensive par défaut, mais peut être modifiée à l'aide de l' ftp-proftpd-backdoor.cmdargument de script.
123. **ftp-syst**
Envoie les commandes FTP et STAT FTP et renvoie le résultat.

124. **ftp-vsftpd-backdoor**
Tests de présence de la porte dérobée vsFTPd 2.3.4 signalé le 2011-07-04 (CVE-2011-2523). Ce script tente d'exploiter la porte dérobée à l'aide de la idcommande inoffensive par défaut, mais cela peut être modifié avec les arguments de script exploit.cmdou ftp-vsftpd-backdoor.cmd.
125. **ftp-vuln-cve2010-4221**
Recherche un dépassement de mémoire tampon basé sur une pile dans le serveur ProFTPD, version comprise entre 1.3.2rc3 et 1.3.3b. En envoyant un grand nombre de séquences d'échappement TELNET_IAC, le processus proftpd calcule mal la longueur du tampon et un attaquant distant peut corrompre la pile et exécuter du code arbitraire dans le contexte du processus proftpd (CVE-2010-4221). L'authentification n'est pas nécessaire pour exploiter cette vulnérabilité.
126. **ganglia-info**
Récupère les informations système (version du système d'exploitation, mémoire disponible, etc.) d'un démon de surveillance Ganglia à l'écoute ou d'un démon Ganglia Meta.
127. **giop-info**
Interroge un serveur de nommage CORBA pour obtenir une liste d'objets.
128. **gkrellm-info**
Demande à un service GKRellM de surveiller les informations. Un seul cycle de collecte est effectué, montrant un instantané des informations au moment de la demande.
129. **Gopher-ls**
Répertorie les fichiers et les répertoires à la racine d'un service gopher.
130. **gpsd-info**
Récupère l'heure, les coordonnées et la vitesse GPS du démon du réseau GPSD.
131. **hadoop-datanode-info**
Découvre des informations telles que les répertoires de journal à partir d'une page d'état HTTP Apache Hadoop DataNode.
132. **hadoop-jobtracker-info**
Récupère les informations d'une page d'état HTTP Apache Hadoop JobTracker.
133. **hadoop-namenode-info**
Récupère les informations d'une page d'état HTTP Apache Hadoop NameNode.
134. hadoop-secondary-namenode-info
Récupère les informations d'une page d'état HTTP du NameNode secondaire Apache Hadoop.
135. **hadoop-tasktracker-info**
Récupère les informations d'une page d'état HTTP Apache Hadoop TaskTracker.
136. **hbase-master-info**
Récupère les informations d'une page d'état HTTP maître Apache HBase (base de données Hadoop).
137. **hbase-region-info**
Récupère les informations d'une page d'état HTTP du serveur de région Apache HBase (base de données Hadoop).
138. **hddtemp-info**
Lit les informations du disque dur (telles que la marque, le modèle et parfois la température) à partir d'un service d'écoute hddtemp.
139. **hnap-info**
Récupérez les détails du matériel et les informations de configuration en utilisant HNAP, le « protocole d'administration de réseau domestique ». Il s'agit d'un protocole SOAP (HTTP-Simple Object Access Protocol) qui permet la découverte, la configuration et la gestion de la topologie à distance, ainsi que la gestion de périphériques (routeurs, caméras, PC, NAS, etc.).
140. **hostmap-bfk**
Découvre les noms d'hôte résolus en adresse IP de la cible en interrogeant la base de données en ligne à l' adresse http://www.bfk.de/bfk_dnslogger.html .
141. **hostmap-crtsh**
Recherche les sous-domaines d'un serveur Web en interrogeant la base de données de journaux de certificats en transparence de Google ( https://crt.sh ).
142. **hostmap-robtex**
Découvre les noms d'hôte résolus en adresse IP de la cible en interrogeant le service Robtex en ligne à l'adresse http://ip.robtex.com/ .

143. **http-adobe-coldfusion-apsa1301**
Tente d'exploiter une vulnérabilité liée au contournement de l'authentification sur les serveurs Adobe Coldfusion afin de récupérer un cookie de session d'administrateur valide.
144. **http-affiliate-id**
Récupère les identifiants de réseau d'affiliés (Google AdSense ou Analytics, Amazon Associates, etc.) à partir d'une page Web. Ceux-ci peuvent être utilisés pour identifier des pages avec le même propriétaire.
145. **http-apache-négociation**
Vérifie si mod_negotiation est activé sur le serveur http cible. Cette fonctionnalité peut être mise à profit pour rechercher des ressources cachées et spider un site Web en utilisant moins de demandes.
146. **http-apache-server-status**
Tente de récupérer la page d'état du serveur pour les serveurs Web Apache sur lesquels mod_status est activé. Si la page d'état du serveur existe et semble provenir de mod_status, le script analysera des informations utiles telles que la disponibilité du système, la version d'Apache et les requêtes HTTP récentes.
147. **http-aspnet-debug**
Détermine si le débogage d'une application ASP.NET est activé à l'aide d'une demande HTTP DEBUG.
148. **http-auth**
Récupère le schéma d'authentification et le domaine d'un service Web nécessitant une authentification.
149. **http-auth-finder**
Araignées un site Web pour trouver des pages Web nécessitant une authentification basée sur un formulaire ou basée sur HTTP. Les résultats sont renvoyés dans un tableau avec chaque URL et la méthode détectée.
150. **http-avaya-ipoffice-users**
Tentatives d'énumération des utilisateurs dans les systèmes Avaya IP Office 7.x.
151. **http-awstatstotals-exec**
Exploite une vulnérabilité d'exécution de code à distance dans Awstats Totals 1.0 à 1.14 et éventuellement d'autres produits qui en découlent (CVE: 2008-3922).
152. **http-axis2-dir-traversal**
Exploite une vulnérabilité de traversée de répertoire dans Apache Axis2 version 1.4.1 en envoyant une demande spécialement conçue au paramètre xsd (BID 40343). Par défaut, il tentera de récupérer le fichier de configuration du service Axis2 en '/conf/axis2.xml'utilisant le chemin '/axis2/services/'d' accès pour renvoyer le nom d'utilisateur et le mot de passe du compte admin.
153. **http-backup-finder**
Spiders un site Web et tente d'identifier les copies de sauvegarde des fichiers découverts. Pour ce faire, il demande différentes combinaisons de noms de fichiers (par exemple, index.bak, index.html ~, une copie de index.html).
154. **http-barracuda-dir-traversal**
Tente de récupérer les paramètres de configuration d'un périphérique Barracuda Networks Spam & Virus Firewall à l'aide de la vulnérabilité de traversée de répertoires décrite à l' adresse http://seclists.org/fulldisclosure/2010/Oct/119 .
155. **http-bigip-cookie**
Décode tous les cookies F5 BIG-IP non chiffrés dans la réponse HTTP. Les cookies BIG-IP contiennent des informations sur les systèmes dorsaux tels que les adresses IP internes et les numéros de port. Voir ici pour plus d'informations: https://support.f5.com/csp/article/K6917
156. **http-brute**
Effectue un audit de mot de passe brute avec l'authentification HTTP de base, Digest et NTLM.
157. **http-cakephp-version**
Obtient la version CakePHP d'une application Web construite avec le framework CakePHP en prenant les empreintes digitales des fichiers par défaut fournis avec le framework CakePHP.
158. **http-chrono**
Mesure le temps nécessaire à un site Web pour créer une page Web et renvoie le temps maximal, minimal et moyen nécessaire pour récupérer une page.

159. **http-cisco-anyconnect**
Connectez-vous en tant que client Cisco AnyConnect à un VPN SSL Cisco et récupérez les informations de version et de tunnel.
160. **http-coldfusion-subzero**
Tente de récupérer la version, le chemin absolu du panneau d'administration et le fichier 'password.properties' à partir d'installations vulnérables de ColdFusion 9 et 10.
161. **http-comments-displayer**
Extrait et génère des commentaires HTML et JavaScript à partir de réponses HTTP.
162. **http-config-backup**
Vérifie les sauvegardes et les fichiers d'échange des fichiers de configuration du système de gestion de contenu et du serveur Web courants.
163. **http-cookie-flags**
Examine les cookies définis par les services HTTP. Rapporte tous les cookies de session définis sans l'indicateur httponly. Rapporte tous les cookies de session configurés sur SSL sans l'indicateur sécurisé. Si http-enum.nse est également exécuté, tous les chemins intéressants trouvés par celui-ci seront vérifiés en plus de la racine.
164. **http-cors**
Teste sur un serveur http le partage de ressources inter-origines (CORS), une méthode permettant aux domaines de décider explicitement de faire en sorte que certaines méthodes soient appelées par un autre domaine.
165. **http-cross-domain-policy**
Vérifie le fichier de stratégie interdomaine (/crossdomain.xml) et le fichier de stratégie client-acces (/clientaccesspolicy.xml) dans les applications Web et répertorie les domaines approuvés. Des paramètres trop permissifs activent les attaques de contrefaçon de type demande multisite et peuvent permettre aux attaquants d'accéder à des données sensibles. Ce script est utile pour détecter les configurations permissives et les noms de domaine possibles disponibles à l'achat pour exploiter l'application.
166. **http-csrf**
Ce script détecte les vulnérabilités de type CSRF (Cross Site Request Forgeries).
167. **http-date**
Obtient la date des services de type HTTP. Indique également combien la date diffère de l'heure locale. L'heure locale correspond à l'heure d'envoi de la demande HTTP. La différence inclut donc au moins la durée d'un RTT.
168. **http-default-accounts**
Tests d'accès avec les informations d'identification par défaut utilisées par une variété d'applications et de périphériques Web.
169. **http-devframework**
**http-dlink-backdoor**
Détecte une porte dérobée du microprogramme sur certains routeurs D-Link en modifiant la valeur « secrète » de User-Agent. L'utilisation du « secret » User-Agent contourne l'authentification et permet à l'administrateur d'accéder au routeur.
170. **http-dombased-xss**
Il recherche les endroits où les informations contrôlées par un attaquant dans le DOM peuvent être utilisées pour affecter l'exécution de JavaScript de certaines manières. L'attaque est expliquée ici: http://www.webappsec.org/projects/articles/071105.shtml
171. **http-domino-enum-passwords**
Tente d'énumérer les mots de passe Internet Domino hachés qui sont (par défaut) accessibles à tous les utilisateurs authentifiés. Ce script peut également télécharger les fichiers d'ID Domino attachés au document Personne. Les mots de passe sont présentés sous une forme adaptée à l'exécution dans John the Ripper.
172. **http-drupal-enum**
Énumère les modules / thèmes Drupal installés en utilisant une liste de modules et de thèmes connus.
173. **http-drupal-enum-users**
Énumère les utilisateurs de Drupal en exploitant une vulnérabilité de divulgation d'informations dans Views, le module le plus populaire de Drupal.
174. **http-enum**
Énumère les répertoires utilisés par les applications et les serveurs Web populaires.
175. **http-exif-araignée**
Araignées les images d'un site à la recherche de données exif intéressantes intégrées dans

des fichiers .jpg. Affiche la marque et le modèle de l'appareil photo, la date à laquelle la photo a été prise et les informations de géolocalisation incorporées.

176. **http-favicon**
Obtient le favicon (« icône de favoris ») à partir d'une page Web et le compare à une base de données des icônes d'applications Web connues. S'il y a correspondance, le nom de l'application est imprimé; sinon, le hachage MD5 des données d'icône est imprimé.
177. **http-feed**
Ce script parcourt le site Web pour rechercher les flux rss ou atom.
178. **http-fetch**
Le script est utilisé pour récupérer les fichiers des serveurs.
179. **http-fileupload-exploiter**
Exploite les formulaires non sécurisés de téléchargement de fichiers dans les applications Web en utilisant diverses techniques, telles que la modification de l'en-tête Content-type ou la création de fichiers image valides contenant la charge utile dans le commentaire.
180. **http-forme-brute**
Effectue un audit de mot de passe brutal avec une authentification basée sur un formulaire http.
181. **http-form-fuzzer**
Effectue un fuzzing de formulaire simple contre des formulaires trouvés sur des sites Web. Essaie les chaînes et les nombres de longueur croissante et tente de déterminer si le fuzzing a réussi.
182. **http-frontpage-login**
Vérifie si les machines cibles sont vulnérables à la connexion anonyme à Frontpage.
183. générateur http
Affiche le contenu de la balise méta « générateur » d'une page Web (par défaut: /), le cas échéant.
184. **http-git**
Vérifie qu'un référentiel Git se trouve dans le document racine du site Web /.git/ ) et récupère autant d'informations de référentiel que possible, y compris la langue / la structure, les télécommandes, le dernier message de validation et la description du référentiel.
185. **http-gitweb-projects-enum**
Récupère une liste de projets Git, de propriétaires et de descriptions d'un gitweb (interface Web avec le système de contrôle de révision Git).
186. **http-google-malware**
Vérifie si les hôtes figurent sur la liste noire des suspects de logiciels malveillants et de phishing de Google. Ces listes sont constamment mises à jour et font partie du service de navigation sécurisée de Google.
187. **http-grep**
Spiders un site Web et tente de faire correspondre toutes les pages et les URL à une chaîne donnée. Les matchs sont comptés et groupés par url sous laquelle ils ont été découverts.
188. **en-têtes http**
Effectue une demande HEAD pour le dossier racine (« / ») d'un serveur Web et affiche les en-têtes HTTP renvoyés.
189. **http-hp-ilo-info**
Tente d'extraire des informations des cartes HP iLO, y compris les versions et les adresses.
190. **http-huawei-hg5xx-vuln**
Détecte les modèles de modems Huawei HG530x, HG520x, HG510x (et éventuellement d'autres …) vulnérables à une vulnérabilité liée aux informations d'identité et aux informations à distance. Il extrait également les informations d'identification PPPoE et d'autres valeurs de configuration intéressantes.
191. **http-icloud-findmyiphone**
Récupère les emplacements de tous les périphériques iOS activés « Trouvez mon iPhone » en interrogeant le service Web MobileMe (authentification requise).
192. **http-icloud-sendmsg**
Envoie un message à un périphérique iOS via le service Web Apple MobileMe. L'appareil doit être enregistré avec un identifiant Apple à l'aide de l'application Find My Iphone.
193. **http-iis-short-name-brute**
Les tentatives visant à forcer brutalement les noms de fichiers 8.3 (communément appelés noms abrégés) des fichiers et des répertoires du dossier racine des serveurs IIS vulnérables. Ce script est une implémentation du PoC « scanner de nom abrégé iis ».

194. **http-iis-webdav-vuln**
Recherche une vulnérabilité dans IIS 5.1 / 6.0 permettant aux utilisateurs arbitraires d'accéder aux dossiers WebDAV sécurisés en recherchant un dossier protégé par mot de passe et en tentant d'y accéder. Cette vulnérabilité a été corrigée dans le bulletin de sécurité Microsoft MS09-020, https://nmap.org/r/ms09-020 .
195. **http-internal-ip-divulgation**
Détermine si le serveur Web perd son adresse IP interne lors de l'envoi d'une requête HTTP / 1.0 sans en-tête d'hôte.
196. **http-joomla-brute**
Effectue un audit de mot de passe brute contre les installations du CMS Web Joomla.
197. **http-jsonp-detection**
Essaie de découvrir les points de terminaison JSONP dans les serveurs Web. Les points de terminaison JSONP peuvent être utilisés pour contourner les restrictions de politique d'origine identique dans les navigateurs Web.
198. **http-litespeed-sourcecode-download**
Exploite une vulnérabilité d'empoisonnement par octet nul dans Litespeed Web Servers 4.0.x avant 4.0.15 pour extraire le code source du script cible en envoyant une demande HTTP avec un octet nul suivi d'une extension de fichier .txt (CVE-2010-2333).
199. **http-ls**
Affiche le contenu d'une page Web « index ».
200. **http-majordomo2-dir-traversal**
Exploite une vulnérabilité de traversée de répertoire existante dans Majordomo2 pour récupérer des fichiers distants. (CVE-2011-0049).
201. **http-malware-host**
Recherche la signature des compromis de serveur connus.
202. **http-mcmp**
Vérifie si le serveur Web autorise les méthodes MCMP (Mod_cluster Management Protocol).
203. **http-method-tamper**
Tente de contourner les ressources protégées par mot de passe (statut HTTP 401) en effectuant une modification de verbe HTTP. Si aucun tableau de chemins à vérifier n'est défini, le serveur Web sera analysé et vérifié par rapport à toute ressource protégée par mot de passe trouvée.
204. **http-mobileversion-checker**
Vérifie si le site Web contient une version mobile.
205. **http-ntlm-info**
Ce script énumère les informations des services HTTP distants avec l'authentification NTLM activée.
206. **http-open-proxy**
Vérifie si un proxy HTTP est ouvert.
207. **http-open-redirect**
Araignées un site Web et tente d'identifier les redirections ouvertes. Les redirections ouvertes sont des gestionnaires qui prennent généralement une URL en tant que paramètre et répondent par une redirection HTTP (3XX) à la cible. Les risques liés aux redirections ouvertes sont décrits à l' adresse http://cwe.mitre.org/data/definitions/601.html .
208. **http-passwd**
Vérifie si un serveur Web est vulnérable à la traversée de répertoires en tentant de récupérer /etc/passwdou \boot.ini.
209. **http-phpself-xss**
Analyse un serveur Web et tente de trouver les fichiers PHP vulnérables aux scripts intersites réfléchis via la variable $_SERVER[« PHP_SELF »].
210. **http-proxy-brute**
Exécute le mot de passe brutal en devinant les serveurs proxy HTTP.
211. **http-put**
Télécharge un fichier local sur un serveur Web distant à l'aide de la méthode HTTP PUT. Vous devez spécifier le nom du fichier et le chemin de l'URL avec les arguments NSE.
212. **http-qnap-nas-info**
Tente de récupérer le modèle, la version du micrologiciel et les services activés à partir d'un périphérique QNAP Network Attached Storage (NAS).
213. **http-referer-checker**
Informations sur l'inclusion de scripts entre domaines. Les sites Web qui incluent des scripts javascript externes délèguent une partie de leur sécurité à des entités tierces.

214. **http-rfi-spider**
Analyse les serveurs Web à la recherche de vulnérabilités RFI (inclusion de fichier à distance). Il teste tous les champs de formulaire trouvés et tous les paramètres d'une URL contenant une requête.
215. **http-robots.txt**
Vérifie les entrées non autorisées /robots.txtsur un serveur Web.
216. **http-robtex-reverse-ip**
Obtient jusqu'à 100 noms DNS de transfert pour une adresse IP cible en interrogeant le service Robtex ( https://www.robtex.com/ip-lookup/ ).
217. **http-robtex-shared-ns**
Trouve jusqu'à 100 noms de domaine utilisant le même nom de serveur que la cible en interrogeant le service Robtex à l' adresse http://www.robtex.com/dns/ .
218. **http-sap-netweaver-leak**
Détecte les instances de SAP Netweaver Portal qui permettent un accès anonyme à la page de navigation de l'unité KM. Cette page contient des noms de fichiers, des utilisateurs de LDAP, etc.
219. **http-shellshock**
Tentatives d'exploitation de la vulnérabilité « shellshock » (CVE-2014-6271 et CVE-2014-7169) dans des applications Web.
220. **http-slowloris**
Teste la vulnérabilité d'un serveur Web à l'attaque Slowloris DoS en lançant une attaque Slowloris.
221. **http-slowloris-check**
Teste la vulnérabilité d'un serveur Web à l'attaque Slowloris DoS sans lancer une attaque DoS.
222. **http-sql-injection**
Spiders un serveur HTTP recherchant des URL contenant des requêtes vulnérables à une attaque par injection SQL. Il extrait également les formulaires des sites Web trouvés et tente d'identifier les champs vulnérables.
223. **http-modified-xss**
Non filtré '>' (plus grand que le signe). Une indication de la vulnérabilité XSS potentielle.
224. **http-svn-enum**
Enumère les utilisateurs d'un référentiel Subversion en examinant les journaux des derniers commits.
225. **http-svn-info**
Demande des informations à partir d'un référentiel Subversion.
226. **http-tplink-dir-traversal**
Exploite une vulnérabilité liée à la traversée de répertoires existant dans plusieurs routeurs sans fil TP-Link. Les pirates peuvent exploiter cette vulnérabilité pour lire n'importe quel fichier de configuration et de mot de passe à distance et sans authentification.
227. **http-trace**
Envoie une demande HTTP TRACE et indique si la méthode TRACE est activée. Si le débogage est activé, il renvoie les champs d'en-tête qui ont été modifiés dans la réponse.
228. **http-traceroute**
Exploite l'en-tête HTTP Max-Forwards pour détecter la présence de proxys inverses.
229. **http-trane-info**
Tentatives d'obtention d'informations à partir de périphériques Trane Tracer SC. Trane Tracer SC est un panneau de terrain intelligent permettant de communiquer avec les contrôleurs d'équipements CVC déployés dans plusieurs secteurs, y compris les installations commerciales.
230. **http-unsafe-output-escaping**
Spiders un site Web et tente d'identifier les problèmes d'échappement en sortie où le contenu est renvoyé à l'utilisateur. Ce script localise tous les paramètres? X = foo & y = bar et vérifie si les valeurs sont reflétées sur la page. S'ils sont effectivement reflétés, le script essaiera d'insérer ghz> hzx « zxc'xcv et de vérifier quels caractères (le cas échéant) ont été reflétés sur la page sans que le code HTML ne s'échappe. Cela indique la vulnérabilité potentielle XSS.
231. **http-useragent-tester**
Vérifie si l'hôte autorise plusieurs utilitaires d'analyse.

232. **http-userdir-enum**
Tente d'énumérer les noms d'utilisateurs valides sur les serveurs Web exécutés avec le module mod_userdir ou similaire activé.
233. **http-vhosts**
Recherche des noms d'hôte virtuels Web en effectuant un grand nombre de demandes HEAD sur des serveurs http à l'aide de noms d'hôte courants.
234. **http-virustotal**
Vérifie si un fichier a été déterminé comme un malware par Virustotal. Virustotal est un service qui permet d'analyser un fichier ou de vérifier une somme de contrôle par rapport à un certain nombre des principaux fournisseurs d'antivirus. Le script utilise l'API publique qui requiert une clé d'API valide et est limitée à 4 requêtes par minute.
235. **http-vlcstreamer-ls**
Se connecte à un service d'assistance VLC Streamer et répertorie le contenu du répertoire. Le service d'assistance de VLC Streamer est utilisé par l'application iOS VLC Streamer pour permettre la diffusion en continu de contenu multimédia du serveur distant au périphérique.
236. **http-vmware-path-vuln**
Vérifie la présence d'une vulnérabilité liée à la traversée du chemin dans VMWare ESX, ESXi et Server (CVE-2009-3733).
237. **http-vuln-cve2006-3392**
Exploite une vulnérabilité de divulgation de fichier dans Webmin (CVE-2006-3392)
238. **http-vuln-cve2009-3960**
Exploits cve-2009-3960 également connu sous le nom d'injection d'instance externe Adobe XML.
239. **http-vuln-cve2010-0738**
Teste si une cible JBoss est vulnérable au contournement de l'authentification de la console jmx (CVE-2010-0738).
240. **http-vuln-cve2010-2861**
Exécute une attaque de traversée de répertoire contre un serveur ColdFusion et tente de récupérer le hachage de mot de passe pour l'utilisateur administrateur. Il utilise ensuite la valeur salt (masquée dans la page Web) pour créer le hachage SHA1 HMAC dont le serveur Web a besoin pour s'authentifier en tant qu'administrateur. Vous pouvez transmettre cette valeur au serveur ColdFusion en tant qu'administrateur sans déchiffrer le hachage du mot de passe.
241. h**ttp-vuln-cve2011-3192**
Détecte une vulnérabilité de déni de service dans la manière dont le serveur Web Apache traite les demandes de plusieurs plages superposées / simples d'une page.
242. **http-vuln-cve2011-3368**
Tests de la vulnérabilité CVE-2011-3368 (contournement du proxy inverse) en mode proxy inverse du serveur Apache HTTP
243. **http-vuln-cve2013-0156**
Détecte les serveurs Ruby on Rails vulnérables à l'injection d'objets, à l'exécution de commandes à distance et aux attaques par déni de service. (CVE-2013-0156)
244. **http-vuln-cve2013-6786**
Détecte une redirection d'URL et reflète la vulnérabilité XSS dans le serveur Web Allegro RomPager. La vulnérabilité a été attribuée à CVE-2013-6786.
245. **http-vuln-cve2013-7091**
Un 0 jour a été libéré le 6 décembre 2013 par rubina119 et a été corrigé dans Zimbra 7.2.6.
246. **http-vuln-cve2014-2126**
Détecte si le dispositif Cisco ASA est vulnérable à la vulnérabilité liée à l'escalade de privilèges ASDM de Cisco ASA (CVE-2014-2126).
247. **http-vuln-cve2014-2127**
Détecte si le dispositif Cisco ASA est vulnérable à la vulnérabilité liée à l'escalade de privilèges SSL VPN Cisco ASA (CVE-2014-2127).
248. **http-vuln-cve2014-2128**
Détecte si le dispositif Cisco ASA est vulnérable à la vulnérabilité liée au contournement de l'authentification par VPN SSL de Cisco ASA (CVE-2014-2128).
249. **http-vuln-cve2014-2129**
Détecte si le dispositif Cisco ASA est vulnérable à la vulnérabilité de déni de service SIP de Cisco ASA (CVE-2014-2129).

250. **http-vuln-cve2014-3704**
Exploits CVE-2014-3704 également appelé «Drupageddon» dans Drupal. Les versions <7.32 du noyau Drupal sont connues pour être affectées.
251. **http-vuln-cve2014-8877**
Exploite une vulnérabilité d'injection de code à distance (CVE-2014-8877) dans le plug-in du gestionnaire de téléchargement WordPress CM. Les versions <= 2.0.0 sont connues pour être affectées.
252. **http-vuln-cve2015-1427**
Ce script tente de détecter une vulnérabilité, CVE-2015-1427, qui permet aux attaquants d'exploiter les fonctionnalités de cette API pour obtenir une exécution de code à distance non authentifiée.
253. **http-vuln-cve2015-1635**
Recherche une vulnérabilité d'exécution de code à distance (MS15-034) dans les systèmes Microsoft Windows (CVE2015-2015-1635).
254. **http-vuln-cve2017-1001000**
Tente de détecter une vulnérabilité d'élévation de privilèges dans WordPress 4.7.0 et 4.7.1 permettant aux utilisateurs non authentifiés d'injecter du contenu dans des publications.
255. **http-vuln-cve2017-5638**
Détecte si l'URL spécifiée est vulnérable à la vulnérabilité d'exécution de code à distance dans Apache Struts (CVE-2017-5638).
256. **http-vuln-cve2017-5689**
Détecte si un système doté de la technologie Intel Active Management est vulnérable à la vulnérabilité d'élévation de privilèges INTEL-SA-00075 (CVE2017-5689).
257. **http-vuln-cve2017-8917**
Une vulnérabilité d'injection SQL affectant Joomla! 3.7.x avant 3.7.1 permet aux utilisateurs non authentifiés d'exécuter des commandes SQL arbitraires. Cette vulnérabilité était due à un nouveau composant, com_fieldsintroduit dans la version 3.7. Ce composant est accessible au public, ce qui signifie que toute personne malveillante visitant le site pourra l'exploiter.
258. **http-vuln-misfortune-cookie**
Détecte la vulnérabilité de RomPager 4.07 Misfortune Cookie en l'exploitant en toute sécurité.
259. **http-vuln-wnr1000-creds**
Une vulnérabilité a été découverte dans WNR 1000 series qui permet à un attaquant de récupérer les informations d'identification de l'administrateur avec l'interface du routeur. Testé sur la (les) version (s) du micrologiciel: V1.0.2.60_60.0.86 (dernière version) et V1.0.2.54_60.0.82NA
260. **http-waf-detect**
Essaie de déterminer si un serveur Web est protégé par un système IPS (Intrusion Prevention System), IDS (Système de détection d'intrusion) ou WAF (Web Application Firewall) en analysant le serveur Web avec des charges utiles malveillantes et en détectant les modifications apportées au code et au corps de la réponse.
261. **http-waf-fingerprint**
Essaie de détecter la présence d'un pare-feu d'application Web, ainsi que son type et sa version.
262. **http-webdav-scan**
Un script pour détecter les installations WebDAV. Utilise les méthodes OPTIONS et PROPFIND.
263. **http-wordpress-brute**
effectue l'audit du mot de passe en force brute contre les installations de WordPress CMS / blog.
264. **http-wordpress-enum**
Énumère les thèmes et les plugins des installations WordPress. Le script peut également détecter les plugins obsolètes en comparant les numéros de version avec les informations extraites de api.wordpress.org.
265. **http-wordpress-users**
Énumère les noms d'utilisateur dans les installations de blog / CMS WordPress en exploitant une vulnérabilité de divulgation d'informations existante dans les versions 2.6, 3.1, 3.1.1, 3.1.3 et 3.2-beta2 et éventuellement d'autres.
266. **http-xssed**
Ce script effectue une recherche dans la base de données xssed.com et génère le résultat.

267. **https-redirect**
Recherchez les services HTTP qui redirigent vers le protocole HTTPS sur le même port.
268. **iax2-brute**
Effectue un audit de mot de passe brute par rapport au protocole Asterisk IAX2. La estimation échoue lorsqu'un grand nombre de tentatives est effectué en raison du nombre maximal d'appels (2048 par défaut). Si vous obtenez « ERREUR: Trop de tentatives, annulées … » après un certain temps, c'est probablement ce qui se produit. Pour éviter ce problème, essayez: – de réduire la taille de votre dictionnaire – utilisez l'option de délai brutal pour introduire un délai entre les suppositions – divisez les devinettes en morceaux et attendez un moment entre eux
269. **icap-info**
Teste une liste de noms de services ICAP connus et imprime des informations sur tous ceux qu'il détecte. Le protocole ICAP (Internet Content Adaptation Protocol) est utilisé pour étendre les serveurs proxy transparents et est généralement utilisé pour le filtrage du contenu et l'analyse antivirus.
270. **iec-identifier**
Tentatives d'identification du protocole ICS IEC 60870-5-104.
271. **ike-version**
Obtient des informations (telles que le fournisseur et le type de périphérique, le cas échéant) d'un service IKE en envoyant quatre paquets à l'hôte. Ce script teste avec le mode principal et le mode agressif et envoie plusieurs transformations par demande.
272. **imap-brute**
Effectue un audit de mot de passe brutal sur les serveurs IMAP à l'aide de l'authentification LOGIN, PLAIN, CRAM-MD5, DIGEST-MD5 ou NTLM.
273. **imap-ntlm-info**
Ce script énumère les informations des services IMAP distants avec l'authentification NTLM activée.
274. **informix-brute**
Effectue un audit du mot de passe brutal sur IBM Informix Dynamic Server.
275. **ip-geolocation-geoplugin**
Essaie d'identifier l'emplacement physique d'une adresse IP à l'aide du service Web de géolocalisation de Geoplugin ( http://www.geoplugin.com/ ). Il n'y a aucune limite sur les recherches utilisant ce service.
276. **ip-geolocation-ipinfodb**
Essaie d'identifier l'emplacement physique d'une adresse IP à l'aide du service Web de géolocalisation IPInfoDB ( http://ipinfodb.com/ip_location_api.php ).
277. **ip-geolocation-map-bing**
Ce script interroge le registre Nmap pour obtenir les coordonnées GPS des cibles stockées par les scripts de géolocalisation précédents et affiche une carte Bing de marqueurs représentant les cibles.
278. **ip-geolocation-map-google**
Ce script interroge le registre Nmap pour obtenir les coordonnées GPS des cibles stockées par les scripts de géolocalisation précédents et affiche une carte Google Map de marqueurs représentant les cibles.
279. **ip-geolocation-map-kml**
Ce script interroge le registre Nmap pour obtenir les coordonnées GPS des cibles stockées par les scripts de géolocalisation précédents et génère un fichier KML de points représentant les cibles.
280. **ip-geolocation-maxmind**
Essaie d'identifier l'emplacement physique d'une adresse IP à l'aide d'un fichier de base de données Geolocation Maxmind (disponible à l' adresse http://www.maxmind.com/app/ip-location ). Ce script prend en charge les requêtes utilisant toutes les bases de données Maxmind prises en charge par leur API, y compris les bases de données commerciales.
281. **ip-https-discover**
Vérifie si le protocole de tunneling IP sur HTTPS (IP-HTTPS) [1] est pris en charge.
282. **ipidseq**
Classifie la séquence d'identifiant IP d'un hôte (test de sensibilité à l'analyse en veille).
283. **ipmi-brute**
Effectue un audit du mot de passe brutal sur le serveur IPMI RPC.
284. **ipmi-chiffre-zéro**
Scanner de contournement avec authentification zéro et chiffrement IPMI 2.0. Ce module

identifie les systèmes compatibles IPMI 2.0 qui sont vulnérables à une vulnérabilité de contournement d'authentification via l'utilisation du chiffre zéro.

285. **ipmi-version**
Effectue la découverte d'informations IPMI via des sondes d'authentification de canal.
286. **ipv6-multicast-mld-list**
Utilise la découverte d'écouteur multidiffusion pour répertorier les adresses de multidiffusion auxquelles souscrivent les écouteurs de multidiffusion IPv6 sur la portée du lien-local. Les descriptions des adresses du registre d'espaces d'adresses de multidiffusion IANA IPv6 sont répertoriées.
287. **ipv6-node-info**
Obtient les noms d'hôte, les adresses IPv4 et IPv6 via des requêtes d'informations de nœud IPv6.
288. **ipv6-ra-flood**
Génère un flux d'annonces de routeur (RA) avec des adresses MAC source et des préfixes IPv6 aléatoires. Les ordinateurs pour lesquels la configuration automatique sans état est activée par défaut (tous les principaux systèmes d'exploitation) commenceront à calculer le suffixe IPv6 et à mettre à jour leur table de routage pour refléter l'annonce acceptée. Cela entraînera une utilisation à 100% du processeur sur Windows et les plates-formes, empêchant ainsi le traitement d'autres requêtes d'application.
289. **irc-botnet-channels**
Vérifie un serveur IRC pour les canaux qui sont couramment utilisés par les botnets malveillants.
290. **irc-brute**
Effectue un audit de mot de passe brutal sur des serveurs IRC (Internet Relay Chat).
291. **irc-info**
Recueille des informations d'un serveur IRC.
292. **irc-sasl-brute**
Effectue un audit de mot de passe brutal sur les serveurs IRC (Internet Relay Chat) prenant en charge l'authentification SASL.
293. **irc-unrealircd-backdoor**
Vérifie si un serveur IRC est en porte dérobée en exécutant une commande temporelle (ping) et en contrôlant le temps requis pour répondre.
294. **iscsi-brute**
Effectue l'audit de mot de passe brute par rapport aux cibles iSCSI.
295. **iscsi-info**
Collecte et affiche les informations des cibles iSCSI distantes.
296. **isns-info**
Répertorie les portails et les nœuds iSCSI enregistrés auprès du service de nom de stockage Internet (iSNS).
297. **jdwp-exec**
Tente d'exploiter le port de débogage distant de Java. Lorsque le port de débogage distant est ouvert, il est possible d'injecter du bytecode java et d'exécuter le code à distance. Ce script en abuse pour injecter et exécuter un fichier de classe Java qui exécute la commande shell fournie et renvoie sa sortie.
298. **jdwp-info**
Tente d'exploiter le port de débogage distant de Java. Lorsque le port de débogage distant est ouvert, il est possible d'injecter du bytecode java et d'exécuter le code à distance. Ce script injecte et exécute un fichier de classe Java qui renvoie des informations sur le système distant.
299. **jdwp-inject**
Tente d'exploiter le port de débogage distant de Java. Lorsque le port de débogage distant est ouvert, il est possible d'injecter du bytecode java et d'exécuter le code à distance. Ce script permet l'injection de fichiers de classe arbitraires.
300. **knx-gateway-découvrir**
Découvre les passerelles KNX en envoyant une demande de recherche KNX à l'adresse de multidiffusion 224.0.23.12, y compris une charge UDP avec le port de destination 3671. Les passerelles KNX répondent par une réponse de recherche KNX comprenant diverses informations sur la passerelle, telles que l'adresse KNX et les services pris en charge.
301. **knx-gateway-info**
Identifie une passerelle KNX sur le port UDP 3671 en envoyant une demande de description KNX.

302. **krb5-enum-users**
Découvre les noms d'utilisateur valides par la force brute en interrogeant les noms d'utilisateur probables sur un service Kerberos. Lorsqu'un nom d'utilisateur non valide est demandé, le serveur répond en utilisant le code d'erreur Kerberos KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN, ce qui nous permet de déterminer que le nom d'utilisateur n'est pas valide. Les noms d'utilisateur valides illicitent le TGT dans une réponse AS-REP ou l'erreur KRB5KDC_ERR_PREAUTH_REQUIRED, signalant que l'utilisateur doit effectuer une pré-authentification.
303. **ldap-brute**
Essaie de forcer brutalement l'authentification LDAP. Par défaut, il utilise les listes de nom d'utilisateur et de mot de passe intégrées. Pour utiliser vos propres listes, utilisez les arguments userdbet passdbscript.
304. **ldap-novell-getpass**
Universal Password active les stratégies de mot de passe avancées, y compris les caractères étendus dans les mots de passe, la synchronisation des mots de passe d'eDirectory vers d'autres systèmes et un mot de passe unique pour tous les accès à eDirectory.
305. l**dap-rootdse**
Récupère l'entrée DSE spécifique à la racine LDAP
306. **ldap-search**
Tente d'effectuer une recherche LDAP et renvoie toutes les correspondances.
307. **Lexmark-config**
Récupère les informations de configuration d'une imprimante Lexmark S300-S400.
308. **llmnr-resol**
Résout un nom d'hôte à l'aide du protocole LLMNR (Résolution de noms de multidiffusion de liens locaux).
309. **lltd-discovery**
Utilise le protocole Microsoft LLTD pour découvrir des hôtes sur un réseau local.
310. lu-enum
Tente d'énumérer les unités logiques (LU) des serveurs TN3270E.
311. **maxdb-info**
Récupère les informations de version et de base de données d'une base de données SAP Max DB.
312. **mcafee-epo-agent**
Vérifiez si l'agent ePO est exécuté sur le port 8081 ou sur le port identifié comme port d'agent ePO.
313. **membase-brute**
Effectue un audit de mot de passe brute contre les serveurs Couchbase Membase.
314. **membase-http-info**
Récupère les informations (nom d'hôte, système d'exploitation, durée de disponibilité, etc.) du port d'administration Web de CouchBase. Les informations récupérées par ce script ne nécessitent aucune information d'identification.
315. **memcached-info**
Récupère les informations (y compris l'architecture système, l'ID de processus et l'heure du serveur) de la mémoire distribuée mettant en cache les objets système memcached.
316. **metasploit-info**
Recueille des informations du service RPC de Metasploit. Il nécessite une paire de connexion valide. Après l'authentification, il essaie de déterminer la version de Metasploit et d'en déduire le type de système d'exploitation. Ensuite, il crée une nouvelle console et exécute quelques commandes pour obtenir des informations supplémentaires.
317. **metasploit-msgrpc-brute**
Effectue l'audit du nom d'utilisateur et du mot de passe en force brute sur l'interface msgrpc de Metasploit.
318. **metasploit-xmlrpc-brute**
Effectue un audit du mot de passe brutal sur un serveur Metasploit RPC à l'aide du protocole XMLRPC.
319. **Mikrotik-routeuros-brute**
Effectue l'audit brutal du mot de passe sur les périphériques Mikrotik RouterOS avec l'interface API RouterOS activée.
320. **mmouse-brute**
Effectue un audit de mot de passe brutal sur les serveurs RPA Tech Mobile Mouse.

321. **mmouse-exec**
Se connecte à un serveur RPA Tech Mobile Mouse, lance une application et lui envoie une séquence de clés. Toute application à laquelle l'utilisateur a accès peut être démarrée et la séquence de touches est envoyée à l'application après son démarrage.
322. **modbus-découvrir**
Énumère les identifiants d'esclave Modbus SCADA (SID) et collecte leurs informations de périphérique.
323. **mongodb-brute**
Effectue un audit de mot de passe brutal sur la base de données MongoDB.
324. **mongodb-database**
Tente d'obtenir une liste de tables à partir d'une base de données MongoDB.
325. **mongodb-info**
Tente d'obtenir des informations de construction et l'état du serveur à partir d'une base de données MongoDB.
326. **mqtt-subscribe**
Décharge le trafic de messages des courtiers MQTT.
327. **mrinfo**
Interroge les cibles sur les informations de routage multidiffusion.
328. **ms-sql-brute**
Effectue un test de mot de passe par rapport à Microsoft SQL Server (ms-sql). Fonctionne mieux en conjonction avec le broadcast-ms-sql-discoverscript.
329. **ms-sql-config**
Demande aux instances de Microsoft SQL Server (ms-sql) une liste des bases de données, des serveurs liés et des paramètres de configuration.
330. **ms-sql-dac**
Interroge le service Microsoft SQL Browser sur le port DAC (Dedicated Admin Connection) d'une instance donnée (ou de toutes) SQL Server. Le port DAC est utilisé pour se connecter à l'instance de base de données lorsque les tentatives de connexion normales échouent, par exemple lorsque le serveur est en attente, que sa mémoire est insuffisante ou dans d'autres états défectueux. De plus, le port DAC fournit à un administrateur un accès aux objets système, autrement inaccessibles via des connexions normales.
331. **ms-sql-dump-hash**
Décharge les hachages de mots de passe d'un serveur MS-SQL dans un format approprié pour le cracking par des outils tels que John-the-ripper. Pour ce faire, l'utilisateur doit disposer des privilèges de base de données appropriés.
332. **ms-sql-empty-password**
Essaie de s'authentifier auprès des serveurs Microsoft SQL en utilisant un mot de passe vide pour le compte sysadmin (sa).
333. **ms-sql-hasdbaccess**
Demande aux instances de Microsoft SQL Server (ms-sql) la liste des bases de données auxquelles un utilisateur a accès.
334. **ms-sql-info**
Tente de déterminer les informations de configuration et de version des instances de Microsoft SQL Server.
335. **ms-sql-ntlm-info**
Ce script énumère les informations des services Microsoft SQL distants avec l'authentification NTLM activée.
336. **ms-sql-query**
Exécute une requête sur Microsoft SQL Server (ms-sql).
337. **ms-sql-tables**
Demande à Microsoft SQL Server (ms-sql) une liste de tables par base de données.
338. **ms-sql-xp-cmdshell**
Tente d'exécuter une commande à l'aide du shell de commandes de Microsoft SQL Server (ms-sql).
339. **msrpc-enum**
Demande à un mappeur de points de terminaison MSRPC une liste des services mappés et affiche les informations rassemblées.
340. **mtrace**
Requêtes pour le chemin de multidiffusion d'une source à un hôte de destination.

341. **murmure-version**
Détecte le service Murmur (serveur du client de communication vocale Mumble) versions 1.2.X.
342. **mysql-audit**
Audite la configuration de la sécurité du serveur de base de données MySQL par rapport à des éléments du test de performance CIS MySQL v1.0.2 (le moteur peut être utilisé pour d'autres audits MySQL en créant des fichiers d'audit appropriés).
343. **mysql-brute**
Effectue un test de mot de passe contre MySQL.
344. **mysql-dump-hashes**
Décharge les hachages de mots de passe d'un serveur MySQL dans un format approprié pour le cracking par des outils tels que John the Ripper. Des privilèges de base de données appropriés (racine) sont requis.
345. **mysql-empty-password**
Vérifie les serveurs MySQL avec un mot de passe vide pour rootou anonymous.
346. **mysql-enum**
Effectue une énumération des utilisateurs valides sur le serveur MySQL à l'aide d'un bogue découvert et publié par Kingcope ( http://seclists.org/fulldisclosure/2012/Dec/9 ).
347. **mysql-info**
Se connecte à un serveur MySQL et imprime des informations telles que les numéros de protocole et de version, l'ID de thread, l'état, les capacités et le mot de passe.
348. **mysql-query**
Exécute une requête sur une base de données MySQL et renvoie les résultats sous forme de table.
349. **mysql-users**
Tente de répertorier tous les utilisateurs sur un serveur MySQL.
350. **mysql-variables**
Tente d'afficher toutes les variables sur un serveur MySQL.
351. **mysql-vuln-cve2012-2122**
352. **nat-pmp-info**
Obtient les routeurs IP WAN à l'aide du protocole NAT-PMP (NAT Port Mapping Protocol). Le protocole NAT-PMP est pris en charge par une large gamme de routeurs,
353. **nat-pmp-mapport**
Mappe un port WAN du routeur sur un port local du client à l'aide du protocole de mappage de port NAT (NAT-PMP).
354. **ncp-enum-users**
Récupère une liste de tous les utilisateurs eDirectory du service NCP (Novell NetWare Core Protocol).
355. **ncp-serverinfo**
Récupère les informations du serveur eDirectory (version du système d'exploitation, nom du serveur, montages, etc.) du service NCP (Novell NetWare Core Protocol).
356. **ndmp-fs-info**
Répertorie les systèmes de fichiers distants en interrogeant le périphérique distant à l'aide du protocole ndmp (Network Data Management Protocol). NDMP est un protocole destiné à transporter des données entre un périphérique NAS et le périphérique de sauvegarde
357. **ndmp-version**
Récupère les informations de version à partir du service ndmp (Network Data Management Protocol) distant. NDMP est un protocole destiné à transporter des données entre un périphérique NAS et le périphérique de sauvegarde, ce qui évite aux données de transiter par le serveur de sauvegarde.
358. **nessus-brute**
Effectue un audit de mot de passe brute contre un démon d'analyse de vulnérabilité Nessus à l'aide du protocole NTP 1.2.
359. **nessus-xmlrpc-brute**
Effectue un audit de mot de passe brute contre un démon d'analyse de vulnérabilité Nessus à l'aide du protocole XMLRPC.
360. **netbus-auth-bypass**
Vérifie si un serveur NetBus est vulnérable à une vulnérabilité de contournement d'authentification permettant un accès complet sans connaître le mot de passe.

361. **netbus-brute**
Effectue un audit de mot de passe brute avec le service de backdoor (« administration à distance ») de Netbus.
362. **netbus-info**
Ouvre une connexion à un serveur NetBus et extrait des informations sur l'hôte et le service NetBus lui-même.
363. **nexpose-brute**
Effectue l'audit de mot de passe brute avec un scanner de vulnérabilités Nexpose à l'aide de l'API 1.1.
364. **nfs-ls**
Tente d'obtenir des informations utiles sur les fichiers provenant des exportations NFS. La sortie est destinée à ressembler à la sortie de ls.
365. **nfs-showmount**
Affiche les exportations NFS, comme la showmount -ecommande.
366. **nfs-statfs**
Récupère les statistiques et les informations sur l'espace disque d'un partage NFS distant. La sortie est destinée à ressembler à la sortie de df.
367. **nje-node-brute**
Force brute du nom de noeud cible JES (Network Job Entry) NES JES z / OS.
368. **nje-pass-brute**
Entrée de travaux réseau JES z / OS (NJE) «J'enregistre» un mot de passe brutal.
369. **nntp-ntlm-info**
Ce script énumère les informations des services NNTP distants avec l'authentification NTLM activée.
370. **nping-brute**
Effectue un audit de mot de passe brutal avec un service Nping Echo.
371. **nrpe-enum**
Interroge les démons NRPE (Nagios Remote Plugin Executor) pour obtenir des informations telles que les charges moyennes, le nombre de processus, les informations utilisateur enregistrées, etc.
372. **ntp-info**
Obtient les variables de temps et de configuration d'un serveur NTP. Nous envoyons deux demandes: une demande de temps et un message de contrôle « lire les variables » (opcode 2). Sans verbosité, le script affiche l'heure et la valeur du version, processor, system, refidet les stratumvariables. Avec verbosité, toutes les variables sont affichées.
373. **ntp-monlist**
Obtient et imprime les données de contrôle d'un serveur NTP.
374. **omp2-brute**
Effectue un audit de mot de passe brute avec le gestionnaire OpenVAS à l'aide d'OMPv2.
375. **omp2-enum-cibles**
Tente de récupérer la liste des systèmes et réseaux cibles à partir d'un serveur OpenVAS Manager.
376. **omron-info**
Ce script NSE est utilisé pour envoyer un paquet FINS à un périphérique distant. Le script enverra une commande de lecture des données du contrôleur et une fois la réponse reçue, il confirmera qu'il s'agissait d'une réponse appropriée à la commande envoyée, puis analysera les données.
377. **openlookup-info**
Analyse et affiche les informations de bannière d'un serveur OpenLookup (magasin de clés de valeurs réseau).
378. **openvas-otp-brute**
Effectue un audit de mot de passe brutal avec un démon du scanner de vulnérabilités OpenVAS à l'aide du protocole OTP 1.0.
379. **openwebnet-discovery**
OpenWebNet est un protocole de communication développé par Bticino depuis 2000. Récupère les informations d'identification du périphérique et le nombre de périphériques connectés.
380. **oracle-brute**
Effectue un audit de mot de passe brutal sur les serveurs Oracle.
381. **oracle-enum-users**
Tentatives d'énumération de noms d'utilisateur Oracle valides sur des serveurs Oracle 11g

non corrigés (ce bogue a été corrigé dans la mise à jour de correctif critique d'octobre 2009 d'Oracle).

382. **oracle-sid-brute**
Devine les noms d'instance / SID Oracle par rapport au TNS-listener.
383. **oracle-tns-version**
Décode le numéro de version de VSNNUM à partir d'un écouteur Oracle TNS.
384. **ovs-agent-version**
Détecte la version d'un agent Oracle Virtual Server en prenant les empreintes digitales des réponses à une demande HTTP GET et à un appel de méthode XML-RPC.
385. **p2p-conficker**
Vérifie si un hôte est infecté par Conficker.C ou supérieur, en fonction de la communication poste à poste de Conficker.
386. **chemin-mtu**
Effectue une découverte MTU par chemin simple pour cibler des hôtes.
387. **pcanywhere-brute**
Effectue un audit du mot de passe brute force par rapport au protocole d'accès à distance pcAnywhere.
388. **pcworx-info**
Ce script NSE interroge et analyse le protocole pcworx sur un automate distant. Le script enverra un paquet de requête initial et une fois la réponse reçue, il confirmera qu'il s'agissait d'une réponse appropriée à la commande envoyée, puis analysera les données. PCWorx est un protocole et programme de Phoenix Contact.
389. **pgsql-brute**
Effectue un test de mot de passe par rapport à PostgreSQL.
390. **pjl-ready-message**
Récupère ou définit le message prêt sur les imprimantes prenant en charge le langage de travail d'imprimante. Cela inclut la plupart des imprimantes PostScript qui écoutent sur le port 9100. Sans argument, affiche le message Prêt actuel. Avec l' pjl_ready_messageargument de script, affiche l'ancien message Ready et le remplace par le message donné.
391. **pop3-brute**
Essaie de se connecter à un compte POP3 en devinant les noms d'utilisateur et les mots de passe.
392. **pop3-ntlm-info**
Ce script énumère les informations des services POP3 distants avec l'authentification NTLM activée.
393. **pptp-version**
Tente d'extraire les informations système du service PPTP (tunneling tunneling) point à point.
394. **qconn-exec**
Essaie de déterminer si un démon QNX QCONN en écoute permet aux utilisateurs non authentifiés d'exécuter des commandes arbitraires du système d'exploitation.
395. **qscan**
Sondez de manière répétée les ports ouverts et / ou fermés sur un hôte pour obtenir une série de valeurs de temps d'aller-retour pour chaque port. Ces valeurs permettent de regrouper des collections de ports statistiquement différents des autres groupes. Les ports appartenant à différents groupes (ou « familles ») peuvent être dus à des mécanismes de réseau tels que le transfert de port vers des machines situées derrière un NAT.
396. **quake1-info**
Extrait les informations des serveurs de jeux Quake et d'autres serveurs de jeux utilisant le même protocole.
397. **quake3-info**
Extrait des informations d'un serveur de jeux Quake3 et d'autres jeux utilisant le même protocole.
398. **quake3-master-getservers**
Requêtes Serveurs maîtres de style Quake3 pour serveurs de jeux (beaucoup de jeux autres que Quake 3 utilisent ce même protocole).
399. **rdp-enum-encryption**
Détermine la couche de sécurité et le niveau de chiffrement pris en charge par le service RDP. Il le fait en parcourant tous les protocoles et les chiffrements existants. Lorsqu'il est

exécuté en mode débogage, le script renvoie également les protocoles et les chiffrements qui échouent, ainsi que toutes les erreurs signalées.

400. **rdp-ntlm-info**
Ce script énumère les informations des services RDP distants avec l'authentification CredSSP (NLA) activée.
401. **rdp-vuln-ms12-020**
Vérifie si une machine est vulnérable à la vulnérabilité MS12-020 RDP.
402. **realvnc-auth-bypass**
Vérifie si un serveur VNC est vulnérable au contournement de l'authentification RealVNC (CVE-2006-2369).
403. **redis-brute**
Effectue l'audit des mots de passe en force brute sur un magasin de clés-valeurs Redis.
404. **redis-info**
Récupère les informations (telles que le numéro de version et l'architecture) d'un magasin de clés-valeurs Redis.
405. **rexec-brute**
Effectue un audit de mot de passe brute avec le service classique UNIX rexec (Remote exec).
406. **riak-http-info**
Récupère des informations (telles que le nom du noeud et l'architecture) d'une base de données distribuée Basho Riak à l'aide du protocole HTTP.
407. **rlogin-brute**
Effectue un audit de mot de passe brute avec le service classique UNIX rlogin (connexion à distance). Ce script doit être exécuté en mode privilégié sous UNIX car il doit être lié à un numéro de port source faible.
408. **rmi-dumpregistry**
Se connecte à un registre RMI distant et tente de vider tous ses objets.
409. **rmi-vuln-classloader**
Teste si Java rmiregistry autorise le chargement de classe. La configuration par défaut de rmiregistry permet de charger des classes à partir d'URL distantes, ce qui peut entraîner l'exécution de code à distance. Le fournisseur (Oracle / Sun) considère cela comme une fonctionnalité de conception.
410. **rpc-grind**
Empreintes digitales sur le port RPC cible pour extraire le service cible, le numéro RPC et la version.
411. **rpcap-brute**
Effectue un audit de mot de passe brutal avec le démon de capture distant WinPcap (rpcap).
412. **rpcap-info**
Se connecte au service rpcap (fournit des fonctionnalités de détection à distance via WinPcap) et récupère les informations d'interface. Le service peut être configuré pour exiger une authentification ou non et prend également en charge les restrictions IP.
413. **rpcinfo**
Se connecte à portmapper et récupère une liste de tous les programmes enregistrés. Il imprime ensuite une table comprenant (pour chaque programme) le numéro de programme RPC, les numéros de version pris en charge, le numéro de port et le protocole, ainsi que le nom du programme.
414. **rsa-vuln-roca**
Détecte les clés RSA vulnérables à la factorisation ROCA (Return Of Coppersmith Attack).
415. **rsync-brute**
Effectue un audit de mot de passe brute avec le protocole de synchronisation de fichiers distants rsync.
416. **rsync-list-modules**
Répertorie les modules disponibles pour la synchronisation rsync (synchronisation de fichier à distance).
417. **rtsp-url-brute**
Tente d'énumérer les URL de média RTSP en testant les chemins d'accès communs sur des périphériques tels que les caméras de surveillance IP.
418. **rusers**
Se connecte au service RPC de rusersd et récupère une liste des utilisateurs connectés.
419. **s7-info**
Énumère les périphériques automates Siemens S7 et collecte leurs informations de

périphérique. Ce script est basé sur PLCScan développé par Positive Research et Scadastrangelove ( https://code.google.com/p/plcscan/ ). Ce script est censé fournir les mêmes fonctionnalités que PLCScan dans Nmap. Certaines des informations collectées par PLCScan n'ont pas été transférées; ces informations peuvent être analysées à partir des paquets reçus.

420. **samba-vuln-cve-2012-1182**
Vérifie si les machines cibles sont vulnérables à la vulnérabilité de débordement de tas dans Samba CVE-2012-1182.
421. **sip-brute**
Effectue un audit de mot de passe brutal sur les comptes SIP (Session Initiation Protocol). Ce protocole est le plus souvent associé aux sessions VoIP.
422. **sip-call-spoof**
Spoofs un appel vers un téléphone SIP et détecte l'action entreprise par la cible (occupé, refusé, raccroché, etc.)
423. **sip-enum-users**
Énumère les extensions valides d'un serveur SIP (utilisateurs).
424. **smb-brute**
Essaie de deviner les combinaisons nom d'utilisateur / mot de passe sur SMB, en stockant les combinaisons découvertes à utiliser dans d'autres scripts. Tous les efforts seront faits pour obtenir une liste d'utilisateurs valides et vérifier chaque nom d'utilisateur avant de les utiliser. Lorsqu'un nom d'utilisateur est découvert, en plus d'être imprimé, il est également enregistré dans le registre Nmap afin que les autres scripts Nmap puissent l'utiliser. Cela signifie que si vous voulez exécuter smb-brute.nse, vous devez exécuter les autres smbscripts de votre choix. Cela vérifie les mots de passe sans tenir compte de la casse, en déterminant la casse après la découverte d'un mot de passe, pour les versions de Windows antérieures à Vista.
425. **smb-double-pulsar-backdoor**
Vérifie si la machine cible exécute la porte dérobée Double Pulsar SMB.
426. **smb-enum-domain**
Tentatives d'énumérer les domaines d'un système, ainsi que leurs stratégies. Cela nécessite généralement des informations d'identification, à l'exception de Windows 2000. En plus du domaine réel, le domaine « Intégré » est généralement affiché. Windows renvoie cela dans la liste des domaines, mais ses stratégies ne semblent pas être utilisées nulle part.
427. **smb-enum-groups**
Obtient une liste des groupes du système Windows distant, ainsi qu'une liste des utilisateurs du groupe. Cela fonctionne de la même manière enum.exequ'avec le /Gcommutateur.
428. **smb-enum-processus**
Extrait une liste de processus du serveur distant via SMB. Cela déterminera tous les processus en cours d'exécution, leurs ID de processus et leurs processus parents. Cela se fait en interrogeant le service de registre distant, qui est désactivé par défaut sous Vista; sur toutes les autres versions de Windows, il nécessite des privilèges d'administrateur.
429. **smb-enum-services**
Récupère la liste des services en cours d'exécution sur un système Windows distant. Chaque attribut de service contient le nom du service, le nom d'affichage et l'état du service de chaque service.
430. **smb-enum-sessions**
Énumère les utilisateurs connectés à un système localement ou via un partage SMB. Les utilisateurs locaux peuvent être connectés physiquement sur la machine ou via une session de services de terminal. Les connexions à un partage SMB sont, par exemple, des personnes connectées à des fichiers ou à des appels RPC. La connexion de Nmap apparaîtra également et est généralement identifiée par celle qui s'est connectée « il y a 0 seconde ».
431. **smb-enum-shares**
Tente de répertorier les partages à l'aide de la srvsvc.NetShareEnumAllfonction MSRPC et d'extraire plus d'informations à leur sujet à l'aide de srvsvc.NetShareGetInfo. Si l'accès à ces fonctions est refusé, une liste de noms de partage courants est vérifiée.
432. **smb-enum-users**
Tentatives d'énumération des utilisateurs d'un système Windows distant, avec le plus d'informations possible, selon deux techniques différentes (à la fois sur MSRPC, qui utilise les ports 445 ou 139; voir smb.lua). Le but de ce script est de découvrir tous les comptes d'utilisateurs existant sur un système distant. Cela peut être utile pour l'administration, car

elle permet de voir qui a un compte sur un serveur, ou pour les tests d'intrusion ou l'empreinte réseau, en déterminant quels comptes existent sur un système.

433. **smb-flood**
Épuise la limite de connexion d'un serveur SMB distant en ouvrant autant de connexions que possible. La plupart des implémentations de SMB ont une limite globale stricte de 11 connexions pour les comptes d'utilisateurs et de 10 connexions pour les connexions anonymes. Une fois cette limite atteinte, les connexions supplémentaires sont refusées. Ce script exploite cette limite en prenant toutes les connexions et en les maintenant.
434. **smb-ls**
Tente de récupérer des informations utiles sur les fichiers partagés sur des volumes SMB. La sortie est destinée à ressembler à la sortie de la lscommande UNIX .
435. **smb-mbenum**
Requiert des informations gérées par le Windows Master Browser.
436. **smb-os-decouverte**
Tente de déterminer le système d'exploitation, le nom de l'ordinateur, le domaine, le groupe de travail et l'heure actuelle via le protocole SMB (ports 445 ou 139). Pour ce faire, vous démarrez une session avec le compte anonyme (ou avec un compte d'utilisateur approprié, le cas échéant; cela ne fera probablement aucune différence); en réponse au démarrage d'une session, le serveur renvoie toutes ces informations.
437. **smb-print-text**
Tente d'imprimer du texte sur une imprimante partagée en appelant les fonctions RPC du service Spouleur d'impression.
438. **smb-psexec**
Implémente une exécution de processus à distance similaire à l'outil psexec de Sysinternals, permettant à un utilisateur d'exécuter une série de programmes sur une machine distante et de lire le résultat. C'est idéal pour collecter des informations sur les serveurs, exécuter le même outil sur plusieurs systèmes ou même installer une porte dérobée sur un ensemble d'ordinateurs.
439. **smb-security-mode**
Renvoie des informations sur le niveau de sécurité SMB déterminé par SMB.
440. **smb-server-stats**
Essaie de récupérer les statistiques du serveur sur SMB et MSRPC, qui utilise les ports TCP 445 ou 139.
441. **smb-system-info**
Extrait les informations sur le système distant du registre. L'obtention de toutes les informations nécessite un compte administratif, bien qu'un compte utilisateur en obtienne toujours beaucoup. Invité ne sera probablement pas obtenir, ni anonyme. Cela vaut pour tous les systèmes d'exploitation, y compris Windows 2000.
442. **smb-vuln-conficker**
Détecte les systèmes Microsoft Windows infectés par le ver Conficker. Cette vérification est dangereuse et peut entraîner une panne des systèmes.
443. **smb-vuln-cve-2017-7494**
Vérifie si les ordinateurs cibles sont vulnérables à la vulnérabilité de chargement de bibliothèque partagée arbitraire CVE-2017-7494.
444. **smb-vuln-cve2009-3103**
Détecte les systèmes Microsoft Windows vulnérables au déni de service (CVE-2009-3103). Ce script plantera le service s'il est vulnérable.
445. **smb-vuln-ms06-025**
Détecte les systèmes Microsoft Windows avec le service Ras RPC vulnérable à MS06-025.
446. **smb-vuln-ms07-029**
Détecte les systèmes Microsoft Windows avec Dns Server RPC vulnérables à MS07-029.
447. **smb-vuln-ms08-067**
Détecte les systèmes Microsoft Windows vulnérables à la vulnérabilité d'exécution de code à distance connue sous le nom de MS08-067. Cette vérification est dangereuse et peut entraîner une panne des systèmes.
448. **smb-vuln-ms10-054**
Teste si les ordinateurs cibles sont vulnérables à la vulnérabilité de corruption de la mémoire distante ms10-054 SMB.
449. **smb-vuln-ms10-061**
Teste si les ordinateurs cibles sont vulnérables à la vulnérabilité d'usurpation d'identité du spouleur d'imprimante ms10-061.

450. **smb-vuln-ms17-010**
Tente de détecter si un serveur Microsoft SMBv1 est vulnérable à une vulnérabilité d'exécution de code à distance (ms17-010, aussi appelée EternalBlue). La vulnérabilité est activement exploitée par WannaCry et Petya ransomware et autres logiciels malveillants.
451. **smb-vuln-regsvc-dos**
Vérifie si un système Microsoft Windows 2000 est vulnérable à un blocage de regsvc causé par une déréférence de pointeur null. Cette vérification va bloquer le service s'il est vulnérable et nécessite un compte invité ou plus pour fonctionner.
452. **smb-vuln-webexec**
Une vulnérabilité critique d'exécution de code à distance existe dans WebExService (WebExec).
453. **smb-webexec-exploit**
Tente d'exécuter une commande via WebExService, à l'aide de la vulnérabilité WebExec. Avec un compte Windows (local ou domaine), cela lancera un exécutable arbitraire avec des privilèges SYSTEM sur le protocole SMB.
454. **smb2-capacités**
Tente de répertorier les fonctionnalités prises en charge sur un serveur SMBv2 pour chaque dialecte activé.
455. **smb2-security-mode**
Détermine la configuration de la signature de message dans les serveurs SMBv2 pour tous les dialectes pris en charge.
456. **smb2-fois**
Tente d'obtenir la date système actuelle et la date de début d'un serveur SMB2.
457. **smb2-vuln-uptime**
Tente de détecter les correctifs manquants sur les systèmes Windows en vérifiant le temps de disponibilité retourné lors de la négociation du protocole SMB2.
458. **smtp-brute**
Effectue un audit de mot de passe brutal sur les serveurs SMTP à l'aide de l'authentification LOGIN, PLAIN, CRAM-MD5, DIGEST-MD5 ou NTLM.
459. **smtp-enum-users**
Tente d'énumérer les utilisateurs sur un serveur SMTP en émettant les commandes VRFY, EXPN ou RCPT TO. Le but de ce script est de découvrir tous les comptes d'utilisateurs du système distant.
460. **smtp-ntlm-info**
Ce script énumère les informations des services SMTP distants avec l'authentification NTLM activée.
461. **smtp-open-relay**
Tente de relayer le courrier en émettant une combinaison prédéfinie de commandes SMTP. Ce script a pour objectif de déterminer si un serveur SMTP est vulnérable au relais de messagerie.
462. **smtp-strangeport**
Vérifie si SMTP s'exécute sur un port non standard.
463. **smtp-vuln-cve2010-4344**
Vérifie et / ou exploite un débordement de tas dans les versions d'Exim antérieures à la version 4.69 (CVE-2010-4344) et une vulnérabilité d'élévation de privilèges dans Exim 4.72 et versions antérieures (CVE-2010-4345).
464. **smtp-vuln-cve2011-1720**
Recherche une corruption de mémoire sur le serveur SMTP Postfix lorsqu'il utilise les mécanismes d'authentification de la bibliothèque Cyrus SASL (CVE-2011-1720). Cette vulnérabilité peut permettre un déni de service et éventuellement l'exécution de code à distance.
465. **smtp-vuln-cve2011-1764**
Recherche une vulnérabilité de chaîne de format dans le serveur SMTP Exim (versions 4.70 à 4.75) avec prise en charge de DKIM (DomainKeys Identified Mail) (CVE-2011-1764). Le mécanisme de journalisation DKIM n'utilisait pas de spécificateurs de chaîne de format lors de la journalisation de certaines parties du champ d'en-tête DKIM-Signature. Un attaquant distant capable d'envoyer des emails peut exploiter cette vulnérabilité et exécuter du code arbitraire avec les privilèges du démon Exim.
466. **snmp-brute**
Essaie de trouver une chaîne de communauté SNMP en utilisant une force brute.

467. **snmp-hh3c-logins**
Tentatives d'énumération des utilisateurs définis localement dans Huawei / HP / H3C via l'OID hh3c-user.mib
468. **snmp-info**
Extrait les informations de base d'une requête SNMPv3 GET. La même sonde est utilisée ici que dans l'analyse de détection de version de service.
469. **snmp-ios-config**
Essaie de télécharger les fichiers de configuration IOS du routeur Cisco à l'aide de SNMP RW (v1) et de les afficher ou de les enregistrer.
470. **snmp-netstat**
Tente d'interroger SNMP pour obtenir un résultat de type netstat. Le script peut être utilisé pour identifier et ajouter automatiquement de nouvelles cibles à l'analyse en fournissant l'argument de script newtargets.
471. **snmp-sysdescr**
Tente d'extraire les informations système d'un service SNMP version 1.
472. **snmp-win32-services**
Tentatives d'énumérer les services Windows via SNMP.
473. **snmp-win32-shares**
Tente d'énumérer les partages Windows via SNMP.
474. **logiciel snmp-win32**
Tente d'énumérer les logiciels installés via SNMP.
475. **snmp-win32-utilisateurs**
Tentatives d'énumérer les comptes d'utilisateur Windows via SNMP
476. **chaussettes-auth-info**
Détermine les mécanismes d'authentification pris en charge d'un serveur proxy SOCKS distant. À partir de la version 5 de SOCKS, les serveurs chaussettes peuvent prendre en charge l'authentification. Le script recherche les types d'authentification suivants: 0 – Aucune authentification 1 – GSSAPI 2 – Nom d'utilisateur et mot de passe
477. **chaussettes-brute**
Effectue l'audit brutal du mot de passe sur les serveurs proxy SOCKS 5.
478. **chaussettes-open-proxy**
Vérifie si un proxy socks ouvert est en cours d'exécution sur la cible.
479. **ssh-auth-method**
Renvoie les méthodes d'authentification prises en charge par un serveur SSH.
480. **ssh-brute**
Exécute le mot de passe brute en essayant de deviner par rapport aux serveurs ssh
481. **ssh-hostkey**
Affiche les clés d'hôte SSH.
482. **ssh-publickey-acceptation**
Ce script utilise une table de chemins d'accès aux clés privées, aux phrases secrètes et aux noms d'utilisateur, et vérifie chaque paire pour voir si le serveur ssh cible les accepte pour l'authentification publique. Si aucune clé n'est fournie ou si l'option not-bad est spécifiée, le script vérifie si une liste de clés publiques statiques connues est acceptée pour l'authentification.
483. **ssh-run**
Exécute la commande à distance sur le serveur ssh et renvoie le résultat de la commande.
484. ssh2-enum-algos
Indique le nombre d'algorithmes (de cryptage, de compression, etc.) proposés par le serveur SSH2 cible. Si la verbosité est définie, les algorithmes proposés sont listés par type.
485. **sshv1**
Vérifie si un serveur SSH prend en charge la version 1 du protocole SSH obsolète et moins sécurisé.
486. **ssl-ccs-injection**
Détecte si un serveur est vulnérable à la vulnérabilité SSL / TLS « CCS Injection » (CVE-2014-0224), découverte pour la première fois par Masashi Kikuchi. Le script est basé sur le code ccsinjection.c rédigé par Ramon de C Valle ( https://gist.github.com/rcvalle/71f4b027d61a78c42607 ).
487. **ssl-cert**
Récupère le certificat SSL d'un serveur. La quantité d'informations imprimées sur le certificat dépend du niveau de verbosité. Sans plus de verbosité, le script imprime la période de

validité ainsi que le commonName, le nom d'organisation, le stateOrProvinceName et le nom de pays du sujet.

488. **ssl-cert-intaddr**
Signale toutes les adresses IPv4 privées (RFC1918) trouvées dans les différents champs du certificat d'un service SSL. Celles-ci ne seront signalées que si l'adresse cible elle-même n'est pas privée. Nmap v7.30 ou version ultérieure est requis.
489. **ssl-date**
Récupère l'heure et la date d'un hôte cible de sa réponse TLS ServerHello.
490. **ssl-dh-params**
Détection de paramètres Diffie-Hellman éphémère faible pour les services SSL / TLS.
491. **ssl-enum-ciphers**
Ce script initie à plusieurs reprises les connexions SSLv3 / TLS, chaque fois qu'il essaie un nouveau chiffrement ou un nouveau compresseur tout en enregistrant si un hôte l'accepte ou le refuse. Le résultat final est une liste de toutes les suites de chiffrement et de compresseurs acceptés par un serveur.
492. **ssl-heartbleed**
Détecte si un serveur est vulnérable au bogue OpenSSL Heartbleed (CVE-2014-0160). Le code est basé sur le script Python ssltest.py écrit par Jared Stafford (jspenguin@jspenguin.org).
493. **ssl-caniche**
Vérifie si les chiffrements SSLv3 CBC sont autorisés (POODLE)
494. **sslv2**
Détermine si le serveur prend en charge SSLv2 obsolète et moins sécurisé, et identifie les chiffrements pris en charge.
495. **sslv2-noyé**
Détermine si le serveur prend en charge SSLv2, quels types de chiffrement il prend en charge et teste pour CVE-2015-3197, CVE-2016-0703 et CVE-2016-0800 (DROWN).
496. **sstp-découvrir**
Vérifiez si le protocole Secure Socket Tunneling est pris en charge. Pour ce faire, essayez d'établir la couche HTTPS utilisée pour transporter le trafic SSTP, comme indiqué dans: – http://msdn.microsoft.com/en-us/library/cc247364.aspx
497. **stun-info**
Récupère l'adresse IP externe d'un hôte NAT: ed à l'aide du protocole STUN.
498. **stuxnet-detect**
Détecte si un hôte est infecté par le ver Stuxnet ( http://en.wikipedia.org/wiki/Stuxnet ).
499. **supermicro-ipmi-conf**
Tente de télécharger un fichier de configuration non protégé contenant les informations d'identification utilisateur en texte brut dans les contrôleurs vulnérables Supermicro Onboard IPMI.
500. **svn-brute**
Effectue un audit de mot de passe brutal sur les serveurs de contrôle de code source Subversion.
501. **objectifs-asn**
Produit une liste de préfixes IP pour un numéro AS d'acheminement donné (ASN).
502. **cibles-ipv6-map4to6**
Ce script s'exécute pendant la phase de pré-analyse pour mapper des adresses IPv4 sur des réseaux IPv6 et les ajouter à la file d'attente d'analyse.
503. **cibles-ipv6-multicast-echo**
Envoie un paquet de requête d'écho ICMPv6 à l'adresse de multidiffusion locale du lien – tous les nœuds ( ff02::1) pour découvrir les hôtes réactifs sur un réseau local sans qu'il soit nécessaire d' envoyer une requête ping à chaque adresse IPv6.
504. **cibles-ipv6-multicast-invalid-dst**
Envoie un paquet ICMPv6 avec un en-tête d'extension non valide à l'adresse de multidiffusion locale de lien tout-nœuds ( ff02::1) pour découvrir (certains) hôtes disponibles sur le réseau local. Cela fonctionne parce que certains hôtes vont répondre à cette sonde avec un paquet ICMPv6 Parameter Problem.
505. **cibles-ipv6-multicast-mld**
Tente de découvrir les hôtes IPv6 disponibles sur le réseau local en envoyant une requête MLD (découverte du programme d'écoute de multidiffusion) à l'adresse de multidiffusion du lien local (ff02 :: 1) et en écoutant les réponses éventuelles. Le délai de réponse maximal de

la requête est défini sur 1 pour inciter les hôtes à répondre immédiatement au lieu d'attendre les autres réponses de leur groupe de multidiffusion.

506. **cibles-ipv6-multicast-slaac**
Effectue la découverte d'hôte IPv6 en déclenchant la configuration automatique d'adresse sans état (SLAAC).
507. **target-ipv6-wordlist**
Ajoute des adresses IPv6 à la file d'attente d'analyse en utilisant une liste de mots « mots » hexadécimaux qui forment des adresses dans un sous-réseau donné.
508. **cibles-renifleur**
Renifle le réseau local pendant une durée configurable (10 secondes par défaut) et imprime les adresses découvertes. Si l' newtargetsargument de script est défini, les adresses découvertes sont ajoutées à la file d'attente d'analyse.
509. **cibles-traceroute**
Insère les sauts de traceroute dans la file d'analyse Nmap. Cela ne fonctionne que si l' –traceroutеoption de Nmap est utilisée et que l' newtargets argument de script est donné.
510. **objectifs-xml**
Charge les adresses d'un fichier de sortie XML Nmap pour la numérisation..
511. **telnet-brute**
Effectue un audit de mot de passe brute contre les serveurs telnet.
512. **telnet-ntlm-info**
Ce script énumère les informations des services Microsoft Telnet distants avec l'authentification NTLM activée.
513. **tftp-enum**
Énumère les noms de fichiers TFTP (protocole de transfert de fichiers trivial) en recherchant une liste des noms courants.
514. **tls-alpn**
Énumère les protocoles de couche d'application pris en charge par un serveur TLS à l'aide du protocole ALPN.
515. **tls-nextprotoneg**
Énumère les protocoles pris en charge d'un serveur TLS à l'aide de l'extension de négociation de protocole suivante.
516. **tls-ticketbleed**
Détecte si un serveur est vulnérable au bogue F5 Ticketbleed (CVE-2016-9244).
517. **tn3270-screen**
Se connecte à un « serveur » tn3270 et renvoie l'écran.
518. **traceroute-géolocalisation**
Répertorie les emplacements géographiques de chaque saut dans un traceroute et enregistre éventuellement les résultats dans un fichier KML, traçable sur Google Earth et sur des cartes.
519. **tso-brute**
Compte TSO brute forcer.
520. **tso-enum**
Enumérateur d'ID utilisateur TSO pour les grands systèmes IBM (z / OS). Le panneau d'ouverture de session TSO vous indique quand un ID utilisateur est valide ou non valide avec le message: IKJ56420I Userid not authorized to use TSO.
521. **ubiquiti-découverte**
Extrait les informations des périphériques réseau Ubiquiti.
522. **upnp-info**
Tente d'extraire les informations système du service UPnP.
523. **url-snarf**
Renifle une interface pour le trafic HTTP et vide toutes les URL et leur adresse IP d'origine. La sortie du script diffère des autres scripts car les URL sont écrites directement sur stdout. Il existe également une option pour enregistrer les résultats dans un fichier.
524. **ventrilo-info**
Détecte les versions de service du serveur de communication vocale Ventrilo 2.1.2 et supérieures et tente de déterminer les informations de version et de configuration. Certaines des versions plus anciennes (antérieures à la version 3.0.0) peuvent ne pas activer le service UDP sur lequel repose cette sonde par défaut.
525. **versant-info**
Extrait les informations, y compris les chemins de fichier, la version et les noms de base de données d'une base de données d'objet Versant.

526. **vmauthd-brute**
Effectue un audit du mot de passe brutal sur le démon d'authentification VMWare (vmware-authd).
527. **vmware-version**
Interroge l'API SOAP du serveur VMware (vCenter, ESX, ESXi) pour extraire les informations de version.
528. **vnc-brute**
Effectue un audit de mot de passe brutal sur les serveurs VNC.
529. **vnc-info**
Interroge un serveur VNC sur sa version de protocole et les types de sécurité pris en charge.
530. **vnc-title**
Essaie de se connecter à un serveur VNC et d'obtenir son nom de bureau. Utilise les informations d'identification découvertes par les types d'authentification vnc-brute ou None. Si a realvnc-auth-bypassété exécuté et renvoyé VULNERABLE, ce script utilisera cette vulnérabilité pour contourner l'authentification.
531. **voldemort-info**
Récupère le cluster et stocke les informations du magasin de clés-valeurs distribué Voldemort à l'aide du protocole natif Voldemort.
532. **vtam-enum**
De nombreux ordinateurs centraux utilisent des écrans VTAM pour se connecter à diverses applications (CICS, IMS, TSO, etc.).
533. **vulners**
Pour chaque CPE disponible, le script imprime des références connues (liens vers les informations correspondantes) et les scores CVSS correspondants.
534. **vuze-dht-info**
Récupère certaines informations de base, y compris la version du protocole d'un nœud de partage de fichiers Vuze.
535. **wdb-version**
Détecte les vulnérabilités et rassemble des informations (telles que les numéros de version et le support matériel) à partir des agents VxWorks Wind DeBug.
536. **weblogic-t3-info**
Détecter le protocole TMI R3 et la version de Weblogic
537. **whois-domain**
Tente de récupérer des informations sur le nom de domaine de la cible
538. **whois-ip**
Interroge les services WHOIS des registres Internet régionaux (RIR) et tente de récupérer des informations sur l'attribution d'adresse IP contenant l'adresse IP cible.
539. **WSDD-découvrir**
Récupère et affiche les informations des périphériques prenant en charge le protocole Web Services Dynamic Discovery (WS-Discovery). Il tente également de localiser tous les services Web publiés Windows Communication Framework (WCF) (.NET 4.0 ou version ultérieure).
540. **xdmcp-découvrir**
Demande une session XDMCP (protocole de contrôle du gestionnaire d'affichage X) et répertorie les mécanismes d'authentification et d'autorisation pris en charge.
541. **xmpp-brute**
Effectue un audit de mot de passe brutal sur les serveurs de messagerie instantanée XMPP (Jabber).
542. **xmpp-info**
Se connecte au serveur XMPP (port 5222) et collecte des informations sur le serveur, telles que: mécanismes d'authentification pris en charge, méthodes de compression, si TLS est pris en charge ou non, gestion de flux, langue, prise en charge de l'enregistrement intrabande, capacités du serveur. Si possible, étudie le fournisseur de serveur.