

Pour commencer on nous demande ce que signifie "SMB" pour cela petite recherche Google.

TÂCHE 1

Que signifie l'acronyme à 3 lettres SMB ?

\*\*\*\*\* \*\*\*\*\* \*\*\*\*\*k

ENVOYER UNE RÉPONSE

INDICE

Google

que signifie SMB

Tous Vidéos Images Actualités Livres Web Finance Outils

En SMS Français Militaire Informatique

Les protocoles **Server Message Block** (SMB) et Network File System (NFS) fonctionnent tous deux selon un modèle client-serveur, dans lequel les fichiers sont partagés sur le serveur distant et utilisés par le client local.

On peut donc voir que l'acronyme "SMB" signifie Server Message Block on peut donc répondre à la question.

On nous demande ensuite quel port utilise "SMB"

TÂCHE 2

Quel port SMB utilise-t-il pour opérer ?

\*\*\*

ENVOYER UNE RÉPONSE

INDICE

Nous allons donc dans un premier temps chercher sur Google



que port utilise SMB



Tous

Images

Vidéos

Actualités

Livres

Finance

Web

Outils

Le trafic SMB netBIOS hébergé direct utilise le port **445 (TCP)**. 20 mars 2024



Microsoft Learn

<https://learn.microsoft.com> > ... > Windows Server

**SMB hôte direct sur TCP/IP - Windows Server - Microsoft Learn**

À propos des extraits optimisés • Commentaires

On peut voir ici qu'on nous parle du port "445" mais quand on regarde le lien Microsoft on nous parle d'autres port ainsi que le port "445".

Lien du site Microsoft : <https://learn.microsoft.com/fr-fr/troubleshoot/windows-server/networking/direct-hosting-of-smb-over-tcpip>

## Informations supplémentaires

NetBIOS sur TCP utilise traditionnellement les ports suivants :

- NBName : 137/UDP
- NBName : 137/TCP
- NBDatagram : 138/UDP
- NBSession : 139/TCP

Le trafic *SMB netBIOS hébergé* direct utilise le port **445 (TCP)**. Dans ce cas, un en-tête de quatre octets précède le trafic SMB. Le premier octet de cet en-tête est toujours 0x00, et les 3 octets suivants correspondent à la longueur des données restantes.

pour cela nous pouvons essayer un scan avec l'outils "nmap" avec l'option "-sV"

```
[Sep 17, 2024 - 13:36:14 (CEST)] exego1-HTB /workspace # nmap -sV 10.129.89.167
Starting Nmap 7.93 ( https://nmap.org ) at 2024-09-17 14:05 CEST
Nmap scan report for 10.129.89.167
Host is up (0.024s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

On peut voir ici qu'il y a bien le port "139" et le port "445" et après une petite recherche sur Google on nous dit que le port "445" est utilisé sur les versions les plus récente de "SMB"

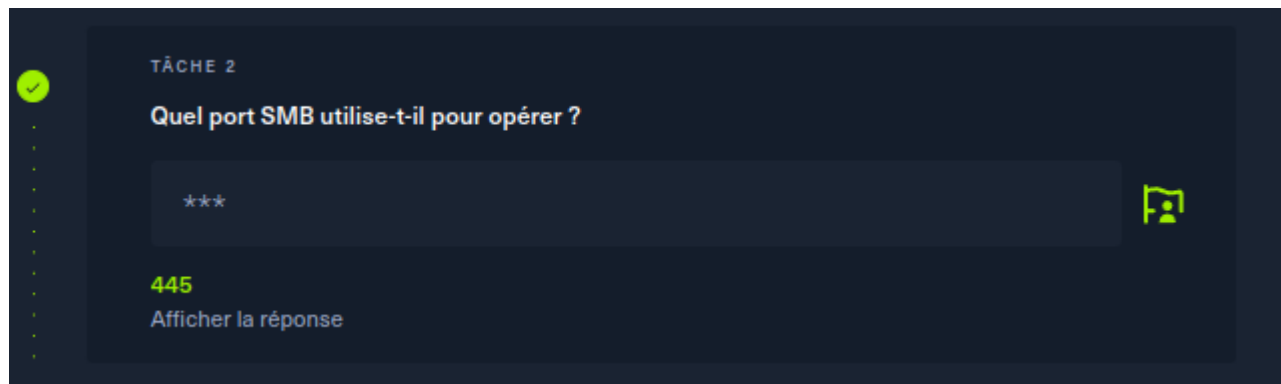
### À quoi servent les ports 139 et 445 ?

SMB a toujours été un protocole de partage de fichiers sur le réseau. À ce titre, il a besoin de ports réseau sur un ordinateur ou sur un serveur pour communiquer avec d'autres systèmes. SMB utilise le port IP 139 ou 445.

+ **Port 139** : SMB fonctionnait à l'origine sur NetBIOS via le port 139. NetBIOS est une couche de transport plus ancienne qui permet aux ordinateurs Windows de se parler sur un même réseau.

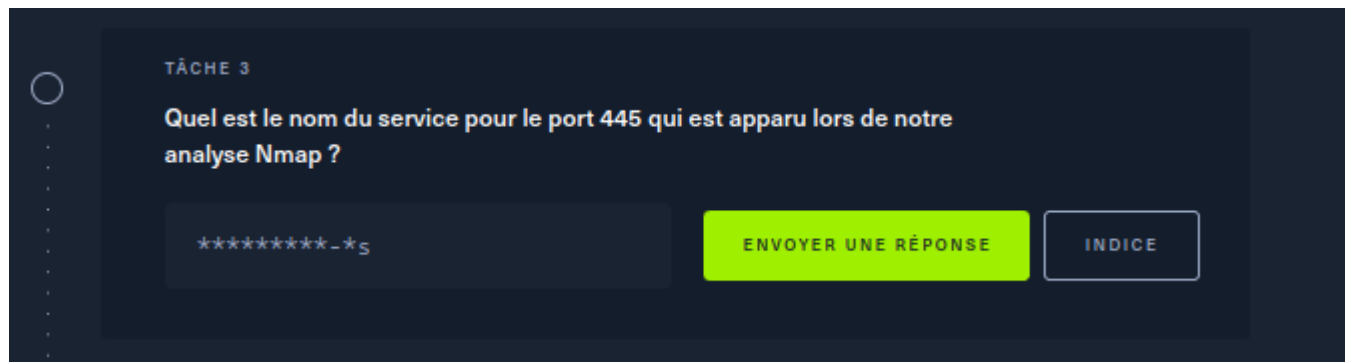
+ **Port 445** : les versions plus récentes de SMB (postérieures à Windows 2000) ont commencé à utiliser le port 445 sur une pile TCP. L'utilisation de TCP permet à SMB de fonctionner par Internet.

Nous allons donc répondre à la question en utilisant le port "445" comme réponse.



The screenshot shows a quiz interface with a dark blue background. On the left, there is a vertical list of questions, with the first one highlighted by a green checkmark. The main area displays 'TÂCHE 2' and the question 'Quel port SMB utilise-t-il pour opérer ?'. Below the question is a text input field containing '\*\*\*'. To the right of the input field is a green icon of a document with a checkmark. Below the input field, the number '445' is displayed in green, followed by the text 'Afficher la réponse'.

On nous demande ensuite quel est le nom du service qui tourne sur le port "445" suite au scan "nmap".



The screenshot shows a quiz interface with a dark blue background. On the left, there is a vertical list of questions, with the third one highlighted by a white circle. The main area displays 'TÂCHE 3' and the question 'Quel est le nom du service pour le port 445 qui est apparu lors de notre analyse Nmap ?'. Below the question is a text input field containing '\*\*\*\*\*-\*s'. To the right of the input field are two buttons: a green button labeled 'ENVOYER UNE RÉPONSE' and a white button labeled 'INDICE'.

On peut voir que lors de notre scan pour trouver le port qu'utilise "SMB" nous avons eu le nom du service qui tourne sur le port "445".

```
[Sep 17, 2024 - 13:36:14 (CEST)] exegol-HTB /workspace # nmap -sV 10.129.89.167
Starting Nmap 7.93 ( https://nmap.org ) at 2024-09-17 14:05 CEST
Nmap scan report for 10.129.89.167
Host is up (0.024s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Nous pouvons donc répondre à la question en indiquant qu'il s'agit du service "microsoft-ds".

TÂCHE 3

Quel est le nom du service pour le port 445 qui est apparu lors de notre analyse Nmap ?

\*\*\*\*\*-s

**Microsoft DS**

Afficher la réponse

Pour la question 4 on nous demande quel commande utiliser avec l'utilitaire "smbclient" pour lister les partages disponible.

TÂCHE 4

Quel est le « drapeau » ou le « commutateur » que nous pouvons utiliser avec l'utilitaire smbclient pour « répertorier » les partages disponibles sur Dancing ?

\*\*

ENVOYER UNE RÉPONSE

INDICE

Soit on peut faire une recherche Google ou alors comme pour beaucoup d'outils la commande "--help" nous affiche les options.

```

[Sep 17, 2024 - 14:54:48 (CEST)] exegol-HTB /workspace # smbclient --help
Usage: smbclient [OPTIONS] service <password>
  -M, --message=HOST      Send message
  -I, --ip-address=IP      Use this IP to connect to
  -E, --stderr             Write messages to stderr instead of stdout
  -L, --list=HOST          Get a list of shares available on a host
  -T, --tar=<c|x>IXFvgbNan Command line tar
  -D, --directory=DIR     Start from directory
  -c, --command=STRING     Execute semicolon separated commands
  -b, --send-buffer=BYTES  Changes the transmit/send buffer
  -t, --timeout=SECONDS    Changes the per-operation timeout
  -p, --port=PORT          Port to connect to
  -g, --grepable           Produce grepable output
  -q, --quiet              Suppress help message
  -B, --browse             Browse SMB servers using DNS

Help options:
  -?, --help              Show this help message
  --usage                 Display brief usage message

Common Samba options:
  -d, --debuglevel=DEBUGLEVEL Set debug level
  --debug-stdout              Send debug output to standard output
  -s, --configfile=CONFIGFILE Use alternative configuration file

```

Grace a la commande on peut voir que la commande qui nous intéresse est "-L" qui nous permet de pouvoir lister.

```

[Sep 17, 2024 - 14:54:48 (CEST)] exegol-HTB /workspace # smbclient --help
Usage: smbclient [OPTIONS] service <password>
  -M, --message=HOST      Send message
  -I, --ip-address=IP      Use this IP to connect to
  -E, --stderr             Write messages to stderr instead of stdout
  -L, --list=HOST          Get a list of shares available on a host
  -T, --tar=<c|x>IXFvgbNan Command line tar
  -D, --directory=DIR     Start from directory
  -c, --command=STRING     Execute semicolon separated commands
  -b, --send-buffer=BYTES  Changes the transmit/send buffer
  -t, --timeout=SECONDS    Changes the per-operation timeout
  -p, --port=PORT          Port to connect to
  -g, --grepable           Produce grepable output
  -q, --quiet              Suppress help message
  -B, --browse             Browse SMB servers using DNS

Help options:
  -?, --help              Show this help message
  --usage                 Display brief usage message

Common Samba options:
  -d, --debuglevel=DEBUGLEVEL Set debug level
  --debug-stdout              Send debug output to standard output
  -s, --configfile=CONFIGFILE Use alternative configuration file

```

Nous pouvons donc répondre a la question.

**TÂCHE 4**

**Quel est le « drapeau » ou le « commutateur » que nous pouvons utiliser avec l'utilitaire smbclient pour « répertorier » les partages disponibles sur Dancing ?**

★★

**-L**

Afficher la réponse

Pour la question 5 on nous demande combien de partages y a-t-il sur la machine "Dancing"

Pour cela nous allons donc utiliser la commande "smbclient -L ip machine"

```
[Sep 17, 2024 - 14:54:54 (CEST)] exego1-HTB /workspace # smbclient -L 10.129.89.167
Password for [WORKGROUP\root]:

Sharename      Type      Comment
-----
ADMIN$         Disk      Remote Admin
C$             Disk      Default share
IPC$           IPC       Remote IPC
WorkShares     Disk
```

On peut donc voir qu'il y a 4 partages sur la machine.

```
[Sep 17, 2024 - 14:54:54 (CEST)] exego1-HTB /workspace # smbclient -L 10.129.89.167
Password for [WORKGROUP\root]:

Sharename      Type      Comment
-----
ADMIN$         Disk      Remote Admin
C$             Disk      Default share
IPC$           IPC       Remote IPC
WorkShares     Disk
```

Nous pouvons donc répondre a la question.

TÂCHE 5

Combien de partages y a-t-il sur Dancing ?

\*

4

Afficher la réponse

Pour la question 6 on nous demande quel est le nom du fichier auquel nous pouvons accéder sans mot de passe.

TÂCHE 6

Quel est le nom du partage auquel nous pouvons accéder au final avec un mot de passe vide ?

\*\*\*\*\*\$

ENVOYER UNE RÉPONSE


INDICE

Nous pouvons voir que le seul fichier qui ne comporte pas le symbole "\$" et donc au quel nous pouvons accéder sans mot de passe c'est "WorkShare"


```
[Sep 17, 2024 - 15:40:20 (CEST)] exegol-HTB /workspace # smbclient -L 10.129.89.167
Password for [WORKGROUP\root]:

Sharename      Type      Comment
-----
ADMIN$         Disk      Remote Admin
C$             Disk      Default share
IPC$           IPC       Remote IPC
WorkShares     Disk
SMB1 disabled -- no workgroup available
```

Nous pouvons donc répondre a la question.

 TASK 6


What is the name of the share we are able to access in the end with a blank password?



**WorkShares**

Hide Answer

Pour la question 7 on nous demande quel commande nous pouvons utiliser dans le shell "SMB" pour télécharger les fichiers que nous trouvons.

 TÂCHE 7

Quelle est la commande que nous pouvons utiliser dans le shell SMB pour télécharger les fichiers que nous trouvons ?

**ENVOYER UNE RÉPONSE**

INDICE

Donc pour cela nous allons nous connecter et nous rendre dans le dossier WorkShares.

```
[Sep 17, 2024 - 19:07:07 (CEST)] exegol-HTB /workspace # smbclient \10.129.14.78\WorkShares
Password for [WORKGROUP\root]:
10.129.14.78WorkShares: Not enough '\' characters in service
Usage: smbclient [-?EgqBNPKV] [-?|--help] [--usage] [-M|--message=HOST] [-I|--ip-address=IP] [-E|--stderr]
[-L|--list=HOST] [-T|--tar=<c|x>IXFvgbNan] [-D|--directory=DIR] [-c|--command=STRING]
[-b|--send-buffer=BYTES] [-t|--timeout=SECONDS] [-p|--port=PORT] [-g|--grepable] [-q|--quiet]
[-B|--browse] [-d|--debuglevel=DEBUGLEVEL] [--debug-stdout] [-s|--configfile=CONFIGFILE]
[--option=name=value] [-l|--log-basename=LOGFILEBASE] [--leak-report] [--leak-report-full]
[-R|--name-resolve=NAME-RESOLVE-ORDER] [-O|--socket-options=SOCKETOPTIONS]
[-m|--max-protocol=MAXPROTOCOL] [-n|--netbiosname=NETBIOSNAME] [--netbios-scope=SCOPE]
[-W|--workgroup=WORKGROUP] [--realm=REALM] [-U|--user=[DOMAIN/]USERNAME[%PASSWORD]] [-N|--no-pass]
[--password=STRING] [--pw-nt-hash] [-A|--authentication-file=FILE] [-P|--machine-pass]
[--simple-bind-dn=DN] [--use-kerberos=desired|required|off] [--use-krb5-ccache=CCACHE]
[--use-winbind-ccache] [--client-protection=sign|encrypt|off] [-k|--kerberos] [-V|--version]
[OPTIONS] service <password>
```

Comme on peut le voir il y a une erreur avec "".

Après une petite recherche sur Google voici ce qu'on nous conseil si jamais nous avons cette erreur.

Lien : <https://www.malekal.com/comment-utiliser-smbclient-exemples/>

Si vous rencontrez l'erreur suivante lors de la connexion SMB :

```
Not enough '\' characters in service
```

Triplez l'antislash pour la résoudre, comme ceci :

```
mbclient -U sambauser -L "\\10.0.0.43\partagedemo"
```

Nous allons donc essayer.

Après plusieurs essais la bonne commande pour pouvoir accéder au dossier "WorkShares" était "smbclient \\10.129.14.78\WorkShares".

```
[Sep 17, 2024 - 19:18:10 (CEST)] exegol-HTB /workspace # smbclient \\10.129.14.78\WorkShares
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \>
```

Nous allons utiliser la commande "help" pour savoir les commandes disponibles.



```

5114111 blocks of size 4096. 1753258 blocks available
smb: \> help
?                allinfo          altname          archive          backup
blocksize        cancel          case_sensitive  cd               chmod
chown            close          del              deltree          dir
du               echo           exit             get              getfacl
geteas           hardlink       help             history          iosize
lcd              link           lock             lowercase        ls
l                mask           md               mget             mkdir
more             mput           newer            notify           open
posix            posix_encrypt  posix_open       posix_mkdir      posix_rmdir
posix_unlink     posix_whoami   print            prompt           put
pwd              q              queue            quit             readlink
rd               recurse        reget            rename            reput
rm               rmdir          showacls         setea            setmode
scopy            stat           symlink          tar              tarmode
timeout          translate      unlock           volume           void
wdel             logon          listconnect      showconnect      tcon
tdis             tid            utimes           logoff           ..
!
```

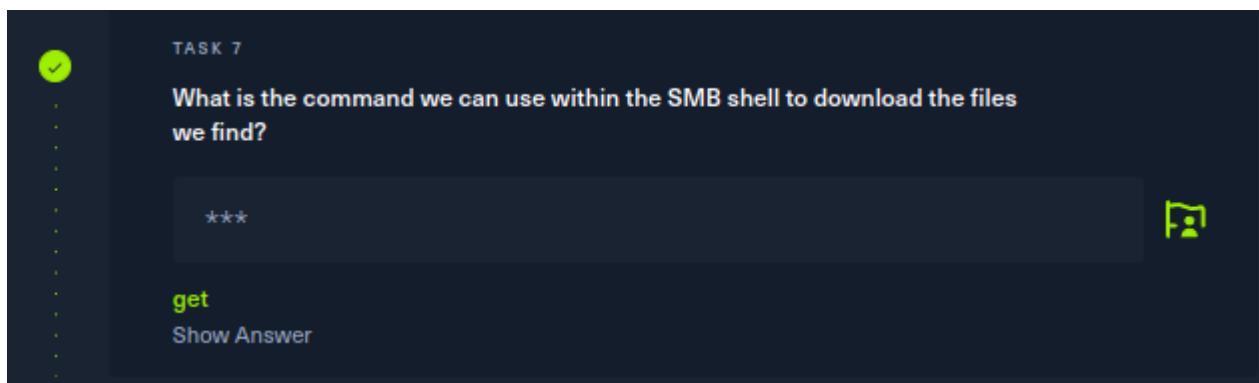
Nous allons donc utiliser "ls" pour lister le contenu du dossier "Workshare"

```

!
smb: \> ls
.                D            0   Mon Mar 29 10:22:01 2021
..               D            0   Mon Mar 29 10:22:01 2021
Amy.J            D            0   Mon Mar 29 11:08:24 2021
James.P          D            0   Thu Jun  3 10:38:03 2021

5114111 blocks of size 4096. 1753242 blocks available
```

on peut voir qu'il y a deux dossiers et pour pouvoir télécharger un fichier nous avons vu dans la liste des commandes qu'il y avait "get" nous pouvons donc répondre à la question.



Pour la dernière question il nous suffit de récupérer le flag présent dans un des deux dossiers.

SUBMIT FLAG

Submit root flag

\*\*\*\*\*

SUBMIT FLAG

✓

SUBMIT FLAG

Submit root flag

\*\*\*\*\*

🚩

Show Answer