Machine: Lame

* + - Easy

# Challenge Description :

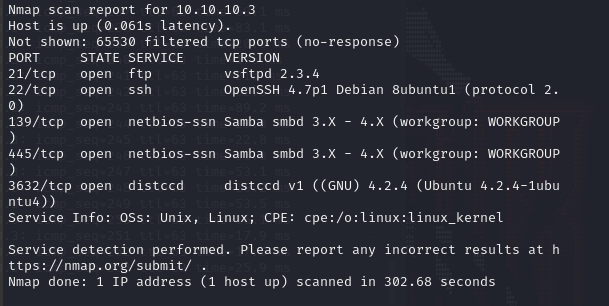
A super easy Machine, easily done with just Metasploit scripts to directly get a root shell.

# Notes :

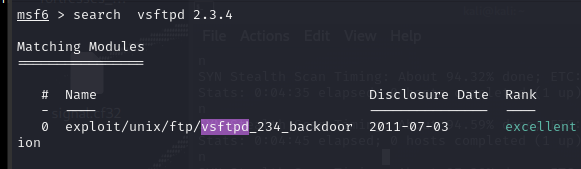
* MsfConsole (MetaSploit)
* Nmap (Network Mapper)
  + - Make sure you Read the Full report / scan on nmap.
    - Make sure to use nmap properly / efficiently.
    - MsfConsole not required, just highly recommended for gaining the exploits.

# Getting Down to Flag :

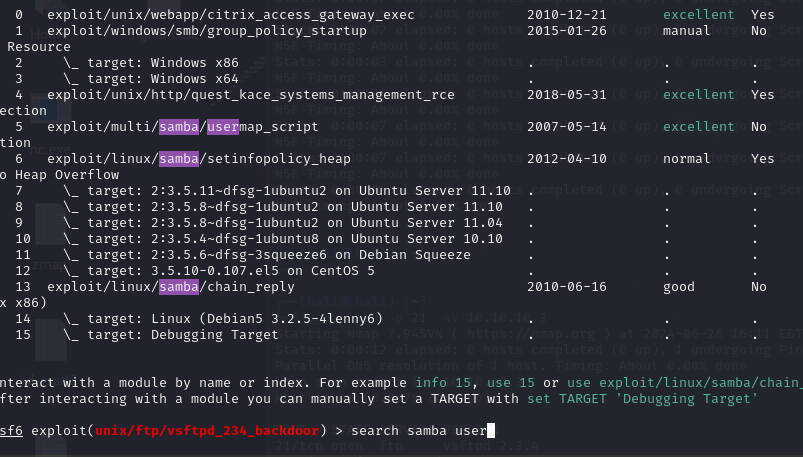
* First Connect to the Machine via your Own Configuration / either by VPN or a PWNBox, while spawning up the machine.
* After its Up begin to Nmap it.
* You can add it too /etc/host, to a domain like lame.htb to make it easier to remember rather than an IP.



* 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.



* 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.

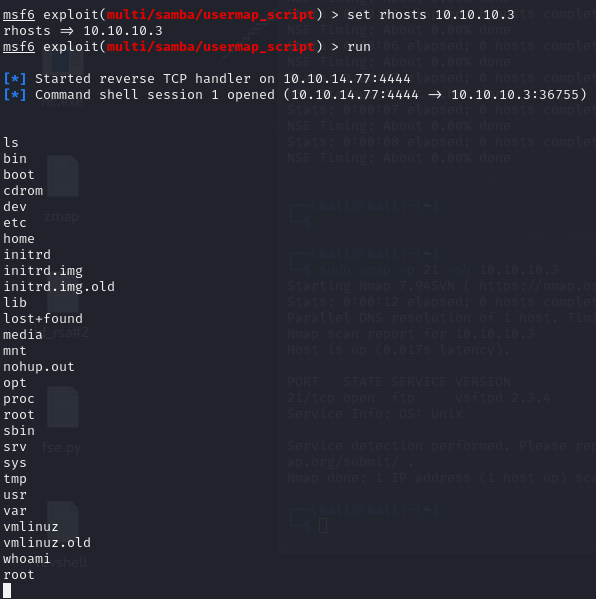


* We then execute the multi/samba/usermap\_script as it will give you a shell, you can look for this via msfconsole from this:

’Search samba user’

’use multi/samba/usermap\_script’

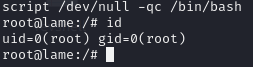
* We then execute the exploit by setting the remote host and running it.
* Success, We finally get a shell and its Root so we don't need to do any privilege escalation.



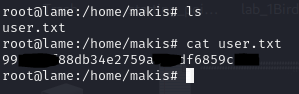
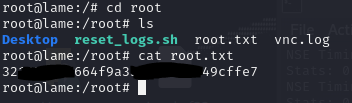
* To get a proper shell we set the TTY for a terminal prompt,

I normal use this to get it

‘script /dev/null -qc /bin/bash’

****

See more [TTY’S](https://book.hacktricks.xyz/generic-methodologies-and-resources/shells/full-ttys)here

* The first flag, the ‘’User flag’’ can be found exploring the user directories
* And the second flag as you can guess is in the root directory.

First Machine - Birdo