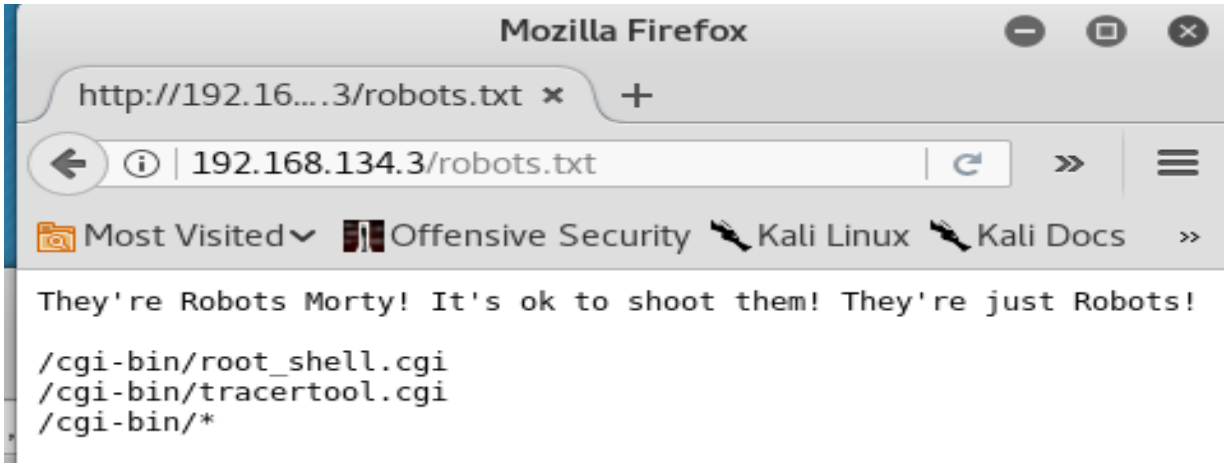
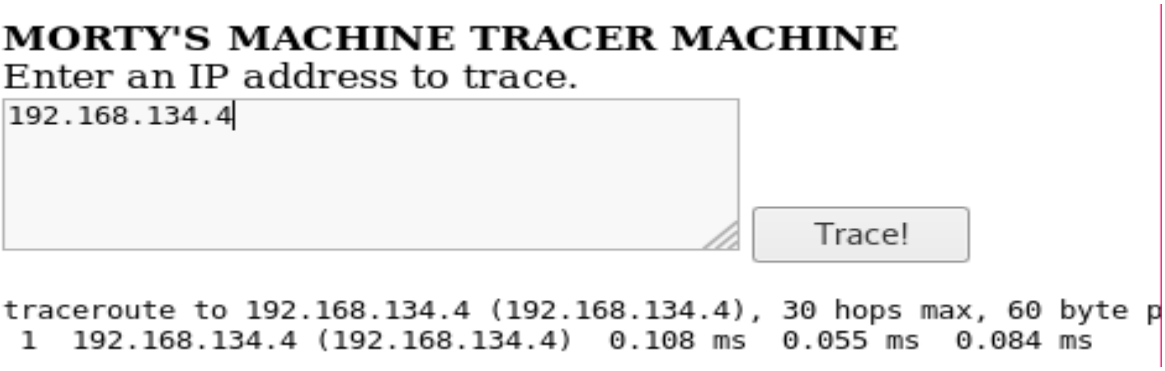
RickdiculouslyEasy 1

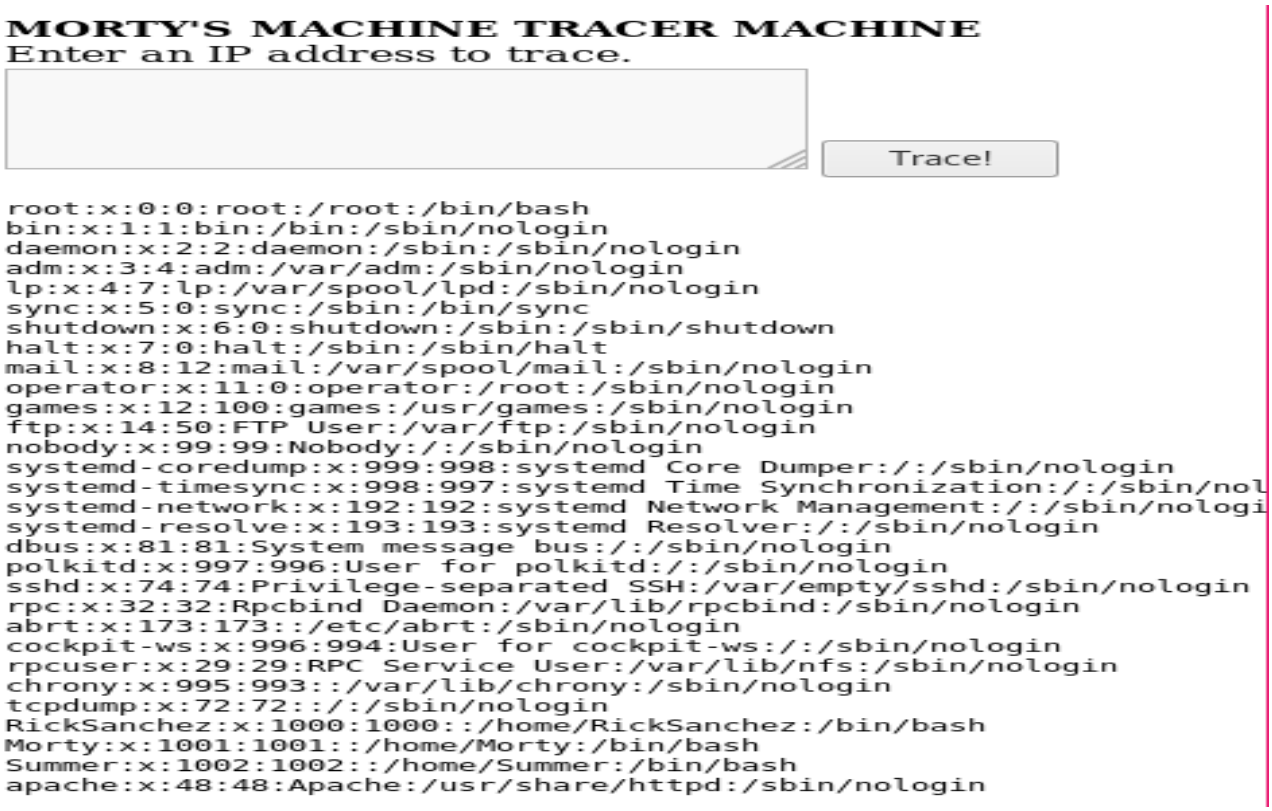
This is a simple walkthough based on the RickdiculouslyEasy: 1 Vm from vulnhub posted by Luke I scanned the machine using zenmap and looked at the website in the meantime. Robots.txt was the first obvious place to look.





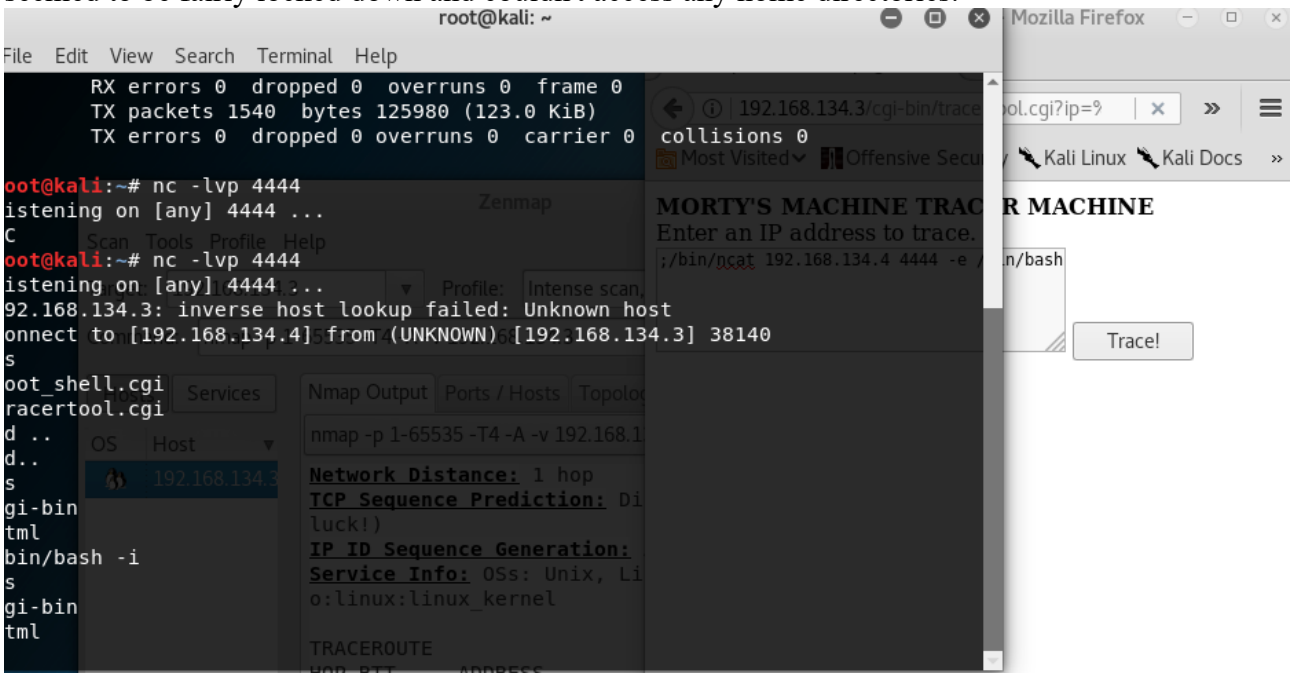
It revealed some files in the /cgi-bin/. Notably one called root_shell which was a red herring. But the tracertool appeared to be executing the trace command. Potential command injection?. Absolutely.

Doing this I was able to dump the /etc/passwd file to enumerate usernames. Although cat would just print out an ascii art, less and more were still available.



Gathered Usernames from the passwd file dump:
Morty
Summer
RickSanchez

I did managed to get a reverse shelll after some time playing around using netcat. However it seemed to be fairly locked down and couldn't access any home directories.



Once the scan had returned there was an obvious flag hidden in the anonymous FTP
FLAG{Whoa this is unexpected} – 10 points

port 13337
The scan showed the flag already
FLAG:{TheyFoundMyBackDoorMorty}-10Points
But i netcat'ed to it anyway which didn't return anymore information.

port 60000
a half baked shell
netcat once again used which returedn
FLAG{Flip the pickle Morty!} - 10 Points

port 9090
FLAG {There is no Zeus, in your face!} - 10 Points

At This point i had covered most of the open ports, versions all seemed to be in check so it was timeto further investigate the website. I dirbustered the website to find a password directory containng passwords.html and a flag

FLAG{Yeah d- just don't do it.} - 10 Points

Password = winter
Ok cool so now we have usernames and a password. I tried to use the password with the Morty account to no avail. The obvious choice being Summer did work however with the home directory containing a flag.
FLAG{Get off the high road Summer!} - 10 Points

Poking around in morties home directory i managed to find a journal that is zip locked and an image called safe-password.jpg.So i just SCP'd both files to my kali machine. Running strings on the image returned the password to the journal zip. And unzipping the journal returned a flag
FLAG: {131333} - 20 Points
In the journal it was also mentioned that is was the password to a safe that rick had been mentioning.

Back onto the target machine i looked around in RickSanchez's home directory where there was a file called safe in a folder. This must be the safe mentioned earlier. We do not have permissions to execute it locally so i just once again scp it back to my kali machine.
Running the program we can see it takes in a command line argument. This command line argument is the password provided by the flag above.

Running the program with the input 131333 gives us a clue on what rick sanchez's password is and a flag.
FLAG{And Awwwaaaaayyyy we Go!} - 20 Points

The hint is that the password has an upper case letter, a digit, and then the name of his previous band in that order. So this obviously required a quick script. So i booted up python and wrote a quick script to generate all possible passwords. With this password list i then booted up medusa and fired it straight at the ssh on port 22222. Success! We found a password and was able to access RickSanchez's account. This account has sudo priviledges and will let us access the last flag. We still cannot change to the root directory but running the find command on the root directory using

sudo listed out all available files. One of these files being the flag!. So a quick sudo less Flag.txt and boom we have collected all the flags!

FLAG: {Ionic Defibrillator} - 30 points