Walkthrough – Connect the dots 1

Contents

[Host Discovery 2](#_Toc146544041)

# Host Discovery



# Nmap







# 



# NFS



Nothing really of interest here.

# Dirb

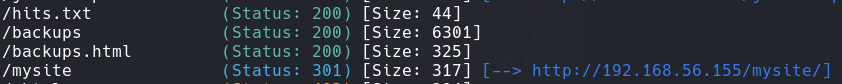






Nothing too interesting was found.

# Gobuster

Inside hits.txt there is a message: “Keep your enumeration game strong”.

I then went to view mysite directory and found numerous files. One of the files downloaded, the others just opened. Once it downloaded I viewed it and realised it is obufuscated in JSFuck.

I decoded it and found a clue: [TryToGuessThisNorris@2k19](mailto:TryToGuessThisNorris@2k19) (could be a password).



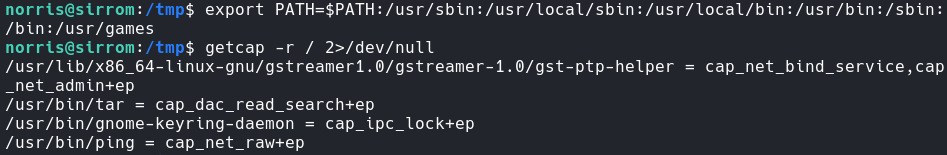
# Flag 1



There was a hidden file found with this message.

# Escalation

Good resource: https://tbhaxor.com/exploiting-linux-capabilities-part-2/

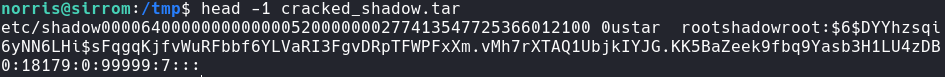
Before getting the file capabilities I had to quickly reset the path. For some reason it wasn’t set properly?

The binary I want is /usr/bin/tar because it contains the ‘cap\_dac\_read\_search+ep’. This means it can read anything without being blocked.

I first zip/tar the shadow file.



Then I quickly view the first line of the cracked\_shadow file.

However, since I don’t need the account to get the root flag I can just tar the root directory.

# Flag 2

I first begin my zipping the root flag file.



Now that I have zipped the file into the tmp directory I can then unzip it.



Now I traverse into the directory and get the root flag.

