Wireshark en la filtración de WikiLeaks (Vault 7: CIA Hacking Tools Revealed)

Configure Wireshark on Ubuntu

By default, wireshark can not be run as a non-root user when attempting to capture traffic on an interface. The following steps can rectify this issue:

1. Install Wireshark
   [crayon-6a9dad34a2557681014207/]
2. Create a wireshark group
   [crayon-6a9dad34a255d537149727/]
3. Add your username to the wireshark group
   [crayon-6a9dad34a255f766298015/]
4. Change the group ownership of the file dumpcap to wireshark
   [crayon-6a9dad34a2561495923208/]
5. Chage the mode of the file dumpcap to allow execution by the group wireshark
   [crayon-6a9dad34a2562382310596/]
6. Grant capabilities with setcap
   [crayon-6a9dad34a2564359101438/]
7. Verify the change
   [crayon-6a9dad34a2565443835144/]

config_wireshark-ubuntu_user.txt

Attachments:

- config_wireshark-ubuntu_user.txt

Previous versions:

| 1 | 2 |