EXPLIOT
www.expliot.io

Attacking Hardware

UART

Lab 3: Find credentials in the Camera filesystem

- Objective: Find any important credentials in the camera filesystem except /etc/shadow
- NOTE: If you see a lot of “sending discover” messages

- They are annoying when working on the shell, just kill the processes writing the message
- Or just ignore the messages as whatever you type will go to the shell.
- Ps axj | grep -i dhcp

Lab 3: Find credentials in the Camera filesystem

- Kill (Kill -9 <pid>) the dhcp scripts running to disable to messages
  - /etc/script/run_dhcpc.sh
  - Udhcpc
  - igd*

OEM Backdoors/Hidden commandsfilesystem

- General practice for vendors to have hidden commands custom consoles
- Typically custom consoles are accessed via the UART ports
- Security implications

- Backdoors
- Privilege escalation
- Modification of sensitive data

Lab 4: Finding Hidden commands

- Objective: Find a hidden command in DIVA and use it to subvert another DIVA challenge
- Steps

- Connect VM to DIVA
- pen DIVA shell – sudo screen /dev/ttyACM0
- Type .h
- See all valid commands.
- Type blabla
    - Note error message for invalid commands

Lab 4: Finding Hidden commands

- Use python itertools.product() and Serial class to automate sending and receiving data
- Or use expliot serialbrute plugin.

- $ efconsole
- ef> run serialbrute -h

- Check for error message in the response. If error message is not received, most likely it is a hidden command.

The End