Jake Crane

4/16/2015

For this project I chose to use Ubuntu 14.10 (32-bit) because it is my preferred distribution of linux.

For this project, the first thing that I did was disable Address space layout randomization (ASLR). Disabling ASLR makes stack smashing far more reliable.

I disabled ASLR by using the following command: sudo sysctl -w kernel.randomize\_va\_space=0

I also installed zsh to compare running the exploit using bash and zsh.

I accomplished this by using the following command: sudo apt-get install zsh

The next thing I did was remove the symbolic link located at /bin/sh and replace it with a link that pointed to /bin/zsh. I did this because the shellcode that was provided to me executes /bin/sh and I wanted to test the zsh shell. I also experimented with changing the link back to bash.

**Task 1:**

For the first task I modified the exploit program to store the provided shell code along with NOPs into memory. Next, I compiled the exploit program using the following command: gcc -o exploit exploit.c -std=c99

I then ran exploit to create badfile.

Next, I compiled the stack program using the following command:

sudo gcc -o stack stack.c -zexecstack -fno-stack-protector

Then I set the stack file's permissions to -rwsr-xr-x so users have the ability to tun the program with a uid of 0. I did this using the following command: sudo chmod 4755 stack

I then ran the stack program and was presented with the zsh prompt. By using the id command I was able to verify that I had obtained an euid of 0(root).

**Task 2:**

In my tests, bash did not seem to behave any differently than zsh. I was able to get full root access(uid=0) using both shells. I verified this by using the id command.

**Task 3:**

When I enable address randomization and attempt to smash the stack I generally get a Segmentation fault. If I run the following command, a shell is eventually spawned, but it can take quite some time.

command: sh -c "while [ 1 ]; do ./stack; done;"

**Task 4:**

When I compile and run stack without disabling the stack protection, I get the following message:

\*\*\* stack smashing detected \*\*\*: ./stack terminated

./test\_exploit.sh: line 21: 7470 Aborted (core dumped) ./stack