CS315 · Computer Security

Lab 6

胡玉斌 / 11712121

November 11, 2020

1 Lab 6 Part 1

1.1 Read the lab instructions above and finish all the tasks.

Done

1.2 Answer the questions in the Introduction section, and justify your answers. Simple yes or no answer will not get any credits.

1.2.1 What security features does Zephyr have?

- The security functionality in Zephyr hinges mainly on the inclusion of cryptographic algorithms, and on its monolithic system design.
- The security architecture is based on a monolithic design where the Zephyr kernel and all applications are compiled into a single static binary. System calls are implemented as function calls without requiring context switches. Static linking eliminates the potential for dynamically loading malicious code.
- Stack protection mechanisms are provided to protect against stack overruns.

1.2.2 Do applications share the same address space with the OS kernel?

- No
- It is very dangerous to share the the same address space with the OS kernel which means we can modify the value in that address space.

1.2.3 Does Zephyr have defense mechanisms such as non-executable stack or Address Space Layout Randomization (ASLR)?

- No
- Due to the exploration, we can see that the EIP register has the same value for the same payload and generate the special value for the EIP register.
- So Zephyr do not defense mechanisms.

1.2.4 Do textbook attacks(e.g., buffer overflow or heap spray)work on Zephyr?

- Yes
- Due to the exploration, we generate a payload to cause the buffer overflow.
- As we expected, the application crashes due to an invalid return address.
- Furthermore, QEMU also crashes and you will see a pop-up window as the screenshot below.

1.3 Change the EIP register to the value 0xdeadbeef, and show me the screenshot of the EIP value when the application crashes.

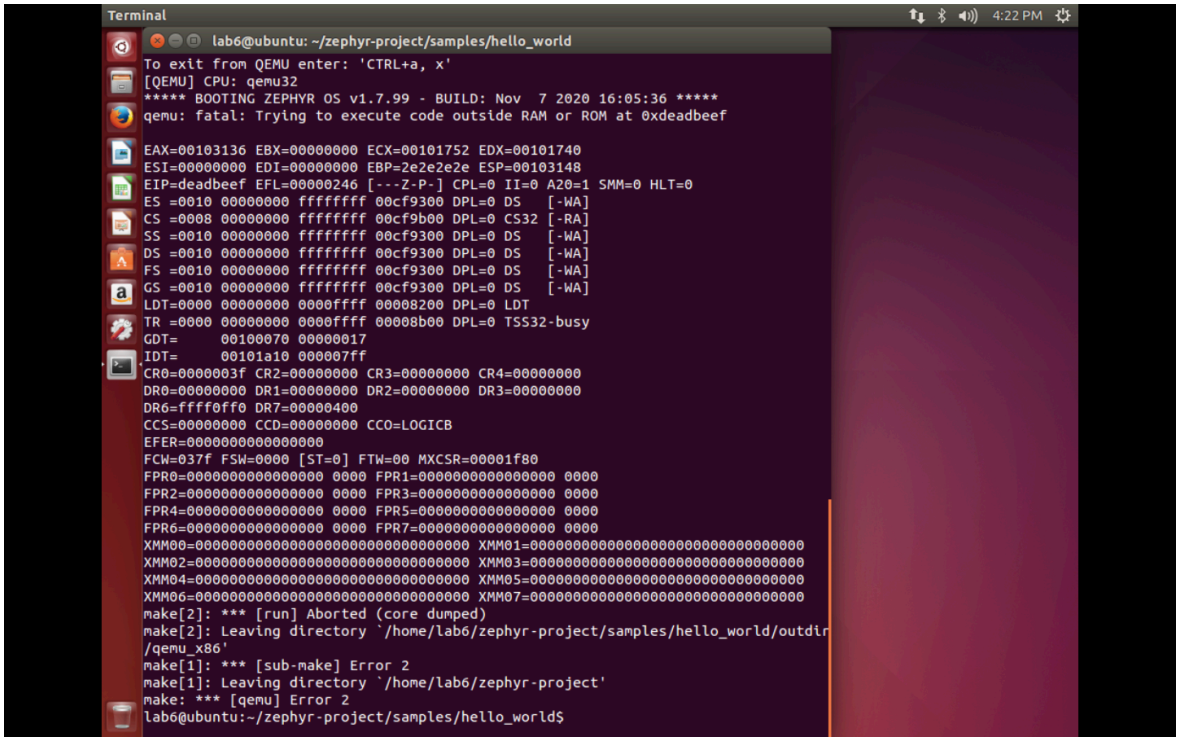

Figure 1: EIP value

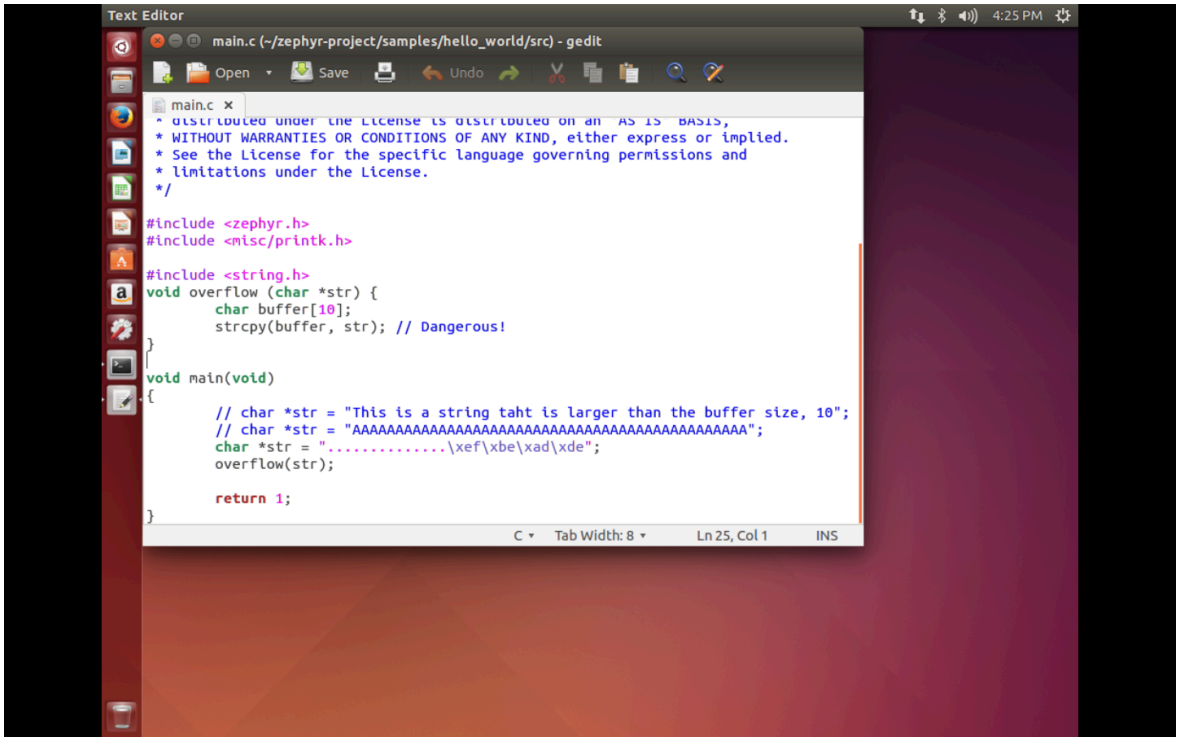

Figure 2: obfuscate

2 Lab 6 Part 2

2.1 Read the lab instructions above and finish all the tasks.

Done

2.2 Answer the questions in the Introduction section,and justify your answers. Simple yes or no answer will not get any credits.

2.2.1 What is the difference between Monitor Mode and Promiscuous Mode

- Monitor mode: Sniffing the packets in the air without connecting (associating) with any access point.
- Promiscuous mode: Sniffing the packets after connecting to an access point. This is possible because the wireless-enabled devices send the data in the air but only "mark" them to be processed by the intended receiver. They cannot send the packets and make sure they only reach a specific device, unlike with switched LANs.

2.2.2 What lessons we learned from this lab about setting the WiFi password?

- We should use strong password.
- Avoid using weak password to be blasted by weak password tables.

2.3 Change your router to a different pass phrase, and use the Wireshark and Aircrach-ng to crack the passphrase. Show screenshots of the result.

Use airport command to enable monitor mode, and monitor on channel 6.

The password of the router is **SUSTech-Eveneko**

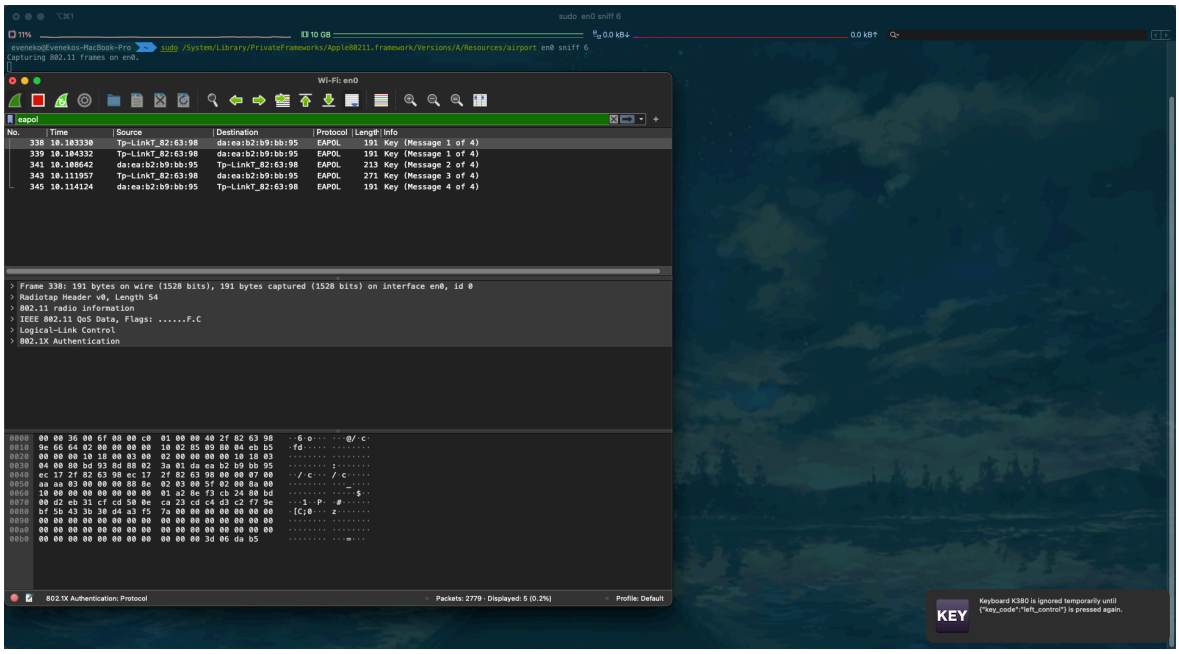

Figure 3: Wireshark

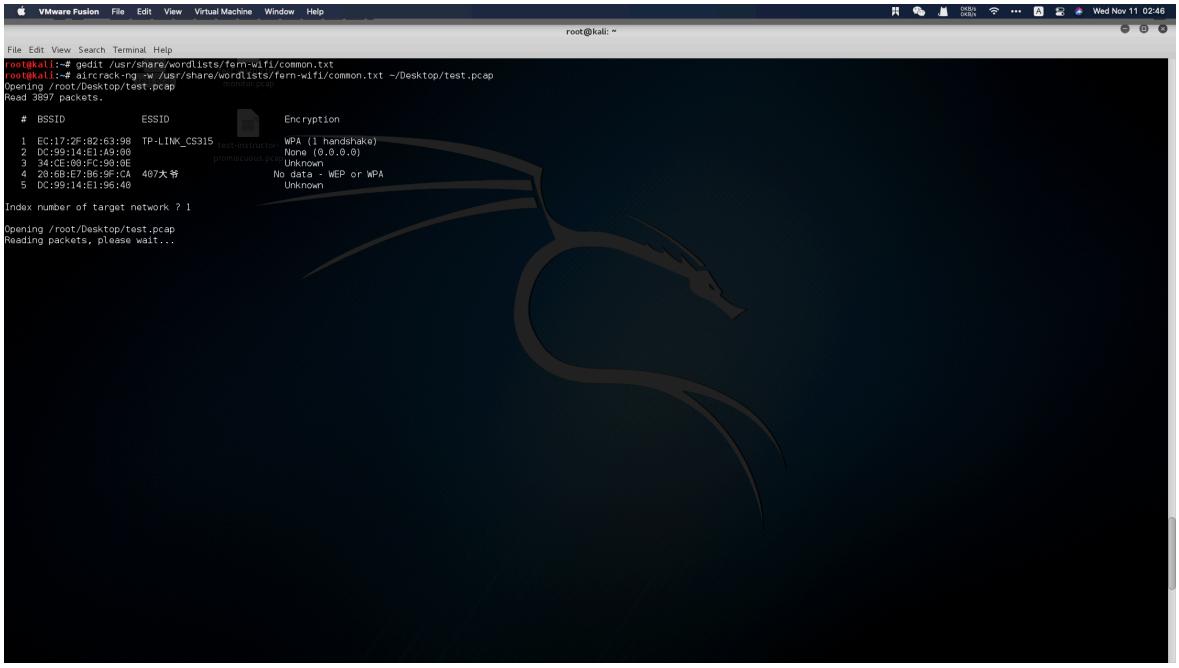

Figure 4: password1

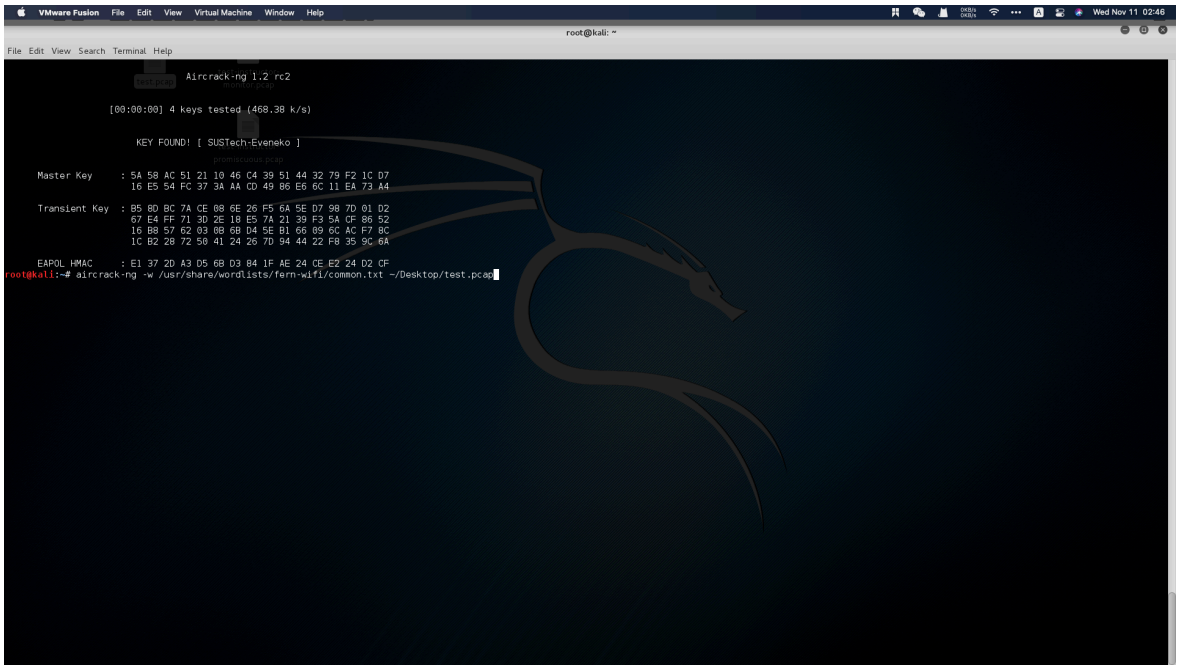

Figure 5: password2