# Infected linux program analysis

## Introduction

In this document, I will show how I analysis this infected linux shell binary, which is malwared by the-backdoor-factory.

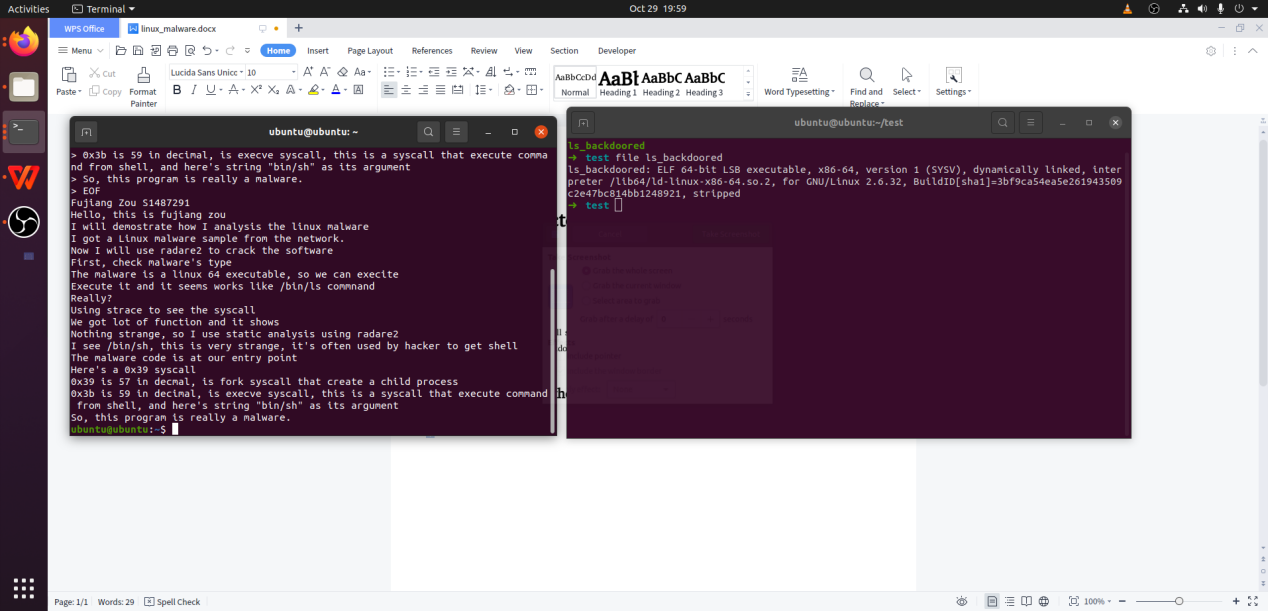
## Executive Summary

Nowadays, almost all server ls running on Linux kernel. And the most fast computing machines runs Linux as well. Linux is very important and it exists in anywhere near us. Our Android phone, labtop, game server, web server are all Linux. But with the rapid growth number of the Linux hosts the Linux malware grows as well. Unix and Unix like system use ELF（executable and linkable format) as its executable format. This is a very complex data structure that describe the executing information. Linux malware is usually insert payload(shellcode) into the normal program and do a reverse shell connection.

## Methods and Techniques

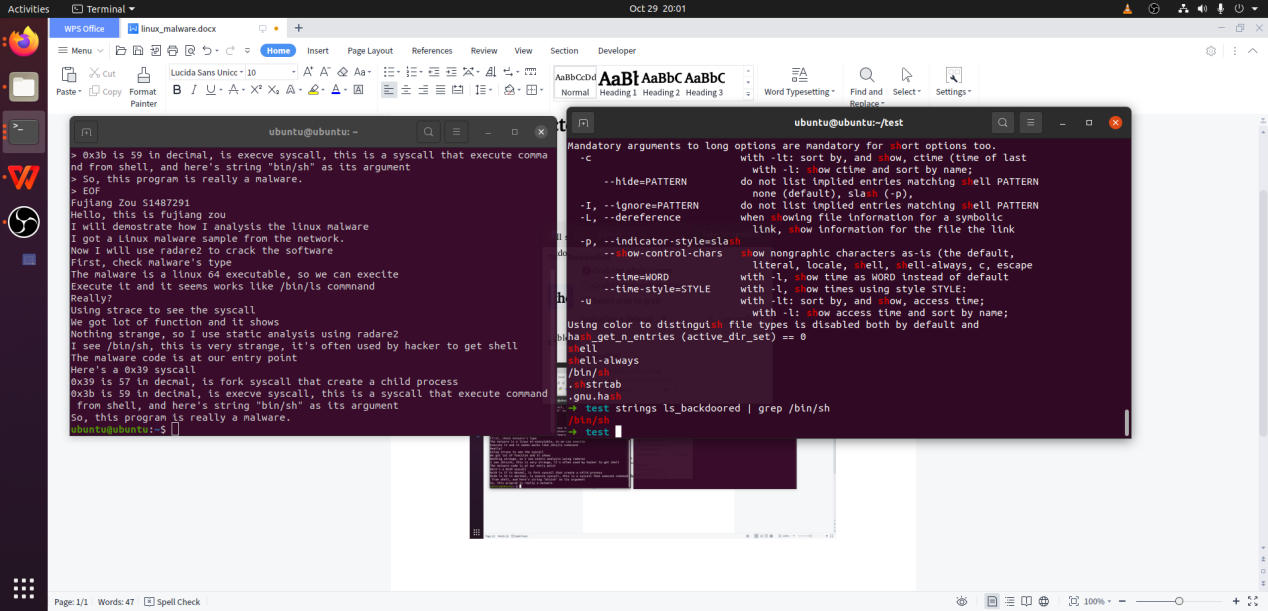
### Brief look at the malware

This is an ELF executable. ELF(Executable and Linkable Format) is a unix and unix like OS bianry format.



### Search for string

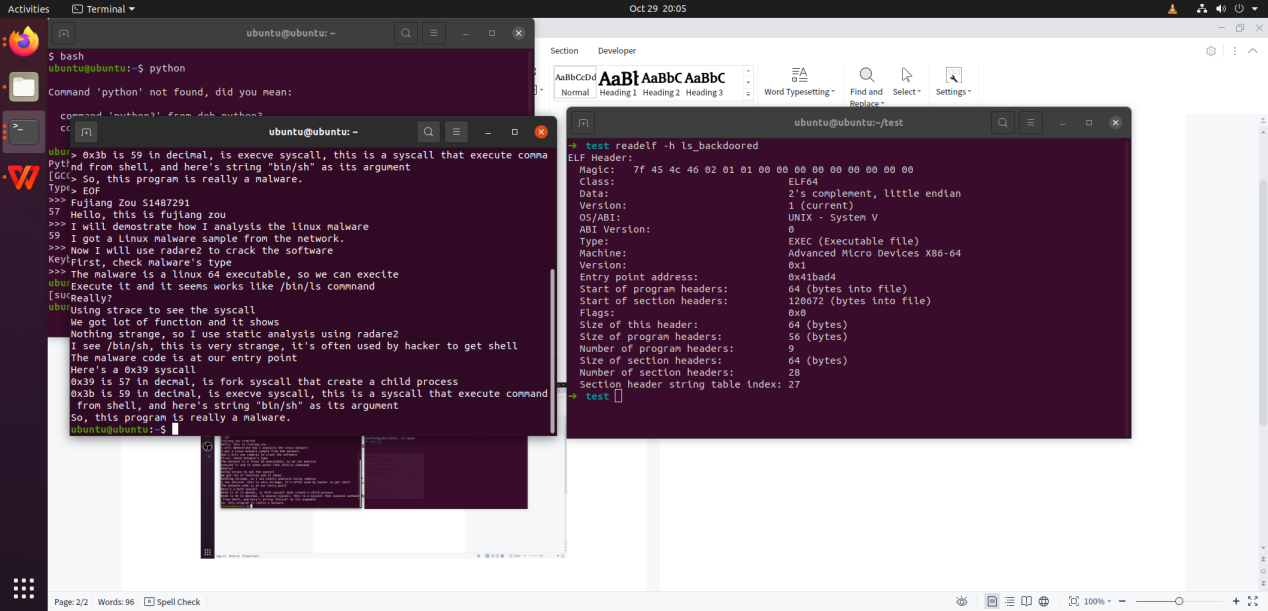
We usually using strings command or cat | grep to search for ascii string abd look for interesting string. The result shows that the malware contains a stinrg “/bin/sh”, which looks interesting. This is very common to a malware that contains such string, “/bin/bash”, “bin/sh”, etc.



### Get the entry point of the malware

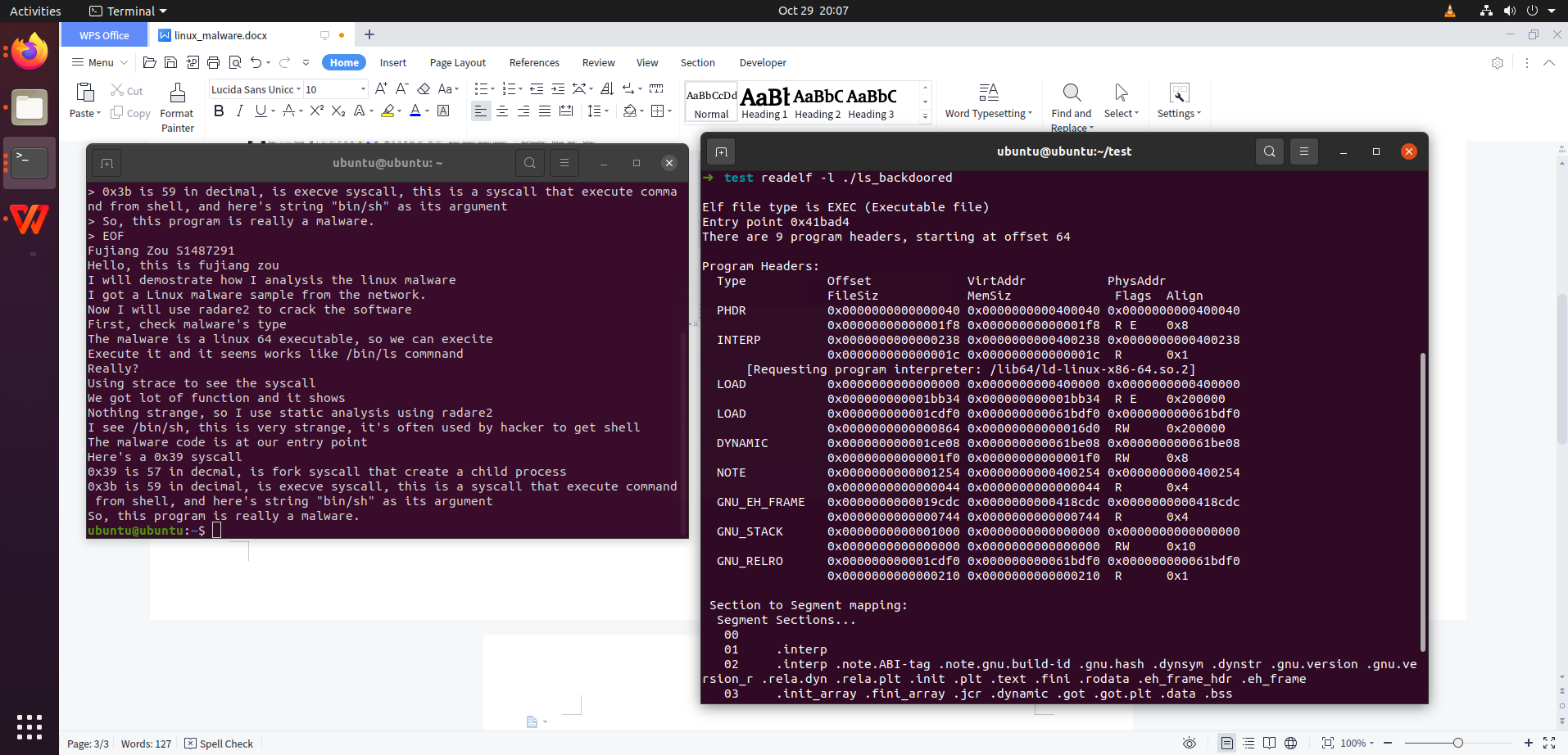
Because this is an ELF file, so we can use readelf command to read information.

use readelf -h to read the ELF header struct.



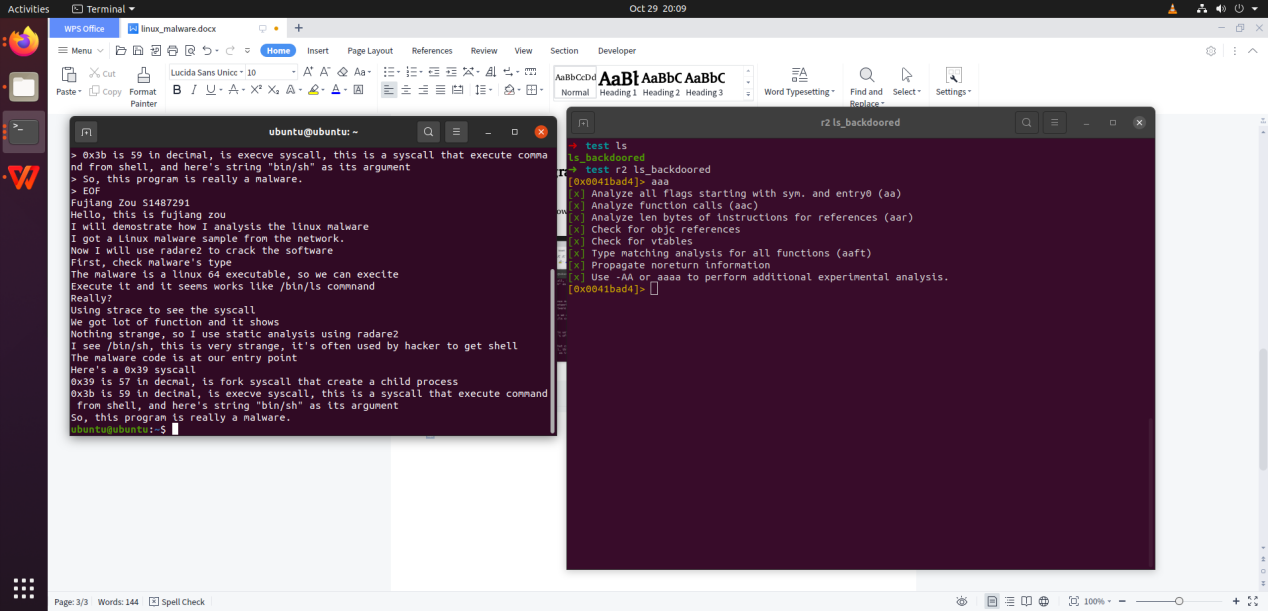
### Read the program header

The program heder show that where’s the entry and sessions, segments mapping information.



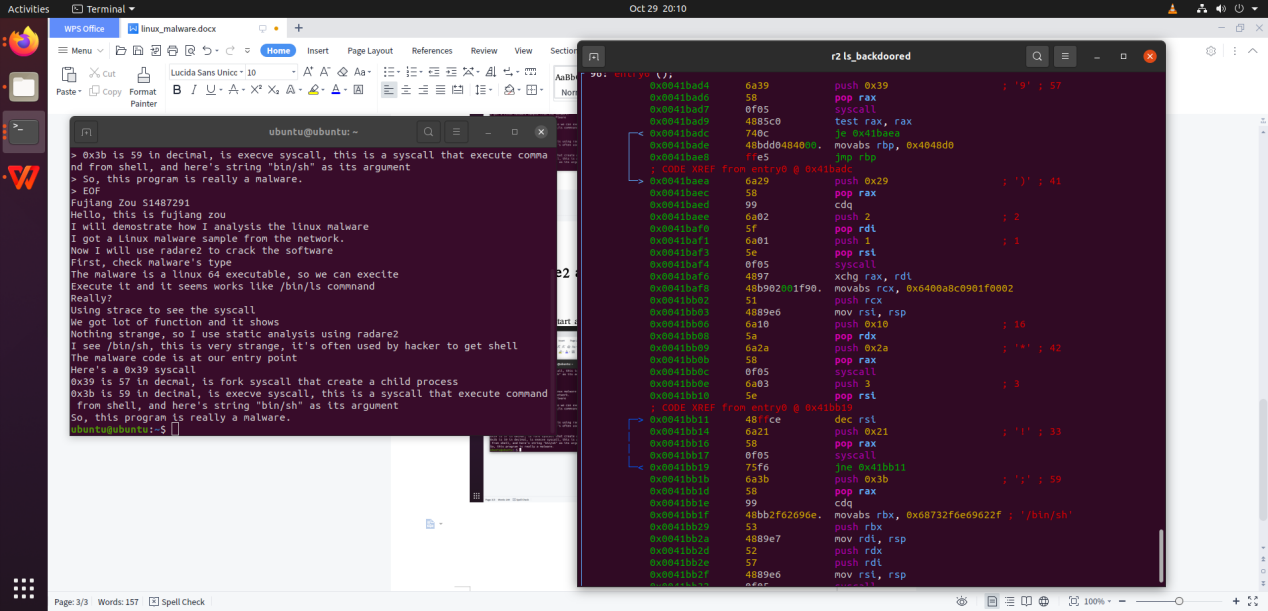
### Load to radare2 and start to analysis

using aaa comand to start analysis



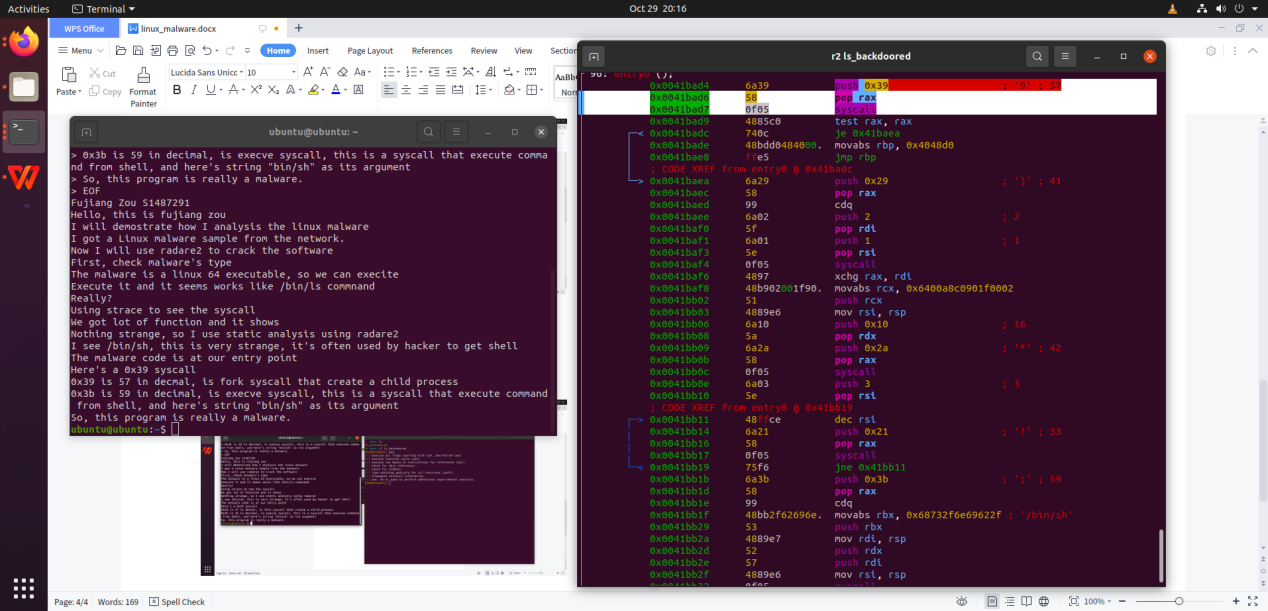
### Take look at the entry

use pdf command to disassembly the code



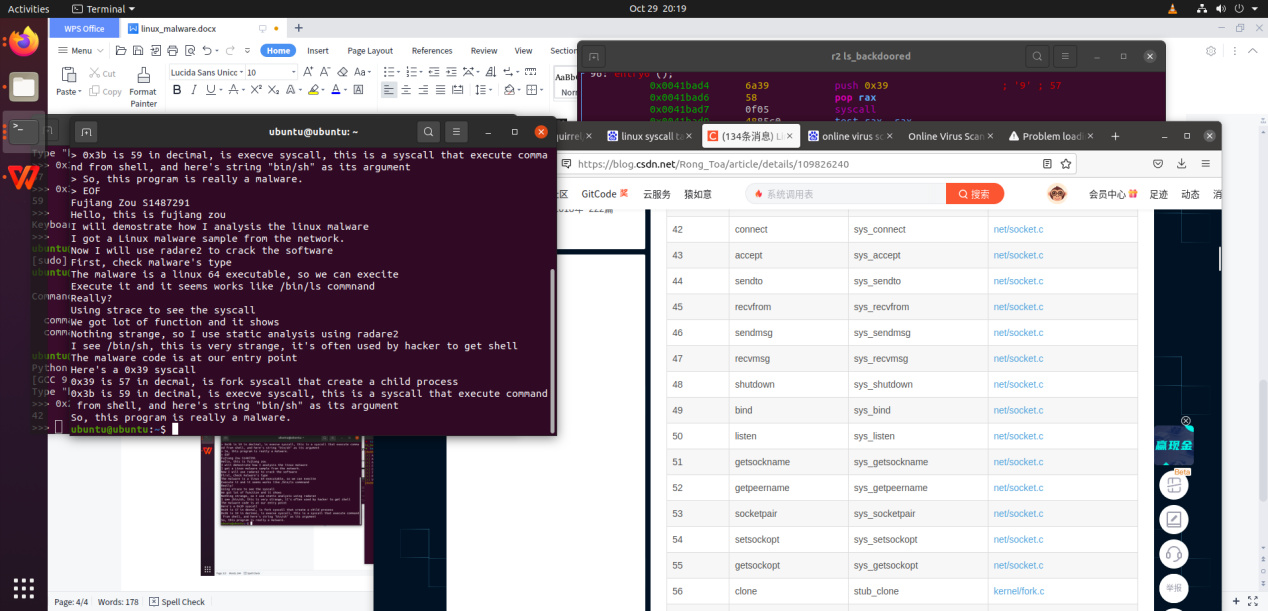
### Check syscall

here are many syscall, 0x39, 0x3b, 0x2a



Here is the syscall table, we can find some common syscall number and relative function name.

In this code, the program call connect, fork, and execve and “/bin/sh” as execve’s arguments. So we can know this is a reverse shell that connect to the remote host and make shell.



## Conclusion

In this assignment I analysis the infected program. The normal /bin/ls program is infected by the malware and injected shellcode into the TEXT segment at the entry of the program.The shellcode is very simple, which is just create a socket and connect the attacker’s host. And use execve function to run the /bin/sh and dup to the socket.