**Mid test**

Course name:Open Source Platform and Network Administration

Course code: OSP201

|  |  |
| --- | --- |
| Student name: | Nguyen Tran Vinh |
| Student ID: | SE160258 |

**Chú ý: chụptoànbộmànhìnhmáytínhchocáchìnhảnh minh họa (khôngcắtbớt)**

**Part 1: (4 marks)**

1.1 Describe in your wordsthe following functionalities of iptables:*(0.5 mark)*

* Filter
* NAT
* Mangle
* Security

Answer:

* Filter function is one of the most widely used functions in iptables. The filter function is used to decide whether to let the packet continue to its destination or refuse its request.
* The NAT function is used to implement network address translation rules. When packets enter the network stack, the rules in this table determine if and how to modify the packet's source or destination address to affect how the packet and any response traffic is routed....
* The Mangle function is used to change the IP headers of a packet in various ways. This Mangle function can also place internal signals on the packet for further processing in other functions and by other network tools.
* Security function is used to place SELinux security signatures inside of packages, which will affect how SELinux or other systems can secure and SELinux handle packages.

1.2 Describe in your words the following chains of iptables:

* INPUT
* OUTPUT
* FORWARD

Answer:

* The rule in the INPUT chain is executed just before the packet encounters a process. Chain INPUT exists only in mangle and nat tables.
* The rule in the OUTPUT chain is executed as soon as the packet is generated by the process. Chain OUTPUT exists in the tables: raw, mangle, nat and filter.
* The FORWARD rule is enforced for packets routed through the current host. Chain FORWARD exists only in table mangle and filter.

**Part 2:** compare: iptables, SELINUX, TCP wrapper **(2 marks)**

Answer:

* Iptables:

+ Add, remove, and edit rules to a packet filter ruleset

+ List and flush the rules to a packet filter ruleset

+ List counters of matched packets to rules

* TCP wrapper

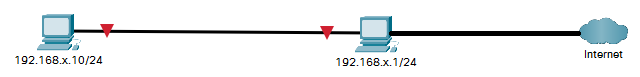
+ Allow or deny access to an application based on an IP Address or hostname

+ Allow or deny access to an application based on time

* SELINUX

+ Firewalls do a great job on filtering out unwanted or malicious activity, but flaws in your security can still be leveraged by external exploits as well as internal flaws in configuration or buggy software.

**Part 3: (4 marks)**

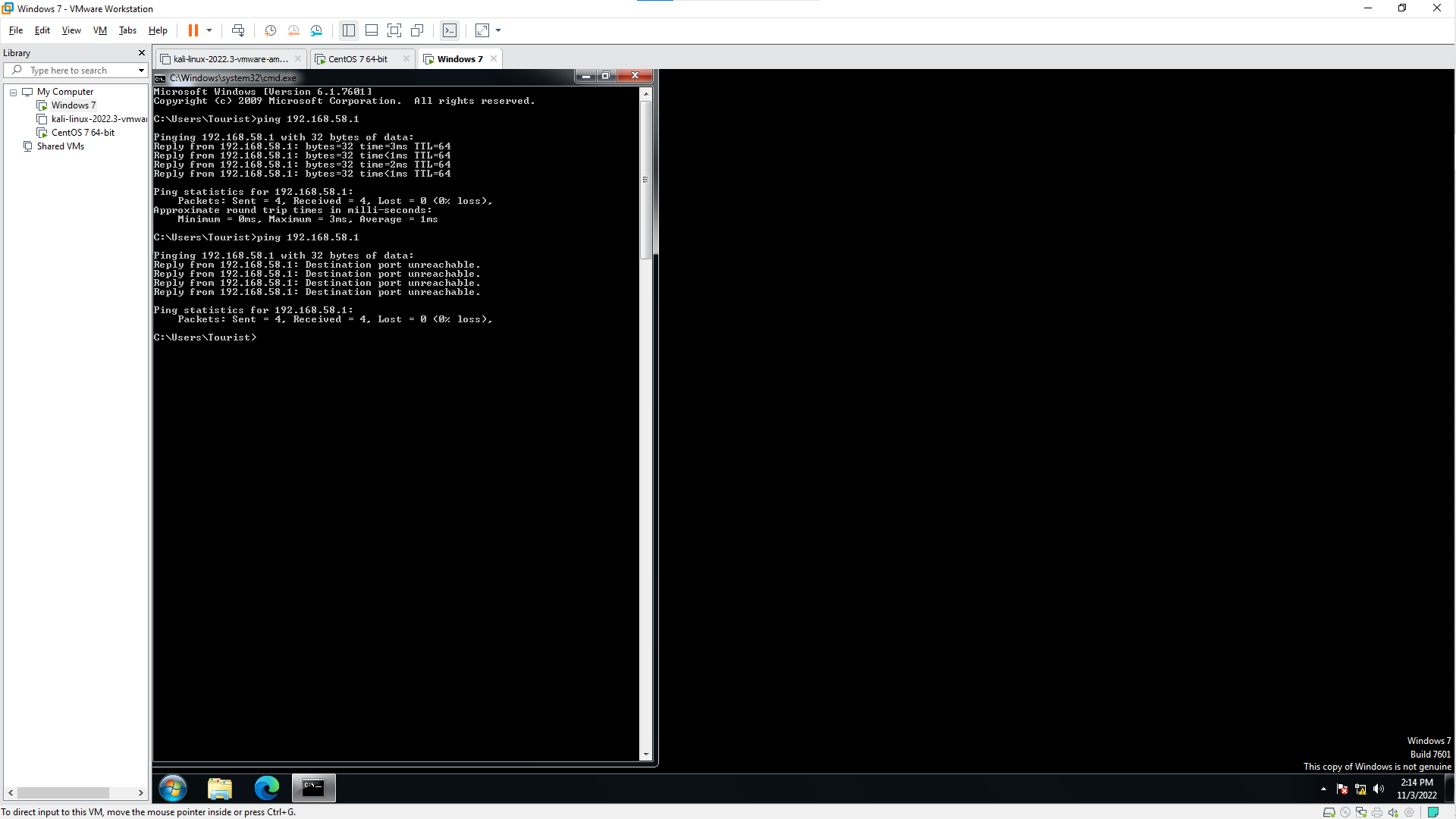
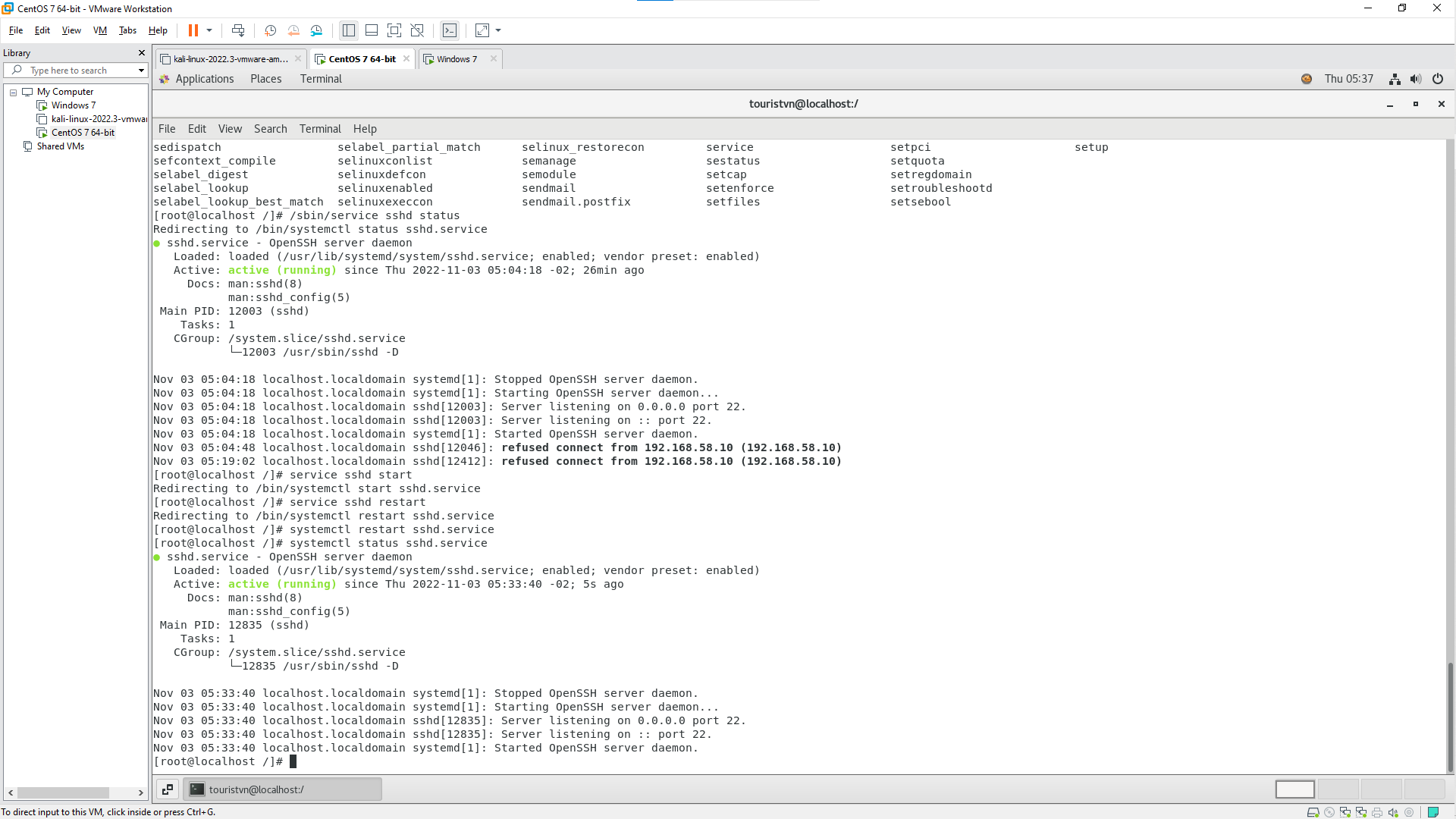
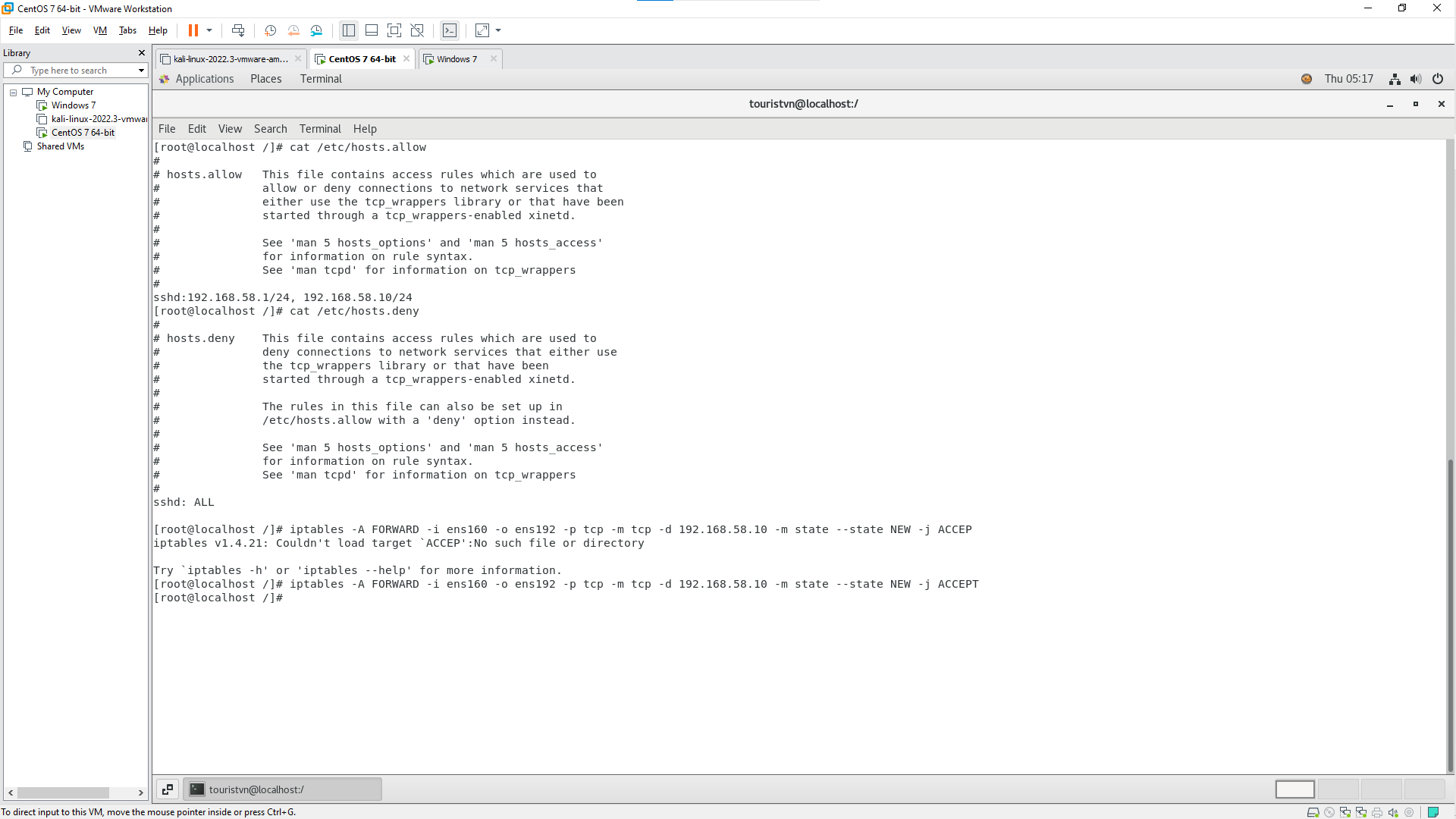
****

Note: x is the two last number of your student ID

Write the following rules:

* Deny all hosts ping to 192.168.x.1/24
* Deny all external traffic (WAN) to SSH and allow only local traffic (192.168.x.10 to 192.168.x.1)
* Accept packets that are part of established connections
* Reject all.

Answer:



END