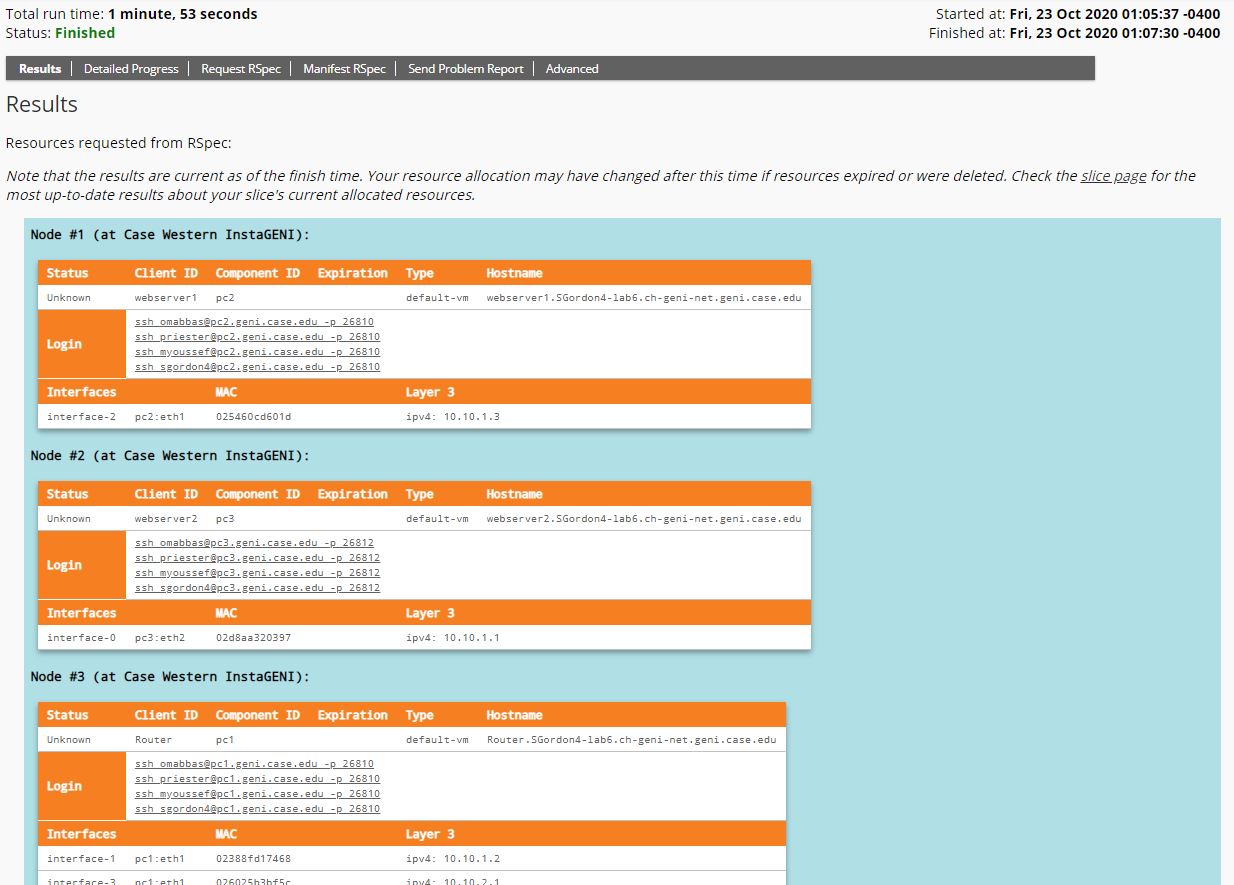
Sean Gordon

CprE 431

Module 6 Lab

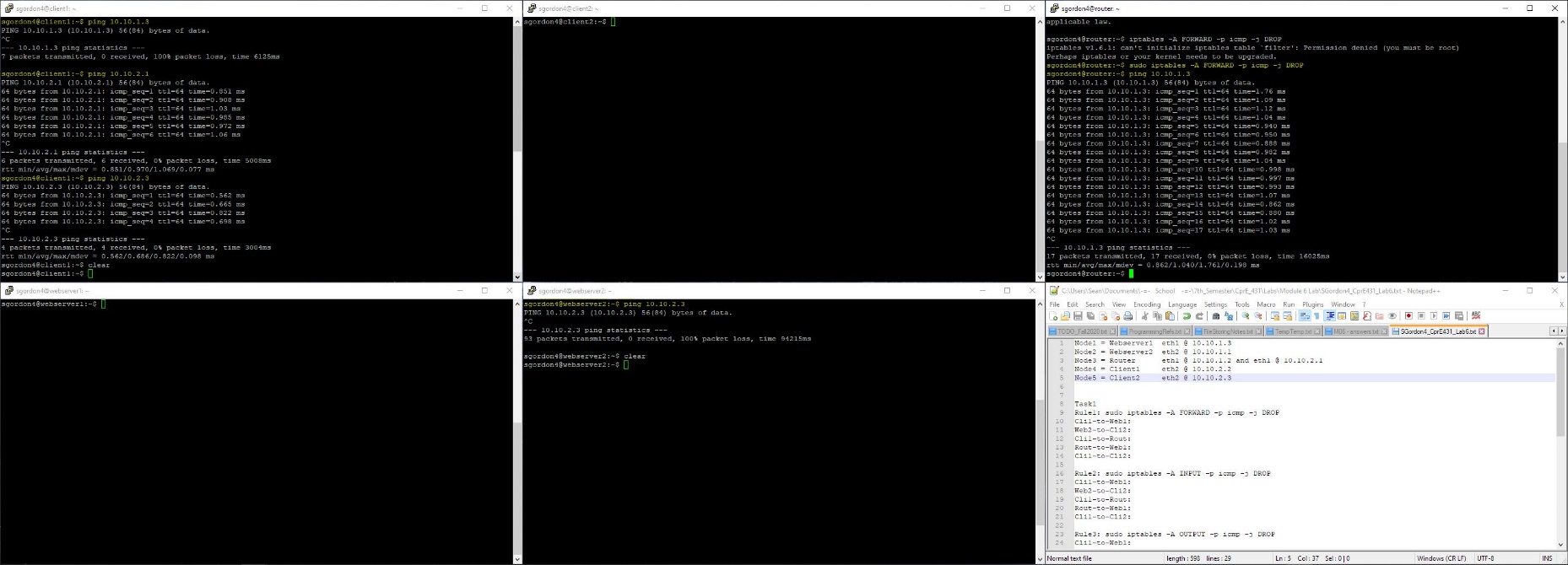
This lab focused on firewall iptables, exploring the different ways to write iptable entries and what rules are necessary for what criteria.

Initial resource allocation and slice:

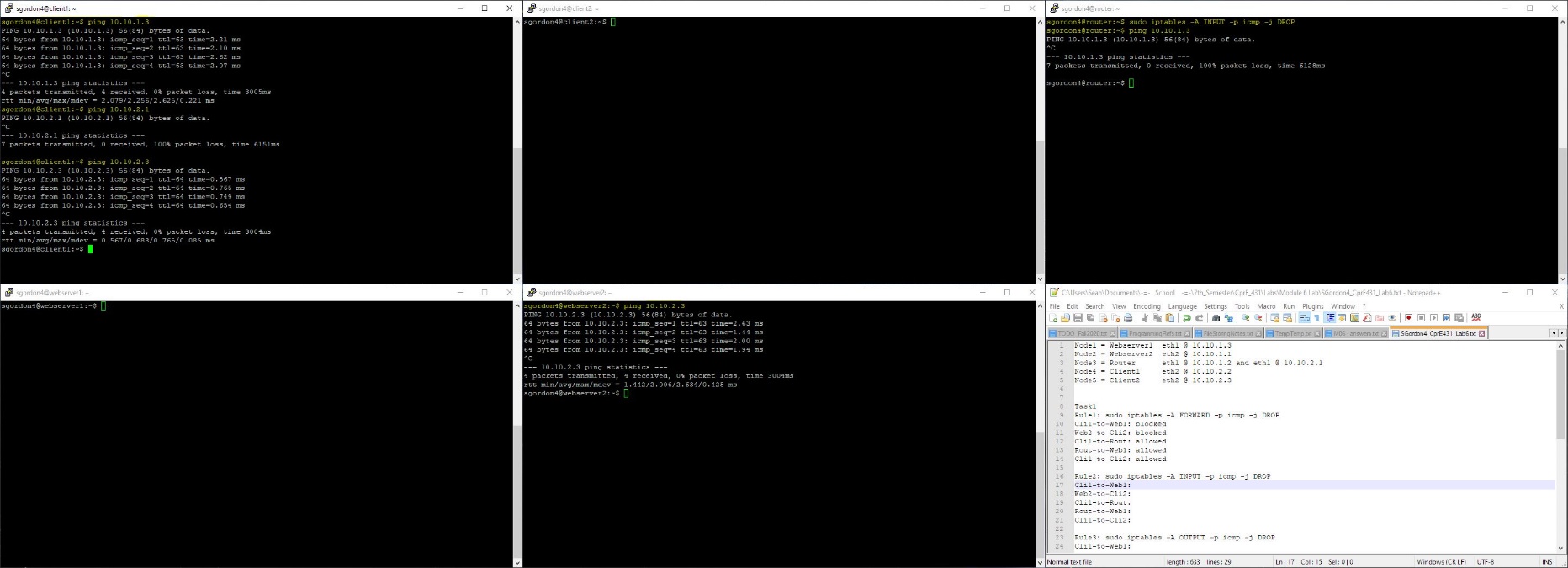




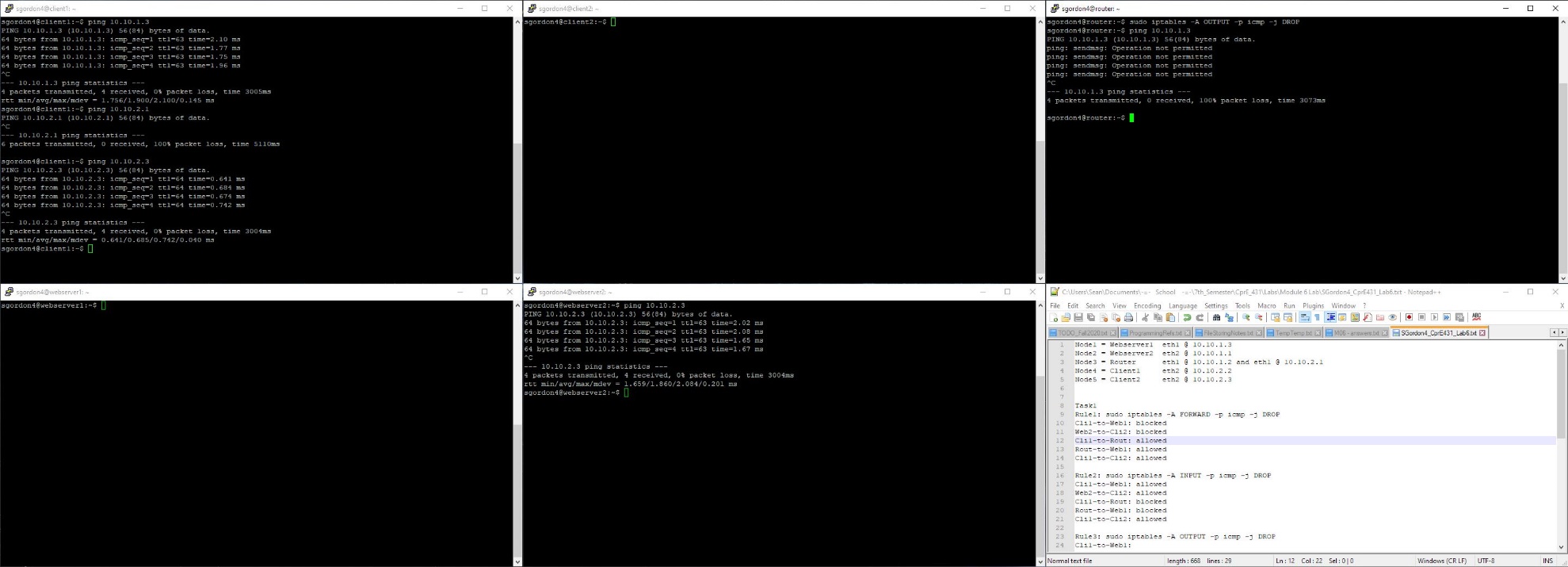
Task 1, part 1



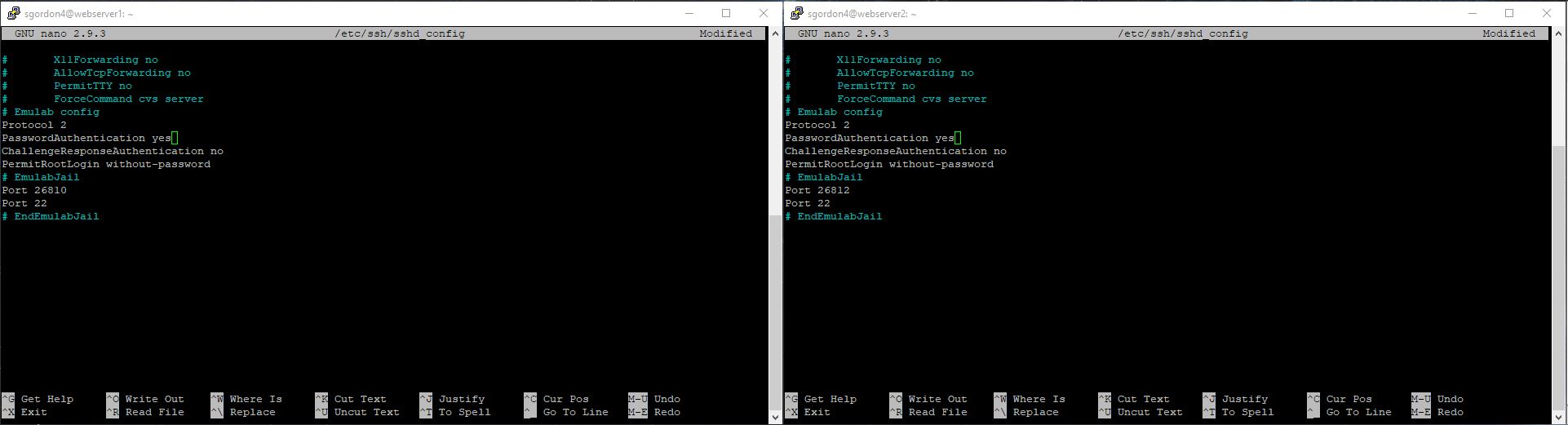
Task 1, part 2



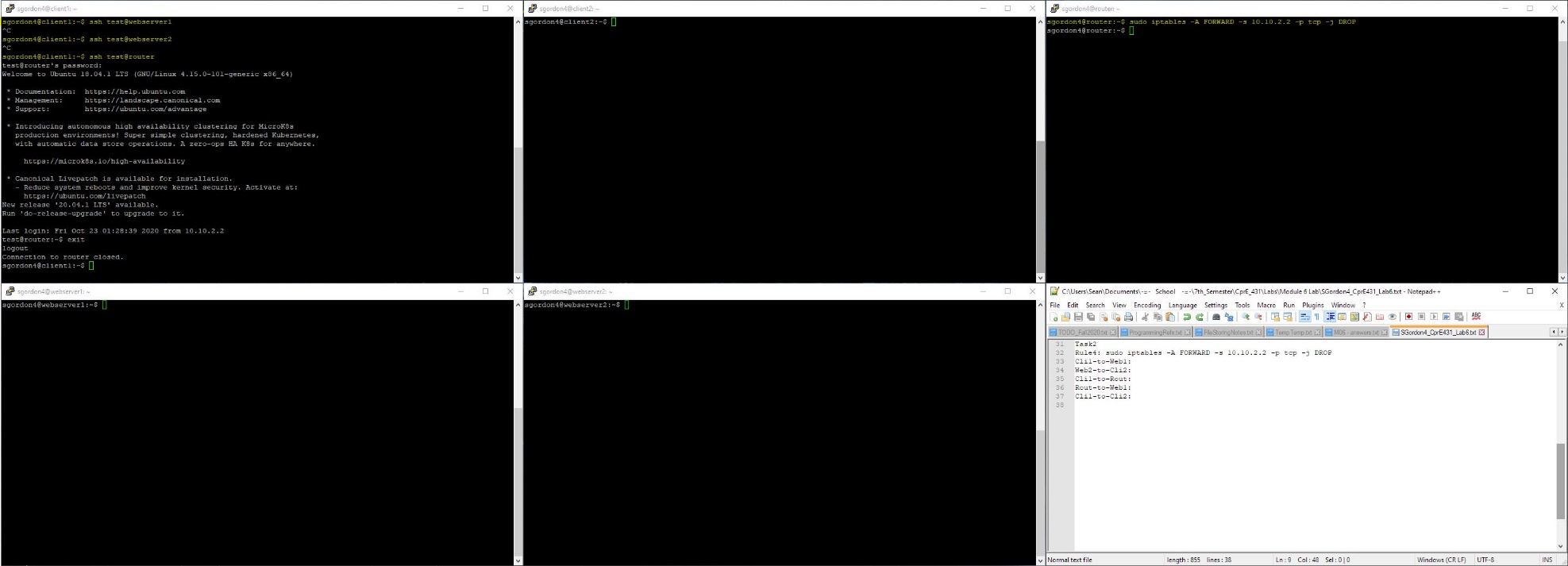
Task 1, part 3



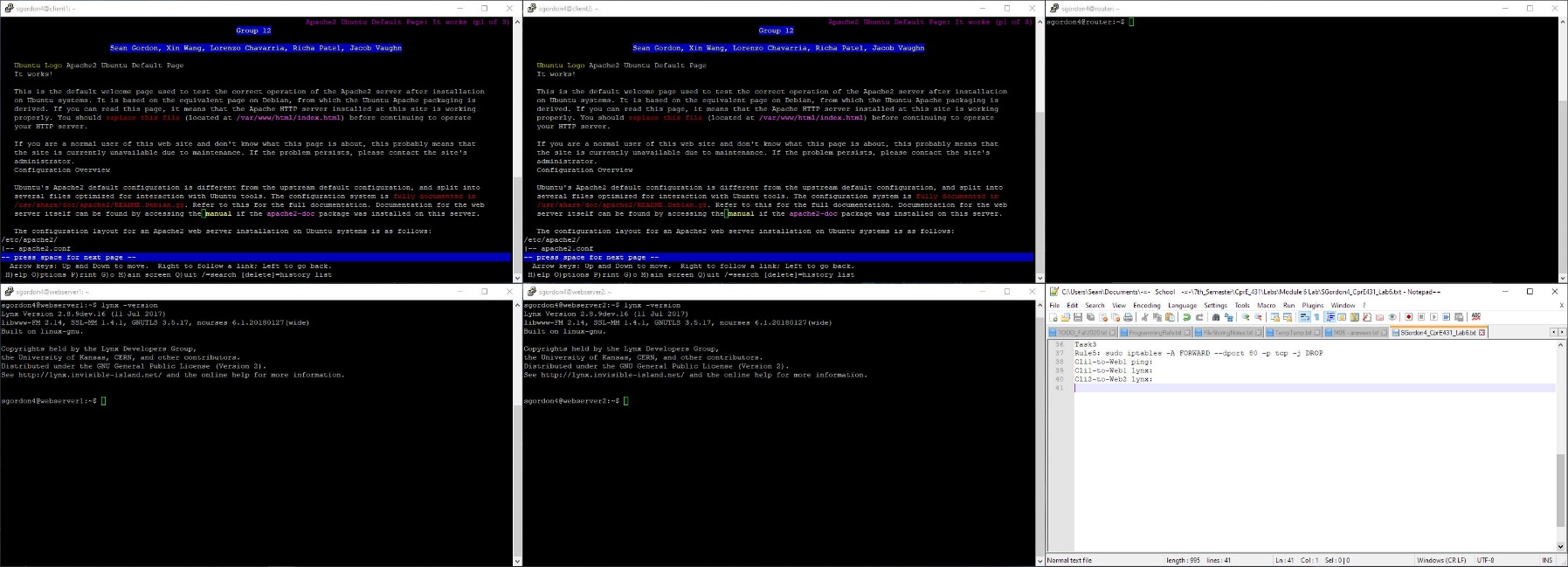
Editing the config files for task 2



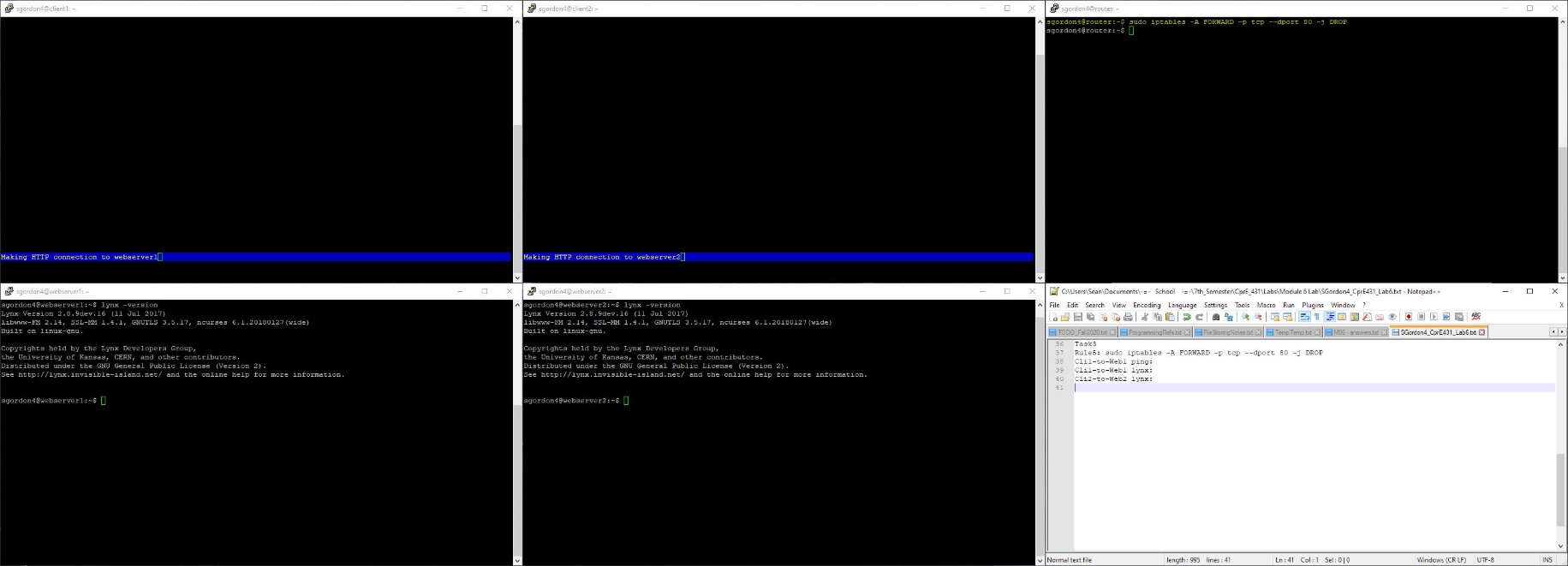
Task 2



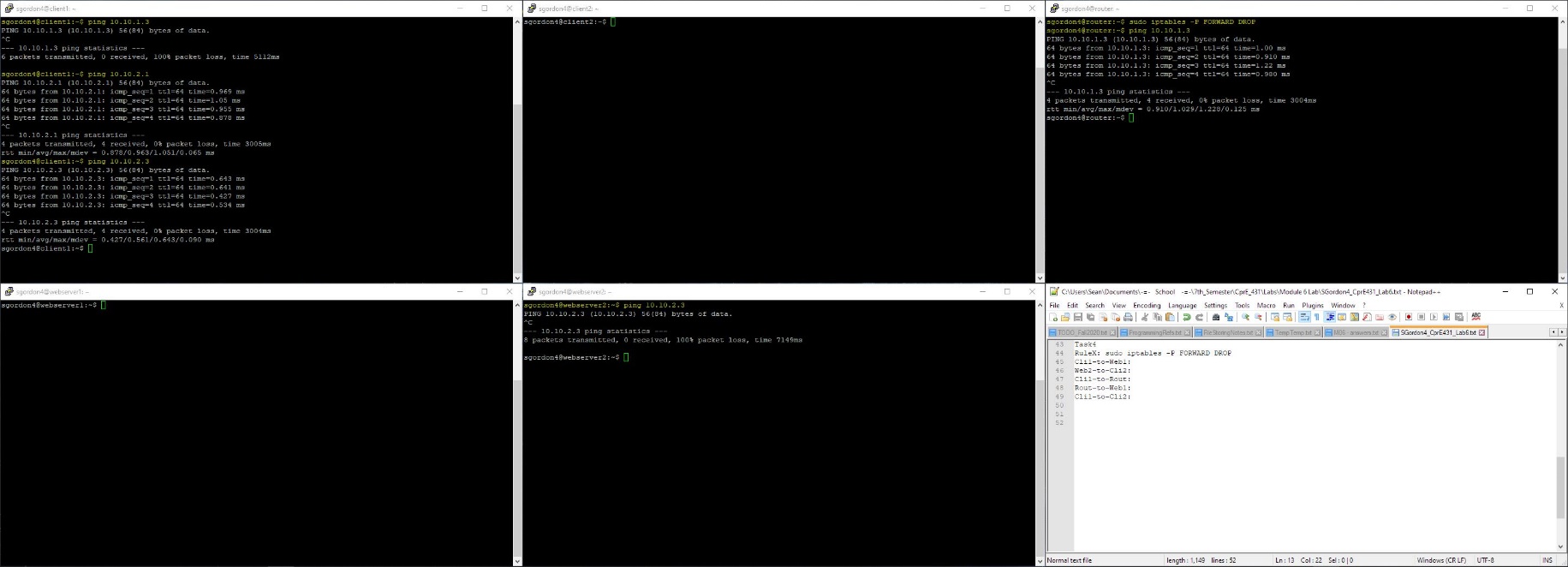
Task 3 pre-rule5



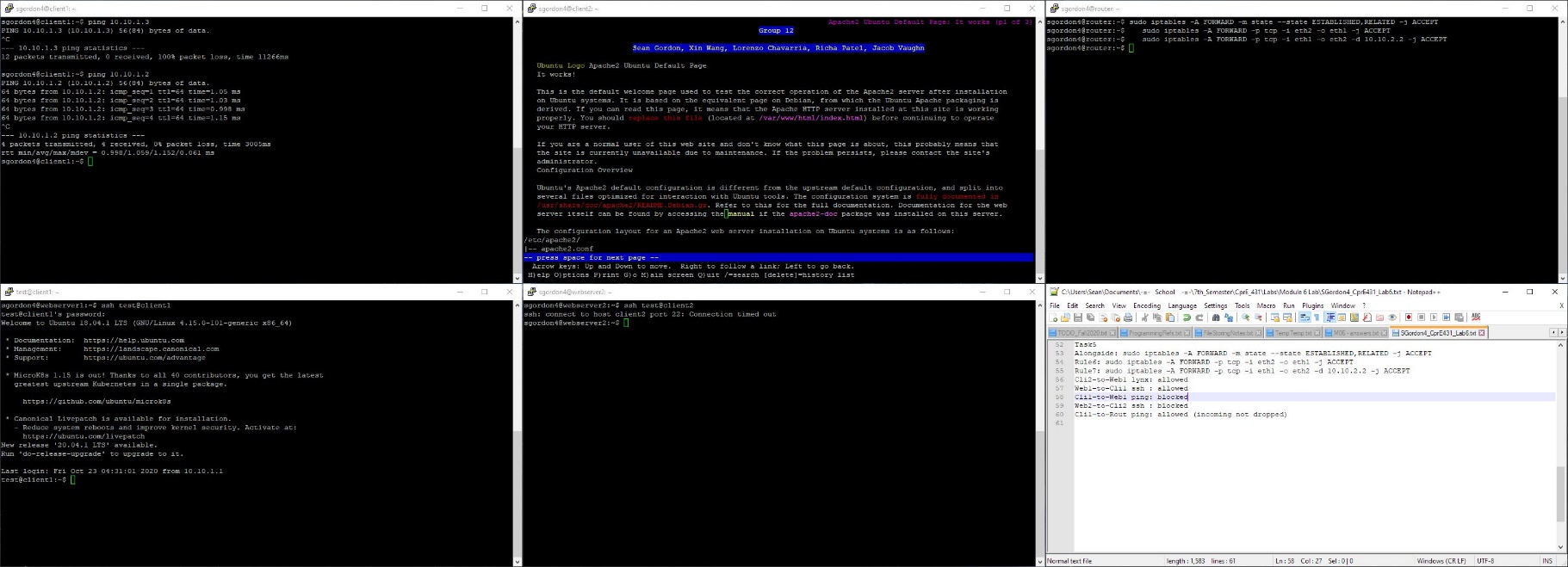
Task 3 post-rule5



Task 4



Task 5



**Resulting Rules:**

Node1 = Webserver1 eth1 @ 10.10.1.3

Node2 = Webserver2 eth2 @ 10.10.1.1

Node3 = Router eth1 @ 10.10.1.2 and eth1 @ 10.10.2.1

Node4 = Client1 eth2 @ 10.10.2.2

Node5 = Client2 eth2 @ 10.10.2.3

**Task1**

Rule1: sudo iptables -A FORWARD -p icmp -j DROP

Cli1-to-Web1: blocked

Web2-to-Cli2: blocked

Cli1-to-Rout: allowed

Rout-to-Web1: allowed

Cli1-to-Cli2: allowed

Rule2: sudo iptables -A INPUT -p icmp -j DROP

Cli1-to-Web1: allowed

Web2-to-Cli2: allowed

Cli1-to-Rout: blocked

Rout-to-Web1: blocked

Cli1-to-Cli2: allowed

Rule3: sudo iptables -A OUTPUT -p icmp -j DROP

Cli1-to-Web1: allowed

Web2-to-Cli2: allowed

Cli1-to-Rout: blocked

Rout-to-Web1: blocked

Cli1-to-Cli2: allowed

Task2

Rule4: sudo iptables -A FORWARD -s 10.10.2.2 -p tcp -j DROP

Client was unable to ssh into webservers 1 and 2, but was able to ssh into the router

Task3

Rule5: sudo iptables -A FORWARD -p tcp --dport 80 -j DROP

Cli1-to-Web1 ping: allowed

Cli1-to-Web1 lynx: blocked

Cli2-to-Web2 lynx: blocked

Task4

RuleX: sudo iptables -P FORWARD DROP

Cli1-to-Web1: blocked

Web2-to-Cli2: blocked

Cli1-to-Rout: allowed

Rout-to-Web1: allowed

Cli1-to-Cli2: allowed

Task5

Alongside: sudo iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

Rule6: sudo iptables -A FORWARD -p tcp -i eth2 -o eth1 -j ACCEPT

Rule7: sudo iptables -A FORWARD -p tcp -i eth1 -o eth2 -d 10.10.2.2 -j ACCEPT

Cli2-to-Web1 lynx: allowed

Web1-to-Cli1 ssh : allowed

Cli1-to-Web1 ping: blocked

Web2-to-Cli2 ssh : blocked

Cli1-to-Rout ping: allowed (incoming not dropped)