Name: Tan Han Nguyen

NetID: TXN200004

Week 11 Lab 1

0. Login

Pre-authentication banner message from server:

| University of Texas at Dallas

| Department of Computer Science

|

| Use of UTD Information Systems is subject to

| the UTD Information Security and Acceptable Use Policy.

|

| Pursuant to Texas Administrative Code 202:

| (1) Unauthorized use is prohibited;

| (2) Usage may be subject to security testing and monitoring;

| (3) Misuse is subject to criminal prosecution; and

| (4) No expectation of privacy except as otherwise provided by applicable

| privacy laws.

|

| ATTENTION: utdnetid != utdnetid@utdallas.edu (UTD != Google!)

|

| \*\*\*\*\* This system will require a connection to the GlobalProtect VPN startin

> g

| on the following dates:

|

| cslinux1.utdallas.edu - June 15, 2020

| cslinux2.utdallas.edu - June 22, 2020

|

| \*\*\*\*\* GlobalProtect VPN Instructions: https://www.utdallas.edu/oit/howto/vpn

> /

|

End of banner message from server

Keyboard-interactive authentication prompts from server:

| Password:

End of keyboard-interactive prompts from server

┌──────────────────────────────────────────────────────────────────────┐

│ • MobaXterm Personal Edition v24.2 • │

│ (SSH client, X server and network tools) │

│ │

│ ⮞ SSH session to txn200004@cslinux2.utdallas.edu │

│ • Direct SSH : ✓ │

│ • SSH compression : ✓ │

│ • SSH-browser : ✓ │

│ • X11-forwarding : ✓ (remote display is forwarded through SSH) │

│ │

│ ⮞ For more info, ctrl+click on help or visit our website. │

└──────────────────────────────────────────────────────────────────────┘

Last login: Mon Oct 28 14:14:48 2024 from 10.50.240.7

\*\*\*---\*\*\*---\*\*\*---\*\*\*---\*\*\*---\*\*\*

csgrads1.utdallas.edu - CentOS Linux 7.9

--All CS Graduate Students should use csgrads1--

cs1.utdallas.edu - CentOS Linux 7.9

cs2.utdallas.edu - CentOS Linux 7.9

\*\*\*---\*\*\*---\*\*\*---\*\*\*---\*\*\*---\*\*\*

This system is for use by CS students who need a general purpose Linux system

to complete homework assignments. Computationally or resource intensive

simulations will be throttled automatically.

Thank you,

CS Lab Manager

cs-labs@utdallas.edu

/scratch disk space can be used for temporary files.

All files within /scratch will be erased on a regular basis (Sunday 0300).

{cslinux2:~} mkdir week11Lab1; cd week11Lab1

1. Try ping command

{cslinux2:~/week11Lab1} ping cs1.utdallas.edu

PING cslinux1.utdallas.edu (10.176.92.15) 56(84) bytes of data.

64 bytes from 10.176.92.15 (10.176.92.15): icmp\_seq=1 ttl=64 time=0.277 ms

64 bytes from 10.176.92.15 (10.176.92.15): icmp\_seq=2 ttl=64 time=0.261 ms

64 bytes from 10.176.92.15 (10.176.92.15): icmp\_seq=3 ttl=64 time=0.562 ms

64 bytes from 10.176.92.15 (10.176.92.15): icmp\_seq=4 ttl=64 time=0.241 ms

64 bytes from 10.176.92.15 (10.176.92.15): icmp\_seq=5 ttl=64 time=0.564 ms

^C

--- cslinux1.utdallas.edu ping statistics ---

5 packets transmitted, 5 received, 0% packet loss, time 4004ms

rtt min/avg/max/mdev = 0.241/0.381/0.564/0.149 ms

{cslinux2:~/week11Lab1} ping www.utdallas.edu

PING utdallas.us-east-2.lb.campuspress.com (3.133.32.155) 56(84) bytes of data.

^C

--- utdallas.us-east-2.lb.campuspress.com ping statistics ---

6 packets transmitted, 0 received, 100% packet loss, time 5000ms

{cslinux2:~/week11Lab1} ping www.google.com

PING www.google.com (142.250.113.105) 56(84) bytes of data.

64 bytes from rs-in-f105.1e100.net (142.250.113.105): icmp\_seq=1 ttl=52 time=3.69 ms

64 bytes from rs-in-f105.1e100.net (142.250.113.105): icmp\_seq=2 ttl=52 time=3.57 ms

64 bytes from rs-in-f105.1e100.net (142.250.113.105): icmp\_seq=3 ttl=52 time=3.46 ms

64 bytes from rs-in-f105.1e100.net (142.250.113.105): icmp\_seq=4 ttl=52 time=3.50 ms

64 bytes from rs-in-f105.1e100.net (142.250.113.105): icmp\_seq=5 ttl=52 time=3.53 ms

^C

--- www.google.com ping statistics ---

5 packets transmitted, 5 received, 0% packet loss, time 4007ms

rtt min/avg/max/mdev = 3.462/3.555/3.695/0.095 ms

2. Try traceroute command

{cslinux2:~/week11Lab1} traceroute -w 3 -q 1 -m 16 www.google.com

traceroute to www.google.com (142.250.113.106), 16 hops max, 60 byte packets

1 gateway (10.176.92.1) 0.759 ms

2 129.110.90.64 (129.110.90.64) 0.646 ms

3 10.222.4.189 (10.222.4.189) 1.850 ms

4 \*

5 10.222.1.2 (10.222.1.2) 1.110 ms

6 \*

7 \*

8 129.110.5.35 (129.110.5.35) 1.310 ms

9 208.76.224.208 (208.76.224.208) 1.299 ms

10 74.200.180.88 (74.200.180.88) 2.160 ms

11 74.200.180.164 (74.200.180.164) 2.382 ms

12 hundredge-0-0-0-24.3791.core1.dall.net.internet2.edu (198.71.47.12) 4.094 ms

13 fourhundredge-0-0-0-48.4079.agg1.dall3.net.internet2.edu (163.253.1.13) 4.236 ms

14 162.252.69.177 (162.252.69.177) 38.105 ms

15 \*

16 142.251.60.44 (142.251.60.44) 2.511 ms

{cslinux2:~/week11Lab1} traceroute -w 3 -q 1 -m 16 www.amazon.com

traceroute to www.amazon.com (108.138.166.151), 16 hops max, 60 byte packets

1 gateway (10.176.92.1) 0.601 ms

2 129.110.90.64 (129.110.90.64) 0.488 ms

3 10.222.4.189 (10.222.4.189) 1.420 ms

4 \*

5 10.222.1.2 (10.222.1.2) 1.036 ms

6 \*

7 \*

8 129.110.5.35 (129.110.5.35) 1.212 ms

9 208.76.224.208 (208.76.224.208) 1.262 ms

10 74.200.180.88 (74.200.180.88) 2.079 ms

11 74.200.180.162 (74.200.180.162) 2.387 ms

12 74.200.189.49 (74.200.189.49) 2.492 ms

13 amazon-2.mus-ix.net (74.200.144.70) 2.826 ms

14 150.222.206.211 (150.222.206.211) 2.975 ms

15 15.230.48.28 (15.230.48.28) 2.363 ms

16 \*

3. Try netstat command

Case 1

{cslinux2:~/week11Lab1} netstat -aont | grep "`hostname -i`:[1-9][0-9]"

tcp 0 0 10.176.92.16:740 10.182.21.15:2049 ESTABLISHED keepalive (9.32/0/0)

tcp 0 0 10.176.92.16:960 10.176.97.11:2049 ESTABLISHED keepalive (4.36/0/0)

tcp 0 1 10.176.92.16:47360 10.176.97.127:514 SYN\_SENT on (25.99/5/0)

tcp 0 0 10.176.92.16:768 10.182.80.20:2049 ESTABLISHED keepalive (14.35/0/0)

tcp 0 0 10.176.92.16:60490 10.160.70.26:389 ESTABLISHED keepalive (6779.91/0/0)

tcp 0 0 10.176.92.16:825 10.182.21.31:2049 ESTABLISHED keepalive (9.25/0/0)

tcp 8 0 10.176.92.16:58274 10.182.68.143:9422 ESTABLISHED off (0.00/0/0)

tcp 0 0 10.176.92.16:765 10.182.21.14:2049 ESTABLISHED keepalive (9.28/0/0)

tcp 0 0 10.176.92.16:57976 10.176.97.176:514 ESTABLISHED off (0.00/0/0)

tcp 0 0 10.176.92.16:22 10.50.240.7:59548 ESTABLISHED keepalive (6222.85/0/0)

tcp 0 0 10.176.92.16:39406 10.182.68.135:9422 ESTABLISHED off (0.00/0/0)

tcp 0 0 10.176.92.16:38198 10.182.68.139:9422 ESTABLISHED off (0.00/0/0)

tcp 0 0 10.176.92.16:34888 10.182.67.9:8086 ESTABLISHED keepalive (0.98/0/0)

tcp 0 0 10.176.92.16:798 10.182.21.40:2049 ESTABLISHED keepalive (9.23/0/0)

tcp 0 0 10.176.92.16:22 10.50.240.7:60969 ESTABLISHED keepalive (7025.65/0/0)

tcp 0 0 10.176.92.16:55050 10.182.68.147:9422 ESTABLISHED off (0.00/0/0)

tcp 0 0 10.176.92.16:832 10.176.97.12:2049 ESTABLISHED keepalive (24.30/0/0)

tcp 0 0 10.176.92.16:22 10.50.240.7:59546 ESTABLISHED keepalive (6190.06/0/0)

tcp 0 0 10.176.92.16:22 10.169.165.135:61591 ESTABLISHED keepalive (6255.60/0/0)

tcp 0 0 10.176.92.16:22 10.50.240.7:60971 ESTABLISHED keepalive (7042.03/0/0)

tcp 0 1 10.176.92.16:47362 10.176.97.127:514 SYN\_SENT on (25.99/5/0)

tcp 0 0 10.176.92.16:22 10.169.165.135:61589 ESTABLISHED keepalive (6255.59/0/0)

tcp 0 0 10.176.92.16:44688 10.182.66.221:9421 ESTABLISHED off (0.00/0/0)

Question 1: Port 22 is for : Secure Shell (SSH), secure logins, file transfers (scp, sftp) and port forwarding

{cslinux2:~/week11Lab1} netstat -aont | grep "`hostname -i`:22" | wc

6 48 614

{cslinux2:~/week11Lab1} netstat -aont | grep "`hostname -i`:22" | wc -l

6

Question 2: There are 6 sessions are using port 22

{cslinux2:~/week11Lab1} netstat -aont | grep "10.50.240.7"

tcp 0 0 10.176.92.16:22 10.50.240.7:59548 ESTABLISHED keepalive (6126.35/0/0)

tcp 0 48 10.176.92.16:22 10.50.240.7:60969 ESTABLISHED on (0.25/0/0)

tcp 0 0 10.176.92.16:22 10.50.240.7:59546 ESTABLISHED keepalive (6093.58/0/0)

tcp 0 0 10.176.92.16:22 10.50.240.7:60971 ESTABLISHED keepalive (6945.55/0/0)

Question 3: My computer’s IP address: 10.50.240.7. Above are sessions with my ip address highlighted.

Case 2:

{cslinux2:~/week11Lab1} netstat -aont | grep "`hostname -i`:2271[0-9]"

Question: Is there any TCP port free? YES all of the port for my NetID is free since there’s no result printed above

Case3:

My NetID: txn200004

My port# range: 22710 – 22719

{cslinux2:~/week11Lab1} netstat -aont | grep "`hostname -i`:2271[0-9]"

As shown above, all of the port# assigned to my NetID are free.

Case 4: Find which port from 10 to 99 being used.

{cslinux2:~/week11Lab1} netstat -aont | grep "`hostname -i`:[1-9][0-9] "

tcp 0 0 10.176.92.16:22 10.50.240.7:59548 ESTABLISHED keepalive (5775.62/0/0)

tcp 0 48 10.176.92.16:22 10.50.240.7:60969 ESTABLISHED on (0.24/0/0)

tcp 0 0 10.176.92.16:22 10.50.240.7:59546 ESTABLISHED keepalive (5742.85/0/0)

tcp 0 0 10.176.92.16:22 10.169.165.135:61591 ESTABLISHED keepalive (5808.39/0/0)

tcp 0 0 10.176.92.16:22 10.50.240.7:60971 ESTABLISHED keepalive (6594.82/0/0)

tcp 0 0 10.176.92.16:22 10.169.165.135:61589 ESTABLISHED keepalive (5808.39/0/0)

Only port 22 is being used at the time of this lab

Case5:

1. Check connection on my computer

[2024-10-28 14:32.37] ~

[Han.DESKTOP-ENTHTDC] ⮞ netstat -aont | grep 10.176.92.16:22

TCP 10.50.240.7:60969 10.176.92.16:22 ESTABLISHED 27476 InHost

TCP 10.50.240.7:60971 10.176.92.16:22 ESTABLISHED 28360 InHost

✓

My IP: 10.50.240.7

CS1 IP: 10.176.92.16

Connect through port#: 22

2. Check connection on cs1

{cslinux2:~/week11Lab1} netstat -aont | grep "10.50.240.7"

tcp 0 0 10.176.92.16:22 10.50.240.7:59548 ESTABLISHED keepalive (5299.41/0/0)

tcp 0 0 10.176.92.16:22 10.50.240.7:60969 ESTABLISHED keepalive (6102.21/0/0)

tcp 0 0 10.176.92.16:22 10.50.240.7:59546 ESTABLISHED keepalive (5266.62/0/0)

tcp 0 0 10.176.92.16:22 10.50.240.7:60971 ESTABLISHED keepalive (6118.58/0/0)

My IP: 10.50.240.7

CS1 IP: 10.176.92.16

Connect through port#: 22

Information from my computer and cs1 matches

4. Try nslookup command

{cslinux2:~/week11Lab1} nslookup www.google.com

Server: 10.182.70.24

Address: 10.182.70.24#53

Non-authoritative answer:

Name: www.google.com

Address: 142.250.114.99

Name: www.google.com

Address: 142.250.114.103

Name: www.google.com

Address: 142.250.114.104

Name: www.google.com

Address: 142.250.114.147

Name: www.google.com

Address: 142.250.114.106

Name: www.google.com

Address: 142.250.114.105

Name: www.google.com

Address: 2607:f8b0:4023:1000::6a

Name: www.google.com

Address: 2607:f8b0:4023:1000::63

Name: www.google.com

Address: 2607:f8b0:4023:1000::68

Name: www.google.com

Address: 2607:f8b0:4023:1000::93

{cslinux2:~/week11Lab1} nslookup www.amazon.com

Server: 10.182.70.24

Address: 10.182.70.24#53

Non-authoritative answer:

www.amazon.com canonical name = tp.47cf2c8c9-frontier.amazon.com.

tp.47cf2c8c9-frontier.amazon.com canonical name = d3ag4hukkh62yn.cloudfront.net.

Name: d3ag4hukkh62yn.cloudfront.net

Address: 108.156.214.21

Name: d3ag4hukkh62yn.cloudfront.net

Address: 2600:9000:2356:a400:7:49a5:5fd4:b121

Name: d3ag4hukkh62yn.cloudfront.net

Address: 2600:9000:2356:b600:7:49a5:5fd4:b121

Name: d3ag4hukkh62yn.cloudfront.net

Address: 2600:9000:2356:ca00:7:49a5:5fd4:b121

Name: d3ag4hukkh62yn.cloudfront.net

Address: 2600:9000:2356:4400:7:49a5:5fd4:b121

Name: d3ag4hukkh62yn.cloudfront.net

Address: 2600:9000:2356:6600:7:49a5:5fd4:b121

Name: d3ag4hukkh62yn.cloudfront.net

Address: 2600:9000:2356:f200:7:49a5:5fd4:b121

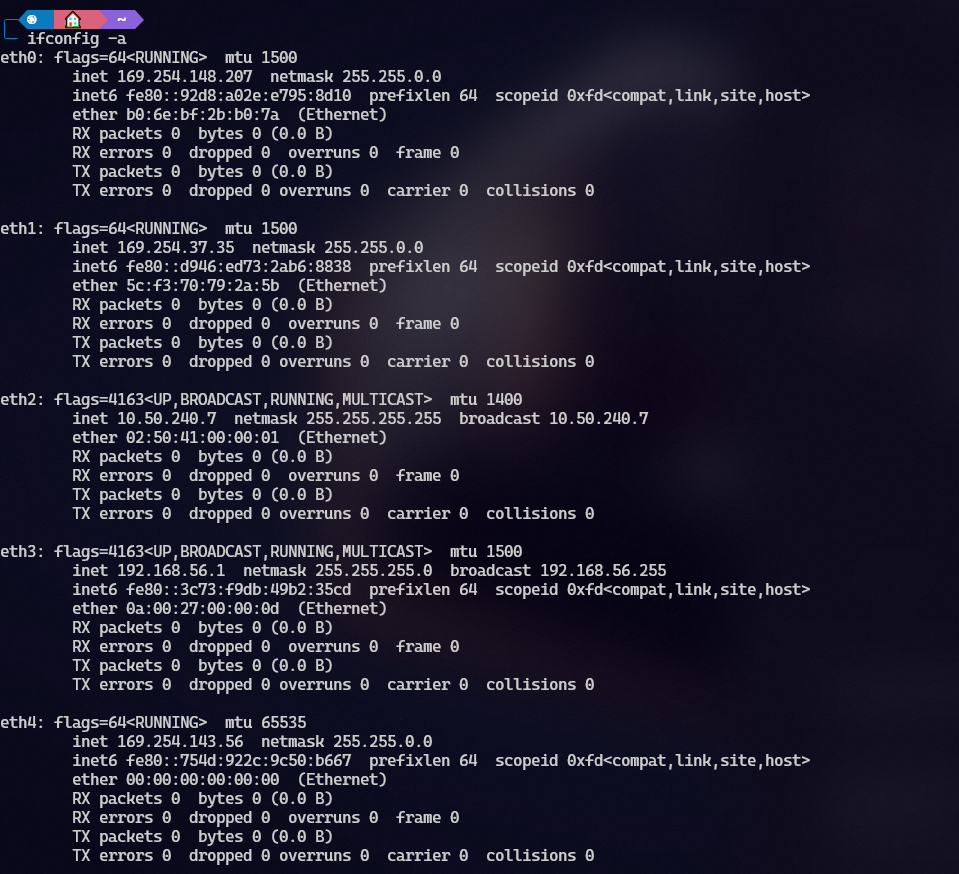
Name: d3ag4hukkh62yn.cloudfront.net

Address: 2600:9000:2356:600:7:49a5:5fd4:b121

Name: d3ag4hukkh62yn.cloudfront.net

Address: 2600:9000:2356:9e00:7:49a5:5fd4:b121

5. Try ifconfig on my computer (Linux) (optional)



End Lab and Exit

{cslinux2:~/week11Lab1} date

Mon Oct 28 14:58:38 CDT 2024

{cslinux2:~/week11Lab1} ls -l

total 0

{cslinux2:~/week11Lab1} uname -a

Linux cslinux2.utdallas.edu 3.10.0-1160.119.1.el7.x86\_64 #1 SMP Tue Jun 4 14:43:51 UTC 2024 x86\_64 x86\_64 x86\_64 GNU/Linux

{cslinux2:~/week11Lab1} exit

logout

───────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────

Session stopped

- Press <Return> to exit tab

- Press R to restart session

- Press S to save terminal output to file