

Lab #6 Report: Network Management
CSC432 – Computer & Network Security
Franklin Nuth
27 February 2018

Abstract

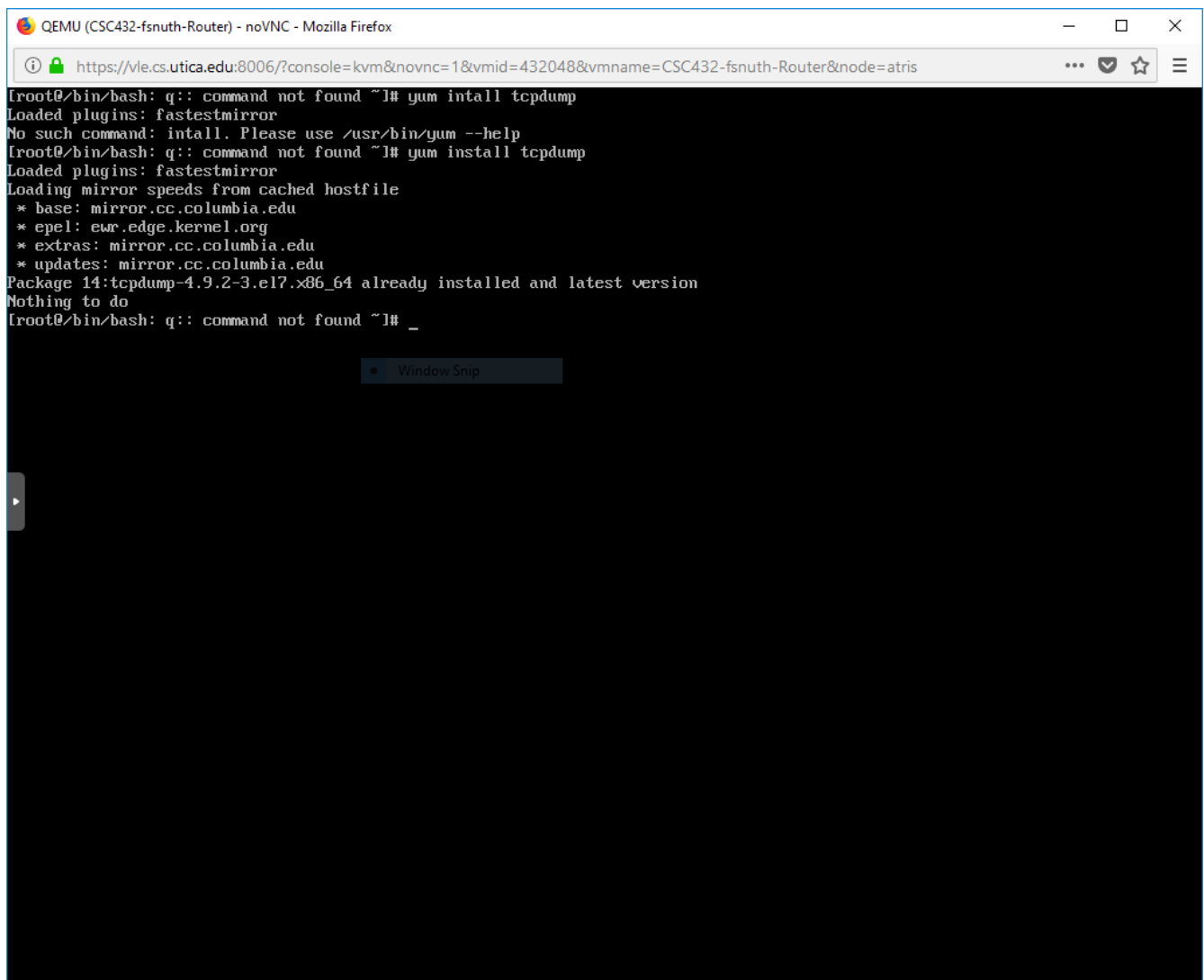
In this lab, I will install **tcpdump** and use it to monitor the network traffic on my internal and external interfaces. The type of traffic that I will monitor includes **SSH** and **HTTP** packets that interacted with the router. In order to study network flow in real time, I will also discuss how to download and use a tool called **argus**. The tool will be used to show how specific **IP** addresses in a network can be listened to for manual supervision of incoming and outgoing traffic. The lab will also include a small demo by one of argus's data clients called **ratop**, which can display data from a network flow.

Introduction

Wireshark is one of the most effective packet sniffers that is free to download for Windows and Linux users. It is used by both security and hackers in equal extremes for monitoring and analyzing traffic traveling through a network. Although not an intrusion detection system, its ability to read all types of packet formats and capture live traffic makes it a powerful analysis tool for individuals of all skill levels. Unfortunately, its capabilities can't be utilized by the Cent OS 7 router. In order for the router to imitate the monitoring capabilities of Wireshark, a spectrum of programs must be installed before monitoring traffic from the Linux router can be possible.

Processes & Screenshots

In order to start sniffing traffic immediately, I first have to download **tcpdump** in the router. I typed "yum install tcpdump" into the command line so I can get the codes I need to use it.



The screenshot shows a web browser window titled "QEMU (CSC432-fsnuth-Router) - noVNC - Mozilla Firefox". The address bar shows the URL: <https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432048&vmname=CSC432-fsnuth-Router&node=atris>. The terminal output is as follows:

```
[root@bin/bash: q:: command not found ~]# yum intall tcpdump
Loaded plugins: fastestmirror
No such command: intall. Please use /usr/bin/yum --help
[root@bin/bash: q:: command not found ~]# yum install tcpdump
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
* base: mirror.cc.columbia.edu
* epel: ewr.edge.kernel.org
* extras: mirror.cc.columbia.edu
* updates: mirror.cc.columbia.edu
Package 14:tcpdump-4.9.2-3.el7.x86_64 already installed and latest version
Nothing to do
[root@bin/bash: q:: command not found ~]# _
```

A "Window Snip" button is visible in the terminal area.

(Downloading tcpdump. According the last couple of lines, I already installed it.)

After installing tcpdump, my goals are to capture traffic going through my private interface and my public interface. For the public interface, I typed “tcpdump -i ens19” and for the private interface I typed “tcpdump -i ens18”.

```
QEMU (CSC432-fsnuth-Router) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432048&vmname=CSC432-fsnuth-Router&node=atris

ns [nop,nop,TS val 669600104 ecr 1173143312], length 0
09:47:24.571979 IP 192.168.0.2.40118 > yyz12s05-in-f3.1e100.net.http: Flags [I], ack 1411, win 251, options [nop,nop,TS val 9650
11833 ecr 978271406], length 0
09:47:24.588527 IP yyz12s05-in-f3.1e100.net.http > 192.168.0.2.40118: Flags [I], ack 855, win 244, options [nop,nop,TS val 97828
1646 ecr 964929117], length 0
09:47:24.828130 IP 192.168.0.2.46502 > 72.21.91.29.http: Flags [I], ack 2364, win 266, options [nop,nop,TS val 3806920406 ecr 91
2048187], length 0
09:47:24.845134 IP 72.21.91.29.http > 192.168.0.2.46502: Flags [I], ack 1294, win 290, options [nop,nop,TS val 912058427 ecr 380
6869268], length 0
09:47:25.116649 IP 192.168.0.2.41174 > iad23s25-in-f14.1e100.net.https: Flags [P], seq 16476:16522, ack 21040, win 606, options
[nop,nop,TS val 3550922158 ecr 1376828106], length 46
09:47:25.116799 IP 192.168.0.2.34808 > server-52-85-105-53.jfk1.r.cloudfront.net.https: Flags [P], seq 868:914, ack 4134, win 3
28, options [nop,nop,TS val 208758368 ecr 1656506896], length 46
09:47:25.131717 IP server-52-85-105-53.jfk1.r.cloudfront.net.https > 192.168.0.2.34808: Flags [P], seq 4134:4180, ack 914, win
126, options [nop,nop,TS val 1656512796 ecr 208758368], length 46
09:47:25.131919 IP 192.168.0.2.34808 > server-52-85-105-53.jfk1.r.cloudfront.net.https: Flags [I], ack 4180, win 328, options [n
op,nop,TS val 208758384 ecr 1656512796], length 0
09:47:25.133011 IP iad23s25-in-f14.1e100.net.https > 192.168.0.2.41174: Flags [P], seq 21040:21086, ack 16522, win 376, options
[nop,nop,TS val 1376887107 ecr 3550922158], length 46
09:47:25.133186 IP 192.168.0.2.41174 > iad23s25-in-f14.1e100.net.https: Flags [I], ack 21086, win 606, options [nop,nop,TS val 3
550922175 ecr 1376887107], length 0
09:47:25.596014 IP 192.168.0.2.40116 > yyz12s05-in-f3.1e100.net.http: Flags [I], ack 1411, win 251, options [nop,nop,TS val 9650
1058 ecr 2180862112], length 0
09:47:25.612253 IP yyz12s05-in-f3.1e100.net.http > 192.168.0.2.40116: Flags [I], ack 855, win 244, options [nop,nop,TS val 21808
72352 ecr 964930324], length 0
09:47:26.620049 IP 192.168.0.2.34894 > server-52-85-105-41.jfk1.r.cloudfront.net.https: Flags [I], ack 362929, win 4316, options
[nop,nop,TS val 1345561898 ecr 442655537], length 0
09:47:26.635206 IP server-52-85-105-41.jfk1.r.cloudfront.net.https > 192.168.0.2.34894: Flags [I], ack 1170, win 126, options [n
op,nop,TS val 442656561 ecr 1345459762], length 0
09:47:28.117730 IP 192.168.0.2.53308 > server-52-85-105-138.jfk1.r.cloudfront.net.https: Flags [P], seq 816:862, ack 5200, win
334, options [nop,nop,TS val 998415321 ecr 442649502], length 46
09:47:28.132376 IP server-52-85-105-138.jfk1.r.cloudfront.net.https > 192.168.0.2.53308: Flags [P], seq 5200:5246, ack 862, win
126, options [nop,nop,TS val 442655403 ecr 998415321], length 46
09:47:28.132571 IP 192.168.0.2.53308 > server-52-85-105-138.jfk1.r.cloudfront.net.https: Flags [I], ack 5246, win 334, options [
nop,nop,TS val 998415336 ecr 442655403], length 0
09:47:29.364452 IP 192.168.0.2.34894 > server-52-85-105-41.jfk1.r.cloudfront.net.https: Flags [P], seq 1170:1201, ack 362929, w
in 4316, options [nop,nop,TS val 1345574867 ecr 442656561], length 31
09:47:29.364575 IP 192.168.0.2.34894 > server-52-85-105-41.jfk1.r.cloudfront.net.https: Flags [F], seq 1201, ack 362929, win 43
16, options [nop,nop,TS val 1345574867 ecr 442656561], length 0
09:47:29.380554 IP server-52-85-105-41.jfk1.r.cloudfront.net.https > 192.168.0.2.34894: Flags [F], seq 362929, ack 1202, win 12
6, options [nop,nop,TS val 442656836 ecr 1345574867], length 0
09:47:29.380772 IP 192.168.0.2.34894 > server-52-85-105-41.jfk1.r.cloudfront.net.https: Flags [I], ack 362930, win 4316, options
[nop,nop,TS val 1345574883 ecr 442656836], length 0
^C
3605 packets captured
3713 packets received by filter
108 packets dropped by kernel
[root@bin/bash: q:: command not found ~]#
```

(Listening to all network traffic being capture by my private interface, ens19)

```
QEMU (CSC432-fsnuth-Router) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432048&vmname=CSC432-fsnuth-Router&node=atris

listening on ens18, link-type EN10MB (Ethernet), capture size 262144 bytes
09:50:05.486773 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:50:07.489622 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:50:09.499007 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:50:11.499085 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:50:13.501816 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:50:15.501134 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:50:17.503927 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:50:19.503193 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:50:21.506260 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:50:23.505632 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:50:25.508534 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:50:27.511383 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:50:29.510778 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:50:31.513634 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:50:33.513248 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:50:35.519750 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:50:37.522223 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:50:39.525266 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:50:41.528060 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:50:43.527478 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:50:45.530393 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:50:47.529829 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:50:49.532612 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:50:51.532011 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:50:53.541270 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:50:55.541277 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:50:57.544295 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:50:59.547069 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:51:01.546453 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:51:03.549395 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:51:05.548690 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:51:07.551593 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:51:09.551025 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:51:11.553863 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:51:13.556735 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:51:15.555949 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:51:17.558990 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:51:19.558611 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:51:21.561316 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:51:23.560775 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:51:25.563646 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
09:51:27.563001 STP 802.1d, Config, Flags Inonet, bridge-id 800a.c8:00:84:00:89:80.801a, length 42
^C
42 packets captured
42 packets received by filter
0 packets dropped by kernel
[root@bin/bash: q:: command not found ~]#
```

(Listening to all network traffic going to my public interface, ens18)

After that, I then went on to typing the commands that will let me listen in on only SSH traffic and HTTP traffic on my private interface. To listen in on SSH traffic, I typed “tcpdump -i ens19 port 22”. For the HTTP traffic, I typed “tcpdump -i ens19 port 80”. Because I know that SSH traffic goes through port 22 and HTTP traffic goes through port 80, I filtered the traffic by port forwarding.

```
QEMU (CSC432-fsnuth-Router) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432048&vmname=CSC432-fsnuth-Router&node=atris

ns [nop,nop,TS val 1100104408 ecr 41548171231, length 100
09:58:11.467869 IP 192.168.0.2.59396 > /bin/bash: q:: command not found.ssh: Flags [I.], ack 2416, win 296, options [nop,nop,TS v
al 4154819137 ecr 1100104408], length 0
09:58:11.467998 IP 192.168.0.2.59396 > /bin/bash: q:: command not found.ssh: Flags [P.], seq 2177:2261, ack 2416, win 296, optio
ns [nop,nop,TS val 4154819137 ecr 1100104408], length 84
09:58:11.468007 IP /bin/bash: q:: command not found.ssh > 192.168.0.2.59396: Flags [I.], ack 2261, win 314, options [nop,nop,TS v
al 1100104408 ecr 4154819137], length 0
09:58:11.479695 IP /bin/bash: q:: command not found.ssh > 192.168.0.2.59396: Flags [P.], seq 2416:2476, ack 2261, win 314, optio
ns [nop,nop,TS val 1100104420 ecr 4154819137], length 60
09:58:11.521939 IP 192.168.0.2.59396 > /bin/bash: q:: command not found.ssh: Flags [I.], ack 2476, win 296, options [nop,nop,TS v
al 4154819149 ecr 1100104420], length 0
09:58:19.246209 IP 192.168.0.2.59396 > /bin/bash: q:: command not found.ssh: Flags [P.], seq 2261:2345, ack 2476, win 296, optio
ns [nop,nop,TS val 4154826915 ecr 1100104420], length 84
09:58:19.270355 IP /bin/bash: q:: command not found.ssh > 192.168.0.2.59396: Flags [P.], seq 2476:2544, ack 2345, win 314, optio
ns [nop,nop,TS val 1100112211 ecr 4154826915], length 68
09:58:19.270560 IP 192.168.0.2.59396 > /bin/bash: q:: command not found.ssh: Flags [I.], ack 2544, win 296, options [nop,nop,TS v
al 4154826939 ecr 1100112211], length 0
09:58:24.054008 IP 192.168.0.2.59396 > /bin/bash: q:: command not found.ssh: Flags [P.], seq 2345:2429, ack 2544, win 296, optio
ns [nop,nop,TS val 4154831723 ecr 1100112211], length 84
09:58:24.060657 IP /bin/bash: q:: command not found.ssh > 192.168.0.2.59396: Flags [P.], seq 2544:2588, ack 2429, win 314, optio
ns [nop,nop,TS val 1100117001 ecr 4154831723], length 44
09:58:24.060900 IP 192.168.0.2.59396 > /bin/bash: q:: command not found.ssh: Flags [I.], ack 2588, win 296, options [nop,nop,TS v
al 4154831730 ecr 1100117001], length 0
09:58:24.061030 IP 192.168.0.2.59396 > /bin/bash: q:: command not found.ssh: Flags [P.], seq 2429:2513, ack 2588, win 296, optio
ns [nop,nop,TS val 4154831730 ecr 1100117001], length 84
09:58:24.064934 IP /bin/bash: q:: command not found.ssh > 192.168.0.2.59396: Flags [P.], seq 2588:2616, ack 2513, win 314, optio
ns [nop,nop,TS val 1100117005 ecr 4154831730], length 28
09:58:24.065227 IP 192.168.0.2.59396 > /bin/bash: q:: command not found.ssh: Flags [P.], seq 2513:2625, ack 2616, win 296, optio
ns [nop,nop,TS val 4154831734 ecr 1100117005], length 112
09:58:24.105290 IP /bin/bash: q:: command not found.ssh > 192.168.0.2.59396: Flags [I.], ack 2625, win 314, options [nop,nop,TS v
al 1100117046 ecr 4154831734], length 0
09:58:24.273411 IP /bin/bash: q:: command not found.ssh > 192.168.0.2.59396: Flags [P.], seq 2616:2660, ack 2625, win 314, optio
ns [nop,nop,TS val 1100117214 ecr 4154831734], length 44
09:58:24.273792 IP 192.168.0.2.59396 > /bin/bash: q:: command not found.ssh: Flags [P.], seq 2625:3085, ack 2660, win 296, optio
ns [nop,nop,TS val 4154831942 ecr 1100117214], length 460
09:58:24.273806 IP /bin/bash: q:: command not found.ssh > 192.168.0.2.59396: Flags [I.], ack 3085, win 357, options [nop,nop,TS v
al 1100117214 ecr 4154831942], length 0
09:58:24.290571 IP /bin/bash: q:: command not found.ssh > 192.168.0.2.59396: Flags [P.], seq 2660:2768, ack 3085, win 357, optio
ns [nop,nop,TS val 1100117231 ecr 4154831942], length 108
09:58:24.299998 IP /bin/bash: q:: command not found.ssh > 192.168.0.2.59396: Flags [P.], seq 2768:3004, ack 3085, win 357, optio
ns [nop,nop,TS val 1100117240 ecr 4154831942], length 236
09:58:24.300269 IP 192.168.0.2.59396 > /bin/bash: q:: command not found.ssh: Flags [I.], ack 3004, win 319, options [nop,nop,TS v
al 4154831969 ecr 1100117231], length 0
09:58:24.321049 IP /bin/bash: q:: command not found.ssh > 192.168.0.2.59396: Flags [P.], seq 3004:3136, ack 3085, win 357, optio
ns [nop,nop,TS val 1100117261 ecr 4154831969], length 132
09:58:24.361993 IP 192.168.0.2.59396 > /bin/bash: q:: command not found.ssh: Flags [I.], ack 3136, win 342, options [nop,nop,TS v
al 4154831990 ecr 1100117261], length 0
```

(tcpdump sniffing for SSH traffic.)

```
QEMU (CSC432-fsnuth-Router) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432048&vmname=CSC432-fsnuth-Router&node=atris

TS val 4016273644 ecr 3039860961, length 0
10:00:40.734504 IP /bin/bash: q:: command not found.46868 > 204.237.142.160.http: Flags [I], ack 869, win 242, options [nop,nop,
TS val 4016273644 ecr 3039860951, length 0
10:00:40.754914 IP 204.237.142.160.http > /bin/bash: q:: command not found.46868: Flags [I], ack 432, win 235, options [nop,nop,
TS val 303996336 ecr 40162636051, length 0
10:00:40.755065 IP 204.237.142.160.http > /bin/bash: q:: command not found.46866: Flags [I], ack 432, win 235, options [nop,nop,
TS val 303996336 ecr 40162636051, length 0
10:00:41.173100 IP a1plpkivs-v03.any.prod.ash1.secureserver.net.http > /bin/bash: q:: command not found.54468: Flags [R], seq 21
06176804, win 0, length 0
10:00:41.173288 IP a1plpkivs-v03.any.prod.ash1.secureserver.net.http > /bin/bash: q:: command not found.54466: Flags [R], seq 22
60319160, win 0, length 0
10:00:41.246433 IP /bin/bash: q:: command not found.51566 > 72.37.164.105.http: Flags [I], ack 769, win 245, options [nop,nop,TS
val 2528001649 ecr 4632019941, length 0
10:00:41.248456 IP /bin/bash: q:: command not found.54462 > a1plpkivs-v03.any.prod.ash1.secureserver.net.http: Flags [F.I], seq 1
, ack 1, win 229, options [nop,nop,TS val 3475279150 ecr 11136988951, length 0
10:00:41.248561 IP /bin/bash: q:: command not found.54464 > a1plpkivs-v03.any.prod.ash1.secureserver.net.http: Flags [F.I], seq 1
, ack 1, win 229, options [nop,nop,TS val 3475279150 ecr 11136820141, length 0
10:00:41.266083 IP 72.37.164.105.http > /bin/bash: q:: command not found.51566: Flags [I], ack 577, win 243, options [nop,nop,TS
val 463212234 ecr 25279580381, length 0
10:00:41.314530 IP a1plpkivs-v03.any.prod.ash1.secureserver.net.http > /bin/bash: q:: command not found.54462: Flags [F.I], seq 1
ack 2, win 227, options [nop,nop,TS val 1113704033 ecr 34752791501, length 0
10:00:41.314610 IP a1plpkivs-v03.any.prod.ash1.secureserver.net.http > /bin/bash: q:: command not found.54464: Flags [F.I], seq 1
ack 2, win 227, options [nop,nop,TS val 1113687152 ecr 34752791501, length 0
10:00:41.314774 IP /bin/bash: q:: command not found.54462 > a1plpkivs-v03.any.prod.ash1.secureserver.net.http: Flags [I], ack 2,
win 229, options [nop,nop,TS val 3475279216 ecr 11137040331, length 0
10:00:41.314824 IP /bin/bash: q:: command not found.54464 > a1plpkivs-v03.any.prod.ash1.secureserver.net.http: Flags [I], ack 2,
win 229, options [nop,nop,TS val 3475279216 ecr 11136871521, length 0
10:00:46.110479 IP /bin/bash: q:: command not found.40220 > yyz12s05-in-f3.1e100.net.http: Flags [I], ack 2821, win 273, options
[nop,nop,TS val 965812686 ecr 30461722791, length 0
10:00:46.110627 IP /bin/bash: q:: command not found.40200 > yyz12s05-in-f3.1e100.net.http: Flags [I], ack 706, win 240, options
[nop,nop,TS val 965812712 ecr 25868529141, length 0
10:00:46.126643 IP yyz12s05-in-f3.1e100.net.http > /bin/bash: q:: command not found.40220: Flags [I], ack 1709, win 252, options
[nop,nop,TS val 3046182485 ecr 9658126861, length 0
10:00:46.126724 IP yyz12s05-in-f3.1e100.net.http > /bin/bash: q:: command not found.40200: Flags [I], ack 420, win 240, options
[nop,nop,TS val 2586863014 ecr 9658127121, length 0
10:00:46.173467 IP a1plpkivs-v03.any.prod.ash1.secureserver.net.http > /bin/bash: q:: command not found.54464: Flags [R], seq 69
3308780, win 0, length 0
10:00:46.173546 IP a1plpkivs-v03.any.prod.ash1.secureserver.net.http > /bin/bash: q:: command not found.54462: Flags [R], seq 35
29711483, win 0, length 0
10:00:47.390415 IP /bin/bash: q:: command not found.35816 > 204.237.142.177.http: Flags [I], ack 1738, win 256, options [nop,nop
,TS val 532473248 ecr 6558751351, length 0
10:00:47.410056 IP 204.237.142.177.http > /bin/bash: q:: command not found.35816: Flags [I], ack 864, win 243, options [nop,nop,
TS val 655885375 ecr 5324631561, length 0
^C
143 packets captured
143 packets received by filter
0 packets dropped by kernel
[root@bin/bash: q:: command not found ~]#
```

(tcpdump sniffing for HTTP traffic.)

After using **tcpdump**, I moved on to download and use a tool called **argus**. Argus is a network monitoring tool that can provide information about active network flows. Because the **argus** package is not in the **yum** repository, I have to download other components to build it back up. I did this by typing “yum install gcc make bison libpcap libpcap-devel readline-devel flex”.

```
QEMU (CSC432-fsnuth-Router) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432048&vmname=CSC432-fsnuth-Router&node=atris

Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Updating      : ncurses-base-5.9-14.20130511.el7_4.noarch                      1/15
  Updating      : ncurses-libs-5.9-14.20130511.el7_4.x86_64                    2/15
  Installing    : ncurses-devel-5.9-14.20130511.el7_4.x86_64                  3/15
  Updating      : readline-6.2-10.el7.x86_64                                  4/15
  Updating      : libcap-2.22-9.el7.x86_64                                     5/15
  Installing    : libcap-devel-2.22-9.el7.x86_64                             6/15
  Installing    : readline-devel-6.2-10.el7.x86_64                           7/15
  Updating      : ncurses-5.9-14.20130511.el7_4.x86_64                       8/15
  Installing    : flex-2.5.37-6.el7.x86_64                                    9/15
  Installing    : bison-3.0.4-2.el7.x86_64                                   10/15
  Cleanup       : ncurses-5.9-13.20130511.el7.x86_64                         11/15
  Cleanup       : readline-6.2-9.el7.x86_64                                  12/15
  Cleanup       : ncurses-libs-5.9-13.20130511.el7.x86_64                   13/15
  Cleanup       : ncurses-base-5.9-13.20130511.el7.noarch                   14/15
  Cleanup       : libcap-2.22-8.el7.x86_64                                   15/15
  Verifying     : bison-3.0.4-2.el7.x86_64                                   1/15
  Verifying     : libcap-2.22-9.el7.x86_64                                   2/15
  Verifying     : ncurses-devel-5.9-14.20130511.el7_4.x86_64                3/15
  Verifying     : ncurses-libs-5.9-14.20130511.el7_4.x86_64                4/15
  Verifying     : libcap-devel-2.22-9.el7.x86_64                           5/15
  Verifying     : flex-2.5.37-6.el7.x86_64                                  6/15
  Verifying     : readline-6.2-10.el7.x86_64                               7/15
  Verifying     : ncurses-5.9-14.20130511.el7_4.x86_64                     8/15
  Verifying     : readline-devel-6.2-10.el7.x86_64                         9/15
  Verifying     : ncurses-base-5.9-14.20130511.el7_4.noarch                10/15
  Verifying     : readline-6.2-9.el7.x86_64                                11/15
  Verifying     : ncurses-5.9-13.20130511.el7.x86_64                      12/15
  Verifying     : libcap-2.22-8.el7.x86_64                                  13/15
  Verifying     : ncurses-libs-5.9-13.20130511.el7.x86_64                  14/15
  Verifying     : ncurses-base-5.9-13.20130511.el7.noarch                  15/15

Installed:
  bison.x86_64 0:3.0.4-2.el7 flex.x86_64 0:2.5.37-6.el7 libcap-devel.x86_64 0:2.22-9.el7 readline-devel.x86_64 0:6.2-10.el7

Dependency Installed:
  ncurses-devel.x86_64 0:5.9-14.20130511.el7_4

Dependency Updated:
  libcap.x86_64 0:2.22-9.el7 ncurses.x86_64 0:5.9-14.20130511.el7_4
  ncurses-base.noarch 0:5.9-14.20130511.el7_4 ncurses-libs.x86_64 0:5.9-14.20130511.el7_4
  readline.x86_64 0:6.2-10.el7

Complete!
[root@/bin/bash: q:: command not found ~]#
```

(Installing all the packages needed for Argus.)

After that, I downloaded all the source code needed to run Argus. There are two types of files I needed to download. I needed to get the latest version of Argus as well as the client component, then compile them afterward.


```
QEMU (CSC432-fsnuth-Router) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432048&vmname=CSC432-fsnuth-Router&node=atris

checking for endpwent... yes
checking for floor... no
checking for gethostbyaddr... yes
checking for gethostbyname... yes
checking for getpass... yes
checking for gettimeofday... yes
checking for inet_ntoa... yes
checking for isascii... yes
checking for localtime_r... yes
checking for memchr... yes
checking for memmove... yes
checking for memset... yes
checking for mkdir... yes
checking for modf... yes
checking for pow... no
checking for putenv... yes
checking for realpath... yes
checking for regcomp... yes
checking for select... yes
checking for setenv... yes
checking for socket... yes
checking for sqrt... no
checking for strcasecmp... yes
checking for strchr... yes
checking for strdup... yes
checking for strlcat... no
checking for strncasecmp... yes
checking for strpbrk... yes
checking for strchr... yes
checking for strstr... yes
checking for strtol... yes
checking for sranddev... no
checking for tzset... yes
checking for .threads... yes
checking for sched_get_priority_min... yes
checking for local tcp_wrappers library... not found
checking for system tcp_wrappers library... checking tcpd.h usability... no
checking tcpd.h presence... no
checking for tcpd.h... no
checking for local pcap library... not found
checking for pcap-config... no
checking for main in -lpcap... no
not found
checking for main in -lpcap... (cached) no
checking for local pcap library... no
configure: error: see the INSTALL doc for more info
[root@bin/bash: q:: command not found argus-3.0.8.2]# cd
[root@bin/bash: q:: command not found ~]# _
```

(Installing Argus with “cd /usr/src”, “yum install wget”, “wget <http://qosient.com/argus/src/argus-3.0.8.2.tar.gz>”, and “tar -xaf argus-3.0.8.2.tar.gz”),

```
QEMU (CSC432-fsnuth-Router) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432048&vmname=CSC432-fsnuth-Router&node=atris

checking for sranddev... no
checking for tzset... yes
checking for .threads... yes
checking for sched_get_priority_min... yes
checking for local tcp_wrappers library... not found
checking for system tcp_wrappers library... no
checking for xdrmem_create... yes
checking ncurses.h usability... yes
checking ncurses.h presence... yes
checking for ncurses.h... yes
checking for initscr in -lncurses... yes
checking for GeoIP_open in -lGeoIP... no
checking for standard GeoIP installation... no
checking for local GeoIP library and includes... no
checking for GeoIP library... not found
checking tm_gmtoff in struct tm... yes
checking sys_errlist in stdio.h... yes
configure: creating ./config.status
config.status: creating Makefile
config.status: creating ./common/Makefile
config.status: creating ./include/Makefile
config.status: creating ./clients/Makefile
config.status: creating ./lib/argus-clients.pc
config.status: creating ./examples/Makefile
config.status: creating ./examples/raconvert/Makefile
config.status: creating ./examples/radark/Makefile
config.status: creating ./examples/radecode/Makefile
config.status: creating ./examples/radump/Makefile
config.status: creating ./examples/raevent/Makefile
config.status: creating ./examples/rafilter/Makefile
config.status: creating ./examples/ragraph/Makefile
config.status: creating ./examples/ragrep/Makefile
config.status: creating ./examples/rahisto/Makefile
config.status: creating ./examples/rahosts/Makefile
config.status: creating ./examples/ralabel/Makefile
config.status: creating ./examples/rapath/Makefile
config.status: creating ./examples/rapolicy/Makefile
config.status: creating ./examples/raports/Makefile
config.status: creating ./examples/rarpwatch/Makefile
config.status: creating ./examples/raservices/Makefile
config.status: creating ./examples/rastream/Makefile
config.status: creating ./examples/rastrip/Makefile
config.status: creating ./examples/ratop/Makefile
config.status: creating ./examples/ratimerange/Makefile
config.status: creating ./examples/ratemplate/Makefile
config.status: creating include/argus_config.h
config.status: include/argus_config.h is unchanged
[root@bin/bash: q:: command not found argus-clients-3.0.8.2]#
```

(Installing Argus with “cd /usr/src”, “yum install wget”, “wget <http://qosient.com/argus/src/argus-clients-3.0.8.2.tar.gz>”, and “tar -xaf argus-clients-3.0.8.2.tar.gz”)

```
QEMU (CSC432-fsnuth-Router) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432048&vmname=CSC432-fsnuth-Router&node=atris

make[1]: Entering directory `/usr/src/argus-3.0.8.2'
./config/mkinstalldirs \
    /usr/local/share/doc/argus-3.0 /usr/local/argus/archive
mkdir /usr/local/share/doc/argus-3.0
mkdir /usr/local/argus/archive
make[1]: Leaving directory `/usr/src/argus-3.0.8.2'
[ -d /usr/local ] || \
    (mkdir -p /usr/local; chmod 755 /usr/local)
[ -d /usr/local/sbin ] || \
    (mkdir -p /usr/local/sbin; chmod 755 /usr/local/sbin)
[ -d /usr/local/bin ] || \
    (mkdir -p /usr/local/bin; chmod 755 /usr/local/bin)
[ -d /usr/local/argus ] || \
    (mkdir -p /usr/local/argus; chmod 755 /usr/local/argus)
[ -d /usr/local/argus/archive ] || \
    (mkdir -p /usr/local/argus/archive; chmod 755 /usr/local/argus/archive)
### Make install in /usr/src/argus-3.0.8.2/common
make[1]: Entering directory `/usr/src/argus-3.0.8.2/common'
make[1]: Nothing to be done for `install'.
make[1]: Leaving directory `/usr/src/argus-3.0.8.2/common'
### Done with /usr/src/argus-3.0.8.2/common
# Make install in /usr/src/argus-3.0.8.2/argus
make[1]: Entering directory `/usr/src/argus-3.0.8.2/argus'
[ -d /usr/local/sbin ] || \
    (mkdir -p /usr/local/sbin; chmod 755 /usr/local/sbin)
/bin/install -c ../bin/argus /usr/local/sbin/argus
make[1]: Leaving directory `/usr/src/argus-3.0.8.2/argus'
### Done with /usr/src/argus-3.0.8.2/argus
### Make install in /usr/src/argus-3.0.8.2/events
make[1]: Entering directory `/usr/src/argus-3.0.8.2/events'
[ -d /usr/local/sbin ] || \
    (mkdir -p /usr/local/sbin; chmod 755 /usr/local/sbin)
/bin/install -c ../bin/argus-extip /usr/local/bin/argus-extip
/bin/install -c ../bin/argus-lsof /usr/local/bin/argus-lsof
/bin/install -c ../bin/argus-snmp /usr/local/bin/argus-snmp
/bin/install -c ../bin/argus-vmstat /usr/local/bin/argus-vmstat
make[1]: Leaving directory `/usr/src/argus-3.0.8.2/events'
### Done with /usr/src/argus-3.0.8.2/events
/bin/install -c -m 0755 ./bin/argusbug /usr/local/bin/argusbug
[ -d /usr/local/share/man ] || \
    (mkdir -p /usr/local/share/man; chmod 755 /usr/local/share/man)
[ -d /usr/local/share/man/man5 ] || \
    (mkdir -p /usr/local/share/man/man5; chmod 755 /usr/local/share/man/man5)
[ -d /usr/local/share/man/man8 ] || \
    (mkdir -p /usr/local/share/man/man8; chmod 755 /usr/local/share/man/man8)
/bin/install -c -m 0644 ./man/man5/argus.conf.5 /usr/local/share/man/man5/argus.conf.5
/bin/install -c -m 0644 ./man/man8/argus.8 /usr/local/share/man/man8/argus.8
[root@bin/bash: q:: command not found argus-3.0.8.2]#
```

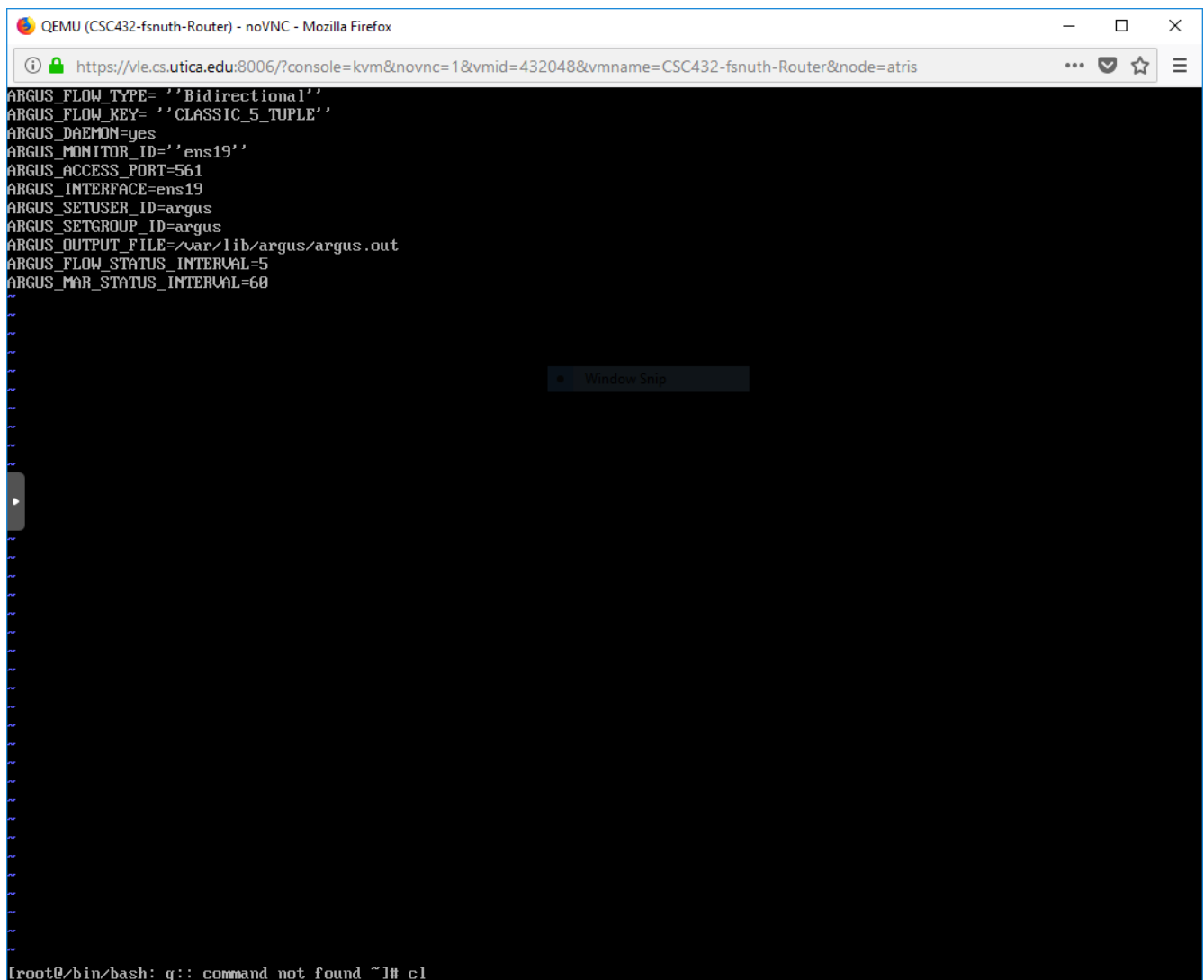
(Compiling Argus with “cd /usr/src/argus-3.0.8.2”, “./configure”, “make && make install”.)

```
QEMU (CSC432-fsnuth-Router) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432048&vmname=CSC432-fsnuth-Router&node=atris

/usr/local/share/man/man1/ralabel.1
/bin/install -c -m 0644 ./man/man1/ranonymize.1 \
/usr/local/share/man/man1/ranonymize.1
/bin/install -c -m 0644 ./man/man1/rapath.1 \
/usr/local/share/man/man1/rapath.1
/bin/install -c -m 0644 ./man/man1/rapolicy.1 \
/usr/local/share/man/man1/rapolicy.1
/bin/install -c -m 0644 ./man/man1/rasort.1 \
/usr/local/share/man/man1/rasort.1
/bin/install -c -m 0644 ./man/man1/rasplit.1 \
/usr/local/share/man/man1/rasplit.1
/bin/install -c -m 0644 ./man/man1/rasql.1 \
/usr/local/share/man/man1/rasql.1
/bin/install -c -m 0644 ./man/man1/rasqlinsert.1 \
/usr/local/share/man/man1/rasqlinsert.1
/bin/install -c -m 0644 ./man/man1/rasqltimeindex.1 \
/usr/local/share/man/man1/rasqltimeindex.1
/bin/install -c -m 0644 ./man/man1/rastream.1 \
/usr/local/share/man/man1/rastream.1
/bin/install -c -m 0644 ./man/man1/rastrip.1 \
/usr/local/share/man/man1/rastrip.1
/bin/install -c -m 0644 ./man/man1/ratop.1 \
/usr/local/share/man/man1/ratop.1
-d /usr/local/share/man/man5 1 1 \
(mkdir -p /usr/local/share/man/man5; chmod 755 /usr/local/share/man/man5)
[ -d /usr/local/share/man/man8 ] 1 1 \
(mkdir -p /usr/local/share/man/man8; chmod 755 /usr/local/share/man/man8)
/bin/install -c -m 0644 ./man/man5/rarc.5 \
/usr/local/share/man/man5/rarc.5
/bin/install -c -m 0644 ./man/man5/racluster.5 \
/usr/local/share/man/man5/racluster.5
/bin/install -c -m 0644 ./man/man5/racolor.conf.5 \
/usr/local/share/man/man5/racolor.conf.5
/bin/install -c -m 0644 ./man/man5/ralabel.conf.5 \
/usr/local/share/man/man5/ralabel.conf.5
/bin/install -c -m 0644 ./man/man5/radium.conf.5 \
/usr/local/share/man/man5/radium.conf.5
/bin/install -c -m 0644 ./man/man5/ranonymize.5 \
/usr/local/share/man/man5/ranonymize.5
/bin/install -c -m 0644 ./man/man8/radium.8 \
/usr/local/share/man/man8/radium.8
[ -d /usr/local ] 1 1 \
(mkdir -p /usr/local; chmod 755 /usr/local)
[ -d /usr/local/share/doc/argus-clients-3.0 ] 1 1 \
(mkdir -p /usr/local/share/doc/argus-clients-3.0; chmod 755 /usr/local/share/doc/argus-clients-3.0)
/bin/install -c -m 0644 ./README /usr/local/share/doc/argus-clients-3.0
/bin/install -c -m 0644 ./COPYING /usr/local/share/doc/argus-clients-3.0
[root@bin/bash: q:: command not found argus-clients-3.0.8.2]#
```

(Compiling Argus with “cd /usr/src/argus-3.0.8.2”, “./configure”, “make && make install”).

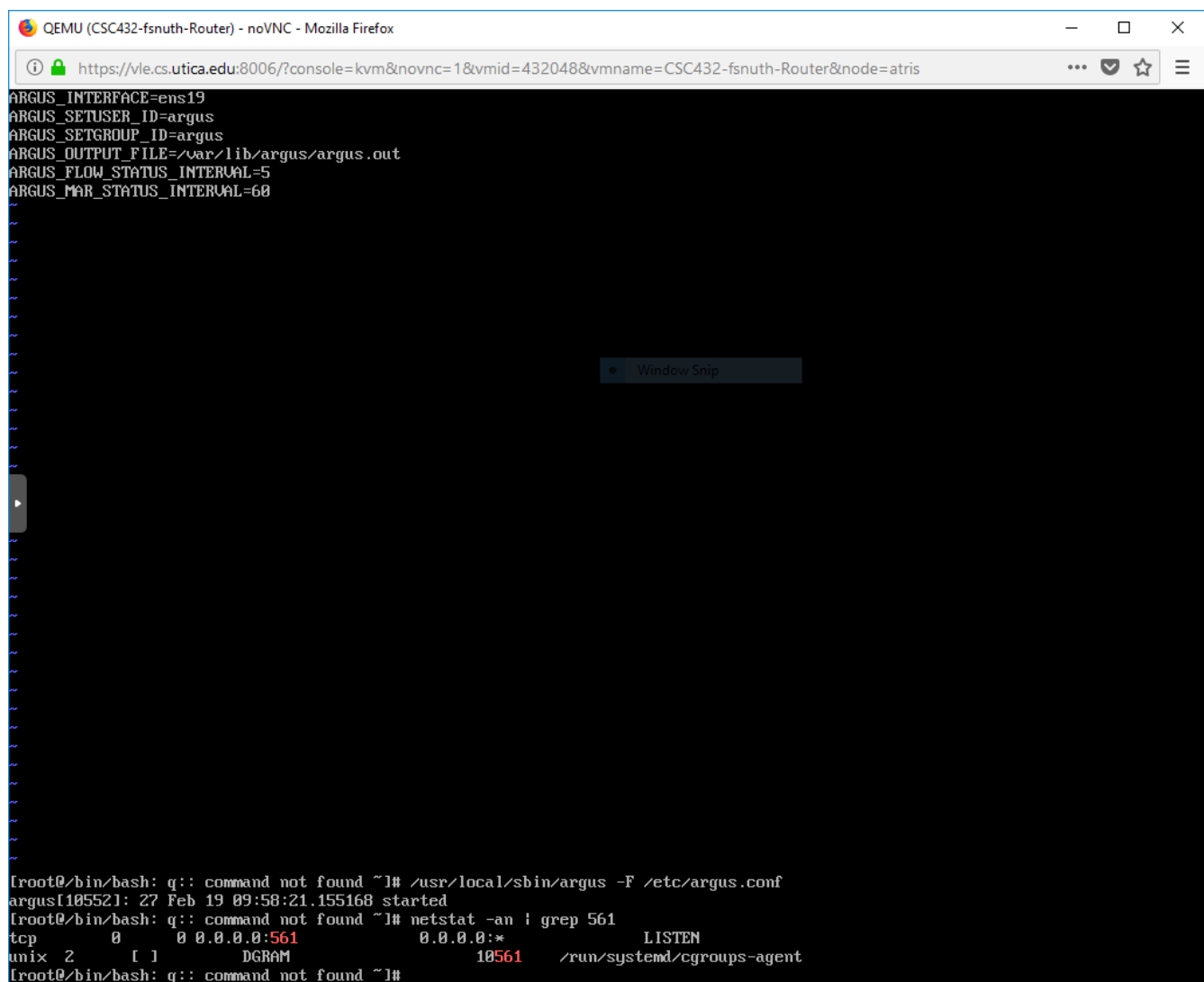
I also worked on creating an **argus.conf** file in the **/etc/argus.conf**. This will alllow us to actually run Argus properly.



The screenshot shows a web browser window titled "QEMU (CSC432-fsnuth-Router) - noVNC - Mozilla Firefox". The address bar contains the URL: `https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432048&vmname=CSC432-fsnuth-Router&node=atris`. The main content area is a black terminal window with white text. The text displays ARGUS configuration parameters: `ARGUS_FLOW_TYPE= ''Bidirectional''`, `ARGUS_FLOW_KEY= ''CLASSIC_5_TUPLE''`, `ARGUS_DAEMON=yes`, `ARGUS_MONITOR_ID='ens19''`, `ARGUS_ACCESS_PORT=561`, `ARGUS_INTERFACE=ens19`, `ARGUS_SETUSER_ID=argus`, `ARGUS_SETGROUPE_ID=argus`, `ARGUS_OUTPUT_FILE=/var/lib/argus/argus.out`, `ARGUS_FLOW_STATUS_INTERVAL=5`, and `ARGUS_MAR_STATUS_INTERVAL=60`. Below these, there are several lines of blue text, likely representing network traffic or log output. At the bottom of the terminal, a bash prompt is visible: `[root@bin/bash: q:: command not found ~]# c1`. A "Window Snip" button is overlaid on the terminal window.

(Creating and customing the argus.conf file.)

We also created an argus user and group with “echo “argus:x:6000:6000:Argus:/home/argus:/sbin/nologin” >> /etc/passwd” and “argus:x:6000 >> /etc/group”. To set the correct permissions with the output directory, we use “mkdir /var/lib/argus”, “touch /var/lib/argus/argus.out”, and “chown -R argus:argus /var/lib/argus”. Then we run “/usr/local/sbin/argus -F /etc/argus.conf”.



The screenshot shows a terminal window titled "QEMU (CSC432-fsnuth-Router) - noVNC - Mozilla Firefox". The address bar shows a URL from vle.cs.utica.edu. The terminal output displays the configuration of Argus, its startup, and the output of a netstat command. A "Window Snip" button is visible in the center of the terminal area.

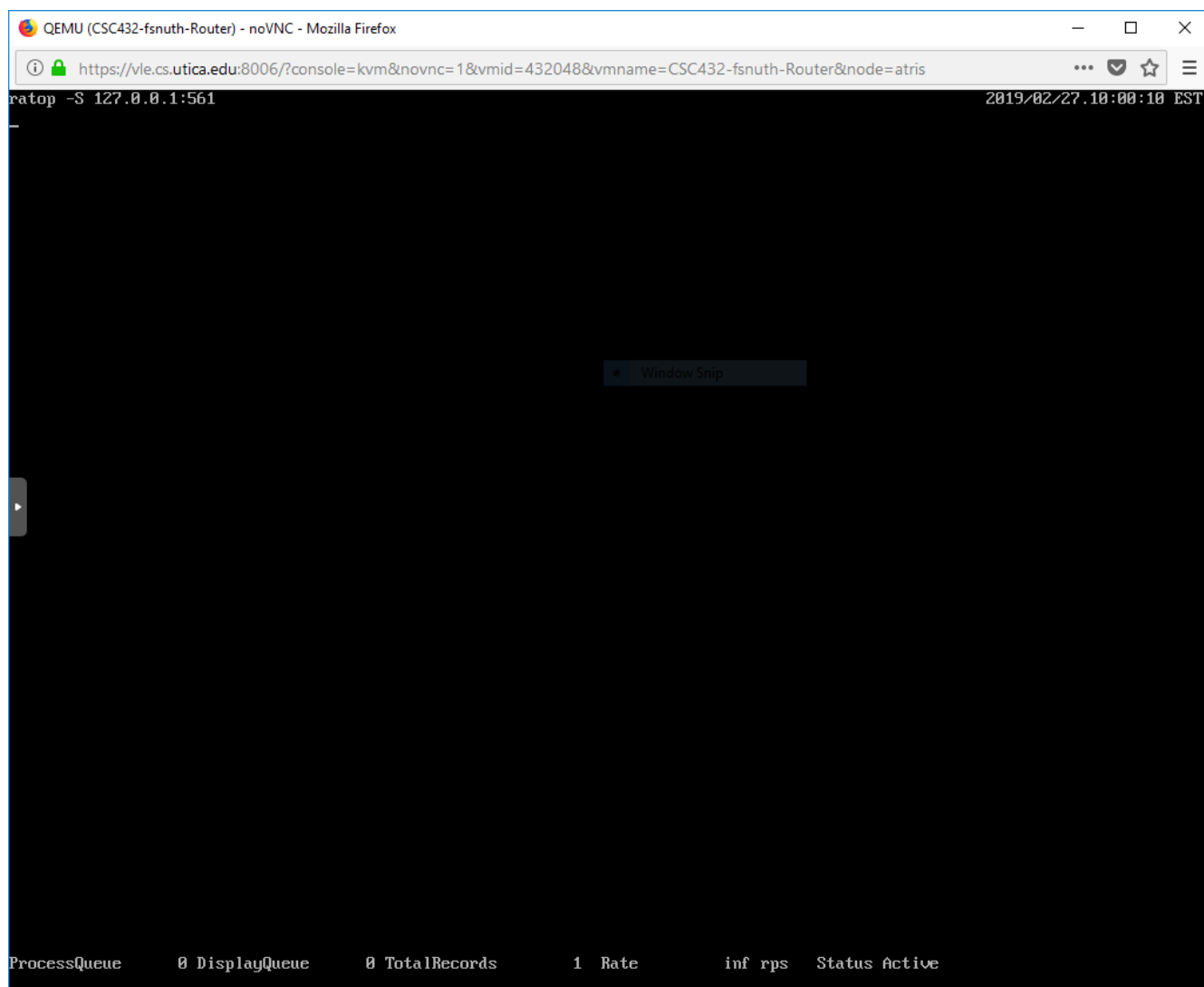
```
ARGUS_INTERFACE=ens19
ARGUS_SETUSER_ID=argus
ARGUS_SETGROUP_ID=argus
ARGUS_OUTPUT_FILE=/var/lib/argus/argus.out
ARGUS_FLOW_STATUS_INTERVAL=5
ARGUS_MAR_STATUS_INTERVAL=60

[... many lines of output ...]

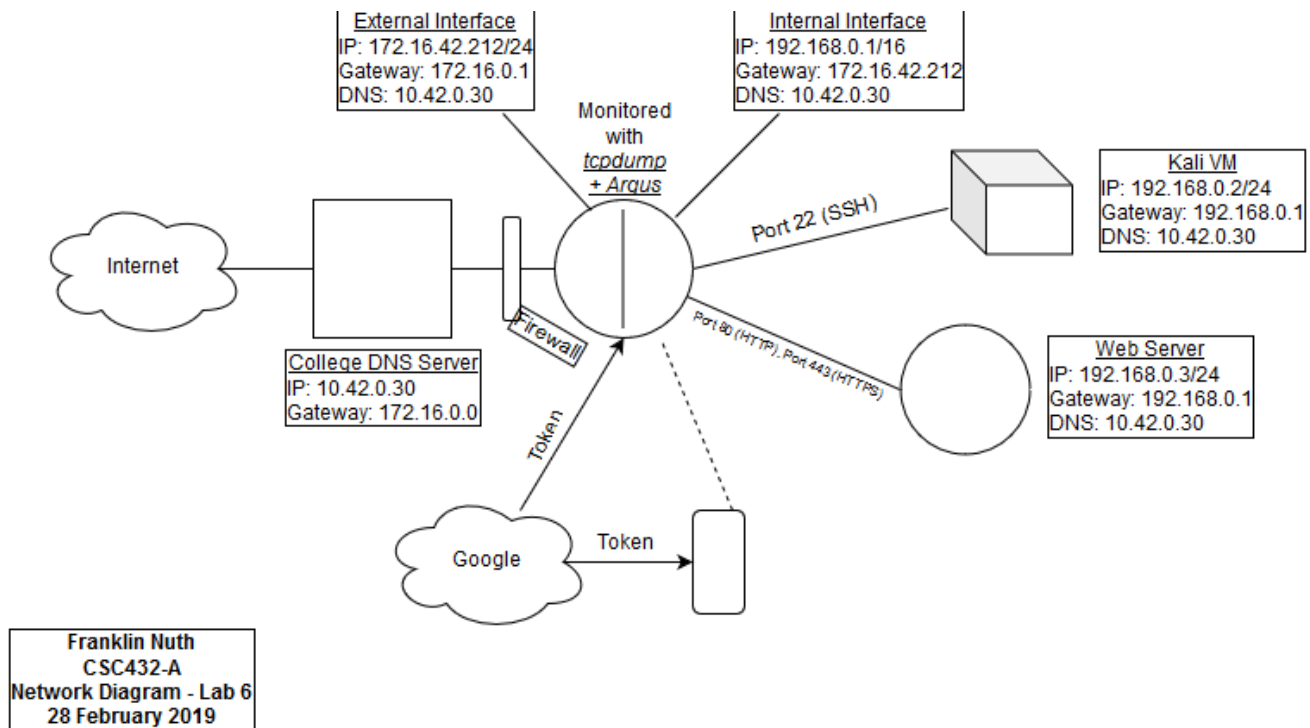
[root@bin/bash: q:: command not found ~]# /usr/local/sbin/argus -F /etc/argus.conf
argus[105521]: 27 Feb 19 09:58:21.155168 started
[root@bin/bash: q:: command not found ~]# netstat -an | grep 561
tcp        0      0  0.0.0.0:561          0.0.0.0:*           LISTEN
unix  2      [ ]          DGRAM               10561      /run/systemd/cgroups-agent
[root@bin/bash: q:: command not found ~]#
```

(Argus running its network flow monitoring services.)

ratop is one of the data cliens that come with Argus. **Ratop** is useful for displaying network flow data for easire use. One way to use **ratop** is “ratop -S 127.0.0.1:561”. Port deals with TCP and UDP information, so this means that this listens in on IP 127.0.0.1 for any protocol from the Transport Layer.



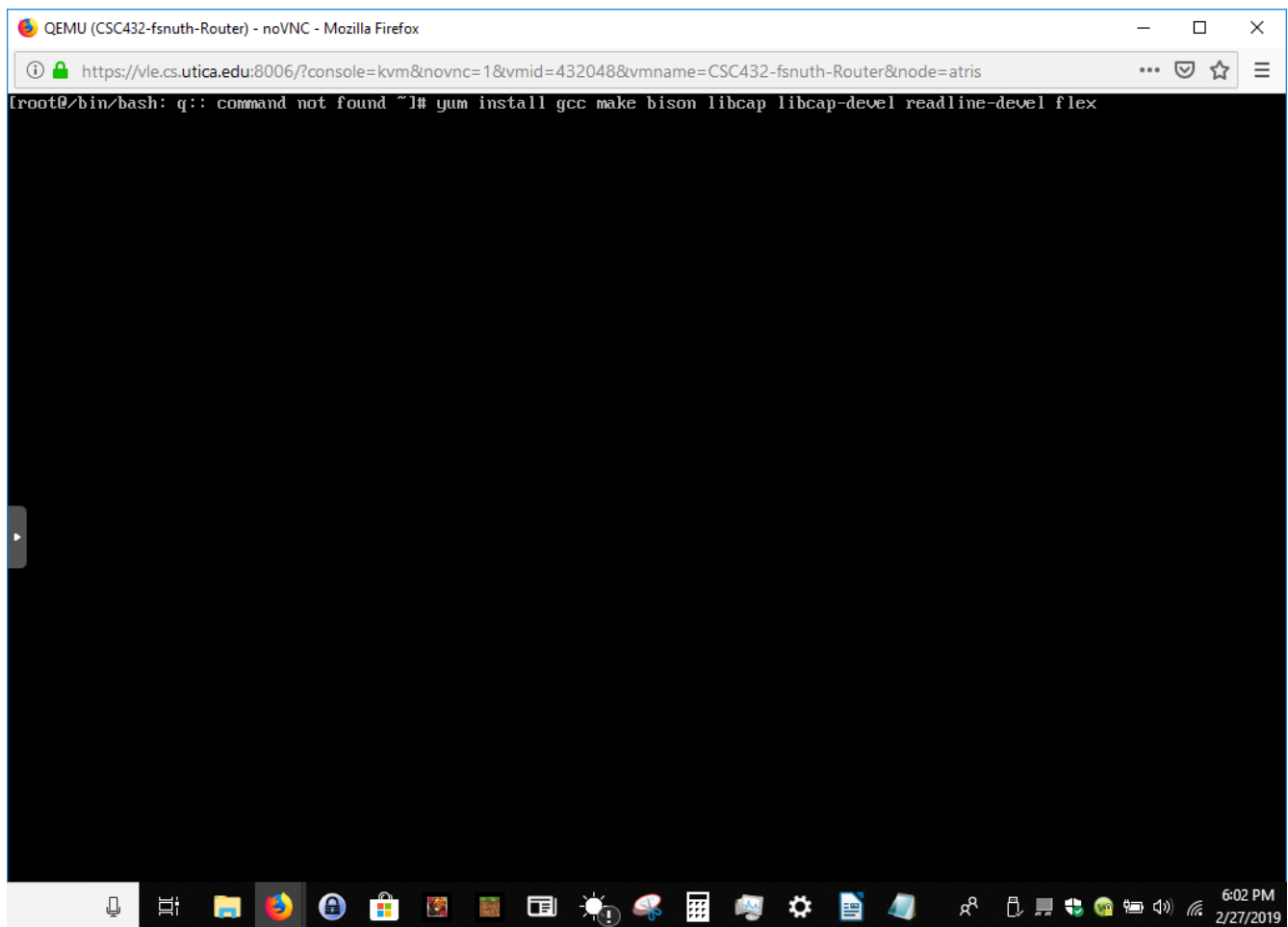
(Using ratop, which is part of the Argus software.)



(The sixth revision of my network diagram after installing tcpdump and Argus)

Issues & Resolutions

I encountered two minor issues in this lab. The first issue that I ran into is that I mistyped one of the packages. In the syntax “yum install gcc make bison libpcap libcap-devel readline-devel flex”, I accidentally typed “lipcap” instead of “libpcap”. This small mistake set me back a couple of days, until my professor and classmates helped pointed it out. I will take measure to start reading the lab slowly to avoid this issue.



(I will start to read more slowly from this point on.)

Another issue I've dealt with is incorrect information in my argus.conf file. While trying to set correct permissions in the output directory, it does not work for me because I had an ID problem. The ID lines in my configuration file was actually two single quotatoin marks, not the double quotations. My classmate pointed this out to me and we immediately changed the single quotations to doubles. I had no problem making users and groups after that small fix.

A screenshot of a web browser window displaying a QEMU console. The browser's address bar shows the URL: https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432048&vmname=CSC432-fsnuth-Router&node=atris. The console output shows the configuration for the ARGUS daemon. The configuration lines are: ARGUS_FLOW_TYPE= "Bidirectional", ARGUS_FLOW_KEY= "CLASSIC_5_TUPLE", ARGUS_DAEMON=yes, ARGUS_MONITOR_ID="ens19", ARGUS_ACCESS_PORT=561, ARGUS_INTERFACE=ens19, ARGUS_SETUSER_ID=argus, ARGUS_SETGROUP_ID=argus, ARGUS_OUTPUT_FILE=/var/lib/argus/argus.out, ARGUS_FLOW_STATUS_INTERVAL=5, and ARGUS_MAR_STATUS_INTERVAL=60. The console background is black with white text. The browser window has standard macOS window controls (red, yellow, green buttons) in the top left. The bottom of the image shows a portion of the macOS desktop with a dock containing various application icons and a status bar in the bottom right corner showing the time as 6:02 PM on 2/27/2019.

```
ARGUS_FLOW_TYPE= "Bidirectional"
ARGUS_FLOW_KEY= "CLASSIC_5_TUPLE"
ARGUS_DAEMON=yes
ARGUS_MONITOR_ID="ens19"
ARGUS_ACCESS_PORT=561
ARGUS_INTERFACE=ens19
ARGUS_SETUSER_ID=argus
ARGUS_SETGROUP_ID=argus
ARGUS_OUTPUT_FILE=/var/lib/argus/argus.out
ARGUS_FLOW_STATUS_INTERVAL=5
ARGUS_MAR_STATUS_INTERVAL=60
```

(Removed the single quotations and inserted the double quotations.)

Conclusion

In this lab, I have shown how to install **tcpdump** and use it for monitoring SSH or HTTP traffic. I also shown how to install Argus as well as a few of its data clients for network flow monitoring. A network administarator can use both of these tools as ways to manually monitor all IP and network traffic on the network. It is intriguing to watch how packets and IP address work with each other through programs like Wireshark and tcpdump. Although it is more technical than standing in front of a door, the techniques and concepts I picked up from this lab are just as good for my network.

References

Bullard, Carter. 2012 August 3. *RAFILTERADDR(1)*. Retrieved from:

<https://qosient.com/argus/man/man1/rafilteraddr.1.pdf>

QoSient.com. 2019 January 14. *Argus Archive*. Retrieved from: <https://qosient.com/argus/>

Shrestha, Narad. 2012 August 20. *12 Tcpdump Commands – A Network Sniffer Tool*. Retrieved from:

<https://www.tecmint.com/12-tcpdump-commands-a-network-sniffer-tool/>

Wireshark.org. 2019 February 28. *Chapter 1 Introduction*. Retrieved from:

https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html