

Webster Cyberlab

Live Training Environment

*Chris Blask – Management Analytics
- April, 2015*

Instructors: Getting Credentials

- Get a set of credentials for your students to access the cyberlab. You get them by emailing to cyberlab@all.net. You will receive an email that looks like this:

Goto:

<http://cyberlab.all.net>

Select "Reservation"

The proper answers are:

SkibberBlog UID 2015Q1

UID is any of:

aad3bf2a1ffc642c0fe2c90692e6bdag

2c07e3627127263d4d79d42fe8aeacfe

7087348833a34b81f923171d00c07bf1

fdde0d49743401362c884395fb52d0f4

Each is allocated 5 slots of 24 hours

You can dole out these instructions (with the requested number of students each getting one of the UIDs) to professors (and yourselves) as needed. We don't want the identities of who they were given to.

Instructors: Supplying Credentials

- Send each of your students credentials to access the Cyberlab. Example:

Goto:

<http://cyberlab.all.net>

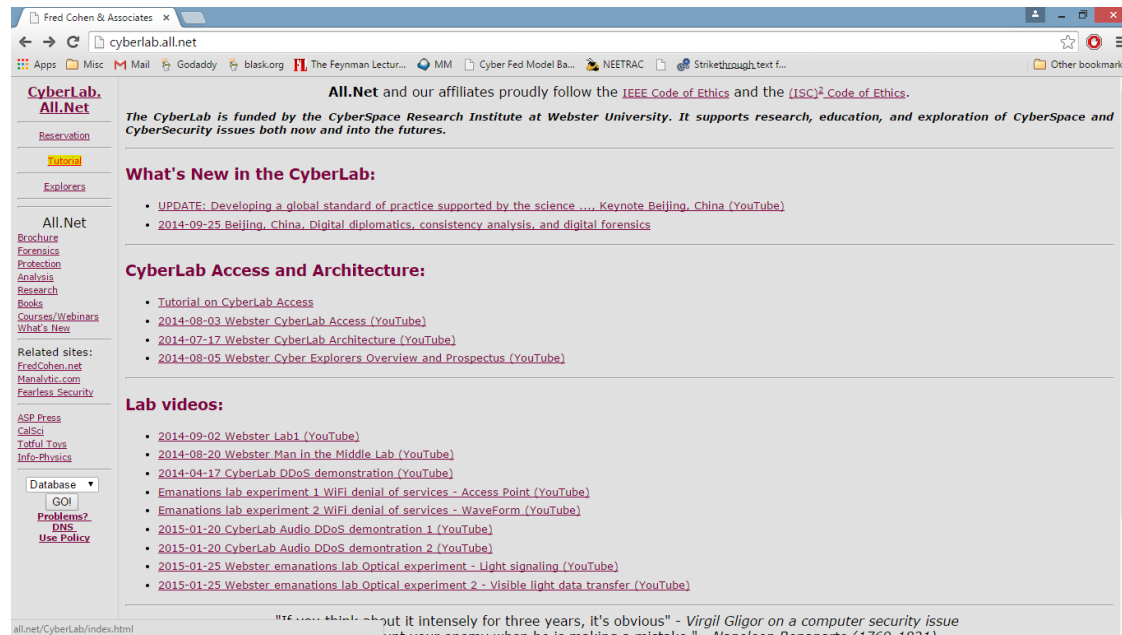
Select "Reservation"

The proper answers are:

SkibberBlog aad3bf2a1ffc642c0fe2c90692e6bdag 2015Q1

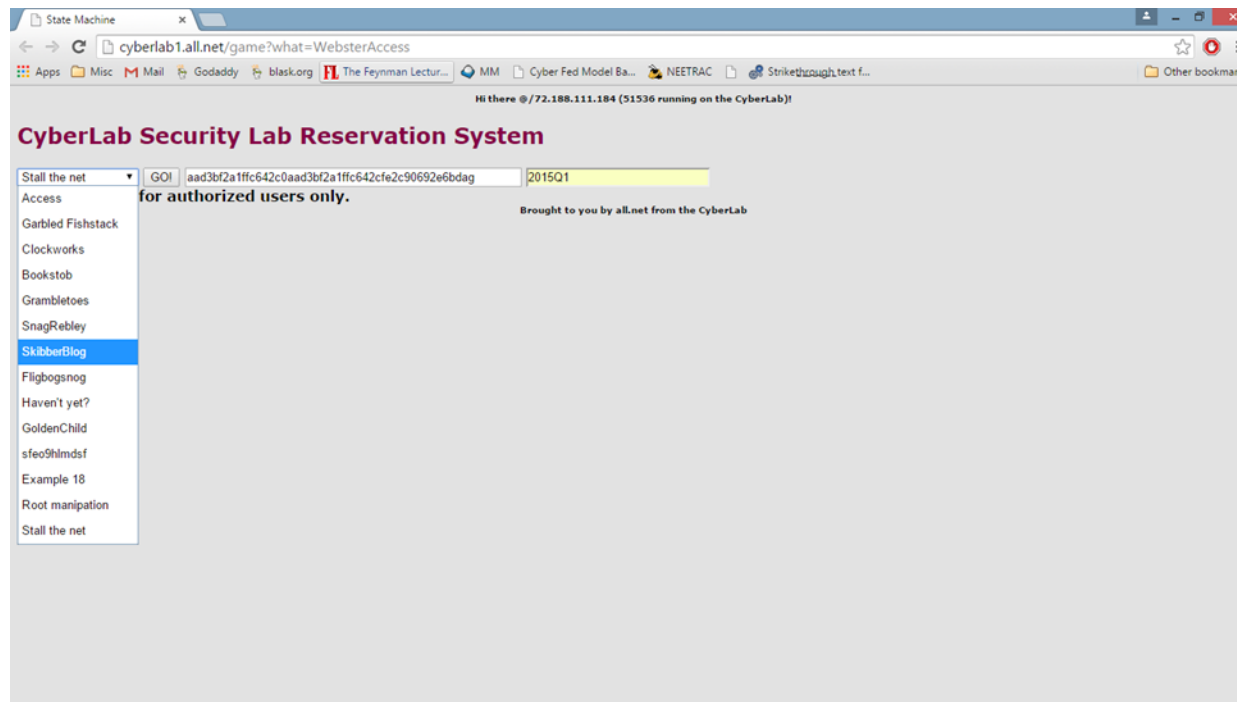
Students: Read the Tutorials

- Cyberlab.all.net
- Tutorials, videos and other content



Login to the Cyberlab

- Using the credentials your instructor gave you, login as follows:



Reservations

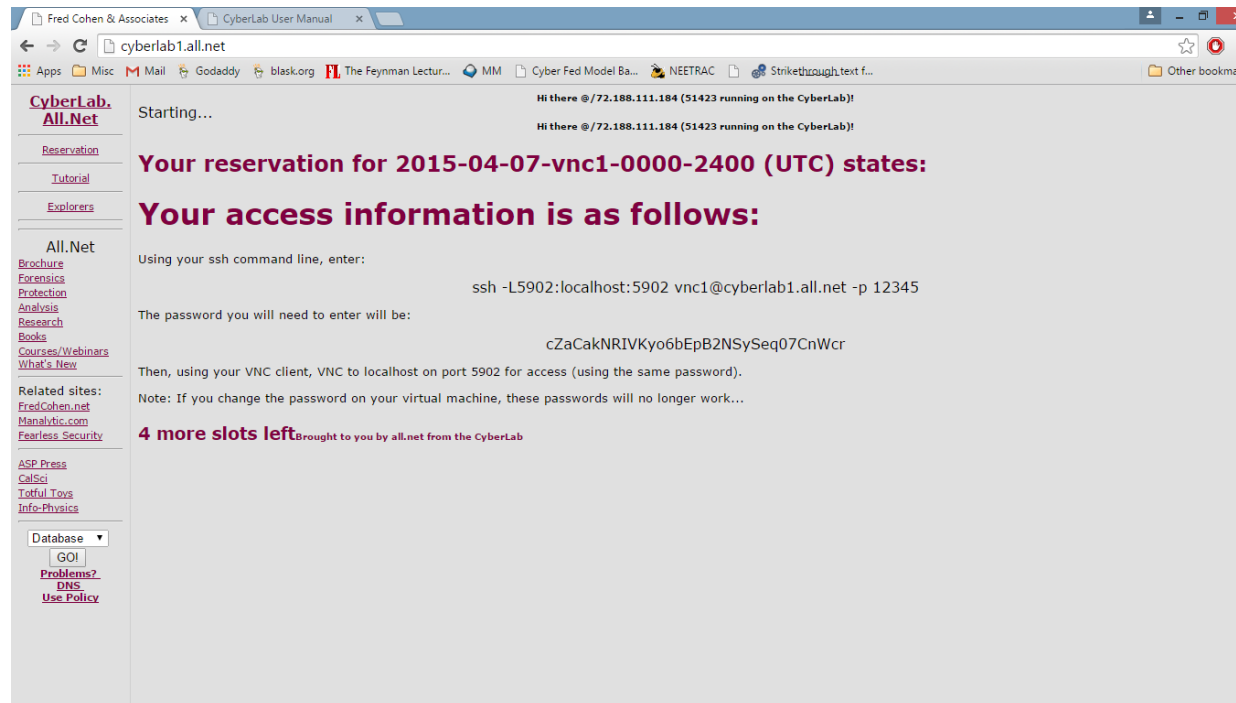
- Select your reservation times

The screenshot shows a web browser window with the URL `cyberlab1.all.net`. The page content includes:

- Navigation links: [Reservation](#), [Tutorial](#), [Explorers](#)
- Left sidebar menu: [All.Net](#), [Brochure](#), [Forensics](#), [Protection](#), [Analysis](#), [Research](#), [Books](#), [Courses/Webinars](#), [What's New](#), [Related sites: FredCohen.net, Manalytic.com, Fearless Security](#), [ASP Press](#), [CalSci](#), [Totful Toys](#), [Info-Physics](#), [Database](#) (dropdown), [GO!](#), [Problems?](#), [DNS](#), [Use Policy](#)
- Main content area:
 - Starting...
Called with `what=edg0l4fes&Field1=aad3bf2a1ffc642c0fe2c90692e6bdaf&Field2=2015Q1`
Current reference date and time: 2015/04/07 10:19:24
 - Your reservation options are:**
 - A list of reservation options, each with a dropdown menu and a "GO!" button. The first option is selected: `2015Q1:2015-04-07-vnc1-0000-2400`.
 - Footer: **Brought to you by all.net from the CyberLab**

Reservation Information

- This will take you to a screen that tells you how to login:



The screenshot shows a web browser window with the address bar displaying `cyberlab1.all.net`. The page content includes:

- CyberLab. All.Net** logo and navigation links: [Reservation](#), [Tutorial](#), [Explorers](#).
- All.Net** section with links: [Brochure](#), [Forensics](#), [Protection](#), [Analysis](#), [Research](#), [Books](#), [Courses/Webinars](#), [What's New](#).
- Related sites:** [FredCohen.net](#), [Manalytic.com](#), [Fearless Security](#).
- ASP Press** section with links: [CalSci](#), [Toful Toys](#), [Info-Physica](#).
- A search bar with a dropdown menu set to "Database" and a "GO!" button.
- [Problems?](#), [BNS](#), and [Use Policy](#) links.

The main content area displays the following information:

Starting... Hi there @/72.188.111.184 (51423 running on the CyberLab)!

Your reservation for 2015-04-07-vnc1-0000-2400 (UTC) states:

Your access information is as follows:

Using your ssh command line, enter:

```
ssh -L5902:localhost:5902 vnc1@cyberlab1.all.net -p 12345
```

The password you will need to enter will be:

```
cZaCakNRIVKyo6bEpB2NSySeq07CnWcr
```

Then, using your VNC client, VNC to localhost on port 5902 for access (using the same password).

Note: If you change the password on your virtual machine, these passwords will no longer work...

4 more slots left brought to you by all.net from the CyberLab

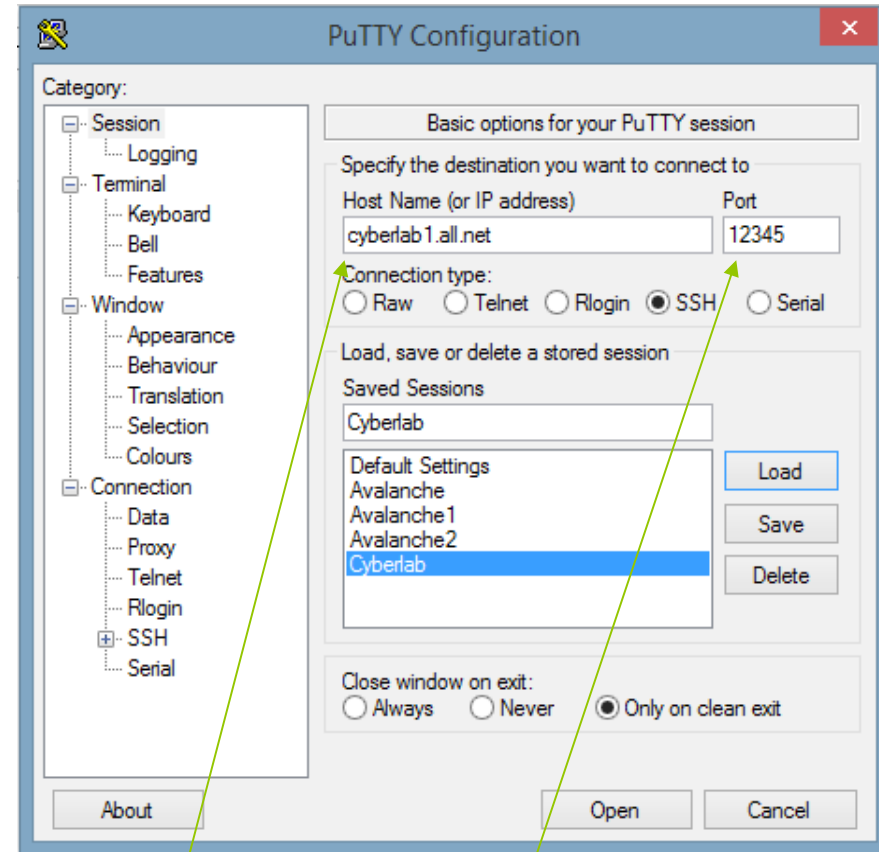
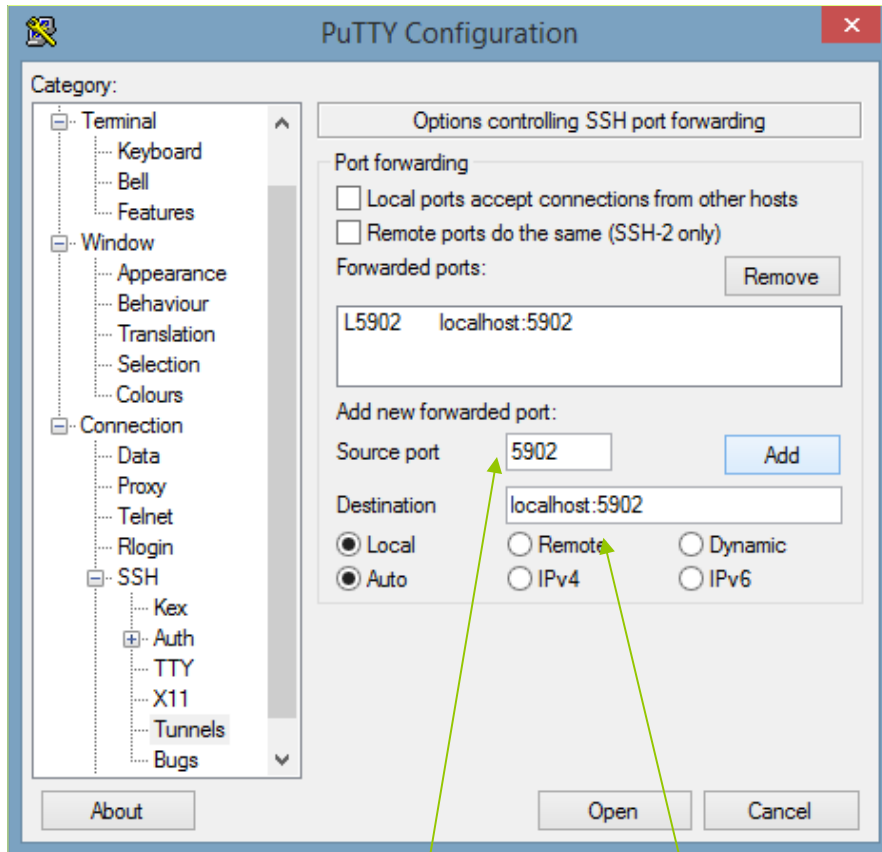
Using Reservation Information: SSH

- There are two pieces of information you need here to go further. The first is the SSH command line, the second is the password.
- SSH Command Line:

```
ssh -L5902:localhost:5902 vnc1@cyberlab1.all.net -p 12345
```

- If you using a linux command line, you can enter this command directly. If you are using a tool like Putty, configure Putty as follows for this example.

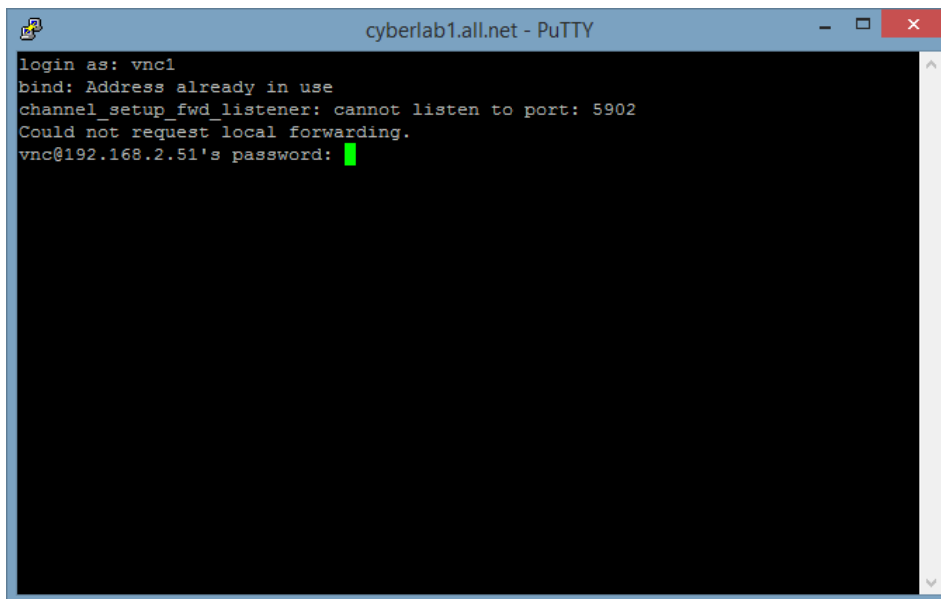
SSH: Configure Putty for Windows



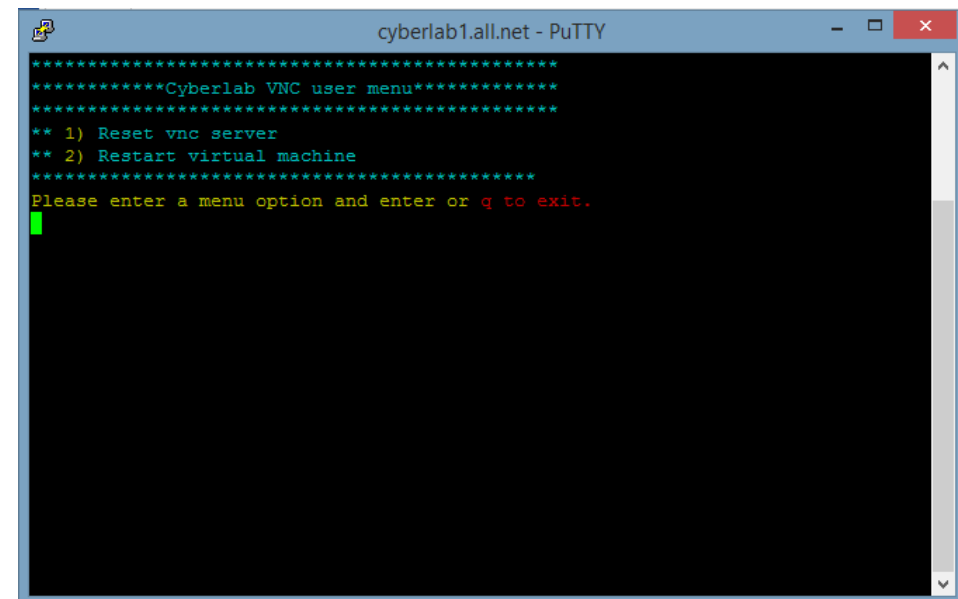
ssh -L5902:localhost:5902 vnc1@cyberlab1.all.net -p 12345

Creating SSH Tunnel to Cyberlab

- Login to Cyberlab with SSH. When you connect, use the username and password provided.



```
cyberlab1.all.net - PuTTY
login as: vnc1
bind: Address already in use
channel_setup_fwd_listener: cannot listen to port: 5902
Could not request local forwarding.
vnc@192.168.2.51's password: █
```

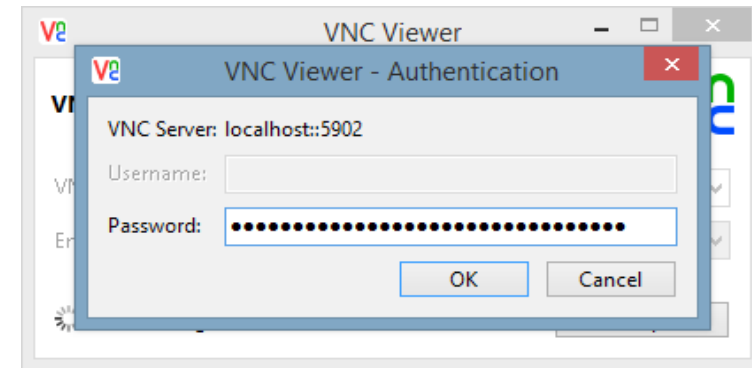
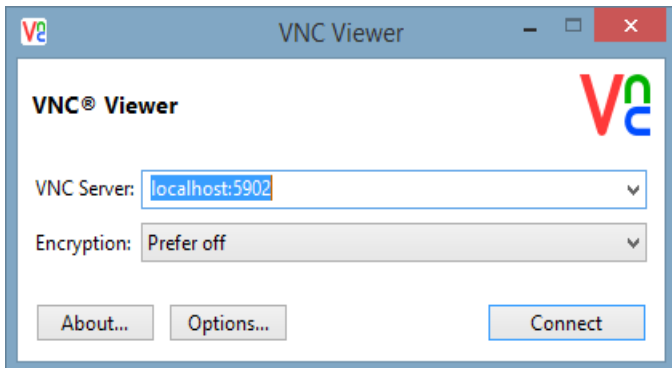


```
cyberlab1.all.net - PuTTY
*****Cyberlab VNC user menu*****
** 1) Reset vnc server
** 2) Restart virtual machine
*****
Please enter a menu option and enter or q to exit.
█
```

```
ssh -L5902:localhost:5902 vnc1@cyberlab1.all.net -p 12345
```

Connecting with VNC: Using VNC Viewer

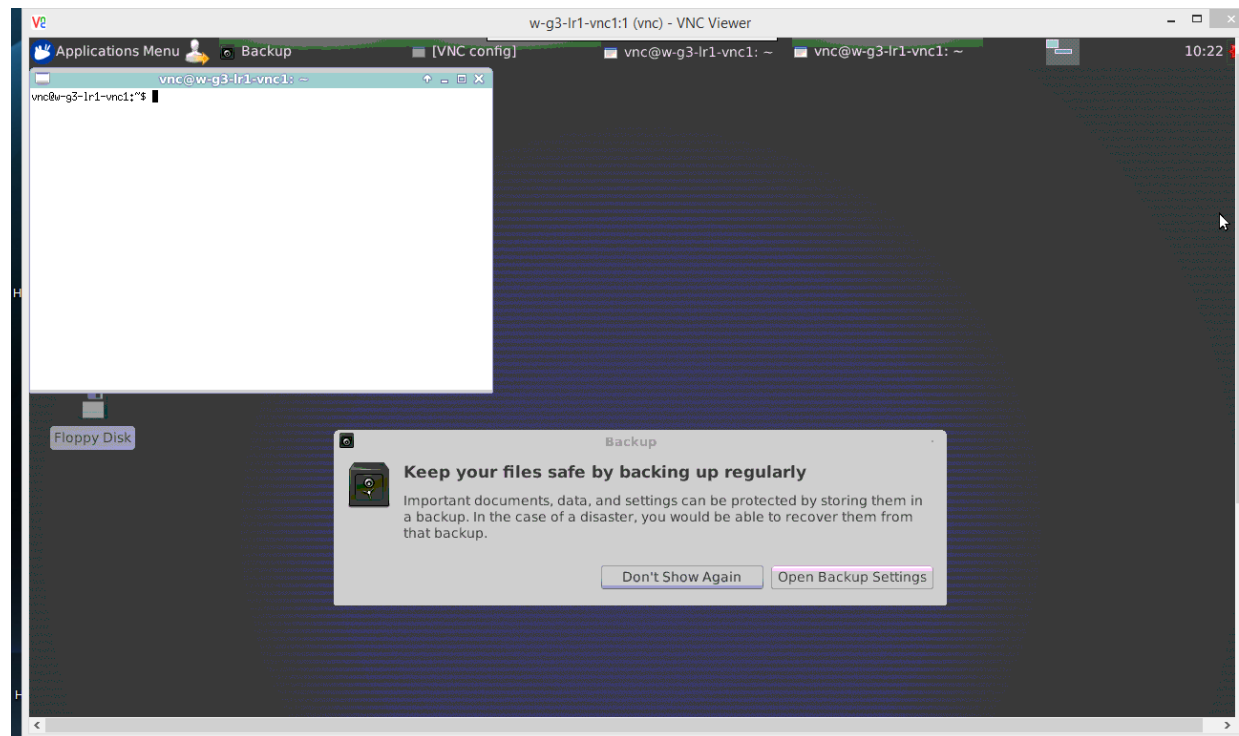
- Note settings: use information for your reservation



```
ssh -L5902:localhost:5902 vnc1@cyberlab1.all.net -p 12345
```

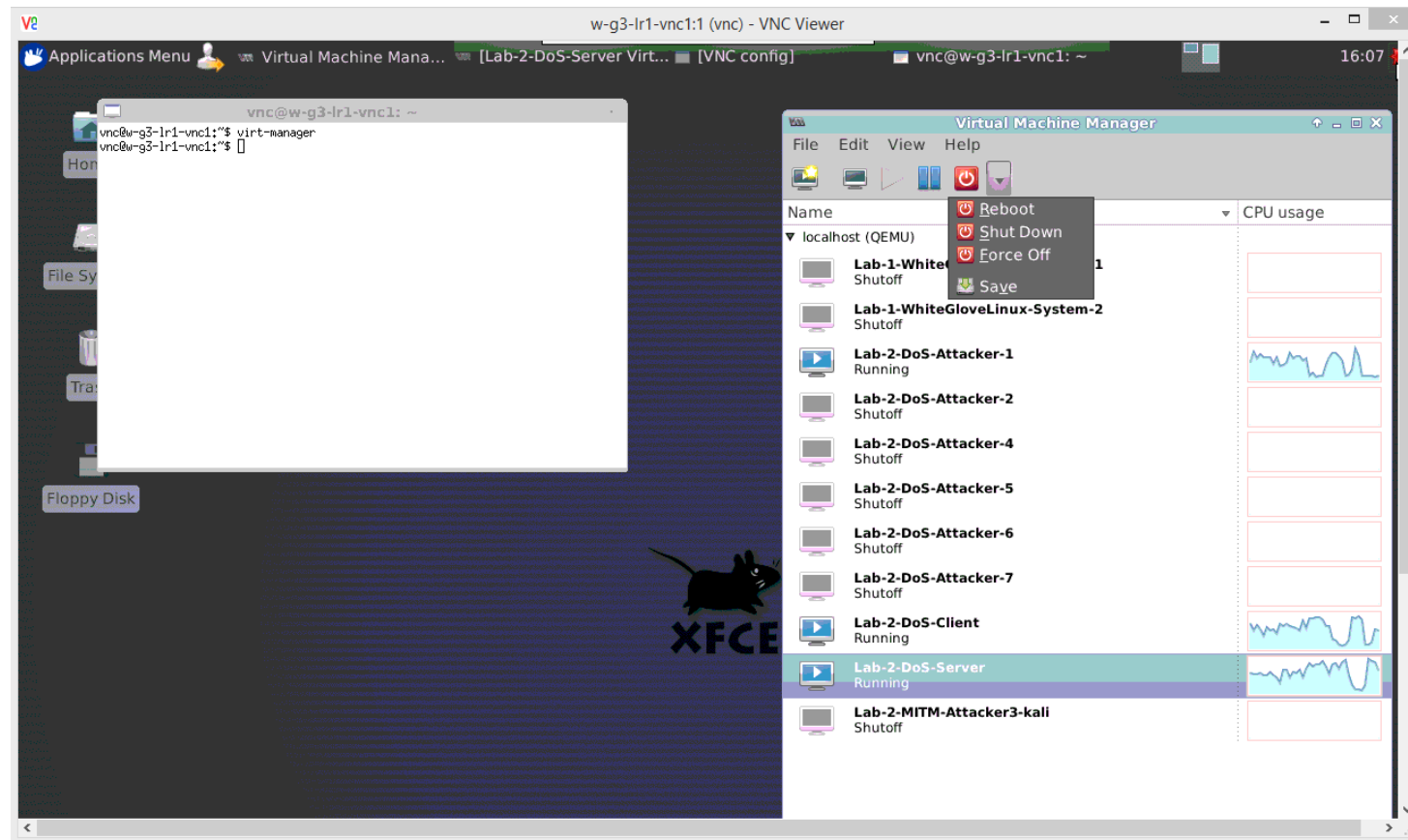
The Cyberlab Environment

- Your Cyberlab Virtual Machine
- Hosts additional VMs



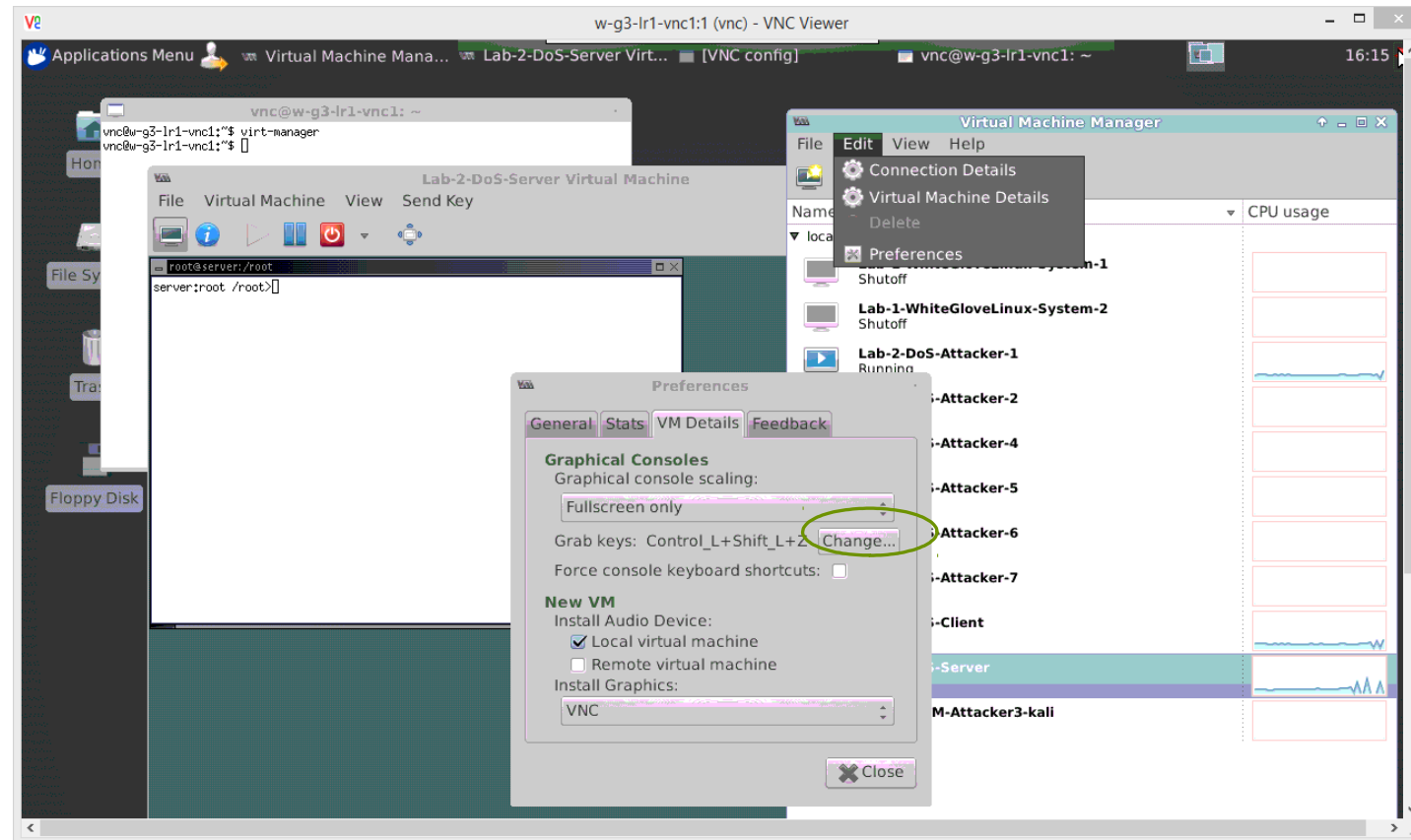
The Cyberlab Environment

- o *virtmanager*



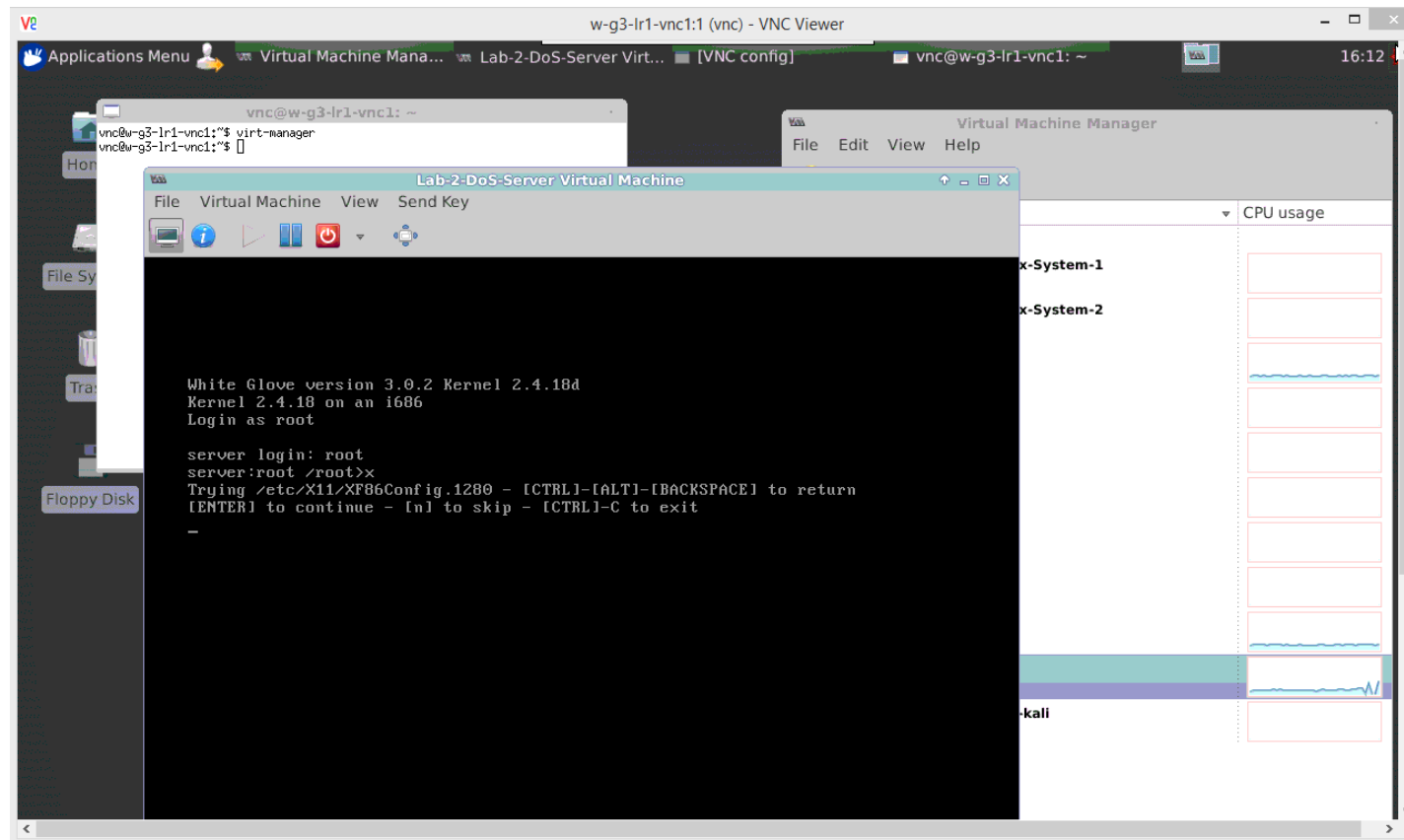
The Cyberlab Environment

- Set Escape keys



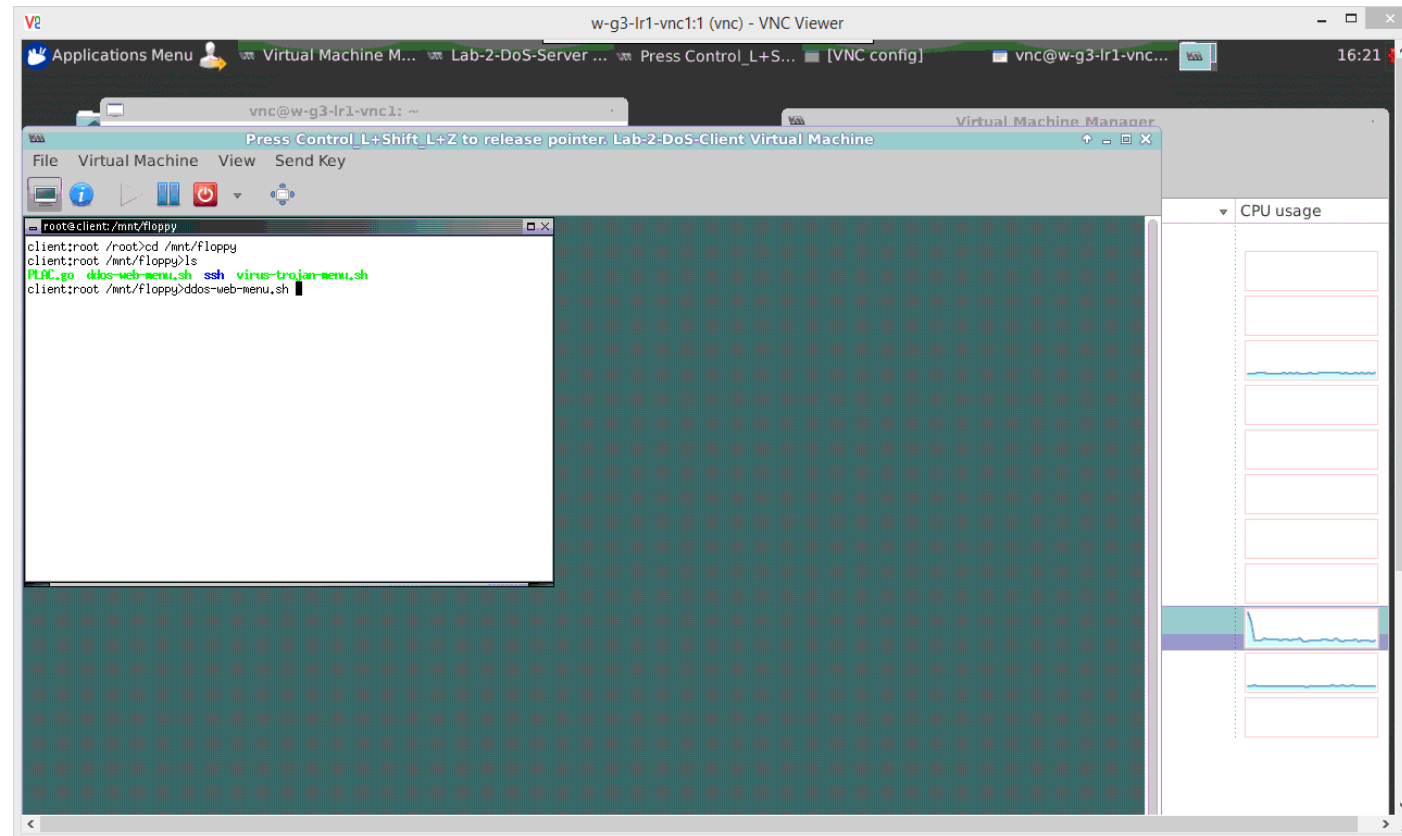
The Cyberlab Environment

- Start Virtual Machines and X Windows



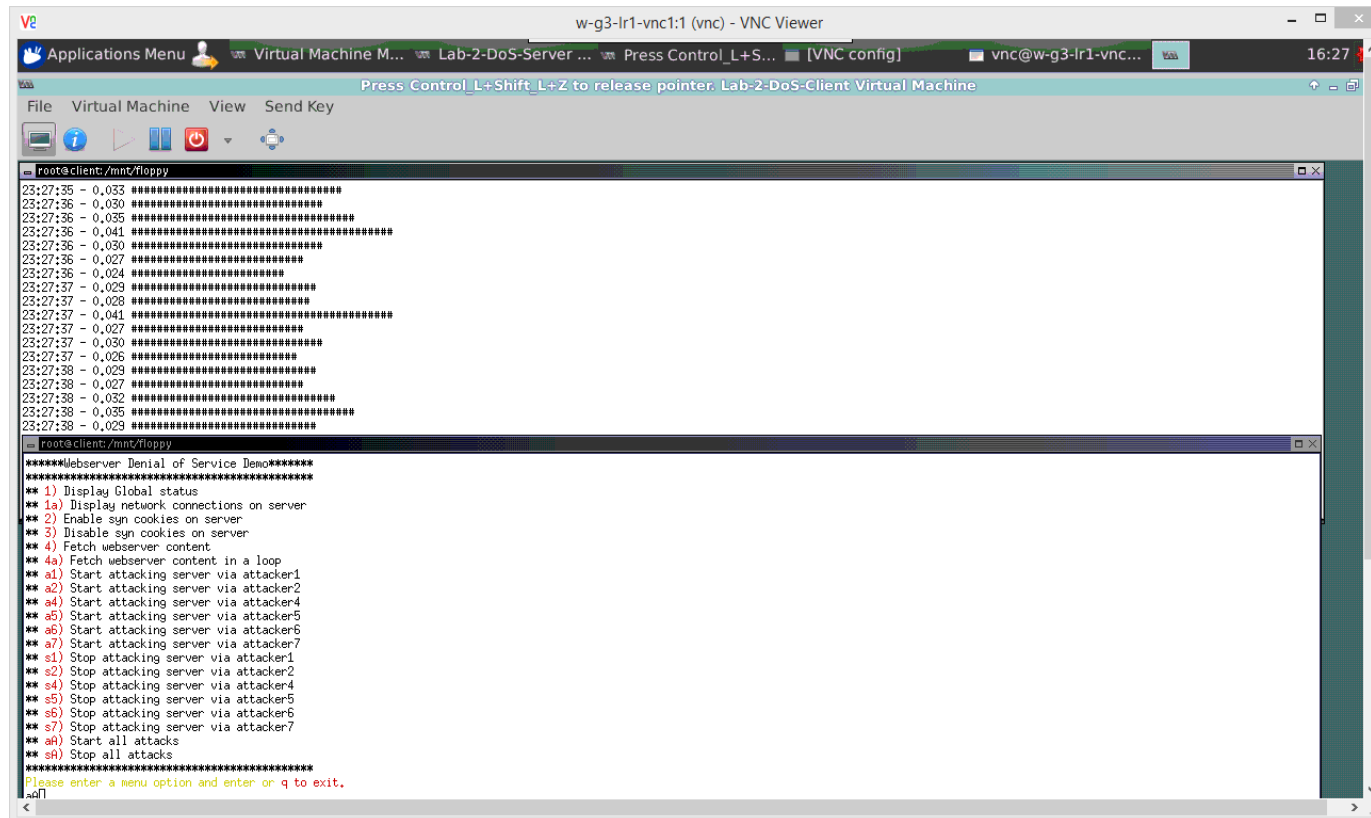
The Cyberlab Environment

- Find and run experiments



The Cyberlab Environment

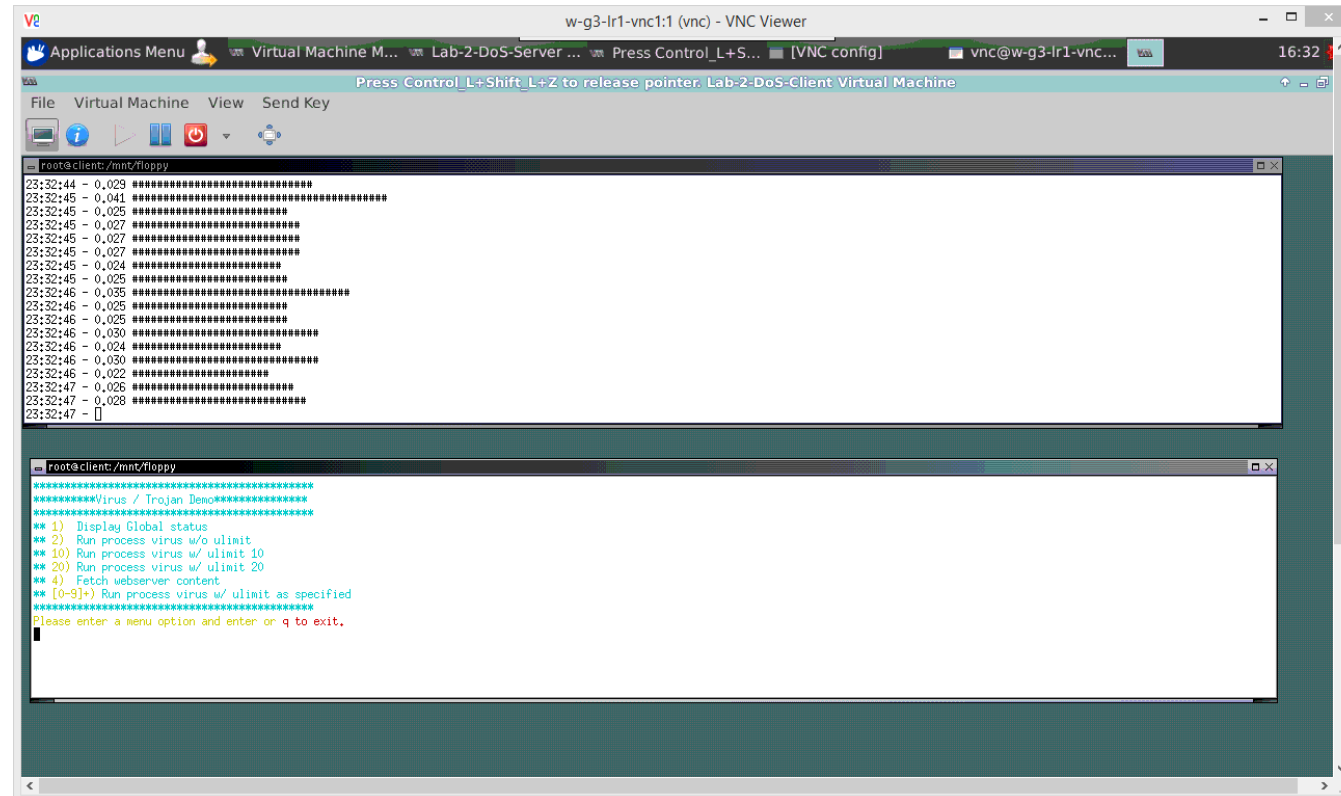
- External Denial of Service



```
w-g3-lr1-vnc1:1 (vnc) - VNC Viewer
Applications Menu Virtual Machine M... Lab-2-DoS-Server ... Press Control_L+S... [VNC config] vnc@w-g3-lr1-vnc... 16:27
Press Control_L+Shift_L+Z to release pointer. Lab-2-DoS-Client Virtual Machine
File Virtual Machine View Send Key
root@client:/mnt/floppy
23:27:35 - 0,033 #####
23:27:35 - 0,030 #####
23:27:36 - 0,035 #####
23:27:36 - 0,041 #####
23:27:36 - 0,030 #####
23:27:36 - 0,027 #####
23:27:36 - 0,024 #####
23:27:37 - 0,029 #####
23:27:37 - 0,028 #####
23:27:37 - 0,041 #####
23:27:37 - 0,027 #####
23:27:37 - 0,030 #####
23:27:37 - 0,026 #####
23:27:38 - 0,029 #####
23:27:38 - 0,027 #####
23:27:38 - 0,032 #####
23:27:38 - 0,035 #####
23:27:38 - 0,029 #####
root@client:/mnt/floppy
*****Webserver Denial of Service Demo*****
*****
** 1) Display Global status
** 1a) Display network connections on server
** 2) Enable syn cookies on server
** 3) Disable syn cookies on server
** 4) Fetch webservice content
** 4a) Fetch webservice content in a loop
** a1) Start attacking server via attacker1
** a2) Start attacking server via attacker2
** a4) Start attacking server via attacker4
** a5) Start attacking server via attacker5
** a6) Start attacking server via attacker6
** a7) Start attacking server via attacker7
** s1) Stop attacking server via attacker1
** s2) Stop attacking server via attacker2
** s4) Stop attacking server via attacker4
** s5) Stop attacking server via attacker5
** s6) Stop attacking server via attacker6
** s7) Stop attacking server via attacker7
** ah) Start all attacks
** sa) Stop all attacks
*****
Please enter a menu option and enter q to exit.
<
```

The Cyberlab Environment

- Internal Denial of Service



```
w-g3-lr1-vnc1:1 (vnc) - VNC Viewer
Applications Menu Virtual Machine M... Lab-2-DoS-Server ... Press Control_L+S... [VNC config] vnc@w-g3-lr1-vnc... 16:32
Press Control_L+Shift_L+Z to release pointer. Lab-2-DoS-Client Virtual Machine
File Virtual Machine View Send Key
root@client: /mnt/floppy
23:32:44 - 0.029 *****
23:32:45 - 0.041 *****
23:32:45 - 0.025 *****
23:32:45 - 0.027 *****
23:32:45 - 0.027 *****
23:32:45 - 0.027 *****
23:32:45 - 0.024 *****
23:32:45 - 0.025 *****
23:32:46 - 0.035 *****
23:32:46 - 0.025 *****
23:32:46 - 0.025 *****
23:32:46 - 0.030 *****
23:32:46 - 0.024 *****
23:32:46 - 0.030 *****
23:32:46 - 0.022 *****
23:32:47 - 0.026 *****
23:32:47 - 0.028 *****
23:32:47 - []
root@client: /mnt/floppy
*****Virus / Irojan Demo*****
*****
** 1) Display Global status
** 2) Run process virus w/o ulimit
** 10) Run process virus w/ ulimit 10
** 20) Run process virus w/ ulimit 20
** 4) Fetch webservice content
** [0-9]+) Run process virus w/ ulimit as specified
*****
Please enter a menu option and enter or q to exit.

```

Build Your Own Experiments

- The Cyberlab is intended for education and research
- Design and build experiments
- Group projects
- Tutorials explain how to save work
- Your experiments may be added to Cyberlab