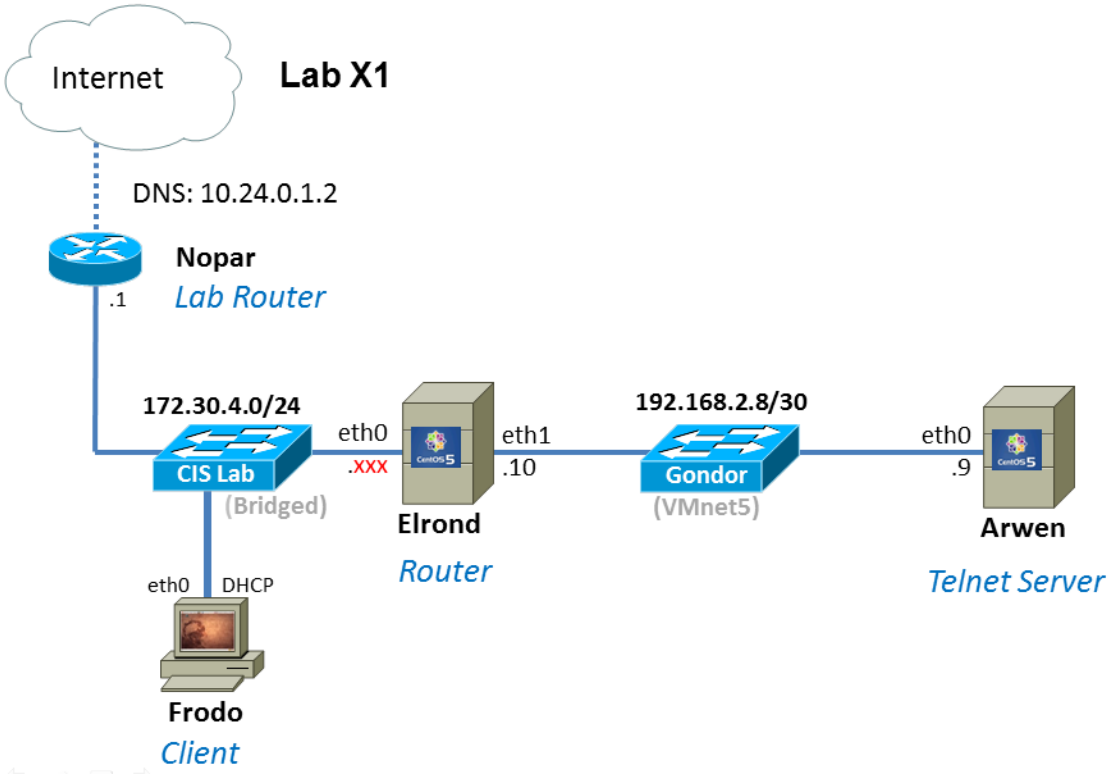
Cabrillo College

Lab X1: SSH Tunnel

In this lab an SSH tunnel will be implemented through Elrond to a Telnet server on Arwen.



Lab X1 NETWORK DIAGRAM: Each switch above is really a virtual network. The white labels are the names used in the VLab pods (VMware ESXi/vSphere) and the gray labels in parenthesis are the names used in on the workstations in the CIS Lab (VMware Workstation).

Supplies

- VLab pod or CIS Lab workstation
- 192 VMs shown above

Preparation

1. Revert all VMs to the “Pristine” snapshot.

2. Make sure Frodo has the **telnet** (client) and **wireshark** packages installed. To see if a package is installed use:
   `dpkg -l | grep` *`packagename`*
   and to install use:
   `apt-get install` *`packagename`*

3. Make sure Arwen has both the **telnet** (client) and **telnet-server** packages installed. To see if a package is installed use:
   `rpm -qa | grep` *`packagename`*
   and to install use:
   `yum install` *`packagename`*

4. On Opus, make a copy of the labX1 report template file in /home/cis192/depot in your home directory. Edit the header of this file with your own information and record all the information requested.

Forum
Use the forum to ask questions, collaborate, post tips and any lessons learned when you have finished. Forum is at: http://opus.cabrillo.edu/forum/viewforum.php?f=39

Background
This lab covers the use of the secure shell (ssh) utility to forward ports. We'll use port 8000 to forward to the remote port 23, but any port can be substituted. However it is important to remember that ports 1023 and lower are considered reserved and require root access to forward. Because this lab uses only port 8000, root access is not required. You need a regular user (cis192) account on the destination and pass-through computers.

Forwarding ports using ssh is a convenient way to protect information sent over the Internet, because unlike telnet and ftp, ssh encrypts data to protect against eavesdropping programs. Port forwarding is required in situations in which normal connections cannot be established. If a computer is part of a LAN and cannot be reached directly because of a firewall or some other barrier, it might be easier to use port forwarding. Telnet traffic travels in clear text and is not secure.

We will configure **Arwen** to be a Telnet server and then set up a secure SSH tunnel through **Elrond** to access it from the outside.

1. Cable up, power on and configure all the VMs to match implement the diagram above.

2. Test and make sure Elrond can ping both Frodo and Arwen.

3. On Arwen, review the current firewall with **`iptables -L --line-numbers`** and locate the line number, ***`n`***, for the line that accepts new connections to SSH (TCP port 22).

4. On Arwen, open a port for Telnet (TCP 23) by inserting a new line above the line allowing SSH connections:

iptables -I INPUT *n* -p tcp -m state --state NEW -m tcp --dport 23 -j ACCEPT
(all on one line)

5. On Arwen, check your new entry with **iptables -L** and look for:

   ```
   ACCEPT  tcp  --  anywhere  anywhere  state NEW tcp dpt:telnet
   ```

   If all is OK, then save your firewall permanently with:

   service iptables save

6. On Arwen, configure the Telnet service to be enabled but only accept logins from Elrond:

/etc/xinetd.d/telnet

```
# default: on
# description: The telnet server serves telnet sessions; it uses
# unencrypted username/password pairs for authentication.
service telnet
{
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        only_from       = 192.168.2.10
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
        disable         = no
}
```

7. Finally, on Arwen, use **service xinetd restart** to make the settings take effect.

8. On Frodo now, try logging in through an SSH tunnel. Use the following to create the tunnel:
   ssh -L 8000:192.168.2.9:23 cis192@172.30.4.xxx
   (where 172.30.4.xxx is Elrond)

9. On Frodo, from a different terminal, e.g. tty2, use the following to connect to the Telnet server on Arwen:
   telnet localhost 8000
   (after an annoying delay, login as cis192)
   echo this is a secret
   exit

10. Now repeat Step 9 two more times, but capture the packets in a file for viewing on Wireshark.
    a. On Elrond, set up to capture encrypted traffic from Frodo to Elrond:
       tcpdump -i eth0 -s 0 -w elrond.eth0.capture
    b. Repeat Step 9 above on Frodo so you can capture the login, echo and exit commands. Use Ctrl-C to end capture.

c. On Elrond, set up to capture clear text traffic from Elrond to Frodo:
`tcpdump -i eth1 -s 0 -w elrond.eth1.capture`

d. Repeat Step 9 above on Frodo so you can capture the login, echo and exit commands. Use Ctrl-C to end capture.

e. Copy your captures to Frodo:
`scp elrond.eth* cis192@172.30.4.yyy:`

11. On Frodo, run Wireshark and open the two capture files. Get screen shots of the following:
    - The encrypted (Frodo to Elrond) "Follow TCP stream" of logging in as cis192 and typing the **`echo this is a secret`** command.
    - The clear text (Elrond to Arwen) "Follow TCP stream" of logging in as cis192 and typing the **`echo this is a secret`** command.

12. Copy the following information to your lab report:
    - **route -n** output for Frodo
    - **route -n** output for Elrond
    - **route -n** output for Arwen
    - **cat /etc/xinetd.d/telnet** output for Arwen
    - **iptables -L** output on Arwen

To turn in
Check your work for completeness then submit as many times as you wish up until the due date deadline. Remember, extra credit labs are not due till the last day of class.

Email me two Wireshark screen captures at risimms@cabrillo.edu showing:

- The encrypted (Frodo to Elrond) "Follow TCP stream" of logging in as cis192 and typing the **echo this is a secret** command.
- The clear text (Elrond to Arwen) "Follow TCP stream" of logging in as cis192 and typing the **echo this is a secret** command.

Submit your lab report on Opus using:

cp labX1 /home/rsimms/turnin/labX1.$LOGNAME

Grading rubric (30 points)
3 points for correct submittal of lab report into turnin directory
3 points for 100% complete header in lab report
4 points for correct Frodo route -n output
4 points for correct Elrond route -n output
4 points for correct Arwen route -n output
4 points for correct Arwen telnet server configuration
4 points for showing encrypted Frodo to Elrond Wireshark TCP stream
4 points for showing clear text Elrond to Arwen Wireshark TCP stream