— Lesson Plan —

Using Protocol Analyser Software*

geoffrey hector robertson
geoffrey@zip.com.au

December 14, 2002

Document Description: Lesson Plan for a Cisco CCAI Semester 1 Demonstration Presentation

References: Cisco course material: CCNA Semester 1 Chapter 11.9

`http://cisco.netacad.net`

Instructions: Read through these notes and do the practical exercises.

1 Lesson Preparation

- Prepare this Document!
- Check that `Ethereal` is installed on Lab machines
- Prepare Slides
- Photocopy Lab for students
- Check Laptop will work with Lab Projector
- Capture some sample TCP dumps (and remove passwds)
- Publish lesson on web

1.1 Underpinning Knowledge—Review

This lesson presumes knowledge of TCP/IP port numbers and addressing. Knowledge of ARP and protocols is also assumed.

- ARP—Finding a MAC address Slide 11.3.3
- TCP Segment Format Slide 12.2.1-2
- TCP three way handshake Slide 12.3.2-1

2 Lesson Presentation

2.1 Objectives per Cisco e-materials

Objective 11.9.1 The purpose of this target indicator is to expose the students to a fun an informative network troubleshooting tool, that is the protocol analyzer software.

Objective 12.3.1 The purpose is to illustrate that the way TCP provides software services to upper layers is through these numbers—they are a menu of services. Students should know the port numbers for ftp, telnet, smtp, dns, tftp, and snmp.

2.2 Vocabulary

TBA

2.3 Focus Questions

Wing

2.4 Teaching sequence

1. Show objectives
2. Review of stuff from 1.1 above
3. Look at lesson on web:

   ```
   http:
   lcdp.sh.net
   ```

4. Do Lab 4.1
5. Display and discuss firewall logs
6. Demo of `ethereal`
   (a) jellybean.logs
   (b) arp
   (c) telnet

(d) ssh

7. Show pictures of Fluke Protocol Inspector
8. Do Lab 11.9.1
9. Do Lab 12.1.3
10. Homework: do it at home and look at your own network

2.5 Key Graphics

- Picture of the Fluke protocol analyzer

2.6 Online

`http://lcdp.sh.net/cisco`

3 Lab/Activity

3.1 Activate a `telnet` session

1. login to zipper using telnet

```
C:\> telnet zipper.zip.com.au
Username: zork
Passwd: saturday
```

2. cat the list of TCP/IP ports: (press arrow keys for up and down, q to quit)

```
$ less /etc/services
```

3. do some nameserver lookups:

```
$ nslookup 216.239.32.10

$ nslookup microsoft.com
```

3.2 Check the Online Documentation

1. use a web browser to look at lcdp.sf.net

3.3 Explore *Fluke Protocol Inspector*

1. Open the application:

```
Start > Programs > Fluke Protocol Inspector > Fluke Pro-
tocol Inspector
```

2. Use intuition to use *Fluke Protocol Inspector*

3.4 Further Investigations

1. Use a web browser to look at `http://lcdp.sf.net`
2. Use `ftp` to upload something to a web site
3. Look at `arp` tables
4. Look at `/var/log/kernel.log`: walk through the data
5. Explore for other tools for protocol analysis and packet sniffing.

4 Assessment

- Do the 10 review question at the end of Chapter 12.
- Do the Chapter 12 test.

5 Reflection

mmm... reflect on this.

6 Homework

Do one of the sections below depending on the platform available to you. Note that you may view private and possibly sensitive data such as other peoples email and passwords. Do not abuse this access to information.

6.1 On a Legacy Commercial Operating System

1. Purchase and install `Fluke Protocol Inspector` software
2. Capture, examine and explore some dumps from a network near you.

6.2 On Linux

1. Install `tcpdump` and `ethereal` as required.
2. Capture, examine and explore some dumps from a network near you.

7 Resources

7.1 Web Sites

`http://lcdp.sh.net/cisco`