Quick Reference Step-by-Step Lab 5 Instructions: Just a Scan, Ma'am

Step-by-Step Instructions: **justascan.pdf**
Trace File: **justascan.dmp**
"Watch the Lab" File: ***justascan.avi (XviD codec) or justascan.wmv***

Step 1: **Create an *Ethereal Labs* directory** on your hard drive and **copy the trace files** from the LLK6 over to that directory.

Step 2: **Launch Ethereal**.

Step 3: Select **File > Open** on the Ethereal menu bar. Select **your local drive** off the drive list and double-click on the **Ethereal Labs directory** you created in Step 1. Double-click on the ***justascan.dmp*** trace file.

Step 4: This trace file contains what appears to be a scan on a target system, 10.1.0.1. Are these scans really coming from 10.1.0.2? **Look closely at packets 13, 14 and 15**.

Step 5: **Click on packet 13**. Ethereal decodes the destination port as "echo." Click on packet 14 – uh, oh. We can see the scanner has responded with an ACK to complete the handshake. If this was a spoofed address, the scanner doesn't need to finish up the handshake. This is a great indication that the scanner is really using IP address 10.1.0.2 at this time. Now they may have stolen it temporarily from another user on the network – but at this time, it appears that this scanner is using 10.1.0.2.

Step 6: What else is happening in this trace? **Scroll through the trace to the end**. What changed?

Step 7: Did you notice the sudden change in the destination port numbers? **Look for the pattern**.

Step 8: **Click on packet 29**. Ethereal has decoded the destination port field as "nameserver." To learn what port number is defined, look inside the detail decode of that packet.

Step 9: **Continue scrolling through the trace and write down the port number pattern**.

Step 10: Ok… so now we can clearly see a pattern—start at x, increment by 4 and repeat three times in a row, then drop back to x+1. Repeat. Unfortunately our target isn't responding any more. In fact when this trace was taken our target never did respond again – it died. Why?

Well – did you notice what else changed suddenly at packet 27? Click **View > Time Display Format > Seconds Since Previous Packet** to ensure you are looking at the time from the end of one packet to the end of the next packet.

Now **examine the trace from packet 27 to packet 38**. What is the new rate of the scan? How does that compare to the scan process in packets 1 through 26?

If you'd like to be walked through this process, check out the *BYOL* section of LLKv6.
See the ***Laura Chappell Master Library (LCML)*** at www.packet-level.com for additional self-paced labs.