Advanced Unix System Administration
Spring 2008
Homework 3

This assignment is due via email to <sluo+decal@ocf.berkeley.edu> by 11:59 PM on **Monday, April 28**.

1. *Networking on paper.* Here's an exercise to test your understanding of TCP/IP over Ethernet.

   a. Your company needs five different networks, four small networks of about 20 servers each, and a larger network of clients with addresses assigned by DHCP. You have the IP address range `172.17.42.0/24` to work with (I know this is RFC 1918 space – it's an example). Suggest a way to divide up this netblock into the networks you need.

   b. A computer on an Ethernet network with MAC address `FF:FF:FE:09:42:A3` and IP address `172.17.42.37` sends the message `Hello, world!\r\n` via UDP from port 51500 to a computer with MAC address `FF:FF:FB:3D:28:9C` and IP address `172.17.42.58` on port 9. Describe each of the Ethernet frames resulting from this conversation. Assume the sender's ARP cache is empty at the beginning of the conversation. *Note:* you do not need to write out each frame byte-by-byte – a description of the header and contents of each frame will do.

   c. A computer with IP address `172.17.42.37` initiates a TCP connection from port 51501 to a computer with IP address `172.17.42.58` on port 7. The computer on `.37` sends the string `Hello, world!\r\n` to the peer, which echos back the same message; the two computers then close the connection. Describe each of the IPv4 packets resulting from this conversation. *Note:* you do not need to write out each packet byte-by-byte – a description of the header and contents of each packet will do.

2. *Idle scan.* TCP initial sequence numbers aren't the only numbers that are problematic if they are predictable. There's an interesting technique called "idle scan", implemented in recent versions of `nmap`, that relies on a "zombie" host whose IPID numbers are predictable.

   a. How does this scan work? Why does the zombie host have to be idle? Where do the predictable IPID numbers come in?

   b. From where does the scan appear to be coming from, the scanning host or the zombie? Why? Why might this be a problem if a zombie on your network is being used to scan one of your machines? *Optional:* If you have access to a suitable zombie host and a machine which you can do network configuration on (not your scanning host!), verify this.

c. What can you do to prevent idle scans from being launched from inside your network?

3. *Packet sniffing. Optional.* Go capture some packets on your favorite network. Analyze the traffic streams, and identify the conversations going on in the capture (who's involved, what protocols they're using, what they're doing). *Note:* This is a lot more fun if you do it on a non-switched network – public wireless networks are probably best.