Scapy

Spoofing Packets (Part I)

You are going to create a variety of spoofed packets using scapy. For each of the following, the source IP of your packet should be 1.1.1.1 and the destination IP should be 144.38.193.245. (So, unless otherwise indicated, all your packets will be in an IP datagram).

After you have created the correct packet, use the scapy send function to send it. If your send was successful for a particular test you should be able to see an entry for it on this simple php page here
You should use a VM that is on the CIT VM farm.

Each packet should carry your last name as raw data (innermost layer of packet). To add raw data to a TCP datagram you would just do: TCP()/'francom' . 'francom' is the raw data. (lowercase)

Note that we arent' doing any FLOODING!!! We are just creating a single spoofed packet.

Packet 1 (2 pt)

IP datagram should carry an ICMP (echo-reply).

Packet 2 (2 pt)

IP datagram should carry a TCP segment with source port set at 9999, destination port at 34567.

Packet 3 (2 pt)

Spoof a TCP Syn segment. Source port should be 4567, destination should be 3210. Similar to the last one but make it a Syn. (Only one argument changes)

Packet 4 (2pt)

Spoof a UDP packet. Source port should be 55555, destination should be 33333.

Packet 5 (4pt)

Spoof a DNS answer. You need to spoof a DNS answer to `computing.utahtech.edu`. You need to make an answer look legitimate.

The easiest way to do this is as follows:

Copy the following code to a file called dns_scapy.py and run it using `python dns_scapy.py`. From the same machine (but different terminal), issue a dig request to the site `computing.utahtech.edu`. You should see information about how to correctly build the packet from that result. You will want to edit the dns_student.py file to do this. I have provided some hints in the file to get you started.

The resultant IP datagram that you send to the above host should contain the spoofed source IP (1.1.1.1). The resultant spoofed answer you should change the actual response (bling was 216.343.131.135) to a spoofed machine under your control (3.3.3.3). You should still include your firstname in the raw data, (i.e. IP()/UDP()/DNS()/'joe')

NOTE: As you do the above, if you do not recreate the UDP packet, you will have a checksum error and the packet will not send!

To Submit

Nada, I will look at the website.