

Homework 3

1. A network interface is the hardware or software interface between two devices on a network and the IP address is the address assigned to each device on the network. Therefore each device with a NIC needs its own IP address. However, people on different LAN's get their IP address assigned by the router and all traffic exiting the LAN goes through the router and so the packets ultimately get the routers IP address.....this means that the IP addresses of devices on different LAN's won't interfere so they can have the same IP address (again, as long as they are on different LAN's).
2. If your computer is on a LAN that uses NAT, the computer outside of the LAN can't generally initiate a communication session directly with my computer because my computer is connected to the internet via the router. So any communication must go through the router and then the router sends it to me. The IP address I have only makes sense locally so anyone outside of the LAN that tries to send me via my IP address directly will not make it to my computer.
3. You could do a few things to discover if a man-in-the-middle is intercepting your communication with the server
 - a. Since the server is capable of public key encryption you could encrypt your message with the servers public key and send it to the "server". Upon receiving the message, the server must decrypt it with the matching private key. The attacker however does not have this key and can thus not properly decrypt the message.
 - b. You could also sniff packets yourself (there are ways to identify if other devices NIC is running in promiscuous mode which can definitely be an indication of an attacker.)
 - c. You could also check for multiple mac addresses on the network since the attacker would have had to fake being the server (probably send you a generated arp reply) in order to connect with you.
4. Three subnets: Orlando (4000 computers), Chicago (2000 computers), LA (8000 computers); IP addresses start at 192.200.0.0
 - a. Orlando has 4000 computers so it needs 12 ($2^{12} = 4096$) bits.
 192.200.0000**0000.00000000**-192.200.0000**1111.11111111**
 192.200.**0.0**-192.200.**15.255**
 - b. Orlando's subnet in CIDR Format: 192.200.0.0/**20**
 - c. Chicago has 2000 computers so it needs 11 ($2^{11} = 2048$) bits.
 192.200.0001 **0000.00000000** - 192.200.0001 **0111.11111111**
 192.200.**16.255** - 192.200.**23.255**
 - d. Chicago's subnet in CIDR Format: 192.200.**16.0/19**
 - e. LA has 8000 computers so it needs 13 ($2^{13} = 8192$) bits.
 192.200.0010 **0000.0000 0000** - 192.200.0011 **1111.1111 1111**
 192.200.**32.0** - 192.200.**63.255**
 - f. LA's subnet in CIDR Format: 192.200.**32.0/19**
5. IP broadcast messages can be used to perform a smurf DOS attack. This is really very

simple in that when a computer is in “broadcast” mode it can send a broadcast packet that is received by every address on the network. Therefore the attacker can send an ICMP packet to the broadcast address with source address of the target (spoofed). Then all the other computers on the network will send an ICMP reply to the spoofed target all at once and overwhelm the targets bandwidth.

6. The attacker should trigger 64 requests to compromise the DNS cache with 99% probability.

- a. DNS ID's (16 bits) pseudorandomly chosen in range: $1 - 65,536 = 2^{16}$
- b. Attacker sends 1024 false replies per request
- c. So the failure to match probability per request is therefore

$$P(F) = (1 - n/2^{16})^m$$

n = number of requests

m = number of responses

$$P(S/request) = 1 - [(1 - 1/2^{16})^{1024}] = 1/64 = .0156$$

so he has a ~.0156 chance of success with each request

therefore if he makes ____ requests

$$P(S) = .99 = P(S/request) * requests = .99/.0156 = 63.46$$

so he needs to make ~64 requests

7. Deep packet inspection cannot be performed on protocols such as SSL and SSH because the data part of the packet is not plain text....it is encrypted. Though DPI firewalls can see that it is encrypted and block the packet.