ITP 125 – Lab 3

2/5/17

Questions

1. The ping of death is a malicious ping to a computer. The ping of death consists of a ping packet that is larger than the typical 56 bytes, which causes a buffer overflow. This buffer overflow can lead to the system crashing and can even inject malicious code into the system.
2. ARP spoofing’s goal is make someone’s computer look like it’s someone else’s computer. ARP does this by associating a number to your computer that actually belongs to another computer. ARP spoofing allows attackers to intercept data going into your computer and stop or modify the data going into your computer. ARP is also dangerous because it allows attackers to spy on information entering and exiting your computer, which can include and modify the data so that you cannot tell the difference between the real and fake information.
3. DNS spoofing causes the wrong IP address to be returned by a computer’s name server. This results in the information that is supposed to be sent to the victim’s computer to be sent to the attacker’s computer instead. Regular people may not notice that they are not receiving the correct information because they do not understand how their IP address is connected to the sending and retrieval of information. To prevent this type of attack, people can ignore DNS information packets that do not appear relevant to the query they made. People can also use source port randomization for DNS requests and cryptographically secure random numbers for selecting the source port.
4. Step 2 was under the Network layer

Step 3 was under Data Link, Network, and Session layers

Step 4 was under Network and Session layer

Step 5 was under Network layer

Step 6, 7, and 8 were under the Network and Session layers

5. TTL stands for Time to Live and is a tool that limits the lifespan of data in a computer network. This prevents data from moving around indefinitely. TTL is set by the sender and is an upper bound on the time the data can exist in the system. If time is up before the data reaches the system then the data is discarded and an error message is sent back to the sender.