

Name:

Information Assurance: Homework 7

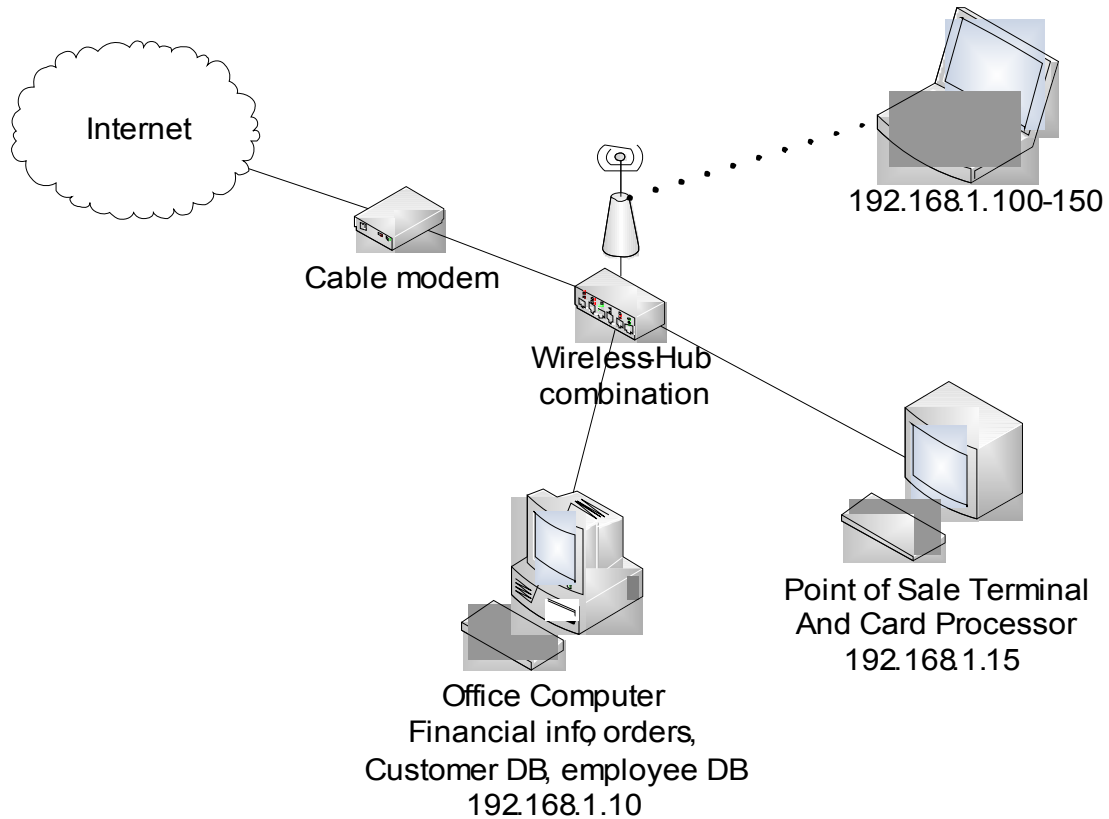
Due November 14, 2007.

1. Both ARP and DHCP have traded off security for flexibility and ease of use. Thus, on start up, a malicious player can use these protocols to gain a man-in-the-middle position between his victim and the outside world
 - a. Describe how this can be done for either ARP or DHCP.
 - b. In class we mentioned that encrypting all traffic would mitigate this problem. How would encryption defeat this attack?

2. Use SSH to access a machine in the network security lab. See the newsgroup for the address and login information. Scp access will be allowed from the lab machine back to the outside world.
 - a. From this machine, use nmap to discover what is running on the 192.168.50.0/24 network. Use the -A flag to get additional information. Submit the nmap output.
 - b. Try to fingerprint a service directly using telnet. Assuming that nmap reports one of the other machines is hosting a web server, use “telnet <address> <port>” to connect to the service directly. Anything you type in will be feed to the web server. Save the response from the service and describe how you used this information to deduce that it is indeed talking HTTP and the type and version of the service.

3. Your friend has opened a coffee shop, and he wants to offer free wireless Internet access to attract lingering customers who will buy much coffee and many overpriced pastries. His initial network plan is below. He would like your opinion and suggestions for improvements. He wants to make sure that his customers have a hassle-free experience, so he is very reluctant to add WPA (authentication and encryption) to his network. Currently, it is an open network and he advertises his SSID as “coffee”. He is using the hub built into the wireless router to connect his main office machine and his networked point of sale terminal (cash register). The wireless router also performed basic address hiding address translation of all the internal non-routable addresses behind the one routable address given by his Internet service provider. The hub also connects to the cable modem that leads to the outside world.

Name:



- a. Analyze the current architecture and identify three potential threats that could affect confidentiality, integrity, or availability for him, his customers, or the surrounding community
 - b. Update the original architecture to address the threats you identified in part A plus any additional changes you feel would be beneficial. Describe how your changes improve network security.
4. Below are three scenarios and three technologies. Match up each technology to the most appropriate scenarios, and explain why this is the best match.

Scenarios

- a. Concerned about ill-defined inappropriate activity on the desktop network at work.
- b. Desire to reduce clearly bad traffic as soon as it enters the enterprise environment.
- c. Ensure that no one at your site intentionally or accidentally visits a set of known bad web sites or executes scripts or script segments that are known to be malevolent.

Technologies

- W. Packet filter
- X. Application firewall
- Y. Network intrusion detection