

Name:

Information Assurance: Homework 7 Answers and Comments

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.

Both protocols have the same dynamic style. For ARP consider a case where machine A at IP address X and MAC address A, needs to learn the MAC address that corresponds to IP address Y. Machine A issues a broadcast request for the MAC address that is currently using IP address Y.

Say machine B with MAC address B is really using IP address Y, but machine C with MAC address C wants to intercept all traffic from A to B. B issues an ARP response to A saying that the MAC address for IP Y is B. However, C also issues a response (in fact machine copies of a response) saying that the MAC address for IP Y is C.

If A picks C's response, it will mistakenly send traffic meant for machine B to the physical address for machine C. Machine C can then turn around and forward the packet to machine B, so it will be difficult to notice the interception.

With DHCP, the attacker can similarly step up and answer a client's broadcasted request for an IP address assignment. Just providing the address does not give the attacker much advantage. But the attacker can also provide assignments for default gateways and name servers. Through this assignment, the attacker can guide traffic from the client through machines the attacker controls.

- b. In class we mentioned that encrypting all traffic would mitigate this problem. How would encryption defeat this attack?

The encryption would not prevent C from placing itself in the middle. But it would reduce the value of being in the middle. If C does not know the key used by A and B, it cannot read the data passed between them.

Some of you noted that one could augment ARP and DHCP packets to be authenticated and/or encrypted. However, in this case you lose the dynamic benefits of these protocols. There would be a start up step to register keying information on each participating host.

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.

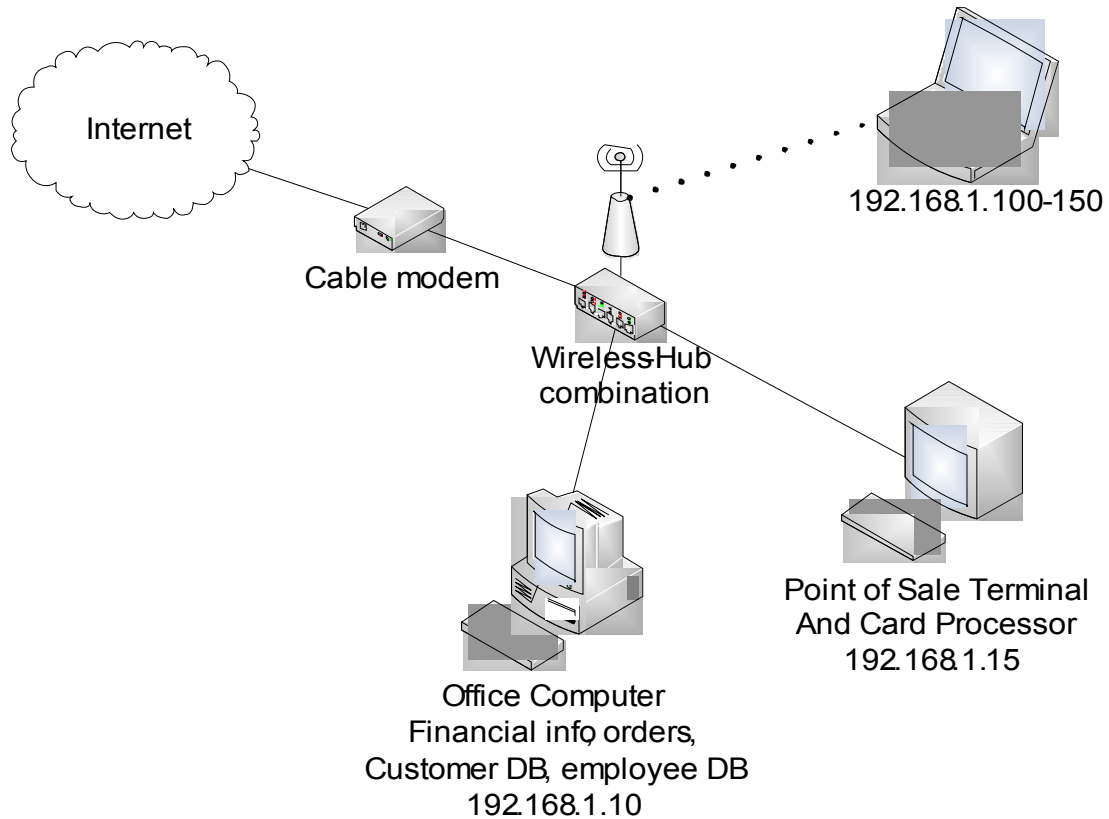
Name:

- 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.

Almost everyone did fine on this. Most people found 3 machines. Some found four. The Vista machine must have gone down pretty early on.

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

Potential threats:

- *Someone within range of the wireless hub connects, and uses the coffee shop Internet connection to perform unsavory activity, e.g., launch spam, attack other systems, make criminal connections.*
- *All computers are on the same network link. If an untrusted entity can get on the link (e.g., by the wireless network), they are in an excellent position to probe the more sensitive machines (e.g. Cash register and office computer) for vulnerabilities to exploit.*
- *There is minimal protection from traffic coming in from the Internet. Entities on the Internet could try to attack the fixed coffee shop machines and the wireless customer machines.*
- *Almost all critical and sensitive applications are running on a single computer. A breach of one application on that computer makes all critical applications vulnerable.*
- *Denial of service by attackers using up all network bandwidth.*
- *Denial of service by attackers using up all DHCP addresses preventing legitimate customers from getting and address and communicating on the network.*

Name:

- 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.

There are a variety of new network architectures possible. The new architecture should introduce changes to directly address threats identified in part A

- *Introduce a basic firewall after the cable modem. Block all (or nearly all) incoming traffic. Introduce address translation. Presumably, the original design already had address translation someplace. It is unlikely that the coffee shop owner would have paid for a large number of routable addresses.*
- *Adding WPA would address the problem of random individuals taking advantage of the network connection for undesirable behavior, but it would degrade the experience for legitimate customers. If the shop owner isn't willing to turn on WPA, he should invest in some intrusion detection software and watch and act upon the results.*
- *The design should have a segmented network. The office machine and the point of sale machine should be on a separate network from the wireless network. There probably should be some filtering between those two networks. You probably do not need any communication between those two fixed computers and the wireless network.*
- *The single office computer should be replaced with several computers to help prevent a domino effect if a exploitable vulnerability is found in one of the applications. Perhaps virtualization software could be use to better isolate applications with out the cost of additional hardware.*
- *Addressing the denial of service attacks is a bit more difficult. If the attacker is working from a single machine or a fixed set of machines, you could block access by MAC address, but the savvy attacker is likely varying his MAC. You could incorporate QoS to limit the bandwidth used by an individual address.*

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

Name:

My answers would be

A and Y – On the inside network, you cannot statically constrain packets of expected services. You may not know enough about current address assignments to traffic filter on an employee by employee basis. Some protocols with many known attacks (like netbios) might be needed internally. With IDS, you could allow netbios but look for and react to odd behavior on that protocol. With packet filtering and application firewall, you have more fixed constraints. An intrusion detection device could in theory detect and notify you of unusual characteristics of otherwise allowable traffic (e.g., a sudden burst of traffic accessing the departmental design file server.

B and W – At the entry point of the network, you want to make sure that you don't slow things down much. If there are known bad addresses or very clear rules about services that aren't accessible from the outside (like netbios), a packet filter can quickly drop obviously bad packets. By eliminating these packets early, you reduce the workload on the rest of the network. As many of you noted, this won't catch all the bad traffic, but it reduces the workload on the IDS device. The IDS would also work in general. However, if you know that all traffic from a particular address is suspect, the IDS will likely allow in some traffic from that address if it does not detect a problem.

C and X – To filter for bad web sites and scripts, the tool must have access to the HTTP application level data. This is not available in the packet filter. Since you are filtering for a fixed set of bad things, the intrusion detection would be overkill. The application firewall completely reconstructs the layer 7 stream, so this is the best place for filtering for fixed characteristics for that layer 7 traffic.