Homework 3: Strategy

**Due: April 16, 2012 5:30pm EDT**

For the purposes of this assignment, the following two fictitious entities are described. You may use other entities in your solutions, but must describe them in at least the level of detail provided here.

**Sales:** This is a network supporting on-line sales for a large corporation. This network uses a mix of current Windows Server and Linux systems, with a total of about 40 servers. There is a firewall with a fairly open rule-set (network login open in and out, file sharing in and out with password authentication) anti-virus and anti-spam filtering and Windows update configured.

**Evil:** Small site owned and configured by an intruder. The site is on-line only when actively in use. Shared T1 access through commercial ISP that has no monitoring installed. Evil controls a small (10,000 node) botnet.

1. (35 points) Assume you are the head of the intrusion response team at Sales. You do not have a-priori knowledge of threats to your network or likely attackers. You can control the internal and border configurations of Sales, and may degrade, but not halt, network services.

a) (12 points) What strategic principles (as discussed in class) would guide your deployment?

b) (12 points) What methods would you apply to implement those principles? Assume you must minimize service degradation.

c) (11 points) How can you assess the success of your defenses?

2. (35 points) Assume you are the intruder running Evil. You have a strong motivation to interfere with Sales by compromising a host or by redirecting those attempting to contact Sales, You have limited resources (i.e., you cannot relocate and Sales is not in physical proximity to you.)

a) (12 points) What strategies could you employ to compromise the privacy of Sales?

b) (12 points) What strategies could you employ to compromise the availability of Sales?

c) (11 points) How can you assess the success of the strategies outlined in a and b?

3. (30 points) Describe three policy issues that arise out of these offensive and defensive strategies.