Homework 1

CIS 4930 / CIS 5930
Offensive Computer Security (OCS2014)
Spring 2014

Due January 15th, 2014, by *MIDNIGHT*
Worth: 100 points

Electronic turn in (Turn in via email to: redwood@cs.fsu.edu) DO NOT EMAIL TO MY @fsu.edu account. The email must be titled in the following format:
"[OCS2014] hw1 <your last name>". (where <your last name> is your last name)
Example: [OCS2014] hw1 redwood

#1) [15 points total] Visit http://www.digitalattackmap.com/ and pick out three interesting periods of activity (at the bottom). For each provide the following [each is worth 5 points]:

A. The date (period)
B. Pick a major botnet's activity and list:
   a. [1 point] Source and Destination
   b. [1 point] How long the attack has been occurring
   c. [2 points] How has the attack been pulled off ? (Briefly describe and explain, not just list "Traffic Misuse", or "SYN Flood". Go into a little detail).
C. [1 point] Which country(s) seemed to be generating the most botnet attacks

#2) [15 points] Consider the disclosure debate for this question, and how in the past companies reacted hostile to vulnerability researchers disclosing vulnerabilities in their systems:

A. [10 points (5 each)] Pick two major companies that suffered major breaches (by hackers) and explain what happened and how they informed their customers (right away? delayed? never? by "i'm sorry" on twitter??). What were the consequences of the breach? Who really was the victim?

B. [3 points] It is likely that the two companies you picked already have internal security auditing as well as contracted out penetration testing to comply with government / industry regulations.

   In many cases the regulations do not require the company enact any of the suggested security changes from the audit / test results. For each of the above incidents do you think better regulations or better testing (or something else or nothing at all) would have helped prevent the incident? Explain for each [1.5 point each].

C. [2 points] Do you think most small business or startup could afford proportional consequences? Why or why not?

#3) [15 points (one point each)]

1. What is confidentiality?
2. What is integrity?
3. What is availability?
4. What is a Denial of Service attack?
5. What is a virus?
6. What is a trojan?
7. What is a botnet?
8. What is a zero day?
9. What is a n-day?
10. Is a bug the same as a vulnerability?
11. What is a weakness?
12. [4 pts] Name 4 ways an attacker can act anonymously online

#4) [55 points] Read Dan Geer's 2013 FALL UNC CHARLOTTE CYBER SECURITY SYMPOSIUM keynote speech: http://geer.tinho.net/geer.uncc.9x13.txt

A. [20 pts] What is the thesis of his talk? (Explain well)
B. [5] What is your stance on the subject?
C. [5] What is the problem with the defensive mindset? Do you agree?
D. [5] What aspects of the internet provide a permanent structural advantage to attackers?
E. [5] How do biometric-based authentication systems (like the new iphone's fingerprint password) change the debate over the 5th amendment?
F. [5] What are the two aspects of privacy the author discusses?
G. [5] The author asks "Is all the technologic[al] dependency and the data that fuels it making us more resilient or more fragile?". What do you think?
H. [5] Do you think you would change any of your opinions so far if a cyber attack seriously crippled the nation's critical infrastructure, (electric grid, water / sewer, oil & natural gas), cost many lives, and forever changed "modern society" as we know it (AKA a cyber 9/11 (a term that your instructor hates))? If so explain.