CS 4235: Introduction to Information Security November 8, 2011

Problem Set 4: Attacks

Instructor: Prof. Nick Feamster *College of Computing, Georgia Tech*

This problem set has three questions, each with several parts (plus a fourth fun activity). Answer them as clearly and concisely as possible. You may discuss ideas with others in the class, but your solutions and presentation must be your own. Do not look at anyone else's solutions or copy them from anywhere. (Please refer to the Georgia Tech honor code, posted on the course Web site).

Turn in your writeup **November 22, 2011** by 11:59pm. *Please upload your solutions to T-Square. Other forms of submission will not be accepted!* We will be providing more information about how to turn in your assignment as the due date approaches.

1. **One-Time Pads (30 points).** Eve has been eavesdropping on Alice and Bob's communications with each other for some time. They appear to be using a one-time pad to keep their messages secret. Eve suspects that the plaintexts are just English sentences encoded in the standard ASCII character set, and the ciphertexts are generated using bitwise exclusive-or (XOR) with the pad. For example, in ASCII the character 'a' has hexadecimal value 61 (or 01100001 in binary), which when bitwise-XORed with the hexadecimal pad value 83 (10000011 in binary) yields the hexadecimal ciphertext e2 (11100010 in binary).

   Knowing that the one-time pad is hard to use properly, Eve has been storing every ciphertext sent between Alice and Bob, and XORing pairs of them to look for any anomalies. One day she notices that a pair of ciphertexts XOR to a value (shown below in hexademical) that appears "strange". She suspects that Alice and Bob may have reused part of their pad, and asks you to recover the plaintexts.

   - (10 points.) Why has Eve been XORing pairs of ciphertexts? What is "strange" about the XOR value below that she found?
   - (10 points.) Formulate and describe your approach for helping Eve. The messages may be time-sensitive, so your attack should work as quickly as possible.
   - (10 points.) Give as much of the plaintexts as you can find.

```
03 03 0b 4f 45 5b 48 09 0b 54 54 1b 4f 1d 0d 12 45 57 0c 54 48 00
02 45 4e 2a 19 0b 09 53 00 3a 55 1f 19 15 01 07 45 48 11 17 17 54
0b 5a 55 53 28 05 4b 0a 55 01 55 02 04 44 58 4f 42 00 07 45 49 1b
52 01 00 1f 1c 0a 4f 15 0b 01 1c 00 1e 0e 44 42 1a 08 00 17 0d 04
4c 44 42 48 53 2b 51 11 00 11 06 00 43 54 4f 10 02 45 13 42 01 1a
00 49 0a 11 00
```

2. **Port Scanning (40 points).** In this hands-on problem, you will re-create some of the results that we performed in lecture, using the `nmap`.

   - (10 points) Explain how port scanning works, and why an attacker might run a port scanning tool.
   - Download the nmap tool and install it somewhere where you can run it. (`http://nmap.org/download.html`).
   - (5 points) Run `nmap` against `porter-square.cc.gt.atl.ga.us`. What ports do you see open on the machine? How did `nmap` discover this? Copy the output of running the tool into your writeup. Based on the list of open ports, make your best guess at the services running on this machine. *Extra credit:* Extra credit if you can figure out the versions of services running on the machine! (This will require tools other than `nmap`.)
   - (5 points) Use `nmap` to determine the version of the operating system that `porter-square` is running. What operating system is running? How does `nmap` determine the operating system?
   - (10 points) Use `nmap` (or, if you prefer, a script) to determine all hosts on `130.207.0.0/16` that are running a Web server. *Hint:* You can use some options in `nmap` to scan an entire network subnet, and to restrict the scanning to a particular port. This will go much, much faster if you ise the "-p" option in `nmap`.
   - (10 points) Find a machine on the wide-area Internet that has the Simple Mail Transport Protocol (SMTP, port 25) open. List the IP address of the machine that you found and show the output from your `nmap` tool. This is called an "open mail relay". How might an attacker be able to use an open mail relay?

3. **Search Engine Optimization Competition (30 points + quiz bonus points).** *Complete in your project groups!* Construct a Web page that comes up #1 (or as high as you can manage) in Google's search engine when a user searches "radiator palace summit seaweed". The winner of the competition will be judged *in class* on November 22. All members of the group will receive 5 quiz bonus points!

4. **For fun: Tor.** Run and install Tor (`http://torproject.org/`, if you haven't done so before. More to come on anonymity and privacy on the next (and last!) problem set!