CS 161 Computer Security

Fall 2006 Joseph/Tygar

Midterm 3

PRINT your name: ______________________________, ______________________________
(last) (first)

SIGN your name: ____

PRINT your Unix account name: ___________________________

PRINT your TA's name: ___________________________

READ ALL INSTRUCTIONS CAREFULLY.

You are allowed to bring one 8.5”×11” page of handwritten notes with you, but no books, printouts, or other study aids. Calculators, computers, and other electronic devices are not permitted. Please turn off cell phones and music players and keep them off your desk, and remove headphones.

Write your answers in the spaces provided in the test; in particular, we will not grade anything on the back of an exam page unless we are clearly told on the front of the page to look there.

Please explain all work, but be concise.

If you think there is an error in the exam, please bring it to the attention of the exam proctor. If you find a question to be ambiguous, choose the most likely interpretation and state your interpretation explicitly.

You have 80 minutes. There are four questions, of varying credit (100 points total). The questions are of varying difficulty, so avoid spending too long on any one question.

Do not turn this page until your proctor tells you to do so.

Problem 1	
Problem 2	
Problem 3	
Problem 4	
Total	

Problem 1. [Auctions] (20 points)

This question will consider different types of auctions. For each auction type, we will ask you to describe how it works, and then to describe whether it ever makes sense for a bidder to bid less than his or her actual valuation (that is, the amount he or she considers to be a fair price for the item being sold.) Of course, the bidder wants to achieve the lowest price possible. Here is an example:

(x) How does a sealed bid auction work? Does it ever make sense for a bidder to bid less than the actual valuation?

> *A: In a sealed bid auction, each of the bidders sends a sealed, secret bid to the auctioneer, that only the auctioneer can read. The auctioneer sells the item to the highest bidder at the price bid. In some cases, it makes sense to bid less that the actual valuation; if a bidder suspects she will be the highest bidder, then she should only bid slightly more than what she expects the second highest-bid to be: in that way, she can save substantial money.*

Answer the following (maximum 4 sentences each):

(a) (10 points) How does a Dutch auction work? Does it ever make sense for a bidder to bid less than his or her actual valuation?

(b) (10 points) How does a second price ”Vickrey” auction work? Does it ever make sense for a bidder to bid less than his or her actual valuation?

Problem 2. [Attacks] (24 points)

Consider the Berkeley CalNet Authentication Web Server, which uses a web page with a user name and user password (the password must be between 9 and 255 characters, and must contain at least three of the following: uppercase letters, lowercase letters, numbers, punctuation, and all other characters), connected via SSL to net-auth.berkeley.edu.

Give at least 3 different plausible ways to attack such a system and gain unauthorized access (1-3 sentences each). (8 points each)

Problem 3. [Short answer] (30 points)

Give a 1-2 sentence answer for each question. (6 points each)

1. Why is having a non-executable stack and heap insufficient to protect against buffer overflow code execution attacks?

2. Firewalls can be used to block all distributed denial of service attacks while allowing all authorized communications. True or false, and why?

3. How can a targeted worm or virus avoid detection by a virus scanner? Give the most relevant answer.

4. Joe wants to protect himself against rootkits, so he runs a virtual Windows XP system on top of Mac OS X. Is Joe vulnerable to Windows XP rootkits? Why or why not?

5. In a Mandatory Access Control system, how can an insider with access to a high-security file leak information to a low-security process using the virtual memory system? What is this type of attack called?

Problem 4. [E-Voting] (26 points)

Your task is to help the State of California develop certification standards for electronic voting machines (DREs).

For each of the three phases of electronic voting at a polling place, give the necessary preconditions and postconditions for a DRE to preserve the *integrity* of the vote. Assume that there are several multiple candidate races, each race has only one winner, and voters may vote for at most one candidate per race (voters may chose to leave any race blank).

Here are the three phases you will consider:

1. Machine preparation on Election day (before polling starts)
2. Accepting a cast vote (repeated throughout election day)
3. Finalization after the polls close

You do not need to consider transparency, privacy, or secrecy for this problem. Please limit yourself to conditions necessary for integrity. State your conditions clearly and precisely, and you shouldn't need additional explanation.

(a) (8 points) The first phase is preparation of the machine on election day before polling begins.

Preconditions:

Postconditions:

(b) (10 points) The second phase is casting of each vote. Specify the preconditions before a vote is cast and the postconditions after a vote is cast.

Preconditions:

Postconditions:

(c) (8 points) The final phase is finalization of vote totals at the end of election day after the polls close.

Preconditions:

Postconditions: