CS6573 MIDTERM, FALL 2009

OBJECTIVE

- This midterm was posted online October 22nd and is due on October 29th at midnight (1 week)
- This midterm is worth 15% of your grade
- In Sections 1 through 3, you are allowed to skip one 'A' question and one 'B' question total.
- In Section 4, you must answer two questions in no more than a half page each.
- Your grade will be determined out of 100 points (make sure it adds up in the end!)

Good luck!

CHANGELOG

10/22/2009 11:00pm - Fixed minor typos

1. SOURCE CODE AUDITING

1A. CODE COMPREHENSION – 15 POINTS

When presented with an unknown source code package, experienced software security auditors have learned that it's best to use several code comprehension techniques and switch between them for the following reasons:

- You can only concentrate intensely for a limited amount of time
- Different vulnerabilities are easier to find from difference perspectives
- Variety helps you maintain discipline and motivation
- Different people think in different ways

Describe the process you would take towards understanding an unknown source code package and the advantages and disadvantages of following that process (for example, differences in coverage of certain types of bugs, auditing speed, level of comprehension, etc).

1B. AUDIT ME – 25 POINTS

Identify and explain one vulnerability in two of the three attached files: midterm1.c, midterm2.c and midterm3.c

2. REVERSE ENGINEERING

2A. FIND THE KEY – 15 POINTS

Find the key in two of the three attached executable files: 1.exe, 2.exe, 3.exe. You must include a two to three sentence description of how you were able to obtain it and a screenshot of you solving it.

2B. FIND THE VULNERABILITY – 25 POINTS

Identify and explain any vulnerabilities in opcode 0x06 of GreenMan. Note the source of input and the line the vulnerability occurs on.

3. EXPLOITATION

3A. EXPLOIT MITIGATIONS – 15 POINTS

Describe one mitigation technique, implemented in a major OS, used to protect against the classic stack overflow.

3B. EXPLOIT ME – 25 POINTS

Write an exploit that executes a payload for any one vulnerable code path in GreenMan on Windows 2000.

4. GRAB BAG

The following questions are hypothetical and no "right" answers exist for them. You will instead be graded on your thought process and your evaluation of the scenarios. If there are any details about the scenarios that you feel are required to answer them, you may make up those details yourself.

4.1 PENETRATION TESTING GOALS – 10 POINTS

Is penetration testing goal-oriented or coverage-oriented? Is the purpose of a pentest to test the possibility that a goal can be achieved or to identify every possible path someone might take to reach that goal? More information about this argument is available here: http://seclists.org/pen-test/2009/Oct/23 . Take a side and argue it.

4.2 VULNERABILITY DISCLOSURE – 10 POINTS

You have identified an unknown vulnerability in a commercial product while performing a penetration test for a customer.

1. Why would you not be able to disclose this vulnerability?
2. Assuming you can disclose it, how do you disclose the vulnerability and why? What are the pros/cons of your approach?
    a. Disclose to security mailing list
    b. Disclose to specialized organization (ex. CERT, ZDI)
    c. Disclose directly to vendor
    d. Disclose to other clients of yours
    e. Do not disclose
    f. Other
3. Assume the vulnerability is in a Microsoft product. Using your answer from above, gather all of the e-mail addresses and other contact information you would need to report the vulnerability.

4.3 OPEN-SOURCE VS. COMMERCIAL SECURITY – 10 POINTS

Make an argument for what type of development model leads to better security – open-source or commercial product development.

4.4 IS THE OFFENSE WINNING – 10 POINTS

The defensive line has continually moved back in the figurative sand as the infosec industry has "matured." First we thought we could secure our perimeter, and then we thought we could secure our hosts, now we think we can secure our apps. Give a compelling reason why "Infosec" will not be synonymous with "Malware Analysis" and "Incident Response" in five years.