CS6573 MIDTERM, SPRING 2011

OBJECTIVE

- This midterm was posted online March 21st and is due on March 28th at midnight (1 week)
- This midterm is worth 20% of your overall grade
- In Part 1, you are allowed to skip one question
- In Part 2, you are allowed to skip one question
- In Part 3, 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!)

Bonus Points:

- You get 5 bonus points if you came up with a reasonable final project idea that gets approved

Good luck!

CHANGELOG

03/21/2011 6:20pm – Released to mailing list and Blackboard

03/21/2011 11:15pm – Fixed issue with Reversing #2

PART 1 (SKIP ONE QUESTION, 15 POINTS EACH)

1A. SOURCE CODE AUDITING

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 steps you would take in the first hour after receiving a large source code package to identify vulnerabilities in it and why those steps would be effective.

1B. REVERSING

Describe the steps you would take in *only the first hour* after receiving a large Windows binary to identify vulnerabilities in it and why those steps would be effective. You can list tools, techniques, processes, functions to breakpoint, imports, etc.

1C. EXPLOITATION

Choose two exploit mitigations from the following list. Explain a) what exploitation techniques they attempt to guard against and b) describe the techniques for bypassing them:

- Stack Canaries (/GS)
- SafeSEH
- SEH Overwrite Protection (SEHOP)
- Data Execution Protection (DEP)
- Address Space Layout Randomization (ASLR)
- Pointer Encoding
- Heap Metadata Protections (RTL Heap Safe Unlinking)

PART 2 (SKIP ONE QUESTION, 25 POINTS EACH)

2A. SOURCE CODE AUDITING

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

2B. REVERSING

Identify and explain the vulnerability in opcode 0x01 of the GreenMan server.

HINT: 00401030 is memset, 00401745 is strtol, 0040176E is printf, and 00401882 is malloc.

2C. EXPLOITATION

Your task is to exploit a simple stack buffer overflow in the IE6 browser included on the class VM. The VM has been pre-configured to disable DEP for that version of Internet Explorer. You should begin with the Vulnerable.js file and implement your exploit within the FooExploit() function. You may place the included files on the VM hard drive and open the index.html with IE6 or use the included webserver.rb script on another machine to host a simple webserver to launch the exploit from.

All the files required for this question have been included in 'C:\Windows\system32\TrailOfBits' in your VM but are also included in the midterm zip file for your convenience. Do not move the files from their location in system32 or the DEP exceptions will not work.

HINTS

1. The Vulnerable.js file already includes a pattern string that you may use to find offsets for significant elements of the exploit string.
2. There is a function called MakeString() that will build a string of a given length for you.
3. To create a payload with Metasploit use: './msfpayload windows/shell_bind_tcp R | ./msfencode -t js_le'. Don't forget that you also need to specify the badchars.

Partial credit will be given for demonstration of EIP control without a payload.

PART 3 (CHOOSE TWO QUESTIONS, 10 POINTS EACH)

You will instead be graded on your thought process and your evaluation of the scenarios in the following questions. If there are any details about the scenarios that you feel are required to answer them, you may make up those details yourself.

3.1 PENETRATION TESTING GOALS

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.

3.2 STATIC VS DYNAMIC REVERSING

Why are static and dynamic reversing looked at as different topics? Asked another way, why would you want to do both static and dynamic reversing to understand an unknown binary?

3.3 FACTORS INFLUENCING APPLICATION SECURITY

What factors surrounding an application influence its security more than whether it is open or closed-source? List at least three and how they affect the security of an application.

3.4 MOBILE DEVICES

Describe the process you would take towards compromising a modern smartphone or other mobile device. Identify which attack vectors you would assess, why, how you would test them, and what vulnerabilities you might expect to find.

PART 4 (FINAL PROJECT SELECTION, 5 BONUS POINTS TOTAL)

4A. WHAT IS YOUR PRIMARY FINAL PROJECT SELECTION?

4B. WHAT IS YOUR BACKUP FINAL PROJECT SELECTION?