

CS6573 MIDTERM, SPRING 2009

OBJECTIVE

- This midterm was posted online February 24th and it is due March 3rd at midnight (you have 1 week).
- Your grade will be determined out of 100 points.
- This midterm is worth 15% of your grade.

1. ANSWER ANY 2 OF THE FOLLOWING 3 QUESTIONS (30 POINTS):

1.1 SOURCE CODE ANALYSIS – CODE COMPREHENSION

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 different 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).

1.2 REVERSE ENGINEERING – FIND THE KEYS (CHOOSE ANY 2)

Choose any 2 of the following binaries, find the key/password to it, and document the method you used to find it.

- whatsthepassword.exe
- whatsthepassword2.exe
- pentest_midterm_spring2009.exe

Note: Your solution documentation can be as short as 3 sentences if it clearly explains what you did.

1.3 EXPLOITATION – THE BASICS (ANSWER BOTH)

PART 1 (10 POINTS):

```
int foo(int arg1, int arg2) {
    char bar;
    char buffer[10];
}

int main() {
    foo(42, 1);
    return 1;
}
```

Provide a picture of the call stack for the following code assuming we have just arrived in foo. Notes:

- The call stack is the stack after the prologue has been executed.
- I want to see everything including args, vars, etc, in proper places.
- Go with the more "generalized" picture if you think that something is compiler dependent.

PART 2 (5 POINTS):

You are "testing" an x86 application and receive an error stating "Cannot access memory at address 0x41414242". What was the part of your input string that overwrote EIP?

2. ANSWER ANY 2 OF THE FOLLOWING 3 QUESTIONS (50 POINTS):

2.1 SOURCE CODE ANALYSIS – VULNERABILITY IDENTIFICATION

The attached source code (htpasswd.c) contains a number of vulnerabilities. Identify and explain as many vulnerabilities as you can. Assume it is running on Linux.

Background about the application: htpasswd.c is used to update the flat-files used to store usernames. When you provide the htpasswd application with the correct username/password to authenticate to it, you are allowed to add usernames to a given flat-file userlist. Users in that userlist are then allowed to access whatever service that passwd file applies to.

2.2 REVERSE ENGINEERING – MALWARE REVERSING

The binary inside of malware_pw_is_infected.zip (password is 'infected') represents unknown malware which was found on a client's network. Answer the following questions about it:

1. Identify and explain the purpose of the binary.
2. The binary sends data on the network. Identify the protocol and the contents of its messages.
3. Identify one method of detecting this network traffic using a method that is not just specific to this situation, but to other ones as well (ie. for an IDS rule).
4. Identify and explain any techniques in the binary that protect it from being analyzed or reverse engineered.

Note: This virus is HIGHLY contagious. Make sure to analyze it in VMware with shared folders turned off!

2.3 EXPLOITATION – EXPLOITME

htpasswd.exe is a compiled binary of the application you audited in SCA 'Vulnerability Identification'. Write a stack overflow exploit for a vulnerability in the program which executes a payload. You do not have to use Metasploit.

Hint: Set Immunity Debugger to the JIT debugger for your system.

Note:htpasswd-static.exe and htpasswd-int3.exe have been provided for your convenience. You may write your exploit for whichever one you find easiest.

3. ANSWER ANY 2 OF THE FOLLOWING 4 QUESTIONS (20 POINTS):

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.

3.1 OPTION 1 – CHANGE YOUR GRADE

What methods, tools, and techniques would you use to change your grade to an A in this course? Assume the grades are created by Dan, entered into Blackboard, and processed by the Registrar.

3.2 OPTION 2 – BYPASS SECURITY CONTROLS

For those of you who attended Joe Rosenblatt's Wednesday talk at the ISIS lab on February 18th, explain how you would bypass the security controls on the Columbia University network *without being detected* to gain access to sensitive data.

3.3 OPTION 3 – RESOURCE ALLOCATION / TECHNIQUE EFFECTIVENESS

You have been given \$300,000 and a one-year timeline to provide risk transparency into a firm's Internet facing applications. How would you use your time and money?

3.4 OPTION 4 – MITIGATING CONTROLS

While on a penetration test, you identify a stack overflow in server software running on your client's mail server. The mail server is running Windows 2003 SP2 and the server software is written in C and compiled with a Microsoft compiler. What mitigating controls exist on the target device that would prevent successful exploitation of this vulnerability and (briefly) how do the major ones work¹? How would you rate the criticality of your finding in light of this knowledge?

¹ For example: <http://phreedom.org/presentations/how-to-impress-girls/>