**Answers and grading comments for Assignment 9 – Week 11**

**DO NOT COPY, SHARE OR REPRODUCE THIS MATERIAL AS IT CAN GET YOU EXPELLED FROM M.U.M.**

**(1) Which of the following are true about penetration testing?**

a) it considers the environment in which the computer system runs  
b) it is a formal method  
c) it can find a security flaw  
d) it can prove that a security flaw does not exist  
e) it should be authorized by management  
f) it is a very informal, non-rigorous technique for checking the security of a system.

**ANS: a, c, e, f**  
b,f-Testing is not a formal method. A formal method mathematically proves that a program is correct.  
c,d-No testing can prove that bugs do not exist; testing can only find bugs. If you are a tester and do not find any bugs during the day, you had a bad day.  
e-Since penetration testing may reveal vulnerabilities that show confidential data, management should give approval first.  
a-To be effective, a penetration test must consider the environment, eg.. the building, the personnel, the software. Vulnerabiliites are often caused by these things.

**(2) Which of these types of attackers is most likely to use social engineering?**

a) external attacker with no knowledge of system  
b) external attacker with access to system  
c) internal attacker with access to system

**ANS: a**  
Social engineering is used to get knowledge of the system that will allow the attack to know what the possible vulnerabilities are. If the attacker already has access to the system, either externally or internally, he already knows something about the system.

**(3) Which of the following describe what a vulnerability in a computer system is?**

a) it is a specific failure of one or more controls  
b) it is a security flaw  
c) it is something that an attacker wants  
d) none of the above

**ANS: a, b**  
A threat is what an attacker wants. If you have a junk car that nobody wants then there is no threat that somebody will take it and since there is no threat, any vulnerabilities (i.e., a broken lock) does't matter. But if you have a valuable car, there is a threat because some people want it. A control against that threat is to lock the car. If the lock is broken, then that is a vulnerability. If the lock is not broken there is no vulnerability. In either case the threat remains.

**(4) One exploits a**

a) vulnerability  
b) threat  
c) access control  
d) security model

**ANS: a**

**(5) Which one of the following layers is normally skipped in penetration testing  done during design and development?**

a) external attacker with no knowledge of the system  
b) external attacker with access to the system  
c) internal attacker with access to the system  
  
**ANS: a**  
External attacker with no knowledge of the system becomes a problem when the system is installed and in use. During design and development this is not the case.

**(6) Which one of the following sources is least likely to provide useful information during the information gathering step of the Flaw Hypothesis Methodology?**

a) design documents  
b) manuals  
c) source code of programs  
d) past experience with the system  
e) newspapers  
f) google

**ANS: e**  
Google is a good way to discover if confidential information has leaked to the Internet. It is also a way to discover documentation on vulnerabilities that other systems have. Newspapers usually don't contain that kind of information. However, if you commented that newspapers might contain something of interest, I gave you credit for selecting newspapers. But, it is extremely unlikely that a penetration team will sit around reading newspapers to find vulnerabilities. All of the other sources mentioned are much, much more likely to reveal vulnerabilities.

**(7) Flaw generalization often leads the tester to a new flaw.**

a) true  
b) false

**ANS: a**  
See next question for an example of this phenomenon.

**(8) Which of the following are not steps in the Flaw Hypothesis Methodology**

a) information gathering  
b) flaw hypothesis  
c) flaw testing  
d) flaw generalization  
e) flaw elimination  
f) flaw creation

**ANS: f**  
If your comment mentioned that "flaw elimination" was often optional, I gave you credit for selecting flaw elimination. But you had to make a comment to that effect.

**(9) Which of the following layers might use a guest account?**

a) external attacker with no knowledge of the system  
b) external attacker with access to the system  
c) internal attacker with access to the system

**ANS: c**  
Guest accounts are OS accounts. This means the attacker must have internal access to the system, i.e., can sit down at a computer on the LAN and log in using an OS login. An external attacker with access to the system can not sit down at a computer on the LAN, instead he can use the mail server or FTP. He does not log on using the OS.

**(10) Which of the following are true about the flaw testing step of the flaw hypothesis methodology?**

a) the tester's goal should be to demonstrate what a hostile explorer of the system could do, not to be that hostile attacker  
b) a tester should do no harm to the system in demonstrating the flaw  
c) a tester must exploit the flaw only if management doesn't believe the flaw exists  
d) a tester must describe how to duplicate a test that exposes a security flaw  
e) the test that demonstrates the flaw should be as complex as possible

**ANS: a, b, d**  
Demonstrations of flaws should be as simple as possible so the flaw can be reproduced easily.

**(11) From the book: "Ultimately, the testers (and not the developers) must decide which layers are appropriate." This is reminiscent of which type of security model?**

a) Clark-Wilson  
b) Bell-LaPadula  
c) Biba  
d) Chinese Wall  
  
**ANS: a**  
This is an example of separation of duty which is a fundamental feature of the Clark-Wilson model. It is not found in the other models listed.

**(12) Let's say that a penetration test revealed that an adminstrator was using the password "Admin" which was easily guessed. Briefly describe two generalizations of this flaw.**

**ANS:**  
Some generalizations:

1. Check other system accounts for obvious or default passwords  
2. Check password program to see if it allows a user to select easy passwords to guess.  
3. Users of system are not properly trained (security is not a top priority for them)  
  
If you got one of the above answers, I gave you full credit.

**(13) What three questions does the NRL taxonomy attempt to answer?**

a) how did flaw enter system?  
b) when did flaw enter system?  
c) where did flaw enter system?  
d) why did flaw enter system?  
e) what did the flaw do when it entered the system?

**ANS: a, b, c**  
"Why" the flaw entered the system probably has something to do with the psychology of the programmers and is not considered by the taxonomy. What the flaw does is just the definition of the flaw.

**(14) Knowledge of which area is most critical to understand the Michigan terminal penetration test?**

a) networks  
b) operating systems  
c) distributed computing  
d) compilers  
e) software engineering

**ANS: b**

**(15) What is the difference between formal verification and penetration testing?**

**ANS:**  
Formal verification

– A tester had a bad day when he finds a bug.  
- Mathematically verifying that a system satisfies certain constraints  
- Required: postconditions satisfy constraints

 Penetration Testing

– Penetration tester had a bad day if he doesn’t find a bug.  
- Testing to verify that a system satisfies certain constraints          
- Hypothesis stating system characteristics, environment, and state relevant to vulnerability  
- Result is compromised system state

- Apply tests to try to move system from state in hypothesis to compromised system state

|  |  |
| --- | --- |
| **Formal Verification** | **Penetration Testing** |
| *Preconditions* state assumptions about the  system | *System characteristics, environment and state* |
| Program | *Program or system* |
| *Postconditions* are result of applying  system operations to preconditions, inputs | *System state* |

**(16) Explain briefly what a buffer overflow attack is.**

**ANS:**  
A buffer overflow attack causes data to flow outside the boundaries of the memory reserved for it.

**DO NOT COPY, SHARE OR REPRODUCE THIS MATERIAL AS IT CAN GET YOU EXPELLED FROM M.U.M.**