**Final Exam Questions**

1. (A) [8]

**What is the difference between Logic bombs and Bacteria? Explain with an example.**

**Answer:**

A programs that performs an action that violates the site security policy when some external event occurs. Example: program that deletes company’s payroll records when one particular record is deleted. The “particular record” is usually that of the person writing the logic bombs.

**Bacteria**: A program that absorbs all of some class of resources. Example: Shell commands of Unix system, while true do mkdir x chdir x done

Bacteria:, or rabbit programs, make copies of themselves to overwhelm a computer system's resources. Bacteria do not explicitly damage any files. Their sole purpose is to replicate themselves. A typical bacteria program may do nothing more than execute two copies of itself simultaneously on multiprogramming systems, or perhaps create two new files, each of which is a copy of the original source file of the bacteria program. Both of those programs then may copy themselves twice, and so on. Bacteria reproduce exponentially, eventually taking up all the processor capacity, memory, or disk space, denying the user access to those resources.

**(B)[10] One of the ways to defend against a computer virus is to distinguish between data & instructions.Explain how this protection mechanism helpsto prevent a  virus spread.**

Virus - data: written to program, Instructions: then executes

Treating data and instructions as separate types, and requires certifying authority to approve conversion. Certifying authority will not make mistakes and assumption that tools, supporting infrastructure used in certifying process are not corrupt. All the virus have data and instructions, so distinguishing between data and instructions helps to determine which resources have the possibility to hold the viruses.

**(C)[4] Which of these types of malicious logic and designed to avoid detection by a virus detection program**

1. TSR Virus
2. Encrypted Virus
3. Trojan horses
4. boot sector infectors
5. Polymorphic Viruses

**Answer:**

* **Polymorphic**
* **Encrypted Viruses**

**References**

http://www.techexams.net/technotes/securityplus/malicious\_code.shtml

http://security4web.org/glossary.php?w=Encrypted%20Virus

1. **(A)[4] What are two desirable characteristic of an IDS.**

Detect wide variety of intrusions

– Previously known and unknown attacks

– Suggests need to learn/adapt to new attacks or

changes in behavior

• Detect intrusions in timely fashion

– May need to be be real-time, especially when system

responds to intrusion

• Problem: analyzing commands may impact response time of

system

– May suffice to report intrusion occurred a few minutes

or hours ago

**It must run continually without human supervision**

The system must be reliable enough to allow it to run in the background of

the system being observed

**It must be fault tolerant**

It must survive a system crash and not have its knowledge-base rebuilt at

restart

**It should not be a "black box**

Its internal workings should be examinable from outside

**It must resist subversion**

The system can monitor itself to ensure that it has not been subverted

Reference

http://www.cs.unibo.it/~babaoglu/courses/security06-07/lucidi/IDS.pdf

**(B)[12]** **One view of intrusion detection systems is that they should be of value to an analyst trying to disprove that an intrusion has taken place.** **Consider the following scenario. A system has both classified and unclassified documents in it. An Employee is accused of using a word processing program to save an unclassified copy of a classified document. Discuss if, and how** **each of the three forms of intrusion(Anomaly, Misuse, Specification) detection mechanisms could be used to argue this accusation.**

**Answer:**

That there was no unusual activity by the employee (no anomaly).

That the employee did not violate any security policies regarding access and saving of classified documents. (no misuse)

That the employee only accessed and saved documents that he/she has permission to access. (followed specification)

So the employee is not guilty.  You got full points only if you were able to explain your answer on these lines.

An analyst trying to disprove intrusion, can use at least two models out of the three in order to detect if an intrusion has taken place.

**Anomaly model**, intrusion can be detected when such documents that were characterized as classified enter an unclassified state once they were saved using the word processing program;

**Misuse model**: would apply the rule that classified documents can be opened by a simple word processing programs without a password, once the rule has been tripped the system is compromised and there is an intrusion, this cannot happened since the system has granted the user access were classified and unclassified files reside.

**Specification model** a detection mechanism would not be able to detect an intrusion because the file systems would keep working as normal.

Therefore we can conclude that only one out of the three models can be used to detect intrusion.

**Reference**

https://github.com/StEdwardsU-COSC/Homework-6-Palmerin/blob/master/Homework6.md

**(c)[4]Security guard at a professional soccer notice that two men are climbing over the fence; security guard detain these men. which intrusion model is used here ? Support your answer with brief explanation.**

Specification Model there is very specific rule if anyone is seen climbing the fence he should be arrested.

**3(A)[12] Briefly explain the 4 step in the flaw hypothesis methodology?**

**1. Information gathering**

• Become familiar with system’s functioning. Ideally acquire the knowledge of the system that a potential hacker has.

a. Read the manuals and specifications! (principle of open design).

b. Review management of system looking for potential people problems.

**2. Flaw hypothesis**

• Draw on knowledge to hypothesize vulnerabilities, e.g, if manual indicates a maximum length of some field, try a longer length.

**3. Flaw testing (do no harm!)**

• Assign priorities and test out hypotheses (e.g. focus on external attack rather than

inside job).

• Make sure system is backed up in case some test goes too far.

• Avoid actually exploiting the flaw unless management doesn't believe that flaw exists.

• As with any test, it must be as simple as possible and it must be able to be duplicated

**4 Flaw generalization**

• Generalize vulnerability to find others like it

• For example, if an account with a default password is found,

generalize to two things:

1. Users poorly educated about password management

2. There may be other accounts with default passwords

**5-Flaw Elimination (May be)**

**3.(B)What are the goals of Penetration testing how does this compare with the goals of formal verification.**

Goals: Attempt to violate specific constraints in security and / or integrity policy .implies metric for determining success, Must be well-defined. Ex. Subsystem designed to allow owner to require others to give password before accessing file.

Formal Verification:

A tester had a bad day when he finds a bug

Mathematically verifying that a system satisfies certain constraints

Required: post conditions satisfy constraint

Penetration technique:

Penetration tester had a bad day if he does not 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** |
| **Mathematically verifying that a system satisfies certain constraints** | **Testing to verify that a system satisfies certain constraints.** |
| **Precondition: states assumptions about the system** | **Hypothesis stating system characteristics, environment and state relevant to vulnerability** |
| **Postconditions: result of applying system operations of preconditions input. Postcondition satisfies constraint.** | **Result is compromised system state. Apply tests to try to move system from state in hypothesis to compromised system state.** |
| **Program** | **Program / system** |

**4.(A) Users are classified into four classes. Moving information from one class to another requires approval of more than user.**

**Answer**

Principle of separation of privilege

**b) Each Server has the minimum amount of knowledge of the network necessary to perform its task**

**Answer:**

Principle of least privilege

**c) In the Drib Corporation, the four servers in the DMZ zone are all on separate computers.**

**Answer:**

Principle of Least Common Mechanism

**d) The use of write-once media in the log server. (Deny all modifications to write-once media)**

**Answer:**

Principle of Fail-Safe defaults

**e) Configuration of firewalls should be simple so that administrators will feel comfortable doing it.**

**Answer:**

Principle of Psychological Acceptability

**5 Briefly explain any 3 of your favorite SCI points that you have learned in this course so far.**

There are two main forms of malicious logic, viruses and worms. There is only one form of “delicious” logic: deep rest and then perform dynamic activity.

The DMZ is what is between the inner and outer firewalls. These two firewalls

strictly control access to the DMZ bothfrom the Internet and the internal net. The

firewalls epitomize the discriminating and integrating nature of Creative Intelligence

A given developer machine can be accessed by any developer on the internal network. Developers are trusted. The field of transcendental consciousness can be accessed by anyone with a human physiology provided that the correct technique is used.

In Security system lecture we learned 8the contrast that how a machine used by developer is configured with how the DMZ web server is configured. Knowledge is different in different state of consciousness.

**6 What do you mean by a distinguished name? How will it look like for a person named Jack Davis who works at IBM in QA dept?**

A distinguished name identifies a principal. It consists of a series of fields, each with a key and a value.

/O=IBM/OU=Quality Assurance/CN=Jack Davis/

**7 Is cryptography used in the Drib system for integrity, confidentiality, or both? Justify**

Integrity is main concern and confidentiality is secondary with regard to updating the web server since most of the data is public and displaying on public web page (open design). Only the commercial transaction data is considered private. So cryptography is primarily used to ensure used to ensure data integrity(I,e Turdy makes no changes during transfer) and secondarily for confidentiality.

**Example:**

Cryptography is used when administrator moves the customer data from web clone server to the customer services group server. The web clone server should always maintain high integrity and make sure that no body overwrites the information in it. The administrator have no need to know the customer data (confidentiality) so cryptography used both.

**8. Explain in short the difference between authentication and authorization.**

**Authentication**:

Authentication provides a way of identifying a user, typically by having the user enter a valid user name and valid password before access is granted. The process of authentication is based on each user having a unique set of criteria for gaining access.

**Authorization:**

The authorization process determines whether the user has the authority to issue such commands. Simply put, authorization is the process of enforcing policies.

**9. In the dribble corporation, the IP address of outer firewall is x, that of the DMZ web server is y and that of the DMZ DNS server is z. Which of these IP addresses are known to the external Internet users.**

Since DMZ purely separating internal network from external network, external internet user will get IP address x.

**10. Which statistical model is likely to be used to detect someone guessing passwords?**

Threshold metric

**11a. A manipulation detection code is based on timestamps**

False: It is based on permission bits which included in the signature and a keyless cryptographic checksum. But not Timestamp which is used to prevent replay attacks.

**11b. The access control policy that is implemented in the internal drib network is originator controlled.**

False. It is mandatory controlled. Suppose a corporate employee does not have the ability to give a customer service employee access to files that contain financial data.

**11c. Vulnerability of a system increases when threats high.**

False: Vulnerability and threats are not directly proportional to each other. A potential buffer overflow exists even if there is no one that wants to exploit it

**11d. Security logging is the analysis of records to present information about the system in a clear and understandable manner.**

False. Security logging is the recording of events or statistics to provide information about system use and performance. Auditing is the analysis of log records to present information about the system in a clear, understandable manner.

**11e. A Programming language has no effect on whether or not a program is vulnerable to a buffer overflow attack.**

False. Since it modifies the data beyond its buffer, the program behaves abnormally.

Buffer Overflow: A buffer overflow occurs when a program or process tries to store more data in a buffer than it was intended to hold.

You have been commissioned to write an article on security for employees in the Customer Service Group of the Dribble Corporation. What would you tell them about computer security?

Remember that these are customer service group employees, not college professors or developers or students in a computer security course. The advice should be appropriate for a new employee with very little experience with computers. Keep your advice practical and concrete. I just want the most important points, not the entire article.

Ans:

As we can assume Customer Service Group employees are non-technical individuals. So these could be some helpful security points for those with very little experience with computers and security knowledge.

1) Don't share your user name and password, don't write it down.

2) Change password on some fixed time interval.

3) Use strong password, most of the system states how many characters it should have, letters, numbers,special characters.

4) Never share customer's information with any un-authenticated person.

5) Try to avoid customer information sharing through phone or any indirect medium. If you have to then first get authentication from senior, and make sure about about receiving person's identity.

6) Do not manipulate customer's information for any other uses or use customer information for any other reasons for your personal benefit.