FIT3031 TUTORIAL 9 SOLUTIONS

INTRUSION DETECTION

REVIEW QUESTIONS

Q1. List and briefly define three classes of intruders.

ANS: **Masquerader:** An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account.

Misfeasor: A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges.

Clandestine user: An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection.

Q2. What are two common techniques used to protect a password file?

ANS:

- **One-way encryption:** The system stores only an encrypted form of the user's password. When the user presents a password, the system encrypts that password and compares it with the stored value. In practice, the system usually performs a one-way transformation (not reversible) in which the password is used to generate a key for the encryption function and in which a fixed-length output is produced.
- **Access control:** Access to the password file is limited to one or a very few accounts.

Q3. What are the benefits that can be provided by an intrusion detection system?

ANS:

- If an intrusion is detected quickly enough, the intruder can be identified and ejected from the system before any damage is done or any data are compromised. Even if the detection is not sufficiently timely to preempt the intruder, the sooner that the intrusion is detected, the less the amount of damage and the more quickly that recovery can be achieved.
- An effective intrusion detection system can serve as a deterrent, so acting to prevent intrusions.
- Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facility.

Q4. What is the difference between statistical anomaly detection and rule-based intrusion detection?

ANS:

- **Statistical anomaly detection** involves the collection of data relating to the behaviour of legitimate users over a period of time. Then statistical tests are applied to observed behaviour to determine with a high level of confidence whether that behaviour is not legitimate user behaviour.
- **Rule-Based Detection** involves an attempt to define a set of rules that can be used to decide that a given behaviour is that of an intruder.

Q5. What metrics are useful for profile-based intrusion detection?

ANS:

- **Counter:** A nonnegative integer that may be incremented but not decremented until it is reset by management action. Typically, a count of certain event types is kept over a particular period of time. Examples include number of logins by a single user during one hour, the number of times a given command is executed during an hour.
- **Gauge:** A nonnegative integer that may be incremented or decremented. Typically, a gauge is used to measure the current value of some entity. Examples include number of logical connections assigned to a user application and number of outgoing messages queued for a user process.
- **Interval timer:** The length of time between two related events. An example is the length of time between successive logins to an account.
- **Resource utilization:** Quantity of resources consumed during a specified period. Examples include the number of pages printed during a user session and total time consumed by a program execution.

Q6. What is the difference between rule-based anomaly detection and rule-based penetration identification?

ANS:

1. **With rule-based anomaly detection**, historical audit records are analyzed to identify usage patterns and to generate automatically rules that describe those patterns. Rules may represent past behavior patterns of users, programs, privileges, time slots, terminals, and so on. Current behavior is then observed, and each transaction is matched against the set of rules to determine if it conforms to any historically observed pattern of behavior.
2. **Rule-based penetration identification** uses rules for identifying known penetrations or penetrations that would exploit known weaknesses. Rules can also be defined that identify suspicious behaviour, even when the behaviour is within the bounds of established patterns of usage. Typically, the rules used in these systems are specific to the machine and operating system. Also, such rules are generated by "experts" rather than by means of an automated analysis of audit records.

Q7. What is a salt in the context of UNIX password management?

ANS: The salt is combined with the password at the input to the one-way encryption routine.

Q8. List and briefly define techniques used to avoid guessable passwords.

ANS:

- **User education:** Users can be told the importance of using hard-to-guess passwords and can be provided with guidelines for selecting strong passwords.
- **Computer-generated passwords:** Users are provided passwords generated by a computer algorithm.
- **Reactive password checking:** the system periodically runs its own password cracker to find guessable passwords. The system cancels any passwords that are guessed and notifies the user.
- **Proactive password checking:** a user is allowed to select his or her own password. However, at the time of selection, the system checks to see if the password is allowable and, if not, rejects it.

Q9. What is a Honeypot?

ANS: Honeypots are decoy systems that are designed to lure a potential attacker away from critical systems.

PROBLEMS

1. Explain the suitability or unsuitability of the following passwords:

ANS:

a. YK 334 : If this is a license plate number, that is easily guessable.
b. mfmitm (for "my favourite movie is tender mercies") : suitable
c. Natalie1 : easily guessable
d. Washington : easily guessable
e. Aristotle : easily guessable
f. Tv9stove : suitable
g. 12345678 : very unsuitable
h. dribgib : This is bigbird in reverse; not suitable.

2. A phonetic password generator picks two segments randomly for each six-letter password. The form of each segment is CVC (consonant, vowel, consonant), where
V= <a, e, i, o, u> and C = $\overline{V}$

a. What is the total password population?
ANS: T = (21 X 5 X 21)^2 = 4,862,025

b. What is the probability of an adversary guessing a password correctly?
ANS: p = 1/T ≈ 2 X 10^{-7}

3. Assume passwords are limited to the use of 95 printable ASCII characters and that all passwords are 10 characters in length. Assume a password cracker with an encryption rate of 6.4 million encryptions per second. How long will it take to test exhaustively all possible passwords in a UNIX system?

ANS: There are $95^{10} \approx 6 \times 10^{19}$ possible passwords. The time required is: $\left(\frac{6 \times 10^{19}}{6.4 \times 10^{6}/\text{sec}}\right.$

$$= 9.4 \times 10^{12}\,\text{sec} = 300{,}000\,years$$