FIT3031 TUTORIAL 9

INTRUSION DETECTION

REVIEW QUESTIONS

Q1. List and briefly define three classes of intruders.

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

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

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

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

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

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

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

Q9. What is a Honeypot?

PROBLEMS

1. Explain the suitability or unsuitability of the following passwords:
    a. YK 334
    b. mfmitm (for "my favourite movie is tender mercies")
    c. Natalie1
    d. Washington

e. Aristotle

f. Tv9stove

g. 12345678

h. dribgib

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?

   b. What is the probability of an adversary guessing a password correctly?

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?