CS381 Exercise 18

Name: Zhang Yupeng

Student ID: 5130309468

1. What is the most important thing against intrusion?

Solution:

The most important thing against intrusion is password protection. It's to protect and manage the password file on system.

2. Describe the 2 approaches of intrusion detection.

Solution:

The first one is statistical anomaly detection. It attempt to define normal or expected behavior, and it's effective against masqueraders. However, it isn't effective against misfeasors

The second one is rule-based detection. It define a set of rules to decide whether a given behavior is of an intruder. It attempt to define proper behavior and it's appropriate for misfeasors.

3. Describe effective rules to detect/prevent the Standard Backdoors.

Solution:

1. Use firewall to detect and prevent the standarf backdoors by its anti-backdoor functions.
2. Pay attention to the unusual network traffic of any web application, a standard backdoor will use internet to communicate with the attackers.
3. Pay attention to the unusual behaviours of any software in the system, a standard backdoor will do some specific operations to interact with the attackers.