popular techniques of intrusion detection

Intrusion

detection

based

on

analysis

of

state

transition

Intrusion

detection

based

on

pattern

matching

Expert

system

based

on

regulation

Intrusion

detection

based

on

statistics

Techniques

of

intrusion

detection

based

on

bionics

computation

Methods

of

intrusion

detection

based

on

data

mining

Methods

of

exception

detection

based

on

flows

detection

Figure 2.5: Popular techniques of intrusion detection

(3) Intrusion detection based on pattern matching

Pattern matching mainly build repository of feature regulation by means of gathering feature string which stand for normal of aggressive behavior, and then distinguishes exception by the way of comparing feature data of host or network data package string gathered with regulation in repository of regulation.

(4) Intrusion detection based on analysis of state transition

This detection method is mainly used to analyse the impact on system state transition, which is caused by every state, in exception detection and misuse detection. In some occasion of attacking, system transfer from a state to next state. In the process, every state symbolize a attribute. The transition, i.e., the movement of states, between two states is called signature.

(5) Methods of exception detection based on flows detection

The method of exception detection based on flows detection was put forward by Moore after analysing IP address range from 2001 to 2004. He discover that there are 24.5 IP addresses that is different are attacked every hour.

(6) Techniques of intrusion detection based on bionics computation

With appearing and increasingly rising of interdiscipline, such as neural network computation, genetic evolution computation, immune computation and so on, scholars use them in network security, and then various technologies, which include detection model based on neural network, ways of attack detection based on genetic algorithm and exception detection based on immune principle on the whole, emerge. As shown in the figure 2.6:

Techniques

of

intrusion

detection

based

on

bionics

Detection model based on neural network

Ways of attack detection based on genetic algorithm

Exception detection based on immune principle

Figure 2.6: Techniques of intrusion detection based on bionics

➀Techniques of attack detection based on genetic algorithm

➁Detection model based on neural network

➂Method of exception detection based on immune principle

(7) Method of intrusion detection based on data mining