Popular intrusion detection technology

Intrusion

detection

based

on

analysis

of

state

transition

Intrusion

detection

based

on

pattern

matching

Expert

system

based

on

regulation

Intrusion

detection

based

on

statistics

Intrusion

detection

technology

based

on

bionics

computation

Methods

of

intrusion

detection

based

on

data

mining

Methods

of

exception

detection

based

on

flows

detection

Figure 2.5: Popular intrusion detection technology

(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) Intrusion detection technology based on bionics computation

As interdiscipline, such as neural network computation, genetic evolution computation, immune computation and so on, appearing and continually rising, scholars apply them to 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:

Intrusion

detection

technology

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: Intrusion detection technology based on bionics

➀Attack detection technology based on genetic algorithm

Genetic algorithm derived from Darwinian evolution has strong learning capacity. This algorithm simulates natural evolution regulation, selecting the superior and eliminating the inferior. It is usually applied to deal with nonlinear problems traditional searching methods are difficult to or can’t solve on account of its huge advantage of dealing with all kinds of optimization problems with multiple targets. There are advantages of genetic algorithm, avoiding local optimum and combination explosion problem during global search, but they are at the expense of high complexity.

➁Detection model based on neural network

Artificial neural network simulates the process of human neural network taking shape neure, establishing neural network and matching and classifying patterns. Neural network does well in extracting feature data in intrusion detection system and recognizing aggressive behavior effectively.

➂Method of exception detection based on immune principle

There are numerous peculiarities, such as adaptivity, diversity, self-learning, self-organizing, cosmically distributing, robustness and tolerance, in immune system. Therefore, scholars are keen on applying immune mechanism to research IDS.

(7) Method of intrusion detection based on data mining

Data mining, meaning extracting valuable or useful information from mass data, usually includes selecting data, data pre-processing and data conversion. Common data mining technologies include rule deduction, decision tree, rough set, fuzzy set, association rule, etc.

2.2 Artificial immune theory

Artificial immune theory(AIT) is an interdiscipline derived from computer system where scholars import peculiarities of biological immune system. The theory researches all kinds of characters and mechanisms of biological immune system, which is applied to solve science or project problems.

2.2.1 Biological immune system

Biological immune system composed of mass molecules, cells and tissues is very complex and the most intelligentized system except neural system. Its main function is to protect organism from antigens and pathogens, thereby maintain balance and stabilization within the organism and health of organism. The subject with respect to study this system particularly is called biological immunology. The following introduce basic conceptions and important mechanisms of immune system.

1.Basic conceptions of immunization

(1) Immunization: Biological function of maintaining physiological equilibrium by means of distinguishing between self and non-self and excluding outsiders.

(2) Antigen: A material causing immunoreaction. Its two essential features are immunogenicity and immunoreactivity. Immunogenicity refers to the character of leading to immune system activating, propagating and differentiating, thereby producing immune substance such as antibody by the way of motivating some specific immune cells.

(3) Antibody: Antibody is a immune globulin used to identify foreign materials. It is produced by plasmocyte after B cells are motivated. There are the same type of antibody on the surface of B cells. In normal occasion, antibodies on the surface of B cells can recognize specific foreign materials after B cells are activated, then give rise to immunoreaction of organism to kill antigen by means of specifically combining with corresponding antigen.

(4) Affinity: Affinity refers to the ability of receptors on the surface of immune cells specifically combining with epitope. The more complementary structures of these two are, the more high probability and strength of combination is.

2.Significant mechanism of immunization

Immune system is primary protection system which rid biont of foreign pathogens and antigens. The following are principal mechanisms:

(1) Immunological recognition

Immunological recognition, i.e., biological immune system can distinguish between self and non-self by immune cells and eliminate harmful non-self from body. As shown in the figure 2.7, immunological recognition realizes by the combination modes of epitope on the surface of antigen and receptor of immune cells largely.

Epitope

Receptor

Lymphocyte

Similar structure

High affinity

Low affinity

Figure 2.7: Immunological recognition theory

(2) Immunological learning and memory

Biological immune system can remember antigens having been responded by learning, and then produce memory cells, thereby increases speed of identifying and wiping out antigens known. When the same antigen attacks organisms again, organisms will generate numerous antibodies that have higher affinity according to memory cells, and make second response faster and intenser. As shown in the figure 2.8:

Second response

First response

Concentration

of

antibodies

Delay

Delay

...

Time

Antibody Ag

Antigen Ag

Figure 2.8: Immunological memory theory

(3) Diversity of receptor

Diversity refers to receptors of immune cells are imposed of different genes randomly, so there is likely to exponential growth in the number of their receptors. In order to guarantee organisms can identify detrimental antigens with effect, organisms must assure the diversity of immune cells when faced with various epitope.