Intrusion Detection System (IDS) (Part 2)

In the previous section we have solved IDS architectural and classification issues. In this second part, we will show you more in-depth tutorials on IDS including an overview of classifications and an introduction to the reader some basic concepts about IDS: audit analysis and handle 'online' as well as discovery

Classify; methods and techniques

In the previous section we have solved IDS architectural and classification issues. In this second part, we will show you more in-depth tutorials on IDS including an overview of classifications and an introduction to the reader some basic concepts about IDS: audit analysis and 'online' processing as well as anomalous detection and detection methods. We will also introduce key detection techniques.

Classification of intrusion detection systems

First of all IDS intrusion detection system involves the detection of attack operations. Therefore this network security tool uses both main techniques. The first technique is to detect anomalies in order to find out the intrusion detection problem related to the wrong commands compared to the normal system or in user behavior. The second technique uses signal detection to distinguish between unusual attack patterns and signs of known intrusion detection. Both methods have advantages and disadvantages as well as reasonable application.

When considering the data storage area used for intrusion detection, we have another classification used here as a protected system type. The IDS tool group uses information obtained from a host (system) - IDS host (HIDS) and IDSs to use information obtained from the local network segment (network IDS).

The two main types of HIDS can be distinguished as:

- The system checks incoming connection attempts (RealSecure Agent, PortSentry). This system checks incoming and outgoing network connections of a host. There is an association of unauthorized connection attempts with TCP or UDP ports and can also detect incoming port scans.

- Systems that check network traffic (network packets) are trying to access the host. These systems protect the host by blocking suspicious packets and consider the payload issue of the link (packet inspection).

- Systems that check log activity to the network layer of the protected host (HostSentry). This role is to test attempts to log in and log out, look for unusual activities on a system at unexpected intervals, specific network locations or detect multiple attempts to post. enter (typically attempts to fail).

- The system checks super user activities, the highest priority (check the record). IDS scans abnormal activities, super user activity is increased or operations have been performed at specific times, .

- File integrity checking system (Tripwire, AIDE). Tools with this capability (integrity checker) allow to detect any changes that occur to important files for the operating system.

- System to check register status (Windows system only). They are designed to detect any invalid changes in system registers and alerts for system administrators.

- Kernel-based intrusion detection system is popular with Linux (LIDS, OpenWall). These systems check the main state of the file and the flow of the operating system, to prevent buffer overflows, block abnormal communications, prevent intrusion attacks on the system. In addition, they can block some activities that only super-users have (query rights).

HIDS reside on a specific computer and provide protection for certain computer systems. They are not only equipped to facilitate easy system testing, but also include other typical IDS modules, for example, response modules (see Part 1).

HIDS products like Snort, Dragon Squire, Emerald eXpert-BSM, NFR HID, Intruder Alert, all carry this type of test.

Type IDS - network (NIDS) provides data about internal network performance. NIDS gather packages and analyze them. They not only handle packages that are sending to specific hosts but can also be installed on active network components, for example on routers.

Because intrusion detection uses statistical data on network payloads, a declared NIDS can be clearly distinguished, such as traffic monitors (Novell Analyzer, Microsoft Network Monitor). They collect all the packets they see on the network segment without analyzing them and only focus on creating network traffic statistics.

Typical network intrusion systems are: Cisco Secure IDS (formerly known as NetRanger), Hogwash, Dragon, E-Trust IDS.

Some authors consider the mix of HIDS and NIDS as a separate layer with Network Node IDS (NNIDS), Network Node IDS (NNIDS) that have deployment agents on each host within the network (typical NIDS use operative network to check all LAN segments). In fact, an NNIDS acts like a hybrid host NIDS because the agent usually handles network traffic directly to the host it runs on. The main reason for introducing hybrid IDS is to use it when online with encrypted networks and data intended for a host (only the source and destination can view encrypted network traffic.). Most intrusion detection systems provided to the commercial sector are often hybrid tools, . This can see the power of HIDS and NIDS in a single concept.

HIDS observe their host traffic and can easily detect local-to-local attacks or local-to-root attacks, because they have a clear concept of proper internal information, for example : they can exploit user IDS. Also, anomalous detection tools have better coverage for internal problems because their detection capabilities are based on a user's normal behavior pattern.

IDS can operate independently within centralized or integrated applications to create a distributed system. Recently we have a special architecture with autonomous agents that can take precedence and react to measured parameters, can even move across the network. The AAFID architecture of these systems is presented in Part 1.

It is possible to classify an infringing detection system under their behaviors, be it passive (simply by giving

warning and network log packets) or can be positive - that is, possible Detects and responds to attacks, attempts to patch software vulnerabilities before being attacked, preemptively log off potential intruders, or block services. This section will be discussed in section 3.

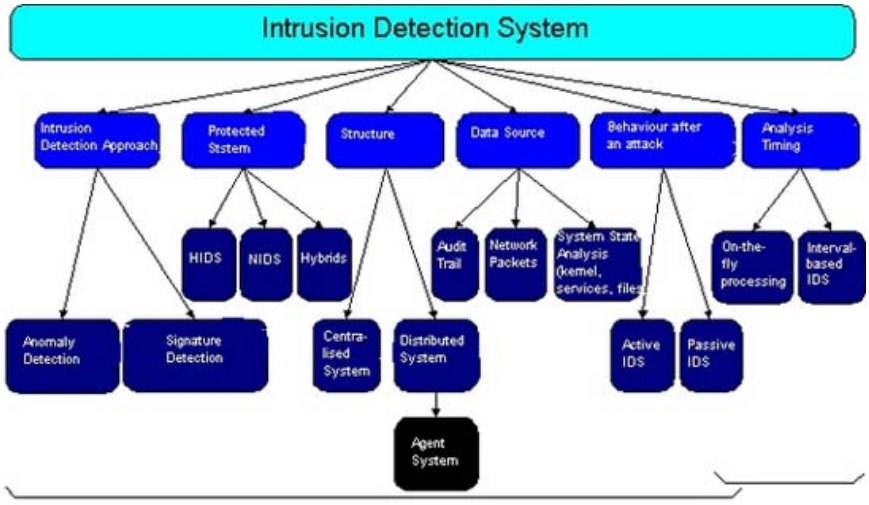

Figure 1 : Classification of intrusion detection systems

Processing online verification

IDS can operate either continuously or cyclically (respectively real-time IDS and interval IDS), so they use two different intrusion detection methods. Audit analysis is a common method used by operating systems periodically. In contrast, IDS can be deployed in a real-time environment designed for online testing and analysis of system events and user activity.

Handling inspection

There are many issues related to verification processing (event logs). Storing audit reports must avoid archiving in files because intruders can use that feature to create many unwanted changes. A certain number of event logs should be kept on the network, although it may have to add overhead to both the system and the network.

In addition, recording each event means consuming a bit of system resources (both internal and network related). Therefore, performing log compression will be a way to increase system load. Specifying verified events is a difficult issue because there are many types of attacks that may not be detected. It is also difficult to predict how large the file size must be because experienced people can only create an estimate from start to finish. Also, an appropriate save cycle setting for current audit files is not an easy task. In general, this depends on the specific IDS solution and its correlation engine. Obviously, archived files need to be saved as copies for recovery analysis purposes.

Log processing systems may also have vulnerabilities in denial-of-service (DoS) attacks, from which they provide authentication mechanisms that are not authentic and irrelevant due to overflow of system space. .

The main reasons for this appraisal function are:

1. Detecting offensive manifestations to analyze and draw experiences;
2. Detect periodic intrusion activities;
3. Distinguish successful attacks;
4. Distinguish weaknesses of the system itself;
5. Expanding user access and signs, defining important rules for network traffic for IDS to detect abnormal signs.
6. Repel potential attacks simply by making them aware of the existence of the meaning of testing.
7. Inspection reports can provide a form of prevention for legitimate users.
8. Log event IDS method should have the following capabilities:
9. Giving event log and user activity parameters an easy way, provides binding options for event logging mechanisms when there is no free space or DoS attack.
10. Verification processing needs to use additional mechanisms (retrieval, fake information and minimum data) because the file size is very large.
11. Minimum system resource consumption can be allowed for verification purposes.

Examples of intrusion detection systems that use audit processing are:

1. SecureView to check the logs provided by CheckPoint Firewall-1
2. CMDS (*Computer Misuse Detection System*). With an accompanying expert system, it will analyze all event logs to recognize unusual user behavior.
3. ACID (*Analysis Console for Intrusion Databases*) - is an analytical PHP database for searching and processing databases of incidents created with various security tools like IDS, firewall and network traffic analyzers. ACID has a user queue generator, which can analyze packages in its payload, thus finding the right warnings between databases, which is done with which standard combination there. It can also manage alerts and create statistics.

Process online

With online processing, an IDS performs online system authentication. In general, the network packet stream will be checked continuously. With this type of processing, intrusion detection uses knowledge of the current activity on the network to identify possible attack attempts (if it doesn't find a successful attack in the past).

This creates complexity in computation, the algorithms used here must require fast and effective therefore simple algorithms must be applied. This is due to the response between the key conditions - the ability to detect attacks and the complexity of the data processing mechanisms used in them.

At the same time, setting up an 'online' IDS tool requires a large amount of RAM because no data storage is used here. Therefore, such an IDS sometimes misses packages because in fact, there are too many packages that don't fit.

The amount of data selected by the detector is very small because it only observes the memory contents. So only a small part of the information is analyzed for a string or value that is being searched.

The main method used in real-time detection is simply to search for character strings in the transport layer package, namely in their headers. This can be done by checking the IP addresses that initiate the connection or by checking the combination of inappropriate TCP / IP flags (to catch packets that do not conform to known standards). An example of packet research here is when the source and destination port addresses are set to 21. This does not follow the FTP specifications because the source port number must be greater than 1024. Another

example may be is a type of service with a value of 0, a package with SYN and FIN flags are set not to match the numbering of the string or what is known, the ACK value is set to be different from zero when the ACK flag is not set, .
In contrast to standard verification methods, only select packages in the data stream that are disputed and the inspection process only looks for status information such as whether the package includes malicious code.

Another method is somewhat applied in application layer analysis (FTP, POP3, HTTP, .). Application-based IDS uses standard package checks to analyze TCP payloads (including headers). With this method, the relevant packages in the data stream are checked and the test process looks for information about which packets are valid for the typical package (commands) of a given protocol. Thus, POP3 denial of service vulnerability is exploited by saturating the POP3 server with multiple requests to execute a command. Therefore, the attack signal is expanded by the number of commands sent by a system and alarm threshold. This method recognizes the anomaly found while checking packages, checking package size and threshold values ??is to find signs of denial of service attacks, also at the transport layer. Other examples of standard packet inspection IDS also have the detection of email viruses before they reach the mailboxes by looking for a valid email title or attachment name. A tool that can search for malicious code can compromise the system if it is attacked, for example, exploits for buffer vulnerabilities are looking for signs to check the user session state to prevent, List the directory structure on an FTP server before a user logs in successfully. One obstacle to the high-class analysis method lies in the fact that it is time-consuming and dependent on the working environment (application layer protocols vary in different operating systems).

Advantages of real-time IDS:

1. Better about detecting attacks and even processing them;
2. The ability to cover successive security vulnerabilities has been pre-existing for specific types of attacks, such as DoS, that cannot be detected by using general inspection analysis - network traffic analysis is needed. here;
3. Consume less system resources than other cases.

Weakness:

1. Resource identification is done based on the network address taken from the package (for example, do not use a network ID). Resource addresses can be tampered with, making attacks more difficult to track and handle automatically.
2. Encrypted packages cannot be managed so they do not provide the information needed for intrusion detection.
3. Because the analysis module uses limited resources (only in the buffer), the detection capability is limited accordingly.
4. Continuous scanning of network traffic will reduce network throughput. This is an important issue when IDS tools are deployed near firewalls.

Unusual signs detected

The intrusion detection system must be able to distinguish between normal user activities and abnormal operations to find dangerous attacks in time. However, translating user behaviors (or complete user system sessions) in a decision related to security is often not straightforward - many behaviors are not intended and unclear (Figure 2). To classify actions, IDS must take advantage of anomalous detection methods, sometimes basic behavior or attack signs, etc. a device describing known abnormal behavior (detection of a sign). Also

called basic knowledge.

Figure 2 : User behavior in the system

Common behavior patterns - abnormal detection

Common behavior patterns are useful in predicting users and system behavior. Therefore, abnormal detectors build profiles that show normal usage and then use common behavioral data to detect invalidations between profiles and identify possible attacks.

In order to be reasonable with event profiles, the system is required to create the initial user profile to 'train' the system with regard to legalizing user behavior. There is a problem with profile making here: when the system is allowed to 'learn' on itself, intruders can also train the system at this point, where the infringement acts. before becoming normal behavior. An incompatible profile will be able to detect all possible intrusion activities. In addition, there is another need to upgrade the profile and "train" the system, a difficult and time-consuming task.

Given a set of common behavioral profiles, everything that doesn't match the saved profile will be treated as a suspicious activity. Therefore, these systems are characterized by very high detection efficiency (they can recognize many attacks even though the attack is new to the system), but they do have the phenomenon of creating scenes. Falsely reported some problems.

The advantage of this unusual detection method is: being able to detect new attacks when there is an intrusion; Unusual problems are realized without their inner cause and personality; less dependent on IDS for operating environments (when compared to sign-based systems); ability to detect abuse of user rights.

The biggest disadvantages of this method are:

1. Probability of many false alarms. System performance is not checked during profile building and training phase. Therefore, all user activities ignored during this period will be unreasonable. User behaviors may change over time, so there is a need for a continuous upgrade to the usual behavioral profile database.
2. The need for system training when changing behavior will make the system unrecognizable during the training period. (negative error)

Signs of bad behavior - detecting signs

Information handling systems in unusual and unsafe acts (system-based attacks) are often used in real-time intrusion detection systems (because of the complexity in computing Their math is not high.

Signs of bad behavior are divided into two categories:

1. Attack signs - they describe active patterns that can pose a security threat. Typically, they are expressed when a time-dependent relationship between a series of activities can be combined with neutral activities.
2. Text strings are selected - markers matching text strings are looking for suspicious activity.

Any unclear activity may be considered and prevented. Therefore, their accuracy is very high (low false alarm number). However, they do not perform completely and do not completely prevent new attacks.

There are two main methods that combine the detection of this signal:

1. Examining problems in lower layer packages - many types of attacks exploit vulnerabilities in IP, TCP, UDP or ICMP packets. With a simple test of a set of flags on a featured package it is possible to detect which packages are valid, which ones are not. The difficulty here may be to open the package and assemble them. Similarly, some other problems may be related to the TCP / IP layer of the system being protected. Often an attacker uses a way to open packages to bypass many IDS tools.
2. Test application layer protocols - many types of attacks (WinNuke) exploit program vulnerabilities, for example, special data sent to an established network connection. In order to effectively detect such attacks, IDS must be added to many application layer protocols.

Sign detection methods have some advantages: low false alarm rate, simple algorithm, easy to create attack sign database, easy addition and resource efficiency. Minimum system.

Some disadvantages

1. Difficulty in upgrading new types of attacks.
2. They cannot inherit to detect new and unknown attacks. Must upgrade an attack signature database associated with it.
3. The management and maintenance of an IDS is required in combination with the analysis and patching of security vulnerabilities, which is a time-consuming process.
4. Knowledge of attack depends on the operating environment - therefore, IDS based on bad behavior must be configured to comply with its strict rules with the operating system (version, platform, applications used, .)
5. They seem to be difficult to manage internal attacks. Typically, abuse of authenticated user rights cannot be detected when there is malicious code activity (because they lack information about user rights and the structure of the attack signal).

Commercial IDS products often use sign detection methods for two reasons. First, it is easier to provide known attack-related signs and to assign names to an attack. Second, the attack signature database is upgraded regularly (by adding new attack detection signs).

The following example shows an attack mark taken from the Snort program, which detects ICMP ping packets larger than 800 bytes coming from an external network and combined with any port:

alert icmp $ EXTERNAL_NET any -> $ HOME_NET any (msg: "MISC large ICMP"; dsize:> 800; reference: arachnids, 246; classtype: bad-unknown; sid: 499;)

Correlation of parameter patterns

The third method of intrusion detection is more wise than the previous two methods. It was born due to the fact that administrators check different systems and network attributes (no need to target security issues). Information

obtained in this way has a specific environment that is unchanged. This method involves using the daily operating experience of administrators as the basics for detecting abnormal signs. It can be seen as a special case of the usual Profile method. The difference here is that in fact, a profile is a part of human knowledge.

This is a powerful technique, because it allows intrusion based on unknown attacks. System operation can detect subtle changes that are not obvious to the activity itself. It inherits the disadvantages in the fact that people only understand a limited portion of information at a time, which means that certain attacks can pass without being detected.

Data processing techniques are used in intrusion detection systems

Depending on the type of method used for intrusion detection, different processing mechanisms (techniques) are also used for data for an IDS. Here are some briefly described systems:

- **Expert system** , this system works on a set of predefined rules to describe attacks. All security-related events are combined into audits and translated as if-then-else rules. Take for example Wisdom & Sense and ComputerWatch (developed at AT&T).

- **Phân tích d?u hi?u** gi?ng nh? ph??ng pháp h? th?ng Expert, ph??ng pháp này d?a trên nh?ng hi?u bi?t v? t?n công. Chúng bi?n ??i s? mô t? v? ng? ngh?a t? c?a m?i t?n công thành ??nh d?ng ki?m ??nh thích h?p. Nh? v?y, d?u hi?u t?n công có th? ???c tìm th?y trong các b?n ghi ho?c ??u vào c?a lu?ng d? li?u theo m?t cách d? hi?u. M ?t k?ch b?n t?n công có th? ???c mô t?, ví d? nh? m?t chu?i s? ki?n ki?m ??nh ??i v?i các t?n công ho?c m?u d? li?u có th? tìm ki?m ?ã l?y ???c trong cu?c ki?m ??nh. Ph??ng pháp này s? d?ng các t? t??ng ???ng tr?u t??ng c? a d? li?u ki?m ??nh. S? phát hi?n ???c th?c hi?n b?ng cách s? d?ng chu?i v?n b?n chung h?p v?i các c? ch?. ?i?n hình, nó là m?t k? thu?t r?t m?nh và th??ng ???c s? d?ng trong các h? th?ng th??ng m?i (ví d? nh? Stalker, Real Secure, NetRanger, Emerald eXpert-BSM).

- **Ph??ng pháp Colored Petri Nets** th??ng ???c s? d?ng ?? t?ng quát hóa các t?n công t? nh?ng hi?u bi?t c? b?n và ?? th? hi?n các t?n công theo ?? h?a. H? th?ng IDIOT c?a ??i h?c Purdue s? d?ng Colored Petri Nets. V?i k? thu?t này, các qu?n tr? viên s? d? dàng h?n trong vi?c b? sung thêm d?u hi?u m?i. M?c dù v?y, vi?c làm cho h?p m?t d?u hi?u ph?c t?p v?i d? li?u ki?m ??nh là m?t v?n ?? gây t?n nhi?u th?i gian. K? thu?t này không ???c s? d? ng trong các h? th?ng th??ng m?i.

- **Phân tích tr?ng thái phiên** , m?t t?n công ???c miêu t? b?ng m?t t?p các m?c tiêu và phiên c?n ???c th?c hi?n b?i m?t k? xâm nh?p ?? gây t?n h?i h? th?ng. Các phiên ???c trình bày trong s? ?? tr?ng thái phiên.

- **Ph??ng pháp phân tích th?ng kê** , ?ây là ph??ng pháp th??ng ???c s? d?ng. Hành vi ng??i dùng ho?c h? th?ng (t?p các thu?c tính) ???c tính theo m?t s? bi?n th?i gian. Ví d?, các bi?n nh? là: ??ng nh?p ng??i dùng, ??ng xu?t, s? file truy nh?p trong m?t chu k? th?i gian, hi?u su?t s? d?ng không gian ??a, b? nh?, CPU,… Chu k? nâng c?p có th? thay ??i t? m?t vài phút ??n m?t tháng. H? th?ng l?u giá tr? có ngh?a cho m?i bi?n ???c s? d?ng ?? phát hi ?n s? v??t quá ng??ng ???c ??nh ngh?a t? tr??c. Ngay c? ph??ng pháp ??n gi?n này c?ng không th? h?p ???c v?i mô hình hành vi ng??i dùng ?i?n hình. Các ph??ng pháp d?a vào vi?c làm t??ng quan profile ng??i dùng riêng l? v?i các bi?n nhóm ?ã ???c g?p l?i c?ng ít có hi?u qu?.

Vì v?y, m?t mô hình tinh vi h?n v? hành vi ng??i dùng ?ã ???c phát tri?n b?ng cách s? d?ng profile ng??i dùng ng?n h?n ho?c dài h?n. Các profile này th??ng xuyên ???c nâng c?p ?? b?t k?p v?i thay ??i trong hành vi ng??i dùng. Các ph??ng pháp th?ng kê th??ng ???c s? d?ng trong vi?c b? sung trong IDS d?a trên profile hành vi ng??i dùng thông th??ng.

- **Neural Networks** s? d?ng các thu?t toán ?ang ???c nghiên c?u c?a chúng ?? nghiên c?u v? m?i quan h? gi?a các vector ??u vào - ??u ra và t?ng quát hóa chúng ?? rút ra m?i quan h? vào/ra m?i. Ph??ng pháp neural network ???c s? d?ng cho phát hi?n xâm nh?p, m?c ?ích chính là ?? nghiên c?u hành vi c?a ng??i tham gia vào m?ng (ng ??i dùng hay k? xâm ph?m). Th?c ra các ph??ng pháp th?ng kê c?ng m?t ph?n ???c coi nh? neural networks. S? d?ng m?ng neural trên th?ng kê hi?n có ho?c t?p trung vào các ??n gi?n ?? bi?u di?n m?i quan h? không tuy?n tính gi?a các bi?n và trong vi?c nghiên c?u các m?i quan h? m?t cách t? ??ng. Các th?c nghi?m ?ã ???c ti?n hành v?i s? d? ?oán m?ng neural v? hành vi ng??i dùng. T? nh?ng k?t qu? cho th?y r?ng các hành vi c?a siêu ng??i dùng UNIX (root) là có th? d? ?oán. V?i m?t s? ít ngo?i l?, hành vi c?a h?u h?t ng??i dùng khác c?ng có th? d? ? oán. Neural networks v?n là m?t k? thu?t tính toán m?nh và không ???c s? d?ng r?ng rãi trong c?ng ??ng phát hi ?n xâm nh?p.

- **Phân bi?t ý ??nh ng??i dùng** . K? thu?t này mô hình hóa các hành vi thông th??ng c?a ng??i dùng b?ng m?t t ?p nhi?m v? m?c cao mà h? có th? th?c hi?n ???c trên h? th?ng (liên quan ??n ch?c n?ng ng??i dùng). Các nhi?m v? ?ó th??ng c?n ??n m?t s? ho?t ??ng ???c ?i?u ch?nh sao cho h?p v?i d? li?u ki?m ??nh thích h?p. B? phân tích gi? m?t t?p h?p nhi?m v? có th? ch?p nh?n cho m?i ng??i dùng. B?t c? khi nào m?t s? không h?p l? ???c phát hi? n thì m?t c?nh báo s? ???c sinh ra.

- **Computer immunology Analogies** v?i s? nghiên c?u mi?n d?ch ???c ch? ??nh ?? phát tri?n các k? thu?t ???c xây d?ng t? mô hình hành vi thông th??ng trong các d?ch v? m?ng UNIX h?n là ng??i dùng riêng l?. Mô hình này g?m có các chu?i ng?n cu?c g?i h? th?ng ???c t?o thành b?i các quá trình. Các t?n công khai thác l? h?ng trong mã ?ng d?ng r?t có kh? n?ng gây ra ???ng d?n th?c thi không bình th??ng. ??u tiên, m?t t?p d? li?u ki?m ?? nh tham chi?u ???c s?u t?p ?? trình bày hành vi h?p l? c?a các d?ch v?, sau ?ó ki?n th?c c? b?n ???c b? sung thêm v?i t?t c? các chu?i ???c bi?t rõ v? cu?c g?i h? th?ng. Các m?u ?ó sau ?ó ???c s? d?ng cho vi?c ki?m tra liên t?c các cu?c g?i h? th?ng, ?? xem chu?i ???c t?o ra ?ã ???c li?t kê trong c? s? ki?n th?c ch?a; n?u không, m?t báo c?nh s? ???c t?o ra. K? thu?t này có t? l? báo c?nh sai r?t th?p. Tr? ng?i c?a nó là s? b?t l?c trong vi?c phát hi ?n l?i trong c?u hình d?ch v? m?ng.

- **Machine learning** (nghiên c?u c? ch?). ?ây là m?t k? thu?t thông minh nhân t?o, nó l?u lu?ng l?nh ??u ra ng??i dùng vào các bi?u m?u vector và s? d?ng nh? m?t tham chi?u c?a profile hành vi ng??i dùng thông th??ng. Các profile sau ?ó ???c nhóm vào trong m?t th? vi?n l?nh ng??i dùng có các thành ph?n chung nào ?ó.

- **Vi?c t?i thi?u hóa d? li?u** th??ng ph?i dùng ??n m?t s? k? thu?t s? d?ng quá trình trích d? li?u ch?a bi?t nh?ng có kh? n?ng h?u d?ng tr??c ?ó t? nh?ng v? trí d? li?u ???c l?u tr? v?i s? l??ng l?n. ph??ng pháp t?i thi?u d? li?u này v??t tr?i h?n ??i v?i vi?c s? lý b?n ghi h? th?ng l?n (d? li?u ki?m ??nh). M?c dù v?y, chúng kém h?u d?ng ?? i v?i vi?c phân tích lu?ng l?u l??ng m?ng. M?t trong nh?ng k? thu?t t?i thi?u hóa d? li?u c? b?n ???c s? d?ng trong phát hi?n xâm nh?p ???c k?t h?p v?i các cây phán quy?t. Các mô hình cây phán quy?t cho phép ai ?ó có th ? phát hi?n các s? b?t th??ng trong m?t c? s? d? li?u l?n. K? thu?t khác ph?i dùng ??n các ?o?n, cho phép trích m ?u c?a các t?n công ch?a bi?t. ?i?u ?ó ???c th?c hi?n b?ng vi?c h?p l? hóa các m?u ?ã ???c trích t? m?t t?p ki?m ??nh ??n gi?n v?i các m?u khác ???c cung c?p cho t?n công ch?a bi?t ?ã c?t gi?. M?t k? thu?t t?i thi?u hóa d? li? u ?i?n hình ???c k?t h?p v?i vi?c tìm ki?m các nguyên t?c k?t h?p. Nó cho phép ai ?ó có th? trích ki?n th?c ch?a hi?u tr??c ?ó v? các t?n công m?i ho?c ?ã xây d?ng trên m?u hành vi thông th??ng. S? phát hi?n b?t th??ng th?? ng gây ra các báo c?nh sai. V?i vi?c t?i thi?u hóa d? li?u, nó d? dàng t??ng quan d? li?u ?ã liên quan ??n các báo c?nh v?i d? li?u ki?m ??nh t?i thi?u, do ?ó gi?m ?áng k? xác su?t báo c?nh sai.

You finished reading the article "**Intrusion Detection System (IDS) (Part 2)**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com