[illegible] CEH [illegible] :([illegible])

[illegible] (Intrusion Detection Systems [illegible]) IDS [illegible]

[illegible] (Intrusion Prevention Systems [illegible]) IPS [illegible]

[illegible] CEH [illegible]

[illegible] (Intrusion Detection System) [illegible]

Intrusion Detection and Prevention Systems

Intrusion Detection and Prevention Systems (IDPS) are network security appliances that monitor network and system activities for malicious activity. The main functions of intrusion detection and prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.

IDPS are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting the occurrences to security administrators. In addition, organizations use IDPS for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies. IDPS have become a necessary addition to the security infrastructure of nearly every organization.

IDPS typically record information related to observed events, notify security administrators of important observed events, and produce reports. Many IDPS can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g., reconfiguring a firewall), or changing the content of the attack.

Detection Methods

IDPS use several detection methods, including signature-based detection (misuse detection), anomaly detection, and stateful protocol analysis.

Signature-Based Detection

Signature-based detection is the process of comparing signatures against observed events to identify possible incidents. A signature is a pattern that corresponds to a known threat. Signature-based detection is very effective at detecting known threats but largely ineffective at detecting unknown threats, and many types of threats often have obvious signatures. For example, a signature can look for a certain sequence of bytes in a network packet or for certain keywords in a log entry. Signature-based detection is also known as misuse detection.

Anomaly Detection

Anomaly detection is the process of comparing definitions of what activity is considered normal against observed events to identify significant deviations. An IDPS using anomaly detection first learns what is normal for the network and system activity by collecting information over a period of time. Then, it uses this baseline to identify abnormal activity. The baseline can be developed for many characteristics, such as the number of e-mails sent by a user, the amount of bandwidth typically used by a protocol, and the number of processes running on a server. Anomaly detection is effective at detecting previously unknown threats. Common challenges with anomaly detection are the difficulty of building an accurate baseline and the large amount of resources that are often needed.

Stateful Protocol Analysis

Stateful protocol analysis is the process of comparing predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state against observed events to identify deviations. Unlike anomaly detection, which uses host or application-specific profiles, stateful protocol analysis relies on vendor-developed universal profiles that specify how particular protocols should and should not be used. It understands and tracks the state of network, transport, and application protocols that have a notion of state. For example, in a TCP session, the client first requests a connection with the server, and the server responds. Stateful protocol analysis can determine whether the server's response is appropriate given the client's request. Stateful protocol analysis is capable of understanding and tracking the state of some application protocols that have a notion of state, such as TLS, HTTP, and FTP. However, it is usually not effective at detecting attacks at the application level, as most application protocols are complex and their behavior is difficult to profile.

Common Challenges

IDPS technologies have several common challenges. IDPS sensors cannot fully understand the context in which network activity occurs, so they frequently misinterpret the meaning of events. This leads to a large number of false positives (benign activity misidentified as malicious) and false negatives (malicious activity misidentified as benign). Tuning IDPS sensors to increase the percentage of true positives is usually a significant effort. IDPS sensors usually require considerable tuning to reduce the number of false positives and false negatives. Many IDPS technologies require frequent signature updates to ensure effectiveness against new threats. Also, in many cases, the security administrators who are responsible for the IDPS technologies are not notified promptly when new versions of software are released, so they are not aware of the need to perform updates.

Selection and Implementation

Organizations should carefully select IDPS technologies that meet their particular needs. Organizations should first identify their requirements and then use that information to evaluate candidate solutions. Key requirements include the following:

- Which types of events need to be monitored (e.g., network activity, host activity)
- Whether the IDPS technology must work in a particular environment (e.g., large enterprise network, high-speed network)
- Whether the IDPS technology must be able to interface with existing software (e.g., security information and event management software)
- Whether the IDPS technology must be able to support a particular security policy
- Whether the IDPS technology must be able to support a particular level of performance
- Whether the IDPS technology must be able to support a particular level of reliability
- Whether the IDPS technology must be able to support a particular level of scalability
- Whether the IDPS technology must be able to support a particular level of flexibility
- Whether the IDPS technology must be able to support a particular level of usability
- Whether the IDPS technology must be able to support a particular level of maintainability
- Whether the IDPS technology must be able to support a particular level of portability
- Whether the IDPS technology must be able to support a particular level of interoperability
- Whether the IDPS technology must be able to support a particular level of security
- Whether the IDPS technology must be able to support a particular level of privacy
- Whether the IDPS technology must be able to support a particular level of compliance
- Whether the IDPS technology must be able to support a particular level of auditability
- Whether the IDPS technology must be able to support a particular level of accountability
- Whether the IDPS technology must be able to support a particular level of traceability
- Whether the IDPS technology must be able to support a particular level of integrity
- Whether the IDPS technology must be able to support a particular level of availability
- Whether the IDPS technology must be able to support a particular level of confidentiality
- Whether the IDPS technology must be able to support a particular level of authentication
- Whether the IDPS technology must be able to support a particular level of authorization
- Whether the IDPS technology must be able to support a particular level of nonrepudiation

Распределенные системы обнаружения вторжений

Распределенная система обнаружения вторжений (DIDS) — это система, которая объединяет в себе несколько (NIDS) и/или (HIDS).

Преимущества использования распределенных систем

Распределенные системы обнаружения вторжений имеют ряд преимуществ по сравнению с (...) Они могут обеспечивать более высокий уровень безопасности, поскольку они могут обнаруживать вторжения, которые могут быть пропущены (NIC) или (HIDS).

Недостатки использования распределенных систем

Распределенные системы обнаружения вторжений также имеют некоторые недостатки. Они могут быть более сложными в настройке и управлении, чем (NIDS) или (HIDS). Они также могут быть более дорогими.

Как работают распределенные системы обнаружения вторжений

Распределенные системы обнаружения вторжений работают, собирая данные с нескольких (NIDS) и/или (HIDS). Эти данные затем анализируются для выявления вторжений. Если вторжение обнаружено, система может предпринять различные действия, такие как блокирование трафика или отправка предупреждения.

Типы распределенных систем обнаружения вторжений

Существует несколько типов распределенных систем обнаружения вторжений. Некоторые из наиболее распространенных типов включают:

- **Распределенные системы обнаружения вторжений (DIDS)**

Развертывание распределенных систем обнаружения вторжений

Развертывание распределенной системы обнаружения вторжений может быть сложным процессом. Необходимо тщательно спланировать, где будут размещены NIDS и HIDS, а также как они будут взаимодействовать друг с другом. Также необходимо настроить систему для обнаружения конкретных типов вторжений.

Управление распределенными системами обнаружения вторжений

Управление распределенной системой обнаружения вторжений может быть сложным процессом. Необходимо регулярно обновлять систему, чтобы она могла обнаруживать новые типы вторжений. Также необходимо анализировать данные, собранные системой, чтобы выявлять тенденции и закономерности.

Безопасность распределенных систем обнаружения вторжений

Безопасность распределенной системы обнаружения вторжений имеет решающее значение. Необходимо защитить систему от несанкционированного доступа, чтобы злоумышленники не могли отключить ее или изменить ее настройки. Также необходимо защитить данные, собранные системой, чтобы они не были украдены или изменены.

پاسخ فعال در سامانه تشخیص نفوذ

سامانههای تشخیص نفوذ از لحظهای که به کار میافتند، ضمن به دست آوردن اطلاعات مربوط به رخدادها و تجزیه و تحلیل آنها، اگر نشانهایی دال بر وقوع یک حمله را تشخیص دهند، پاسخ لازم را در قبال آن به نحوههای مختلف تولید میکنند . گاهی این پاسخ به صورت یک هشدار به مدیر شبکهاست و گاهی نوشتن یک اطلاع در فایل رخدادها یا به صورت تنظیم مجدد دیواره آتش یا دستگاههای دیگری در شبکه است . سامانههای تشخیص نفوذ فعال هر نفوذی را که تشخیص دهند بهطور خودکار پاسخ میدهند . این پاسخها به سه گروه پاسخ فعال براساس جمعآوری اطلاعات اضافی، پاسخ فعال از نوع تغییر محیط و پاسخ فعال از نوع عکسالعمل در مقابل حمله تقسیم میشوند .

سامانههای تشخیص نفوذ رایگان

از رایجترین سامانههای تشخیص نفوذ رایگانی که در دسترس کاربران و کسبوکارها قرار دارد باید به Snort، Samhain، Prelude Hybrid IDS، OSSEC HIDS، Bro NIDS، AIDE و Suricata اشاره کرد .

بهطور □□□□، OSSEC سامانه تشخیص نفوذ مبتنی بر سیستم میزبان(HIDS) به صورت متن باز و رایگان است. ابزار فوق دارای قابلیتهایی نظیر تحلیل گزارشها (Log Analysis)، صحهگذاری بر یکپارچگی (Integrity Checking)، پایش رجیستری ویندوز، کشف و شناسایی روتکیتها، هشداردهی مبتنی بر زمان و پاسخدهی فعال (Active Response) است. قابلیت HIDS را برای بسیاری از سیستمعاملها نظیر لینوکس، اوپنبیاسدی، فریبیاسدی، اواس ده، سولاریس (سیستمعامل) و ویندوز میتوان به کار گرفت . ابزار فوق با استفاده از مرکز کنترل متمرکز و معماری چندسکویی توانایی مدیریت تعداد زیادی از سیستمهای تحت کنترل خود را دارد .

اسنورت (snort) که در مطالب قبلی نیز به آن اشاره داشتیم، یک سامانه کشف نفوذ است که تحت لایسنس جیپیال عرضه میشود. اسنورت در حال حاضر توسط Sourcefire توسعه مییابد . این برنامه در سال ۲۰۰۹ به عنوان یکی از بهترین و کاربردیترین نرمافزارهای آزاد انتخاب شد . این سیستم بهطور کلی میتواند در ۳ حالت کار کند . حالت اول این است که سیستم به تمام بستههای عبوری از شبکه گوش کرده و آنها را نمایش میدهد. یک حالت دیگر این است که سیستم به بستههای عبوری گوش کرده و آنها را روی حافظه ذخیره میکند . حالت سوم که پیشرفته تر از حالتهای قبلی است تشخیص نفوذ است. در این حالت سیستم ترافیک عبوری را تحلیل کرده و با توجه به قوانینی که کاربر برای آن تعریف کرده است خطرات احتمالی را تشخیص میدهد .

در شماره آینده مبحث فوق را ادامه میدهیم .

برای مطالعه رایگان تمام بخشهای دوره **CEH** روی لینک زیر کلیک کنید :

آموزش رایگان دوره CEH

دسته بندی:
امنیت
تاریخ انتشار :
13:20 - 03/06/1399
برچسب:
دوره CEH - آموزش رایگان CEH - آموزش رایگان دوره CEH - هکر کلاه سفید - آموزش CEH v10 - آموزش رایگان CEH10 - هک اخلاقی - سامانههای تشخیص نفوذ - Intrusion Detection System - سامانه پیشگیری از نفوذ

نشانی
□□□□: https://www.shabakeh-mag.com/security/17301/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-ceh-%D9%87%DA%A9%D8%B1-%DA%A9%D9%84%D8%A7%D9%87-%D8%B3%D9%81%DB%8C%D8%AF-%D8%B3%D8%A7%D9%85%D8%A7%D9%86%D9%87-%D8%AA%D8%B4%D8%AE%DB%8C%D8%B5-%D9%86%D9%81%D9%88%D8%B0-%DA%86%DA%AF%D9%88%D9%86%D9%87-%D8%A7%D8%B2-

%D8%B3%D8%A7%D9%85%D8%A7%D9%86%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-
%D9%85%D8%AD%D8%A7%D9%81%D8%B8%D8%AA-
%D9%85%DB%8C%E2%80%8C%DA%A9%D9%86%D8%AF%D8%9F