Урок №9. Виявлення атак. Захист периметра комп'ютерних мереж

Процес виявлення атак є процесом оцінки підозрілих дій, які відбуваються в корпоративній мережі. Інакше кажучи, виявлення атак (intrusion detection) це процес ідентифікації й реагування на підозрілу діяльність, спрямовану на обчислювальні або мережні ресурси.

Основні підходи до виявлення атак практично не змінилися за останню чверть століття, і, незважаючи на гучні заяви розробників, можна з упевненістю стверджувати, що виявлення атак базується або на методах *сигнатурного аналізу*, або на методах *виявлення аномалій*. Можливо також спільне використання зазначених вище методів.

Існує кілька способів класифікації систем виявлення атак, кожен з яких заснований на різних характеристиках:

1. *Спосіб контролю за системою* (поділяються на network-based, host-based і applicationbased).
2. *Спосіб аналізу.* (частина системи визначення проникнення, яка аналізує події, отримані з джерела інформації, і приймає рішення, чи відбувається проникнення). Способами аналізу є виявлення зловживань (misuse detection) та виявлення аномалій (anomaly detection).
3. *Затримка в часі між отриманням інформації з джерела та її аналізом і прийняттям рішення*. Залежно від затримки в часі, системи виявлення атак діляться на interval-based (або пакетний режим) і real-time.

Механізми виявлення атак, застосовувані в сучасних системах виявлення атак IDS (Intrusion Detection System), засновані на декількох загальних методах.

Класифікація систем виявлення атак може бути виконана за декількома ознаками:

- *за способом реагування*; розрізняють пасивні й активні IDS. **Пасивні** IDS просто фіксують факт атаки, записують дані у файл журналу й видають попередження. **Активні** IDS намагаються протидіяти атаці.
- за способом виявлення атаки; За способом виявлення атаки системи IDS прийнято ділити на дві категорії: *виявлення аномального поводження* (anomaly-based); *виявлення зловживань* (misuse detection або signature-based). Аномальне поводження користувача (тобто атака або яка-небудь ворожа дія) часте проявляється як відхилення від нормального поводження. Прикладом аномального поводження може служити велика кількість з'єднань за короткий проміжок часу, високе завантаження центрального процесора й т.ін. Однак аномальне поводження не завжди є атакою. Наприклад, одночасну посилку

великої кількості запитів від адміністратора мережі система виявлення атак може ідентифікувати як атаку типу “відмова в обслуговуванні” (denial of service).

- *за способом збору інформації про атаку*.

Статичні і динамічні IDS

1. Статичні засоби роблять «знімки» (snapshot) середовища та здійснюють їх аналіз, розшукуючи вразливе ПО, помилки в конфігураціях і т. д. Статичні IDS перевіряють версії прикладних програм на наявність відомих вразливостей і слабких паролів, перевіряють вміст спеціальних файлів в директоріях користувачів або перевіряють конфігурацію відкритих мережевих сервісів. Статичні IDS виявляють сліди вторгнення.
2. Динамічні IDS здійснюють моніторинг у реальному часі всіх дій, що відбуваються в системі, переглядаючи файли аудиту або мережні пакети, що передаються за певний проміжок часу. Динамічні IDS реалізують аналіз в реальному часі і дозволяють постійно стежити за безпекою системи.

Мережеві IDS

Мережеві IDS (англ. *Network-based IDS, NIDS*) розташовуються в стратегічному місці або у таких місцях мережі, де можливий контроль трафіку всіх пристроїв у мережі. Вони здійснюють контроль усього трафіку даних всієї підмережі та порівнюють трафік, який передається у підмережі з бібліотекою відомих атак. Як тільки розпізнана атака або визначено відхилення у поведінці, відразу відсилається попередження адміністратору.

Хостові IDS

IDS, які встановлюються на хості і виявляють зловмисні дії на ньому називаються хостовими або системними IDS.

Експертні системи.

Експертна система складається з набору правил, які охоплюють знання людини-експерта. Використання експертних систем являє собою розповсюджений метод виявлення атак, при якому інформація про атаки формулюється у вигляді правил. Ці правила можуть бути записані, наприклад, у вигляді послідовності дій або сигнатури. При виконанні кожного із цих правил приймається рішення про наявність несанкціонованої діяльності. Важливим достоїнством такого підходу є практично повна відсутність фіктивних тривог.

Сигнатурний аналіз заснований на припущенні, що сценарій атаки відомий і спроба її реалізації може бути виявлена в журналах реєстрації подій або шляхом аналізу мережевого трафіку.

Аналіз активності

Стандарти кібербезпеки

Стандарти кібербезпеки – це методи, що зазвичай викладені в опублікованих матеріалах, які намагаються захистити кібернетичне середовище користувача чи організації.Це середовище включає в себе користувачів, мережі, пристрої, все програмне забезпечення, процеси, інформацію в режимі зберігання або транзиту, програми, служби та системи, які можуть бути безпосередньо або опосередковано підключені до мереж.

Основна мета — знизити ризики, включаючи попередження або пом'якшення кібер-атак. Ці опубліковані матеріали включають збірки інструментів, політику, концепції безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, навчання, найкращі практики, забезпечення та технології.

Міжнародні стандарти

BS 7799-1: 2005 — Британський стандарт BS 7799 перша частина. BS 7799 Частина 1 — Кодекс практики управління інформаційною безпекою (Практичні правила управління інформаційної безпеки) описує 127 механізмів контролю, необхідних для побудови системи управління інформаційною безпекою (СУІБ) організації, визначених на основі кращих прикладів світового досвіду в цій області . Цей документ служить практичним керівництвом по створенню СУІБ

BS 7799-2: 2005 — Британський стандарт BS 7799 друга частина стандарту. BS 7799 Частина 2 — Управління інформаційною безпекою — специфікація систем управління інформаційною безпекою (Специфікація системи управління інформаційної безпеки) визначає специфікацію СУИБ. Втора частина стандарту використовується як критерії при проведенні офіційної процедури сертифікації СУІБ організації.

BS 7799-3: 2006 — Британський стандарт BS 7799 третя частина стандарту. Новий стандарт в області управління ризиками інформаційної безпеки

ISO/IEC 17799: 2005 — «Інформаційні технології — Технології безпеки — Практичні правила управління інформаційної безпеки». Міжнародний стандарт, базувався на BS 7799-1: 2005.

ISO/IEC 27000 — Словарь і визначення.

ISO/IEC 27001 — «Інформаційні технології — Методи забезпечення безпеки — Системы управління інформаційної безпеки — Требования». Міжнародний стандарт, базувався на BS 7799-2: 2005.

ISO/IEC 27002 — Зараз**: ISO/IEC 17799: 2005**. «Інформаційні технології — Технології безпеки — Практичні правила управління інформаційної безпеки». Дата выхода — 2007 год.

ISO/IEC 27005 — Зараз: **BS 7799-3: 2006** — Руководство по управлению рисками ИБ.

Німецьке агентство з інформаційної безпеки. Інструкція з захисту базової лінії — стандартні гарантії безпеки (керівництво по базовому рівню захисту інформаційних технологій).