Львівський державний університет безпеки життєдіяльності

Кафедра управління проектами, інформаційних технологій та телекомунікацій

Лекція

з курсу:

" Безпека інформаційно-комунікаційних систем"

на тему: **" Засоби захисту в розподілених інформаційно-комунікаційних системах "**

(для курсантів та студентів 5-го курсу спеціальності «Комп'ютені науки)

ПЛАН ЛЕКЦІЇ

1. Архітектура захищених мереж.
2. Міжмережні екрани.
3. Системи виявлення атак.
4. Системи аналізу та оцінювання вразливостей.

ЛІТЕРАТУРА

1. **Андрианов В.И., Бородин В.А., Соколов А.В.** "Шпионские штучки" и устройства для защиты объектов и информации: Справочное пособие. – СПб.: Лань, 1996. – 272 с.
2. **Анин Б.** Защита компьютерной информации. — СПб.: БХВ-Петербург, 2000. — 384 с.
3. **Гайворонський М.В., Новіков О.М.** Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с. іл.
4. **Тимошенко А.О.** Методи аналізу та проектування систем захисту інформації: Курс лекцій. - К.: Політехніка, 2007. – 174 с.
5. **Kahn D.** The Codebreakers: The Story of Secret Writing. - N.Y.: MacMillan, 1967. – 1164 p.
6. **Мельников В.В.** Защита информации в компьютерных системах. – М.: Финансы и статистика: Эмектроинформ, 1997. – 368 с.

1. Архітектура захищених мереж.

У сучасних інформаційно-комунікаційних системах застосовують різні засоби і заходи захисту. До заходів захисту насамперед належать розроблення політики безпеки інформації в системі та проектування ІКС з урахуванням вимог цієї політики. Необхідною умовою також є призначення осіб, які б відповідали за захист інформації в системі, з визначенням їхніх обов'язків і повноважень, або навіть створення спеціального структурного підрозділу — служби захисту інформації (СЗІ).

Протидія прослуховуванню трафіку

Для побудови захищених ІКС архітектура мережі має задовольняти певні вимоги. Головною вимогою є відмова від використання таких фізичних і логічних топологій мереж, в яких можливе безпосереднє прослуховування трафіку цілого сегмента мережі з будь-якого вузла у ній. Типовими прикладами є мережі Ethernet 10BASE-2 та 10BASE-5 («тонкий» і «товстий» Ethernet), у яких використовується фізична топологія *спільна шина* — всі станції сегмента підключені до єдиного коаксіального кабелю, який утворює розподілене середовище передавання даних. Ці технології — вже застарілі, і їх майже не використовують у сучасних ІКС. Але прослуховування трафіку можливе і в мережах із фізичною топологією «зірка». Наприклад, у мережах Ethernet 10BASE-T та 100BASE-T інколи використовують *концентратори* (Hub). Ці пристрої транслюють отриманий блок даних (кадр) на всі порти, за винятком того, з якого цей блок даних надійшов. Таким чином, до кожного вузла надходить весь трафік цілого сегмента, що дає змогу його безперешкодно захоплювати й аналізувати. У мережах TokenRing трафік передається по логічному кільцю, тому весь трафік сегмента також проходить через кожний із вузлів.

Сучасні мережі Ethernet побудовано з використанням *комутаторів* (Switch). Комутатори діють на основі алгоритму мосту (IEEE 802.ID) [240], зберігаючи таблиці відомих їм апаратних адрес і передаючи кадри з відомими їм адресатами лише на ті порти, що ведуть до цих адресатів. Тому, коли два вузли здійснюють між собою обмін інформацією, пакети не потрапляють до жодного зайвого кінцевого вузла. Відтак мережі, побудовані на комутаторах, суттєво обмежують можливості з перехоплення трафіку.

Сегментація мережі

Щоб розмежувати доступ до окремих ресурсів у мережі, використовують її сегментацію, яка, крім того, дає змогу значно покращити масштабованість мережі. Для сегментації мережі на канальному рівні застосовують дуже потужний засіб — віртуальні локальні обчислювальні мережі, ВЛОМ (Virtual Local Area Network, VLAN). *Віртуальна локальна мережа* — це підмножина вузлів мережі, трафік між якими на канальному рівні повністю ізольований від інших вузлів. Тобто кадри із ВЛОМ (зокрема, широкомовні) комутатор не передає за її межі. Віртуальні локальні мережі створюють, відповідним чином настроївши конфігурацію комутаторів. Для цього використовують номери портів, MAC-адреси, протоколи. Стандарт IEEE 802.1Q, визначає спосіб маркування кадрів спеціальними тегами, які задають для В ЛОМ 12-розрядний номер і дають змогу будувати складні ієрархічні мережі з великою кількістю ВЛОМ, що охоплюють багато комутаторів.

Недоліком ВЛОМ є те, що обмін між цими мережами може бути заблокований повністю. Засоби канального рівня не дають змоги здійснювати контрольований обмін інформацією між різними сегментами мережі. Для цього залучають засоби мережного рівня. Як правило, IP-підмережі організують таким чином, аби вони збігалися з віртуальними локальними мережами. Передавання трафіку між підмережами здійснюють маршрутизатори. За такої будови мережі трафік у межах окремої підмережі передається на канальному рівні, без залучення засобів мережного рівня, оскільки він повністю локалізований в межах однієї ВЛОМ. За потреби передати трафік між підмережами в дію вступають засоби мережного рівня. При цьому можна здійснювати фільтрацію трафіку. Найпростішу фільтрацію здійснюють маршрутизатори. Для реалізації складніших правил фільтрації залучають

спеціальні програмні засоби або програмно-апаратні пристрої — *міжмережні екрани,* або *брандмауери* (Firewall). їх буде розглянуто далі у цьому розділі.

Резервування мережного обладнання і каналів зв'язку

Важливою складовою безпеки інформації в мережі є забезпечення доступності вузлів. Зазвичай це завдання розглядається не в контексті захисту інформації, а в контексті підвищення надійності та продуктивності комп'ютерних мереж. Утім розглянемо деякі основні принципи і можливості сучасних мережних технологій, які забезпечують цю важливу складову безпеки інформації.

Оскільки будь-яке обладнання не може бути стовідсотково надійним, під час створення чутливих до доступності окремих ресурсів ІКС передбачають резервування мережного обладнання і каналів зв'язку. У цьому випадку бажано забезпечити можливість автоматичного перенастроювання мережі з основних каналів та вузлів комутації на резервні.

На канальному рівні за таких обставин можуть виникати певні проблеми. Якщо розглядати топологію мережі, в якій наявні резервні вузли комутації та канали зв'язку, то в такій мережі неодмінно будуть виникати кільця. Але наявність кілець не сумісна з алгоритмом мосту, за яким працюють комутатори. За наявності кілець у мережі почнуть швидко розмножуватися широкомовні пакети, і за дуже короткий час (кілька секунд) настане перенавантаження мережі.

Недолік протоколу STP полягає у тому, що резервні зв'язки у звичайному режимі вимкнено, тобто частина портів комутаторів не функціонує. Для окремих каналів, що потребують підвищеної пропускної здатності та надійності, ефективно застосовувати агрегацію каналів — утворення одного логічного каналу з кількох паралельних фізичних каналів. Комутатори відрізняють такий канал від звичайних з'єднань і збалансовують навантаження між окремими зв'язками. Комутатори виявляють обрив будь-якого зі зв'язків і автоматично змінюють режим балансування навантаження таким чином, щоб кадри було спрямовано лише на ті зв'язки, що функціонують. Раніше діяв стандарт агрегації каналів на рівні MAC лише для мереж Ethernet (IEEE 802.3 ad). Із січня 2008 року почав діяти стандарт IEEE 802.1AX, що описує агрегацію каналів на рівні, не залежному від MAC.

2. Міжмережні екрани.

Міжмережні екрани (МЕ), або брандмауери, призначені для захисту внутрішніх ресурсів мереж шляхом обмеження можливостей обміну між ними. Комп'ютер, на якому функціонує ПЗ міжмережного екрана, або спеціалізований програмно- апаратний пристрій, що реалізує функції МЕ, виконує роль шлюзу між двома мережами, найчастіше — між Інтернетом і корпоративною мережею.

Термін «брандмауер» походить від німецького слова «brandmauer», що, як і англійське слово «firewall», означає «протипожежна капітальна стіна» (але в жодному разі не «стіна вогню» чи «вогняна стіна», як дехто помилково вважає).

Засіб, подібний до міжмережного екрана, інколи використовують для захисту окремого комп'ютера. У цьому випадку екран у вигляді спеціалізованого програмного забезпечення встановлюють на комп'ютер, що підлягає захисту, для здійснення контролю всього вхідного і вихідного трафіку. Такий мережний екран часто називають *персональним брандмауером.*

Можливості міжмережних екранів

У загальному випадку робота міжмережного екрана базується на динамічному виконанні двох груп функцій:

- фільтрація інформаційних потоків, що проходять крізь нього;
- посередництво під час реалізації міжмережної взаємодії (проксі-сервер).

Фільтрація трафіку здійснюється згідно з попередньо завантаженими до МЕ правилами, які є відображенням мережних аспектів політики безпеки. Оскільки результат оброблення пакета в загальному випадку залежить від послідовності застосування правил, останні мають бути належним

чином упорядковані. Механізм застосування правил можна описати як послідовність фільтрів, кожний з яких містить низку критеріїв, які має задовольняти пакет. Якщо пакет відповідає критеріям цього фільтра, до нього застосовують певну дію:

- пакет вилучається з інформаційного потоку і знищується (може відбутися реєстрація відповідної події, поінформування відправника пакета щодо унеможливлення його доставления тощо);
- пакет пропускається, тобто надсилається на адресу призначення;
- пакет обробляється від імені одержувача і результат повертається відправнику;
- пакет передається певній програмі на оброблення (наприклад, для шифрування-дешифрування, антивірусної перевірки, трансляції мережних адрес тощо), після чого він, як правило, повертається для аналізу наступними фільтрами;
- пакет передається для аналізу наступним фільтром або фільтром, визначеним із послідовності (тобто певну кількість фільтрів може бути пропущено).

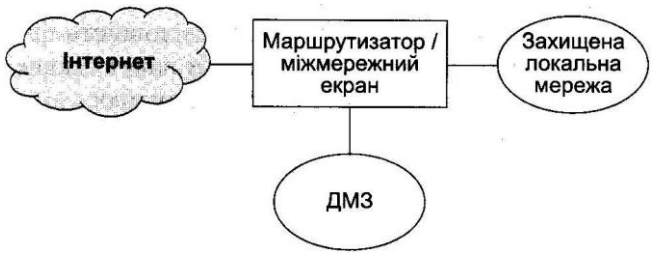
Якщо пакет не відповідає критеріям фільтра, він передається на наступний фільтр. Оскільки правила мають забезпечувати визначеність дій, які застосовують до кожного пакета, є правила за умовчанням, що застосовують до пакета, для якого не знайшлося відповідного фільтра. Від цих правил залежить принцип політики безпеки, який реалізує МЕ. Позаяк фактично є два правила за умовчанням — пропустити чи не пропустити пакет, — відповідно до них, реалізують два різних принципи політики безпеки.

Перший принцип полягає у фільтруванні всіх потенційно небезпечних пакетів. Такий підхід забезпечує доступність ресурсів мережі, але не гарантує достатнього рівня захисту, позаяк пропущеним може бути будь-який пакет із непередбаченими параметрами. Тому цей підхід вважають хибним.

Інший підхід базується на принципі мінімуму повноважень, що означає: «заборонено все, що не дозволено явно». Правило за умовчанням таке: відкинути всі пакети, що не відповідають явно заданим фільтрам. Звісно, такий підхід не гарантуватиме достатнього рівня захисту, якщо до пакетів вживати занадто ліберальні правила, що їх пропускають. За відсутності таких правил кожний доступний у мережі сервіс потребуватиме окремого явного дозволу.

Розміщення міжмережних екранів

Типовим є виокремлення так званої *демілітаризованої зони* (ДМЗ), правила обміну з якою відмінні від правил обміну із внутрішньою (захищеною) мережею. У ДМЗ переважно розміщують сервери, до яких необхідно відкрити доступ із зовнішньої мережі (наприклад, корпоративний веб-сайт). Це дає змогу встановити більш жорсткі обмеження на взаємодію із внутрішньою мережею. Наприклад, додавання до ДМЗ серверів FTP та HTTP, а також поштового сервера дає можливість повністю заборонити доступ до внутрішньої мережі за номерами портів 21, 25 і 80. При цьому на внутрішніх серверах і робочих станціях можуть функціонувати сервери, доступ до яких можна здійснити лише зсередини захищеної мережі.



Рівні реалізації

Розрізняють три рівні функціональності МЕ .

1. Пакетні фільтри, або екрануючі маршрутизатори, — функціонують переважно на третьому (мережному) рівні моделі взаємодії відкритих систем (OSI); як правило, аналізують також інформацію із заголовків протоколів четвертого (транспортного) рівня.

2. Шлюзи сеансового рівня, які ще називають екрануючим транспортом, — функціонують здебільшого на п'ятому (сеансовому) рівні моделі OSI.

3. Прикладні, або екранні шлюзи, — функціонують на прикладному рівні моделі OSI.

Мережні екрани, що реалізують функціональність якогось із рівнів, зазвичай реалізують функціональність нижчих рівнів.

Пакетні фільтри

Пакетні фільтри здійснюють аналіз заголовків пакетів для протоколів TCP, UDP та IP і, відповідно до заданого адміністратором безпеки набору правил, приймають рішення про дії з пакетом. Кожний пакет аналізують окремо від інших, отримуючи такі параметри:

- IP-адреси відправника й одержувача;
- тип пакета (протокол);
- прапорець фрагментації пакета;
- номери портів TCP (UDP) відправника й одержувача;
- прапорець SYN (ознака першого пакета під час встановлення з'єднання);
- інші прапорці.

Пакетні фільтри мають свої переваги:

- легкість у застосуванні самого МЕ;
- прості процедури інсталяції та конфігурування;
- прозорість для прикладних програм;
- мінімальний вплив на продуктивність мережі;
- низька вартість.

Як пакетний фільтр використовують програмний засіб, що встановлюють на звичайному комп'ютері. Такі засоби входять, зокрема, до стандартних комплектацій ОС Linux та FreeBSD. Функції фільтрації пакетів вбудовують також у більшість сучасних маршрутизаторів.

Пакетні фільтри мають низку суттєвих недоліків, що знижують їхню надійність. Серед цих недоліків:

- перевірка лише заголовків пакетів, що спричиняє вразливість до підроблення решти параметрів (наприклад, адрес відправника);
- відсутність перевірки цілісності й справжності пакетів;
- відсутність автентифікації кінцевих вузлів.

Шлюзи сеансового рівня

Шлюзи сеансового рівня призначені для здійснення контролю за віртуальними з'єднаннями і трансляції IP-адрес (Network Address Translation, NAT) під час взаємодії із зовнішньою мережею. Захисні функції шлюзів сеансового рівня є посередницькими.

Наприклад, такий шлюз може удавати, що з'єднання встановлюється з одним із його власних TCP-портів, тоді як насправді він згідно із своїми настроюваннями ініціює з'єднання з портом іншого комп'ютера (як правило, всередині захищеної мережі), після чого передає дані в обох напрямках. Для комп'ютера-іні- ціатора з'єднання виглядатиме так, ніби він працює з сервісом на самому МЕ. Ще типовішим випадком є дозвіл ініціювати з'єднання лише зсередини захищеної мережі, при цьому для зовнішніх комп'ютерів ініціатором з'єднання буде МЕ. Головна перевага таких МЕ полягає в наявності можливості приховати внутрішню структуру захищеної мережі.

Контроль віртуальних з'єднань полягає у контролі за встановленням TCP- з'єднання і здійсненні стеження за послідовністю пакетів і квитанцій-підтверджень у встановлених з'єднаннях. Для цього шлюз сеансового рівня має зберігати інформацію про встановлені з'єднання у спеціальних таблицях.

Переважна більшість шлюзів сеансового рівня постачаються разом зі шлюзами прикладного рівня. Але слід зазначити, що функції шлюзів сеансового рівня можуть мати і програмні засоби, які

здебільшого розглядаються як пакетні фільтри. Як приклад можна назвати програму ipfw, що входить до складу ОС FreeBSD. Вона містить функції, які реалізують шлюз сеансового рівня.

Прикладний шлюз

Прикладні шлюзи, або МЕ прикладного рівня, працюють як проксі-сервери протоколів прикладного рівня (HTTP, FTP, Telnet тощо). їхні функції, як і функції шлюзів сеансового рівня, — посередницькі. Але, на відміну від шлюзу сеансового рівня, такий МЕ містить у собі не лише транслятор з'єднань, а й сервери прикладних протоколів. Окрім можливості приховувати внутрішню структуру захищеної мережі такі МЕ дають змогу використовувати для розмежування доступу достатньо широкий спектр засобів автентифікації прикладного рівня, обмежуючи доступ на основі комбінації адрес, номерів портів, повноважень окремих користувачів, реального часу.

Прикладний шлюз забезпечує такі додаткові функції захисту:

- ідентифікація й автентифікація користувачів за спроби встановити з'єднання через МЕ;
- перевірка достовірності інформації, яку передають через МЕ; 4- розмежування доступу до ресурсів мереж;
- фільтрація й перетворення потоку повідомлень (наприклад, антивірусні й антиспамові перевірки, шифрування й дешифрування);
- реєстрація подій, реагування на події, аналіз зареєстрованої інформації, генерування звітів;
- кешування даних, що надходять із зовнішньої мережі.

Шлюзи прикладного рівня мають також суттєві недоліки:

1. значна складність самого МЕ, а також процедур його встановлення й конфігурування;
2. підвищені вимоги до продуктивності та наявних ресурсів комп'ютерної платформи, на якій реалізовано МЕ;
3. висока вартість;
4. відсутність прозорості для користувачів;
5. зниження пропускної здатності мережі під час передавання трафіку через МЕ.

Особливості персональних брандмауерів

Серед програмних МЕ виокремлюють клас так званих персональних брандмауерів. Такі програми встановлюють на кінцевих вузлах мережі (найчастіше — на робочих станціях користувачів); вони контролюють лише трафік, адресований конкретному комп'ютеру.

У загальному випадку персональні брандмауери контролюють вхідний і вихідний трафіки. Оскільки такий брандмауер вбудовано в ланцюг драйверів, що працюють із мережним адаптером, він здатен перехоплювати весь трафік, що обробляється стандартним стеком протоколів у системі, і може здійснювати контроль на всіх рівнях взаємодії.

Перевагою персонального брандмауера є його інтеграція з ОС комп'ютера, що дає змогу визначати, від яких прикладних програм надходять запити на встановлення з'єднань із віддаленими вузлами і яким прикладним програмам адресовані пакети, що надходять із мережі. Таким чином легко реалізувати контроль не лише на рівні мережних, транспортних (IP-адреси, номери портів) і прикладних протоколів (скажімо, FTP, HTTP), а й на рівні прикладних програм. Наприклад, можна визначити таке: запит на встановлення з'єднання за протоколом HTTP надходить від браузера, якому таку діяльність дозволено, чи від іншої програми (на кшталт медіа-плеєра), рішення про дозвіл щодо якої слід приймати окремо.

Типові можливості персонального брандмауера:

- встановлення правил фільтрації пакетів за мережними адресами, протоколами і номерами портів;

- встановлення правил для прикладних програм, які можуть повністю дозволяти або забороняти взаємодію конкретної програми з мережею, а можуть вводити конкретні обмеження (конкретні дозволи) на окремі мережні адреси, протоколи, номери портів тощо;
- виявлення типових атак за параметрами отриманих пакетів або характеристиками трафіку (наприклад, пакети зі спеціальними комбінаціями прапорців і параметрів заголовків або сканування портів);
- реєстрація подій, пов'язаних із мережною взаємодією, а саме вхідних і вихідних пакетів (наприклад, спроба атаки або встановлення з'єднання за ініціативою певної програми);
- реакція на виявлені атаки, яка може бути пасивною (реєстрація події, сигнал тривоги) чи активною (блокування вузла, з якого розпочато атаку);
- інтелектуальний дружній до користувача режим встановлення правил, коли за умовчанням усе заборонено; за наявності будь-якої активності користувача буде поінформовано щодо події та запропоновано дозволити її одноразово чи заборонити, дозволити перманентно чи заборонити або ж відредагувати правило щодо цієї події; в подальшому така процедура виконуватиметься лише для тих події, для яких ще не було створено відповідних правил.

Отже, персональний брандмауер здатний виявляти атаки. Його інколи використовують для перевірки цілісності програм, що працюють із мережею. Наприклад, після встановлення нової версії браузера під час першої спроби виходу в Інтернет персональний брандмауер заблокує роботу браузера, допоки користувач не підтвердить, що знає про заміну програми і так само їй довіряє. За допомогою персональних брандмауерів можна також здійснювати антиспамову фільтрацію.

Персональні брандмауери мають свої недоліки, іноді зовсім несподівані. Наприклад, деякі персональні брандмауери не розрізняють мережні інтерфейси, тобто застосовують одні й ті самі правила до них усіх. У типових портативних комп'ютерах (ноутбуках) такими інтерфейсами є: вбудований інтерфейс Ethernet 10/100, вбудований модем, FireWire, безпроводовий інтерфейс. Додатково може бути встановлено різні USB-інтерфейси (наприклад, безпосередній зв'язок з іншим комп'ютером або кабельний модем). Очевидно, що методи застосування таких інтерфейсів різні, а тому потрібно, щоб до них застосовували такі правила фільтрації, які б враховували особливості цих інтерфейсів.

Ще один недолік персональних брандмауерів — специфічна політика безпеки, яку вони реалізують. Наприклад, вбудований брандмауер Windows досить коректно захищає комп'ютер від усіх вхідних з'єднань, але жодним чином не забороняє будь-які вихідні з'єднання. Відтак, застосовуючи брандмауер Windows, неможливо проконтролювати доступ встановлених на комп'ютері прикладних програм до інтернету, що фактично означає наявність можливості витоку конфіденційної інформації.

На комп'ютері, що має безпосередній вихід в Інтернет, обов'язково слід встановлювати персональний брандмауер як необхідний захід захисту.

Недоліки міжмережного екрана

Хоча міжмережні екрани — ефективний засіб захисту мереж, вони мають свої недоліки і не можуть гарантувати безпеку мережі без застосування додаткових інструментів і організаційних заходів. Зазвичай зловмисники намагаються обійти МЕ. Розглянемо типові способи обходу та недоліки політики безпеки, що роблять такий обхід можливим.

Однією з найтиповіших ситуацій є проникнення в захищену мережу через не- контрольований МЕ канал. Звісно, у правильно спроектований ІКС таких каналів не мало б бути, але, на жаль, це не так. Найпоширенішою причиною утворення такого неконтрольованого каналу є використання модемів. Адміністратори систем не завжди можуть відстежити, скільки модемів установлено і для чого їх використовують. Користувачі, порушуючи політику безпеки, встановлюють модеми для доступу до робочих каталогів із дому або для несанкціонованого виходу в Інтернет, Найважче здійснювати контроль, коли як модеми використовують мобільні телефони. Через такі канали в захищену мережу

можуть потрапляти віруси та «троянські коні». Якщо модем встановлено стаціонарно, безпосередня атака через нього буде цілком імовірною.

Ще один варіант — атака зсередини захищеної мережі. Для її здійснення зловмисники можуть вербувати легальних користувачів або певним чином додавати «своїх» людей до їх числа. Іноді довірливих користувачів вводять в оману, зокрема провокуючи їх на дії, що, зрештою, призводять до порушення політики безпеки. Для цього користувачам передають програми, які містять віруси або приховані функції («троянських коней»). У результаті атаку буде здійснено всередині мережі (тоді її трафік узагалі не буде проходити через МЕ) або ініціатором з'єднання з комп'ютером зловмисника вважатиметься комп'ютер із захищеної мережі (і таке з'єднання не буде заборонено).

Якщо навіть зловмисник змушений діяти через МЕ, у нього залишається достатньо можливостей. МЕ майже завжди дозволяє обмін за протоколом SMTP (електронна пошта) і дуже часто — за протоколами HTTP (Веб). Якщо МЕ є пакетним фільтром, він не контролюватиме вміст пакетів. Кваліфіковані зловмисники можуть здійснювати атаки, створюючи тунель у рамках дозволеного протоколу. Найпростіший приклад використання тунелів — мережні хробаки та віруси, які потрапляють у корпоративну мережу як вкладення в повідомлення електронної пошти. Ще один приклад — атака Loki (яку було розглянуто в розділі 16), що дає змогу тунелювати різні команди (наприклад, запити на передавання файлів) у запити ICMP Echo Request і реакцію на них у відповіді ICMP Echo Reply.

Таким чином, у захисті мережі не слід покладатися тільки на МЕ. Лише комплексні заходи і поєднання різних засобів можуть надати певні гарантії захищеності мережі.

3. Системи виявлення атак.

Система виявлення атак, СВА (Intrusion Detection System, IDS) — це програмна або програмно-апаратна система, яка автоматизує процес аналізу подій в інформаційно-комунікаційній системі, що впливають на її безпеку. У наш час СВА вважають необхідним елементом інфраструктури безпеки.

Технологія виявлення атак базується на трьох складових [18]:

- ознаках, що описують порушення політики безпеки;
- джерелах, в яких шукають ознаки порушень політики безпеки;
- методах аналізу інформації, яку отримують із різних джерел.

Окрім того, що СВА виявляють атаки (реальні або потенційно можливі), ці системи можуть певним чином реагувати на них — надавати найпростіші звіти або, визначивши проникнення, навіть активно втручатися.

3.1. Можливості систем виявлення атак

Системи виявлення атак надають такі можливості захисту мереж.

- Реагування на атаку (якщо система зафіксувала такий факт і джерело атаки), що змушує атакуючого відповідати за свою діяльність.
- Блокування джерела атаки з метою перешкоджання її здійсненню. Найбільш ефективним є блокування атак у випадках, коли в системі є вже відомі, але ще не виправлені вразливості. Причини виникнення такої ситуації добре відомі:
  - у деяких системах не можуть бути виконані всі необхідні оновлення й модифікації;
  - адміністратори іноді не мають достатньо часу або ресурсів для відстеження й встановлення всіх необхідних оновлень, передусім у середовищах, що містять велику кількість хостів із різною апаратурою та програмним забезпеченням;
  - користувачі застосовують мережні сервіси і протоколи, які мають відомі вразливості;

♦ користувачі та адміністратори роблять помилки під час конфігурування й використання систем.

Виявлення підготовки атаки, яка полягає у здійсненні зондування мережі чи будь-якому іншому тестуванні задля пошуку вразливостей. За наявності СВА сканування буде виявлено і доступ зловмисника до системи може бути заблокований. Навіть наявність простої реакції на зондування мережі вказуватиме атакуючому про підвищений рівень ризику і може змусити його відмовитися від подальших спроб проникнення в мережу.

Отримання інформації щодо проникнень, які мали місце. Надана СВА інформація може бути корисною для відновлення й коригування факторів, що сприяли компрометації системи. Навіть коли СВА не має можливості блокувати атаку, вона може збирати про неї детальну і вірогідну інформацію, яку буде покладено в основу відповідних правових і адміністративних заходів.

Визначення джерела атак. СВА дає змогу з'ясувати, як стосовно локальної мережі розташовано джерело атак (зовнішні або внутрішні атаки), що важливо під час прийняття рішень із розташування ресурсів у мережі.

Різні типи систем виявлення атак

Є кілька способів класифікації СВА, що спираються на різні характеристики.

На якому етапі здійснення атаки її було зафіксовано. Типовим для СВА є виявлення атак у реальному часі, тобто в момент їх здійснення. Такі системи виявлення атак є класичними. Є також системи, які аналізують журнали реєстрацій і таким чином виявляють здійснені атаки. Іноді до СВА відносять засоби, які аналізують системи та попереджають про потенційну можливість здійснення атаки. До таких засобів належать сканери вразливостей.

Інформаційні джерела. Це одна з найголовніших характеристик СВА. За інформаційними джерелами розрізняють СВА рівня мережі (Network Based IDS) та СВА рівня вузлів (Host Based IDS). Останні, у свою чергу, поділяють на СВА рівня ОС, СВА рівня СКБД та СВА рівня прикладних програм.

Метод аналізу. Аналіз даних про події, отримані з джерела інформації, і прийняття рішення щодо того, чи відбувається атака, здійснюють за допомогою методу виявлення зловживань (Misuse Detection) або методу виявлення аномалій (Anomaly Detection).

Швидкість реакції, або затримка в часі між отриманням інформації із джерела та її аналізом і реакцією на неї. Залежно від затримки в часі розрізняють СВА пакетного режиму (Interval Based IDS) і СВА реального часу (Real Time IDS). У СВА пакетного режиму інформаційний потік від точок моніторингу до інструментів аналізу не є безперервним. Багато ранніх СВА рівня вузлів використовували таку схему роботи, оскільки були цілком залежними від накопичення записів аудита в ОС. СВА пакетного режиму не виконують жодних активних дій у відповідь на виявлені атаки.

СВА реального часу обробляють безперервний потік інформації від джерел. Така схема роботи характерна для систем виявлення атак рівня мережі, які отримують інформацію з потоку мережного трафіку. СВА реального часу виявляють проникнення досить швидко, що дає їм можливість в автоматичному режимі виконувати певні дії у відповідь.

Характер відповіді. Дії, які система виконує після виявлення проникнень, зазвичай поділяють на активні й пасивні заходи. Під активними заходами розуміють автоматичне втручання в деяку іншу систему (наприклад, керування комутатором або мережним екраном), а пасивні заходи — це звіт СВА, який користувачі можуть застосовувати для виконання певних дій.

Архітектура СВА. Архітектура СВА визначає, які функціональні компоненти СВА наявні та як вони взаємодіють один з одним. Основними архітектурними компонентами є система, на якій виконується ПЗ СВА (Host), і система, за якою СВА спостерігає (Target). Раніше СВА реалізовували переважно на тих системах, які вони захищали. Так робили через те, що більшість систем були великими комп'ютерами (класу mainframe) і вартість виконання СВА на кожному комп'ютері була

дуже високою. Але це створювало проблему безпеки, оскільки будь-який зловмисник, що успішно атакував цільову систему, міг заборонити функціонування СВА. З появою робочих станцій і персональних комп'ютерів у більшості архітектур СВА почали передбачати виконання СВА на окремій системі, розділяючи таким чином системи Host і Target. Це поліпшило безпеку функціонування СВА.

Сучасні системи виявлення атак, як правило, складаються з таких компонентів:

- сенсора, що відстежує події в мережі або системі;
- аналізатора виявлених сенсорами подій;
- компоненти ухвалення рішення.

Способи керування. Стратегія керування визначає, яким чином можна керувати елементами СВА, їхніми вхідними та вихідними даними. Розрізняють централізоване, частково розподілене та повністю розподілене керування. За централізованого керування весь моніторинг, виявлення й звітність здійснюються з одного «поста». Для цього застосовують єдину консоль IDS, зв'язану з усіма розташованими в мережі сенсорами. У разі частково розподіленого керування моніторинг і виявлення здійснюються з локального вузла, а ієрархічна звітність спрямовується в одне (чи більше) центральне місце розташування.

За повністю розподіленого керування моніторинг і виявлення виконуються з використанням підходу, заснованого на агентах, коли рішення про відповідь приймаються в точках аналізу.

На рис. 1 показано приклад класифікації систем виявлення атак, яку наведено у .

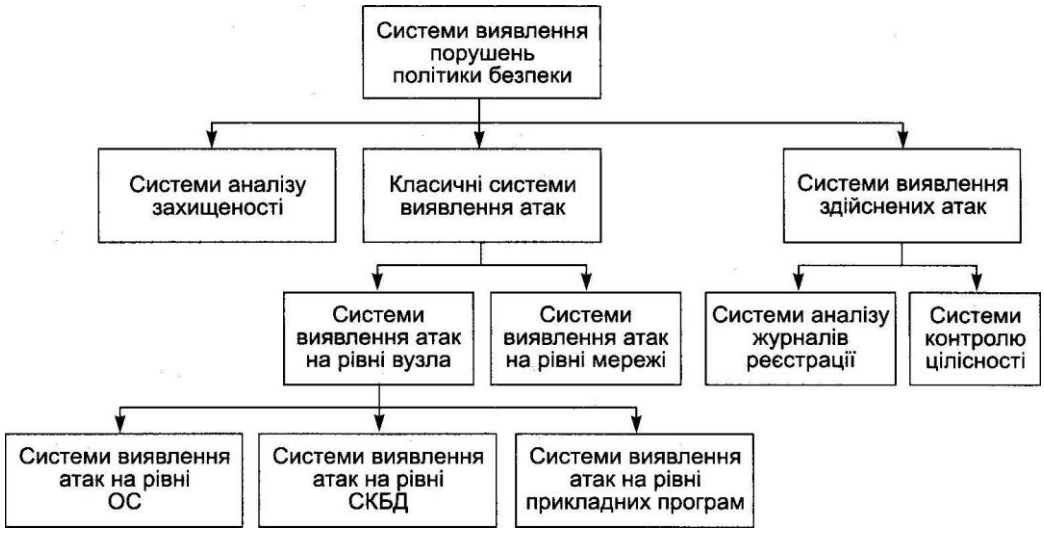


Рис. **1.** Узагальнена класифікація систем виявлення атак

Інформаційні джерела

За загальною класифікацією системи виявлення атак групують за джерелами інформації. Деякі СВА аналізують насамперед пакети даних, захоплені ними з мережі. Інші для виявлення ознак проникнення аналізують джерела інформації, створені ПЗ окремого вузла (ОС, СКБД або прикладними програмами).

СВА рівня мережі

Системи виявлення атак рівня мережі є найпоширенішими. До них належить переважна більшість комерційних СВА. Вони виявляють атаки, захоплюючи й аналізуючи мережні пакети. У сучасних системах часто використовують множину сенсорів, розташованих у різних точках мережі. Ці пристрої переглядають мереж- ний трафік, виконуючи його локальний аналіз та створюючи звіти про атаки для центральної керуючої консолі.

СВА рівня мережі має низку переваг. Кілька оптимально розташованих СВА можуть переглядати велику мережу. Розгортання СВА рівня мережі сильно не впливає на продуктивність мережі. Сенсори, як правило, є пасивними пристроями, які прослуховують мережний канал, не

перешкоджаючи нормальному функціонуванню мережі. СВА рівня мережі може зробити її практично не вразливою до атак або навіть абсолютно не видимою для атакуючих.

СВА рівня мережі має й свої недоліки. Хоча СВА, захопивши трафік, не гальмує роботу самої мережі, вона може не встигати обробляти всі пакети у великій або зайнятій мережі, а відтак у разі підвищеного навантаження в мережі може пропустити атаку (не виявити її). Деякі виробники намагаються вирішити проблему, повністю реалізуючи СВА апаратно, що робить таку систему більш швидкою. Потреба у швидкому аналізі пакетів також може призвести до того, що розробники СВА обмежуватимуть її можливості виявленням невеликої кількості атак або ж використовуватимуть якнайменші обчислювальні ресурси, що знижуватиме ефективність виявлення.

СВА рівня мережі не можуть аналізувати зашифровану інформацію. Ця проблема стає актуальною під час використання віртуальних приватних мереж

Більшість СВА рівня мережі не здатні зробити висновок про те, чи була атака успішною; вони лише можуть визначити, що атаку було розпочато. Це означає, що після виявлення атаки адміністратору доведеться вручну досліджувати кожний атакований хост, щоб з'ясувати, чи відбулося реальне проникнення.

СВА рівня вузла

Системи виявлення атак рівня вузла мають справу з інформацією, зібраною всередині одного комп'ютера. Це дає змогу СВА рівня вузла аналізувати діяльність із великою вірогідністю й точністю, визначаючи лише ті процеси й користувачів, що якимось чином стосуються конкретної атаки. На відміну від СВА рівня мережі, СВА рівня вузла можуть «бачити» наслідки розпочатої атаки, тому що мають доступ до інформації, файлів даних і процесів системи, які є ціллю атаки.

СВА рівня вузла звичайно використовують як інформаційні джерела журнали реєстрації подій, що створюються ОС та прикладними програмами. Деякі СВА рівня вузла розроблені для підтримки централізованої інфраструктури керування й отримання звітів СВА, що може допускати єдину консоль керування для відстеження багатьох хостів.

Системи виявлення атак рівня вузла мають низку переваг.

Маючи змогу стежити за подіями локально, виявляють атаки, які не можуть виявити СВА рівня мережі. Можуть функціонувати в середовищі із зашифрованим мережним трафіком, якщо джерела інформації рівня вузла було створено до шифрування даних або після їх розшифровування на хості призначення. На функціонування СВА рівня вузла не впливає топологія мережі.

Системи виявлення атак рівня вузла мають не лише переваги, а й недоліки.

Оскільки принаймні джерела інформації системи виявлення атак рівня вузла (а іноді й деякі засоби аналізу) розташовані на хості, що піддається атаці, то під час атаки цю систему може бути атаковано й вимкнено.

СВА рівня вузла не завжди може виявити сканування мережі чи інші впливи, метою яких є вся мережа, оскільки СВА спостерігає лише за мережними пакетами, які отримує конкретний хост.

СВА рівня вузла можуть бути блоковані деякими DoS-атаками. СВА рівня вузла використовує результати аудита ОС як джерело інформації; об'єм інформації може бути величезним, а це потребуватиме додаткових ресурсів для її зберігання в системі.

СВА рівня вузла використовують обчислювальні ресурси хостів, за якими вони спостерігають, що впливає на продуктивність їхніх систем.

СВА рівня прикладних програм

Система виявлення атак рівня прикладних програм (Application Based IDS) — специфічний різновид СВА рівня вузла, що аналізує події, пов'язані з конкретним прикладним ПЗ. Найзагальнішими джерелами інформації, що використовують такі СВА, є журнали реєстрації прикладного ПЗ.

Здатність взаємодіяти безпосередньо з прикладною програмою або використовувати дані, специфічні для певної прикладної програми, дає змогу СВА рівня прикладних програм виявляти таку

поведінку авторизованих користувачів, що перевищує їхні повноваження. Такі порушення можна виявити, лише аналізуючи взаємодії користувача з прикладною програмою.

Наведемо переваги систем виявлення атак рівня прикладних програм.

СВА рівня прикладних програм можуть аналізувати взаємодію між користувачем і програмою, що дає їм змогу відстежувати неавторизовану діяльність конкретного користувача.

Ці системи, як правило, можуть працювати у зашифрованих оточеннях, тому що вони отримують інформацію у кінцевій точці транзакції, де інформацію подано вже в незашифрованому вигляді.

Системи виявлення атак рівня прикладних програм мають кілька недоліків. Вони більш уразливі до атак на записи реєстрації подій, ніж СВА рівня ОС, оскільки журнали реєстрації прикладного ПЗ захищені менш надійно, ніж результати аудита ОС. Ці системи часто не здатні виявити «троянських коней» або інші атаки, пов'язані з порушенням цілісності ПЗ.

Можна зробити висновок, що СВА рівня прикладних програм доцільно використовувати разом із СВА рівня ОС і (або) СВА рівня мережі.

4. Системи аналізу та оцінювання вразливостей.

Інструментальні засоби аналізу вразливостей (ЗАВ), відомі також як *сканери безпеки*, тестують мережу або хост для виявлення вразливостей до відомих атак. Аналіз уразливостей надає додаткову інформацію для систем виявлення проникнень. ЗАВ виявляють такі вразливості та вади захисту:

- «люки» у програмах і програми типу «троянський кінь»;
- слабкі паролі й неправильні настроювання механізмів автентифікації;
- сприйнятливість до проникнення внаслідок неявних довірчих відносин між системами;
- сприйнятливість до атак на відмову в обслуговуванні;
- неправильні настроювання міжмережних екранів, мережних і прикладних сервісів;
- нездатність засобів захисту системи адекватно реагувати на спроби збирання інформації.

Загальний процес оцінювання вразливостей складається з таких етапів:

- визначення множини атрибутів системи як шаблону;
- збереження шаблону в безпечному сховищі даних (множину атрибутів шаблону можна визначити вручну та зберегти як зразок «ідеальної конфігурації» або зробити моментальний знімок стану системи);
- визначення поточних значень атрибутів і порівняння їх із шаблоном;
- виявлення розбіжностей між шаблоном і поточними значеннями та створення звіту.

Класифікація інструментальних засобів аналізу вразливостей

ЗАВ можуть здійснювати сканування системи ззовні, використовуючи для доступу до системи мережні засоби, і зсередини, працюючи безпосередньо на хості, який вони аналізують. Як правило, мережні сканери також здатні здійснювати сканування локальної системи через зворотний інтерфейс (127.0.0.1).

Аналіз уразливостей на рівні вузла

Засоби аналізу вразливостей на рівні вузла, або локальні ЗАВ (Host-Based), виявляють уразливість, аналізуючи доступні джерела системних даних (наприклад, уміст файлів, параметри конфігурації та інші дані про статус). Така інформація звичайно доступна у разі використання стандартних системних запитів і перевірки системних атрибутів. Об'єм отриманої інформації залежить від того, з якими правами ЗАВ має доступ до хоста. Найкращого результату досягають локальні ЗАВ, які мають повноваження root в UNIX-системі або повноваження адміністратора у Windows-системі.

Аналіз уразливостей на рівні мережі

Мережні ЗАВ (Network Based) останнім часом дістали значне поширення. Такі системи потребують встановлення віддаленого з'єднання із системою, яку досліджують. Вони можуть реально

проводити атаки на систему, розуміти й записувати відповіді на ці атаки або тестувати різні цілі для пошуку слабких місць. Таке проведення атак або тестування може відбуватися як за наявності дозволу на доступ до цільової системи, так і без нього.

Мережні ЗАВ виявляють уразливості у два способи: скануванням і зондуванням. *Сканування* (Banner Check) — механізм пасивного аналізу, коли сканер намагається виявити вразливість за непрямими ознаками без фактичного підтвердження її наявності. Цей метод є найшвидшим і найпростішим для реалізації. Процес сканування ідентифікує відкриті порти, виявлені на кожному мережному пристрої, і збирає заголовки (Banner), отримані під час сканування портів. Аналіз заголовків дає змогу ідентифікувати ОС і активні сервіси з визначенням конкретної версії.

На підставі апріорних знань про наявність уразливостей в тій чи іншій версії ПЗ робиться висновок щодо наявності чи відсутності вразливості в системі, що аналізується.

Зондування (Active Check) — механізм активного аналізу, який дає змогу пересвідчитися в наявності вразливості на вузлі, що аналізується.

Зондування виконується шляхом імітування атаки, що використовує вразливість, яку перевіряють. Цей метод повільніший, ніж сканування, але майже завжди більш точний. Процес зондування використовує інформацію, отриману під час сканування, для детального аналізу кожного мережного пристрою.

Наприклад, під час сканування можна отримати відомості про відкриті TCP- порти 135, 139. Це ознака того, що в мережі використовується служба NetBIOS. Майже напевно в системі, яку сканують, встановлено ОС Windows. Сканування дає змогу визначити версію ОС і встановлені пакети оновлень (Service Pack). Далі логічною є взаємодія з системою за протоколом NetBIOS для вивчення наявності загальнодоступних ресурсів (Shared), захищеності цих ресурсів паролем. Можна також отримати відомості про користувачів системи, можливість її адміністрування через мережу тощо. Ці дані дають детальну й достатньо достовірну картину щодо наявності вразливостей.

Під час зондування інколи використовують відомі методи реалізації атак задля остаточного підтвердження або спростування наявності вразливостей, виявлених скануванням, а також знайти інші вразливості, які не можна виявити з використанням пасивних методів, такі як нестійкість до атак типу відмова в обслуговуванні (DoS-атак).

Відмінності технологій аналізу вразливостей і виявлення атак

Аналіз уразливостей — дуже потужна технологія керування безпекою, але вона є лише доповненням до системи виявлення атак і не може замінити її. ЗАВ створюють моментальний знімок стану безпеки системи в конкретний момент часу. Більше того, оскільки ці засоби є виключно тестовими системами пошуку вразливостей для великої кількості відомих атак, вони дають змогу адміністратору контролювати деякі помилки користувачів або виконувати аудит системи, щоб з’ясувати чи відповідає п стан політиці безпеки.

Засоби аналізу вразливостей аналогічні системам виявлення проникнень, оскільки так само стежать за конкретними симптомами проникнення й іншими порушеннями політики безпеки. Однак ЗАВ застосовують статичний погляд на такі симптоми, а СВА досліджують їх динамічно.

Переваги та недоліки систем аналізу вразливості

Системи аналізу вразливостей мають низку переваг.

- Аналіз уразливостей відіграє важливу роль у системі моніторингу безпеки, надаючи можливість виявляти проблеми в системі, які не може визначити ЗВА.
- ЗАВ дають змогу задокументувати стан систем у певний момент часу для подальшого здійснення контролю змінень.
- Якщо ЗАВ використовувати регулярно, вони можуть із високою надійністю виявляти змінення в стані безпеки системи, сповіщаючи адміністраторів про проблеми, які потребують вирішення.

Системи аналізу вразливостей мають також свої недоліки.

- Аналізатори вразливостей рівня вузлів сильно пов'язані з конкретними ОС і прикладним ПЗ, вони дорожчі та складніші в розгортанні, супроводженні й керуванні.
- Мережні аналізатори вразливостей менш точні й створюють більше фіктивних тривог.
- Деякі мережні перевірки в режимі зондування, переважно ті, що стосуються DoS-атак, можуть зашкодити системі, яку вони тестують.
- Є проблеми з виконанням оцінювання вразливостей у мережах, де працюють СВА. З одного боку, діючі СВА, виявивши сканування, можуть заблокувати подальше здійснення оцінювання, а з іншого боку, такі регулярні мережні сканування і зондування можуть «навчити» СВА, засновані на виявленні аномалій, ігнорувати реальні атаки.

Приклади мережних ЗАВ

Одним із перших мережних ЗАВ був засіб System Administrator Tool for Analysis of the Network (SATAN). Коли він з'явився на ринку (перша половина 90-х років минулого століття), ситуація з безпекою в Інтернеті була просто катастрофічна (достатньо пригадати успішне розповсюдження хробака Morpica). Тому поява SATAN — засобу, доступного для використання всіма зацікавленими, — викликала величезний розголос.

ЗАВ мають комерційні та безкоштовні версії. Один із найвідоміших комерційних сканерів — Internet Scanner, продукт компанії Internet Security Systems. Його перевага полягає в тісній інтеграції з мережною СВА тієї самої фірми.

З некомерційних сканерів слід відзначити сканер Nessus, який складається з ядра, що працює під керуванням UNIX, і клієнтської частини, яка може бути різною для різних систем. Ядро здійснює сканування, використовуючи базу даних уразливостей. Клієнтська частина реалізує інтерфейс користувача. Сканер розповсюджується безкоштовно з відкритим кодом (хоча останнім часом з'явилася також його комерційна версія).

Дуже великого поширення набула програма російських розробників XSpider (компанія Positive Technologies), яку спочатку розповсюджували безкоштовно. Хоча бази даних цієї програми були розраховані на пошук уразливостей переважно в операційних системах Windows (для інших платформ програма також надавала певний обсяг інформації, проте менш детальної і точної), вона мала зручний інтерфейс, надавала детальні звіти, а під час імітування атак ефективно використовувала вразливості, зокрема добирала слабкі паролі. Успіх програми дав змогу розробникам перевести її на комерційну основу (остання безкоштовна версія датована груднем 2002 року). Для перевірки власної мережі можна використовувати демоверсію XSpider (вона не здійснює DoS-атак і не формує звіти).

Також слід враховувати, що для платформи Windows є безкоштовний сканер безпеки Microsoft Baseline Security Analyzer. Його застосування вимагає повноважень адміністратора, і хоча ніхто не знає вади Windows краще за розробників цієї системи з корпорації Майкрософт, деякі слабкі місця політики безпеки ОС цей сканер не помічає через те, що розробники не вважають їх уразливостями. З іншого боку, цей продукт дуже зручний для оцінювання поточного стану системи, особливо стосовно встановлення необхідних оновлень і виправлень.