УДК 004.056.53

Приходько Т.О.

Донецький національний технічний університет, Донецьк

ПРОБЛЕМИ БЕЗПЕКИ ЛОКАЛЬНИХ МЕРЕЖ НА КАНАЛЬНОМУ ТА МЕРЕЖНОМУ РІВНЯХ МОДЕЛІ OSI

Розглянуто проблеми пов'язані з безпекою мереж на канальному та мережному рівнях моделі OSI. Ппроаналізовано різні типи атак на локальні комп'ютерні мережі, а також сучасні методи їх виявлення та попередження. Запропоновано найбільш перспективні напрямки розвитку систем виявлення вторгнень.

Ключові слова: аналіз мережного трафіку, системи виявлення вторгнень (СВВ) - IDS (Intrusion Detection System), протоколи канального рівня, прослуховування (sniffing), комутовані мережі, стек TCP/IP, Denial of Service – відмова в обслуговуванні

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ЛОКАЛЬНЫХ СЕТЕЙ НА КАНАЛЬНОМ И СЕТЕВОМ УРОВНЯХ МОДЕЛИ OSI

Рассмотрены проблемы связанные с безопасностью сетей на канальном и сетевом уровнях модели OSI. Ппроанализовано различные типы атак на локальные компьютерные сети, а также современные методы их выявления и предупреждения. Предложено наиболее перспективные направления развития систем обнаружения вторжений.

SECURITY ISSUES LAN ON CHANNEL AND NETWORK LAYER OF THE OSI MODEL

The problems associated with network security at the data link and network layer model OSI. Pproanalizovano different types of attacks on LANs as well as modern methods of detection and prevention. A most promising areas of intrusion detection system.

Постановка проблеми

Уразливість локальних мереж великою мірою заснована на широкому використанні мереж, побудованих на принципі розподіленого середовища передачі даних. Для організації атак на канальному і мережному рівнях OSI цілком достатньо гарного знання стека протоколів TCP/IP та принципів роботи комутаторів і маршрутизаторів.

Небезпека уразливості протоколів канального рівня OSI полягає в тому, що, зламавши мережу на канальному рівні, атакуючий може переступити через засоби захисту на вищих рівнях, тому атаки на мережному рівні їм компліментарні.

Типи атак на канальному та мережному рівнях локальних обчислювальних мереж

Є різні типи класифікації атак, але ми розглянемо тільки віддалені (Network Based) атаки з точки зору їх активності [1;2;3]: пасивні чи активні

А) Пасивні:

- Підслуховування (sniffing) і аналіз мережного трафіку [1;2;3], використовують недоліки в протоколах і мережному устаткуванні. За допомогою сніфера можна отримати корисну, а інколи і конфіденційну інформацію (наприклад, імена користувачів і паролі).

Приклади: Атаки на STP — відправка повідомлень BPDU для зміни поточної топології

STP. VLAN hopping — несанкціоноване здобуття доступу до VLAN;

- Підміна довіреного суб'єкта. Велика частина мереж і операційних систем (ОС) використовують IP-адресу комп'ютера, для того, щоб визначати, чи той це адресат, який потрібний. В деяких випадках можливе некоректне привласнення IP (або MAC) - адреси або підміна цих адрес відправника іншою адресою. Такий спосіб атаки називають фальсифікацією адреси (IP (MAC) - spoofing). Як варіант - ARP-spoofing (ARP-poisoning).

В) Активні:

- Відмова в обслуговуванні (Denial of Service, DOS). Цей тип атак не націлений на діставання доступу до мережі або на здобуття з цієї мережі якої-небудь інформації. Атака DOS робить мережу організації недоступною для звичайного використання за рахунок перевищення допустимих меж функціонування якого-небудь ресурсу мережі, ОС або застосування. Вона паралізує роботу мережі і позбавляє звичайних користувачів доступу до загальних ресурсів організації. При цьому використовуються протоколи TCP і ICMP. Найбільш відомі: TCP SYN Flood; Ping of Death.
- Порушення роботи мережі або її ділянок — деякі недоліки протоколів канального рівню не можуть використовуватися передбаченим чином. Тобто, не можна навмисно вплинути на їх поведінку, але є можливість порушити їх нормальну роботу і таким чином розхитати відмовостійкість ділянки мережі або всієї мережі. Приклад: Переповнення таблиці комутації.

Хотілося б звернути увагу на уразливості протоколу STP. Spanning Tree Protocol – протокол другого рівня моделі OSI. Основним його завданням є приведення комутованої мережі Ethernet з резервними зв'язками до деревоподібної топології, що виключає циклічні зв'язки шляхом автоматичного блокування надлишкових на даний момент зв'язків з утворенням покриваючого дерева (ненадлишкового графа).

Найцікавіше і найбільш глибоке дослідження стандартів [4] було проведене авторами [5], що призвело до виявлення величезного набору вразливостей даного протоколу:

1. Перша заснована на відсутності механізмів аутентифікації STP, що дозволяє без зусиль організувати атаку проти мережі на базі комутаторів.

2. Крім того, це протокол без встановлення з'єднання і без фільтрації помилкових пакетів, що підсилює його уразливість. Особливості алгоритму STP дозволяють ініціювати постійну переконфігурацію STP-дерева з подальшим частковим DOS, серед яких можливі: STP DOS: "вічні вибори" кореневого комутатора, DOS: алгоритм "зникнення кореня" і др [5];

3. Ще один вигляд можливої атаки - Провокаційний сниффинг - це атака, направлена на переклад комутатора в режим концентратора шляхом переповнювання його динамічної таблиці адрес, або використання ситуації її обнулення в разі зміни STP-дерева з метою подальшого підслуховування трафіку.

Методи виявлення мережних атак

Переважно сучасні системи виявлення вторгнень (СВВ) працюють із протоколами канального, мережного та транспортного рівней. Механізми, використовувані в СВВ здебільшого засновані на декількох загальних методах, які не є взаємовиключними. У багатьох системах використовуються їх комбінації. Ці механізми включають:

- методи аналізу мережної інформації і зокрема статистичний метод, який має на увазі, що спочатку для всіх суб'єктів аналізованої системи визначаються профілі. Будь-яке відхилення використовуваного профілю від еталонного вважається несанкціонованою діяльністю;
- експертні системи, зокрема методи штучного інтелекту.

Тенденції розвитку СВВ

Як і прогнозували аналітики кілька років тому [6] розвиток СВВ йде **по шляху комбінування:**

1.Технологій виявлення аномальної активності і виявлення зловмисної поведінки:

Перші – здатні виявляти нові типи атак, сигнатури для яких ще не розроблені, не потребують оновлення сигнатур і правил виявлення атак, генерують інформацію, яка може бути використана в системах виявлення зловмисної поведінки, але при цьому вимагають тривалого і якісного навчання, - генерують багато помилок другого роду (виявлення аномальної поведінки, яка не є атакою, і віднесення її до класу атак), дуже повільні в роботі і вимагають великої кількості обчислювальних ресурсів.

Другі – компенсують недоліки перших тим, що не створюють у процесі пошуку величезної кількості помилкових повідомлень і детектори зловживань можуть швидко і надійно діагностувати використання конкретного інструментального засобу або технології атаки, але при цьому працюють на базі лише відомих конкретних сигнатур.

2. Способів моніторингу:

Є видимою тенденція злиття network-based (NIDS), host-based (HIDS) і application-based (AIDS) способів моніторингу, що спричиняє за собою розподілене розташування сенсорів стеження: "В області розгортання ми бачитимемо розширення числа місць виявлення атак: на мережному рівні (на міжмережних екранах, на комутаторах, на маршрутизаторах), на рівні операційної системи (на серверах, на робочих станціях) і на прикладному рівні (у СУБД або на сервері SAP, наприклад)." [1].

Завдяки централізації інформації про атаку від різних складових IDS (центральний аналізуючий сервер, агенти мережі, мережні сенсори) така система максимально підсилює захищеність корпоративної підмережі.

На жаль, деякі переваги network-based IDS непридатні до сучасних комутованих мереж в тому випадку, якщо комутатори мережі не надають універсального моніторингу портів - це обмежує діапазон моніторингу сенсора network-based IDS лише одним хостом. Крім того, network-based IDS самі можуть стати предметом атаки DOS, заснованої, наприклад, на сегментації пакетів. Ще один недолік - network-based IDS не можуть аналізувати зашифровану інформацію. Зате host-based системи можуть компенсувати вищеназвані недоліки, оскільки справляються з проблемою шифрування, на них не впливає наявність комутаторів, проте при цьому вони обмежені ресурсами ОС і використовують частину обчислювальної потужності хостів, за якими вони спостерігають, що впливає на продуктивність спостережуваної системи.

3. Принципів сигналізуючих і експертних систем виявлення атак.

Найбільш поширеним підходом є використання засобів штучного інтелекту (тобто різних адаптивних методів) в комбінації з класичними статичними методами. Найчастіше використовуються нейронні мережі, які добре проявили себе в системах розпізнавання. Рідше - молодші методи теорії імунних систем, можливо в комбінації з нечіткою логікою (НЛ), генетичними алгоритмами, методами нечіткого багатокритеріального ухвалення рішень і чисельними методами оптимізації [7].

Вживання адаптивних методів обумовлене необхідністю налаштування на свій індивідуальний специфічний набір параметрів для кожної системи, що захищається. Поєднання нейронних мереж і інформаційних систем НЛ з одного боку забезпечують можливість навчання, а з іншого - процес вирішення завдань НЛ системами досить прозорий для пояснення отримуваних виводів [7].

4. Програмного і апаратного рівнів забезпечення захисту інформації.

Мережні сенсори, про які вище йшла мова, найчастіше реалізуються апаратно-програмними пристроями відомих фірм – виробників (Cisco). У мережних комутаторах Cisco як сенсор використовується технологія – SPAN - Switch Port Analyzer і RSPAN - Remote Switch Port Analyzer. Вона дозволяє "зеркалювати" трафік з одного порту, на інший, або наприклад з VLAN вказаного, на порт, де знаходиться аналізатор трафіку, або якесь ПО. Ця технологія дозволяє здолати обмеження комутованих мереж для network-based IDS, про які згадувалося вище.

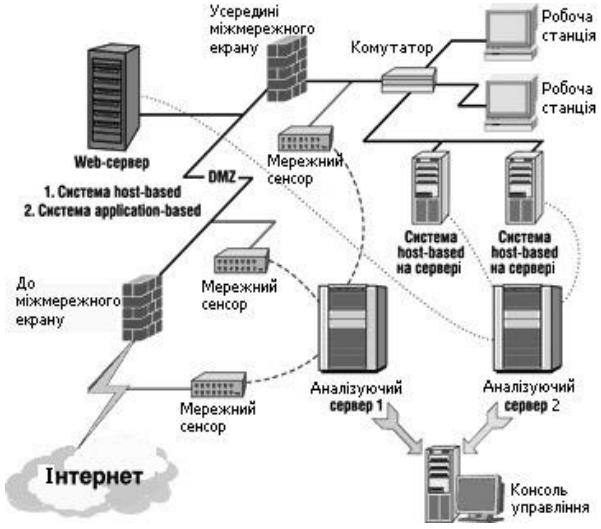

Рисунок. Розподілене розташування сенсорів стеження в IDPS і host-based агентах.

Висновок

Типова архітектура СОА, як правило, включає такі функціональні компоненти (рисунок):

- сенсор (засіб збору інформації – мережний датчик і хостовий агент). Реалізується програмними, апаратними або комбінованими засобами;
- аналізатори (засоби аналізу інформації) - сигнатурні, інтелектуальні, а частіше комбіновані;
- засоби реагування;
- засоби управління.

Взаємне розташування і функціональні зв'язки між цими компонентами інтуїтивно зрозумілі. Найуразливішими для різносторонньої критики компонентами є перші два, тому вони ж є найцікавішими і перспективнішими для вивчення і вдосконалення.

Ще один перспективний напрям досліджень розвивається в працях [7; 8] і пов'язаний з тестуванням якості СОА. Перспективи пов'язані з тим що на думку авторів, до цих пір не існувало стандартизованої методики тестування СОА, що дозволяє виявити всі достоїнства і недоліки тестованої системи виявлення атак.

Список літератури

1. Біячуєв Т.А. Безпека корпоративних мереж. / під ред. Л.Г.Осовецкого – СПб: СПб ГУ ІТМО, 2004.- 161 с.

2. Аграновский А.В, Хади Р.А."Системы обнаружения компьютерных угроз" http://www.nestor.minsk.by/sr/ 2008/05/ sr80513.html

3. Анализ угроз сетевой безопасности http://ypn.ru/138/analysis-of-threats-to-network-security/

4. MEDIA ACCESS CONTROL (MAC) BRIDGES ANSI/IEEE Std 802.1D, 1998 Edition

5. Артемьев О.К. Мяснянкин В.В. Введение в недокументированное применение протокола Spanning Tree.

6. "Експерти дискутують про сьогодення і майбутнє систем виявлення атак" Річард Пауер, переклад Олексія Лукацкого. Опубліковано: 21.11.02 Computer Security Journal vol. XIV, #1 2. Лапоніна О.Р . Intrusion Detection Systems (IDS). 2006г. Електронний ресурс. Сторінка доступу: http://citforum.ru/security/internet/firewalls_ids/2.shtml

7. Абрамов Е.С. Построение адаптивной системы информационной безопасности // «Известия ЮФУ. Технические науки». Тематический выпуск «Информационная безопасность». - Таганрог: Изд-во ТТИ ЮФУ, 2011. - №12 (125). - С. 99-109.

8. Половко И.Ю. Методы тестирования эффективности сетевых СОА // «Известия ЮФУ. Технические науки». Тематический выпуск «Информационная безопасность». - Таганрог: Изд-во ТТИ ЮФУ, 2009. - №11 (100). - С. 110-116.

Стаття надійшла до редколегії 23.05.2012

Рецензент: д-р техн.наук, проф. В.А. Святний, Донецький Національний технічний університет, Донецьк.