Classification of network threats

Igor Ruban[1], Prybylnov Dmitry[2]

Mathmatics and programming provision of automatic control systems department, Kharkov air force university, UKRAINE, Kharkov, Sumska street 77/79,
E-mail: [1]ruban_i@ukr.net; [2]kamun1st@mail.ru

The article deals with the classification of network threats for intrusion detection and warning facilities. With the purpose of comprehensive examination of the set task and conduction of the analysis on the information security and network threats problematics, an attempt to introduce the detailed classification of network threats is made, what, by turn, allows to develop appropriate computer system security facilities. This is going to favour the formulating of the task on specified countermeasures apparatus formation against all types of threats with the assigned guarantee in terms of defined network segment. Basic approaches to the classification of network intrusions are studied and fundamental types of threats are exemplified in the main body. In a course of the analysis conducted it becomes obviously seen that there is a full-scale system of classifications and different approaches to them. The classification, that is the object of examination of the present article, will facilitate into the comparison of principle types of intrusions by a formal matter. At a later stage it will assist in the definition of information influence model, aiming at the development of intrusion detection and warning methods and algorithms. At this, it should be emphasized that existing countermeasures are to reveal reliable performance only with known types of intrusions, and incapable in reference to unknown, i.e. those ones which can not be clearly classified due to their absolute novelty. The conduction of comprehensive classification by a formal matter allows to develop “genetic” algorthms of intrusins detection, which are based on the apparatus of neural networks and fuzzy-set theory.

Класифікація мережевих загроз

Ігор Рубан[1], Дмитро Прибильнов[2]

[1]Кафедра математичного та програмного забезпечення АСУ, Харківський університет Повітряних Сил, УКРАЇНА, м.Харків, вул.Сумська 77/79,
E-mail: [1]ruban_i@ukr.net; [2]kamun1st@mail.ru

В статті розглятнута та наведена класифікація мережевих загроз для засобів виявлення вторгнення та засобів попередження вторгнення. З метою постановки завдання на всебічне вивчення та проведення аналізу проблематики інформаційної безпеки та мережевих загроз, робиться спроба приведення всебічної класифікації мережевих загроз, що, у свою чергу, надає можливість побудови засобів захисту від небезпеки у компютерній мережі. Це дозволить зформулювати завдання на побудову певного апарату протидії всім видам небезпеки із заданою гарантією у межах визначеного сегменту мережі.

Ключові слова: ***класифікація мережевих загроз, мережева загроза, комп’ютерна безпека, засоби виявлення вторгнення, засоби попередження вторгнення.***

I. Вступ

Сучасний період розвитку цивілізованого суспільства по праву називають етапом інформатизації. Сучасне матеріальне виробництво та інші сфери діяльності все більше потребують інформаційного обслуговування, переробки величезної кількості інформації. Універсальним технічним засобом обробки будь-якої інформації є комп'ютер, який грає роль підсилювача інтелектуальних можливостей людини і суспільства в цілому, а комунікаційні засоби, що використовують комп'ютери, служать для зв'язку і передачі інформації. Поява і розвиток комп'ютерів - це необхідна складова процесу інформатизації суспільства. [1]. У свою чергу бурхливий розвиток комп’ютерної техніки та мережевих технологій призводять до автоматизації виробництва та обліку документів. Створення глобальних баз даних скорочує час на отримання відповідей на запити з будь-яких питань. Саме це породжує необхідність захисту інформації від стороннього як редагування, так і від володіння доступом до неї. Цінність інформації породжує лавину тих, хто охоче використає інформацію із обмеженим доступом у власних цілях з метою збагачення. Але не лише сама інформація виступає кінцевою ціллю. Визначення точної класифікації мережевих загроз надасть можливість точно визначити повний спектр необхідних заходів для забезпечення надійної та стабільної роботи мережі, що у свою чергу надасть можливість гарантувати збереження як інформації, так і її грифу конфіденційності, тобто не розголошення. За даними Computer Emergency Response Team (CERT) кількість випадків несанкціонованого доступу до комп’ютерних мереж та до кінцевих робочих станцій абонентів з кожним

роком збільшується в логарифмічній залежності Рис.1 [2].

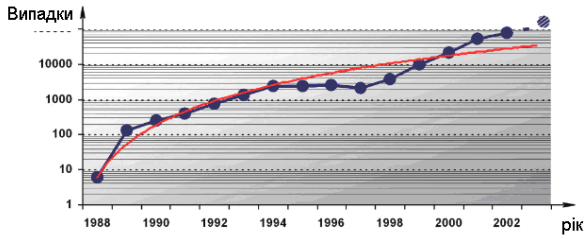

Рис.1 Зростання числа випадків несанкціонованого використання мережевих ресурсів.

Число випадків зростає, але у той же час проблематика попередження вторгнень та збереження цілісності інформації залишається на високому рівні необхідності. Даній тематиці присвячені публікації [3-7]. Це лише невелика кількість робіт, що призначені для нотатків системному адміністратору у налагодженні мережевої безпеки. У кожній з робіт автори намагалися дати практичні поради щодо захисту мережі від стороннього доступу, але лише у публікації [8] було наведено конкретний приклад із реалізованою системою виявлення атак, у побудову якої було покладено ґрунтовний аналіз класифікації усіх видів загроз. Тобто, виходячи із необхідності налагодження мережевої безпеки, постає необхідність у класифікації мережевих загроз з метою розроблення методів їх попередження та виявлення.

II. Основна частина

Мережеві атаки також різноманітні, як і системи, проти яких вони направлені. Деякі атаки відрізняються великою складністю, інші під силу звичайному оператору, що навіть не передбачає, до яких наслідків може навести його діяльність. Для оцінки типів атак необхідно знати деякі обмеження, спочатку властиві протоколу TPC/IP. Мережа Інтернет створювалася для зв'язку між державними установами і університетами з метою надання допомги учбовому процесу і науковим дослідженням. Творці цієї мережі не підозрювали, наскільки широке розповсюдження вона отримає. В результаті в специфікаціях ранніх версій Інтернет-протоколу (IP) були відсутні вимоги безпеки. Саме тому багато реалізацій IP є уразливими. Через багато років, після множини рекламацій (Request for Comments, RFC), стали упроваджуватися засоби безпеки для IP. Проте з огляду на те, що спочатку засоби захисту для протоколу IP не розроблялися, всі його реалізації стали доповнюватися різноманітними мережевими процедурами, послугами і продуктами, що знижують ризики, властиві цьому протоколу.

Отже, розглянемо класифікацію мережевих загроз.

1. За характером впливу мережеві атаки поділяються на:
   - Пасивні
   - Активні

Пасивна дія на розподілену обчислювальну систему - дія, яка не робить безпосереднього впливу на роботу системи, але може порушувати її політику безпеки. Пасивний видалений вплив практично неможливо детектувати.

Активна дія на розподілену обчислювальну систему - дія, що робить безпосередній вплив на роботу системи (зміна конфігурації, порушення працездатності і т. д.) і порушуючи встановлену у ній політику безпеки.

Практично всі типи видалених атак є активними. Особливістю активної атаки у порівнянні з пасивною є принципова можливість її виявлення, оскільки в результаті здійснення в системі відбуваються певні зміни. На відміну від активного впливу, при пасивному не залишається ніяких слідів.

2. З метою впливу:
   - порушенні конфіденційності інформації;
   - порушення цілісності інформації;
   - порушення працездатності (доступності) системи.

При перехваті інформації порушується її конфіденційність. При викривленні – її цілісність. При порушенні працездатності не відбувається несанкціонований доступ, тобто зберігається цілісність і конфіденційність інформації, проте доступ до неї легальних користувачів також неможливий.

3. За умовами початку здійснення впливу
   - атака по запиту об’єкта, що атакується;
   - атака по настанню події, яка очікувалася на об’єкті, який атакується;
   - безумовна атака.

У разі запиту атакуючий чекає передачі від потенційної цілі атаки запиту певного типу, який і буде умовою почала здійснення дій. Ініціатором здійснення початку атаки є об'єкт, що атакується.

Наприклад, DNS- і ARP-запити у стеку TCP/IP.

У разі настання події, атакуючий здійснює постійне спостереження за станом операційної системи видаленої цілі атаки і при виникненні певної події в цій системі починає дію.

Ініціатором здійснення почала атаки є об'єкт, що атакується.

Наприклад, переривання сеансу роботи користувача з сервером в сітьових ОС без видачі команди LOGOUT.

У разі безумовної атаки початок її здійснення безумовно по відношенню до цілі атаки, тобто атака здійснюється негайно і безвідносно до стану системи і об'єкта, що атакується. Отже, в цьому випадку атакуючий є ініціатором почала здійснення атаки.

4. За наявності зворотного зв’язку з тим, хто атакується:
   - зі зворотнім зв’язком;
   - без зворотного зв’язку (однонаправлений вплив).

Атака без зворотного зв'язку – атака, коли не враховується реакція та поведінка системи, що атакується.

5. За знаходженням атакуючого відносно об'єкта, що атакується.
   - сегментна атака;
   - між сегментна атака.

6. За кількістю тих, хто атакує:
   - розподілена атака;
   - не розподілена.

7. За рівнем еталонної моделі OSI
   - фізичний;
   - канальний;
   - мережевий;
   - транспортний;
   - сеансовий;
   - представницький;
   - прикладний.

Вище перераховані типи класифікації виконують покладені на них функції лише з точки зору деталізації по тих або інших критеріях, але часто виділяють окремі класи, що мають мінімальне значення з точки зору систем виявлення атак. Тому найперспективнішою представляється вже описана в літературі наступна класифікація, що розділяє атаки на класи, в яких їх буде легше виявити і класифікувати[9]:

1. Видалене проникнення (remote penetration). Атаки, які дозволяють реалізувати видалене управління комп'ютером через мережу. Прикладами програм, що реалізують таке управління, є, NetBus або Back Orifice, реверсивний сеанс telnet

2. Локальне проникнення (local penetration). Атака, що приводить до отримання несанкціонованого доступу до вузла, на якому вона була запущена, або підвищення прав користувача. Прикладом такої програми є GetAdmin або реалізація експлойта для уразливості в ядрах Linux через ptrace.

3. Видалена відмова в обслуговуванні (remote DoS (denial of service)). Атаки, які дозволяють порушити функціонування системи або перезавантажити видалений комп'ютер. Прикладами такої атаки є teardrop, trinoo, fapi.

4. Локальна відмова в обслуговуванні (local DoS). Атаки, що дозволяють порушити функціонування системи або перезавантажити комп'ютер, на якому вони реалізуються. Як приклад такої атаки можна навести ворожий апплет, який завантажує центральний процесор нескінченним циклом, що приводить до неможливості обробки запитів інших додатків. Також, у разі неправильної настройки, це може бути додаток, що відгалужується, з купою нащадків, що займають всі вільні ідентифікатори PID.

5. Мережеві сканери (network scanners). Програми, які аналізують топологію мережі і виявляють сервіси, доступні для атаки. Прикладом такої програми може служити nmap.

6. Сканери слабких місць (vulnerability scanners). Програми, що здійснюють пошук вразливостей на вузлах мережі і які можуть бути використані для реалізації атак. Приклади: система SATAN або Shadow Security Scanner, XSpider, LanGuard, XFocus-X-Scan і ін.

7. Зломщики паролів (password crackers). Програми, які підбирають паролі користувачів. Прикладом зломщика паролів може служити L0pht Crack для Windows або Crack для *nix.

8. Аналізатори протоколів і сніфери (sniffers). Програми, які «прослуховують» сітьовий трафик. За допомогою цих програм можна автоматично шукати таку інформацію, як ідентифікатори і паролі користувачів, інформацію про кредитні карти і так далі. Фактично аналізатор протоколу - це сніфер плюс деяка частина, що здійснює фільтрацію і розбір перехоплених пакетів за деякими правилами. Часто обидві задачі виконує один і той же продукт. Прикладами таких програм можуть служити tcpdump, ethereal, Microsoft Network Monitor, NetXRay компанії Network Associates, Lan Explorer.[10]

Також необхідно розглянути список усіх найбільш відомих мережевих атак різного рівня. Атаки розбиті на 4 класи, виходячи з виду тієї загрози, яку вони представляють[12] :
   - відмова в обслуговуванні,
   - спроба несанкціонованого доступу,
   - попереднє зондування,
   - підозріла мережева активність

Відмова в обслуговуванні (denial of service) - це будь-яка дія або послідовність дій, яка приводить будь-яку частину системи, що атакується, до виходу з ладу, при якому система перестає виконувати свої функції. Причиною може бути несанкціонований доступ, затримка в обслуговуванні і так далі.

Спроба несанкціонованого доступу до даних (unauthorized access attempt) є будь-якою дією або послідовністю дій, яка призводить до спроби читання файлів або виконання команд в обхід встановленої політики безпеки. Також включає спроби зловмисника отримати привілеї, більші, ніж встановлені адміністратором системи.

Попереднє зондування (pre - attack probe) - будь-яка дія або послідовність дій з отримання інформації мережі або про неї (наприклад, імена і паролі користувачів) для здійснення неавторизованого доступу.

Попереднє зондування (pre - attack probe) - будь-яка дія або послідовність дій з отримання інформації мережі або про неї (наприклад, імена і паролі користувачів) для здійснення неавторизованого доступу.

"Підозріла" мережева активність (suspicious activity) представляє клас атак, характерною особливістю яких є наявність мережевого трафіку, що виходить за рамки визначення "стандартного" трафіку. Подібна активність може вказувати на підозрілі дії, здійснювані в мережі.

Інший підхід був застосований в класифікації, що була використана у програмному продукті Nessus, який був призначений для аналізу безпеки серверів. Тут використовується класифікація "по характеру

слабкого місця" для реалізації атаки. Уразливі місця за типом програмного середовища підрозділяються на уразливості в операційній системі, уразливості в певному сервісі і уразливості в певному програмному забезпеченні. Уразливості в конкретних сервісах і в певному програмному забезпеченні класифікуються по групах.

У цій класифікації детальніше, у порівнянні з попередніми, опрацьовано атаки, що використовують уразливості в системному, прикладному і мережевому програмному забезпеченні. Проте ця класифікація не охоплює усіх існуючих мережевих атак. За межами розгляду залишаються такі небезпечні атаки, як "відмова в обслуговуванні", перехоплення даних і атаки, спрямовані на мережеве устаткування. Позитивною рисою цієї класифікації є наявність класу "Інші помилки, що не увійшли до жодної з категорій", оскільки формально до будь-якої атаки, у тому числі нової, завдяки цьому класу буде застосовна дана класифікація.

Не зважаючи на досить чітку визначеність між всіма видами мережевих атак, віднести однозначно той чи інший випадок до певного класу не можливо тому, що атака у більшості випадків – це комплекс заходів. Саме через це кожна велика корпорація віддає перевагу власній класифікації мережевих загроз. Так, наприклад, компанія Internet Security Systems, Inc. [11] ще більше скоротила число можливих категоріїв, лишивши лише п’ять:

- збір інформації (Information gathering);
- спроби несанкціонованого доступу (Unauthorized access attempts);
- відмова в обслуговуванні (Denial of service);
- підозріла активність (Suspicious activity);
- системні атаки (System attack).

Перші чотири категорії відносяться до видалених атак, а остання - швидше до локальних, оскільки видалена реалізація системних атак практично неможлива. Також в цю класифікацію не попали деякі атаки, наприклад «хибний DNS-сервер» або «заміна ARP-сервера».

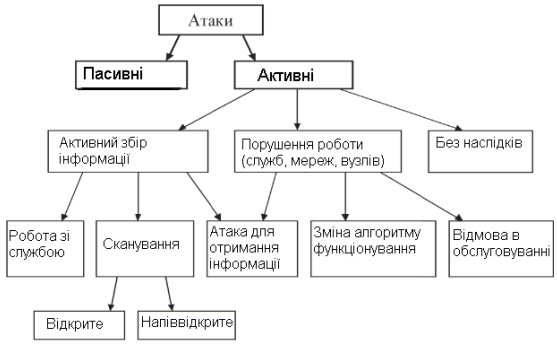

Рис. 2 Узагальнена класифікація мережевих атак.

Виходячи із вище приведеного, можливо скласти наступну класифікацію мережевих атак, яка представлена на рис. 2

Висновок

Класифікація, що була розглянута в межах даної статті, надасть можливість порівняти всі основні види атак за формальною ознакою. У подальшому це дозволить побудувати модель інформаційного впливу на систему, що має на меті розробку методів та алгоритмів виявлення та протидії атакам. При цьому необхідно зауважити, що існуючі методи протидії стабільно працюють лише над виявленням відомих типів атак, але у той же час є недієздатними по відношенню до невідомих, тобто тих, які не можливо чітко класифікувати, через те, що вони є абсолютно новими. Після проведення повної класифікації за формальними ознаками виникає можливість розробки «генетичних» алгоритмів виявлення атак, що ґрунтуються на апараті нейронних мереж та теорії нечітких множин.

Література

[1] Болотов Е., Шумаєв В. Проблеми інформатизації // Економіст, 2001, № 2

[2] Статистика CERT http://www.cert.org/stats/cert_stats.html

[3] С.Яремчук. L.I.D.S. //Системный администратор, №4(5), 2003.

[4] В.Мешков. Система крипрографической защиты информации //Системный администратор, №4(5), 2003.

[5] С.Яремчук. Контрольная сумма на защите Linux/FreeBSD // Системный администратор, №6(7), 2003.

[6] А.Даниленко. Технологии протоколирования Honeypot в обеспечении безопасности сетевых Unix-систем // Системный администратор, №5(6), 2003

[7] Лукацкий А.В., Обнаружение атак. - СПб: БХВ-Петер-бург, 2001. – 624 с.

[8] Сайт системы обнаружения атак IDS «Snort» http://www.snort.org/

[9] Мак-Клар, Стюарт, Скембрей, Джоел, Курц, Джордж. Секреты хакеров. Безопасность сетей - готовые решения, 2-е изд.: Пер. с англ. - М.: Издательский дом «Вильямс», 2001.

[10] П.Н.Девянин, О.О.Михальский, Д.И.Правиков, А.Ю.Щербаков. Теоретические основы компьютерной безопасности: Учеб. пособие для вузов. - М: Радио и связь, 2000.

[11] Сайт компании Internet Security Systems, Inc. http://www.iss.net/

[12] Мак-Клар, Стюарт. Секреты хакеров. Безопасность сетей - готовые решения, 2-е изд.: Пер. с англ. – М.: Издательский дом «Вильямс», 2001..