Methods for detecting remote attacks on the Internet

Yuriy Kostiv[1], Myroslav Mykytyuk[2]

[1]Information Security Technologies Department,
Lviv Polytechnic National University,
UKRAINE, Lviv, 12, S. Bandery street,
E-mail: yura.kostiv@gmail.com

[2]Information Security Department,
Lviv Polytechnic National University,
UKRAINE, Lviv, 12, S. Bandery street,
E-mail: myroslav10@ukr.net

The objective of the research is in-depth detection analysis of remote attacks on the Internet. This paper examines the main ways to detect attacks which increase the risk of the system affection through a network. The basic concepts and types of attacks and information through the network are examined and the basic methods and measures to detect remote attacks are proposed.

Attack on a computer system - an act that is done by an attacker who is searching for a vulnerability in order to use it. Researchers usually distinguish three main types of security threats - a threat of disclosure, integrity, and denial of service.

The threat of disclosure is that information becomes known to people who should not know it. In terms of computer security risk of disclosure occurs whenever somebody got access to some confidential information stored in computer system, or transmitted from one system to another. Sometimes instead of the word "disclosure" the terms "theft" or "leakage" can be used.

The threat to the integrity includes any deliberate change (modification or even delete) of the data stored in computer system, or transmitted from one system to another. Usually it is believed that state structures are more likely to the threat of disclosure, and business structures – to the threat of integrity.

The threat of denial of service occurs each time, when as a result of some action the access is blocked to some resource of computer system. Real block may be permanent, in order that the requested resource will never be received, or it may cause only delay of the requested invited resource, it is sufficiently long so that it became useless.

Keywords – attack, attack detection, information security.

Переклад виконано Малиновською О. А., центр іноземних мов «Universal Talk», www.utalk.com.ua

Методи виявлення віддалених атак в мережі Internet

Юрій Костів[1], Мирослав Микитюк[2]

[1]Кафедра безпеки інформаційних технологій,
Національний університет "Львівська політехніка",
УКРАЇНА, м.Львів, вул.С.Бандери, 12,
E-mail: yura.kostiv@gmail.com

[2]Кафедра захисту інформації,
Національний університет "Львівська політехніка",
УКРАЇНА, м. Львів, вул. С. Бандери, 12,
E-mail: myroslav10@ukr.net

В статті здійснюється аналіз основних методів виявлення віддалених атак, та порівняння основних принципів роботи цих методів для оцінки ефективності їх використання.

Ключові слова – атака, виявлення атак, захист інформації.

I. Вступ

Підключення організації до корпоративної мережі, вимагає створення системи захисту інформаційних ресурсів, від тих, хто схоче їх використовувати, модифікувати або просто знищити. Не дивлячись на свою специфіку, система захисту організації при роботі в Корпоративних мережах повинна бути продовженням загального комплексу зусиль, направлених на забезпечення безпеки інформаційних ресурсів.

Для забезпечення збереження інформації в корпоративних мережах широко використовують технологію RAID-масивів. Ця технологія забезпечує збереження існуючої та відновлення втраченої інформації [1].

Також, однією з проблем є забезпечення захисту корпоративної мережі від віддалених атак на мережеву систему, які також направлені на заподіяння шкоди інформації яка циркулює в мережі.

Історично так склалося, що технологія, по яких будуються системи виявлення атак, прийнято умовно ділити на дві категорії: виявлення аномальної поведінки (anomaly detection) і виявлення зловживань (misuse detection). Проте в практичній діяльності застосовується інша класифікація, що враховує принципи практичної реалізації таких систем: виявлення атак на рівні мережі (network-based) і на рівні хоста (host-based). Перші системи аналізують мережевий трафік, тоді як другі реєстраційні журнали операційної системи або додатку. Існує два класи систем, що виявляють атаки на мережевому і операційному рівні. Системи виявлення атак (Intrusion Detection Systems, IDS) використовують для розпізнавання і віддзеркалення атак або мережевий, або системний підхід. У будь-якому випадку ці продукти шукають сигнатури атак, специфічні шаблони, які зазвичай указують на ворожі або підозрілі дії. У разі пошуку цих шаблонів в мережевому трафіку, IDS працює на мережевому

рівні. Якщо IDS шукає сигнатури атак в журналах реєстрації операційної системи або додатку, то це системний рівень [2].

II. Виявлення атак на мережевому рівні

Системи виявлення атак мережевого рівня використовують як джерело даних для аналізу необроблені (raw) мережеві пакети. Як правило, IDS мережевого рівня використовують мережевий що функціонує в режимі "прослуховування " (promiscuous), і аналізують трафік в реальному масштабі часу у міру його проходження через сегмент мережі. Модуль розпізнавання атак використовує чотири широко відомі методи для розпізнавання сигнатури атаки:

- Відповідність трафіку шаблону (сигнатурі), виразу або байткоду, що

характеризують про атаку або підозрі лу дію;

- Контроль частоти подій або перевищення порогової величини;
- Кореляція декількох подій з низьким пріоритетом;
- Виявлення статистичних аномалій.

Як тільки атака виявлена, модуль реагування надає широкий набір варіантів повідомлення, видачі сигналу тривоги і реалізації контрзаходів у відповідь на атаку. Ці варіанти змінюються від системи до системи, але, як правило, включають: повідомлення адміністратора через консоль або по електронній пошті, завершення з'єднання з атакуючим вузлом або запис сесії для подальшого аналізу і збору доказів [3,4].

III. Виявлення атак на системному рівні

На початку 80-х років, ще до того, як мережі отримали свій розвиток, найбільш поширена практика виявлення атак полягала в прогляданні журналів реєстрації на предмет наявності в них подій, що свідчать про підозрілу активність. Сучасні системи виявлення атак системного рівня залишаються могутнім інструментом для розуміння вже здійснених атак і визначення відповідних методів для усунення можливостей Їх майбутнього застосування. Сучасні IDS системного рівня як і раніше використовують журнали реєстрації, але вони стали більш автоматизованими і включають складні методи виявлення, засновані на новітніх дослідженнях в області математики. Як правило, IDS системного рівня контролюють систему, події і журнали реєстрації подій безпеки (security log або syslog) в мережах, що працюють під управлінням Windows XP або Unix. Коли який-небудь з цих файлів змінюється, IDS порівнює нові записи з сигнатурами атак, щоб перевірити, чи є відповідність. Якщо така відповідність знайдена, то система посилає адміністраторові сигнал тривоги або приводить в дію інші задані механізми реагування [5,6].

IDS системного рівня постійно розвиваються, поступово включаючи все нові і нові методи виявлення. Один Їх таких популярних методів полягає в перевірці контрольних сум ключових системних і виконуваних файлів через регулярні інтервали часу на предмет несанкціонованих змін. Своєчасність реагування безпосередньо пов'язана з частотою опиту. Деякі продукти прослуховують активні порти і повідомляють адміністратора, коли хтось намагається дістати до них доступ. Такий тип виявлення вносить до операційного середовища елементарний рівень виявлення атак на мережевому рівні

IV. Висновок

Як ми бачимо, кожен підхід має свої і недоліки, але вони обидва доповнюють один одного. Найбільш ефективною є система виявлення атак, яка використовує в своїй роботі обидві технології.

У даному матеріалі обговорюються відмінності в методах виявлення атак на мережевому і системному рівнях з метою демонстрації їх слабких і сильних сторін. Також описуються варіанти застосування кожного із способів для найбільш ефективного виявлення атак.

Наступне покоління IDS, таким чином, повинне включати інтегровані системні і мережеві компоненти. Оскільки одні події виявляються тільки за допомогою мережевих систем. Інші - тільки за допомогою системних. Деякі вимагають застосування обох типів виявлення атак для надійного виявлення.

Комбінування цих двох технологій значно поліпшить опір мережі до атак і зловживань, дозволить посилити політику безпеки і внести велику гнучкість до процесу експлуатації мережевих ресурсів.

Література

[1] Микитюк М.Я. Використання технології RAID для забезпечення живучості корпоративних мереж зв’язку / Збірник тез доповідей IV міжнародної конференції CSE-2010 Львів: Видавництво НУ «Львівська політехніка»

[2] Домарев – Безопасность информационных технологий. Методология создания систем защиты

[3] Романцев Ю.В., Тимофеєв П.А., Шаньгин В.Ф. – Защита информации в компьютерных системах и сетях, Москва – 2001р.

[4] Шаньгин В.Ф. – Защита компьютерной информации, Москва – 2008р.

[5] Гарасим Ю. Р. IDS – технологія захищених корпоративних мереж зв’язку / Ю. Р. Гарасим, В. Б. Дудикевич // Науковий журнал «Інформаційна безпека». – 2009. – №1 (1). – С. 58-62.

[6] Гарасим Ю. IDS – технологія захищених корпоративних мереж зв’язку. Оптимізація вибору номенклатури / Ю. Гарасим // Збірник тез доповідей 67-ої студентської науково-технічної конференції. – Львів : Видавництво НУ «Львівська політехніка», 2010. – С. 173-174.