УДК 004

А.З.Піскозуб
Національний університет «Львівська політехніка»

ДО ПИТАННЯ ПІДВИЩЕННЯ РІВНЯ ЗАХИЩЕНОСТІ КОМП'ЮТЕРНИХ МЕРЕЖ ТА СИСТЕМ

The problems of different kinds of software security instruments, such as IDS, vulnerability assessment and penetration testing tools, log auditing and analysis tools are been discussed in this paper. The trend toward establishing minimum required level of security has affected many security safeguards and thus determined the integrated approach of mentioned above tools.

Keywords: information security, vulnerability assessment, penetration testing, log auditing, SIEM, ISO 27001

В даній статті обговорюються проблеми різних інструментів підвищення рівня захищеності комп'ютерних мереж та систем: систем виявлення втручань сканерів вразливостей, системи тестування на проникнення та системи журналізації подій. Тенденція на встановлення мінімального рівня захищеності ІТ-середовища фактично визначила необхідність комплексного підходу – використання широкого спектру програмних засобів для підвищення рівня захищеності комп'ютерних мереж та систем.

Ключові слова: захист інформації, сканування вразливостей, тестування на проникнення, журналізація подій, SIEM, ISO 27001

Вступ

Питання підвищення рівня захищеності ІТ-середовища є на сьогодні актуальним не лише для великих корпорацій, але і для невеликих організацій, як для потреб бізнесу, так і для навчальних установ.

Як правило, такі питання вимагають інвестування певної суми коштів на організацію програмно-апаратних засобів підвищення рівня захищеності ІТ-середовища, причому левова частка тих коштів виділяється на закупівлю ліцензій відповідних програмних продуктів. І якщо раніше організації часто використовували піратське програмне забезпечення (ПЗ), то зараз на фоні загального підвищення рівня легального використання ліцензійного ПЗ чимала вартість таких програмних засобів є стримуючим фактором для багатьох організацій у їх використанні. В результаті захищеність даних та інфраструктури таких організацій залишається під питанням.

Тому сьогодні для виконання даної задачі можна і потрібно використовувати вільне та відкрите ПЗ (ВВПЗ). Мета даної статті – показати шляхи підвищення рівня захищеності комп'ютерних систем та мереж та навести приклад практичної реалізації таких кроків на базі використання ВВПЗ.

Сучасний стан використання програмно-апаратних засобів підвищення рівня захищеності ІТ-середовища

Як правило, більшість організацій для підвищення рівня захищеності ІТ-середовища використовують антивірусний захист та захист на рівні використання міжмережевих екранів (firewalls). Подекуди цей список доповнюється використанням рядом організацій засобів виявлення/запобігання втручань (intrusion detection/prevention systems – IDS/IPS), які допомагають в залежності від налаштувань цих засобів оперативно реагувати на події в системах.

Насправді, список інструментів підвищення рівня захищеності комп'ютерних мереж та систем доповнюють сканери вразливостей, системи тестування на проникнення та системи журналізації подій, описи та рекомендації використання яких можна знайти в багатьох відомих

документах, зокрема стандарті як ISO/IEC 27001:2005 [1], що описує методи захисту та системи менеджменту захисту інформації в інформаційних технологіях.

Сканери вразливостей дозволяють сканувати мережі, комп'ютери та програми на предмет виявлення можливих проблем в системі безпеки, оцінювати і рекомендувати усунення вразливостей. Побутує думка, що сканери при виявленні окремих потенційних вразливостей виконують злам системи, використовуючи отриману інформацію та відповідні програми-експлоїти. Насправді на цьому етапі застосовуються інші системи – системи тестування на проникнення, які на базі знайденої сканерами вразливостей інформації моделюють атаки зловмисників, використовуючи при цьому активний аналіз системи на наявність потенційних вразливостей. Ці вразливості, своєю чергою, можуть спровокувати некоректну роботу цільової системи, або повну відмову в обслуговуванні. Аналіз ведеться з позиції потенційного атакуючого і може включати в себе активне використання вразливостей системи. Результатом роботи є звіт, який містить в собі всі знайдені вразливості системи безпеки, а також може містити рекомендації щодо їх усунення. Мета випробувань на проникнення - оцінити його можливість здійснення і спрогнозувати економічні втрати в результаті успішного здійснення атаки. Випробування на проникнення є частиною аудиту безпеки, який повинна пройти кожна компанія, яка має на меті отримати сертифікати відповідності міжнародним стандартам, таким як ISO/IEC 27001:2005.

Журналізація подій - проблеми сьогодення

Доповнюють список інструментальних засобів системи журналізації подій. Роль журналізації подій в комп’ютерних системах не можна недооцінити, оскільки вони є невід’ємною частиною будь-якої системи захисту інформації і дозволяють не лише бути доказом подій, що сталися в системі, але і допомагають підвищити рівень захищеності системи.

Журнали подій містять важливу інформацію, що дозволяє визначити вразливості в системі, зупинити несанкціоноване втручання і визначити місце чи сервіс в системі, які вимагають негайної уваги. В основному, журналізація подій використовується для детектування та аналізу інцидентів, пов’язаних з проблемами безпеки чи продуктивності, для відповідності вимогам політик безпеки, нормативних документів, аудиту чи стандартів, правових питань, а також для мінімізації простоїв.

Питання налаштування журналізації подій залежить від багатьох факторів, які впливають на кількість записуваних даних, їх деталізацію, час їх збереження, ранжування за критичністю подій тощо. Зокрема, зазначимо, що відомий міжнародний стандарт в галузі інформаційної безпеки ISO 27001:2005 [1] – прямий нащадок ISO/IEC 17799:2005 (який, у свою чергу, базувався на Британському стандарті BS 7799), передбачає журналізацію подій в системі, аналіз цих подій та потребу їх збереження. Хоча даний стандарт містить у собі загальні принципи і кращу практику впровадження, забезпечення і оптимізації управління інформаційної безпеки на всіх етапах життєвого циклу інформаційних систем компанії, однак він не надає жодних подальших рекомендацій стосовно того, що повинно зберігатись в журналах подій, як довго ці події повинні зберігатися. В пункті A.10.10.1 стандарту ISO 27001:2005 [1] зазначається лише, що контрольні журнали, що записують діяльність користувачів, винятки та події в системі захисту інформації, повинні генеруватися і зберігатися протягом узгодженого періоду з метою допомогти в майбутніх розслідуваннях та в постійному контролі над управлінням доступом.

Одною з основних проблем на сьогодні є опрацювання даних журналів подій, а особливо в реальному масштабі часу. Аналіз журналів подій по суті зводиться до того, що необхідно якісно виокремити важливе і відкинути непотрібне, а це є насправді важко.

В більшості випадків, IT-персонал звертається до журналів подій тоді, коли щось трапилось. Левова частка підприємств та організацій не здійснює моніторинг систем цілодобово, 7 днів в тиждень, цілий рік. Ця ситуація може бути неприпустимою в системах з підвищеними вимогами до захисту інформації, до систем з високою відмовостійкістю тощо. Хіба що будуть застосовані найсучасніші системи управління інформацією та повідомленнями безпеки (Security Information and Event Management (SIEM)).

У цьому випадку стає можливим централізований онлайн-моніторинг подій з різноманітних джерел – операційних систем, прикладних сервісів, мережевих пристроїв тощо з відображенням в режимі реального часу, кореляція результатів, надання звітів, ранжування за критичністю сервісів, нотифікація/попередження користувачів при настанні певних подій, що дозволяє забезпечити відповідальний персонал та користувачів системи повною інформацією про її стан і, тим самим, забезпечити можливість ефективно управляти ризиками системи. SIEM-системи дозволяють забезпечити інцидент менеджмент подій, пов'язаних з безпекою інформації, з побудовою послідовностей кроків по усуненню цих інцидентів відповідно до попередньо заданих правил.

Рекомендації по використанню SIEM-систем

Організації, які планують проходити аудит на відповідність вимогам стандарту ISO27001:2005, можуть розгортати SIEM-системи чи системи управління журналами подій.

Дослідження показали, що з практичної точки зору SIEM-системи для багатьох організацій служать по принципу: "купляємо для відповідності нормативним вимогам, використовуємо для підвищення рівня захищеності системи" [2].

Однією з найбільших помилок сьогодні при використанні SIEM-систем є думка організацій про те, що, просто володіючи цим інструментом, організація вже має відповідність вимогам стандартів чи вимогам аудиторів. Насправді ті організації, які переслідували мету лише відповідності нормативним вимогам, виявили, що вони не лише не відповідають цим вимогам, але і не є достатньо захищеними при цьому. Ті ж організації, які зосередилися на питанні захищеності із використанням SIEM-систем, виявили, що вони підвищили свій рівень захищеності та відповідають нормативним чинникам.

Ще однією великою помилкою при використанні систем управління журналів подій чи SIEM-систем є думка людей про те, що достатньо лише збирати журнали подій. Нехтується процес обробки даних журналів подій, захист цих журналів, ранжування даних за важливістю, ступінь деталізації подій для різних категорій сервісів, обробка нештатних ситуацій тощо.

Окремо слід звернути увагу на потребу ретельного налаштування SIEM-систем, оскільки в іншому випадку гарантовані так звані "false positive"- та "false negative"-спрацювання і ефективність та адекватність такої системи буде під питанням.

Мінімальна процедура налаштування SIEM-системи передбачає реєстрацію в ній усіх ресурсів, які підлягають аудиту (серверів, робочих станцій, прикладних сервісів, мережевого обладнання тощо), ранжування самих ресурсів, виставлення пріоритету кожному типу подій від окремих ресурсів, виставлення значення надійності тощо. Це дасть змогу провести оцінку ризиків, на основі якої SIEM-система буде генерувати свої звіти.

Згідно принципів найкращих світових практик при використанні SIEM-систем рекомендовано дотримуватися так званих прецедентів чи типових процедур (use cases), що описують послідовність дій взаємодії користувача з системою і забезпечують функціональність системи, необхідну для отримання користувачем вагомого результату.

Приклад реалізації системи захисту IT-середовища із використанням вищезгаданих типів інструментальних засобів підвищення рівня захищеності комп'ютерних мереж та систем на базі ВВПЗ

Кінцева реалізація системи захисту складається з 3 операційних систем (ОС), розгорнутих в віртуальному режимі під управлінням VMWare ESXi 5, розташованих на одному фізичному хості (Intel Core i5, 8GB, 500 Gb HDD):

- системи централізованого збору та обробки інформації журналів подій (ОС Linux CentOS 6.2);
- системи оцінки вразливостей та тестування на проникнення (Back Track 5 на базі ОС Linux Ubuntu 10.04);
- системи управління інформацією та повідомленнями безпеки (OSSIM на базі ОС Linux Debian 6).

Критерії вибору операційних систем виходять за рамки даної статті, проте зазначимо, що вибір ОС CentOS та Debian в даному випадку обґрунтований тим, що вони вважаються одними з найстабільніших серверних Linux-дистрибутивів. Система оцінки вразливостей та тестування на втручання використовується як клієнтська станція без доступу ззовні, тому для цих задач був вибраний спеціалізований Linux-дистрибутив на базі Ubuntu з величезною кількістю програм для оцінки вразливостей та тестування на проникнення.

На системі централізованого збору та обробки інформації журналів подій під управлінням ОС Linux CentOS 6.2 використовуються наступне ВВПЗ: фаєрвол iptables, системи журналізації syslog-подій у складі rsyslogd, loganalyzer, які забезпечують централізований збір інформації з усіх відповідальних вузлів мережі – активного мережевого обладнання та серверів під управлінням ОС Linux та ОС Windows (за допомогою використання програми Snare), системи Sagan – монітору журналів подій реального часу, який інтегрується з IDS-системою виявлення втручань на базі Snort, встановленою на даному хості. Snort забезпечує моніторинг мережі через дзеркалюючий CPAN-порт кореневого комутатора мережі. Окрім цього даний хост відіграє роль центрального сервера часу IT-інфраструктури.

Для оцінки вразливостей систем та тестування на їх проникнення на однойменній системі використовуються наступне ВВПЗ: міжмережевий екран iptables, сніффери tcpdump, wireshark; сканер портів nmap; сканери вразливостей openvas, Nexpose Community edition (окремо відзначимо, що продукт Nexpose компанії Rapid7, freeware-версію якого ми використовуємо, вважається одним з найкращим в своєму класі [3]), веб-сканери w3af, wapiti, nikto, arachni; системи тестування на проникнення Metasloit Framework, Metasploit Community edition.

Сьогодні відомо біля 85 продуктів класу SIEM-систем [4], кожна з яких заслуговує окремого аналізу. Серед списку з 85 позицій лише 8 відносяться до безкоштовних продуктів і лише 2 з них належать до продуктів з відкритим кодом.

Тож, за основу був вибраний продукт AlienVault Open Source SIEM (OSSIM) [5], що являє собою повноцінну безкоштовну відкриту SIEM-систему. Разом з AlienVault Unified SIEM, AlienVault OSSIM використовується в більшій кількості організацій, ніж усі інші SIEM-продукти разом взяті. AlienVault OSSIM забезпечує усю функціональність, яка вимагається для детектування та профілювання атак, і забезпечує всебічну, інтелектуальну платформу управління безпекою з набором відповідних інструментальних засобів.

Висновки

Резюмуючи наведений матеріал, можна відзначити необхідність комплексного підходу – використання широкого спектру програмних засобів для підвищення рівня захищеності комп'ютерних мереж та систем. При цьому є можливо забезпечити ці рішення на базі ВВПЗ. Доцільним є розширення використання SIEM-систем з акцентом на вдосконалення практик реагування на інциденти і перехід на автоматизований моніторинг безпеки в режимі реального часу, не обмежуючись лише питанням відповідності нормативним чинникам з безпеки інформації та діючими типовими процедурами. Такий підхід є єдиним способом отримати реальну картину стану захищеності системи, і, отже, отримати контроль над постійно зростаючим IT-середовищем.

Література

1. ISO/IEC 27001:2005, Information technology — Security techniques — Information security management systems — Requirements. 2. Dr. Anton Chuvakin. A Pragmatic Approach to SIEM: Buy for Compliance, Use for Security. White Paper. // http://www.infosec.co.uk/ExhibitorLibrary/829/Tripwire_Pragmatic_SIEM_WP_20.pdf . 3. Gartner: MarketScope for Vulnerability Assessment 2011. // http://www.gartner.com/technology/media-products/reprints/qualys/article1/article1.html 4. Mosaic Security Research. Log Management & Security Information and Event Management (SIEM). // https://mosaicsecurity.com/categories/85-log-management-security-information-and-event-management . 5. AlienVault Open Source SIEM (OSSIM). // http://www.alienvault.com/ .