Використання ВПЗ для підвищення рівня захищеності комп'ютерних мереж та систем

Піскозуб А.З.

Національний університет «Львівська політехніка», azpiskozub@gmail.com

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. Modern security tools simplify network discovery and vulnerability verification for specific exploits, help organizations improve stability/availability, meet security event management objectives and adhere to demands of regulatory compliance requirements.

Питання підвищення рівня захищеності IT-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 IT-інфраструктури, причому левова частка тих коштів виділяється на закупівлю ліцензій відповідних програмних продуктів. Сьогодні, без сумніву, заслуговує особливої уваги питання використання вільного та відкритого ПЗ (ВВПЗ) для потреб підвищення рівня захищеності комп'ютерних мереж і систем.

Як правило, більшість організацій для підвищення рівня захищеності IT-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 про-

грами-експлоїти. Насправді на цьому етапі застосовуються інші системи – системи тестування на проникнення, які на базі знайденої сканерами інформації моделюють атаки зловмисників, використовуючи при цьому активний аналіз системи на наявність потенційних вразливостей, які, 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.

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.

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. Ніхто, практично, 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 мож-

ливість 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.

Опишемо приклад конкретної реалізації системи захисту IT-інфраструктури 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 втручання (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: фаєрвол 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 [2]), веб-сканери w3af, wapiti,

nikto, arachni; системи тестування на проникнення Metasloit Framework, Metasploit Community edition.

OSSIM (open source SIEM) [3] вибрана з поміж 85 продуктів класу SIEM-систем [4]. Серед списку з 85 позицій лише 8 відносяться до безкоштовних продуктів і лише 2 з них належать до продуктів з відкритим кодом. Вона 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.

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.

Література:

1. *ISO/IEC 27001:2005, Information technology — Security techniques — Information security management systems — Requirements*
2. *Gartner: MarketScope for Vulnerability Assessment 2011. http://www.gartner.com/technology/media-products/reprints/qualys/article1/article1.html*
3. *AlienVault Open Source SIEM (OSSIM). http://www.alienvault.com/ .*
4. *Mosaic Security Research. Log Management & Security Information and Event Management (SIEM). https://mosaicsecurity.com/categories/85-log-management-security-information-and-event-management .*