ШЛЯХИ ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ ПРИ ВИКОРИСТАННІ LINUX-ПОДІБНИХ СЕРВЕРНИХ ОПЕРАЦІЙНИХ СИСТЕМ

Добринін К.І.
Науковий керівник – к.т.н., доц. Добринін І.С.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14, каф. Інфокомунікаційної інженерії,
тел. (057) 702-13-20)
e-mail: kyrylo.dobrynin@nure.ua

The report is devoted to the problem of security of Linux servers when used in the enterprise on the example of a web server or a virtual server. The report shows the main attacks on Linux servers and the main ways to increase security on the server.

На сьогоднішній день значна кількість серверів працюють під операційною системою (ОС) Linux, яка поширюється під вільною і безкоштовною ліцензією. Абсолютна більшість спеціалізованих комп'ютерів, таких як веб-сервер, поштовий сервер, сервер баз даних або файл-сервер, працюють під ОС Linux. Основне завдання сервера полягає у виконанні сервісних функцій за запитом клієнта, надаючи йому доступ до певних ресурсів.

Для коректної роботи серверу актуальним є питання безпеки, тому що ОС Linux і пов'язані з нею сервіси сприйнятливі до спільних загроз, таким як: атака з метою заволодіти чужими даними, виведення серверу з робочого стану, отримання повного доступу до системи, тощо. Тому слід розглянути методи забезпечення безпеки сервера, що має важливе значення для захисту інформації на підприємстві.

У доповіді наведено рекомендації щодо забезпечення інформаційної безпеки і підвищення відмовостійкості Linux-сервера, не залежно від дистрибутива. Для злагодженої і коректної роботи сервера рекомендується подбати про безпеку системи ще на початковій стадії впровадження: встановити пароль на BIOS / UEFI, використовувати шифрування диску, встановлення надійного пароля для root-доступу.

Показано, що для підвищення захищеності системи доцільно виконати наступні рекомендації:

1. Своєчасно виконувати оновлення безпеки, які часто знаходять і виправляють критичні уразливості;
2. Не використовувати root-доступ для виконання неадміністративних команд;
3. Створити користувача з обмеженими правами і делегувати йому права суперкористувача (додаванням в групу sudo) для виконання повсякденних завдань, для яких не потрібні root-повноваження, від імені цього користувача;

4. Вимикати непотрібні сервіси. Деякі фонові процеси встановлені на автозавантаження і працюють до відключення системи, що може нести в собі певну небезпеку;

5. Використовувати двофакторну аутентифікацію з надійними ключами для доступу до сервера через SSH-з'єднання;

6. Змінити порт для SSH-з'єднання, що встановлений за замовчуванням, на будь-який інший;

7. Налаштувати права доступу для користувачів і впровадити регулярні зміни паролів;

8. Встановити вимогу складних паролів і блокування облікового запису після кількох невдалих спроб введення пароля;

9. Встановити і налаштувати міжмережний екран за допомогою вбудованого в ОС Linux контролера iptables;

10. Виконувати регулярне резервне копіювання на окремий диск, розділ або в безпечне віддалене сховище;

11. Використовувати систему моніторингу IDS/IPS (Snort, Suricata, Bro, Kismet);

12. Регулярно переглядати системні log-файли аудиту операційної системи, щоб своєчасно дізнаватися про помилки, а також про уразливості, з якими зіткнулися інші користувачі;

13. Використовувати один сервер для одного основного сервісу (ролі сервера);

14. Обґрунтовано використовувати різноманітні програмні продукти, наприклад: Linux-ACLs, LIDS (Linux Intrusion Detection / Defense System), AIDE (Advanced Intrusion Detection Environment) та інш.

Таким чином, використання перерахованих вище рекомендацій може призвести до збільшення захищеності інформації при використанні Linux-подібних серверних операційних систем.

Список використаних джерел:

1. Як захистити Linux-систему. [Електронний ресурс] - Режим доступу: https://habr.com/ru/company/1cloud/blog/309696/

2. Захист системи Linux: 11 порад з безпеки. [Електронний ресурс] - Режим доступу: https://proglib.io/p/linux-security/

3. Як захистити віртуальний сервер. [Електронний ресурс] - Режим доступу: https://vps.ua/wiki/install-linux-vps/security/