МЕТОДИКА ПРОВЕДЕННЯ СИСТЕМНОГО АУДИТУ НА LINUX СЕРВЕРАХ

Гонтарь І. А., Снігуров А.В.

Кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки,
Україна.

E-mail: ivan.hontar@nure.ua,
arkadii.snihurov@nure.ua

Abstract

Linux server is a powerful and versatile system that is widely used for complex enterprise-class data centers and workload environments. One of the important ways to use the server is to perform audit server functions. This approach analyzes the state of the server for its network configurations, internal settings, handling of server resources, etc. to establish the state of the system. The state of the system affects not only server performance, but also security. Since the server may host databases, services, etc., auditing is necessary to ensure smooth and secure operation. The report identifies issues based on their prioritization for rapid countermeasures against threats.

У світі не існує програмного забезпечення, котре не має вразливостей. Розробники програмного забезпечення час від часу виправляють ці помилки щоб запобігти проблемам з безпекою, продуктивністю або зручністю використання. Представники не несуть відповідальності за настройку їх продукту. Під настройкою продукту вважається створення оптимального середовища для запуску цього програмного забезпечення. Наприклад: під середовищем можна прийняти Linux сервер, а продуктом – MySQL сервер. Компанія Oracle, яка підтримує та розвиває MySQL сервера та не тільки, не несе відповідальності за настройку Linux сервера, на котрому він встановлений.

Для того, щоб підтримувати сервери, їх правильну роботу та безпеку – проводиться аудит серверів, де з'ясовується, чи існують на них потенційні проблеми, які можуть вплинути на безпеку або стабільність серверів.

У кожного сервера можуть бути різні складові для аудиту, але ключові аспекти перевірки будуть розглянуті у даній статті.

Спочатку, як один з основних речей – це перевірка правомірного використання ресурсів, таких як оперативна пам'ять, ресурсів процесора, введення/виведення, дисковий простір, інше. Надмірне використання ресурсів, зазвичай, свідчить про проблеми, тому після аудиту потрібно розслідувати надмірне споживання ресурсів. Однією з проблем може бути знайдене вузьке місце продуктивності. В іншому випадку можливо, що хтось скористався вразливістю.

Для рішення даного завдання знадобляться такі інструменти моніторингу, як sysstat. Якщо потрібно виявити аномалію, то визначаємо службу, яка працює з проблемним місцем, та над ким проводиться сама дія, над користувачем або програмою.

Після огляду на ресурси сервера – йде аналіз логів. Лог – це запис у будь-який текстовий файл, дію котру виконували, а також її ініціатора. Повинен бути проведений аналіз лог-файлів на знаходження аномальних записів. Аномальними записами у лог-файлів – це записи систем чи програм, над котрими проводились несанкціоновані дії.

Нижче наведені основні журнали, які потрібно перевірити під час аудиту [1]:

- журнали авторизації у систему;
- системний журнал;
- журнал запуску програм;
- журнал Cron.

Одна з найважливіших дій при проведенні аудиту це перевірка змін системних налаштувань, програмних файлів і файлів конфігурації. Вразливості системного програмного забезпечення можуть надати зловмисникам доступ адміністратора до серверів.

Зловмисники можуть замінити системні файли на змінені версії файлу, які можуть бути схожі на оригінал, але в них може вміститися шкідливе програмне забезпечення, яке можна використовувати для подальших атак. Отже, завжди варто перевірити, чи є які-небудь із ваших програмних файлів або файлів конфігурації були нещодавно змінені. Потенційні зміни можуть відбуватися у наступних директоріях [1]:

- /bin/;
- /sbin/;
- /etc/;
- /boot/;
- /dev/.

Деякі автоматизовані інструменти, такі як Lynis, можуть пришвидшити цей процес.

Перевірка серверів на наявність шкідливих програм та rootkit являється обов'язковою операцією при аудиті. Цей процес має бути налаштований на автоматичне оновлення антивірусної програми, її бази даних. Під час аудиту сервера, виконавець повинен проаналізувати звіти зі сканування.

Під час даної фази повинно бути здійснено сканування для рішення наступних цілей:

- сканування на наявність шкідливих програм, таких як LMD, CXS тощо;
- сканування на наявність вірусів, наприклад, ClamD;
- сканування на наявність rootkit, наприклад, RkHunter, ChkRootKit.

Якщо при скануванні було виявлено зловмисне програмне забезпечення, недостатньо його видалити. В даному випадку потрібно з'ясувати, як зловмисне програмне забезпечення потрапило на сервер, і виправити вразливість.

Постачальники програмного забезпечення постійно знаходять і виправляють вразливості. Під час аудиту, аудитор знаходить усі програми, які встановлені на сервері, аналізує їх версії. Якщо деякі програми мають оновлення, фахівець спочатку повинен вивчити ці оновлення, потому що деякі оновлення можуть вмістити більше відкритих вразливостей на відміну від старих версій.

Основні приклади програм та утиліт, які допомагають аудиторам проводити перевірку Linux серверів [2]:

- settimeofday, clock_adjtime – моніторинг системних викликів, які пов'язані за часом. Аудит можна налаштувати для створення запису журналу щоразу, коли використання певний системний виклик;
- pam_faillock – модуль авторизації, який може записувати помилку спроби входу. Аудит можна налаштувати для запису недавніх спроб входу та надає додаткову інформацію про користувача, у якого були спроби на вхід;
- ausearch – утиліта, пошуку подій, за допомогою якої можна фільтрувати лог-записи та забезпечити повний процес записаних дій на основі різних критеріїв пошуку;
- aureport – утиліта, яку можна використовувати, для щоденного створення звітів про зареєстровані події.;
- nftables, iptables і ebtables – утиліти, які використовують для налаштування для запуску Події аудиту, що дозволяє системним адміністраторам контролювати мережу доступу.
- Nmap – утиліта для сканування мереж та знаходженням вразливостей;
- Metaspolit – фреймворк, який включає в себе велику кількість модулів та баз даних з різними інструментами для знаходження вразливостей на сервері.

У даній статті було розглянуто методики проведення аудиту на Linux серверах та приклади програм, утиліт та фреймворків, які дозволяють не тільки просканувати, а й за спеціальними умовами настроїти сповіщення для аномальної поведінки та програм, на основі звітів яких, можна скласти рекомендації, котрі допоможуть оптимізувати та покращити захист Linux серверів.

Література

1. Understanding Linux Audit [Електронний ресурс] – Режим доступу до ресурсу: https://documentation.suse.com/sles/12-SP5/html/SLES-all/cha-audit-comp.html

2. IzyKnows. Linux auditd for Threat Detection [Part 1] [Електронний ресурс] / IzyKnows. – 2022. – Режим доступу до ресурсу: https://izyknows.medium.com/linux-auditd-for-threat-detection-d06c8b941505.