



Дослідження налаштувань вебсерверів та проксісерверів під керування програмного засобу Nginx

Олександр Гожий

Черкаський НДЕКЦ МВС України, м. Черкаси, Україна

Дослідження конфігураційних файлів Nginx під час судової експертизи є ключовим елементом у виявленні злочинних дій у вебсерверах, воно забезпечує ефективне розслідування кіберзлочинів, виявляє кіберзагрози та формує кібербезпеку.

Ключові слова: Nginx; Linux; судова експертиза.

Investigation of Web Server and Proxy Server Configurations Managed by the Nginx Software

Oleksandr Hozhyi

Investigating Nginx configuration files within forensic examinations is pivotal in uncovering illicit activities on web servers, facilitating cybercrime investigations, identifying cyber threats, and shaping cybersecurity concepts.

Keywords: Nginx; Linux; forensic examination.

Вебсервер є ключовою складовою інтернету, забезпечуючи передачу вебсторінок та інших вебресурсів користувачам. Це програмне забезпечення, яке обробляє та відповідає на запити від клієнтів, що надходять через протокол HTTP. Основними функціями вебсервера є обробка та відправка вебсторінок, управління з'єднаннями з клієнтами, реалізація безпеки та контроль доступу до ресурсів, а також ведення журналів запитів [1].

Однією з найпопулярніших програм для виконання функцій вебсервера є Nginx, хоча існують інші популярні вебсервери (Apache, Microsoft IIS, Lighttpd). Кожен із них має свої особливості та переваги, що враховуються під час вибору вебсервера для конкретного проекту.

Nginx, або engine X — це вебсервер і проксі-сервер (розробник — І. Сисоєв, 2004), що має високу ефективність і надійність у високонавантажених вебсистемах. Основною перевагою Nginx є асинхронна, подієва модель обробки з'єднань, що дає змогу обробляти тисячі одночасних з'єднань із мінімальним споживанням ресурсів. Для нього характерна висока швидкість передачі даних і здатність працювати водночас як вебсервер і проксісервер. Він також здатний ефективно обробляти статичний і динамічний контент, а його налаштування завдяки зрозумілому конфігураційному файлу та можливості

вносити зміни без перезавантаження сервера вважають простими та зручними.

На відміну від функціонально схожого програмного забезпечення, Nginx використовує власний принцип обробки вхідних даних — кожен запит користувача розділяється на кілька дрібних, спрощуючи обробку кожного. У термінології Nginx вони мають назву «робоче з'єднання».

Після обробки кожне з'єднання збирається в одному віртуальному контейнері та трансформується в єдиний первинний запит, а після відправляється користувачеві. Одне з'єднання може опрацювати до 1024 запитів кінцевого користувача. Для зменшення навантаження на оперативну пам'ять вебсервер використовує виділений сегмент пам'яті, що має назву «пул» (англ. pool). Він динамічний і розширюється у разі збільшення довжини запиту [2].

Під час проведення судової експертизи у сфері дослідження комп'ютерної техніки та програмних продуктів згідно з експертною спеціальністю 10.9, виникає необхідність в докладному аналізі налаштувань програмного забезпечення та вивченні зв'язків між різними програмними компонентами. Поміж найпоширеніших об'єктів дослідження у межах судової експертизи є вебсервери, які працюють під управлінням операційних систем типу Linux, а також зазначене програмне забезпечення Nginx.



Аналізуючи роботи про особливості налаштування вебсерверів на *Nginx*, варто визначити, що основні налаштування цього програмного засобу знаходиться в каталогах */etc/nginx/* та */etc/nginx/conf.d/*, а також у файлі */etc/nginx/nginx.conf*. Аналіз саме цих файлів є обов'язковим під час проведення комп'ютерно-технічних експертиз та досліджень [2, 3].

Зазвичай програмний засіб *Nginx* на вебсервер налаштований на прослуховування *http/https* портів 80 і 443, хоча фактично можна змінити налаштування, щоб він прослуховував будь-які порти протоколу *TCP/IP*.

Основними складовими конфігурації *Nginx* є розділи *upstream* та *server*. Перший відповідає за розподіл навантаження між різними мережевими елементами та визначає адреси, на які спрямовуватимуться запити, другий — визначає параметри прослуховування окремих віртуальних елементів серверу (зокрема, перелік доменів, портів) та параметри обробки запитів [3].

Розділ *http* визначає загальний режим функціонування вебсерверу та містить параметри стиснення та шифрування потоків даних, він не визначає ключі шифрування, які встановлюють окремо для кожного віртуального сервера в розділі *server*.

Поміж конфігураційних параметрів розділу *server* особливу увагу привертає параметр

location, що визначає спосіб обробки запитів і дії залежно від запитуваних даних (доступ до директорій, обробка певних типів файлів). Наприклад, популярною конфігурацією є перенаправлення запитів до файлів типу *php* в програмний засіб *php-fpm*.

Отже, розуміння конфігураційних директив програмного засобу *Nginx* і вміння читати файли його налаштувань дає змогу судовим експертам з комп'ютерно-технічних досліджень ефективно аналізувати роботу вебсерверів та точно й об'єктивно визначати його функціональні можливості та цільове призначення.

Перелік джерел посилання

1. Usage Statistics and Market Share of Web Servers / W3Techs. Oct, 2021. URL: https://w3techs.com/technologies/overview/web_server (дата звернення: 28.02.2024).
2. DeJonghe D. NGINX Cookbook: Advanced Recipes for High Performance Load Balancing. O'Reilly Media, 2019. URL: https://www.academia.edu/43382694/Derek_DeJonghe_NGINX_Cookbook (дата звернення: 28.02.2024).
3. Tatroe K., Macintyre P. Programming PHP: Creating Dynamic Web Pages. 4th ed. O'Reilly Media, 2020. 542 p.