Секція 1

ДОСЛІДЖЕННЯ БЕЗПЕКИ САЙТІВ УНІВЕРСИТЕТІВ НА ПРИКЛАДІ ХАІ

Бохан К.А.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник Землянко Г. А.

Актуальність. З розвитком сучасних технологій уся необхідна інформація для студента знаходиться в мережі Інтернет. Є два типи сайтів: інформаційного характеру та сайти для дистанційного навчання, де знаходиться необхідна користувачеві інформація. Як правило, у кожного університету є обидва типи цих сайтів. Наприклад, як є інформаційний сайт ХАІ, та навчальні сайти moodle, mentor, elearn. Тобто, можна сказати, що якість навчання та успішність студента – цілком залежить від доступності подібних ресурсів. З чого можна зробити висновок, що інформаційні та навчальні ресурси мають бути стійкими до навантаження та захищеними від несанкціонованого проникнення.

Метою даної роботи є дослідження сайту університету з метою покращення доступу та надійності роботи сайту, в умовах великого навантаження.

Основні положення. Для того, щоб зрозуміти та перевірити безпеку сайтів – проводять тести на проникнення. Тест на проникнення (penetration test) — метод оцінювання захищеності комп'ютерної системи чи мережі шляхом часткового моделювання дій зовнішніх зловмисників з проникнення у неї (які не мають авторизованих засобів доступу до системи) і внутрішніх зловмисників (які мають певний рівень санкціонованого доступу) [1]. Цей процес включає активний аналіз системи з виявлення основних потенційних вразливостей для сайту. Які можуть виникати внаслідок неправильної конфігурації веб-сервісу, непередбачених дефектів апаратних засобів при створенні сайту, або програмного забезпечення, чи оперативне відставання в процедурних чи технічних контрзаходах. Цей аналіз проводиться з позиції потенційного нападника і може включати активне використання вразливостей.

Основні шляхи взаємодії сайту та користувача – це пошук інформації. Для ідеального сайту, є правило, що уся необхідна інформація, та функціонал сайту повинні знаходитись максимально на 3 рівні вкладеності починаючи з початкової сторінки [2]. Адже, зручніше та краще буде сайт для користувача, коли він зможе робити менше помилок. Якщо, ця умова дотримується – то для користувача немає проблеми щось знайти на сайті без витрати часу на пошук.

Ця умова використовується для усіх сайтів, але основна ціль – це сайти, основною метою яких є надання інформації

Для сайтів, що використовуються для навчання – поряд з цим правилом, стоїть ще одне. Це навантаження великою кількістю користувачів, та при завантаженні великих за обсягом файлів. Навантаження великою кількістю користувачів, в цьому контексті означає тестування продуктивності. Тестування продуктивності - це тестування, яке проводиться з ціллю визначення, як швидко працює програма або її частина під деяким навантаженням [3]. Для тестування будуть обрані більш схожі на реальні цифри навантаження, ніж при тестування критичної відмови. Адже сайт повинен бути готовим до цього, бо в період вступу – кількість користувачів сайту зростає в рази. Для цього використовувався додаток JMeter. Було проведено перевірку навантаженням сайту кафедри – elearn (у середньому 800-1000 людей), та сайтів університету – ХАІ, moodle, mentor (6-7 тис. людей).

Висновки. У результаті, були перевірені такі сайти університету ХАІ: Головний сайт, elearn, moodle, mentor. Усі вони використовуються кожного дня. Але критичні дні для таких сайтів – це тижні модульного контролю, тижні підсумкового контролю, та декілька тижнів до цього моменту, літні дні, коли є температурне навантаження на сервери, та несумлінні студенти, які з метою не навчатись можуть зробити DoS-атаку. Як результат, вони пройшли два види тестування, що були наведені вище. Сьогодні сайти перейшли на хмарну платформу CloudFlare. В безкоштовній версії є базовий захист від невеликих DoS-атак. Окрім цього, вони також витримують середні навантаження, які є на серверах ХАІ. Але, при поточних відключеннях електроенергії, ці сайти стають недоступними, коли в ХАІ немає світла, чи інтернету. Для вирішення цієї проблеми слід перемістити сайти в захищену хмару, щоб вони були доступні студентам 24/7.

Список літератури

1. Тест на проникнення. *Wikipedia*. URL: http://surl.li/dndyh (дата звернення: 30.10.2022);

2. Правила для ідеального сайту. URL: https://sdmne.com/9-pravil-idealnogo-dizayna-sayta/ (дата звернення: 30.10.2022);

3. Тестування продуктивності. *Wikipedia*. URL: http://surl.li/dndyu (дата звернення: 30.10.2022).

Відомості про авторів

Бохан Кирило Андрійович. Студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 050-600-86-03, k.a.bokhan@student.csn.khai.edu.

Землянко Георгій Андрійович, асистент кафедри комп'ютерних систем, мереж і кібербезпеки, g.zemlynko@csn.khai.edu