Завдання з кібербезпеки

1. Що таке WAF? Навіщо його використовувати?

Брандмауер веб-додатків (WAF) захищає сервери та інфраструктуру веб-додатків від атак та порушень, що виникають з Інтернету та зовнішніх мереж.

Це спеціально створений брандмауер, який можна налаштувати на прийняття та відхилення HTTP-запитів і сеансів, використовуючи попередньо визначені правила.

2. Які є рівні firewall?

Firewall (міжмережевий екран або мережевий екран) - комплекс апаратних чи програмних засобів, що здійснює контроль і фільтрацію мережевих пакетів, які проходять через нього, відповідно до заданих правил.

Основним завданням мережевого екрану є захист комп'ютерних мереж або окремих вузлів від несанкціонованого доступу. Також мережеві екрани часто називають фільтрами, так як їх основне завдання - не пропускати (фільтрувати) пакети, що не підходять під критерії, визначені в конфігурації.

Залежно від рівня, на якому відбувається контроль доступу, існує поділ на мережеві екрани, що працюють на:

* мережевому рівні, коли фільтрація відбувається на основі адрес відправника і одержувача пакетів, номерів портів транспортного рівня моделі OSI та статичних правил, заданих адміністратором;
* сеансовом рівні (також відомі як stateful) - відстежують сеанси між додатками, не пропускають пакети, які порушують специфікації TCP/IP, та часто використовуються у зловмисних операціях - скануванні ресурсів, зломи через неправильні реалізації TCP/IP, обриви/уповільнення з'єднань, ін'єкції даних.
* рівні додатків, фільтрація на підставі аналізу даних програми, переданих всередині пакету. Такі типи екранів дозволяють блокувати передачу небажаної і потенційно небезпечної інформації на підставі політик і налаштувань.

3. Що таке IDS/IPS? Чим вони відрізняються?

 IDS - це система, яка забезпечує безпеку діяльності користувача, захищаючи його від різного роду вторгнень і мережевих атак, яких в епоху інформаційних технологій просто не злічити. Крім того, IDS - це можливість отримувати прогноз про майбутні атаках і запобігати їх, а також дізнаватися інформацію про "атакуючих", яка може бути корисною для коригування факторів, які допустили несанкціонованих доступ.

Останнім часом застосування користувачами систем виявлення вторгнення активно набирає популярність. IDS - найважливіший елемент інформаційної безпеки, необхідний кожному далекоглядному користувачеві. Система виявлення вторгнень дозволить не тільки виявити комп'ютерну атаку і блокувати її, а й виконати це в зручному графічному інтерфейсі - від користувача не потрібно спеціальних знань про мережевих протоколах і можливих вразливості.

Існує два основних типи IDS: вузловий(HIDS) та мережевий(NIDS). Система HIDS знаходиться на окремому вузлі та відслідковує прикмети атак на данному вузлі. Система NIDS знаходиться в окремій системі, відслідковуючи мережевий трафік на знаходження прикмет атак.

4. Які засоби можна використовувати для захисту веб-додатків?

Перший крок до забезпечення захищеності - правильна настройка всіх компонентів системи, оновлення всього використовуваного програмного забезпечення до актуальних версій, відключення всіх невикористовуваних служб, зміна всіх паролів за замовчуванням, відключення невикористовуваних облікових записів, в тому числі системних. Важливо також забезпечити шифрування даних всіх мережевих з'єднань всередині системи. У разі якщо це дозволяє веб-додаток, необхідно налаштувати розмежування прав доступу користувачів до даних і налаштувань системи, обмеживши їх мінімально необхідними.

У простих випадках вже тільки перераховані базові заходи дозволять знизити ризики до допустимого рівня. Якщо базових заходів виявиться недостатньо, необхідно звернути увагу на різноманітні спеціалізовані засоби захисту інформації.