4. Software Architecture Patterns by Mark Richards. [Електронний ресурс] - URL: https://www.oreilly.com/library/view/software-architecture-patterns/9781491971437/ch01.html Дата звернення: 21.09.2021
5. Антонов Ю.С. Комп'ютерні системи тестування на основі технології трирівневих баз даних. Інформаційні технології і засоби навчання. 2008. Т.6, №2. URL: https://journal.iitta.gov.ua/index.php/itlt/article/view/133 (дата звертання: 21.04.2021) https://doi.org/10.33407/itlt.v6i2.133
6. Антонов Ю.С., Космінська О.М. Методика аналізу тестових завдань на основі отриманих результатів. Інформаційні технології і засоби навчання. 2009. Т.12, №4. URL: https://journal.iitta.gov.ua/index.php/itlt/article/view/81/. (дата звертання: 21.09.2021) https://doi.org/10.33407/itlt.v12i4.81

УДК 004.8

Сніжинський М.В., студент 4 курсу спеціальності 122 «Комп'ютерні науки»
Потапова Н. А., к.е.н, доцент, доцент кафедри інформаційних технологій

ЗАСОБИ ЗАХИСТУ ПЕРЕДАЧІ ДАНИХ В МЕРЕЖІ INTERNET

Донецький Національний університет імені В. Стуса, м. Вінниця

Сучасне розповсюдження з'єднань з мережею Internet, забезпечує інформаційними та комунікаційними ресурсами, але попри всі переваги приховує загрозу несанкціонованого доступу до конфіденційної інформації. Кожна установа, яка веде обмін даними у всесвітній мережі, повинна зіставляти можливі втрати з перевагами, що надає можливість виходу в Internet, та забезпечувати відповідний захист власних ресурсів.

Серед варіантів захисту web-серверів найпопулярнішим на сьогоднішній день є використання протоколу SSH — засіб організації безпечного доступу до комп 'ютерів під час роботи небезпечними каналами зв'язку. [1, 2]

SSH (Secure Shell) є мережевим протоколом, який використовується для віддаленого керування комп'ютером і передавання інформаційних пакетів. За функціональністю SSH схожий на протоколи Telnet і rlogin, але шифрує увесь трафік разом із паролями, що передаються.

Для організації безпечного доступу застосовується процедура аутентифікації з використанням асиметричного шифрування з відкритим ключем, що забезпечує вищий рівень безпеки, ніж при симетричному шифруванні, яке дозволяє заощаджувати процесорний час і використовується під час подальшого обміну даними.[4]

Протокол надає можливість підтвердження оригінальності хосту, з яким відбувається з 'єднання. SSH підтримує два основних протоколи: SSHv1 і SSHv2.

Перший заснований на алгоритмі асиметричного шифрування RSA, а другий – підтримує RSA та алгоритм асиметричного шифрування DSA.

Серед характеристик протоколу SSHv2 слід виділити стійкість до атак прослуховування, – man-in-middle; атак, що здійснюються шляхом приєднання посередині, – session hijacking; атак – DNS spoffing.

З метою підвищення безпеки здійснюється подвійна аутентифікація «клієнт - сервер», «сервер-клієнт».[3]

Архітектура "клієнт-сервер" є одним із архітектурних шаблонів програмного забезпечення та є домінуючою концепцією у створенні розподілених мережевих ресурсів і передбачає взаємодію та обмін даними між ними. Вона передбачає такі основні компоненти:

- набір серверів, які надають інформацію або інші послуги програмам, які звертаються до них;
- набір клієнтів, які використовують сервіси, що надаються серверами;
- мережа, яка забезпечує взаємодію між клієнтами та серверами.

Автентифікація користувача є процесом, який відповідає за обробку перевірки автентичності клієнта і надає ряд методів автентифікації. Автентифікація є клієнто-орієнтованою. І працює наступним чином: коли користувач отримує запит на введення пароля, то це може бути запит SSH клієнта, а не сервера. Останній просто відповідає на запити клієнта про автентифікацію. Широко вживані методи автентифікації користувачів містять:

- методи з відкритим ключем. Метод відкритого ключа перевірки автентичності підтримують принаймні DSA або RSA пари ключів.

- інтерактивний універсальний метод, коли сервер відправляє один або декілька запитів вводу інформації, клієнт відображає їх і від правляє назад відповідь введену користувачем.

- GSSAPI методи аутентифікації, які забезпечують розширення схеми для виконання SSH аутентифікації з використанням зовнішніх механізмів, таких як Kerberos 5 або NTLM, забезпечуючи Single Sign On Можливість SSH сесій.

Отже, протокол SSH забезпечує високий рівень безпеки, хоча і потребує додаткового обчислювального навантаження. Для безпеки використання SSH пропонуються такі рекомендації: заборонити доступ з потенційно небезпечних адрес; заборонити віддалений root – доступ, підключення з порожнім паролем або відключення входу за паролем; обирати нестандартний порт для SSH-сервера; використовувати довгі SSH2 RSA-ключі; обмежити список IP-адрес, з яких доступ дозволено; регулярно здійснювати перегляд повідомлень про помилки аутентифікації.

Список літературних джерел.

1. Методи і способи захисту інформації. URL: https://pidru4niki.com/1801051351329/ekonomika/metodi_sposobi_zahistu_informatsiyi.
2. Терейковський І.А. Захищеність Web-серверів Apache та IIS Web-сервери. URL: http://citforum.ru/ intranet_app/interintr_03.shtml.
3. Богуш В.М., Довидьков О.А., Кривуца В.Г. Основи захищених інформаційних технологій. *К.: ДУІКТ,* 2010. 454 с.