УДК 004.4

В. С. Балацька, В. І. Ящук, О. І. Полотай,

Львівський державний університет безпеки життєдіяльності, м. Львів

ВРАЗЛИВІСТЬ КОМП'ЮТЕРНОЇ МЕРЕЖІ ЯК ПРОБЛЕМА ЗАКЛАДІВ ВИЩОЇ ОСВІТИ

Комп'ютерна мережа – це об'єкт, який постійно піддається небезпеці. Особливу увагу слід звернути на сервери, серйозну загрозу для яких становлять хакери і віруси. Перші можуть отримати доступ до конфіденційної інформації, розміщеної на сервері, зламати сайти і змінити їх вміст, а також вивести з ладу сервер за допомогою розподіленої атаки (DDoS-атака). Віруси ж, вражаючи веб-сервери, перетворюють їх у джерело інфекції. Крім того, вони істотно сповільнюють його роботу, а також займають інтернет-канал. Багато вірусів, особливо інтернет-хробаки, використовують для розповсюдження вразливості у програмному забезпеченні. Також і хакери прагнуть спрямовувати атаки на відомі «дірки» в програмному забезпеченні. Використовуючи вразливості, і ті й інші одержують досить легкий доступ до віддаленого комп'ютера навіть у тому випадку, якщо останній добре захищений. Необхідно регулярно проводити оцінку вразливості всієї мережі для перевірки рівня безпеки та зміцнення мережі організації. Щоб знайти слабкі місця використовують сканери вразливості, які використовують для виявлення вад безпеки у всій мереж, а також у окремих системах.

Ключові слова: комп'ютерна мережа, вразливість, сканер вразливості, XSpider, сканування портів.

A computer network is an object that is constantly in danger. Particular attention should be paid to servers that are seriously threatened by hackers and viruses. The former can access sensitive information hosted on the server, hack sites and change their content, as well as disable the server with a distributed attack (DDoS-attack). Viruses infect web servers and turn them into a source of infection. In addition, they significantly slow down its work, as well as occupy the Internet channel. Many viruses, especially Internet worms, are used to spread vulnerabilities in software. Hackers also seek to target known "holes" in software. Using vulnerabilities, both gain fairly easy access to a remote computer, even if the latter is well protected. It is necessary to regularly assess the vulnerability of the entire network to check the level of security and strengthen the network of the organization. To find vulnerabilities, vulnerability scanners are used, which are used to detect security flaws throughout networks, as well as in individual systems.

***Key words*:** computer network, vulnerability, vulnerability scanner, XSpider, port scanning.

Майже у будь-якій програмі є вразливості. Наявність вразливостей легко пояснюється через здатність людей допускати помилки. Велике програмне забезпечення (ПЗ) пише не одна людина, а ціла група. І досить часто помилки виникають при компонуванні модулів, створених різними програмістами. Крім того, наявність вразливостей далеко не завжди визначається якістю написання ПЗ.

На сьогоднішній день організації дуже рідко замислюються про безпеку

своєї інформації у мережі і зовсім не приділяють цьому питанню уваги, часто починаючи вживати заходів лише після витоку або втрати важливої інформації. Особливу увагу слід приділити закладам вищої освіти, адже саме на цих об’єктах інформаційної діяльності нехтують безпекою комп’ютерної мережі, що у результаті призводить до порушення безпеки, витоку інформації та хакерських атак.

Щоб забезпечити або ж усунути існуючі проблеми, пов’язані із захистом інформації, атаками зловмисників на комп’ютерну мережу, її бази даних, додатки, у даній роботі розглянуто рішення для діагностики вразливостей і їх моніторингу використовуючи один із засобів пошуку вразливостей [1].

Засоби пошуку вразливостей можуть функціонувати на трьох рівнях: на мережевому рівні (network-based), рівні операційної системи (host-based) і рівні додатку (application-based). Найбільшого поширення набули засоби аналізу захищеності мережевих сервісів і протоколів. Пов’язано це, у першу чергу, з універсальністю використовуваних протоколів. Вивченість і повсюдне використання таких протоколів, як IP, TCP, HTTP, FTP, SMTP, дозволяють з високим ступенем ефективності перевіряти захищеність інформаційної системи, що працює в даному мережевому оточенні.

Другими за поширеністю є засоби аналізу захищеності операційних систем (ОС) [2]. Пов'язано це також з універсальністю і поширеністю деяких операційних систем (наприклад, UNIX і Windows NT). Однак через те, що кожен виробник вносить в операційну систему свої зміни (яскравим прикладом є безліч різновидів ОС UNIX), засоби аналізу захищеності ОС аналізують в першу чергу параметри, характерні для всього сімейства однієї ОС. І лише для деяких систем аналізуються специфічні для неї параметри. Засобів аналізу захищеності додатків на сьогоднішній день не так багато, як цього хотілося б. Такі засоби існують тільки для широко поширених прикладних систем, типу Web-браузери, СУБД і т.д.

Оскільки найбільшого поширення набули засоби, що функціонують на рівні мережі, тому основна увага буде приділена сканерам-вразливості.

Практично будь-який сканер проводить аналіз захищеності в кілька етапів [3]:

1. Збір інформації про мережу.

2. Виявлення потенційних вразливостей.

3. Підтвердження обраних вразливостей.

4. Генерація звітів.

5. Автоматичне усунення вразливостей.

Розглянемо можливості та роботу одного з відомих сканерів на прикладі комп'ютерної мережі Львівського державного університету безпеки життєдіяльності.

Інтелектуальний сканер XSpider здатний виявити максимальну кількість вразливостей в інформаційній системі клієнта до того, як вони будуть виявлені і використані зловмисниками [4]. Регулярне автоматичне сканування за допомогою XSpider майже не вимагає втручання фахівця. Після сканування система видає чіткі рекомендації щодо усунення виявлених вразливостей і вирішення інших проблем безпеки. XSpider відрізняється широким покриттям програмного забезпечення інформаційних систем, включаючи різні ОС (Windows, * nix, Mac OS), СУБД, мережеві пристрої, АСУ. Сканер виявляє вразливості як для системного, так і для прикладного ПЗ, проводить аналіз веб-додатків. Система працює віддалено, ніяких агентів і додаткового ПЗ для перевірки вузлів ставити не потрібно. Під час сканування помітного навантаження на вузол, що перевіряється не створюється.

База вразливостей XSpider оновлюється автоматично і регулярно і містить понад 20 000 перевірок. Завдяки евристичним алгоритмам сканер здатний виявляти ще не опубліковані вразливості і відрізняється вкрай низьким рівнем помилкових спрацьовувань.

Переваги даного програмного продукту:

•контроль змін на сканованих вузлах дозволяє отримати повну картину захищеності в динаміці;

•повна ідентифікація сервісів на випадкових портах для виявлення вразливостей серверів з нестандартною конфігурацією;

•евристичний метод визначення типів і імен серверів (HTTP, FTP, SMTP, POP3, DNS, SSH і інші) для визначення справжнього імені сервера і коректної роботи перевірок;

•обробка RPC-сервісів (Windows і *nix) з повною ідентифікацією, включаючи визначення детальної конфігурації комп'ютера;

•перевірка слабкості парольного захисту: оптимізований підбір паролів практично у всіх сервісах, що вимагають автентифікації. Детальний аналіз контенту веб-сайтів, включаючи виявлення вразливостей в скриптах: SQL, XSS, запуск довільних програм і ін.;

•аналіз структури HTTP-серверів для пошук слабких місць в конфігурації;

•розширена перевірка вузлів під управлінням Windows;

•проведення перевірок на нестандартні DoS-атаки.

На рисунку 1, зображена мережа Львівського державного університету безпеки життєдіяльності, де відображені вразливі місця, що знайшов сканер вразливості XSpider за відповідною IP-адресою та відповідно до кольору вказує на рівень вразливості: червоний – критичний рівень; помаранчевий – середній рівень; зелений – низький або інформативний рівень.

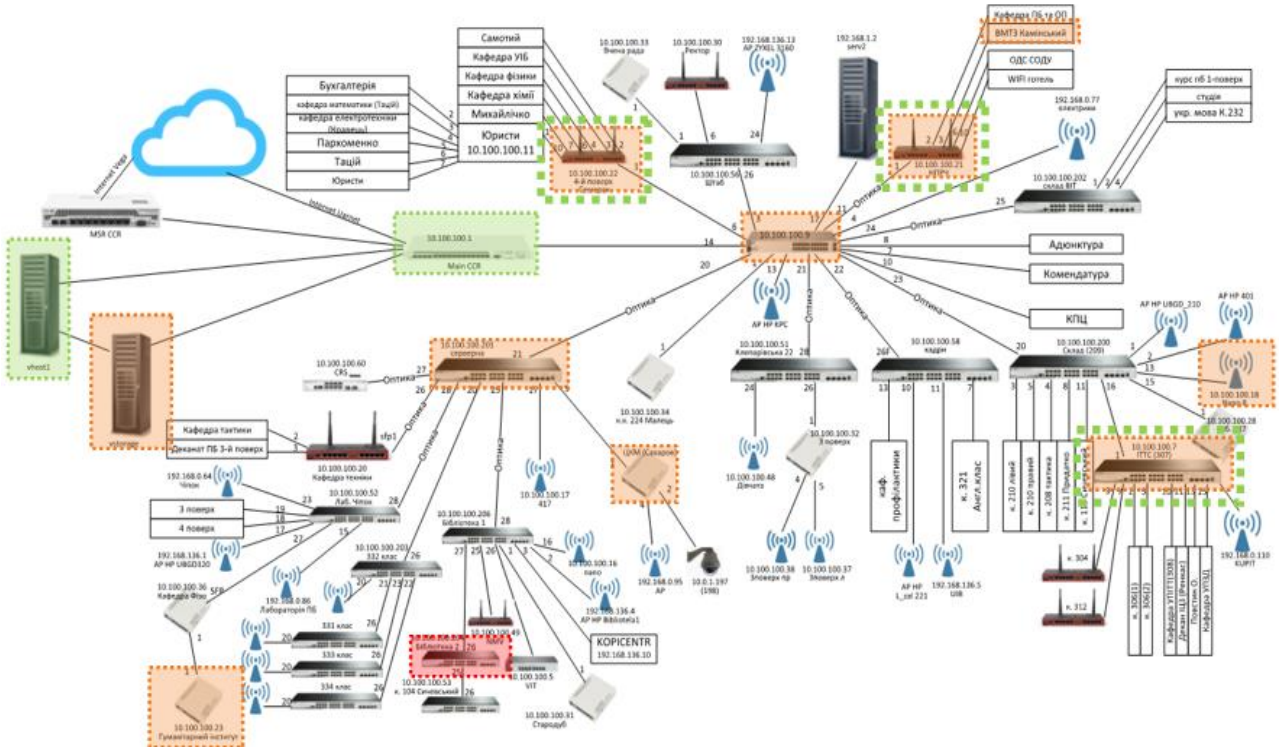

Рис. 1. Вразливі місця комп’ютерної мережі знайдені сканером вразливості XSpider

1) Перша вразливість, яку знайшов сканер та класифікував її до високого рівня небезпеки (позначено червоним кольором), це ***пароль за замовчуванням*** на одному з хостів мережі, що спричиняє такі небезпеки як: несанкціонований вхід в обліковий запис користувача; модифікація даних; запис вірусів та різного роду небезпечних файлів; просто атака на мережу через даний обліковий запис.

Дана проблема вирішується досить просто, необхідно просто дотримуватись правил вибору паролю. Пароль повинен містити не менше восьми символів. Це може бути будь-яка комбінація букв, цифр та інших символів (стандарту ASCII). Надрядкові знаки і символи з наголосами не підтримуються. Рекомендуємо не використовувати пароль, який: занадто простий, наприклад "password123" або як в нашому випадку "masterkey"; був встановлений на обліковий запис раніше; починається або закінчується пропуском.

2) Наступною вразливістю, що виявив сканер та дана небезпека зустрічається на декількох хостах є ***незахищений протокол***. Дана проблема полягає в тому, що Telnet є протоколом віддаленого управління комп'ютером. Цей протокол є відкритим, тобто трафік з'єднання комп'ютерів не шифрується і може бути перехоплений шляхом прослуховування мережі.

Рішенням такої вразливості є використовування захищених протоколів, наприклад SSH або дозволу на доступ до цього сервісу тільки з певних відомих адрес.

3) ***SQL ін'єкція.*** Це спосіб нападу на базу даних в обхід міжмережевого захисту. У цьому методі, параметри, що передаються до бази даних через Web програми, змінюються таким чином, щоб змінити виконуваний SQL запит. Наприклад, додаючи різні символи до параметру, можна виконати додатковий запит спільно з першим.

Напад може використовуватися для наступних цілей:

- Отримати доступ до даних, які зазвичай недоступні, або отримати дані конфігурації системи, які можуть використовуватися для подальших нападів. Наприклад, змінений запит може повернути хешовані паролі користувачів, які в наслідку можуть бути розшифровані методом перебору;

- Отримати доступ до комп'ютерів організації, через комп'ютер, на якому знаходиться база даних. Це можна реалізувати, використовуючи процедури бази даних і розширення 3GL мови, які дозволяють доступ до операційної системи.

Рішенням цієї вразливості є заборона використання даного скрипта або програмно виправити помилку.

4) Вразливість ***слабка криптографія*** у одному з просканованих хостів проявляється через те, що версії протоколу SSH 1.33 і 1.5 не є недостатньо захищені криптографічно. У майбутньому це може призвести до DoS атак.

Рішенням є зміна протоколів використання на 1.99 та 2.0, які більш стійкі до даної вразливості та не дають можливості прочитати приватні сплойти.

5) Наступна вразливість зустрічалась часто, ***обліковий запис***. Проблема полягає у тому, що знайдений обліковий запис, який є відкритим та доступна інформація по ньому: ProCurve J8770A Switch 4204vl, revision L.11.43, ROM L.10.03 (/sw/code/build/rmm). Це може призвести до того, що зловмисник може користуватись цим обліковим записом, читати, змінювати та скомпроментовувати інформацію, що є у мережі.

Закрити доступ до облікового запису, буде простим і дієвим вирішенням даної проблеми.

6) ***Доступний метод TRACE*** [5], за допомогою використання метода TRACE у протоколі HTTP можливе виконання атаки міжсайтовий скриптинг. Основна мета міжсайтового скриптинга – крадіжка cookies користувачів за допомогою вбудованого на сервері скрипта з подальшою вибіркою необхідних даних і використанням їх для наступних атак і зломів. Зловмисник здійснює атаку користувачів не безпосередньо, а з використанням вразливостей веб-сайту, який відвідують жертви, і впроваджує спеціальний JavaScript. У браузері у користувачів цей код відображається як єдина частина сайту. При цьому відвідуваний ресурс за фактом є співучасником XSS-атаки.

Рішенням є заборона використання даного методу, адже він несе велику небезпеку для мережі та порушення її цілісності.

Висновок. Отже, у мережі Львівського державного університету безпеки життєдіяльності сканером вразливостей «XSpider» було виявлено шість найбільш вразливих місць на які можуть проводитись атаки. Описано та проаналізовано тип виявлених вразливостей та можливі наслідки, вразі хакерських атак. Наявна конфігурація мережі, яка функціонує у закладі вищої освіти може призвести до блокування, скомпроментування мережевого зв'язку, веб-додатків та інших негативних наслідків, що буде супроводжуватись втратою важливої інформації та несанкціонованим доступом до інформаційної системи. У роботі запропоновано рекомендації і ряд рішень для уникнення проблем функціонування та безперебійної роботи мережі.

Література:

1. Азаров О. Д., Захарченко С. М., Кадук О. В. Комп'ютерні мережі: навчальний посібник. Вінниця: Вінницький Національний Технічний Університет, 2013. 371 с.
2. Принципи роботи систем аналізу захищеності. URL: http://um.co.ua/13/13-9/13-98065.html. (дата звернення: 08.09.2021)
3. Offensive Cyber 2012. URL: https://cyberwar.nl. (дата звернення: 10.09.2021)
4. XSpiders. URL: https://www.ptsecurity.com/products/XSpider/. (дата звернення: 11.09.2021)
5. TRACE. URL: https://developer.mozilla.org/docs/Web/HTTP/Methods/TRACE. (дата звернення: 11.09.2021)