DOI: https://doi.org/10.36910/6775-2524-0560-2020-41-32
УДК: 004.052
Яцюк Світлана Миколаївна, к.пед.н., доцент
https://orcid.org/0000-0002-8369-6060
Сачук Юрій Володимирович, к.ф.-м.н, ст. викл.
https://orcid.org/0000-0002-1317-1103
Глинчук Людмила Ярославівна, к.ф.-м.н., доцент
https://orcid.org/0000-0002-8943-9604
Прус Руслана Богданівна, к.т.н., ст. викл.
https://orcid.org/0000-0001-7726-1602
Гришанович Тетяна Олександрівна, к.ф.-м.н., ст. викл.
Східноєвропейський національний університет імені Лесі Українки
https://orcid.org/0000-0002-3595-6964
Волинський національний університет імені Лесі Українки, м.Луцьк, Україна

ДОСЛІДЖЕННЯ РОБОТИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ЗАХИСТУ МЕРЕЖ

Яцюк С. М., Сачук Ю. В., Глинчук Л. Я., Прус Р. Б., Гришанович Т. О. Дослідження роботи програмного забезпечення для захисту мереж. Досліджено основні сканери для виявлення уразливості мереж та виявлення впливу на них. Оцінено експозиції для захисту мереж задля застереження проникнення в неї, перевірки журналів та відстеження схеми руху трафіку, а також охорони портів та використання ресурсів.
Ключові слова: мережа, сканер, програмне забезпечення, уразливість, мережеве адміністрування.

Яцюк С. Н., Сачук Ю. В., Глинчук Л. Я., Прус Р. Б., Гришанович Т. А. Исследование работы программного забезпеченения для защиты сетей. Исследованы основные сканеры для определения степени глубины и обнаружения воздействия на них. Оценен исследований для защиты сетей для предостережения проникновения в нее, проверки журналов и отслеживания схем движения трафика, также охраны портов и использования ресурсов.
Ключевые слова: сеть, сканер, программное обеспечение, уливисть, сетевое администрирование.

Yatsyuk S., Sachuk U., Glinchuk L., Prus R., Grishanovich T. Research of software for network protection. The main scanners for detecting network vulnerabilities and detecting their impact have been studied. Exposures have been assessed to protect networks to prevent intrusion, to check logs and track traffic patterns, and to protect ports and use resources.
Keywords: network, scanner, software, vulnerability, network administration.

Постановка наукової проблеми. Будь-яка мережа, що знаходиться за межами найменшого офісу, має надто велику і складну поверхню. Кожна мережа повинна захищатись від несанкціонованого доступу та мережевих атак спеціальним програмним забезпеченням. Навіть якщо необхідно захистити лише декілька хостів і пристроїв, необхідна автоматизована допомога, щоб ефективно та ретельно відстежувати зростаючий список відомих уразливостей і гарантувати, що мережа не піддається впливу.

Аналіз досліджень. Дослідженнями в сфері захисту мереж займалися Єсін В. І., Кузнецов А. А., Сорока Л. С.. Механізми і політику розмежування прав доступу та методи, пристрої забезпечення захисту і безпеки вивчав Бабак В.П., Горбенко І. Д. Гриненко Т. О., Богуш В. М. Кузнецов О.О. теоретично обґрунтував систему захисту інформації в інформаційних системах та методи традиційної криптографії. На нашу думку, авторами недостатньо розкрито питання дослідження сучасних сканерів для виявлення уразливості мереж.

Метою дослідження є аналіз і можливість практичного застосування сучасних сканерів для виявлення уразливості мереж та виявлення впливу на них.

Виклад основного матеріалу. Більшість операційних систем надають автоматизовані оновлення програмного забезпечення. Для невеликої організації це може бути достатньо. Але цього встановленого програмного забезпечення не вистачить для крупних компаній і їх мереж. Будь-який хост або пристрій, що піддається впливу Інтернету, повинен проходити перевірку проникнення, навіть "внутрішні" хости та пристрої повинні регулярно перевірятися.

Саме сканери забезпечать автоматичну допомогу щодо уразливості мереж [1, 2]. Як і багато інструментів мережевого адміністрування, сканер уразливості має як законне, так і нелегітимне використання. Це може бути корисним системному адміністратору, розробнику, досліднику безпеки, тестеру проникнення або хакеру з чорною шапочкою. Він може бути використаний для оцінки захисту мережі або протидії проникнення в неї. Нами досліджено найсучасніші сканери на вразливість мережі. А саме:

© Яцюк С. М., Сачук Ю. В., Глинчук Л. Я., Прус Р. Б., Гришанович Т. О.

1. **Менеджер конфігурації мережі SolarWinds (БЕЗКОШТОВНА ПРОБЛЕМА)** – Безкоштовно протягом 30 днів без жодних зобов'язань переходити на платну версію, це дуже всебічний менеджер конфігурації, який сканує налаштування пристрою, що створює вразливості.

2. **ManageEngine VUNnerability Manager Plus (БЕЗКОШТОВНА ПРОБЛЕМА)** – Безкоштовна та платна версії для середовищ Windows та Windows Server, включає сканування вразливості та автоматизоване зменшення наслідків.

3. **Моніторинг вразливості мережі Paessler за допомогою PRTG (БЕЗКОШТОВНА ПРОБЛЕМА)** – Частина системи моніторингу ресурсів PRTG, цей інструмент перевіряє журнали та відстежує схеми руху трафіку, а також охороняє порти та використання ресурсів. Це безкоштовно для використання до 100 датчиків.

4. **OpenVAS** – Відкрита система оцінки вразливості – це безкоштовний менеджер уразливості для Linux, до якого можна отримати доступ у Windows через VM.

5. **Аналізатор базової безпеки Microsoft (MBSA)** – Безкоштовний і простий у використанні інструмент, який перевіряє продукти Microsoft на вразливості.

6. **Retina Network Scanner Community Edition** – Безкоштовно сканувати до 256 IP-адрес, ця система спирається на центральну базу даних відомих слабких місць.

7. **Nexpose Community Edition** – Безкоштовно сканує до 32 IP-адрес, цей інструмент виявляє та реєструє ваші пристрої, підключені до мережі, виділяючи всі відомі вразливості в кожному.

8. **Оновлення програмного забезпечення Kaspersky** – безкоштовна утиліта для Windows, яка встановить доступні оновлення для будь-якого вашого програмного забезпечення, а не лише продуктів Kaspersky.

Сканер уразливості покладається на базу даних відомих уразливостей та автоматизовані тести на них. Обмежений сканер адресуватиме лише один хост або набір хостів, що працюють на одній платформі операційної системи. Комплексний сканер сканує широкий спектр пристроїв і хостів у одній або декількох мережах, ідентифікуючи тип пристрою та операційну систему та перевіряючи відповідні вразливості з меншою або більшою нав'язливістю.

Сканування може бути виключно мережевим і проводитись із широкого Інтернету (*зовнішнє сканування*) або з внутрішньої локальної мережі (*сканування внутрішнє*). Це може бути *глибокий огляд*, коли сканеру надано облікові дані для аутентифікації себе як законного користувача хоста або пристрою.

Сканування вразливості – це лише одна частина процесу управління вразливістю. Після того, як сканер виявить вразливість, про нього потрібно повідомити, перевірити (чи це не помилка?), Далі слід встановити пріоритети та класифікувати за ризиком та впливом, відремонтувати та відстежити, щоб запобігти регресії..

Якщо організації потрібен формальний процес для вирішення вразливих місць, процес управління включає планові сканування, наведення пріоритетів, управління змінами для версій програмного забезпечення та забезпечення процесу. Більшість сканерів на вразливість можуть бути частиною повного рішення щодо управління вразливістю, тому великим організаціям потрібно підбирати цей контекст під час вибору сканера..

Багато вразливих місць можна усунути шляхом виправлення, але не всі. Аналіз витрат / вигод повинен бути частиною процесу, оскільки не всі вразливості є ризиками в кожному середовищі, і можуть бути бізнес-причини, через які не можна встановити заданий патч. Таким чином, це корисно, коли вказівки щодо виправлення інструменту включатимуть альтернативні засоби (наприклад, відключення послуги або блокування порту через брандмауер).

Існує багато можливостей для оцінки роботи сканера. Вибираючи інструменти, нашими головними міркуваннями були надійність та галузева репутація постачальника програмного забезпечення, їх здатність постійно підтримувати та оновлювати свій продукт, унікальні функції, простота налаштування та використання та можливості масштабування.

Менеджер конфігурації мережі SolarWinds (НКМ) є безкоштовний лише протягом періоду оцінки та охоплює певний (але важливий) підмножину вразливих місць [3]. NCM обробляє як сканування вразливості, так і управління доменом уразливостей, що виникають внаслідок неправильної конфігурації маршрутизатора та комутатора. Основна увага приділяється виправленню, моніторингу несподіваних змін та аудиту відповідності. NCM є безкоштовним лише під час повністю функціонального випробування 30 днів. NCM сканує вразливості в конфігураціях пристроїв на базі Cisco Adaptive Security Appliance (ASA) та Internetwork Operating System (IOS®).

© Яцюк С. М., Сачук Ю. В., Глинчук Л. Я., Прус Р. Б., Гришанович Т. О.

SolarWinds NCM. Для вразливості через помилки конфігурації він забезпечує можливість автоматичного запуску скриптів виправлення після виявлення порушення та автоматично розгортати стандартизовані оновлення конфігурації на сотні пристроїв.

Для усунення несанкціонованих змін, включаючи регресії, він забезпечує моніторинг змін конфігурації та оповіщення. Він може постійно перевіряти маршрутизатори та комутатори на предмет відповідності. Він виконує Національний інститут стандартів і технологій (NIST®), Федеральний закон про управління інформаційною безпекою (FISMA) та Агентство оборонних інформаційних систем (DISA®). Для випробування легка установка може встановлювати та використовувати SQL Server Express, але база даних обмежена 10 гігабайтами (рис.1).

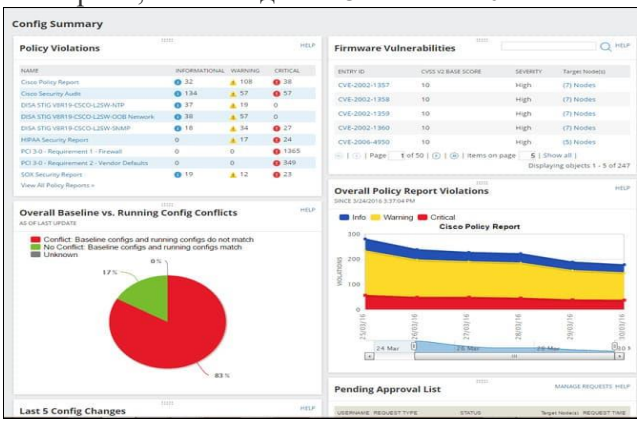

Рис.1. Вікно сканера **SolarWinds NCM**

ManageEngine VUNnerability Manager Plus. ManageEngine виробляє широкий спектр інструментів управління IT-інфраструктурою [4,5]. **Менеджер уразливості Plus** є конкурентом компанії на ринку системного захисту. Повний перелік функцій цього інструменту доступний лише для платної версії утиліти, розробленої для великих локальних мереж та багатопрофільних мереж. Безкоштовна версія підходить для малих та середніх підприємств та захищатиме до 25 пристроїв.

Безкоштовна версія надає як сканування на вимогу, так і планове вразливість, що дозволить виявити проблеми у вашій власній мережі. Передова технологія, розгорнута в сканері, здатна виявити аномальну поведінку. Ця стратегія є більш ефективною для виявлення вразливих місць з нульовим днем, ніж звичайні системи виявлення загроз, засновані на правилах. Ви також отримуєте заходи щодо зменшення загрози, вбудовані у безкоштовне видання Vulnerability Manager Plus.

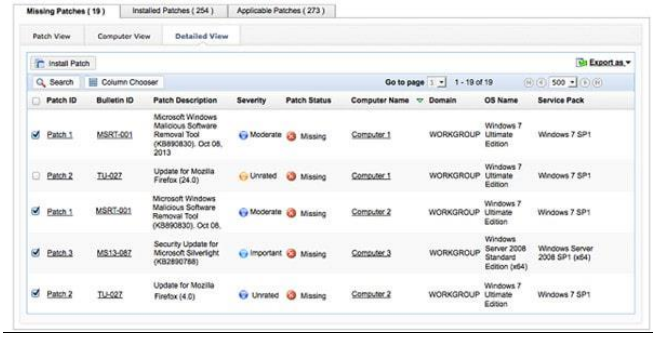

Рис. 2. Вікно сканера **ManageEngine**

Системні загрози можуть полягати в слабкій безпеці конфігурації або застарілому програмному забезпеченні. Менеджер уразливості Plus **включає управління конфігурацією** і **Управління патчем** функції, які закривають ці слабкі місця. Сканування вразливості допоможе виділити неправильно налаштовані пристрої та дасть змогу виконувати стандартні політики конфігурації. Сканування також перевіряє версії програмного забезпечення та дозволяє автоматизувати встановлення патчів. Ви отримуєте можливість виправляти патчі, що дозволяє пропускати версії у

© Яцюк С. М., Сачук Ю. В., Глинчук Л. Я., Прус Р. Б., Гришанович Т. О.

випадках, коли істотні налаштування можуть бути втрачені за допомогою автоматизованих оновлень програмного забезпечення. Ці можливості конфігураційного та програмного моніторингу поширюються на веб-сервери та брандмауери. Сканер визначить ризикове програмне забезпечення і автоматично видалить несанкціоновані встановлення [6]. Безкоштовне видання пакета включає майже всі можливості двох платних версій, які називаються Professional та Enterprise виданнями. Ви можете отримати 30-денну безкоштовну пробну версію будь-якої з двох платних версій, якщо інвентар вашого пристрою занадто великий, щоб отримати право користуватися безкоштовною версією.

Моніторинг вразливості мережі Paessler за допомогою PRTG (БЕЗКОШТОВНИЙ ПЕРІОД ВИПРОБОВУВАННЯ) [7]. Продукт моніторингу системи Paessler називається PRTG. Це єдиний інструмент моніторингу інфраструктури, який охоплює мережі, сервери та додатки. PRTG – це набір інструментів, і кожна з цих утиліт називається "сенсором". У пакеті є ряд датчиків, які захищають ваш бізнес від мережевих атак.

Будь-яка оцінка безпеки повинна починатися з перевірки всієї вашої існуючої інфраструктури. PRTG виявляє та відслідковує всі ваші мережеві пристрої щодо зміни статусу та умов попередження. Моніторинг мережевого трафіку, наданий PRTG, також може виділити незвичайні дії, які можуть свідчити про вторгнення.

Датчик обнюхування пакетів може використовуватися для глибокої перевірки пакетів, надаючи дані про активність протоколу у вашому трафіку. Це можна визначити за номером порту або джерелом трафіку або пунктом призначення, серед інших ідентифікаторів (рис.3).

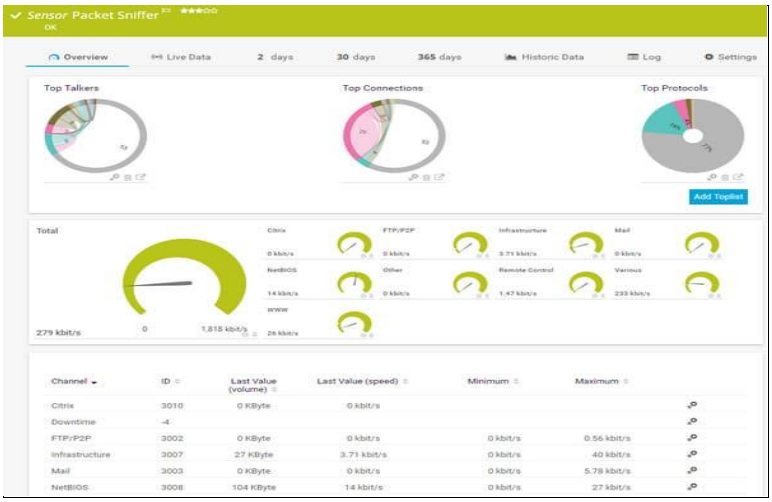

Рис. 3. Екран виходу датчика сніфтера пакетів PRTG

Модуль Syslog Receiver в Paessler PRTG виявить більше функцій сканування безпеки для вашої стратегії захисту системи. Мережева атака залишає паперовий слід і збирає повідомлення журналу подій Syslog та Windows – це перший крок у вашій стратегії сканування вразливості.

PRTG – це чиста система моніторингу, тому вона не включає жодних активних функцій управління та роздільної здатності, таких як управління патчем або управління конфігурацією. Однак він включає деякі додаткові функції оцінки безпеки, такі як утиліта сканування портів та моніторингу.

Будь-який фактор, який контролюється PRTG, може використовуватися як подача в систему оповіщення інструменту. Такі фактори, як гучність повідомлень журналу, суворість повідомлення журналу, дані SNMP Trap та активність порту, можуть бути включені до спеціальних сповіщень.

Повідомлення, що відображаються на екрані зондування здоров'я PRTG Paessler встановлює смуги зарядки для PRTG, які базуються на кількості активованих датчиків. Кожен клієнт отримує доставку повної системи PRTG, але при цьому всі її датчики неактивні. Ви налаштовуєте власну реалізацію, активуючи потрібні датчики. Ви можете використовувати PRTG безкоштовно постійно, якщо активувати до 100 датчиків.

OpenVAS – це всеосяжна система сканування вразливих середовищ з відкритим кодом та управління вразливістю. Це безкоштовно, а його компоненти – це безкоштовне програмне забезпечення, більшість з яких ліцензується згідно з GNU GPL. Коли компанія Nessus стала фірмовим продуктом, її

відключили від відомого (і дорогого) сканера на вразливість Nessus. OpenVAS також є частиною рішення для управління вразливістю мережі Greenbone Network.
OpenVAS використовує автоматично оновлений канал спільноти Тести вразливості мережі (NVT), понад 50 000 і зростаючі. Товарний продукт Greenbone пропонує альтернативний комерційний канал тестів на вразливість, який регулярно оновлюється та має гарантії обслуговування, а також підтримку.
OpenVAS доступний у вигляді пакунків у декількох дистрибутивах Linux, у формі вихідного коду та у вигляді віртуального пристрою, який можна завантажувати у віртуальний комп'ютер у Windows. Він також є частиною Kali Linux.
OpenVAS має веб-інтерфейс, асистент безпеки Greenbone, графічний інтерфейс на основі Qt, робочий стіл Greenbone і CLI.

Рис.4. Інформаційна панель веб-інтерфейсу OpenVAS

Встановлення та використання OpenVAS має значну криву навчання. Незважаючи на те, що OpenVAS – це не просто сканер уразливості, а повноцінна безкоштовна платформа управління відкритим кодом. Крута крива навчання – одна з головних причин **багато адміністраторів мережі шукають альтернативи OpenVAS**, особливо тих, хто віддає перевагу менш практичному підходу, але все ж вимагає надійності грамотного інструменту. Ось чому OpenVAS займає третє місце у нашому списку після пропозицій SolarWinds та Paessler.

Аналізатор безпеки базової лінії Microsoft (MBSA) – це старий штапельний елемент, сканер на вразливість хоста, обмежений домену вразливостей продуктів Microsoft. Він корисний для малого бізнесу, головним чином під керуванням Windows. MBSA – це простий інструмент, який сканує лише машини Windows на конкретні проблеми, що стосуються Microsoft, та основні вразливості та неправильні конфігурації. MBSA може сканувати локальний хост, домен або діапазон IP-адрес (рис. 5)

Рис. 5. **Аналізатор безпеки базової лінії Microsoft**

MBSA може сканувати один або кілька комп'ютерів Windows. MBSA сканує відсутні пакети послуг або оновлення безпеки. Він також сканує адміністративні проблеми в Windows, брандмауері Windows, IIS, SQL Server та Office.
MBSA перевіряє відсутність оновлень та прості адміністративні проблеми.

© Яцюк С. М., Сачук Ю. В., Глинчук Л. Я., Прус Р. Б., Гришанович Т. О.

MBSA створює звіт для кожного відсканованого хоста, з питаннями, позначеними пріоритетом.
Звіт про вразливості в продуктах та послугах Microsoft, таких як SQL Server.
MBSA ще не оновлено для Windows 10, але версія 2.3 значною мірою працює. Для очищення помилкових позитивних даних та виправлення перевірок, які неможливо виконати, потрібно виконати певні налаштування. Наприклад, він подасть хибнопозитивну скаргу на те, що оновлення Windows не ввімкнено.
MBSA не займається вразливими місцями, що не є Microsoft, або складними вразливими місцями, але він простий у використанні і все ще зручний для невеликих магазинів, орієнтованих на Microsoft.

Retina Network Scanner Community Community Edition (**RNSS**) є всеосяжним сканером уразливості, і його можна поєднати з ціною системи управління вразливістю протягом усього життя. RNSS безкоштовний для сканування до 256 IP-адрес [6,7]. Він був розроблений eEye, який зараз є частиною BeyondTrust. База даних про вразливість сканера Retina автоматично оновлюється та визначає вразливості мережі, проблеми з конфігурацією та відсутні патчі, що охоплюють цілий спектр операційних систем, пристроїв, віртуальних середовищ та додатків. Установка проста, а інтерфейс користувача інтуїтивно зрозумілий [6].

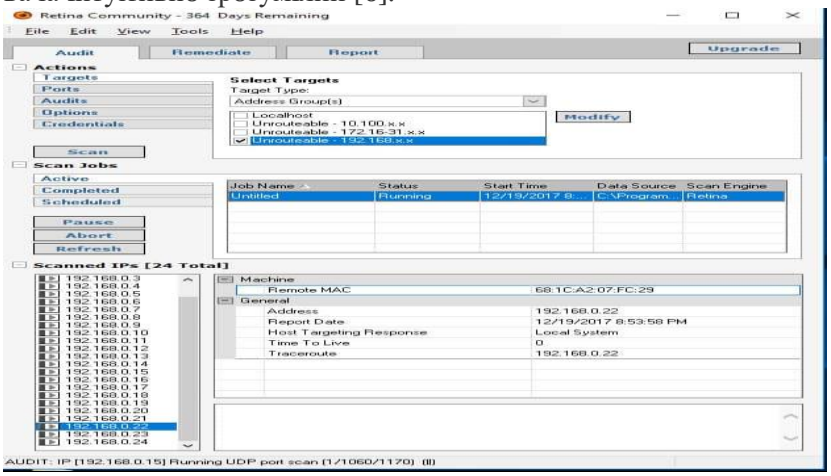

Рис. 6. Інтерфейс користувача Retina

Після запуску сканування через **Аудит** можна перевірити вразливості на **Лікування** вкладки.
На вкладці «Засоби сітківки» перераховані знайдені вразливості. Уразливості можна сортувати та фільтрувати, а також можна розширити до окремих вразливих місць.
Можна створювати різні типи звітів, щоб отримати доступ до результатів сканування поза інструментом.
Nexpose Community Edition – це всебічний сканер на вразливість від Rapid7, власників рамок експлуатації Metasploit. Безкоштовна версія Nexpose обмежена 32 IP-адресами одночасно, і ви повинні повторно подати заявку через рік. Nexpose працює в пристроях Windows, Linux та VM. Він сканує мережі, ОС, веб-додатки, бази даних та віртуальне середовище. Nexpose можна з'єднати з системою управління вразливістю InsightVM Rapid7 для комплексного рішення життєвого циклу управління вразливістю.

Оновлення програмного забезпечення Kaspersky. Один великий недолік безпеки у мережі – це фактично стан підключених до неї комп'ютерів. Розробники програмного забезпечення постійно шукають недоліки в безпеці своїх продуктів і виробляють оновлення для встановлення існуючих клієнтів, щоб закрити будь-які лазівки безпеки. Ці слабкі місця не є наслідком недбалості, коли програмне забезпечення було написане спочатку. Вони виникають через те, що хакери постійно шукають нові способи використання функцій програмного забезпечення для порушення безпеки.
Відстеження існування нових оновлень може зайняти багато часу, тому програма, яка сканує ваш комп'ютер і зберігає список доступних оновлень, заощадить вам багато часу. "Лабораторії Касперського" є провідним виробником антивірусів, і він зробив безкоштовним оновленням програмного забезпечення доступним для користувачів Windows. Інструмент не просто відстежує продукти Kaspersky, але посилається на велику бібліотеку сповіщень про оновлення, які зберігає Касперський. Після завантаження безкоштовного інструменту з сайту Касперського утиліта встановить себе. Перед скануванням комп'ютера інструмент перевіряється на сервері Kaspersky, щоб отримати останній список доступних оновлень. Після закінчення сканування, якщо все в порядку, ви отримаєте повідомлення про відсутність оновлень. Якщо ви знайдете застаріле програмне

© Яцюк С. М., Сачук Ю. В., Глинчук Л. Я., Прус Р. Б., Гришанович Т. О.

забезпечення, програма оновлення програмного забезпечення перелічить їх на екран результатів, подібний до наведеного нижче. Доступний список оновлень.

Висновки та перспективи подальших досліджень

Сканування вразливості, а насправді управління вразливістю – один із аспектів захисту мережі. Сканери можуть виявляти лише вразливості, у яких уже впроваджені тести. Необхідно виробити відчуття нормальної поведінки мережі за допомогою інструментів контролю та пропускної здатності, зокрема інструментів, які дозволяють задавати автоматизовані сповіщення. Мережеві аналізатори та сніфери пакетів є ключовими інструментами для виявлення аномалій. І для адміністратора мережі існує безліч інших засобів захисту, що буде наступною тематикою наших досліджень.

Список бібліографічного опису.

1. Азаров О. Д. Комп'ютерні мережі : навчальний посібник (2013), 371с. АСМ.
2. Буров Є. В. Комп'ютерні мережі: підручник (2010), 262 с. АСМ.
3. Лосев Ю. І. Комп'ютерні мережі: навчальний посібник (2013), 248 с. АСМ.
4. Микитишин А. Г. Комп'ютерні мережі: [навчальний посібник] (2013), 256 с. АСМ.
5. Сайт http://netconfig.ru/ [Електронний ресурс]. Режим доступу до матеріалу сайту: http://netconfig.ru/ server/ids-ips/.
6. Сайт www.ic3.gov [Електронний ресурс]. Режим доступу до матеріалу сайту: http:// www.ic3.gov/ media/IC3-Poster.pdf.
7. Сайт http://ru.wikipedia.org/ [Електронний ресурс. Режим доступу до матеріалу сайту: http://ru. wikipedia.org/wiki/Система_обнаружения_вторжений.

References.

1. Azarov O. Computer networks: a textbook (2013), 371p. ACM.
2. Burov E. Computer networks: a textbook (2010), 262 p. ACM.
3. Losev YI Computer networks: a textbook (2013), 248 p. ACM.
4. Mykytyshyn AG Computer networks: [textbook] (2013), 256 p. ACM.
5. Website http://netconfig.ru/ [Electronic resource]. Mode of access to the site material: http://netconfig.ru/ server / ids-ips /.
6. Website www.ic3.gov [Electronic resource]. Mode of access to the site material: http: // www.ic3.gov/ media / IC3-Poster.pdf.
7. Website http://ru.wikipedia.org/ [Electronic resource. Mode of access to the site material: http: // ru. wikipedia.org/wiki/ Intrusion Detection System.

© Яцюк С. М., Сачук Ю. В., Глинчук Л. Я., Прус Р. Б., Гришанович Т. О.