УДК 004.052.42

В.С. Балацька, М.М. Шабатура

(Львівський державний університет безпеки життєдіяльності)

ДОСЛІДЖЕННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ СКАНЕРОМ ВРАЗЛИВОСТІ NESSUS

На сьогоднішній день комп'ютерні мережі є невід'ємною частиною у нашому повсякденному житті. Як свідчить проведений аналіз мережа надзвичайно вразлива, вона може слугувати місцем витоку інформації, зміни конфігурації налаштувань та модифікації даних зловмисниками. Існує набагато більше загроз тому стан захищеності мережі вимагає значної уваги щодо забезпечення рівня захисту мережі з метою підтримування конфіденційності та цілісності даних. Для перевірки рівня безпеки та зміцнення мережі організації необхідно регулярно проводити оцінку вразливості всієї мережі. Для пошуку слабких місць використовують сканери вразливості, які корисні для виявлення вад безпеки у кожній окремій системі, а також у всій мережі загалом.

Мета роботи – дослідити комп'ютерну мережу на наявність вразливих місць за допомогою сканера Nessus Professional.

Методи дослідження – сканування мережі сканером вразливості Nessus Professional.

Для проведення досліджень було використано сканер вразливості Nessus Professional від компанії Tenable Network Security, який є у вільному доступі. З'ясовано, що сканер Nessus Professional має кращий функціонал і технічні характеристики у порівнянні з іншими доступними сканерами. Єдиним мінусом сканера є його вартість користування протягом року, а також сканування малої кількості хостів у мережі водночас (понад 100 хостів). Після успішного встановлення сканера, здійснювався його огляд від моменту запуску до формування звітів про результати тестування хостів. У роботі тестувалась мережа Львівського державного університету безпеки життєдіяльності. У звіті після сканування, що відображається у HTML форматі, можна побачити: деталі сканування по кожному хосту; кількість та характер вразливостей; інформаційну панель щодо виправленню помилок. За результатами тестування було виявлено вразливості низького, середнього та високого рівнів небезпек, у сумі – 376. Проводився аналіз вразливостей на підставі отриманих результатів, а саме: короткий опис та спосіб вирішення проблеми.

Ключові слова – комп'ютерна мережа, вразливість, сканер вразливості, Nessus Professional, сканування портів.

V.S.Balatska, M.M. Shabatura

(Lviv State University of Life Safety)

EXPLORATION OF COMPUTER NETWORK BY VULNERABILITY SCANNER NESSUS

For today, computer networks are an integral part of our daily lives. As the analysis shows, the network is extremely vulnerable, it can serve as a place of information leakage, changes of configuration of settings and modification of data by the attackers. There are many more threats, and the security of the network requires a great deal of attention to ensure the security of the network in order to maintain the confidentiality and integrity of the data. Organizations must regularly assess the vulnerability of the entire network to test the security level and strengthen the network. We use vulnerability scanners to find weaknesses, which are useful for detecting security vulnerabilities on a case-by-case basis and across the network as a whole.

The purpose of the work is to explore the computer network for vulnerabilities using the Nessus Professional scanner.

Research Methods – network scanning by Nessus Professional vulnerability scanner.

The Nessus Professional vulnerability scanner from Tenable Network Security, which is freely available, was used for the research. The Nessus Professional scanner has been found to have better functionality and performance than other available scanners. The only downside to the scanner is its cost per year, as well as scanning a large number of hosts on the network at a time (over 100 hosts). After the scanner was successfully installed, carried out it was inspected from the moment it was launched to the generation of host test reports. For the work, the Lviv State University of Life Safety network was tested. In the post-scan report, which is displayed in HTML format, you can see scan details for each host; the number and nature of vulnerabilities; the error correction dashboard. According to the results of testing, vulnerabilities of low, medium and high levels of hazards were identified, totaling 376. Vulnerabilities were analyzed based on the obtained results, namely: a brief description and a way to solve the problem.

Keywords – computer network, vulnerability, vulnerability scanner, Nessus Professional, port scanning.

Вступ. З зростанням прогресу в галузі інформаційних технологій безпека комп'ютерних систем викликає більш серйозне занепокоєння. Зазвичай більшість галузей програмного забезпечення, що розвиваються, не знають про різні помилкові уявлення про безпеку, які автоматично існують у системі завдяки мовам програмування, оскільки їх намір зробити хороше програмне забезпечення, яке працює безперебійно і дає бажаний результат, не враховуючи недоліки безпеки; для забезпечення безпеки та безпеки кожної людини дуже важливо планувати нові стратегії та методології [1], які враховуватимуть порушення безпеки, до яких схильний користувач. Не тільки програмне забезпечення, розроблене з недоліками, робить користувача вразливим до атак, найчастіше мережа також стає ключовим фактором за рахунок погіршення аспекту безпеки користувачів. Оцінка та усунення вразливих місць вимагає знання та глибоке розуміння цих вразливостей чи недоліків у безпеці. Вразливість у безпеці системи, яка може призвести до того, що зловмисники експлуатують систему іншими способами [2]. Було впроваджено багато інших методів для виявлення цих вразливих місць та різних підходів до усунення цієї вразливості. Деякі з них є методом генерації графіків атак, методи статичного аналізу для виявлення вразливих ситуацій, які є досить популярними і відомими сьогодні.

Об'єкт тестування

Для виконання роботи вибрано комп'ютерну мережу Львівського державного університету безпеки життєдіяльності. Мережею охоплені три корпуси: головний та навчально-науковий інститут психології та соціального забезпечення, що розташовані на Клепарівській, 35, а також корпус, що знаходиться на Клепарівській, 22.

При такій структурі мережі, будь-який запит ресурсу з Internet проходить логічний ланцюжок:

1. Запит з під мережі корпусу до підлеглого маршрутизатора;
2. Запит від підлеглого маршрутизатора до головного маршрутизатора;
3. Якщо це HTTP-запит, то він переадресовується до проксі-сервера;
4. Якщо результатів даного запиту немає в кеші проксі-сервера, то відправляємо запит проксі-сервером знову до головного маршрутизатора;
5. Пересилаємо запит на наш основний шлюз Internet УАРНЕТ.
6. Приходить відповідь;
7. Відповідь пересилається на проксі сервер;
8. Проксі сервер пересилає відповідь на головний маршрутизатор;
9. Головний маршрутизатор пересилає відповідь на підлеглий маршрутизатор;
10. Підлеглий маршрутизатор пересилає запит на вузол, що запитав даний ресурс.

Фізично комп'ютерна мережа є суттєво завантажена, тому що вона реалізована на основі технології оптоволоконного зв'язку і має достатню пропускну ширину каналу – до 1 Гбіт/с. При цьому, у зв'язку з подібною реалізацією маршрутизації пакетів між вузлами внутрішньої мережі, запит і відповідь проходять по каналах зв'язку у різних напрямках.

Аналіз функціоналу сканера Nessus

Nessus Professional – сканер вразливостей для невеликих організацій, які включають в

себе до 50 робочих машин, а також для аудиторів, які здійснюють аналіз безпеки своїх замовників. Продукт дає змогу оцінювати конфігурації, знаходити уразливості і, в разі виявлення проблем під час налаштування інфраструктури, запобігати мережевим атакам [3].

До основних можливостей Nessus Professional можна віднести:

- широкий вибір режимів аналізу захищеності;
- гнучкі налаштування параметрів аналізу вразливостей;
- управління оновленнями продукту та контенту;
- складання звітів по заданим критеріям;
- сумісність з плагінами Nessus;
- автоматичні щоденні оновлення системи.

Можливі типи аналізу захищеності. Nessus Professional надає можливість проведення перевірок для забезпечення відповідності нормативним вимогам FFIEC, HIPAA, NERC, PCI DSS, а також галузевим стандартам CERT, CIS, COBIT / ITIL, DISA STIG. Таке охоплення забезпечують понад 450 встановлених шаблонів [4].

- сканування вразливостей. Оцінка систем, мереж і додатків на наявність вразливостей;
- аудит конфігурації. Перевірка відповідності мережевих активів політикам і галузевим стандартам;
- виявлення шкідливих програм. Також виявлення потенційно небажаного і некерованого програмного забезпечення;
- сканування веб-додатків. Виявлення вразливостей веб-серверів, служб і вразливостей OWASP;
- гнучкі пошукові запити. Визначення закритої інформації в системах або документах;
- аудит системи управління. Сканування систем SCADA, вбудованих пристроїв і додатків ICS;
- підтримка хмарних обчислень. Оцінка слабких місць конфігурації хмарних рішень, таких як Amazon Web Services, Microsoft Azure і Rackspace.

Можливості аналізу захищеності [5]. Система підтримує кілька варіантів сканування, таких як підтримка віддаленого і локального сканування активів, сканування з аутентифікацією, режим автономного аудиту конфігурації мережевих пристроїв.

- виявлення і сканування активів. Мережеві пристрої, включаючи брандмауери нового покоління, операційні системи, бази даних, веб-додатки, віртуальні і хмарні середовища;
- сканування мереж. Сканування на IPv4, IPv6 і гібридних мережах;
- сканування за розкладом. Сканування з налаштуванням за часом і частоті запуску;
- вибіркове повторне сканування хоста. Виконання повторного сканування всіх або вибіркових хостів;
- автоматичний аналіз сканування. Рекомендації по відновленню та налагодженню сканування.

Сканування мережі

Засоби пошуку вразливостей можуть функціонувати 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, в першу чергу, з універсальністю використовуваних протоколів. Вивченість і повсюдне використання таких протоколів, як IP, TCP, HTTP, FTP, SMTP дають змогу перевіряти захищеність інформаційної системи з високим ступенем ефективності. Програма Nessus дає змогу побачити «дірки» мережі, «слабкі» хости, тощо [6]. Вигляд програми Nessus під час сканування наведено рис. 1.

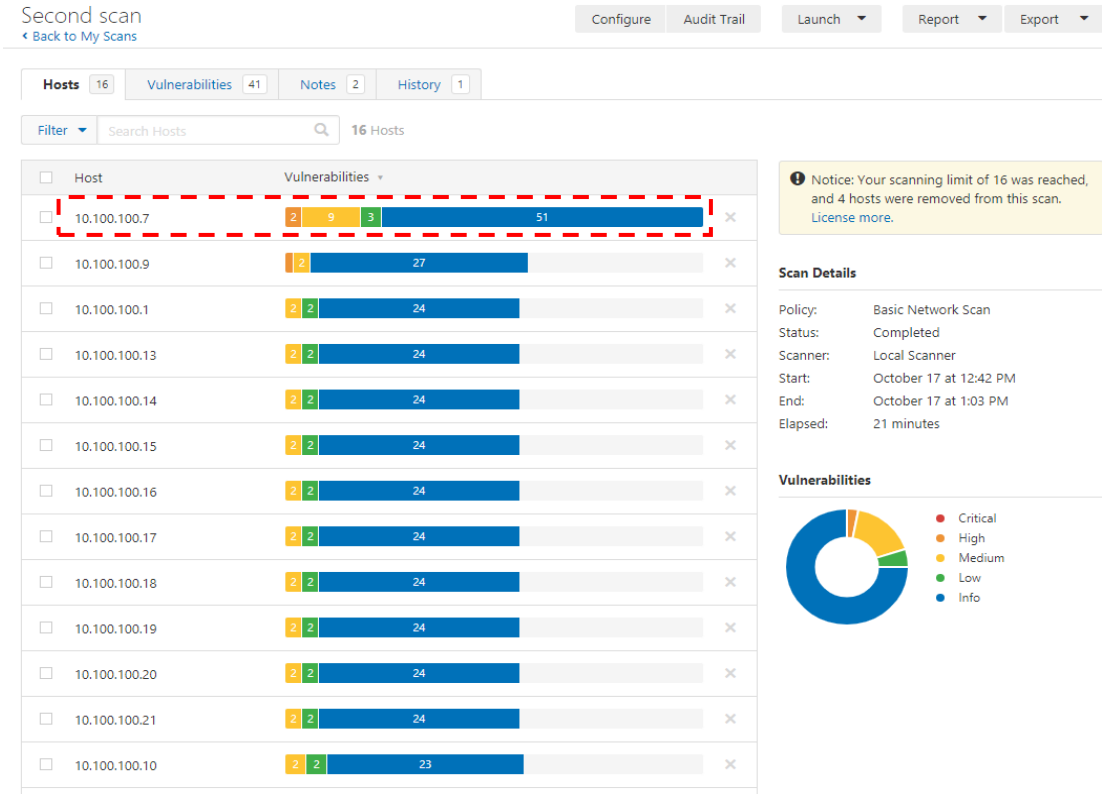
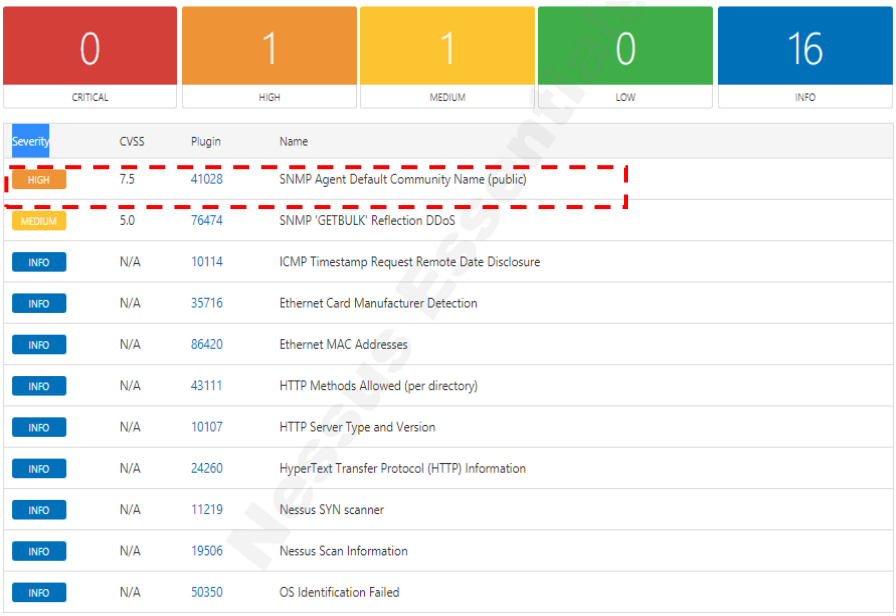


Рисунок 1 – Зображення програми під час сканування

Як видно із рис. 1 досліджувана мережа немає жодної вразливості критичного рівня, 3 вразливостей – високого рівня, 33 – середнього, 25 – низького рівнів та 310 – загальні вразливості інформативного рівня, всього виявлено вразливостей – 376.

У звіті після сканування, відображається результат по кожному хості, кількість та характер вразливостей, інформаційна панель з виправленням помилок. Розглянемо кілька вразливостей, які отримали у результаті сканування (рис. 2)

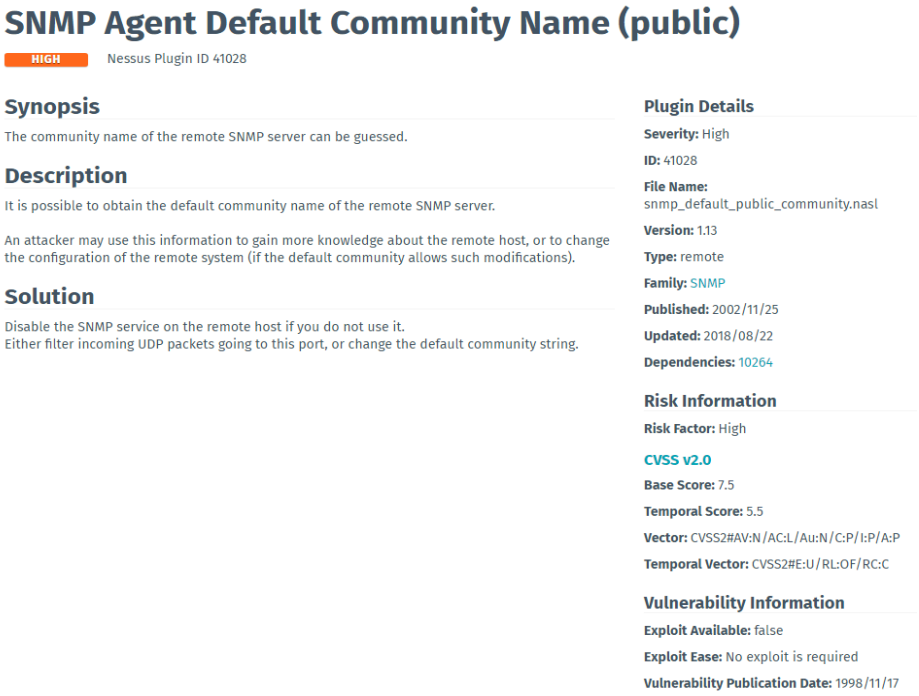


0	1	1	0	16
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS	Plugin	Name
HIGH	7.5	41028	SNMP Agent Default Community Name (public)
MEDIUM	5.0	76474	SNMP 'GETBULK' Reflection DDoS
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	50350	OS Identification Failed

Рисунок 2 – Опис вразливостей хоста 10.100.100.7

На рис. 2 пунктиром виділено вразливість з найвищим рівнем – ***SNMP Agent Default Community Name (public)*** (Ім'я спільноти для агента SNMP (загальнодоступне)). Детальний опис цієї вразливості наведено на рис. 3



SNMP Agent Default Community Name (public)

HIGH Nessus Plugin ID 41028

Synopsis

The community name of the remote SNMP server can be guessed.

Description

It is possible to obtain the default community name of the remote SNMP server.

An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications).

Solution

Disable the SNMP service on the remote host if you do not use it.
Either filter incoming UDP packets going to this port, or change the default community string.

Plugin Details

Severity: High
ID: 41028
File Name: snmp_default_public_community.nasl
Version: 1.13
Type: remote
Family: SNMP
Published: 2002/11/25
Updated: 2018/08/22
Dependencies: 10264

Risk Information

Risk Factor: High

CVSS v2.0

Base Score: 7.5
Temporal Score: 5.5
Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P
Temporal Vector: CVSS2#E:U/RL:OF/RC:C

Vulnerability Information

Exploit Available: false
Exploit Ease: No exploit is required
Vulnerability Publication Date: 1998/11/17

Рисунок 3 – Детальний опис вразливостіID 41028

Ця вразливість дає змогу отримати ім'я спільноти за замовчуванням віддаленого сервера SNMP. Зловмисник може використовувати цю інформацію для отримання відомостей про віддалений хост або для зміни конфігурації віддаленої системи (якщо спільнота за замовчуванням дозволяє такі зміни).

Наступна вразливість середнього рівня – ***SNMP 'GETBULK' Відбиття DDoS*** (рис. 4)**.**

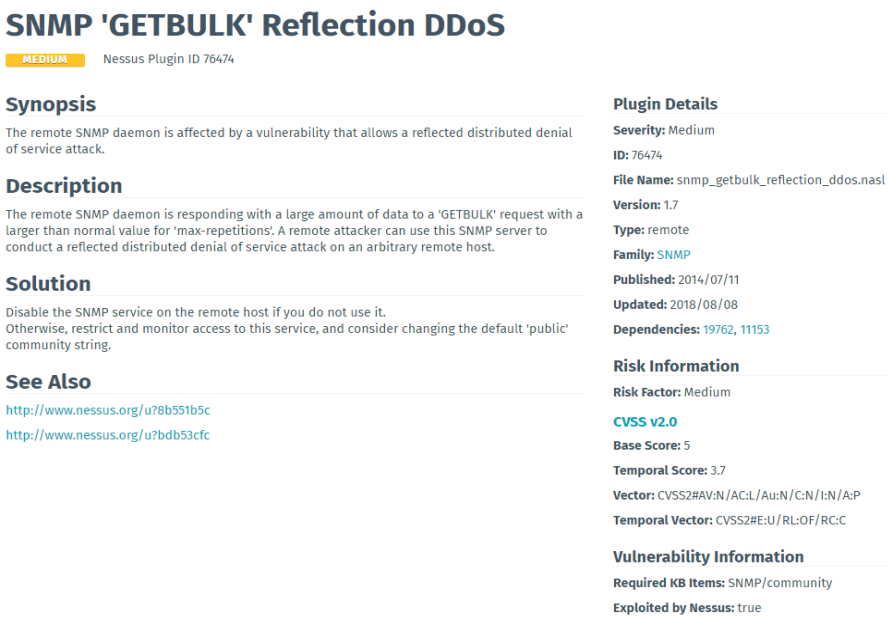


Рисунок 4 – Детальний опис вразливості ID76474

Опис вразливості: ***SNMP 'GETBULK'*** відповідає з великою кількістю даних на запит "GETBULK" з великим значенням, ніж нормальне значення, для "максимальних повторів". Віддалений зловмисник може використовувати цей SNMP-сервер для здійснення відображеної розподіленої атаки відмови в службі на довільному віддаленому хості.

Вразливість низького рівня типу ***SSH Weak Algorithms Supported***, наведено на рис. 5.

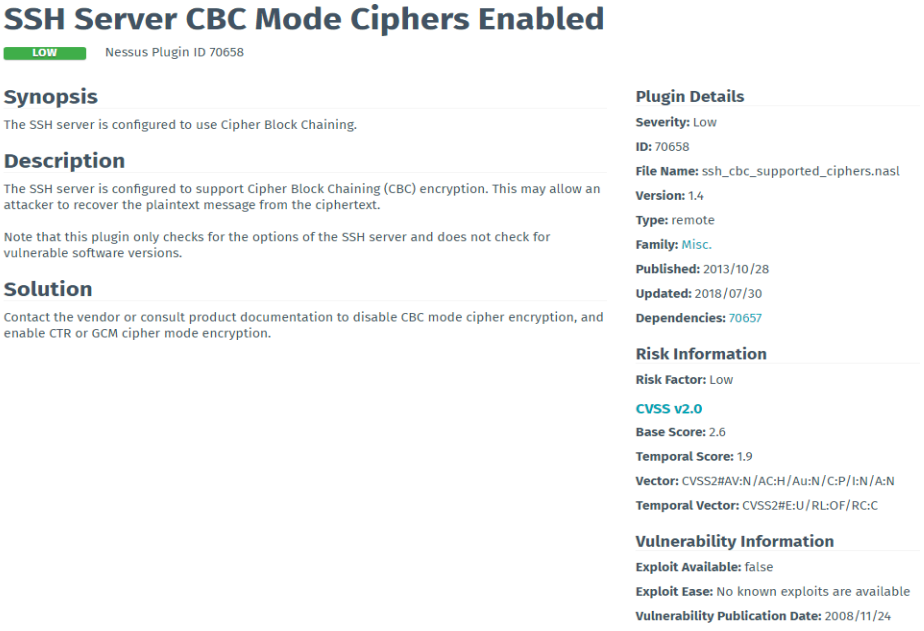


Рисунок 5 – Опис вразливості про використання ланцюга блоків шифрів

З цією вразливістю, Nessus виявив, що віддалений сервер SSH налаштований на використання шифру потоку Arcfour або взагалі немає шифру. RFC 4253 не рекомендує використовувати Arcfour через проблему зі слабкими клавішами. Рішенням даної вразливості є, що під час шифрування необхідно узгодити алгоритм шифрування та ключ-обмін. Коли шифрування діє, довжина пакету, довжина поля, корисне навантаження та заливка кожного

пакету, мають бути зашифровані за заданим алгоритмом. Зашифровані дані у всіх пакетах, що надсилаються в одному напрямку, мають бути єдиним потоком даних. Наприклад, вектори ініціалізації повинен бути переданим від кінця одного пакета до початку наступного пакету. Усі шифри потрібно використовувати з ефективним ключем довжини 128 біт і більше. Шифри в кожному напрямку обов'язково працюватимуть незалежно один від одного.

Висновок: у роботі здійснювалось дослідження комп'ютерної мережі Львівського державного університету безпеки життєдіяльності сканером вразливості Nessus. У результаті сканування виявлено ряд вразливостей, які можуть спричинити серйозні наслідки, такі як витік інформації, модифікація даних, зміна налаштування мережі, а найкритичніше – зупинка функціонування мережі. Отримані результати можуть бути використані адміністратором безпеки мережі для роботи щодо ліквідування визначених вразливостей та організації захисту мережі.

Список літератури:

1. Common Vulnerabilities and Exposures (CVE) [Електронний ресурс] – Режим доступу до ресурсу: https://cve.mitre.org
2. Golnaz Elahi, Eric Yu, and Nicola Zannone, "Security Risk Management by Qualitative Vulnerability Analysis", IEEE, Third International Workshop on Security Measurements and Metrics, 2011.
3. Nessus professional [Електронний ресурс] – Режим доступу до ресурсу: http://www.tenable.com/products/nessus-vulnerability-scanner
4. A Brief Introduction to the Nessus Vulnerability Scanner [Електронний ресурс] – Режим доступу до ресурсу: https://resources.infosecinstitute.com/a-brief-introduction-to-the-nessus-vulnerability-scanner/#gref\
5. Tenable community [Електронний ресурс] – Режим доступу до ресурсу: https://community.tenable.com/s/article/Operating-System-identification-using-Plugin-11936
6. Використання сканера безпеки Nessus [Електронний ресурс] – Режим доступу до ресурсу: http://system-repair.net/2012/05/ispolzovanie-skanera-bezopasnosti-nessus/

References:

1. Common Vulnerabilities and Exposures (CVE) [Elektronnyi resurs] – Rezhym dostupu do resursu: https://cve.mitre.org
2. Golnaz Elahi, Eric Yu, and Nicola Zannone, "Security Risk Management by Qualitative Vulnerability Analysis", IEEE, Third International Workshop on Security Measurements and Metrics, 2011.
3. Nessus professional [Elektronnyi resurs] – Rezhym dostupu do resursu: http://www.tenable.com/products/nessus-vulnerability-scanner
4. A Brief Introduction to the Nessus Vulnerability Scanner [Elektronnyi resurs] – Rezhym dostupu do resursu: https://resources.infosecinstitute.com/a-brief-introduction-to-the-nessus-vulnerability-scanner/#gref\
5. Tenable community [Elektronnyi resurs] – Rezhym dostupu do resursu: https://community.tenable.com/s/article/Operating-System-identification-using-Plugin-11936
6. Vykorystannia skanera Nessus [Elektronnyi resurs] – Rezhym dostupu do resursu: http://system-repair.net/2012/05/ispolzovanie-skanera-bezopasnosti-nessus/