ДОДАТОК А

Графічний матеріал атестаційної роботи

Харківський національний університет радіоелектроніки

Атестаційна робота

«Методи оцінки захищеності комп'ютерної мережі при тестуванні на проникнення»

Виконав:
Студ. гр. КСМзм-19-1
Рязанін С.Г.

Керівник:
к.т.н, доцент
Голубничий Д.Ю.

Мета та завдання атестаційної роботи

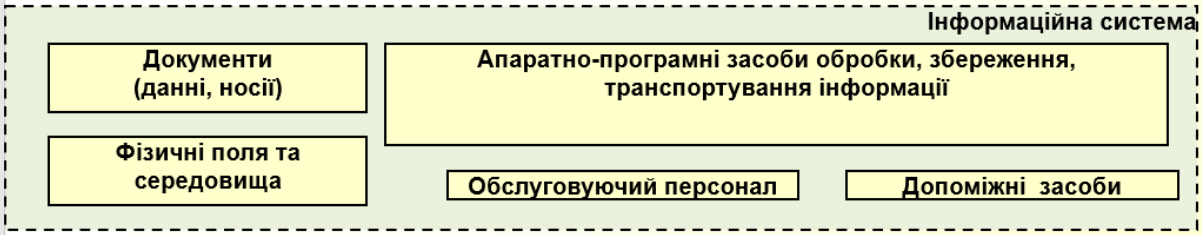
Мета атестаційної роботи :

Підвищення рівня захищеності комп’ютерної мережі за рахунок використання послуги тестування на проникнення, яка дозволяє здійснити санкціонований обхід існуючого комплексу засобів захисту власних інформаційних систем та виявити в них слабкі місця.

Науково-технічна задача, що вирішується у атестаційної роботі :

- Проведення аналізу захищеності комп’ютерної мережі як об’єкта кібербезпеки.
- Проведення аналізу вразливостей інформаційних систем та оцінка їх критичності для комп’ютерних мереж.
- Побудова методу оцінки захищеності комп'ютерної мережі за рахунок використання експлойтів при тестуванні на проникнення

Аналіз стану та вивчення вимог до СЗІ для ІС



1. Визначення інформаційних ресурсів, які підлягають захисту.

7. Здійснення контролю функціонування і управління системою захисту.

2. Виявлення повної множини загроз кібербезпеки ІР, які підлягають захисту.

Аналіз стану та вивчення вимог до СЗІ

6. Визначення якості реалізованої системи захисту.

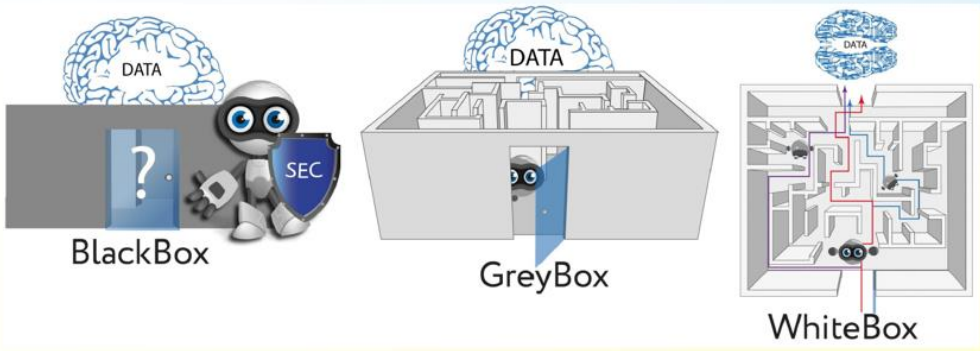
3. Проведення оцінки вразливості і ризиків для ІР, які підлягають захисту, при виявленій множині загроз.

5. Реалізація проекту (плану) захисту інформації.

4. Розробка проекту (плану) системи захисту інформації, що знижує за обраним критерієм ризики для ІР, які підлягають захисту, при виявленій множині загроз.

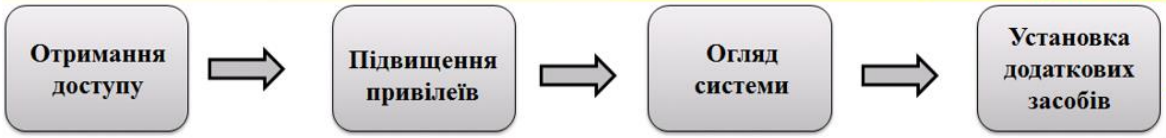
3

Методи тестування на проникнення



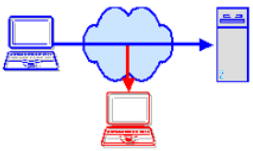
Життєвий цикл тестування

Етапи тестування на проникнення



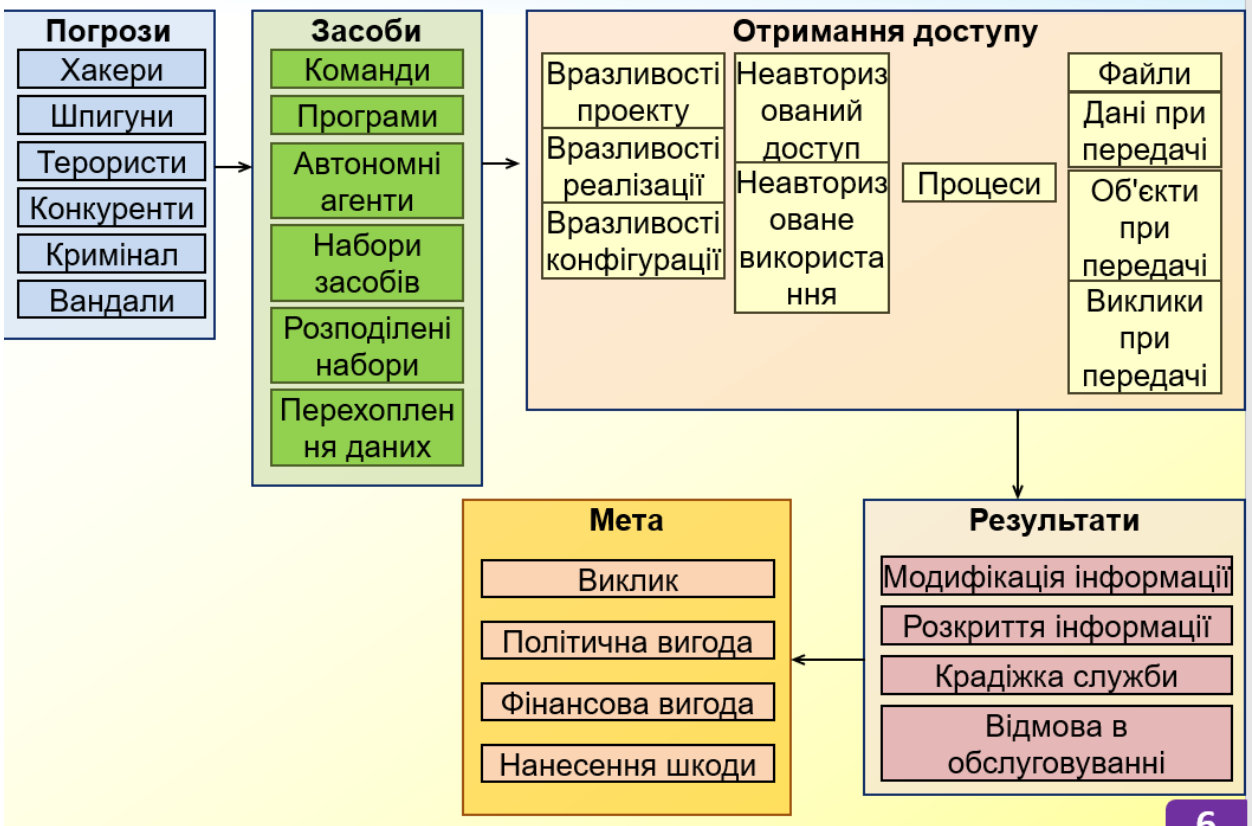
4

Класифікація можливих видів мережевих атак

Опис	Мнемонічна схема
Destruction. Атака на доступність руйнування. Руйнування інформації та/або мережевих ресурсів.	
Interruption. Атака на доступність. Переривання обслуговування, мережа недоступна або непридатна до використання	
Removal. Атака на доступність. Крадіжка, видалення або втрата інформації і/або інших ресурсів.	
Corruption. Атака на цілісність. Несанкціонована модифікація цінної інформації.	
Disclosure. Атака на конфіденційність. Несанкціонований доступ до конфіденційної інформації	

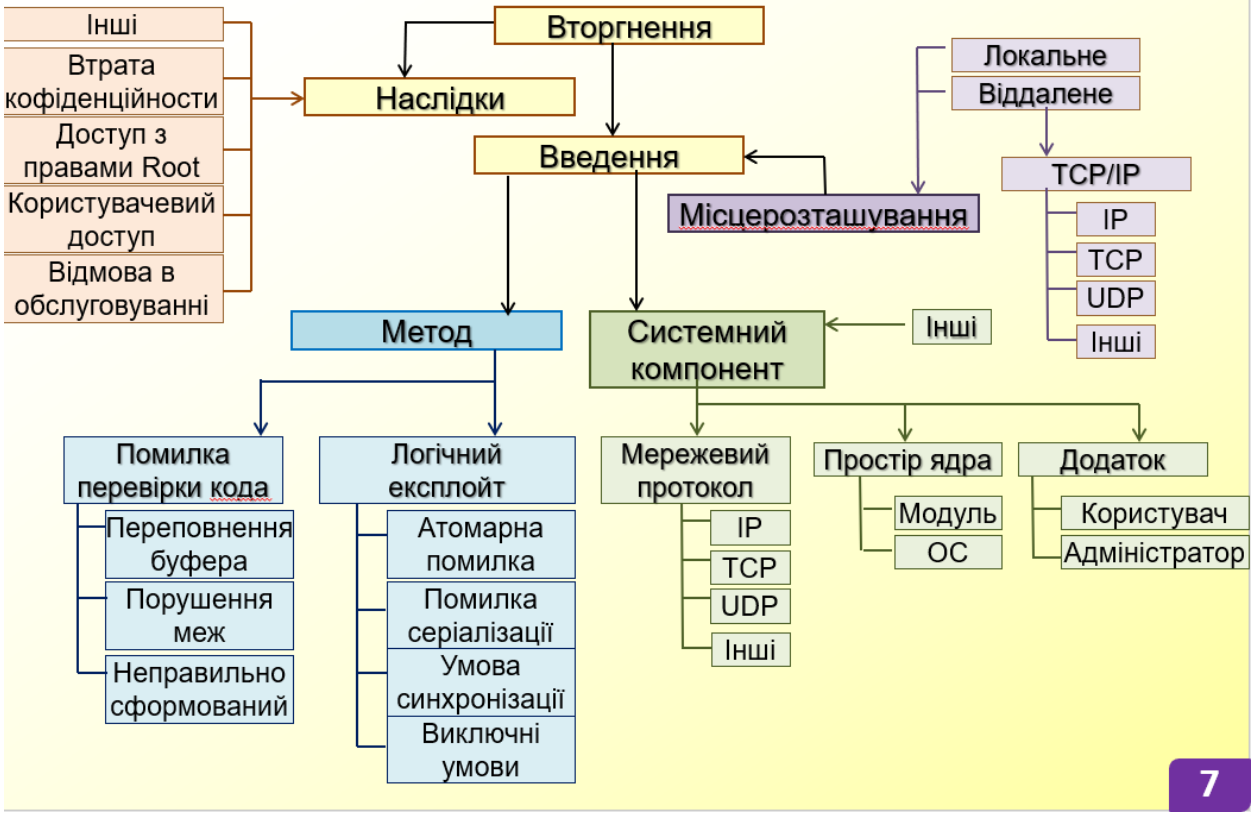
5

Таксономія атак Ховарда



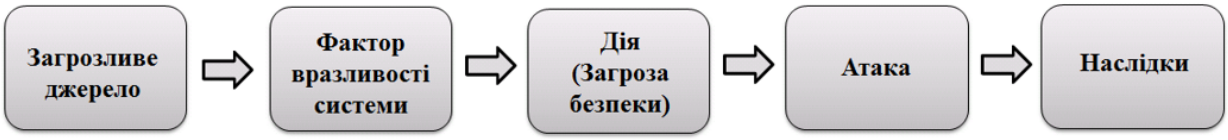
6

Повна онтологія атак



7

Логічний ланцюг трансформації інформації



Метрика	Можливі значення	
Вектор доступу (AV)	AV: L	Локальний
	AV: A	Сусідня мережа
	AV: N	Віддалений
Автентифікація (AC)	AC: H	Висока
	AC: M	Середня
	AC: L	Низька
Вплив на конфіденційність (CI)	CI: N	Ні
	CI: P	Істотне
	CI: C	Критичний
Вплив на цілісність (II)	II: N	Ні
	II: P	Істотне
	II: C	Критичний
Вплив на доступність (AI)	AI: N	Ні
	AI: P	Істотне
	AI: C	Критичний

8

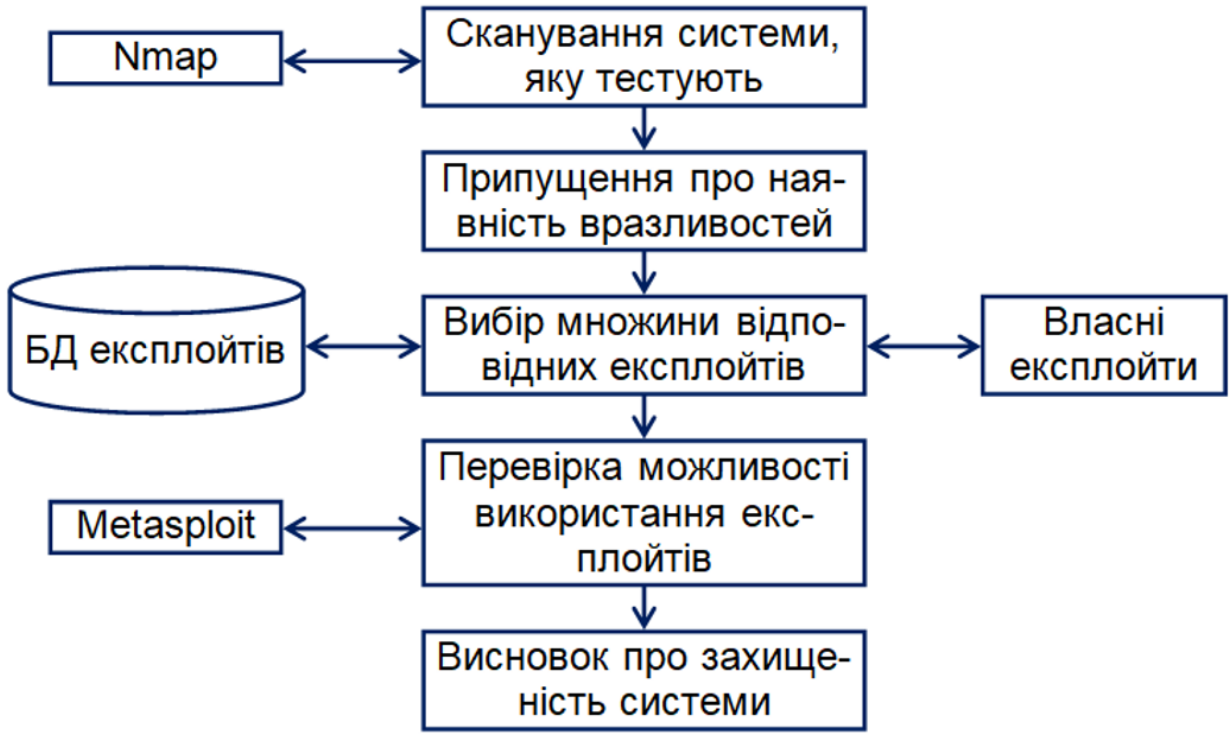
Складові експлойта

- Параметри експлойта
- Обробник мережевих з'єднань
- Shell код / корисне навантаження
- Побудовник запиту
- Стандартний оброблювач

Експлойт (Exploit) – це програма, послідовність команд або частина програмного коду, що використовують вразливості в програмному забезпеченні для проведення атаки на інформаційну систему

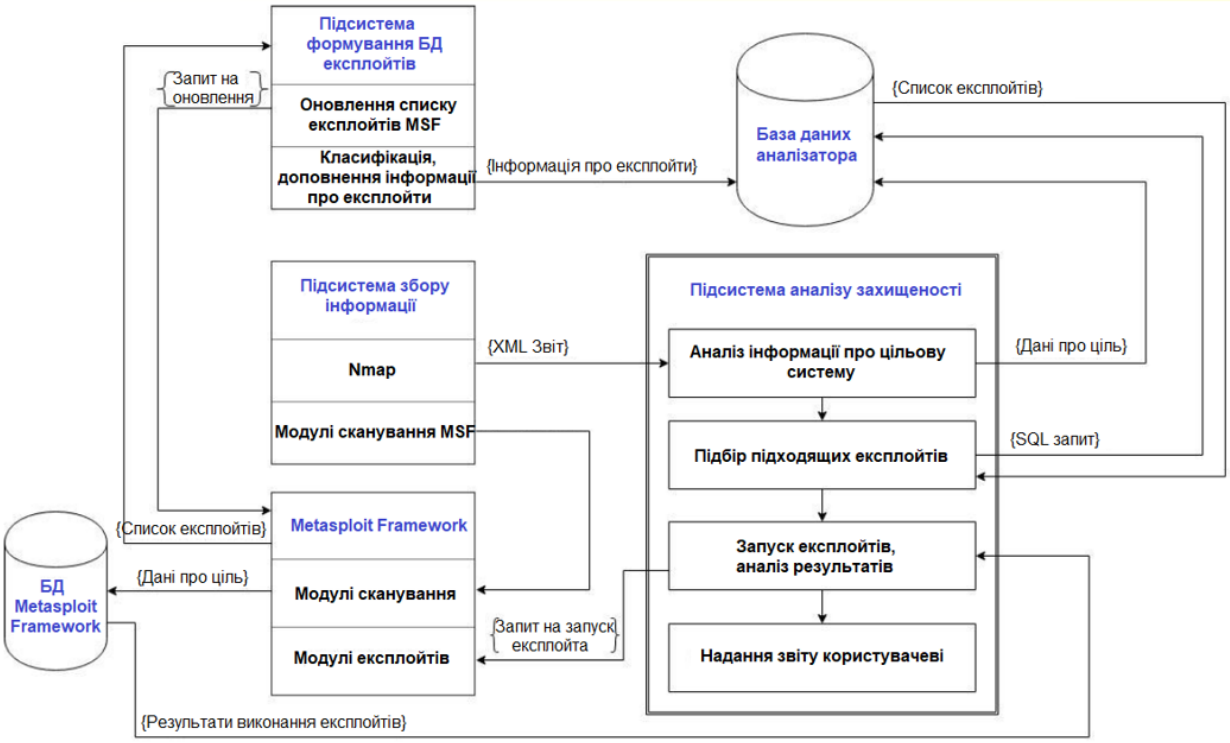
9

Схема автоматизованого тестування на проникнення



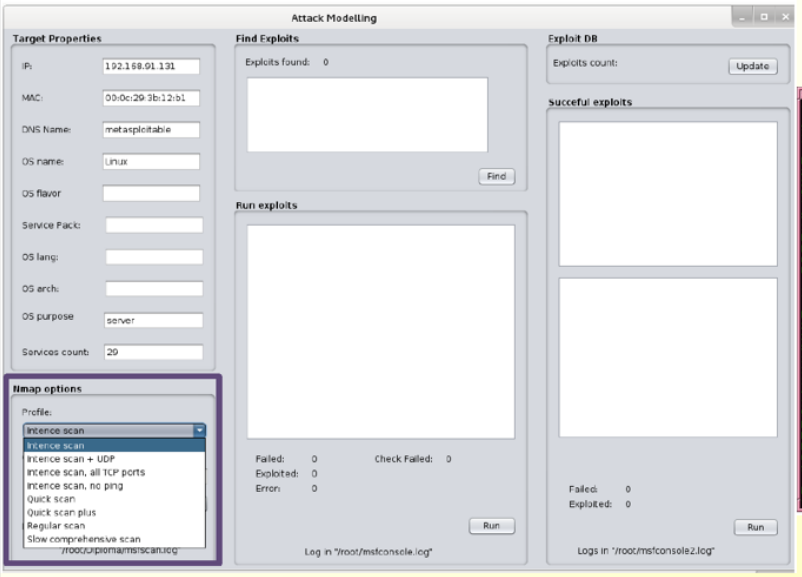
10

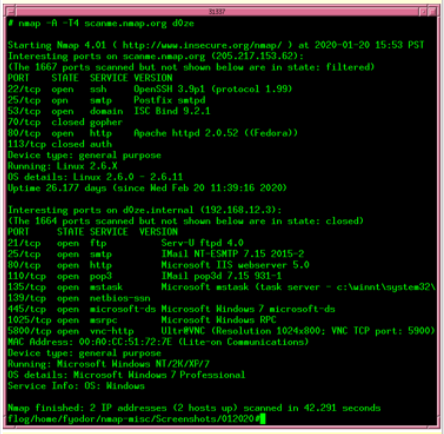
Архітектура розробленої системи тестування на проникнення



11

Приклад збору відомостей утилітою Nmap





12

Результати аналізу різних ОС на хостах комп'ютерної мережі

Операційні системи	Кількість виявлених запущених служб і відкритих портів	Кількість відібраних експлойтів для цільової системи	Кількість успішних експлойтів	Час виконання	
				Загальний, хв. сек.	Нормований, сек/експл.
Windows 10	11/11	45/1450	1/1	3 хв 02 сек	3,75
Windows 7	10/10	39/1450	3/3	2 хв 30 сек	3,84
Windows Vista	9/9	33/1450	2/3	3 хв 06 сек	5,6
Windows XP SP3	9/9	231/1450	1/1	20 хв 02 сек	5,19
Windows Server 2008 R2	10/10	37/1450	2/2	2 хв 46 сек	3,98
Windows Server 2003	4/4	95/1450	3/4	5 хв 30 сек	3,45
Mac OS X High Sierra	4/4	37/1450	1/1	5 хв 30 сек	3,75
Mac OS X Sierra	5/5	65/1450	1/1	4 хв 27 сек	4,23
Linux Mint 17	2/2	84/1450	0/0	4 хв 34 сек	3,25
CentOS 7	1/1	8/1450	1/1	0 хв 41 сек	3,17
Metasploitable 2	30/30	283/1450	7/7	25 хв 45 сек	5,43

13

Методи тестування на проникнення

Метод Open Source Security Testing Methodology

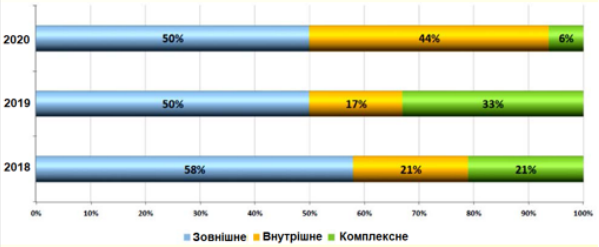
Метод Information Systems Security Assessment Framework

Метод NIST Special Publications 800-115

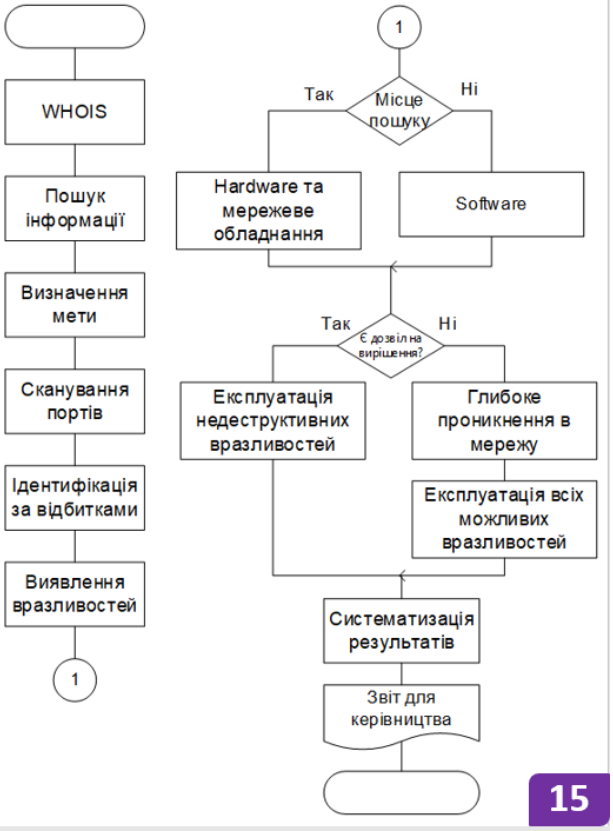
14

Структурно-логічна схема та алгоритм проведення pentest

Структурно-логічна схема pentest

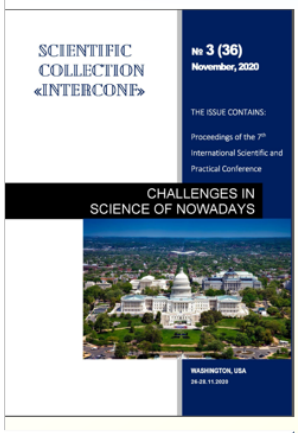


Підходи до проведення pentest



15

Апробація результатів



Голубничий Д.Ю. Технології аудиту кібербезпеки інформаційних систем / Д.Ю.Голубничий, О.В. Коломійцев, В.Ф.Третяк, С.Г.Рязанін // Scientific Collection «InterConf», (36): with the Proceedings of the 7th International Scientific and Practical Conference «Challenges in Science of Nowadays» (November 26 - 28, 2020) in Washington, USA: EnDeavours Publisher, 2020. – Pp. 333 – 342. https://ojs.ukrlogos.in.ua/index.php/interconf/issue/view/26-28.11.2020/396.

16

Висновки

В результаті даної роботи були:

1. **Проаналізовані підходи до проведення аудиту кібербезпеки** за рахунок технології тестування проникнення. Таким чином, на основі приведених результатів досліджень можливо сформулювати основні завдання, рекомендації та базові пропозиції щодо підходів до забезпечення кібербезпеки, яка циркулює в комп'ютерних мережах.
2. **Проведено аналіз вразливостей інформаційних систем** та оцінка її критичності для комп'ютерних мереж. Аналіз дав можливість визначити найбільш ефективний підхід і використати його з метою оптимізації параметрів систем захисту.
3. Проведено аналіз існуючих методів тестування засобів захисту інформації, обрані допоміжні інструменти, з використанням яких була **розроблена архітектура системи моделювання атак і реалізований прототип програмного засобу.**

Розроблену систему можна вдосконалити в декількох напрямках:

✓можливість аудиту цілої комп'ютерної мережі, а не тільки окремого одного хоста;

✓комбінування декількох мережевих сканерів;

✓автоматизація процесів після успішної експлуатації системи.