Чи може тестування на проникнення (Penetration Test) спричинити збій у бізнес-процесах і виток конфіденційної інформації?

Доповідач: ***Шишков Яків Анатолійович***
Керівник Департаменту інформаційної безпеки,
Архітектор рішень з інформаційної безпеки, IBM
CISSP, CISM, CCSP, CEH, MCP

Penetration Test - визначення та основна мета

Визначення: *Тест на проникнення (також Penetration Test, PenTest, пентест або етичний хакінг), це практика тестування комп'ютерних систем, мереж, програмних додатків (включаючи WEB-додатки) та сервісів з метою знаходження вразливостей у системі безпеки, які може використати потенційний абстрактний зловмисник.*

Основна мета пентесту: *повна імітація дій кібер-зловмисників, але з істотною різницею – без нанесення шкоди клієнту або здійснення витоку його інформації.*

Переваги для бізнесу: випередити зловмисників у виявленні та експлуатації вразливостей у інформаційній безпеці замовника, збільшуючи стабільність бізнесу.

Примітка: *слід відрізняти penetration test від сканування на вразливості за допомогою автоматичних сканерів, таких як Nessus, Nexpose, Qualys, OpenVAS й т.ін.*

Penetration Test - Навіщо робити?

«Кожні 1000 рядків коду містять від 15 до 50 дефектів»

(*“Code Complete”, Steve McConnel*)

Цей показник відомий як defects per KLOK (1000 lines of code)

Продукти Miscrosoft містять близько 0,5 defects per KLOK.

Microsoft Windows 10 містить близько 50 млн. рядків коду.

Penetration Test – Фази процесу

Фази типового тесту на проникнення:

- Розвідка: збір інформації про цілі (активний та/або пасивний)
- Сканування цілей
- Формування переліку цілей
- Отримання доступу
- Ескалація привілеїв
- Експлуатація доступу
- Приховування слідів (опціонально)
- Створення звіту та інформування замовника за результатами

Penetration Test – Організація процесу

На цьому етапі необхідно обговорити із замовником, можливий вплив на продуктивні системи замовника та його наслідки.

Мають бути визначені:

- цілі тесту
- обсяг
- строки та «вікна досяжності» систем
- детальні умови виконання тесту
  - чого не можна робити? (DoS, Fuzzng, etc.)
  - чи дозволено використовувати «соціальну інженерію»?
  - чи тестується фізичне середовище?
  - порядок взаємодії з власниками систем, IT, безпекою
  - й т.ін.

Penetration Test – Підходи

Різновид	Переваги	Недоліки
Announced Penetration Tests	- Орієнтовані на системи - Майже виключають «людський фактор» з боку персоналу замовника - Дозволяють економити час на обминання деяких систем безпеки	- Дозволяють персоналу замовника «підготуватись» до тесту - Можуть не показати реальний стан захищеності систем
Unannounced Penetration Tests	- Орієнтовані на результат - Показують реальний стан систем - Дозволяють гнучко змінювати вектор атаки	- Реакція персоналу може заважати, або навіть спричинити зупинку тесту та нести певні ризики для пенстестерів

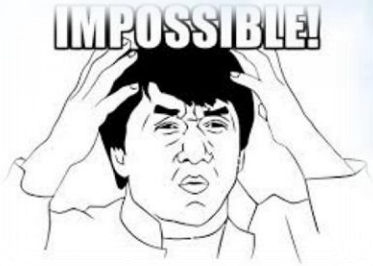
Penetration Test – Можливі проблеми та наслідки

- ✓ Непередбачуваний вплив на обладнання та ПЗ середовища замовника
  - Мережеве обладнання
  - Серверне обладнання
  - Програмне забезпечення

- ✓ Передбачуваний вплив на ПЗ середовища

- ✓ Наявність довготривалих загроз (**A**dvanced **P**ersistent **T**hreat)

- ✓ «Хакнуті хакери» (Hacked Hackers)



Penetration Test – Як уникнути багатьох проблем

Багатьох згаданих проблем замовник може уникнути, якщо слідуватиме декільком простим правилам:

1. Ретельно обговорюйте всі деталі пентесту з виконавцем перед початком тестування
2. Не ускладнюйте штучно виконання пентесту (*«а зараз ми вимкнемо непропатчені сервери та включимо правило «deny any any» на фаерволі…»*)
3. Наймайте досвідчені команди пентестерів з позитивною репутацією.

Варто пам'ятати: якщо пентестер не зміг зкомпрометувати систему замовника, це може не значити, що система добре захищена, це може значити лише те, що пентестер недостатньо досвідчений.

Penetration Test – Фактори успіху

Головні фактори успіху тесту на проникнення:

1. Професійні навички, досвід та репутація пентестера або компанії
2. Мотивація виконавців
3. Фактор часу

Дякую за увагу! Є питання?