УДК 004.7 **doi: 10.26906/SUNZ.2018.4.109**

В. В. Кальченко

Національний аерокосмічний університет імені М. Є. Жуковського "ХАІ", Харків, Україна

ОГЛЯД МЕТОДІВ ПРОВЕДЕННЯ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ДЛЯ ОЦІНКИ ЗАХИЩЕНОСТІ КОМП'ЮТЕРНИХ СИСТЕМ

Предметом статті є аналіз найбільш розповсюджених методів проведення тестування на проникнення в комп'ютерні системи. **Результати**. Проаналізовано міжнародні стандарти і керівництва з інформаційної безпеки, розглянуті методології проведення тестування на проникнення, проаналізовано нормативні акти різних країн в яких закріплено вимоги з проведення даного виду тестування. Наведено перелік найбільш розповсюджених міжнародних методологій проведення пентестінгу, надано їх короткий опис. Проаналізовано методи проведення пентестінгу, визначені основні переваги і недоліки таких методів. **Висновок.** Запропоновано класифікацію методів тестування на проникнення для оцінки захищеності комп'ютерних систем.

Ключові слова: тестування на проникнення, пентестінг, комп'ютерна мережа, захист інформації.

Вступ

Проникнення комп'ютерів у всі сфери життя людини призвело не тільки до пришвидшення фінансових розрахунків, надання послуг, оприлюднення інформації, але й неминуче створило нові загрози, як для суспільства так і держави в цілому. Основними видами загроз для комп'ютерних систем на даний час є загрози порушення доступності інформаційних ресурсів, що зберігаються в даних системах, та порушення конфіденційності і цілісності інформації [1]. Згідно останнього дослідження компанії Cisco, кожна з 53% атак на комп'ютерні мережі завдали підприємствам та організаціям збитків більше ніж на 500 000 доларів США. Причому основною причиною даної ситуації в цій сфері є недостатня кількість спеціалістів в сфері інформаційної безпеки, що призводить до неможливості впровадження нових заходів з захисту та проводити розслідування інцидентів інформаційної безпеки. [2] Проаналізувавши повідомлення в засобах масової інформації, повідомлення команди на реагування на комп'ютерні надзвичайні події України (CERT-UA) за декілька останніх років варто констатувати, що організовані групи зловмисників здійснюють втручання в роботу комп'ютерних систем органів державної влади, органів місцевого самоврядування, установ, підприємств, організацій та об'єктів критичної інфраструктури України. Це в свою чергу призводить до блокування роботи установ, матеріальних та репутаційних збитків. В нашій країні найбільш резонансними стали атаки BlackEnergy на інформаційно-телекомунікаційні системи Міністерства фінансів, Державної казначейської служби, та атаки з застосуванням вірусу PetyaA [2]. Варто визнати, що на даний час в Україні законодавство в сфері захисту інформації застаріло і не відповідає вимогам сьогодення. Це в свою чергу призводить до того, що рівень захисту комп'ютерних систем не відповідає тим загрозам, які існують. Метою даної роботи є аналіз інформації, яка стосується питань визначення рівня захищеності інформації в комп'ютерних системах, узагальнення отриманої інформації та вироблення відповідних пропозицій для вітчизняних підприємств, установ, організацій.

Керівництва з проведення аудиту інформаційної безпеки

В класичному варіанті, для перевірки оцінки захищеності інформації, проводять аудит інформаційної безпеки. Прикладами стандартів і керівництв в області такого роду аудиту є: «IT Audit Framework 2nd Edition» (ITAF), Cobit, International Professional Practices Framework (IPPF) for Internal Auditing Standards, Global Technology Audit Guide» (GATG), Guide to the Assessment of IT Risk» (GAIT), ISO/IEC 27007: Guidelines for information security management systems auditing. Однією з важливих частин такого роду аудиту, є проведення тестування на проникнення до комп'ютерної системи організації-замовника (pentesting, пентест).

Тест на проникнення це симуляція атаки на систему, мережу, частину обладнання чи інші засоби обслуговування, з метою доказу того, наскільки ця система вразлива для реального нападу. Процес тестування максимально схожий на процес злому, який проводить зловмисник. В ході тесту відповідний фахівець (група фахівців) намагається отримати доступ до інформації, яка обробляється в комп'ютерній системі, отримати контроль над роботою системи, або вивести її з ладу. Такий фахівець (пентестер) виступає в ролі злодія і намагається з'ясувати найбільш вразливі місця в системі, зафіксувати їх в звіті і передати відповідним працівникам організації-замовника для усунення. Під час проведення тесту йде визначення того, як система реагує на атаку (в незалежності від того можливо чи ні порушити захист системи) і яку інформацію можна отримати в системі. За результатами проведених робіт власник системи отримує звіт в якому вказуються недоліки в системі інформаційної безпеки підприємства та надаються практичні рекомендації щодо усунення виявлених вразливостей. Тест дозволяє отримати актуальну, незалежну оцінку захищеності інформаційних систем, дозволяє зрозуміти наскільки якісно побудовані процеси інформаційної безпеки, оцінити правильність налагоджень серверів і робочих станцій.

Найчастіше тести проводять для:

– оцінки захищеності нової інформаційної системи, де буде оброблятись чутлива інформація;

– оцінки захищеності системи після її модернізації;

– виконання вимог міжнародних стандартів;

– планування витрат на інформаційну безпеку.

В західних країнах тестування на проникнення є досить розповсюдженим і необхідність його проведення нормативно закріплено в відповідних законах, постановах, стандартах, тощо. Такими прикладами можуть бути:

– для американських публічних компаній, акції яких торгуються на фондових біржах – згідно вимог американського закону SOX Сарбейнса-Окслі (Sarbanes-Oxley Act);

– для американської медичної галузі та компаній, які мають справу з інформацією про здоров'я людей – згідно вимог американського закону про охорону та відповідальність за інформацію отриману в результаті медичного страхування HIPAA (Health Information Portability and Accountability Act);

– для банківської сфери – згідно вимог міжнародного стандарту безпеки даних індустрії платіжних карт PCI DSS (Payment Card Industry Data Security Standard), розробленому платіжними системами Visa і MasterCard.[3];

– для міжнародних компаній – згідно вимог міжнародного стандарту ISO/IEC 27001.

Стосовно українського законодавства варто констатувати, що необхідність проведення тестування на проникнення нормативно закріплена в «Положенні про організацію заходів із забезпечення інформаційної безпеки в банківській системі України», затвердженого Постановою Правління Національного банку України від 28.09.2017 №95 [4] і є обов'язковим для банків.

Враховуючи той факт, що комп'ютерні системи відрізняються одна від одної за сотнями характеристик, постає питання раціонального способу проведення тестування на проникнення. При чому в результаті необхідно отримати якісну оцінку захищеності та надати конкретні пропозиції щодо підвищення рівня захищеності системи, що оцінювалась.

Існуючи методології для тестування інформаційної безпеки

На даний час найбільш розповсюдженими методологіями проведення тестування на проникнення є:

– The Open Source Security Testing Methodology Manual (OSSTMM);

– The National Institute of Standards and Technology (NIST) Special Publication 800-115;

– OWASP Testing Guide;

– Penetration Testing Execution Standard (PTES);

– Information Systems Security Assessment Framework (ISSAF).

OSSTMM – міжнародна методологія для тестування інформаційної безпеки, розроблена ISECOM (Institute for Security and Open Methodologies) [5]. Метою даної методології є надання керівних принципів для процесу оцінки безпеки. Дана методологія виділяє 3 загальні класи безпеки: COMSEC (communication security channel), PHYSSEC(physical security channel), SPECSES(spectrum security channel). Дані класи поділяються на 5 каналів взаємодії з активами організації, які повинен перевірити пентестер, а саме: фізичної безпеки, бездротових мереж, інформаційних та телекомунікаційних мереж, людський фактор (використати методи соціальної інженерії). Основними перевагами даної методології є: детальний опис процедури підготовки до тестування, детально опрацьовані методи і підходи до тестування, детально описані основні терміни та поняття в галузі інформаційної безпеки. Проте дана методологія не містить опису інструментів, які повинні бути використані для цього.

Методологія NIST Special Publication 800-115 виділяє як мінімум 3 фази проведення оцінювання інформаційної безпеки: планування, виконання, пост-експлуатація (аналіз отриманих даних, виявлення причин що призвели до появи вразливостей, розробка рекомендацій до знешкодженню вразливостей і розробка звіту). Перевагою даного документа є те, що в ньому в загальному вигляді описані техніки перевірки безпеки комп'ютерної системи і їх короткий опис. Наприклад сніфінг мережі, перевірка log-файлів, перевірка налаштувань системи, перевірка цілісності файлів, сканування вразливостей, сканування бездротових мереж, тощо. Крім того, в даному документі приводяться посилання на програмні продукти, які необхідно використовувати для проведення тестування та посилання на інші нормативні документи та методології. Проте серед недоліків варто зазначити, що даний документ було розроблено в 2008 році. На даний момент він не відповідає сучасному стану розвитку інформаційних технологій та методам проникнення у комп'ютерні мережі.

Методологія OWASP [6] є прикладом детально опрацьованого документа, який детально охоплює питання безпеки веб-сайтів, веб-додатків. Проте якщо веб-сайт, веб-додатки підприємства не є критичними з точки зору бізнесу, то тестування на проникнення з застосуванням даної методології не є доцільним.

Методологія The Penetration Testing Execution Standard (PTES) фокусується лише на питаннях проведення тестування на проникнення [7]. Дана методологія виділяє 7 фаз тестування: визначення початкової інформації для тестування, збір необхідних даних, визначення векторів атак, аналіз вразливостей цільової системи, використання вразливостей для підтвердження можливості обходу засобів захисту, пост-експлуатація, складання звітних матеріалів. Перевагою даної методології є детально опрацьована послідовність дій з перевірки програмної захищеності комп'ютерних мереж. В свою чергу питанням фізичного захисту комп'ютерної мережі, питанням використання методів соціальній інженерії не приділяється достатньої уваги.

Методологія ISSAF дозволяє змоделювати вимоги до внутрішніх заходів з безпеки, і направлена на оцінку безпеки комп'ютерних мереж, систем та додатків[8]. Дана методологія більш детально ніж PTES фокусується на питаннях перевірки безпеки комп'ютерних систем та визначає яким саме чином

використовувати той чи інший інструмент. Проте як і NIST, дана методологія є застарілою (2005 року).

Класифікація методів тестування та їх використання

Проте, як зазначалось вище, кожна з методологій має деякі свої особливості, недоліки і переваги. При проведенні тестування на проникнення постає питання оптимального вибору методів тестування, їх узгодження з представниками організації-замовника та врахування особливостей цільової системи. Враховуючи даний факт, пропонується наступна класифікація методів тестування на проникнення (табл. 1). За місцем розташування особи, що проводить тестування, відносно периметру організації-замовника, можна виділити 2 напрямки тестування: зовнішнє і внутрішнє.

Так як більшість атак на комп'ютерні системи відбуваються через мережу Інтернет, то зовнішнє тестування на проникнення дозволяє отримати та оцінити ризики таких атак. При зовнішньому тестуванні пентестерам повідомляється початкова інформація (назва компанії, офіційний сайт, адреси електронних поштових скриньок, ір-адреси, тощо) і задачею тестування становиться отримання доступу до внутрішньої мережі організації-замовника та її подальше дослідження. Як правило при такому тестуванні йде оцінка брандмауера, систем які знаходяться в демілітаризованій зоні (Demilitarized Zone - DMZ), сервісів віддаленого доступу (Remote Access Service - RAS), тощо.

Згідно [9] при проведені тестування на проникнення, в 68% випадків вдавалось подолати мережевий периметр та потрапити до корпоративної мережі. При цьому по результатам 2017 року, рівень захищеності мережевого периметру залишився на рівні 2016 року.

При внутрішньому тестуванні пентестеру надається можливість підключити своє обладнання до комп'ютерної мережі, що буде тестуватись. В цьому випадку не потрібно знаходити шляхи потрапляння в внутрішню мережу та обходити засоби захисту. Внутрішній тест дозволяє оцінити які можливості будуть мати зловмисники в разі знаходженні шляхів потрапляння в внутрішню мережу, та можливості зловмисників зі складу працівників організації. За даними компанії Infowatch, 58,3% всіх випадків витоку інформації з комп'ютерних мереж організацій по всьому світу сталося з вини персоналу.[11] В свою чергу, за даними компанії Positive Technologies, в 2016-2017 роках в 100% випадків при внутрішньому тестуванні корпоративних мереж вдавалось отримувати повний контроль над мережою. При чому для отримання повного доступу, висока кваліфікація зловмисника не потребувалась. Основними недоліками в безпеці комп'ютерної мережі були відсутність оновлення операційних систем, використання користувачами словарних паролів, недоліки протоколів які дозволяли перенаправляти трафік та отримувати інформацію про конфігурацію мережі. [5]

Таблиця 1 – **Класифікація методів тестування на проникнення**

№	Ознака тестування	Види тестування
1.	За розташуванням програмно-апаратних засобів та пентестера відносно периметру організації-замовника	Зовнішне
		Внутрішне
2.	За обізнаністю пентестера про цільову систему	Білий ящик
		Чорний ящик
		Сірий ящик
3.	За обізнаністю технічних працівників організації-замовника про проведення тестування	Відкрите
		Приховане
4.	За характером заходів, що проводяться	Пасивне
		Агресивне
		Обережне
		Прораховане
5.	За повнотою виконання тестування	Повне
		Обмежене
		Фокусоване
6.	За видом інструментів, що використовуються	З застосуванням програмно-апаратних засобів
		З застосуванням методів соціальної інженерії та проникнення на контрольовану територію

За рівнем обізнаності пентестера виділяють 3 основних методи тестування: білий ящик (whitebox), чорний ящик (blackbox), сірий ящик (graybox). Дані методи загальновідомі та широко використовуються. В відповідній літературі та наукових статтях наводиться досить короткий опис методів проведення

тестування, як такого. Враховуючи даний факт, автором пропонується наступний узагальнений опис методів тестування на проникнення, для оцінки стану захищеності комп'ютерних систем.

При оцінці методом білого ящика замовник надає пентестеру повну інформацію про цільову систему, засоби захисту, необхідну технічну документацію. Можливе навіть надання адміністративного доступу до відповідних сервісів та систем. Тестування проводиться у взаємодії зі спеціалістами служби інформаційної безпеки підприємства. Основне завдання тестування зводиться до виявлення вразливостей та оцінки ризиків проникнення в систему. Даний спосіб дозволяє отримувати найбільш повну картину вразливостей об'єкта тестування, та виявляти найбільшу кількість векторів атаки. Варто зазначити що при такому підході, тестування проходить досить швидко і більш якісно, але в той же самий час пентестер знаходиться в більш вигідному становищі ніж справжній зловмисник в реальній ситуації.

З метою унеможливлення порушення нормального функціонування системи, даний метод рекомендується застосовувати для тестування комп'ютерних мереж, що забезпечують діяльність критичної інфраструктури або систем де припинення роботи призведе до непередбачуваних наслідків, фінансових збитків, притягнення до адміністративної (кримінальної) відповідальності.

При оцінці методом чорного ящика можна спостерігати зворотню ситуацію. В даному випадку замовник не надає пентестеру ніякої конкретної інформації про об'єкт тестування, або надає необхідний мінімум (назва компанії, сайт,). Це один з найбільш приближених до реальності метод тестування. Про проведення цього тесту знають, як правило, керівники відповідних служб безпеки. Завданням пентестера становиться проникнення в систему максимально непомітно без залишення слідів такого вторгнення.

Результати тестування методом чорного ящика будуть дуже залежати від кваліфікації пентестера, і можуть не відображати справжньої ситуації з інформаційною безпекою через те, що деякі сервіси можуть бути не проаналізовані під час тестування.

Найбільш оптимальним за швидкістю і якістю є метод тестування сірий ящик. В даному випадку пентестеру надають деяку інформацію про систему. Пентестеру не потрібно витрачати час для пошуку інформації для проведення тестування (наприклад ір-адреси серверів, web-сайти підприємства, адреси електронної пошти, тощо). При даному виді тестування пентестер може виступати в ролі інсайдера (менеджера, робітника підприємства), якому доступний мінімальний перелік інформації про об'єкт тестування. Використовуючи дану інформацію (наприклад аккаунт в системі) тестувальники намагаються розширити свої права в системі, отримати доступ до інформації, що захищається.

За рівнем обізнаності працівників організації-замовника про проведення процедури тестування, виділяють: приховане та відкрите тестування.

В разі, якщо замовник хоче перевірити не тільки первинні системи безпеки, але й системи попередження вторгнення (Intrusion Detection System - IDS), організаційні чи кадрові структури (наприклад процедури інформування керівництва про нештатні події) – рекомендується застосувати приховане тестування (без повідомлення відповідних технічних працівників установи). Про приховане сканування повідомляються керівники підрозділів безпеки та/або керівник підрозділу, що здійснює адміністрування комп'ютерних систем. Такий метод крім основної мети дозволяє оцінити дії і професіональні навички працівників організації, недоліки у процедурах взаємодії між підрозділами та перевірити якість реалізації політики безпеки організації. [12]

Проте в тих випадках, коли приховане тестування не призводить до буть-яких дій зі сторони технічних працівників, або коли тестування проводиться методом білого ящика` – варто включити в команду технічних працівників організації замовника. В цьому випадку тестування буде відкритим. Особливо важливо проводити відкрите тестування для критичних систем. В разі непередбачених ситуацій це дозволить технічним працівникам відреагувати на події та попередити небажані наслідки або матеріальні збитки. Крім того відкрите тестування дозволяє технічним спеціалістам ознайомитись з методами і засобами проведення тестування, пройти таким чином навчання і наочно ознайомитись з можливим алгоритмом дій зловмисників. [11]

За характером заходів що проводяться, методи тестування можна поділити на:

– пасивне тестування – при такому тестуванні цільова системи сканується з метою виявлення відомих вразливостей. В разі їх знаходження вони не експлуатуються, а лише фіксуються;

– агресивне тестування – при такому тестуванні пентестер використовує всі можливі вразливості, такі як переповнення буфера навіть на тих системах, призначення яких невідомо, або виведення з ладу системb безпеки за допомогою атаки «відмова в обслуговуванні» (DoS-attack). В цьому випадку тестувальник повинен усвідомлювати, що в доповнення до цільової системи, сусідні системи або мережеві компоненти можуть також постраждати внаслідок тестування.[5, 13]

– обережне тестування – в цьому випадку виявлені вразливості будуть використані лише тоді, коли цільова система не постраждає від їх експлуатації. Прикладом може бути використання стандартних паролів або спроби отримання доступу до каталогів веб-серверу;

– прораховане тестування – пентестер також намагається використати знайдені вразливості, які можуть призвести до системних збоїв. Наприклад – автоматичний підбір паролів і переповнення буферів у точно визначених цільових системах. Але перш ніж використати ці вразливості пентестер прораховує можливі наслідки, і в залежності від цього приймає рішення щодо своїх подальших дій.

За повнотою виконання тестування, методи можна поділити на наступні види:

– повне тестування – даний тип тестування варто проводити для систем, які тестуються вперше. Це дозволить забезпечити виявлення недоліків в усіх комп'ютерних системах організації. При цьому час затрачений на тестування залежить від кількості таких систем та їх одноманітністю. Якщо конфігурації систем суттєво відрізняються одна від одної, кожна система повинна бути окремо обстежена. Проте варто розуміти що системи, які адмініструються іншими організаціями, або зовнішні системи можуть бути необстежені;

– обмежене тестування – при цьому тестування замовник чітко визначає які саме системи або служби повинні бути протестовані. Наприклад всі системи в демілітаризованій зони, або системи які виконують певні задачі;

– фокусоване тестування – застосовується для тестування однієї підмережі, системи або служби. Даний вид тестування є доречним після модифікації або розширення комп'ютерної системи. Такий тест звичайно надає інформацію про протестовану систему, але не дає інформації про захищеність всієї інфраструктури організації.[12]

Тестування в залежності від інструментів, що використовуються, можна поділити на наступні види:

– з застосуванням програмно-апаратних засобів;

– з застосуванням методів соціальної інженерії та проникнення на контрольовану територію.

В класичному випадку тестування на проникнення здійснюється через комп'ютерну мережу. Для його проведення використовуються, як окремі програмні засоби так і набори програм, які постачаються разом зі спеціалізованими операційними системами.

Люди часто являють собою найслабшою ланкою в системі безпеки організації. Як правило це пов'язано з низьким рівнем обізнаності з інформаційної безпеки, довірливістю, формальним підходом до виконання службових обов'язків, тощо. Задачою пентестера є заставити користувача цільової системи (наприклад бухгалтера) запустити програму надіслану в поштовому повідомленні, перейти за посиланням, або повідомити пароль по телефону. Використання методів соціальної інженерії дозволяють отримувати бажані для пентестера результати з меншими затратами сил і засобів ніж класичними методами. Обов'язком пентестера в цьому випадку є детально описати як успішні, так і не успішні атаки. Це дозволить в майбутньому адаптувати програми навчання для працівників і таким чином підвищити їх рівень обізнаності в сфері інформаційної безпеки.

Сучасні засоби безпеки дозволяють забезпечити досить високий рівень захищеності системи, і іноді пентестерам не вдається обійти дані засоби, або більш доцільно отримати доступ до активів іншими шляхами. Часто простіше і швидше отримати доступ до активів, (або обійти засоби захисту) шляхом отримання фізичного доступу до елементів системи, що тестується. Така фізична атака означає, що пентестер отримує доступ до незахищеної паролем робочої станції після потрапляння тими чи іншими шляхами до будівель, приміщень та/або серверних кімнат.

Спеціалісти з інформаційної безпеки радять використовувати даний метод в тому випадку, коли в організації є відповідним чином сформована політика безпеки, розроблені відповідні процедури, інструкції, тощо.

В цьому випадку застосування методів соціальної інженерії дозволяє оцінити ступінь ефективності вжитих заходів безпеки [9].

Висновок

В умовах сьогодення, забезпечення безпеки комп'ютерних систем України є складовою частиною безпеки держави в цілому. Особливо важливим є захист інформаційних систем об'єктів критичної інфраструктури, фінансових установ, державних реєстрів тощо. Існуюча нормативна база України в сфері захисту інформації не передбачає проведення тестувань на проникнення, які дозволять визначити реальну захищеність комп'ютерних мереж. Виключенням є лише банківська сфера. У зв'язку з цим, перспективним напрямом є розробка деякої узагальненої методології, яка дозволить проводити перевірку захищеності комп'ютерних мереж в мінімально можливі терміни і отриманням якісної і об'єктивної оцінки захищеності.

В статті було проаналізовано найбільш розповсюджені міжнародні методології проведення тестування на проникнення.

За результатом аналізу можна констатувати, що на даний момент не існує комплексної методології проведення даного виду тестування. Кожна з розглянутих в даній статті методологій фокусується на певних питаннях, і як наслідок, при проведення комплексного тестування на проникнення неможливо повністю опиратись лише на одну методологію. У зв'язку з цим необхідно використовувати декілька методологій одночасно, а це в свою чергу уповільнює процес оцінювання.

Також отримані результати можуть не відображати реальний стан речей в сфері кібербезпеки. За результатом проведеного аналізу існуючих методологій та публікацій з цього питання, запропонована класифікація методів тестування, надано короткий опис методів тестування, запропоновано класифікацію методів тестування.

Приведена класифікація узагальнює та структурує види пентестів, що в свою чергу дозволяє визначити оптимальні шляхи проведення робіт та погодити їх з замовником.

СПИСОК ЛІТЕРАТУРИ

1. Певнев В.Я. Методы обеспечения целостности информации в инфокоммуникационных системах / В.Я. Певнев // Вісник Національного технічного університету ХПІ. Серія: Техніка та електрофізика високих напруг. – 2015. - № 51. – С. 74-77.

2. Cisco 2018. Годовой отчет по безопасности. [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/dam/global/ru_ru/assets/offers/assets/cisco_2018_acr_ru.pdf (дата звернення: 15.08.2018)
3. PCI DSS. Requirements and Security Assessment Procedures. Version 3.2. [Електронний ресурс]. – Режим доступу: https://www.pcisecuritystandards.org/document_library (дата звернення: 20.08.2018)
4. Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затвердженого Постановою Правління Національного банку України від 28.09.2017 №95. [Електронний ресурс]. – Режим доступу до положення: https://bank.gov.ua/document/download?docId=56426049 (дата звернення: 15.08.2018)
5. The Open Source Security Testing Methodology Manual (OSSTMM). [Електронний ресурс]. – Режим доступу: http://www.isecom.org/mirror/OSSTMM.3.pdf (дата звернення: 20.08.2018)
6. O WASP Testing Guide v4. [Електронний ресурс]. – Режим доступу: https://www.owasp.org/index.php/OWASP_Testing_Project (дата звернення: 20.08.2018)
7. The Penetration Testing Execution Standard (PTES). [Електронний ресурс]. – Режим доступу: http://www.pentest-standard.org/index.php/Main_Page (дата звернення: 20.08.2018)
8. Information Systems Security Assessment Framework (ISSAF). [Електронний ресурс]. – Режим доступу: http://www.oissg.org/files/issaf0.2.1.pdf (дата звернення: 20.08.2018)
9. Анастасия Гришина, Андрей Куликов – Анализируем защищенность IT-систем. Positive Research 2018. Сборник исследований по практической безопасности. [Електронний ресурс]. – Режим доступу: https://www.ptsecurity.com/upload/ corporate/ru-ru/analytics/Positive-Research-2018-rus.pdf (дата звернення: 20.08.2018)
10. Глобальное исследование утечек конфиденциальной информации в 2017 году. Аналитический центр InfoWatch. [Електронний ресурс]. – Режим доступу: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2017_year.pdf (дата звернення: 20.08.2018)
11. Technical Guide to Information Security Testing and Assessment. Recommendations of the National Institute of Standards and Technology. Special Publication 800-115. [Електронний ресурс]. – Режим доступу: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf (дата звернення: 23.08.2018)
12. Я.Я. Стефінко, А.З.Піскозуб. Використання відкритих операційних систем для тестування на проникнення в навчальних цілях/Я.Я. Стефінко, А.З. Піскозуб //Вісник Національного університету "Львівська політехніка" Комп'ютерні системи та мережі. – 2014. - № 806. – С. 258-263.

Рецензент: д-р техн. наук, проф. С. Г. Семенов,
Національний технічний університет "Харківський політехнічний інститут", Харків
Received (Надійшла) 19.06.2018
Accepted for publication (Прийнята до друку) 22.08.2018

Обзор методов проведения тестирования на проникновение для оценки защищенности компьютерных систем

В. В. Кальченко

Предметом статьи является рассмотрение наиболее распространенных методов проведения тестирования на проникновение в компьютерные системы. **Результаты**. Проанализированы международные стандарты и руководства по информационной безопасности, рассмотрены методологии проведения тестирования на проникновение, проанализированы нормативные акты разных стран в которых закреплены требования по проведению данного вида тестирования, приведен перечень наиболее распространенных международных методологий проведения пентестинга, определены основные преимущества и недостатки таких методов. **Вывод.** Предложена классификация методов тестирования на проникновение для оценки защищенности компьютерных систем.

Ключевые слова: тестирование на проникновение, пентестинг, компьютерная сеть, защита информации.

Review of penetration testing methods for assesing the protection of computer systems

V. Kalchenko

The most effective way to evaluate the security of the system is to conduct a penetration test (pentest). A penetration test is a simulation of an attack on a system, network, equipment, service, in order to demonstrate how vulnerable this system is to a real attack. During the test it is estimated how the system responds to the attack, regardless of whether it is possible or not to violate the protection of the system and what information can be taken out of the system. **Subject**. The paper focused on the study of the methods of penetration testing, analyzes the international standards of information security, examines the main methods of penetration testing computer systems. **Results.** It is necessary to check constantly the current state of the security of the computer systems in order to respond in a timely manner to new challenges for information security of state bodies, infrastructure objects on critical importance, commercial enterprises, institutions and organizations. The research substantiates the necessity of conducting this kind of work and gives the advantages of its application. The main approaches to testing are described in detail: WhiteBox, BlackBox, Graybox. The methods of testing systems are described and classified depending on the requirements of the customer, the objectives of testing, time limits and importance of the object under research. Since operating systems, programs, data protocols are constantly changing, penetration testing will not completely solve the problem of data protection, but it allows you to look at computer systems from the intruder's point of view. And this allows to understand the weaknesses of the system and to take timely measures to prevent or significantly reduce possible losses. The choice of penetration testing methods should be performed after the customer has been identified the testing objectives, the definition of the systems to be tested, the definition of critical objects, the timing of the work, etc. Different combinations of testing methods and creative approach will allow to conduct testing the most qualitatively and in the shortest time, to make a report and to provide the customer with recommendations for improving the security of the system. **Conclusions.** A classification and algorithm for choosing penetration testing methods for evaluating the security of computer systems is proposed.

Keywords: penetration testing, pentest, computer network, information security.