УДК 004

А.З. Піскозуб
Національний університет "Львівська політехніка",
кафедра захисту інформації

ВИКОРИСТАННЯ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ В КОМП'ЮТЕРНІ МЕРЕЖІ ТА СИСТЕМИ ДЛЯ ПІДНЯТТЯ ЇХ РІВНЯ ЗАХИЩЕНОСТІ

Розглянуто питання використання тестування на проникнення як методу підвищення рівня захищеності комп'ютерних мереж та систем. Також наведено аналіз методики тестування на проникнення збірки BackTrack, що складається з 10 етапів.

Ключові слова: тестування на проникнення, етичний хакінг, безпека, вразливість, Black-Box, White-Box, Grey-Box, ISO/IEC 27001:2005.

This paper comprises information about penetration testing methodology as a way to improvement of computer system and network security. Also the BackTrack testing methodology incorporating the ten consecutive steps of penetration testing process is given.

Key words: penetration testing, ethical hacking, security, vulnerability, Black-Box, White-Box, Grey-Box, ISO/IEC 27001:2005.

Вступ

Питання захисту інформації є надзвичайно важливими та актуальними сьогодні, оскільки вже давно вийшли на одне з перших місць серед інших завдань, що вирішуються у процесі проектування, створення та використання сучасних інформаційних (ІТ) систем. Як зазначено в [1], надзвичайно актуальним сьогодні є використання вільного та відкритого ПЗ (ВВПЗ) для потреб підвищення рівня захищеності комп'ютерних мереж і систем.

Визначальними у цьому плані є нормативні чинники – стандарти, закони, інфраструктурні рішення, бібліотеки кращих практик тощо. Мета в них одна – забезпечити виконання організаційних та технічних рекомендацій, що підвищують рівень захищеності.

Нормативні чинники

Одним з таких визначальних в плані захисту інформації є міжнародний стандарт ISO/IEC 27001:2005 [2], який забезпечує підтримку рішень на основі ITIL ((Information Technology Infrastructure Library, бібліотека ІТ інфраструктури), що описує найкращу світову практику організації підприємства, що надає послуги у сфері ІТ) та COBIT (Control Objectives for Information and Related Technology ("Задачі інформаційних і суміжних технологій") – відкритий ІТ-стандарт, який, своєю чергою, містить ряд документів зі стандартами щодо оптимізації управління ІТ: аудитом ІТ та ІТ-безпекою). Згідно з ISO/IEC 27001:2005 на підприємстві створюється система управління інформаційною безпекою (СУІБ), яка повинна відповідати усім вимогам міжнародних стандартів в галузі ІБ.

Як випливає з цих стандартів, кожна організація повинна розробити ряд кроків, серед яких, зокрема, оцінити свої активи, розглянути й оцінити специфічні ризики, з якими пов'язана її діяльність щодо збереження, конфіденційності та цілісності інформації, та на основі цієї оцінки сформувати політику безпеки, яка дасть змогу уникнути або мінімізувати ці ризики і, завдяки цьому, зробити Ваш бізнес безпечним. Ефективна політика безпеки повинна бути проактивною, щоб забезпечити достатній захист від різних відомих і невідомих атак і випадків. Дуже часто це хибно розуміють як підтримку в актуальному стані програмного та апаратного забезпечень. Регулярні оновлення необхідні, звичайно, проте вони ніяк не вирішують питання людських помилок – неправильної конфігурації чи підходів, що робить всю мережу вразливою для атак.

Тому метою статті є висвітлення методики тестування на проникнення як засобу забезпечення всебічного рівня безпеки ІТ – інфраструктури компанії.

Використання тестування на проникнення як методу підвищення рівня захищеності комп'ютерних мереж та систем

Етичність тестування безпеки повинна ґрунтуватись на правилах застосування (rules of engagement), яких повинен дотримуватися аудитор, котрого наймає організація для проведення тестування на проникнення до її інформаційних ресурсів, зокрема: як слід проводити тестування; визначення масштабів тестування; підготовка плану тестування; перебіг процесу тестування; забезпечення конфіденційної звітності щодо проведеної роботи тощо.

Загальновідомі два підходи для проведення тестування на проникнення (далі – пентесту) Black-Box та White-Box.

Black-Box пентест також відомий як зовнішнє тестування. Застосовуючи цей підхід, аудитор безпеки оцінюватиме мережеву інфраструктуру організації з віддаленого місця розташування і не знатиме всі внутрішні технології, які тут використовуються. Насправді за цього підходу аудитор (Black Hat) уподібнюється поведінці зловмисників і застосовує усі відомі йому хакерські техніки та інструментальні засоби. При цьому важливо зрозуміти та класифікувати усі знайдені вразливості відповідно до рівня ризику (низький, середній або високий). Ризик, загалом, може бути виміряний відповідно до загрози через виявлену вразливість і відповідні втрати, які сталися після успішного проникнення. Після завершення пентесту створюється звіт з усією необхідною інформацією щодо оцінки рівня безпеки мережевої інфраструктури організації, класифікацією усіх виявлених ризиків у бізнес-контексті.

White-Box пентест також відомий як внутрішнє тестування. Аудитор (White Hat) при цьому повинен знати будову інфраструктури мережі та усіх наявних сервісів організації. White-Box пентест подібний до Black-Box пентесту, але немає потреби проводити такі етапи, як визначення меж тестування, збір інформації про цільову систему та виявлення сервісів, що працюють на цільових хостах. White-Box пентест дає змогу виявити усі вразливості в системі та їх усунути, що, природно, підвищить рівень захищеності системи загалом. Крім того, цей підхід можна легко інтегрувати в звичайний цикл розробки продуктів, що випускає організація, що дозволить викорінити будь-які можливі проблеми з безпекою на ранній стадії, перш ніж їх виявить і використає зловмисник.

Grey-Box пентест, як поєднання обох зазначених підходів пентесту, дає максимально повну інформацію про стан захищеності мережевої інфраструктури організації.

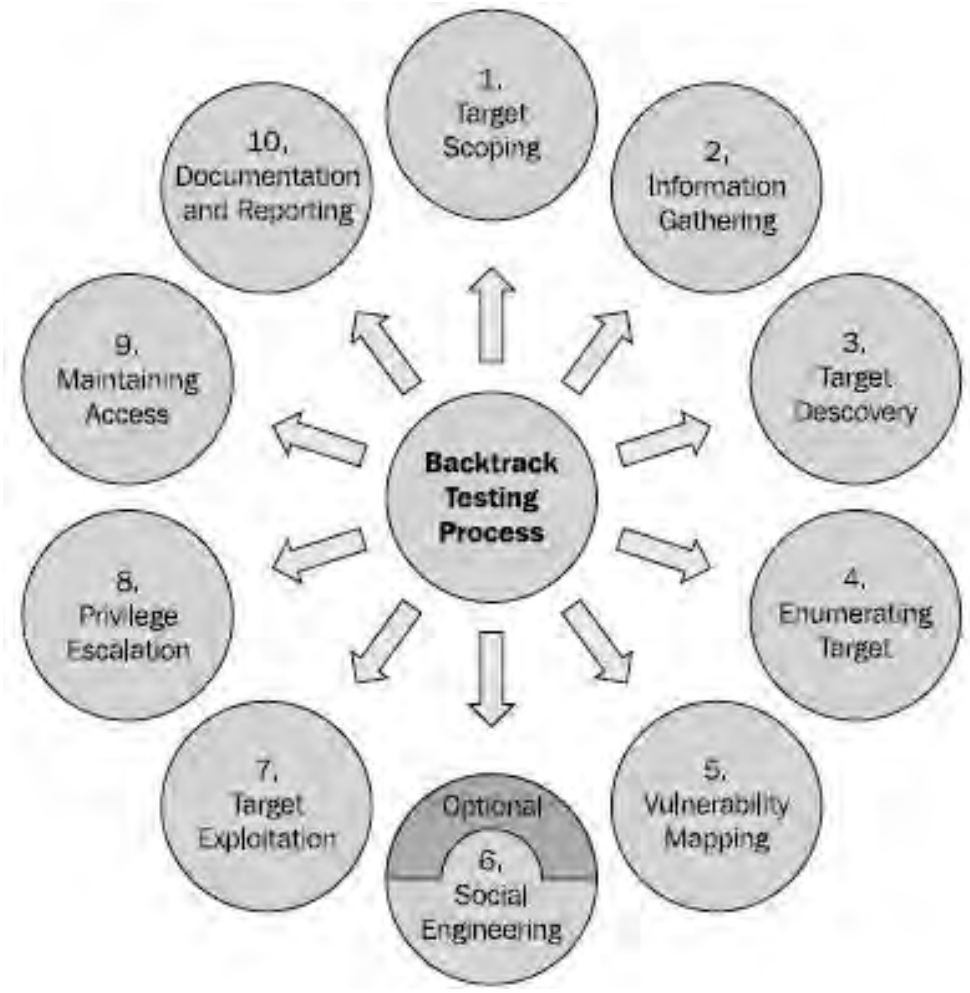
Відомі різні методики з відкритим кодом, покликані задовольнити потреби оцінки безпеки. За допомогою цих методик оцінки можна легко скоротити час на проведення важливих і складних завдань оцінки системи безпеки залежно від його розміру та складності. Деякі з цих методик зосереджуються на технічному аспекті тестування безпеки, тоді як інші націлені на управлінські критерії, і практично є декілька, зорієнтованих на обидві категорії. Основна ідея формалізації цих методологій полягає у виконанні різних видів випробувань крок за кроком, що дасть змогу робити висновки про безпеку системи точніше. Зокрема, такими відомими методиками оцінки безпеки мережевого та прикладного рівнів є:

- Open Source Security Testing Methodology Manual (OSSTMM);
- Information Systems Security Assessment Framework (ISSAF);
- Open Web Application Security Project (OWASP) Top Ten;
- Web Application Security Consortium Threat Classification (WASC-TC).

Наведені методики покликані допомогти фахівцям з безпеки вибрати кращу стратегію, яка могла б вписатися у вимоги клієнтів і кваліфікувати придатний прототип тестування. Перші дві методики надають загальні принципи і методи, забезпечуючи тестування безпеки для практично будь-яких інформаційних активів, останні два – відповідно переважно стосуються оцінки безпеки на прикладному рівні. Визначення правильної стратегії оцінки залежить від декількох факторів, зокрема технічних деталей, що стосуються цільової системи, наявності ресурсів, знань аудитора, бізнес-цілей організації і нормативних питань.

Використання платформи BackTrack для проведення тестування на проникнення комп'ютерних мереж та систем

Сьогодні найвідомішою платформою з відкритим кодом для пентестів є BackTrack – операційна система, базована на Linux Ubuntu 10.04, з цілим рядом програмних продуктів для оцінки захищеності систем та тестування їх на проникнення. Робота BackTrack основана на використанні методики пентесту, що складається з 10 етапів, якими є: визначення меж тестування (Target Scoping); збір інформації про цільову систему (Information Gathering); виявлення цільових хостів, що працюють (Target Discovery); виявлення сервісів, які працюють на цільових хостах (Enumerating Target); визначення вразливостей на цільових хостах (Vulnerability Mapping); соціальна інженерія (Social Engineering), злам цільових систем (Target Exploitation), підвищення привілеїв на цільових системах (Privilege Escalation); збереження доступу після зламу цільових систем (Maintaining Access); документація та звітність (Documentation and Reporting) (див. рисунок) [3].



BackTrack – методика тестування на проникнення

Сьогодні правонаступником BackTrack є ВВПЗ Kali Linux [4], який вже ґрунтується на ОС Linux Debian. Цей перехід дав змогу забезпечити дистрибутиву значно вищу стійкість, великі репозиторії ОС Debian, багатомовну підтримку та сумісність з Filesystem Hierarchy Standard (FHS). Також Kali Linux підтримує APM платформи: rk3306 mk/ss808, Raspberry Pi, ODROID U2/X2 та Samsung Chromebook.

Нині Kali Linux містить понад 300 пентест-інструментів, що робить його незамінним інструментом будь-якого спеціаліста із захисту інформації.

Висновки

Резюмуючи наведений матеріал, потрібно відзначити необхідність дотримання нормативних чинників – стандартів, законів, інфраструктурних рішень, бібліотеки кращих практик ITIL, що дасть змогу підвищити рівень захищеності комп'ютерних мереж та систем. При цьому можливо забезпечити ці рішення на базі ВВПЗ. Доцільно використовувати проактивний захист, одним з методів якого є тестування на проникнення. Такий підхід є єдиним способом отримати реальну картину стану захищеності системи, і, отже, здобути контроль над IT-середовищем, що постійно зростає.

1. Піскозуб А.З. Використання вільного програмного забезпечення для підвищення рівня захищеності комп'ютерних мереж та систем // Матеріали другої міжнародної науково-практичної конференції FOSS Lviv, 2012,. – Львів, 2012. – С. 86–90. 2. ISO/IEC 27001:2005, Information technology — Security techniques — Information security management systems — Requirements 3. Shakeel Ali, Tedi Heriyanto. BackTrack 4. Assuring Security by Penetration Testing. Master the art of penetration testing with BackTrack // Packt Publishing Ltd.- Birmingham, 2011. 373 pp. 4. Kali Linux. // http://www.kali.org/

УДК 006.063:656.13

О. Петренко
Національний університет "Львівська політехніка"

АНАЛІЗ ВИМОГ ЧИННИХ НОРМАТИВНО-ПРАВОВИХ АКТІВ ЩОДО ДОПУСТИМИХ РІВНІВ ШУМУ І ВІБРАЦІЇ АВТОМОБІЛЯ

Проаналізовано чинні нормативно-правові акти та їх вимоги стосовно безпеки, оцінювання негативного впливу перерахованих чинників автотранспортного засобу (АТЗ) і зовнішнього середовища на стан здоров'я і поведінку водія на дорозі, а також ступінь відповідності чинних нормативних документів світовому рівню.

Ключові слова: нормативно-правовий акт, шум, вібрація, транспортний засіб, допустимий рівень шуму, допустимий рівень вібрації, нормовані параметри.

This article analyzes the existing regulations and safety requirements, assessing the negative impact of these factors, the vehicle (ATC) and the external environment on the health and behavior of the driver on the road, as well as assessing the level compliance with existing regulations to international standards.

Key words: legal act, the noise, vibration, the vehicle, allowable noise level, the allowable vibration level, normalized parameters.

Постановка проблеми

У нормативно-технічній документації (НТД), що діє сьогодні на території України, ще недостатньо чітко встановлено шкідливість впливу на здоров'я людини акустичних та механічних чинників, що виникають в процесі експлуатації дорожньо-транспортних засобів (ДТЗ), а саме шуму, інфразвуку, ультразвуку і вібрації. Як наслідок, недостатньо обгрунтовані вимоги до гранично допустимих рівнів цих параметрів у кабіні (салоні) автомобіля. Оскільки у багатьох випадках автомобіль є робочим місцем водія, яке повинно відповідати державним нормам з охорони праці, розроблення уточнених нормативних документів, які б відповідали світовому рівню і забезпечували належну безпеку дорожнього руху, є актуальним науковим завданням.

Відомо, що суттєво впливає на психологічний стан людини шумова дія [5]. Шум – різні небажані, неприємні звукові (акустичні) коливання, що безладно змінюються в часі й містяться в діапазоні частот від 16 Гц до 22 кГц.