

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

© Піскозуб А.З., 2015

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.

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

В даній статті обговорюються питання використання тестування на проникнення як методу підняття рівня захищеності комп'ютерних мереж та систем. Також наведений 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.

Вступ

Питання захисту інформації є надзвичайно важливими та актуальними сьогодні, оскільки вже давно вийшли на одне з перших місць серед інших завдань, що вирішуються в процесі проектування, створення та використання сучасних інформаційних (ІТ) систем. Як зазначалося 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 дозволить підняти 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 ІТІЛ ((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 в свою чергу 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 впливає з даних стандартів, кожна організація повинна розробити ряд кроків, серед яких, зокрема, оцінити свої активи, розглянути і оцінити специфічні ризики, яким піддається її діяльність щодо збереження, конфіденційності та цілісності інформації, та на основі цієї оцінки сформулювати політику безпеки, яка дозволить уникнути або мінімізувати ці ризики і, таким чином, 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 даної статті є висвітлення методики тестування на проникнення як засобу забезпечення всебічного рівня безпеки ІТ – інфраструктури компанії.

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

Етичність тестування безпеки повинна базуватись 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 по проведеній роботі тощо.

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

Black-Vox пентест також відомий як зовнішнє тестування. При застосуванні цього підходу аудитор безпеки буде оцінювати мережеву інфраструктуру організації з віддаленого місця розташування і не бути знати всі внутрішні технології, які тут використовуються. Насправді в цьому підході 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 у відповідності з рівнем ризику (низький, середній або високий). Ризик, в цілому, може бути вимірний відповідно до загрози через виявлену вразливість і відповідні втрати, які сталися після успішного проникнення. По завершенні пентесту створюється звіт з усією необхідною інформацією щодо оцінки рівня безпеки мережевої інфраструктури організації, класифікацією усіх виявлених ризиків в бізнес-контексті.

White-Vox пентест також відомий як внутрішнє тестування. Аудитор (White Hat) при цьому повинен бути в курсі будови інфраструктури мережі та усіх наявних сервісів організації. White-Vox пентест подібний до того, як проводиться Black-Vox пентест, але немає потреби проводити такі етапи як визначення меж тестування, збір інформації про цільову систему та виявлення працюючих сервісів на цільових хостах. White-Vox пентест дозволяє виявити усі вразливості в системі та їх усунути, що природно підніме рівень захищеності системи в цілому. Крім того, цей підхід може бути легко інтегрований в звичайний цикл розробки продуктів, що випускає організація, що дозволить викоринити будь-які можливі проблеми з безпекою на ранній стадії, перш ніж вони будуть розкриті і використані зловмисниками.

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

Відомі є ряд різних методик 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 в залежності від його розміру та складності. Деякі з цих методик зосереджуються на технічному аспекті тестування безпеки, в той час як інші націлені на управлінські критерії, і практично є декілька, що націлені на обидві категорії. Основна ідея формалізації цих методологій полягає у виконанні різних видів випробувань крок за кроком, що дасть змогу судити про безпеку системи більш точно. 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 підходящий прототип тестування. Перші дві методики забезпечують загальні принципи і методи, забезпечуючи тестування безпеки для практично будь-яких інформаційних активів, останні два – відповідно в основному стосуються

оцінки безпеки на прикладному рівні. Визначення правильної стратегії оцінки залежить від декількох факторів, у тому числі, технічних деталей, наданих про цільову систему, наявність ресурсів, знань аудитора, бізнес-цілей організації, і нормативних питань.

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

На сьогодні найвідомішою платформою з відкритим кодом для пентестів є BackTrack – операційна система, базована на Linux Ubuntu 10.04, яка йде з цілим рядом програмних продуктів для оцінки захищеності систем та тестування їх на проникнення. В основі роботи BackTrack лежить використання методики пентесту, що складається з 10 етапів, якими є: визначення меж тестування (Target Scoping), збір інформації про цільову систему (Information Gathering), виявлення працюючих цільових хостів (Target Discovery), виявлення працюючих сервісів 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), і документація та звітність (Documentation and Reporting) (див. рис.1) [3].

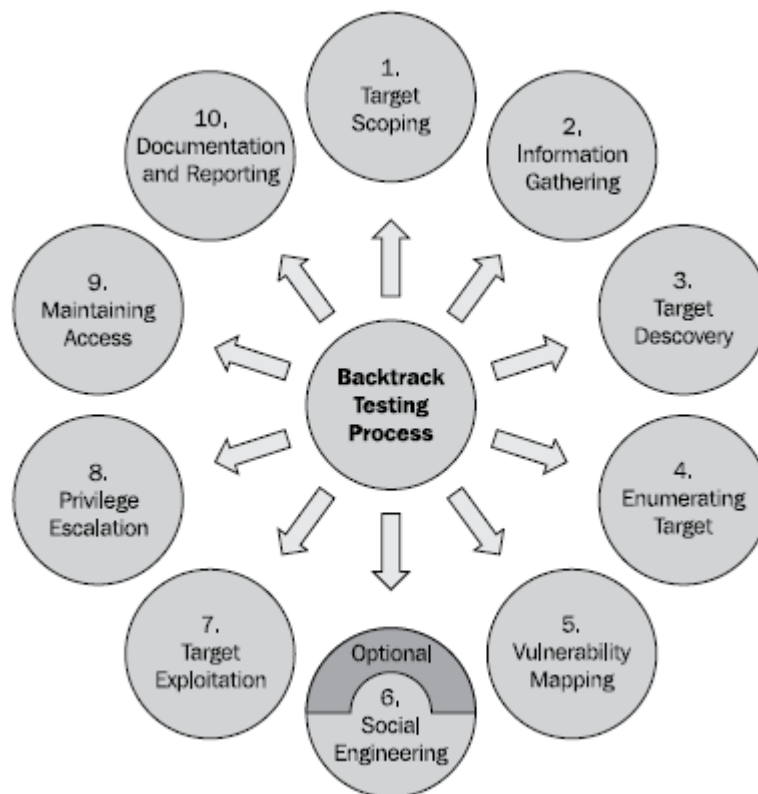


Рис.1. BackTrack – методика тестування на проникнення.

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

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

Висновки

Резюмуючи наведений матеріал, потрібно відзначити необхідність дотримання нормативних чинників – стандартів, законів, інфраструктурних рішень, бібліотеки кращих практик ІТІЛ, що дозволить підняти рівень захищеності комп'ютерних мереж та систем. При цьому є можливо забезпечити ці рішення на базі ВВПЗ. Доцільним є використання проактивного захисту, одним з методів якого є тестування на проникнення. Такий підхід є єдиним способом отримати реальну картину стану захищеності системи, і, отже, отримати контроль над постійно зростаючим ІТ-середовищем.

Література

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/>