запитання (текст з пропущеними словами), коротка відповідь, Правильно/Неправильно, розрахунковий тест, розрахунковий тест з множинним вибором тощо.

Вступний контроль здійснюється, як правило, з метою виявлення рівня попередніх знань студентів. Тому тут доцільно використати тести з множинним вибором відповіді.

Поточний контроль, по суті, це оцінка за виконане завдання, як вид діяльності студента, результатом якого, зазвичай, є створення і завантаження на сервер файлу будь-якого формату або створення тексту безпосередньо в системі Moodle (за допомогою вбудованого візуального редактора). Викладач перевіряє зданий студентом звіт за виконане завдання, пише до нього коментарі; якщо необхідно, то пропонує допрацювати та наново завантажити файл, виставляє оцінку за виконану роботу в електронний журнал. Як форма поточного контролю може бути організоване віртуальне заняття, по завершенню якого також виставляються оцінки.

Модульний та заключний контроль за навчально-пізнавальною діяльністю студентів у системі дистанційного навчання Moodle здійснюється в залежності від специфіки навчального предмету. Якщо це математика або фізика – то це розв'язування задач, виведення формул, тощо, і для цього необхідно використовувати спеціально вмонтований редактор. Якщо ж предмет гуманітарний, то найчастіше вдаються до використання тестів з множинним вибором або написання есе.

Система дистанційного навчання Moodle надає широкі можливості для контролю, оцінки, перевірки навчальних досягнень студентів та корекції уже засвоєних знань, дозволяє з'ясовувати, до якого розділу дисципліни студенти звертаються найчастіше, які розділи викликають труднощі у засвоєнні; організовувати віртуальні семінарські, практичні та лабораторні заняття з виставленням оцінок у електронний журнал; створювати тести різних типів і змісту з автоматичною їх обробкою; встановлювати часовий контроль за виконанням тих чи інших видів діяльності.

Використання FOSS на платформі KALI Linux та Metasploitable для вивчення процесу етичного хакінгу

Стефінко Я.Я., Піскозуб А.З.

Кафедра безпеки інформаційних технологій, НУ "Львівська політехніка", jarik.bit@gmail.com,
Кафедра захисту інформації, НУ "Львівська політехніка", м.Львів, azpiskozub@gmail.com

We discuss the security threats to computer networks and systems, and one of the ways to protect - penetration test. The methods and ways of implementation as well as analysis of the current free software for penetration test are described in this paper.

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. Надзвичайно актуальним сьогодні є використання вільного та відкритого ПЗ (ВВПЗ) для потреб підвищення рівня захищеності комп'ютерних мереж і систем.

Сучасні комп'ютерні системи і мережі зазнають тисяч різних атак, як ззовні так і зсередини. Тому актуальним на даний час є питання різностороннього підходу до питання захищеності: оцінки захищеності системи до зламу та запобігання його руйнівним наслідкам. Тести на проникнення є складовою частиною повного аудиту безпеки.

Тестування на проникнення і його можливості

Тест на проникнення (далі - пентест) дає змогу моделювати несанкціонований доступ в інформаційні системи, а також інші дії, які можуть порушити нормальне функціонування систем і бізнес-процесів. По суті, це метод оцінки захищеності інформаційних систем та/або інформації, та об'єктів, де вона зберігається або обробляється від несанкціонованого використання.

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.

Об'єктами тестів на проникнення є різні компоненти інформаційної інфраструктури: активне мережеве обладнання, сервери, робочі станції, інформаційні системи, бази даних. Завдання пентестера - виявити в них уразливості і з'ясувати можливість їх експлуатації. Проте до тестування на проникнення потрібно обов'язково підходити зі сторони етичного хакінгу [1].

Інструментальні засоби (сканери) використовуються лише на етапі підготовки до проведення пентесту, так як вони допомагають тільки в досить звичайних випадках. В рамках етичного хакінгу аудитори проводять повний аналіз всіх деталей досліджуваного об'єкта, вибирають відповідні сценарії атак з урахуванням людського фактора, можливо, розробляють унікальне для кожного конкретного випадку програмне забезпечення чи скрипти для спроби проникнення в інформаційну систему.

Зазвичай в пентестах використовуються допрацьовані методики Draft Guideline on Network Security Testing (NIST USA) і Open-Source Security Testing Methodology (OSSTM). Вибираються об'єкти дослідження, задається модель порушника і вибирається режим тестування на основі рівня початкових знань виконавця про тестовану систему (Black Box або

White Box) і рівня інформованості замовника про випробування (режим Black Hat або White Hat). Зараз набирає популярність відкритий стандарт PTES (Penetration Testing Execution Standard) та OWASP (Open Web Application Security Project) - методика Web-додатків. Вони, як правило, описують загальні принципи проведення тесту і можуть бути використані в якості довідкового посібника або мінімального стандарту.

При проведенні пентесту важливо чітко регламентувати дії сторін, виділити узгоджені тимчасові інтервали для проведення активних дій, визначити етапність, обмеження, погоджувати дії при переході від етапу до етапу. Крім того, необхідно послідовно документувати отримані результати і на їх основі формувати пропозиції щодо виправлення виявлених проблем. Адже проведення тесту не є самоціллю, важливою частиною є подальша відпрацювання результатів тесту і усунення виявлених вразливостей.

Актуальні інструменти для пентесту

Kali Linux [3] - це Linux-based арсенал для тесту на проникнення, що допомагає фахівцям з безпеки в виконанні оцінювання у чистому середовищі, присвяченому конкретно для етичного хакінгу.

В основі роботи Kali лежить використання методики пентесту, що складається з 10 етапів, якими є: Target Scoping, Information Gathering, Target Discovery, Enumerating Target, Vulnerability Mapping, Social Engineering, Target Exploitation, Privilege Escalation, Maintaining Access, Documentation and Reporting [1]. Практично для кожного з цих етапів характерні свої програми з набору утиліт Kali Linux.

Metasploitable 2 Linux – операційна система, спеціально спроектована на максимальну вразливість для тестування, тестів експлойтів і навчання новачків. На відміну від інших вразливих віртуальних машин Metasploitable фокусується на вразливостях в операційній системі Linux і мережевих сервісах, а не на окремих додатках [4].

Практично кожен з відкритих мережевих портів є точкою для входу в систему, тобто безпосереднього успішного пентесту. Ця операційна система містить вразливі веб-сервіси (DVWA, Mutillidae), бази даних, слабкі паролі, backdoors, ризики розкриття інформації та інші неприємні речі, що вже повинні бути усунуті в найсучасніших та постійно обновлюваних ОС та сервісах.

Застосування вищезгаданого ВВПЗ для проведення тестування на проникнення в навчальних умовах

З метою навчання студентів чи будь-яких інших IT-спеціалістів ми здійснювали два такі приклади пентесту: Kali > Metasploitable2, Kali > Windows XP SP2 (тріал-версія). На нашому сервері вже попередньо встановлені віртуальні ОС, такі як Windows XP SP2, Metasploitable2, Kali Linux та ін. Це тестування дає нам змогу випробувати всі сучасні інструменти з пакету Kali Linux [2].

Таким чином студенти можуть під’єднуватись безпосередньо до сервера з віртуальною машиною ОС Kali Linux через встановлений на ПК VMWare Player. Після цього можна використовувати максимально всі можливості дистрибутива Kali з допомогою значно більших апаратних ресурсів самого сервера ніж звичайного ПК.

Висновки

Як показує практика, більшість виявлених вразливостей пов'язана з несвоєчасним оновленням ПЗ і засобів захисту, використанням попередньо встановлених параметрів налаштування ПЗ та мережевого обладнання, недотриманням політики безпеки, помилками в розробці ПЗ доступних з Інтернету сервісів і т.д.

Наше дослідження дозволить в майбутньому застосувати вищезгадане ВВПЗ в навчальних лабораторіях університету для навчання майбутніх спеціалістів в сфері безпеки. Перевага цьому ВВПЗ надається не з огляду на безкоштовність, а через високу зручність і ефективність.

Література

[1] Піскозуб А.З. Використання тестування на проникнення в комп’ютерні мережі та системи для підняття їх рівня захищеності // Матеріали третьої міжнародної науково-практичної конференції FOSS Lviv 2013,. – Львів,2013.
[2] W.Pritchett,D.Smet. Kali Linux Cookbook - Birmingham-Mumbai, Puckt Publishing, 2013
[3] Kali Linux. https://kali.org
[4] Metasploitable2. https://community.rapid7.com/docs/DOC-1875.

Berkeley Open Infrastructure for Network Computing (BOINC) - distributed computing system based on volunteers

Monika Kwiatkowska and Lukasz Swierczewski

I Maria Curie-Skłodowska University in Lublin, II College of Computer Science and Business Administration in Łomża, lswiercz@icm.edu.pl

This work describes BOINC, an open-source distributed computing system. Author explores the specific nature of a computing project which heavily relies on volunteers.

Introduction

Berkeley Open Infrastructure for Network Computing is a system that allows distributed computing [1] [2] with the use of computers connected only global network the Internet. The system is developed on the basis of a completely non-commercial and was originally initiated for the project SETI@Home [3] [4]. Currently, the solution is also adapted by projects in other areas of science such as Word Community Grid (biochemistry) [5] [6] Einstein@Home (astrophysics, the search for pulsars) [7] or OProject