аналізу волатильних даних, які можна використовувати для огляду засобів комп'ютерної техніки під час розслідування кіберзлочинів та злочинів торгівлі людьми.

Список бібліографічних посилань

1. Про Національну поліцію : Закон України від 02 лип. 2015 р. № 580-VIII. *Відомості Верховної Ради України*. 2015. № 40-41. Ст. 379.

2. Про затвердження Положення про Національну поліцію : постанова Кабінету Міністрів України від 28 жовт. 2015 р. № 877 // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/877-2015-%D0%BF (дата звернення: 31.10.2018).

3. Про основні засади забезпечення кібербезпеки : Закон України від 05 жовт. 2017 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.

4. Про протидію торгівлі людьми : Закон України від 20 вер. 2011 р. № 3739-VI. *Відомості Верховної Ради України*. 2012. № 19-20. Ст. 173.

5. Про затвердження Плану заходів з підтримки розвитку індустрії програмної продукції України на 2018 рік : розпорядження Кабінету Міністрів України від 23 трав. 2018 р. № 344-р. // Кабінет Міністрів України URL: https://www.kmu.gov.ua/ua/npas/pro-zatverdzhennya-planu-za.

6. Виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій : навч. курс / [А. Вінаков, В. Гузій, Д. Девіс та ін.]. Київ : Координатор проектів ОБСЄ в Україні, 2017. 148 с.

Одержано 31.10.2018

УДК 004.056.5

Данило Олександрович КУЛІКОВ,
курсант 3 курсу групи Ф4-302 факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ

ОЦІНКА БЕЗПЕКИ КОМП'ЮТЕРНИХ СИСТЕМ ЗА ДОПОМОГОЮ ПЕНТЕСТА

Вступ і постановка проблеми. Процес пентеста включає в себе активний аналіз системи на наявність потенційних вразливостей, які можуть спровокувати некоректну роботу цільової системи, або ж в результаті повну відмову в обслуговуванні.

Важливо виділити мету самого пентеста – це оцінка можливості його здійснення і прогноз економічних трат в результаті успішного здійснення атаки. Результатом є звіт, який містить в собі всі знайдені вразливості системи безпеки, а також може містити рекомендації щодо їх усунення. Тобто, випробування на проникнення є частиною аудиту безпеки.

Слід виділити кілька різних методик випробувань на проникнення. Основними відмінностями є наявність інформації про

досліджувану систему. Існує чотири типу систем: відкриті, закриті, напівзакриті та цільові.

При перевірці закритої системи атакуючий не має гадки відомостей про пристрій, що атакується. Завданням такого виду перевірки є збір необхідної інформації про розташування цільової системи, її інфраструктури.

У відкритих системах доступна повна інформація про цільовій системі, а в напівзакритих системах доступна часткова інформація.

Розглянемо цільові системи, до них відносяться комп'ютерні системи з доступом з мережі Інтернет. Випробування на проникнення повинно проводитися до запуску цільової системи в масове використання. Це є певний рівень гарантії, що будь-який атакуючий не зможе завдати шкоди, прямої або непрямої, роботі досліджуваної системи.

Тест а проникнення дозволяє досить швидко оцінити реальну захищеність обраних інформаційних активів від несанкціонованого доступу, моделюючи найбільш поширені атаки.

Основною відмінною особливістю тесту на проникнення в порівнянні з традиційним аудитом інформаційної безпеки (ІБ) є:

– зазвичай менша глибина охоплення інформаційної інфраструктури організації;

– велика деталізація знайдених вразливостей;

– більш точна оцінка ризиків ІБ (ґрунтується на результатах реалізації знайдених вразливостей);

– велика вірогідність результатів аудиту);

– оцінка більшої кількості процесів ІБ, ніж при інструментальному аудиті; детальне опрацювання знайдених вразливостей, що дозволяє отримати більш об’єктивну оцінку процесів забезпечення інформаційної безпеки організації.

В даний час існує декілька міжнародних методик проведення тестування на проникнення, орієнтованих в основному на моделювання атак, спрямованих на мережеву інфраструктуру організації:

– OSSTMM (Open Source Security Testing Methodology Manual) – мабуть, єдина методика, яка акцентує увагу не тільки на технічних тестах, але і на атаках пов'язаних з соціальною інженерією і спрямованих на користувачів корпоративної мережі;

– NIST SP800-115 – документ, хоча і не є методикою, але описує загальні аспекти проведення тестів на проникнення;

– ISSAF (The Information Systems Security Assessment Framework) – фреймворк (framework), орієнтований на інструментальний пошук вразливостей;

– PCI DSS (розділ 11.3 стандарту) – згідно з розділом 11.3 стандарту PCI DSS в організаціях, що відповідають стандарту, не рідше разу на рік повинен проводитися тест на проникнення. Для роз'яснення даного розділу PCI DSS був випущений документ

Information Supplement Requirement 11.3 Penetration Testing в дуже загальних рисах описує послідовність проведення інструментальної перевірки зовнішнього периметра мережевої інфраструктури, що тестується компанії (по суті, дана інструментальна перевірка не є тестом на проникнення).

Висновок. Підвівши підсумок, можливо зробити висновок про те, що тестування (пентест) на проникнення є одним з пріоритетних напрямків в інформаційній безпеці. Воно дозволяє отримати об'єктивну оцінку того, наскільки легко здійснити несанкціонований доступ до комп'ютерної системи, а також поглянути на саму систему з точки зору зловмисника, а саме – зрозуміти, яким способом можна скомпрометувати обрану систему і які шкідливі дії на неї можна робити.

Одержано 01.11.2018

УДК 351.865:681.518(477)

Дмитро Анатолійович КУПРІЄНКО,
доктор військових наук, доцент,
заступник начальника з навчально-методичної роботи
факультету підготовки керівних кадрів
Національної академії Державної прикордонної служби України ім.
Б. Хмельницького;
ORCID: https://orcid.org/0000-0002-4086-1310

ОКРЕМІ ПРИЙОМИ І СПОСОБИ ЗБОРУ КОНФІДЕНЦІЙНОЇ ТА ІНШОЇ ІНФОРМАЦІЇ ПРО ОБ'ЄКТИ ЗАЦІКАВЛЕНОСТІ В УМОВАХ ЗАГОСТРЕННЯ ВОЄННО-ПОЛІТИЧНОЇ ОБСТАНОВКИ

Сучасний стан розвитку суспільства та науково-технічного прогресу характеризується динамічними змінами у всіх сферах життєдіяльності людства, що, зокрема, пов'язано з глобальною інформатизацією. З'явились нові засоби зв'язку та вдосконалились способи і методи обміну інформацією, її поширення з використанням Інтернет-технологій. Разом із позитивними змінами, розвиток інформаційних технологій сприяв загостренню існуючих та виникненню нових загроз національній безпеці, що є особливо «чутливим» в умовах загострення воєнно-політичної обстановки. Так, наприклад, супротивник використовує можливості глобальної інформатизації для ідентифікації конкретних посадових осіб, встановлення місць дислокації збройних формувань та підрозділів правоохоронних органів, розташування об'єктів критичної інфраструктури та інших об'єктів зацікавленості з метою організації та здійснення психологічного «тиску», планування вогневого ураження тощо. Отже, наведемо окремі прийоми та способи збору