Змагання CTF у стилі Jeopardy схожий на справжню гру Jeopardy, так як табло виглядає як дошка цієї гри з різними категоріями та точковими значеннями. Там може бути більше двох команд, оскільки команди не намагаються атакувати один одного. Деякі категорії можуть включати криптографію, стеганографію, фізичну безпеку та сканування. Існує кілька інших категорій, які можна використовувати, наприклад деякі виклики можуть бути зроблені проти основного сервера, який був розроблений для CTF, а прапор вводиться до табло CTF. Таймер використовується для запуску та зупинки CTF, і після завершення таймера гра закінчується. Команда з найбільшою кількістю очок на кінець виграє.

Як згадувалось раніше, CTF тепер є глобальним рухом в Інтернеті. Зараз з'явилася велика кількість CTF завдань для підготовки спеціалістів з кібербезпеки. Завдання типу «атака – захист» є симуляцією атак на веб сервери і дозволить кіберполіції навчитися протистояти кібератакам і підтримувати життєдіяльність серверів поліції та державних органів. А завдання Jeopardy являється симуляцією комп'ютерів зі слідами атак зловмисників та прихованої ними інформації, вони краще всього покажуть як на практиці працювати з комп'ютерами справжніх кіберзлочинців та зрозуміти їх тактику.

Одержано 15.04.2019

УДК 004.939

Поліна Іванівна ПОПОВСЬКА,
курсант групи Ф4-302 ХНУВС
Науковий керівник: кандидат технічних наук, доцент Клімушин П. С.

ЦИФРОВА КРИМІНАЛІСТИКА (ФОРЕНЗИКА) ЯК ПРИКЛАДНА НАУКА АНАЛІЗУ ТА РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Форензика – прикладна наука про розкриття злочинів, пов'язаних з комп'ютерною інформацією про дослідження цифрових доказів, методи пошуку, отримання і закріплення таких доказів. Вона вивчає методи отримання та дослідження доказів, обґрунтовує збір і аналіз даних у інформаційних системах (ІС), комунікаційних потоках, системах управління базами даних та зберігання інформації в порядку, допустимого в суді.

Комп'ютерна криміналістика є новим науковим напрямом, де лише починає накопичуватися практичний досвід та технології і розв'язуються такі основні завдання: розроблення криміналістичних характеристик злочинів, пов'язаних з інформаційними відносинами; розроблення тактики оперативно-розшукових заходів (ОРЗ), агентурної роботи і слідчих дій, пов'язаних з інформаційними відносинами; розроблення методів, програмно-апаратних засобів для збору й дослідження доказів скоєння кіберзлочинів.

У комп'ютерній криміналістиці застосовуються і спеціальні методи досліджень, які притаманні тільки цій галузі: створення спеціалізованих криміналістичних ІС; створення віртуального користувача для проведення ОРЗ; збір хеш-функцій відомих файлів для розмежування їх від файлів, які містять оригінальну користувацьку або модифіковану інформацію; архівування повного вмісту фізичних носіїв з метою подальшого розслідування імовірних інцидентів; емулювання мережевих сервісів корпоративних комп'ютерних мереж і VPN-мереж із віддаленим доступом для експертного дослідження вилученого програмно-технічного забезпечення у лабораторних умовах.

До основних завдань комп'ютерно-технічної експертизи (КТЕ) належать: установлення робочого стану комп'ютерно-технічних засобів; установлення обставин, пов'язаних із використанням комп'ютерно-технічних засобів, інформації та програмного забезпечення; виявлення інформації та програмного забезпечення, що містяться на комп'ютерних носіях; установлення відповідності програмних продуктів певним версіям чи вимогам на його розробку.

Одним із найважливіших завдань цифрової судової експертизи є накопичення та збереження доказів так, щоб забезпечити їх цілісність. Як і у випадку звичайних фізичних даних, важливо зберегти ланцюг контролю над усіма цифровими доказами, гарантуючи, що вони збираються та захищаються через структуровані процеси, прийнятні для судів. Це вимагає, щоб був досягнутий визначений базовий рівень контролю безпеки інформації.

Результати наукових досліджень у галузі розслідування злочинів, скоєних із використанням інформаційних технологій, дослідження цифрових доказів, методів пошуку, отримання та фіксування таких доказів дають підстави виокремити такі криміналістичні проблеми: відсутність науково обґрунтованої методики збирання доказів, які фіксуються під час проведення огляду місця події; встановлення автентичності інформації на матеріальних носіях під час проведення КТЕ матеріалів, які отримано шляхом ОРЗ; коректність теоретичних засад і методик, які були застосовані експертом під час проведення досліджень; нехтування у процесі КТЕ вимогами державних та міжнародних стандартів у галузі ІТ.

В Україні розроблені власні національні рекомендації та процедури для накопичення та захисту електронних доказів. Однак це створює проблеми під час розслідування транскордонних кіберзлочинів.

Одержано 16.04.2019