облікових записів. Також важливим є уникнення підозрілих сайтів і збереження вашого комп'ютера від шкідливого програмного забезпечення. Використання більш потужних паролів не допоможе вам захиститися від усіх загроз, але це перший й дуже важливий крок.

Одержано 12.04.2019

УДК 332.012

Владислав Романович ПЛЕХАНОВ,
курсант групи Ф4-202 ХНУВС
Науковий керівник: кандидат технічних наук, доцент Клімушин П. С.

ВИКОРИСТАННЯ ЗМАГАНЬ МІЖ ФАХІВЦЯМИ З БЕЗПЕКИ ДЛЯ ПІДГОТОВКИ КІБЕРПОЛІЦЕЙСЬКИХ

Кібербезпека є високим пріоритетом для держави та компаній, малих і великих, тому що останнім часом в країні спостерігається зростання числа кібератак. У відповідь на це майбутні фахівці повинні пройти ретельну підготовку та зрозуміти як саме працюють хакери та як від них захищатись. Один із новітніх способів навчання в галузі кібербезпеки– це змагання між фахівцями з безпеки під назвою захоплення флага (capturetheflag – CTF). Цей конкурс використовується як навчальний посібник для всіх, хто цікавиться кібербезпекою, і може допомогти покращити навички та інструменти, які вони використовували під час навчання.

CTF для кібербезпеки була вперше розроблена та розміщена ще в 1996 році в Лас-Вегасі, штат Невада, але лише зараз вона має можливість проявити себе, коли обчислювальна техніка на достатньому рівні підтримує функції віртуалізації операційної системи. Турніри CTF глобальні, оскільки вони не мають кордонів і можуть бути зроблені через Інтернет. Міжнародні команди змагаються за різні призи, чемпіонами CTF з України є команда DCUA. Існує два формати CTF для кібербезпеки «атака-захист» та гра Jeopardy з різними категоріями та точковими значеннями.

CTF «атака-захист» –є атакуюча команда, а також та яка захищає свою власну систему. Зазвичай існує два раунди гри, в якій однією командою є атакуюча команда, а інша команда є захисною командою в першому раунді, а потім переходять на другий тур. У оборонних машинах є прапори (текстові файли, папки, зображення тощо), які команда атакуючих намагається знайти, оскільки вони компрометують машини. Команда, що належить, може використовувати різні інструменти зловмисника для того, щоб поставити під загрозу захисні машини, але існують правила, які гарантують, що команди не мають переваг перед іншим. Команда-захисник може зробити що-небудь в рамках правил, щоб захистити свої машини від атакуючої команди. Їм заборонено вимикати будь-які мережні з'єднання або вимикати пристрої. Якщо є якесь порушення правил, команда понесе штраф або дискваліфікується.

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.