НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
“ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМ. ЮРІЯ КОНДРАТЮКА”

КАФЕДРА КОМП’ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І СИСТЕМ

Є.О. ЖИВИЛО

ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

НАВЧАЛЬНИЙ ПОСІБНИК

Частина 2

ПОЛТАВА – 2024

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
“ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМ. ЮРІЯ КОНДРАТЮКА”

КАФЕДРА КОМП’ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І СИСТЕМ

Є.О. ЖИВИЛО

ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

За редакцією Є.О. ЖИВИЛО

НАВЧАЛЬНИЙ ПОСІБНИК

Частина 2

2024

УДК 004.492.2

ББК 32.971.35-5

Рецензенти:

С.А. Мікусь, доктор технічних наук, професор, заступник начальника Інституту інформаційно-комунікаційних технологій та кібероборони Національного університету оборони України;

В.В. Васюта, кандидат технічних наук, доцент, доцент кафедри комп'ютерних та інформаційних технологій і систем Навчально-наукового інституту інформаційних технологій та робототехніки Національного університету "Полтавська політехніка ім. Юрія Кондратюка".

Навчальний посібник розроблено за редакцією доцента кафедри комп'ютерних та інформаційних технологій і систем, кандидатом наук з державного управління Є.О. Живило.

Тестування на проникнення: навч. посіб. / [Є.О. Живило]; за ред. Є.О. Живило. – П.: ПНТУ "Полтавська політехніка ім. Юрія Кондратюка", 2024. – 239 с.

Навчальний посібник охоплює програмний матеріал підготовки студентів 12 Галузі знань «Інформаційні технології» за спеціальностями 125 - Кібербезпека та захист інформації. Навчальне видання укладено за матеріалами лекцій, групових та практичних занять з дисципліни "Основи інформаційної та кібернетичної безпеки", а також з дисциплін "Кібер-безпека", "Захист інформації", "Захист інформації в інфокомунікаційних системах". Посібник призначений для студентів, що навчаються за спеціальностями 12 Галузі знань «Інформаційні технології», а також для самостійного вивчення методів, способів і засобів пентестування студентами інших спеціальностей.

У посібнику висвітлено широкий спектр методик проведення кібератак та алгоритмів аудиту які можна виконати для оцінки стану захищеності об'єкта. Завдяки практичному підходу, слухачі зрозуміють як застосовувати Metasploit Framework, що до експлуатації вразливих додатків, а також порядок використання єдиних прогалин в захисті електронних комунікаційних систем, з метою обходу всіх засобів захисту периметра. Також слухачі

опробують теоретичну складову посібника на її запропонованій практичній складовій щодо обходу антивірусних програм та проведення соціально-інженерійних атак за допомогою таких інструментів, як SocialEngineer Toolkit. Навчаємі зрозуміють як зламати корпоративну Wi-Fi мережу та як використовувати Georgia's Smartphone Pentest Framework, щоб оцінити, наскільки шкідливою може бути політика компанії щодо використання власних пристроїв (або її відсутність).

У першому розділі розглянуті різні методи та сценарії проведення кібератак на системи захисту інформації та кібербезпеки, включаючи атаки на неправильно налаштовані веб-сервери, piggy-бекінгу на уразливе програмне забезпечення, використання слабкого контролю доступу до відкритих та конфіденційних файлів, використання вразливостей у базовій системі та використання проблем у сторонньому програмному забезпеченні.

У другому розділі розкриті основи базової розробки експлойтів з використанням технік перенесення відкритого коду експлойтів для задоволення власних потреб, а також написання власних модулів Metasploit. Також висвітлено деякі методи зменшення впливу експлойтів.

У третьому розділі розглянуто методики проведення кібератак на мобільні пристрої Android та iPhone, віддалене керування пристроями за допомогою USSD-кодів, а також застосування атак, на кшталт NFC та SMS та використання SPF-агенту.

Рекомендовано до друку науково-методичною радою Національного університету "Полтавська політехніка імені Юрія Кондратюка"
Протокол № 3 від 26 квітня 2024 р.

ЗМІСТ