НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
“ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМ. ЮРІЯ КОНДРАТЮКА”

КАФЕДРА КОМП’ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І СИСТЕМ

Є.О. ЖИВИЛО

ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

НАВЧАЛЬНИЙ ПОСІБНИК

Частина 1

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 1

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. Ч.1 / [Є.О. Живило]; за ред. Є.О. Живило. – П.: ПНТУ "Полтавська політехніка ім. Юрія Кондратюка", 2024. – 134 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 "Кібербезпека", "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 атак, які можна виконати для оцінки стану захищеності об'єкта. Завдяки практичному підходу, слухач зрозуміє як застосовувати Metasploit Framework, що до експлуатації вразливих додатків, а також порядок використання прогалин в захисті системи, з метою обходу всіх засобів захисту периметра, викачувати дані з визначених систем. Також слухачі опробують теоретичну складову посібника на її

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

У першому розділі розглянуті основні визначення етапів тестування на проникнення. Розкрито практичний підхід, щодо створення власної лабораторії для виконання вправ з пентестування. Охарактеризовано деякі типові завдання Linux. Також висвітлена навігація файловою системою Linux, робота з даними та запуск служб. Окремо розглянуті команди середовища Linux, їх налаштування та запуск, а також порядок контролю атакуємого об'єкта.

У другому розділі розкриті деякі базові приклади комп'ютерного програмування, а також порядок власного написання програм на декількох мовах. Визначено базові конструкції скриптів, порядок їх виведення та використання, опрацьована система корисного навантаження Metasploit.

У третьому розділі охоплено порядок використання таких інструментів як theHarvester, Maltego, Nmap, що дозволяє здійснити пошук та дослідження вразливостей в системах які можна використати для проведення атак, мислити як зловмисник. Також у цьому розділі було розглянуто вплив на мережевий трафік, а саме порядок його перехопленння та перенаправлення (ARP та DNS – кеш), збирання дійсних облікових даних для FTP-сервера та інше.

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

ЗМІСТ