ВСТУП

Сучасний світ стрімко рухається до цифровізації, що призводить до зростання кількості інформаційних загроз. Хакерські атаки стають дедалі складнішими, а їх наслідки можуть бути критичними для компаній, державних установ та окремих користувачів. Захист інформаційних систем стає першочерговим завданням, і саме етичний хакінг відіграє ключову роль у забезпеченні безпеки цифрового середовища. Етичний хакінг – це дисципліна, що поєднує знання з кібербезпеки, програмування, аналізу ризиків та тестування інформаційних систем. Основна мета етичного хакінгу полягає у виявленні та усуненні вразливостей у системах до того, як ними зможуть скористатися зловмисники. Таким чином, етичні хакери працюють на випередження, допомагаючи організаціям зміцнювати свої системи безпеки.

Етичний хакінг базується на кількох ключових принципах, серед яких законність, прозорість, конфіденційність, аналіз ризиків і впровадження покращень. Усі дії етичного хакера повинні здійснюватися в межах законодавства та етичних норм, бути задокументованими та погодженими з власниками системи, а отримані під час тестувань дані не повинні розголошуватися стороннім особам. Важливим аспектом є також оцінка потенційних загроз та надання рекомендацій щодо усунення виявлених проблем.

Існує кілька основних методів тестування інформаційних систем, які застосовують етичні хакери. Одним із ключових є тестування на проникнення, яке передбачає імітацію атак для оцінки рівня безпеки системи. Аудит безпеки дозволяє перевірити конфігурацію програмного забезпечення та апаратних засобів. Соціальна інженерія зосереджується на тестуванні людського фактора безпеки, включаючи спроби отримати конфіденційну інформацію через маніпуляції. Форензика аналізує

наслідки кібератак та допомагає знайти сліди зловмисників, а реверс-інжиніринг дозволяє досліджувати програмний код для виявлення потенційних загроз.

Для ефективної роботи етичні хакери використовують широкий спектр інструментів, зокрема Nmap для сканування мереж, Metasploit для автоматизованого тестування на проникнення, Wireshark для аналізу трафіку, Burp Suite для тестування веб-додатків та John the Ripper для перевірки стійкості паролів. Використання цих інструментів дозволяє виявляти та аналізувати слабкі місця інформаційних систем.

Тестування на проникнення зазвичай складається з кількох етапів. Спочатку здійснюється розвідка, під час якої збирається інформація про цільову систему. Наступний етап – сканування, яке дозволяє виявити відкриті порти та активні сервіси. Після цього відбувається експлуатація вразливостей, що дає змогу оцінити рівень загрози. Далі перевіряється можливість закріплення доступу, що імітує сценарії довготривалого контролю над системою. Завершальним етапом є аналіз і звітність, що передбачає документування результатів тестування та надання рекомендацій щодо усунення виявлених вразливостей.

Цей підручник має на меті надати читачам як теоретичні знання, так і практичні навички з етичного хакінгу. Він включає детальні описи методів тестування безпеки, інструментів, сценаріїв атак та способів їхнього запобігання. У ньому представлені реальні кейси та практичні завдання, які дозволять здобувачам освіти глибше зрозуміти принципи кібербезпеки. Посібник буде корисним студентам технічних спеціальностей, спеціалістам з інформаційної безпеки, системним адміністраторам, розробникам програмного забезпечення та підприємцям, які прагнуть захистити свої цифрові активи.

Етичний хакінг є важливим напрямком у сфері кібербезпеки, що дозволяє організаціям виявляти та усувати потенційні загрози до того, як ними скористаються зловмисники. Освоєння цієї дисципліни

допоможе спеціалістам запобігати кібератакам, захищати інформаційні системи та забезпечувати безпечне функціонування цифрового простору. Цей підручник допоможе читачам отримати практичний досвід і сформувати необхідні компетенції для успішної кар'єри в галузі етичного хакінгу та кібербезпеки.