УДК 510.635:004.891(045)

А.І. Слюсар
Національна академі Служби безпеки України, Київ

ЕФЕКТИВНІСТЬ СУЧАСНИХ МЕТОДІВ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ В КОНТЕКСТІ КІБЕРБЕЗПЕКИ

З розвитком інформаційних технологій та глобальної інфраструктури Інтернету важливість безпеки мережі стає все більш важливою. Тестування на проникнення є одним із ключових інструментів для захисту комп'ютерних систем і мереж. У цій статті розглядаються сучасні методології тестування на проникнення на основі аналізу авторитетних джерел і практичних застосувань. Особливу увагу приділено технічним аспектам і деталям реалізації цих методів.

Автоматичні сканери вразливостей, такі як Nessus, OpenVAS і Nexpose, можуть швидко виявляти вразливості в системах і мережах [1,2]. Вони забезпечують огляд великої кількості систем за короткий проміжок часу, але можуть забезпечити обмежений аналіз і вимагати ручного втручання експерта для виявлення складніших уразливостей.

Автоматизовані засоби атаки на паролі, такі як John the Ripper, Hashcat і Hydra, можуть виявляти слабкі паролі та відновлювати хешовані паролі [3]. Ці інструменти ефективні для виявлення слабких паролів, але можуть бути менш успішними для взлому надійних паролів і безпечних систем.

Проведення симульованої атаки «Red Team» дозволяє імітувати реальну атаку, що допомагає виявити слабкі місця в системі та оцінити ефективність заходів безпеки [4]. Цей підхід передбачає багатосторонню атаку, включаючи соціальну інженерію, фізичне проникнення та використання вразливостей мережі.

Підхід «Білої команди» передбачає реалізацію заходів активного захисту, спрямованих на підвищення рівня безпеки системи та запобігання можливим атакам [5]. Ці методи включають моніторинг мережі, оцінку ризиків і реагування на інциденти кібербезпеки.

Такі метричні системи, як CVSS, DREAD і метод оцінки ризику OWASP, дозволяють оцінити ефективність тестування на проникнення та розробити стратегії підвищення безпеки [6]. Ці

системи враховують усі аспекти вразливості та допомагають приймати обґрунтовані рішення щодо розподілу ресурсів для підвищення безпеки мережі.

Для підвищення ефективності тестування на проникнення необхідна інтеграція автоматизованих методів і сучасних методів [7]. Це передбачає планування та виконання всебічного тестування, аналіз результатів і внесення змін до систем безпеки для підвищення їх ефективності.

Для забезпечення ефективності тестування на проникнення основна увага приділяється навчанню персоналу та розвитку культури кібербезпеки. Це передбачає проведення навчальних семінарів, регулярне оновлення знань експертів та підвищення обізнаності користувачів щодо кіберзагроз.

Сучасні методи тестування на проникнення в контексті кібербезпеки включають як автоматизовані інструменти, так і комплексні підходи до оцінки та підвищення рівня захисту систем. Інтеграція автоматизованих методів з сучасними підходами дозволяє підвищити ефективність тестування на проникнення та розвивати культуру кібербезпеки. Підготовка персоналу та залучення співробітників до процесу забезпечення кібербезпеки є важливими аспектами успішного застосування методів тестування на проникнення.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Tenable. Nessus. – 2021 https://www.tenable.com/products/nessus

2. Greenbone Networks – 2021 – OpenVAS. https://www.openvas.org

3.Steube, J. Hashcat – 2021 – https://hashcat.net/hashcat/

4.Red Team Journal. What is a Red Team? – 2021 – https://redteamjournal.com

5.National Initiative for Cybersecurity Education (NICE) – 2021 – White Team Roles and Responsibilities. https://www.briskinfosec.com/blogs/blogsdetail/Red-vs-Blue-vs-Purple-vs-Orange-vs-Yellow-vs-Green-vs-White-Cybersecurity-Team

6.CVSS, DREAD, and OWASP Risk Rating Methodology – 2021 – https://owasp.org/www-community/Application_Threat_Modeling

7.McMillan, R. Integrating Automated and Manual Penetration Testing. – 2021 – https://www.darkreading.com/vulnerabilities-threats/integrating-automated-and-manual-penetration-testing/a/d-id/1334610