УДК 004.056.2

Володимир Леонідович БУРЯЧОК,
доктор технічних наук, професор,
завідувач кафедри інформаційної та кібернетичної безпеки
Київського університету імені Бориса Грінченка;
ORCID: https://orcid.org/0000-0002-4055-1494;
Володимир Юрійович СОКОЛОВ,
старший викладач кафедри інформаційної та кібернетичної безпеки
Київського університету імені Бориса Грінченка;
ORCID: https://orcid.org/0000-0002-9349-7946

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ОБ'ЄКТИВНОГО КОНТРОЛЮ ЗАХИЩЕНОСТІ КОРПОРАТИВНИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ І МЕРЕЖ

Історія розвитку інформаційного суспільства тісно переплетена, як відомо, з інформаційними операціями. Останнім часом це призводить до того, що заходи по маніпуляції інформацією, дезінформації конкуруючих сторін і/або введення їх один одного в

оману є невід'ємною частиною внутрішньої і зовнішньої політики переважної більшості держав [1]. Головну роль в цих процесах нині відіграє Інтернет – п'ята влада світу.

Кількість державних і комерційних структур, схильних до таких дій останнім часом значно збільшилася. Насамперед цьому сприяє «продуктивна робота» дійових осіб інформаційного і кіберпростору: легальних користувачів, хакерів, кіберзлочинців і кібертерористів, а також підрозділів сучасних кібервійськ. Саме вони, будучи підкріпленими новими можливостями по злому веб-сайтів, серверів додатків і баз даних, здатні заподіяти не тільки прямі фінансові втрати критично важливим об'єктам інфраструктури країн світу (енергетичній і транспортній магістральним мережам, нафто- і газопроводам, каналам швидкісного і урядового зв'язку, високотехнологічним підприємствам та підприємствам оборонно-промислового комплексу, центральним органам влади, установам освіти та охорони здоров'я, фінансовому сектору тощо).

З огляду на викладене можна сформулювати наступну гіпотезу, що стала останнім часом, на жаль, гнітючою реальністю: чим більше ІТ розвиваються і інтегруються в наше повсякденне життя, тим більш важливими і затребуваними в будь-яких сферах людської діяльності стають технології інформаційної безпеки (ІБ). Підтвердженням цьому можуть служити статистичні дані, оприлюднені корпорацією Web Application Security Consortium (WASC), згідно з якими уразливими до хакерських атак стають більш 96,85% веб-сайтів, близько 74% прикладного та системного програмного забезпечення (ПЗ), приблизно 68% серверних додатків [2]. При цьому не тільки в прикладному і системному ПЗ, але і в серверних додатках домінують ті ж уразливості: відмова в обслуговуванні, компрометація системи і підвищення привілеїв.

З цим погоджуються і фахівці з міжнародної організації Computer Emergency Response Team (CERT). Разом з тим вони стверджують [3], що кількість виявлених вразливостей щорічно стрімко збільшується.

Для запобігання впливу таких і подібних до них вразливостей на власну інфраструктуру, а також її захисту від ряду зовнішніх і внутрішніх загроз, більшість країн світу виділяє нині колосальні фінансові кошти [4]. Але, на жаль, досить часто буває так, що дороге антивірусне ПЗ і дорогі апаратні брандмауери не потрібні більшості замовників, крім для теоретичних доказів того, що вкладені кошти роблять їх мережі від хакерських атак більш захищеними.

Власне аудит ІБ починається з аналізу ризиків і загроз. Він призначений для виявлення найбільш небезпечних загроз з точки зору системи захисту. Елементи тестування на проникнення при цьому можуть (у відповідності зі стандартом ISO 17799) використовуватися для оцінки ефективності реалізації таких захисних механізмів, як «захист від злоякісного коду», «забезпечення мережевої безпеки» та ін. В ході тестування аудитор грає роль зловмисника, мотивованого на

порушення безпеки IT-систем (мереж) замовника (державної або комерційної структури). Його завдання полягає в тому, щоб знайти відповіді на такі питання: «Як простіше потрапити всередину системи, порушити її працездатність або що-небудь отримати?» та «Якою може бути мінімальна ціна злому?». Інтенсивним перевіркам при цьому піддаються, перш за все, програмні і технічні засоби захисту IT систем та мереж з метою визначення в них потенційних проломів: незакритих вразливостей ПЗ, відкритих портів тощо. Для цього аудитор застосовує, як правило, ряд стандартних інструментів, які мають різну чутливість до різного роду загроз [5].

За даними компанії Positive Technologies [6] в ході проведення тестування на проникнення для тестів часто використовуються уразливості наведені на рис. 1.

Рис. 1. Вразливості, характерні для проведення тестів на проникнення

Отримавши перелік можливих вразливостей аудитор проводить їх експлуатацію. Методи та інструментарій вибираються при цьому індивідуально для кожного типу вразливості. Особлива увага приділяється питанню перехоплення паролів користувачів шляхом їх підбору до різних мережевих сервісів [7], проведення атак типу «людина посередині» та ін.

В ході тестування на проникнення вдається, як правило, отримати доступ до: веб-сайтів – в 50% випадків; електронній пошті – в 40%; бізнес-програмам – в 35%; IP-телефонії – в 10%; систем дистанційного банківського обслуговування – в 29%. Повний контроль над інфраструктурою може бути отриманий ними не більше ніж в 25% проектів, а в 5% – тестувальникам взагалі не вдається подолати периметр.

До найпопулярніших вразливостей експерти в області інформаційної безпеки останнім часом відносять: міжсервісне виконання сценаріїв (50%); наявність інтерфейсів віддаленого керування (47%); доступна інформація про додатки (45%); вбудовування SQL-коду (63%).

Найпопулярнішою вразливістю за висновками експертів зараз є прості паролі адміністраторів. Вони зустрічаються в 80% проектів, іноді навіть в тих випадках, коли в організаціях були впроваджені політики щодо забезпечення складності паролів для рядових користувачів. Уразливості веб-додатків і некоректно налаштоване обладнання несуть за собою значно менші ризики, і тому є ключем до злому відповідно в 46 і 38% випадках. Відсутність оновлень сприяє успішному проведенню тестових атак в 25% компаній, а недоліки архітектури – в 9%.

З огляду на таке, саме проведення тестування на проникнення дозволить:

– дізнатися можливості здійснення загроз безпеки інформації;

– оцінити наслідки спрямованої хакерської атаки;

– визначити уразливості в захисті інформаційної системи;

– оцінити ефективність засобів захисту інформації;

– оцінити ефективність менеджменту інформаційної безпеки;

– оцінити можливий рівень кваліфікації порушника для успішної реалізації атаки;

– отримати аргументи для обґрунтування подальшого вкладення ресурсів в ІБ;

– виробити список контрзаходів, з тим щоб знизити можливість реалізації атак.

За погодженням із замовником при тестуванні на проникнення, додатково, може проводитися перевірка [8-10]: базових робіт по контролю захищеності бездротових мереж; зовнішнього периметра і відкритих ресурсів на можливість DOS атак, а також оцінки ступеня стійкості мережевих елементів і можливого збитку при їх проведенні; стійкості мережі, шляхом моделювання атак на протоколи канального

рівня STP, VTP, CDP, ARP; стійкості маршрутизації, шляхом моделювання фальсифікації маршрутів і проведення DOS (DDOS) атак проти використовуваних протоколів маршрутизації; мережевого трафіку, з метою отримання, наприклад, паролів користувачів, конфіденційних документів тощо; можливості отримання зловмисником несанкціонованого доступу до конфіденційної інформації або інформації обмеженого доступу замовника (проводиться перевіркою прав доступу до різних IP-адрес замовника з привілеями, отриманими на різних етапах тестування) і т. ін.

Підготовка фахівців з тестування на проникність є частиною міжнародного проекту «Магістерська програма нового покоління експертів в інформаційній безпеці» (проект 544455-TEMPUS-1-2013-1-SE-TEMPUS-JPCR, 2013–2018 рр.), в межах якого проводилися також наукові роботи [11] і [12] з тестування на проникнення.

Висновок. Не дивлячись на досить часту критику тестування на проникнення, технологія реалізації якого не може гарантувати замовнику того, що: тестувальник виявив все «дірки» в системі безпеки замовника; знайдені тестувальником «дірки» не згодом використані для заволодіння інформацією, що належить замовнику; діяльність тестувальника може бути замовником повністю проконтрольована; в умовах сучасної інформаційної і кібервійни, яка ведеться проти нашої країни, завдання щодо забезпечення безпеки інформаційних систем на об’єктах інформаційної діяльності та, перш за все, ІТ-систем (мереж) органів влади і критичних інфраструктур (соціальних фондів і різних державних реєстрів), а також об’єктивної оцінки рівня безпеки цих структур без проведення тестування на проникнення практично нездійсненна.

Список бібліографічних посилань

1. Киричок Р. В., Складанний П. М., Бурячок В. Л., Гулак Г. М., Козачок В. А. Проблеми забезпечення контролю захищеності корпоративних мереж та шляхи їх вирішення. *Наукові записки Українського науково-дослідного інституту зв’язку*. 2016. № 3 (43). С. 48–61.

2. Статистика уязвимостей web-приложений за 2008 год. URL: https://www.ptsecurity.com/ru-ru/download/WASS-SS-2008-ru.pdf (дата звернення: 31.10.2018).

3. Безопасность АСУ ТП в цифрах. URL: https://www.ptsecurity.com/upload/ptru/analytics/ICS-Vulnerability-2016-rus.pdf (дата звернення: 31.10.2018).

4. Каталков Д. Уязвимости корпоративных информационных систем в 2015 году. URL: https://www.ptsecurity.com/ru-ru/ics/Webinar_14042016.pdf (дата звернення: 31.10.2018).

5. Бурячок В. Л., Козачок В. А., Складанний П. М. Пентестінг як інструмент комплексної оцінки ефективності захисту інформації в розподілених корпоративних мережах. *Сучасний захист інформації*. 2015. № 3. С. 4–12.

6. Контроль защищенности и соответствия стандартам Positive Technologies. URL: ftp://ftp.software.ibm.com/software/security/products/qradar/documents/iTeamaddendum/m_vuln_MaxPatrol.pdf (дата звернення: 31.10.2018).

7. Бурячок В. Л., Борсуковський Ю. В., Складанний П. М. Аналіз сучасних вимог до створення парольних політик корпоративних користувачів. *Сучасний захист інформації*. 2016. № 3. С. 72–76.

8. Впровадження європейської кібербезпеки: загальний огляд. URL: http://www.isaca.org/Knowledge-Center/Research/Documents/European-Cybersecurity-Implementation-Overview_res_Ukr_1215.pdf (дата звернення: 31.10.2018).

9. Дорофеев А. Тестирование на проникновение: демонстрация одной уязвимости или объективная оценка защищенности? URL: http://elibrary.ru/item.asp?id=23143917 (дата звернення: 31.10.2018).

10. Лепихин В. Сравнительный анализ сканеров безопасности. URL: http://www.itsecurity.ru/news/reliase/2008/12_22_08.htm (дата звернення: 31.10.2018).

11. Бурячок В. Л., Астапеня В. М., Соколов В. Ю. Способы повышения доступности информации в беспроводных системах стандарта IEEE 802.11 с MIMO. *Сучасний захист інформації*. 2016. №2. С. 60–68.

12. Taj Dini M., Sokolov V. Yu. Penetration Tests for Bluetooth Low Energy and ZigBee. *Сучасний захист інформації*. 2018. № 1. С. 82–89.

Одержано 31.10.2018