УДК 004.056

Киричок Р.В.

ТЕСТ НА ПРОНИКНЕННЯ ЯК ІМІТАЦІЙНИЙ ПІДХІД ДО АНАЛІЗУ ЗАХИЩЕНОСТІ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

У даній статті проаналізовано основні методи та етапи проведення кібернападу з метою кращого розуміння зловмисників та розглянуто анатомію тесту на проникнення. А також запропоновано використання пентесту як імітаційного підходу до проведення комплексного аналізу та отримання об'єктивної оцінки рівня захищеності, тим самим допомагаючи співробітникам служби безпеки виконати відповідні перевірки системи захисту корпоративних інформаційних систем.

Ключові слова: корпоративна інформаційна система, кібератака, зловмисник, шкідливе програмне забезпечення, тестування на проникнення.

Вступ

Майже щодня з джерел масової інформації або просто мандруючи новинними сайтами всесвітньої павутини можна знайти інформацію щодо нового кіберінциденту, або лише спроби кібернетичного нападу на ту чи іншу компанію. Цьому також свідчить щорічний звіт американської компанії з розслідувань корпоративних кіберінцидентів та аналізу ризиків – Kroll, в якому відображено результати опитувань керівників різноманітних компаній з різних країн світу. Загалом, згідно останнього звіту [1], 84% опитаних, повідомляють про те, що їх компанія стала жертвою принаймні одного випадку шахрайства за останні 12 місяців, а 86% – постраждали від кібернетичних атак або викрадення даних/інформації. Хоча в деяких країнах та галузях ця кількість перебуває майже на 100%-у рівні.

Таким чином, опубліковані дані свідчать про те, що в 2017 році компанії частіше стикалися саме з спробами злому та подальшого проникнення в їх корпоративні інформаційні системи (КІС) аніж зі звичайним шахрайством. Тим самим вказуючи на тенденцію зростання інтересу до кібернетичних атак і появи так званих script kiddy – початківців у хакерській культурі, або людей які хочуть здаватися великими хакерами, при цьому використовуючи вже розроблені програми та написані скрипти для атак на комп'ютерні системи та мережі, не розуміючи механізму їх дії. Цьому факту сприяла розробка все більш новітніх хакерських інструментів, які стають простішими у використанні, оскільки інтуїтивно зрозумілі для початківців та легкодоступні для громадськості, однак разом з цим стають більш функціональними, небезпечними та надзвичайно всеосяжними (всебічними – за рахунок збільшення векторів атак). Та навпаки, можливості інженерно-технічних заходів та засобів забезпечення захищеності корпоративних інформаційних систем (КІС) від кібернетичних нападів, а також побудова дорогих багаторівневих систем захисту мають тенденцію до зниження перед новими загрозами. Саме тому необхідність в проведенні аналізу запропонованих методів захисту та стійкості КІС до атак стає все більш актуальною.

Одним із найдієвіших способів проведення комплексного аналізу та отримання об'єктивної оцінки рівня захищеності, а також поглянути на систему з точки зору зловмисника, залишається проведення так званого пентесту (тестування на проникнення) реально функціонуючих систем, а не лише їх моделей. Даний метод активного аналізу безпеки дозволяє зімітувати реальні кібернетичні напади на інфраструктуру інформаційних систем та мереж, з метою визначення не лише їх потенційно уразливих місць, але й можливостей проексплуатувати дані вразливості, тим самим визначаючи до яких ресурсів порушник може здійснити несанкціонований доступ, і які загрози інформаційної безпеки зможе реалізувати.

Основна частина

Кібератака або хакерська атака (у вузькому розумінні) – це спроба реалізації загрози кіберзловмисниками (хакерами). Використовуючи різноманітні комбінації виявлених вразливостей, недоліки конфігураційних файлів систем та прогалини визначеної в корпорації політики безпеки, в залежності від своїх цілей, зловмисники можуть реалізувати різноманітні

сценарії та навіть цілі стратегії нападу, при цьому залишившись непоміченими. Дані стратегії можуть бути спрямовані на різні ресурси КІС та включати багатоетапні ланцюги атакуючих дій, які в більшості випадків розпочинаються з імпортування та встановлення вірусів чи троянів на комп'ютери компаній через мережу Інтернет або надсилання шкідливих сценаріїв за допомогою електронної пошти, що дозволяє зловмисникам практично з легкістю заражати свої бажані цілі. До того ж, потрібно відзначити, що успіх атак вимірюється (визначається) на основі трьох факторів: (1-й) складність, необхідна для пошуку уразливостей (уразливих точок – дір) в системах; (2-й) складність запуску та успішної реалізації певного виду атаки; (3-й) складність у виявленні самого факту нападу на систему.

З вище сказаного слідує, що для кращого розуміння того як необхідно захищати КІС, тобто запобігати відомим атакам та успішно протистояти новітнім, необхідно зрозуміти атакуючого та поглянути на систему з його точки зору, тим самим максимально дізнатися які цілі (інформаційні активи) можуть цікавити зловмисника, як здійснюється розвідка (збір інформації), яким чином визначаються найбільш критично уразливі місця системи та які з вразливостей можна дійсно використати (проексплуатувати), а також яким чином визначаються підцілі для подальшого розвитку атаки та можливі варіанти надійно прихованого укріплення в системі. Саме тому, далі в статті було проведено аналіз основних методів та етапів проведення кібератак на КІС організацій.

Аналіз сучасних методів кібератак на КІС та тестування на проникнення

Беручи до уваги [1] та [2] в 2016-2017 роках, найбільш розповсюдженими видами кібератак були атаки з використанням комп'ютерних вірусів, а другими за популярністю стали спроби компрометації даних, тобто спроби дізнатися (витягнути, вивідати) конфіденційну інформації за допомогою розсилки фішингових листів.

Техніка та основні цілі кібератак

Графічний огляд сучасних методів атак на корпоративні інформаційні системи компаній представлено на рисунку 1.

Отже, розпочнемо з найбільш розповсюдженого виду кібератаки, а саме атаки з використанням шкідливого програмного забезпечення.

Сам термін «шкідливе програмне забезпечення» (ШПЗ) використовується для опису програмного забезпечення, яке встановлюється в системі користувача (наприклад, на комп'ютері або мобільному пристрої) без його згоди та може спровокувати ряд небажаних або навіть неприємних наслідків як, наприклад, помітне зниження продуктивності комп'ютера, крадіжка (компрометація) персональних даних користувача, видалення даних з системи, отримання повного контролю над зараженою системою та навіть вплив на роботу апаратних засобів комп'ютера та інше. Комп'ютерні віруси, інтернет-хробаки, трояни, руткіти – це лише декілька прикладів подібного програмного забезпечення яке використовують зловмисники і здебільшого всі вони в сукупності називаються шкідливим програмним забезпеченням.

Також необхідно відмітити, що раніше зловмисникам необхідно було володіти чималим досвідом та великими знаннями аби дослідити цільову систему, виявити вразливості та на основі цього створити ШПЗ, впровадити його і отримати бажаний результат. На сьогоднішній же день ситуація в кіберзлочинній сфері змінилася, відбувся розподіл труда і з'явилося таке поняття як «Ransomware as a service» (Вимагачі-Як-Послуга), коли автори ШПЗ не є організаторами кібератак, а лише заробляють на його продажі. Тепер будь-хто без спеціальних знань та навиків може, зайшовши в даркнет і скориставшись послугами посередників, придбати все необхідне, як от наприклад exploit kit, готовий до використання ботнет, утиліти для модифікації malware, модулі шифрування, панель управління та інше, при цьому вартість інструментів починається від декількох сотень доларів за прості утиліти і досягає мільйона за експлойти «нульового дня». Це ще одна причина до загострення уваги на забезпеченні інформаційної безпеки КІС та необхідності в

проведенні повноцінного тестування на проникнення для кращого розуміння ваших проблем, виявлення уразливих місць та як найшвидшого їх закриття.

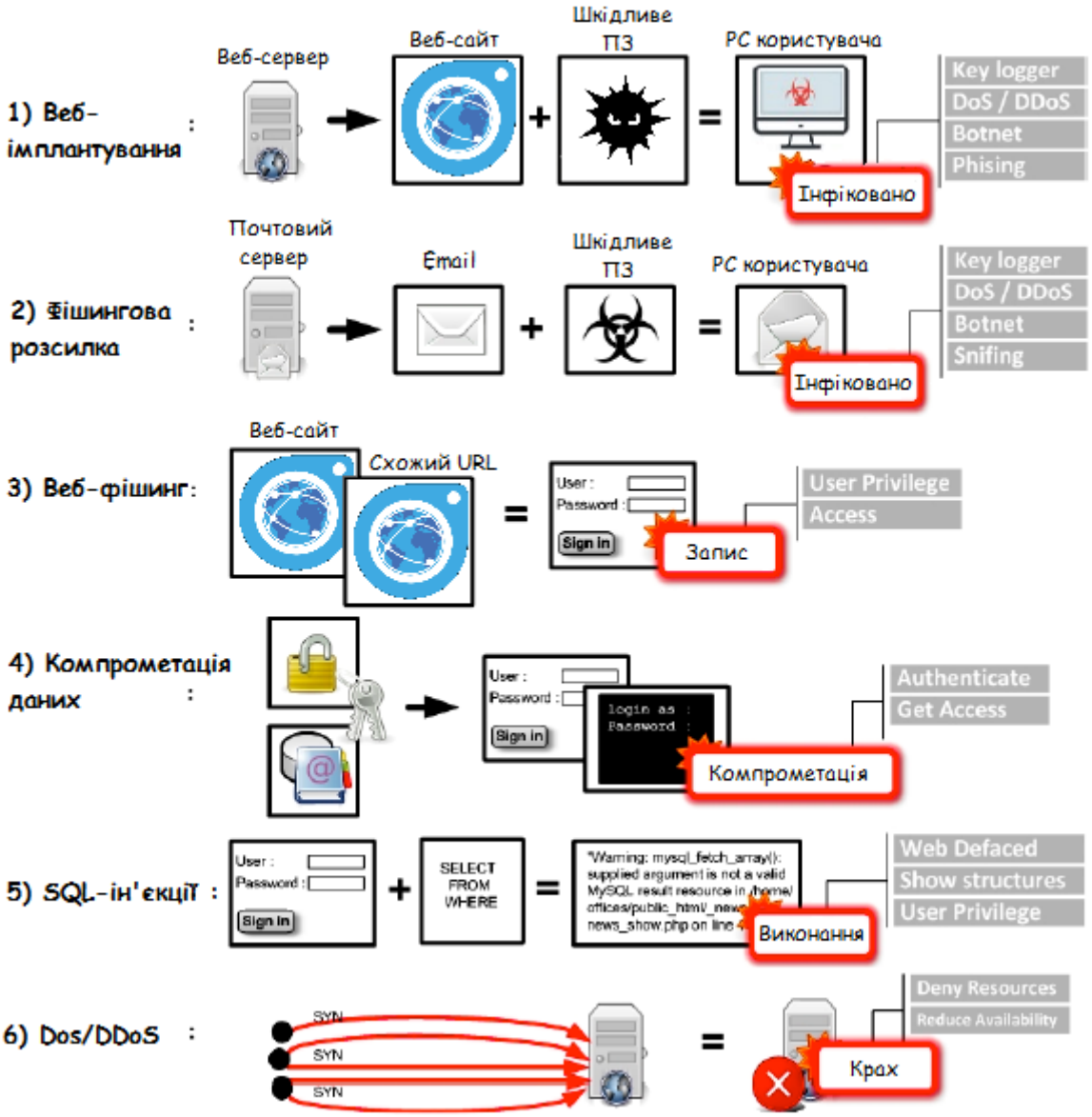

Рис. 1. Основні види кібернетичних атак

Щодо цілей використання ШПЗ переслідуваних зловмисниками, то вони досить різні. Згадати лише початок 2017 року – сплеск популярності троянів-вимагачів та деструктивних масових атак з їх використанням, коли головна ціль зловмисників якомога більший масштаб зараження та нанесення збитків. Так, окрім всім відомих епідемій Wannacry та NotPetya було чимало інших шкідливих кампаній націлених на вимагання коштів у жертв (наприклад Jaff або SOREBRECT), однак не завжди алгоритм роботи шкідливого ПЗ передбачав можливість розшифрування даних, а скоріше за все приховування справжніх мотивів кіберприступних дій та знищення слідів кіберзлочину, що унеможливлювало розслідування кіберінциденту.

При цьому, поширення шкідливого ПЗ відбувається не лише шляхом класичної фішингової розсилки листів персоналу компанії, які містять шкідливі вкладення, але і з використанням уже скомпрометованих веб-сайтів, за рахунок веб-імплантування (мітка 1) різноманітних вірусів, троянів та інших форм шкідливого ПЗ з метою зараження користувачів, які відвідали скомпрометований веб-ресурс – «watering hole» [3]. В ході даної атаки зловмисник спостерігає або припускає які саме веб-сайти відвідують його жертви та заражає один або декілька з них шкідливим ПЗ, при цьому може використовуватися

шкідлива реклама, тайпсквотинг та соціальна інженерія. Також деякі хакери спеціально застосовують різні методи захоплення (наприклад атака SEO Poisoning), за допомогою яких вони змушують користувачів ніби випадково натискати на веб-посилання та переходити на сторінки з розміщеним там malwares. Зрештою, частина цільової аудиторії інфікується і зловмисники можуть виконувати ті чи інші дії в залежності від своїх цілей атаки.

Другим найпоширенішим видом кібератак, як вже згадувалося раніше, є атаки з використанням соціальної інженерії, методи якої на сьогоднішній день продовжують удосконалюватися. Так, в 2017 році зловмисники найчастіше використовували фішингові розсилки (мітка 2) та фішингові сайти (мітка 3) для своїх атак на організації.

Мітка (2) являє собою електронні листи з вкладенням зараженого файлу, при цьому щоб листи виглядали правдоподібно, зловмисники підробляють адреси відправників, реєструють домени, схожі на довірені, і навіть активно атакують постачальників і контрагентів компаній, для того щоб використовувати їх інфраструктуру та облікові записи реальних співробітників з метою відправлення листів від їх імен в обхід спам-фільтрів. У цьому випадку більшість користувачів активно натискають і виконують прикріплений файл, який потім призводить до встановлення ШПЗ на цільову систему. З цього моменту зловмисники можуть використовувати троянець як бекдор, через який отримують доступ до комп'ютера на тих же рівнях привілеїв, що і користувач, який його встановив.

Мітка (3) являє собою сценарій веб-фішингу, в якому атакуючий створює сайт, як дві краплі води схожий на офіційний веб-ресурс [4], наприклад, банку, поштового сервісу або соціальної мережі майже з однаковим URL-адресом, лише з тією різницею, що підроблений сайт підготовлений до атаки на відвідувача. Це робиться для того, щоб змусити користувачів вводити дійсні дані облікового запису на веб-сайт, який, на їхню думку, є справжнім.

Мітка (4) – компрометація даних. Цей тип атаки, як правило, здійснюється шляхом спроби підбору паролів і у випадку погано налаштованої парольної політики в компанії, зловмисник з легкістю отримує облікові дані, які в подальшому використовуються для того, щоб потрапити в КІС організації. Окрім того, часто паролі зберігаються в базах даних у незашифрованому вигляді, і в разі витоку такої бази зловмисникам навіть не доводиться витрачати час на підбір паролів по хеш-функціям. Також необхідно відзначити, що компрометація облікових даних від IoT-пристроїв (англ. Internet of Things, IoT) привела до того, що мільйони роутерів, IP-камер та чимало іншого обладнання підключеного до мережі Інтернет, виявилися в ботнетах і використовуються, наприклад, для стеження за людьми і DDoS-атак.

Наступним видом атаки, не менш небезпечним за попередні, є експлуатація веб-вразливостей, яка використовується в двох основних сценаріях – при атаці безпосередньо на сайт та подальшого його використання (наприклад для хостингу ШПЗ і атак на користувачів); для проникнення в корпоративну мережу компанії через її веб-ресурси. При цьому, кожний четвертий веб-ресурс є уразливим до «Впровадження операторів SQL» (так званих SQL- ін'єкцій – мітка 5). Експлуатація цієї уразливості дозволяє зловмисникові отримати інформацію про користувачів, дізнатися яка версія бази даних працює на цільовій машині та виявити її структуру.

І останнім видом атаки, що розглядається в даній статті є DOS/DDOS-атака (мітка 6), яка передбачає надсилання багатьох запитів на сервер за короткий проміжок часу, тим самим збільшивши завантаження сервера і зменшивши пропускну спосібність мережі, що призводить до унеможливлення використання ресурсів або послуг уповноваженими користувачами.

Основні етапи проведення кібератак та анатомія випробувань на проникнення

Як уже згадувалося раніше, щоб зламати систему будь-якої компанії незалежно від її масштабів і сфери діяльності, хакери використовують цілі стратегії нападу, які складаються здебільшого з п'яти кроків і майже повністю переплітаються з основними етапами

проведення тестування на проникнення [5, 6], при цьому використовуючи щойно згадані види атак:

1) Розвідка. Все починається з того, що зловмисник вибирає компанію-жертву та збирає про неї якомога більше інформації, це і якісь базові відомості, і IP-адреси, і мережива топологія, і дані щодо постачальників ІБ-рішень та навіть особиста інформація про користувача. Знайдені відомості необхідні для розробка сценарію атаки на цільову організацію та підбору інструментів злому.

2) Сканування. Даний етап передбачає сканування і зондування цільової мережі, що дозволяє виявити відкриті порти, уразливості в програмному забезпеченні, помилки в налаштуванні обладнання та інші «діри» в периметрі захисту КІС. Цей етап може розтягнутися на місяці, адже пошук вразливостей повинен бути достатньо «тихим» та акуратним і саме головне, не спровокувати службу безпеки на посилення засобів захисту.

3) Встановлення контролю. Можна сказати, що це найкоротший етап реалізації кібернападу, під час якого зловмисник отримує доступ до цільової системи, а за допомогою таких інструментів як, «Райдужна таблиця» (rainbow table), здобуває права адміністратора, після чого може увійти в будь-яку інформаційну систему з підвищеними привілеями, тим самим отримавши повний контроль над мережею.

4) Організація доступу та управління системою. Після того як знайдено вразливість та реалізований злом КІС, необхідно гарантувати підтримку доступу протягом певного часу (зазвичай, здійснюється за рахунок створення бекдору), без необхідності починати все з нуля. На даному етапі зловмисник може відправляти команди, надсилати нові модулі для розвитку атаки та багато іншого, і взагалі, подальші дії обмежуються виключно фантазією та цілями зловмисника, а невидима «присутність» в системі може тривати місяцями.

5) Знищення або заплутування слідів кібернетичного нападу. Після повної реалізації атаки та досягнення поставленої мети здається розумним видалити або хоча б приховати всю інформацію щодо своєї присутність, однак на практиці не завжди відбувається саме так. Достатньо часто хакери залишають ознаки злому як автограф на своєму злочині, хоча є і більш практична мета – заплутати сліди. Існує безліч способів пустити експертів з розслідування кіберінцидентів по хибному шляху: очищення і підміна записів в журналі, створення зомбі-акаунтів, використання троянських команд та чимало іншого.

Єдиною різницею між етапами проведення тестування на проникнення і здійснення реальної кібератаки, залишаються наступні три етапи.

Перший передує етапу розвідки – це безпосередньо планування тесту на проникнення, під час якого визначаються цілі проведення пентесту, терміни, вартість робіт, які будуть проводитися, методи, які будуть застосовані і форма звіту.

Та два інших, які проводяться після знищення слідів кібератак – це створення звіту та видалення артефактів (очищення системи від наслідків проведення пентесту).

При цьому, звіт повинен містити [6]:

- методику проведення тесту;
- висновки для керівництва, що містять загальну оцінку рівня захищеності;
- опис виявлених недоліків системи управління ІБ (СУІБ);
- опис ходу тестування з інформацією по всіх виявлених вразливостях і результатами їх експлуатації;
- рекомендації щодо усунення виявлених вразливостей.

Висновки

Використання тесту на проникнення є дійсно корисним для виявлення та усунення критичних уразливостей в корпоративних інформаційних системах, показуючи наскільки насправді вони є вразливими до тих чи інших кібернетичних атак.

Детально розглянуті та роз’яснені в даному дослідженні етапи проникнення та сучасні методи проведення атак можуть бути використані при наданні рекомендацій співробітникам служби безпеки, які захищають свої мережі від будь-яких потенційних кібератак. При цьому,

важливо, щоб оператори безпеки могли зрозуміти яким саме чином кіберпорушники проникають в їхні корпоративні інформаційні системи.

Також результати даного дослідження можуть бути використані при розробці методики забезпечення об'єктивного контролю захищеності корпоративних інформаційних систем шляхом проникнення.

Список використаних джерел:

1. Global Fraud & Risk Report: Forging New Paths in Times of Uncertainty. // Kroll. – 2017. – №10. – С. 4.
2. Positive Research 2017: Сборник исследований по практической безопасности. // Positive Technologies. – 2017. – С. 3.
3. Watering hole attack [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Watering_hole_attack
4. Фишинг. Советы по безопасности [Електронний ресурс] – Режим доступу до ресурсу: https://antifraud.drweb.ru/phishing/.
5. Амиров Н. Г. Сравнительный анализ методик тестов на проникновение [Електронний ресурс] / Н. Г. Амиров, А. В. Кручинин. – 2016. – Режим доступу до ресурсу: http://ir.nmu.org.ua/bitstream/handle/123456789/149266/12-13.pdf?sequence=1&isAllowed=y.
6. Киричок Р.В. Проблеми забезпечення контролю захищеності корпоративних мереж та шляхи їх вирішення. / Р.В. Киричок, П.М. Складанний, В.Л. Бурячок, Г.М. Гулак, В.А. Козачок / Наукові записки Українського науково-дослідного інституту зв'язку. - 2016. - №3(43). С. 51 -58.

Надійшла: 25.04.2018 Рецензент: к.т.н. Курченко О.А.