ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія проведення тестування на проникнення в корпоративній мережі»

на здобуття освітнього ступеня магістра
зі спеціальності ____125 Кібербезпека_____
(код, найменування спеціальності)
освітньо-професійної програми _Інформаційна та кібернетична безпека_
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Валентин КИЗИМ

Виконав: здобувач вищої освіти групи БСДМ-61
КИЗИМ Валентин
(ПРІЗВИЩЕ, Ім'я)

Керівник: МАРЧЕНКО Віталій
д.ф., доцент (ПРІЗВИЩЕ, Ім'я)

Рецензент: РАБЧУН Дмитро
к.т.н., доцент (ПРІЗВИЩЕ, Ім'я)

Київ 2024

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

OSINT – розвідка по відкритим джерелам (Open Source Intelligence)

OWASP – Open Web Application Security Project

NIST – National Institute of Standards and Technology

OSSTMM – Open Source Security Testing Methodology Manual

QA – Quality Analyze

НСД – Несанкціонований Доступ

AD – Active Directory

т. зв. – так званий

ASN – Autonomous System Number

IANA – Internet Assigned Numbers Authority

ВСТУП

Актуальність дослідження. Своєчасне проведення тестування на проникнення - це важлива складова інформаційної безпеки в сучасних організаціях. Її актуальність обумовлення у зв’язку з збільшенням загроз кібербезпеки організацій. Зловмисники постійно шукають способи вторгнутися в мережі організацій з метою крадіжки даних, розповсюдження шкідливого програмного забезпечення та інших кібератак. Тестування на проникнення допомагає вчасно виявити вразливості і завчасно захистити мережу та її ресурси від таких загроз.

Зараз багато працівників працюють віддалено або використовують мобільні пристрої для доступу до корпоративних ресурсів. Однією із задач тестування на проникнення може бути перевірка безпечності та правильного налаштування віддаленого доступу.

Багато галузей, такі як фінанси, охорона здоров'я та інші, мають обов'язкові вимоги щодо захисту конфіденційності даних інших ресурсів. Одним із важливих та обов’язкових етапів сертифікації на відповідність стандартам обробки конфіденційних даних є тестування на проникнення

Не тільки зовнішні зловмисники можуть становити загрозу. Інсайдери, тобто внутрішні працівники організації, також можуть бути джерелом загрози для інформаційної безпеки. Тестування на проникнення може проводитись в тому числі і з симуляцією дій зловмисника або інсайдера, що має доступ до внутрішньої корпоративної мережі.

Таким чином, тестування на проникнення сприяє покращенню механізмів захисту корпоративної мережі. Впровадження регулярного тестування дозволяє організаціям тримати в актуальному стані механізми захисту своєї мережі та ресурсів. Тому тема кваліфікаційної роботи є актуальною.

Об’єкт дослідження – процес тестування на проникнення інформаційних ресурсів організації або підприємства.

Предмет дослідження – технології тестування на проникнення за методологіями OSSTMM, OWASP, NIST SP 800-115.

Мета роботи – розробити варіанти технології тестування на проникнення для корпоративної мережі організації та рекомендації щодо застосування технології.

Наукові завдання:

- провести аналіз питання щодо необхідності проведення тестувань на проникнення в корпоративній мережі;
- проаналізувати основні загрози інформаційній системі організації;
- проаналізувати методи та засоби проведення тестування на проникнення в рамках різноманітних сценаріїв;
- розробити варіант технології проведення тестування на проникнення та рекомендації щодо використання запропонованої технології.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу тестування на проникнення на базі професійної діяльності та тестових віртуальних середовищ.

Практичне значення одержаних результатів полягає в розробці технології проведення тестування на проникнення та рекомендації щодо використання запропонованої технології в залежності від масштабів тестування та обраного сценарію проведення.

Апробація результатів. Результати даного дослідження доповідались на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки».

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ПРОВЕДЕННЯ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ В КОРПОРАТИВНІЙ МЕРЕЖІ

1.1. Призначення, методологія, функції та умови проведення тестування на проникнення

Тестування на проникнення – це процес систематичного виявлення і аналізу вразливостей і «слабких» місць в інформаційних системах, додатках, мережі чи програмному забезпеченні. Також тестування на проникнення може включати в себе і роботу з персоналом методами соціальної інженерії та тестування функціоналу ПЗ методами реверс-інжинірингу.

Основною метою тестування на проникнення є всеохоплююча оцінка механізмів захисту та забезпечення безпеки, веб-додатків, сервісів та їх конфігурацій, персоналу та інших факторів, що можуть мати або мають вплив на стан безпеки підприємства чи організації.

Виконуючи тестування на проникнення аудитор може керуватись безліччю відомих методологій, кожна з яких має свої переваги та недоліки, призначення та спеціалізацію на певних технологіях або ж більш загальне призначення в рамках проведення проекту по тестуванню. Найпоширенішими та найвідомішими з них вважають:

1. OSSTMM (Open Source Security Testing Methodology Manual): Орієнтована на розробку безпечних систем і включає перевірку фізичної, технічної та процесуальної безпеки.
2. OWASP (Open Web Application Security Project): Спрямована на безпеку веб-застосунків і включає аналіз вразливостей, пов'язаних із веб-застосунками.
3. NIST SP 800-115: Визначає стандарти для тестування на проникнення в федеральних інформаційних системах.

Докладніше кожну з цих методологій, як і стандарти в області тестування на проникнення буде розглянуто в подальшому.

Основними функціями тестування є виявлення вразливостей, себто слабких місць в системах, що можуть бути використані атакуючими в подальшому. Оцінка реакції систем та служб захисту на загрози, зокрема на спроби отримання НСД та експлуатації вразливостей. Та перевірка валідності і ефективності наявних заходів та засобів безпеки в умовах, приближених до реальних.

Умовами успішного проведення тестування на проникнення є професійність та якісна підготовка аудитора, завчасне вирішення юридичних та технічних аспектів організації проведення тестування, зокрема надання юридичного дозволу на проведення робіт, підготовку робочого місця або доступу для аудитора та внесення необхідних виключень і конфігурацій в механізми захисту та завчасне попередження служб безпеки і надавачів послуг про заплановане проведення робіт. Не менш важливою умовою виконання тестування на проникнення є створення повноцінного звіту за результатами проведених робіт із зазначенням всіх виявлених в ході тестування проблем та вразливостей.

1.2. Аналіз проблеми відсутності регулярного проведення аудиту та тестування на проникнення в корпоративній мережі

В сучасному цифровому світі, де кіберзагрози стають все більш витонченими та агресивними, відсутність регулярного аудиту та тестування на проникнення може стати великою проблемою для безпеки корпоративної мережі.

Зокрема Google's Threat Analysis Group зазначає, що в тільки за період з Січня по Вересень 2023 року було розкрито 69 вразливості нульового дня, з яких 44 було помічено в експлуатації в інформаційному середовищі [1]. На додачу до цього CVE Details зазначає, що в 2023 було виявлено та описано більш ніж 26 тисяч вразливостей

[2]. В той же час багато старих вразливостей, для яких вже існують виправлення та патчі, зустрічаються в корпоративних системах.

Своєчасно проведений аудит або тестування на проникнення могло би виявити ці вразливості та допомогти завчасно виправити їх або нейтралізувати ризики, пов’язані з експлуатацією цих вразливостей.

В той же час відсутність регулярних тестувань збільшує ризики для безпеки підприємства в зв’язку з можливими невиявленими вчасно вразливостями.

1.3. Мета та завдання проведення тестування на проникнення в корпоративній мережі в рамках та поза рамками аудиту корпоративної мережі

Тестування на проникнення може проводитись як в рамках масштабнішого проекту, такого як аудит підприємства на відповідність вимогам або рекомендаціям стандартів інформаційної безпеки (PCI DSS, NIST, ISO IEC, тощо), так і самостійно в рамках оцінки загального рівня захищеності інформаційних ресурсів підприємства. Обидва варіанта мають певні особливості виконання, завдання та мету щодо фінального результату. Розглянемо їх.

Тестування на проникнення в рамках загальної оцінки, в цілому, має за мету всеохоплюючий аналіз механізмів захисту та загальної захищеності інформаційних ресурсів підприємства. Так само як і покращення стану захищеності підприємства в цілому Основним завданням аудитора в такому випадку є загальна оцінка максимальної кількості наявних ресурсів та надання рекомендацій щодо покращення механізмів захисту та виправлення вразливостей в цілому. Таке тестування може розповсюджуватись не тільки на стаціонарні пристрої, але й на засоби віддаленого доступу, мобільні пристрої, веб-додатки та персонал в цілому.

В той же час тестування на проникнення в рамках аудиту на відповідність стандартам відрізняється більшою спеціалізацією виконуваних дій і має за мету перевірити відповідність систем захисту та загального стану інформаційних ресурсів

підприємства до вимог стандарту або стандартів. Таке тестування характеризується фокусуванням виконуваних дій на ресурсах, що згадуються в необхідному стандарті, наприклад, у випадку аудиту для сертифікації PCI DSS тестування буде стосуватись систем, що безпосередньо приймають участь або дотичні до обробки карткових платіжних даних. Результатом такого тестування буде звіт, основна увага в якому буде приділена саме проблемам, наявність яких заважає або не дає визнати захищеність інформаційних систем таким, яке відповідає вимогам стандарту. Варто зазначити, що наявність такого фокусу не означає обов'язкове ігнорування інших проблем, проте дещо зміщує пріоритет з них в сторону основних проблем та вразливостей.

1.4. Аналіз існуючих методологій та стандартів в області тестування на проникнення

Існує багато різних загальноприйнятих методологій тестування на проникнення. Деякі з них охоплюють тестування в загальному сенсі, описуючи процес та необхідні дії для успішного тестування систем захисту в цілому. Інші більше фокусуються на проведенні тестування певного виду систем (веб-додатки, мобільні додатки, тощо). Розглянемо та проаналізуємо найвідоміші з них.

OSSTMM – методологія розроблена і підтримується Institute for Security and Open Methodologies (ISECOM). Вона розміщена у відкритому доступі і розповсюджується авторами на безоплатній основі. Інститут заявляє, що організація вільна від будь-якого стороннього впливу і отримує необхідне фінансування, дані та підтримку через партнерство та власні дослідження. Ознайомитись з методологією можна на офіційному ресурсі інституту [3].

Методологія фокусується на оцінці фізичної, технічної та процесуальної безпеки організації. Сюди входить також аналіз технічних систем, контролю доступу та процедур і політик безпеки. Для кожного з вищезазначених пунктів методологія містить чіткі принципи та метрики для оцінки.

Методологія орієнтована на оцінку ризиків та загроз для підприємства. Вона визначає різні рівні ризиків та різноманітні загрози та дозволяє ідентифікувати конкретні наслідки та потенційний вплив їх реалізації на системи організації або підприємства.

OSSTMM встановлює стандартизовані процедури для тестування, що допомагає забезпечити стандартизованість та порівнянність результатів. Це важливо для того, щоб результати робіт різних команди та проектів можливо було оцінити на одній основі та дозволяє відносно безболісно обирати різних виконавців під час терміну життя організації.

Також однією з основних особливостей методології є реалістичний підхід до опису виконання атак. Це дозволяє враховувати реальні загрози та можливості зловмисників при створені та моделюванні сценарії атаки або виконанні тестувань.

Метрика безпеки у методології OSSTMM визначається як система вимірювань та оцінок, спрямованих на визначення ефективності заходів безпеки та ідентифікацію слабких місць в інформаційній системі або мережі. Основна ідея полягає в тому, щоб мати конкретні критерії та стандарти, за якими можна об'єктивно виміряти та порівнювати рівень безпеки в різних сценаріях тестування.

Недоліками розглянутої методології є, як не дивно, її універсальність та певна застарілість. Через загальність охоплених напрямків використання методології вона може не підходити для специфічних сценаріїв тестування чи для організацій із нестандартними вимогами до проведення робіт. Щодо застарілості, остання версія методології була випущена в 2010 році та може не враховувати реалії інформаційного середовища, що стали актуальними протягом останніх тринадцяти років.

OWASP — це некомерційна організація, яка зосереджується на покращенні безпеки веб-застосунків. OWASP розробила ряд проектів, включаючи свою методологію тестування безпеки веб-застосунків, яка називається OWASP Testing Guide. Методологія, як і будь які інші матеріали організації розповсюджується на відкритій основі і доступна на офіційних ресурсах організації [4]. Методологія

призначена для тестування веб-додатків і може бути використана не тільки в процесі тестування на проникнення, але й розробниками та QA-спеціалістами в рамках циклу розробки та деплою веб-додатку. Розглянемо основні особливості методології.

Методологія OWASP Testing Guide орієнтована на комплексний огляд та аналіз безпеки веб-застосунків та охоплює різні аспекти функціоналу таких застосунків, таких як автентифікація, авторизація, захист даних користувачів, обробка даних на стороні клієнту та серверу, взаємодія з іншими сервісами, тощо.

Методологія фокусується на використання прости та загальнодоступних інструментів для проведення тестувань. Це забезпечує зручність використання методології не тільки для спеціалістів в області тестувань на проникнення, але й розробникам додатків та внутрішнім командам контролю якості.

Основним фокусом методології є саме виявлення та вчасна нейтралізація загроз для веб-додатків. А отже методологія розглядає сценарії, пов’язані з атаками на додатки і відповідні наслідки і ризики пов’язані з їх успішною реалізацією. В тому числі із імітацією реальних сценаріїв та можливих дій зловмисника.

За рахунок залучення до створення та поповнення бази знань організації не тільки співробітників, а й волонтерів та активістів з усього світу, методологія активно підтримується в актуальному стані та регулярно поповнюється новими знахідками та актуальними вразливостями. Що дозволяє підтримувати її в відносно актуальному до сучасних викликів стані.

З недоліків методології варто зазначити її фокус на веб-додатках, що не дозволяє використовувати її для виконання проектів ширшого профілю та потребує вивчена інших методологій спеціалістам, що хочуть мати можливість виконувати проекти, не пов’язані з веб-додатками.

Деякі аспекти методології потребують високого рівня розуміння функціоналу веб-додатків з точки зору безпеки для ефективного виконання рекомендацій методології.

National Institute of Standards and Technology (NIST) - це американське федеральне агентство, яке входить до складу Міністерства торгівлі США. NIST виконує ключову роль у встановленні та сприянні використанню стандартів для підтримки інновацій, конкурентоспроможності та науки у Сполучених Штатах. Організація є федеральною установою США та спонсорується урядом Сполучених Штатів, через що її діяльність може бути ангажованою та сповільненою через юридичні та бюрократичні затримки. Основною методологією щодо тестування на проникнення від організації прийнято вважати стандарт NIST Special Publication 800-115 (NIST SP 800-115). Зі стандартом можна ознайомитись на офіційному ресурсі [5]. Розглянемо його основні особливості та недоліки.

Методологія спрямована на загальне тестування систем, ідентифікацію, вивчення та виявлення вразливостей в інформаційних системах, що можуть бути використані для НСД чи атак.

Методологія рекомендує інтегрувати тестування на проникнення одразу в процес розробки інформаційних систем для забезпечення безпеки вже на етапі створення таких систем, що дозволить уникнути більшості проблем, пов’язаних з введенням в експлуатацію ще не протестованих систем.

Методологія чітко розділяє та вказує етапи тестування, докладно описуючи кожен з них. Починаючи від етапу підготовки і закінчуючи документуванням та звітуванням щодо результатів тестування.

Методологія підкреслює важливість оцінки ризиків та вибору адекватно пропорційних стратегій тестувань для мінімізації потенційної шкоди, викликаної вибором занадто агресивних способів та засобів для тестування.

Методологія окремо виділяє етичну сторону тестувань. Зокрема отримання дозволу від власників систем на проведення робіт з тестування та узгодження проведених робіт, використаних засобів та інструментарії.

До недоліків вказаної методології можна віднести її залежність від урядової організації, що сповільнює розвиток самої методології та ставить її в залежність від

схвалення урядом. Через це, зокрема, методологія досить значний час не оновлювалась (з 2008 року) та може мати дещо меншу актуальність відносно сучасних загроз.

Методологія була створена з оглядом на реалії та юридичні аспекти, актуальні для Сполучених Штатів і може бути неактуальною або недоречною в використанні на підприємствах в інших частинах світу.

Методологія сфокусована більше на зовнішні загрози і може недостатньо враховувати ризики, пов’язані з внутрішніми загрозами та загрозами викликаними соціальною інженерією.

Розглянуті вище методології та стандарти є лише малою частиною офіційно визнаних світовою спільнотою нормативних документів. Значна частина організацій та підприємств, що працюють в сфері інформаційної безпеки в цілому та в сфері тестування на проникнення загалом можуть мати та використовувати власні методології, що базуються на основі вже вказаних або не згаданих вище методологій.

Висновки до Розділу 1

Проблематика тестування на проникнення є досить актуальною темою на сьогоднішній день у зв’язку з постійним розширенням кількості, масштабу та потенційними ризиками, викликаними діяльністю в кіберпросторі зловмисників і інших комерційних, державних або зловмисних організацій. Правильна організація процесу тестування на проникнення потребує плідної співпраці замовника та виконавця тестування на проникнення задля отримання максимального результату та ефективного виправлення виявлених проблем. Виконавцям доступно багато різноманітних методологій для проведення робіт, кожна з яких має як свої переваги і особливості, так і недоліки та спеціалізації. Виконання тестування на проникнення потребує від спеціалістів постійного навчання та покращення своїх навичок. Також важливо постійно слідкувати за змінами та новими тенденціями в сфері інформаційної

безпеки задля актуалізації власних навичок і готовності до виявлення та обробки нових загроз в інформаційному та кіберпросторі.

2 АНАЛІЗ ЕТАПІВ ТА МЕТОДІВ ПРОВЕДЕННЯ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

2.1. Підготовчий етап перед проведенням тестування на проникнення, юридичні та практичні тонкощі попереднього етапу

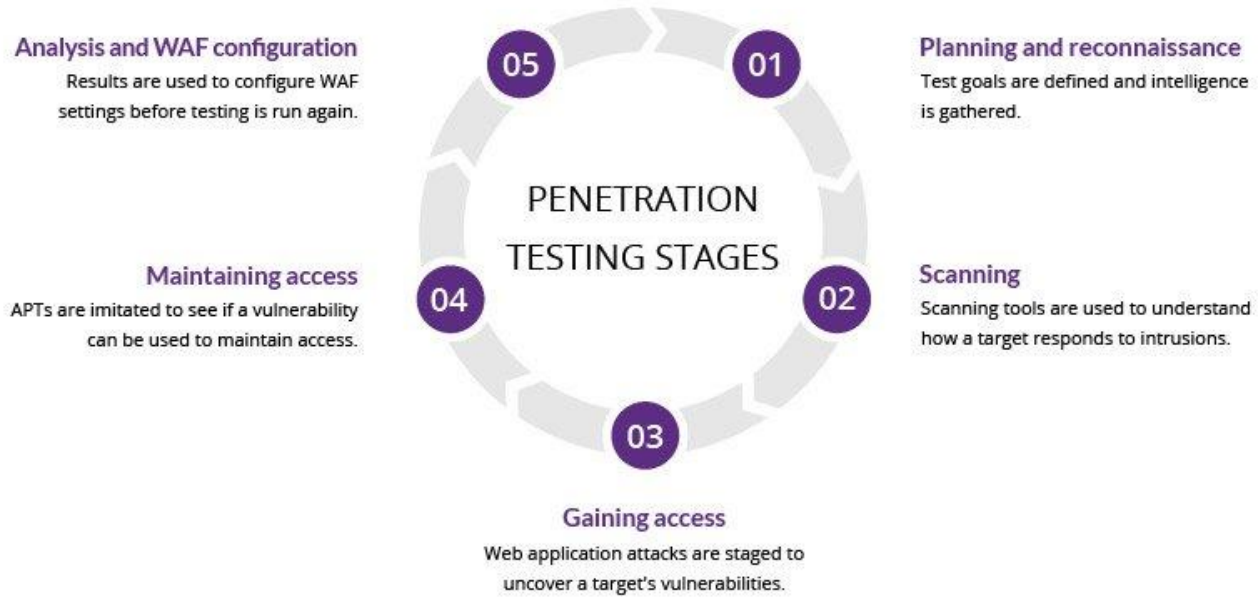


Рис. 2.1. Етапи тестування на проникнення [8]

Процес тестування на проникнення починається задовго до того, як аудитор отримує можливість безпосередньо взаємодіяти з інформаційними системами замовника. Серйозну основу для успішного та вчасного виконання майбутнього тестування закладає саме підготовчий етап.

До підготовчого етапу можна відносити планування, узгодження, підготовку, документальне та юридичне супроводження а також налаштування робочого місця аудитору безпосередньо перед початком взаємодії із визначеними системами замовника. Деякі спеціалісти також відносять до цього етапу і проведення пасивної

розвідки методом збору інформації в відкритих джерелах. Розглянемо ці етапи докладніше.

Підготовчий етап починається з визначення основних аспектів тестування. Який вид робіт буде проводитись, який доступ буде мати виконавець, яка мета проведення тестування, які будуть обмеження по терміну, часу виконання робіт, видам виконуваних робіт, інструментарію, тощо. Зазвичай в професійному середовищі узгодженням цих деталей займається спеціально навчена людина в команді, що має великий досвід в спілкуванні з замовником. Або, простими словами, менеджер проекту.

Наступним пунктом йде визначення рівня обізнаності виконавця щодо систем, які тестуються. З метою симуляції різних сценаріїв та в залежності від цілей тестування аудитору можуть надавати різний об’єм ввідної інформації. Зазвичай класифікація рівня попередніх знань розділяється так: white box, gray box та black box.

White box – означає вид робіт, коли виконавцю надається максимально повний об’єм знань про системи, в яких буде проводитись тестування. Сюди входить надання доступу до документації, API, схеми мережі, код програм та додатків. Зазвичай роботи такого типу проводяться для знаходження максимальної кількості вбудованих вразливостей, що не було виявлено під час процесу розробки або ж імплементації/інтеграції системи чи технології. Зазвичай список цілей для таких робіт обмежується одною або декількома системами.

Grey box – означає вид робіт, коли виконавець отримує обмежену кількість інформації щодо систем. Виконання такого типу робіт націлене на оцінювання механізмів безпеки систем з точки зору осіб, що мають певну обізнаність щодо функціонування інформаційних систем замовника, проте не мають повного доступу до внутрішнього функціоналу або для проведення аудиту систем і ресурсів на відповідність до вимог міжнародних стандартів. Список цілей в таких роботах може обмежуватись від декількох додатків, ресурсів до цілих ланок мереж чи інфраструктури.

Black box – означає вид робіт, коли виконавцю не надається ніякої інформації щодо систем, що тестуються. Роботи такого типу характеризуються максимальною наближеністю до реальних сценаріїв. Список цілей може бути необмежним в рамках ресурсів, що належать замовнику, або ж доповнюватись по ходу проведення тестування на проникнення з метою запобігання завдання зайвих випадкових збитків.

В залежності від визначеного типу робіт визначається список цілей тестування. В цьому списку чітко визначається, які цілі виконавець може тестувати в ході виконання робіт. Це дозволяє винести за межи тестування системи, вплив на які в ході робіт може призвести до виводу з ладу критичних процесів підприємства та принести значні фінансові та репутаційні збитки.

Результуючим документом підготовчого етапу можна вважати т.зв. «Лист Згоди» – документ, в якому чітко визначаються замовник, виконавець, вид виконуваних робіт, терміни виконання робіт, список ресурсів, на яких буде проводитись тестування, та інші юридичні аспекти. Правильно складений Лист Згоди дозволяє замовнику чітко обмежити об’єм необхідних робіт згідно поставлених цілей, а виконавцю уберегти себе від можливих юридичних проблем в майбутньому.

Після узгодження всіх юридичних питань наступає етап технічної підготовки до тестування. З точки зору виконавця цей етап включає в себе налаштування на своїй робочій станцій необхідного інструментарію, встановлення програмного забезпечення, що може знадобитись в тестах. В той же час замовник в цьому етапі мусить забезпечити необхідний доступ виконавцю до цільових систем, налаштувати відповідним образом механізми захисту, виключення в них та, в разі необхідності, надати віддалений зовнішній доступ.

В цілому, коротко підготовчий етап можна описати такими пунктами:

1. Визначення з цілями тестування, його метою та який тип робот буде проводитись.

2. Визначення виду робіт. Надання виконавцю необхідного об’єму інформації щодо систем, на яких буде проводитись тестування.

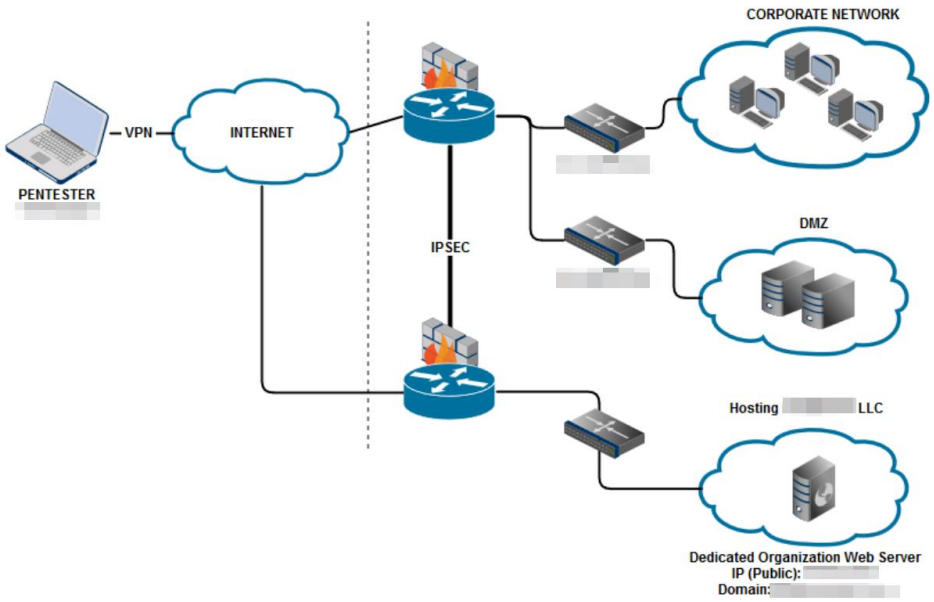


Рис. 2.2 .Приклад схеми мережі, що може бути наданий виконавцю

3. Визначення списку цілей – систем, які будуть безпосередньо задіяні в тестуванні та з якими дозволено працювати виконавцю під час проведення робіт.

4. Формування та надання виконавцю «Листа Згоди» – документа, що підтверджує законність виконуваних робіт і чітко визначає об’єм, обмеження і інші умови щодо виконання тесту на проникнення.

H. Engagement Limitations (“Rules of Engagement”)

During the engagement, the following rules must be adhered to. Any deviations must be determined and approved by Change Management then the Steering Committee.

1. Activities that may potentially or potentially result in a denial of service condition, service interruption, or otherwise general annoyance are prohibited.
2. This engagement is considered “full-scope” with the following network exclusions:
   a. 192.168.0.0/16
   b. 172.16.0.0/16
   c. 10.0.0.0/8
3. Status meetings will occur daily at 10am and 3pm via approved channels.
4. Approved testing window is from 12am-5am: M,W,F,Sa,Su
5. Portscanning is allowed with the following exclusions: TCP 21, 22, 80, 443, 445, 8080, 8443
6. Activities that may result in the locking of accounts are considered unethical and will result in case forwarding to the Ethics line.

Рис. 2.3. Приклад фрагмента Листа Згоди [10]

Окремо варто виділити проведення пасивної розвідки як окремого суб-етапу підготовки до проведення тестування на проникнення. Ця активність вноситься в підготовчий етап деякими професіоналами тому, що вона не зачіпає безпосередньо системи замовників під час свого виконання. Проте вона дозволяє зібрати чималий пласт інформації щодо можливого об’єму робіт та технічні дані, що можуть знадобитись в процесі майбутнього тестування безпосередньо на ресурсах замовника.

Основною метою розвідки по відкритих джерелах є збір максимально можливого об’єму інформації методами пасивного збору інформації. Сюди входять: пошук з використанням пошукових систем, збір технічних даних з автоматичних мережевих агрегаторів інформації, соціальних мереж та інших джерел. Розглянемо деякі основні напрямки такої розвідки.

Пошук по соціальним мережам дозволяє зібрати основний масив загальної інформації про організацію чи підприємство, щодо якого буде проводитись тестування. Зазвичай там можна знайти історію підприємства, його основний напрям діяльності, контактні дані, інформацію про керівництво, та, частіше за все, основних клієнтів. На основі цього можна зробити припущення, які технології використовуються на підприємстві та відповідно підготуватись до майбутнього тестування.

Окрім того, в соціальних мережах також можна дізнатись про персонал. Часто люди нехтують правилами анонімності та безпечного поводження в мережі інтернет і можуть розміщувати цінну для аудитора інформацію в своїх профілях. Також в соцмережах професійної направленості, зокрема таких як, наприклад, LinkedIn, можна зібрати інформацію про сертифікації та посади співробітників. Знову таки, дозволяючи зробити припущення щодо того, який стек технологій може використовуватись в системах в майбутньому тестуванні. Попередній збір інформації про співробітників може бути дуже корисним також у випадку, коли в ході аудиту безпеки підприємства планується проведення тестування персоналу методами соціальної інженерії.

Ще одним способом пасивного збору інформації є використання пасивних сканерів чи метаданих. Такі сервіси проводять регулярне та самостійне сканування мережі Інтернет та можуть надати, зазвичай на комерційній основі, масу інформації щодо зовнішніх ресурсів того чи іншого підприємства. На таких ресурсах можна знайти інформацію про IP-адреси, домени, відкриті порти та сервіси на них (в деяких випадках одразу з потенційними вразливостями або точками входу), домени, субдомени, публічні поштові сервери, тощо.

Хоча проведення розвідки, як окремий етап, зазвичай, виділяється в разі виконання тестування на проникнення типу Black Box, аудитору не варто нехтувати ним і в інших типах тестувань задля підвищення власного рівня обізнаності щодо цільових систем та замовника а також для додаткової перевірки чи в якості додаткового джерела інформації під час проведення зовнішнього тестування на проникнення або тестування методом соціальної інженерії.

2.2. Етап зовнішнього тестування на проникнення, аналіз нюансів та можливих проблем при проведенні

Етап зовнішнього тестування на проникнення є одним із двох найбільш часто виконуваних типів робіт в тестуванні на проникнення. Основною метою зовнішнього тестування є виявлення вразливостей та проблем із захистом на зовнішньому периметрі інформаційних ресурсів організації.

Цей етап включає в себе багато видів активностей та потребує кропіткого дослідження цільових систем і розуміння механізмів роботи систем, в яких проходить тестування. Більшість зовнішніх тестувань на проникнення проходить в такій послідовності:

1. Розвідка активними методами.

2. Дослідження виявлених сервісів та додатків. Тестування типових вразливостей.

3. В разі виявлення таких вразливостей – проведення експлуатації та отримання базового доступу до системи.

4. Закріплення та розширення прав в системі або в додатку.

5. Збір інформації, доступної з розширеними правами або правами адміністратора.

Фактично, даний алгоритм можна виконувати для кожної цільової системи. Розберемо його трохи докладніше.

Активні роботи починаються зі збору інформації про системи, які доступні для тестування. Так як аудитор вже отримав дозвіл на втручання в роботу систем, він може напряму взаємодіяти з цільовими хостами. Існує декілька способів збору інформації. Найбільш базовий і найдоступніший для широкого загалу є використання загальновідомого сканеру nmap, або ж його версії з графічним інтерфейсом zenmap. Його загальнодоступність та універсальність дозволяє зібрати багато необхідної інформації для початку більш активних дій. Проте більш поглиблене дослідження потребує ширшого вивчення документації і розуміння того, як працюють мережеві протоколи. Окремо варто виділити наявність користувацьких скриптів, що дозволяють розширити об’єм отримуваної інформації.

Окремо сюди можна включити також сканування автоматичними засобами, так званими сканерами вразливостей. До них відносяться Nessus Tannable, Rapid7 Nexpose, Portswiger BurpSuite або загальнодоступний для всіх безкоштовний їх аналог OWASP ZAP (важливо зазначити, що останні два розраховані в основному на тестування веб-додатків). Застосувавши автоматичний сканер, аудитор може швидко отримати інформацію по цільовим системам в зручному вигляді та після ознайомлення визначити потенційні точки для входу та подальшої експлуатації. Мінусом застосування таких засобів може бути велика кількість хибних спрацювань, які потребуватимуть додаткової верифікації.

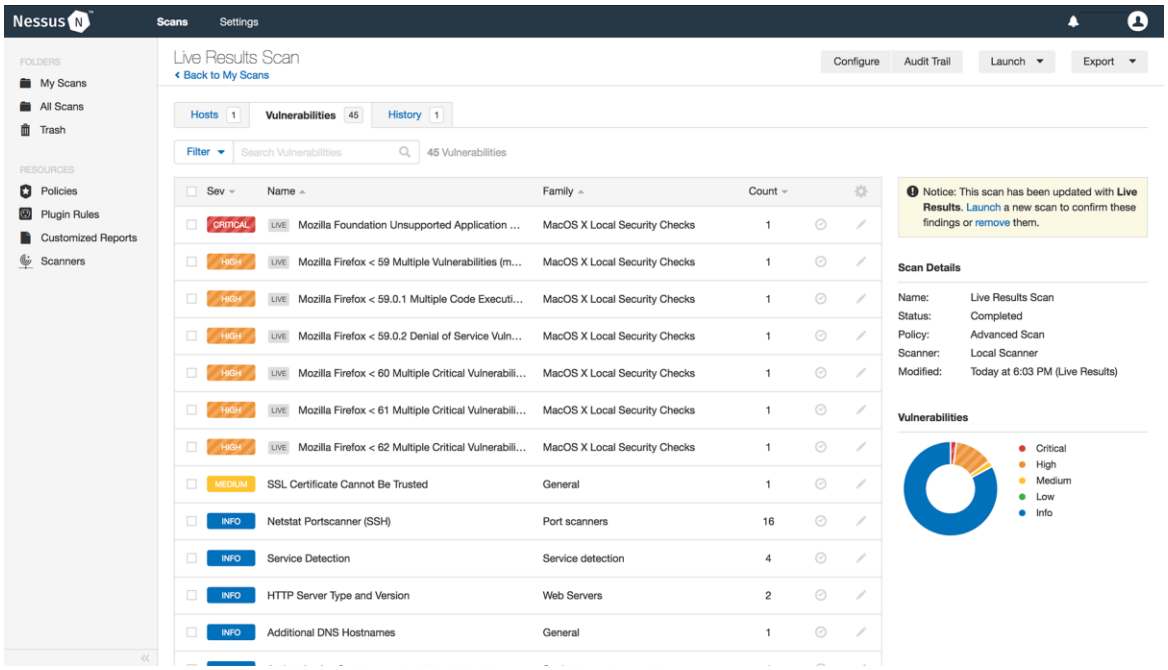


Рис. 2.4. Інтерфейс сканера Nessus з результатами сканування [7]

Отримавши інформацію про активні цілі та сервіси на них, аудитор може починати проникати глибше в системи. Маючи необхідний мінімум в вигляді активних портів, аудитор вже може зробити припущення щодо наявних на них сервісів і пробувати експлуатувати відомі вразливості і техніки. А з отриманням конкретної інформації, такої як точна назва сервісу та/чи його версія, можливо звузити інструментарій до конкретних засобів, підходящих до цього конкретного сервісу. Основною задачею для цього етапу є проникнення за межі сервісу і отримання доступу безпосередньо до самого серверу або ж отримання прав адміністратора на сервісі.

Подальшою ціллю в випадку успішного проникнення на сервер є закріплення та збір інформації. Під закріпленням мається на увазі забезпечення постійного доступу до серверу навіть після можливого перезавантаження та ескалація привілеїв на сервері до максимального рівня доступу. В цьому можуть бути корисні так фреймворки, як metasploit та йому подібні. Також отримання привілеїв адміністратора може бути

корисним для використання захопленої машини в якості ще однієї точки старту на випадок проведення внутрішнього тестування.

Також в файловій системі захопленого серверу може бути багато корисних даних: паролі від інших або технічних облікових записів, хеші доменних паролей, технічна документація, скрипти, бекап файли, залишені співробітниками записи (в тому числі з обліковими даними).

Фактично, ця послідовність повторюється для кожного наступного серверу/сервісу. Тому перейдемо до розгляду можливих нюансів та проблем, що стосуються саме зовнішнього етапу.

Перше, частіше за все зовнішнє тестування на проникнення виконується на «живих» серверах. Тобто на тих, що використовуються компанією і її клієнтами. Це означає, що аудитор може бути обмеженим як в доступних засобах, з метою не допустити виводу з ладу серверу, так і в часі виконання робіт (наприклад, тільки в неробочі години, або, навпаки, тільки в бізнес-години з метою вчасно зреагувати на випадок, якщо щось піде не так). Також замовник може з цієї самої причини обмежувати доступ до окремих портів на цільовому сервері.

Друге, оскільки проводиться тестування на зовнішньому сервері/сервіси, рівень захисту та чутливості на таких машинах може бути досить значним. Це може викликати певні незручності для аудитора у випадку, якщо відключення захисту або додавання робочої станції аудитора не було узгодження на етапі підготовки. Виключенням може бути спеціальний вид робіт, в якому фінальною ціллю є саме перевірка реакції служб захисту та механізмів захисту на нелегітимні дії і спроби отримати НСД.

Інколи в процес тестування може втручатись надавач інтернет послуг або сторонній провайдер мережевого засобу (фаєрволу). Зазвичай ця проблема виникає, коли замовник зі своєї стони або аудитор зі своєї не попередив провайдера послуг про заплановані активності по тестуванню безпеки.

Тестування сервісів, розміщених на сторонніх хостингах може бути проблематичним в тому випадку, коли на одному сервері розміщено багато віртуальних серверів та сервісів сторонніх власників та компаній. В такому випадку аудитор мусить зберігати особливу уважність, щоб не вийти за межі визначеного діапазону цілей. Те ж саме стосується і випадків виявлення серверів та сервісів замовника, що не входять в рамки тестування. Такі випадки повинні оговорюватись окремо з замовником. В деяких випадках вони можуть бути включені в тестування на основі додаткових домовленостей, які обов'язково повинні бути юридично закріплені відповідним документом.

Окремо варто виділити роботи по тестуванню віддаленого доступу. Головною задачею в цьому випадку є виявлення вразливостей таких засобі дослідження можливості отримати НСД до внутрішньої мережі замовника з аналізом подальших можливостей по масштабуванню наслідків НСД в разі успіху. Сюди входить тестування VPN-шлюзів, сервісів SSH та Telnet, тощо. При виконанні таких робіт варто узгоджувати з замовником використання отриманого доступу до робочих станцій співробітників, щоб не нашкодити робочим процесам.

2.3. Етап внутрішнього тестування на проникнення, аналіз нюансів та можливих проблем при проведенні

Внутрішнє тестування на проникнення має, по своїй суті, схожу з зовнішнім структуру послідовності дій. До вище вказаних активностей може додатись тестування доменної групи (AD) підприємства, тестування безпосередньо мережевих пристроїв та сегментації мережі.

Тестування доменної групи (AD) підприємства включає в себе перевірку домену підприємства на предмет наявності вразливостей, неправильних конфігурацій, слабких політик безпеки та механізмів захисту. В рамках цієї активності можуть проводитись атаки на облікові записи співробітників, домен-контролери та інші

сервіси з метою отримання поглибленого доступу. Виконуючи роботи цього роду, аудитор може отримати доступ до внутрішньої документації підприємства та особистих даних співробітників. Важливо завчасно або одразу обговорити з замовником послідовність дій у випадку, якщо станеться така ситуація та можливі способи залучення цих даних до подальших активностей.

Тестування мережевих пристроїв включає в себе перевірку налаштувань таких пристроїв, втручання в їх роботу та перевірку можливості впливати на такі пристрої без відповідних привілеїв або за допомогою сторонніх утиліт і інструментів. Виконавець повинен розумно підходити до вибору методів впливу з метою запобігання виходу з ладу мережевих пристроїв, так як це може призвести до паралізації всього робочого процесу на підприємстві, і відповідно, нанесенню значної фінансової та репутаційної шкоди підприємству у зв'язку з неможливістю виконання робочих зобов'язань перед клієнтами підприємства.

Окремою активністю може бути тестування сегментації мережевих ресурсів. Ця перевірка виконується з метою виявлення неправильного налаштування ізоляції або надання доступу до мережевих ресурсів всередині корпоративної мережі. В рамках цієї активності проводиться сканування доступності відповідних мережевих ресурсів з різних віртуальних мереж всередині корпоративної мережі і за його результатами робиться висновок щодо слідування рекомендаціям найкращих світових практик. В професійній сфері рекомендується давати мінімально-необхідний доступ до критичних мережевих ресурсів згідно робочих обов’язків співробітника або ж механізмів роботи сервісів.

Перейдемо до нюансів та проблем. Внутрішнє тестування на проникнення передбачає, що аудитор буде виконувати роботи зсередини мережевого периметру підприємства. Тобто замовник повинен завчасно подбати про допуск аудитора на локацію або ж забезпечити віддалений доступ. Проблемою в цьому випадку можуть бути затримки, пов’язані з оформленням всіх необхідних допусків та доступів. Також незручності можуть викликати нестандартні методи внутрішнього доступу, такі як

проведення тестування через окремо створену робочу станцію по віддаленому підключенню через SSH або RDP.

Виконуючи роботи всередині периметру, аудитор має дещо більшу свободу дій, ніж на зовнішньому периметрі. Це обумовлено відсутністю ризиків блокувань зі сторони механізмів захисту зовнішнього периметра, більшою кількістю доступних серверів та сервісів а також можливістю отримати інформацію із власних спостережень, якщо тестування відбувається безпосередньо на локації.

Ще одним нюансом є фізичний доступ до деяких мережевих пристроїв та протоколів на локації. Якщо це дозволено в рамках правил тестування, аудитор може використовувати не тільки визначену точку входу, а й ті, які він зможе знайти самостійно. До прикладу – безпровідні мережі.

При тестуванні домену аудитор має змогу досліджувати файлові сховища та файлообмінники підприємства. Це може стати джерелом дуже цінної інформації та допомогти в подальшому просуванні по мережі.

Основним недоліком внутрішнього тестування на локації є обмежений час знаходження аудитора там. Зазвичай проведення тестування можливе тільки в робочий час та, ймовірніше за все, під наглядом супроводжуючої особи. В той же час тестування через засоби віддаленого доступу може бути обмеженим пропускною здатністю мережі та не мати можливості одночасного підключення декількох пристроїв.

2.4. Аналіз використання технологій соціальної інженерії в рамках проведення тестування корпоративної мережі

Людський фактор все ще є значним ризиковим чинником в рамках забезпечення безпеки систем підприємства. 98 відсотків атак містять в собі елементи соціальної інженерії, і до 90 відсотків успішних витоків інформації були спричинені саме з використанням соціальної інженерії [6]. Така жахлива статистика явно показує, що

якою би не була ідеальної технічна система захисту, зловмисники все ще будуть мати шпаринку, в яку зможуть проникнути і нанести чималої шкоди ресурсам підприємства.

Але що щодо соціальної інженерії в рамках тестування на проникнення? Тестування персоналу методами соціальної інженерії є одним із типів тестування, що можуть проводитись на підприємстві чи в організації. Його метою є визначення рівня підготовки персоналу, тренування співробітників щодо загроз, викликаних соціальною інженерією та оцінка ризиків, викликаних компрометацією облікових даних співробітника таким шляхом. Також важливим є то факт, що атаки подібного роду є найбільш приближені до можливих реальних сценаріїв.

Існує декілька методів тестування персоналу в рамках аудиту соціальної інженерії:

Фішинг – атака методом імітації легітимного ресурсу, листа, веб-сайту, тощо, основною задачею якого є змусити співробітника ввести свої облікові дані, завантажити заражений файл або іншими способами надати зловмиснику спосіб проникнути всередину периметра організації. Основними факторами успіху такої атаки є низький рівень підготовки співробітників, відсутність навчання, неуважність або нехтування правилами інформаційної гігієни.

Вішинг – в контексті корпоративного тестування зазвичай є другим етапом фішингу, метою якого є отримати доступ до облікових записів співробітника у випадку, якщо в організації впроваджено мультифакторну систему автентифікацію. Особливістю є необхідність безпосереднього контакту із жертвою зловмисником шляхом телефонного виклику. Потребує довшої і більш глибокої підготовки до атаки, але все ще залишається доволі ефективним способом компрометації. В основному має ті ж самі фактори успішності, що й вішинг.

Атаки такого типу не потребують безпосередньої присутності виконавця на локації у замовника і є найбільш частими в реалізації.

Більш рідке можливе використання технік СІ безпосередньо на локації замовника. Прикладом такого є техніка Tailgating. Або ж проникнення в периметр організації за допомогою неуважності персоналу безпосередньо на фізичній локації організації.

Частіше, проведення СІ є самостійною активністю. Проте в тих випадках, коли це є частиною більш масштабного проекту, результати добуті в ході тестування можуть бути використані для подальшого просування всередину мережі.

2.5. Аналіз етапу написання звіту, як підсумку проведеної роботи при проведені тестування на проникнення

Фінальним і найважливішим результатом виконаних робіт будь-якого роду та типу є звіт – документ, в якому описується суть виконаних робіт, описуються знайдені проблеми та підсумовується загальний стан безпеки підприємства чи організації на основі проведеного тестування. Звіт може бути як самостійним документом, результуючим виконані роботи, так і використаний в подальшому для аргументації модернізації механізмів захисту підприємства або ж лягти в основу висновку щодо відповідності систем міжнародним стандартам.

Розглянемо складові типового звіту Опустимо такі технічні складові, як титульна сторінка та зміст. Першим справді інформативним пунктом в звіті є «Загальна інформація» або ж «Executive Summary». Основною задачею цього розділу є коротко підсумувати мету проведення тестування, об’єм цілей, результати та дати короткий висновок по знахідкам і рекомендаціям, щодо усунення виявлених проблем. Цей розділ характеризується більшим ухилом в сторону більш загального пояснення стану систем захисту, що була виявлена на підприємстві і призначена більше для ознайомлення керівництву або людям, що безпосередньо дотичні до систем безпеки, але не мають достатніх технічних знань та навичок для поглибленого розуміння виявлених проблем і їх виправлення.

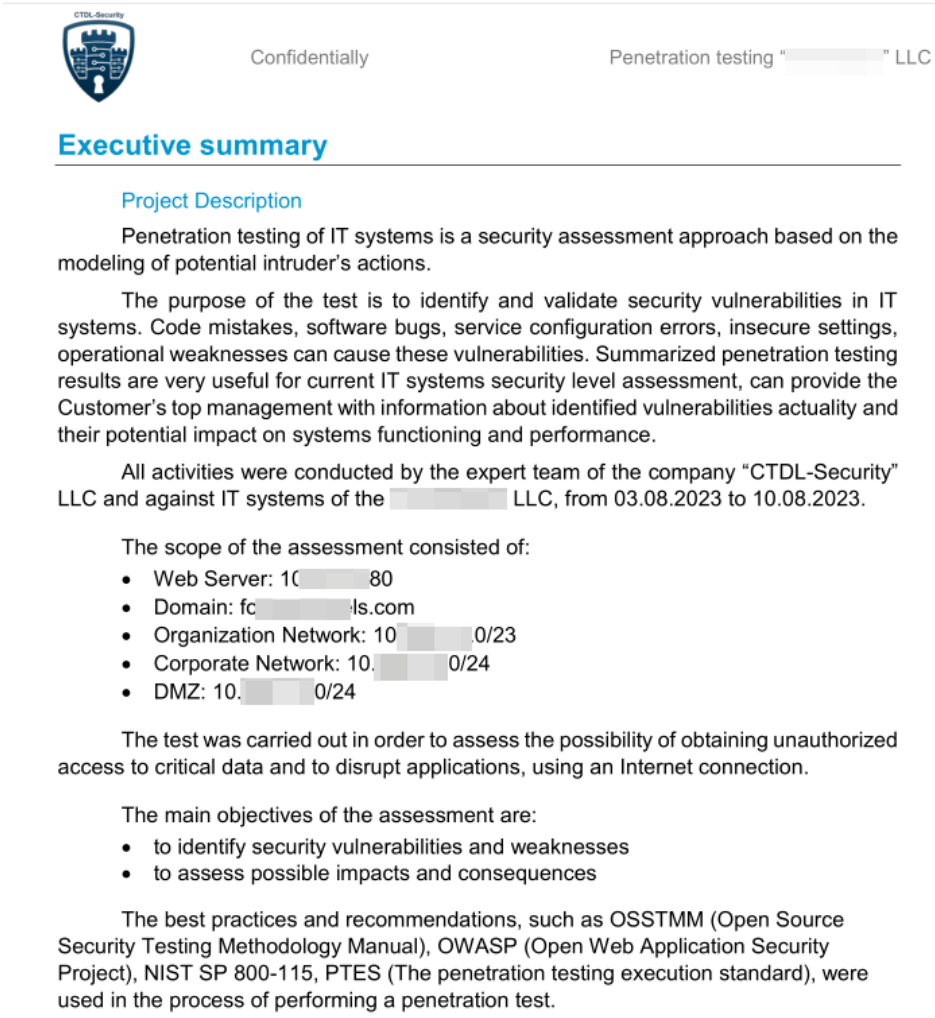


Рис. 2.5. Приклад загального опису проекту в звіті

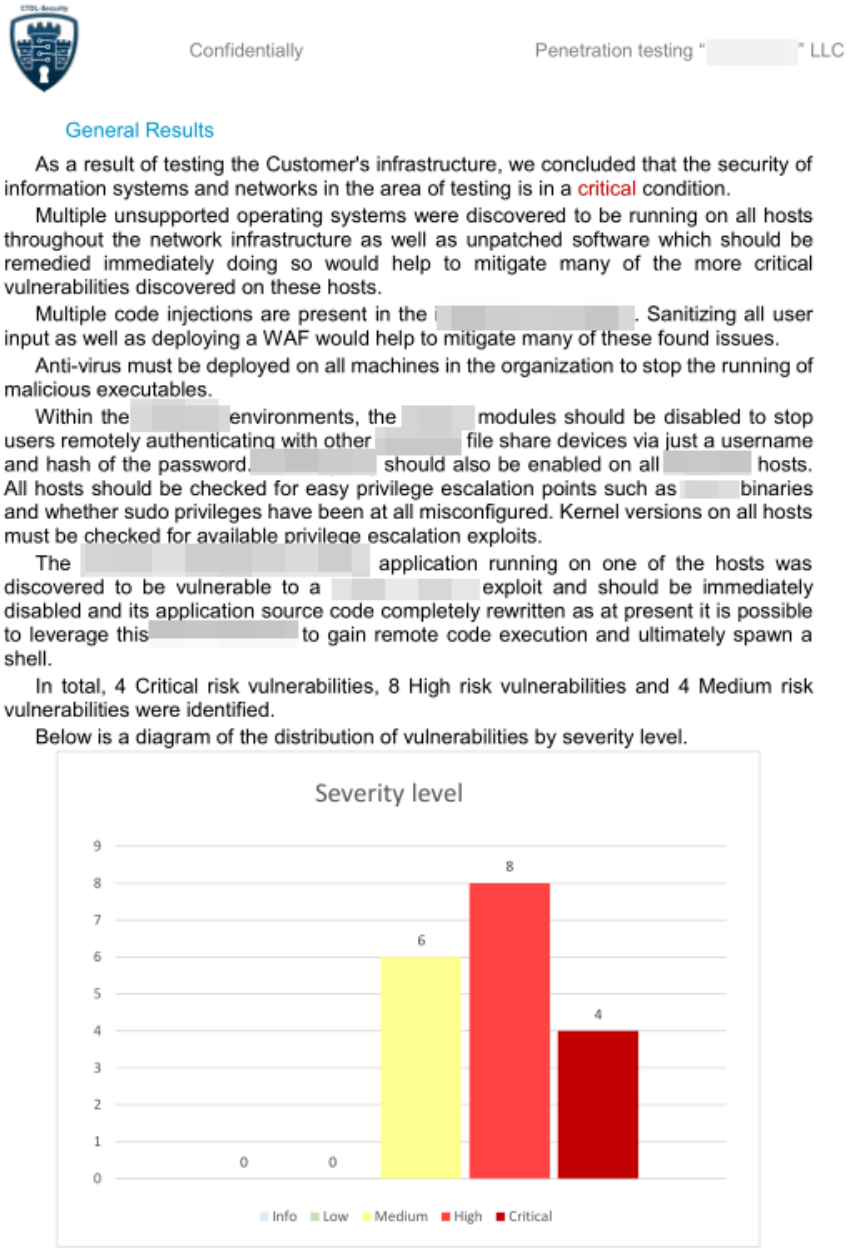
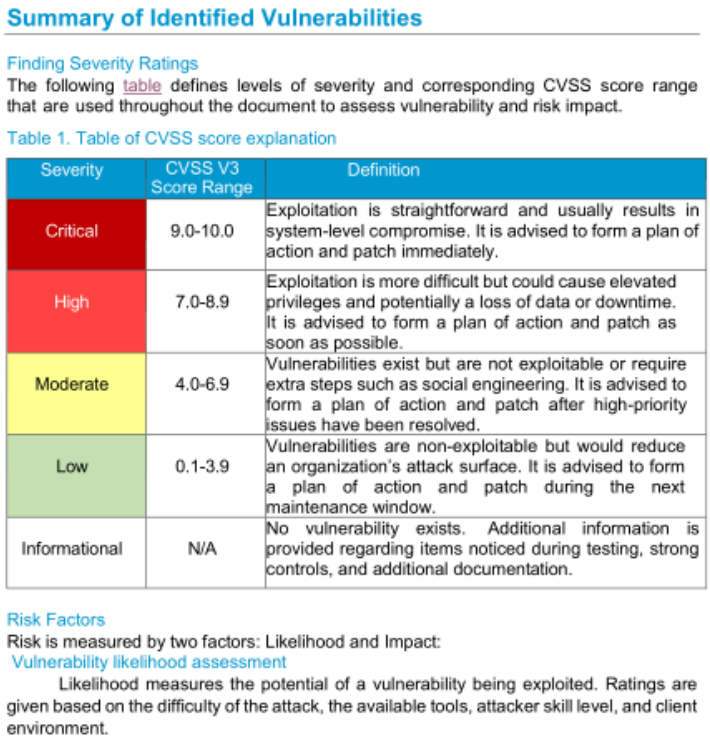


Рис. 2.6. Приклад загального огляду результату тестування

Подальшим обов’язковим розділом є опис методики, що використовувався аудитором під час проведення оцінювання. Зазвичай у кожного підприємства, чи організації, що займається проведенням тестувань, є власна методологія щодо оцінки ризиків при описі виявлених проблем та вразливостях в системах захисту. Цей розділ повинен містити чіткий опис методології, що використовувалась під час робіт,

критерії оцінювання ризиків, метрики оцінювання, роз'яснення, в яких випадках використовується та чи інша метрика і як вона впливає на загальну оцінку. В залежності від виду робіт, тут може бути описано декілька методологій і, відповідно, декілька способів і критеріїв оцінювання серйозності проблем і вразливостей.



Summary of Identified Vulnerabilities

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Table 1. Table of CVSS score explanation

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

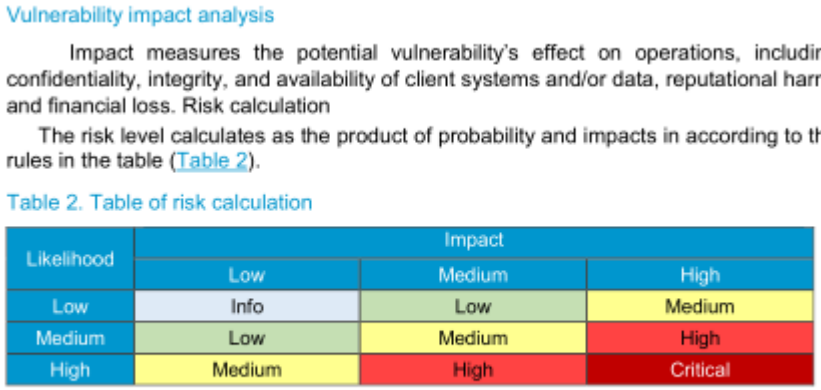
Risk Factors

Risk is measured by two factors: Likelihood and Impact:

Vulnerability likelihood assessment

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

Рис. 2.7. Приклад роз`яснення методології оцінювання



Vulnerability impact analysis

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss. Risk calculation

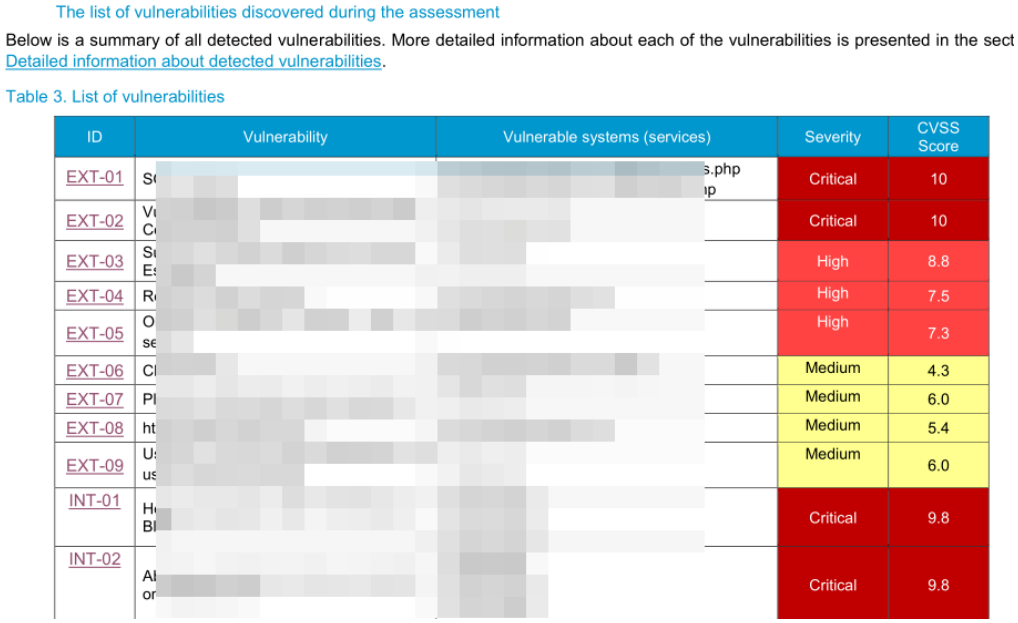
The risk level calculates as the product of probability and impacts in according to the rules in the table (Table 2).

Table 2. Table of risk calculation

Likelihood	Impact		
	Low	Medium	High
Low	Info	Low	Medium
Medium	Low	Medium	High
High	Medium	High	Critical

Рис. 2.8. Приклад роз`яснення методології оцінювання

Наступним по порядку йде розділ, де, зазвичай, в таблицях дають загальний огляд виявлених вразливостей. В цьому розділі зазвичай мінімум опису, проте знаходиться детальне перелічення основних проблем безпеки. Тут вказується назва вразливості або проблеми, перелічується, на яких саме системах вона була виявлена та надається оцінка ризикам. Цей розділ дозволяє оцінити масштабність виявлених вразливостей, чітко зрозуміти, на яких системах було виявлено проблеми та оцінити, наскільки складними можуть в подальшому бути роботи по їх усуненню.



The list of vulnerabilities discovered during the assessment

Below is a summary of all detected vulnerabilities. More detailed information about each of the vulnerabilities is presented in the sect
Detailed information about detected vulnerabilities.

Table 3. List of vulnerabilities

ID	Vulnerability	Vulnerable systems (services)	Severity	CVSS Score
EXT-01			Critical	10
EXT-02			Critical	10
EXT-03			High	8.8
EXT-04			High	7.5
EXT-05			High	7.3
EXT-06			Medium	4.3
EXT-07			Medium	6.0
EXT-08			Medium	5.4
EXT-09			Medium	6.0
INT-01			Critical	9.8
INT-02			Critical	9.8

Рис. 2.9. Загальна таблиця виявлених вразливостей

В наступному розділі опціонально може бути описана послідовність дій, що була виконана аудитором протягом тестування, так званий «KillChain». По свої суті це детальний напівтехнічний опис дій, що призвела до експлуатації критичної вразливості або захопленню повного контролю над критичними ресурсами підприємства в ході тестування. Стиль написання цього розділу, зазвичай, напівтехнічний. Згадується використаний інструментарій та параметри його використання. Але не описуються докладно технічні аспекти та рекомендації щодо уникнення вразливості в майбутньому. Ознайомлення з цим розділом дозволяє

замовнику зрозуміти, як саме аудитору вдалось обійти вбудовані механізми захисту одразу на багатьох рівнях.

Основним і, зазвичай, найбільшим розділом будь якого звіту є розділ технічного опису виявлених вразливостей та проблем. Типова інформаційна картка складається з таких частин:

1. Індекс вразливості – технічна зміна, що описує порядковий номер вразливості та, в деяких випадках її тип (внутрішня, зовнішня, тощо).

2. Назва вразливості/проблеми – технічна назва для вразливості або проблеми, яка передає її суть.

3. Вразливі системи – тут перелічуються системи або додатки, на яких була виявлена дана вразливість/проблема.

4. Рівень ризику – оцінка рівня ризику згідно використовуваної виконавцем методології.

5. Статус вразливості – деякі проблеми під час тестування можуть бути виявлені за опосередкованими ознаками, проте з певних причин можуть бути не підтверджені доказовою базою або реальною експлуатацією. В таких випадках вразливість все ще може бути вказана в звіті, але мати статус потенційної. Це робиться для того, щоб замовник звернув увагу на можливість наявності такої проблеми і прийняв превентивні дії по її усуненню в разі необхідності.

6. Опис – тут докладно описується суть проблеми з усіма технічними деталями, можливими наслідками її експлуатації та роз’яснюються можливі зміни в оцінювані вразливості згідно до середовища та особливості систем конкретно в мережі або інформаційній системі замовника.

7. Докази – в цьому пункті виконавець роз’яснює, як можна підтвердити наявність вразливості та надає докази її знаходження і експлуатації. Докази можуть бути оформлені в вигляді зображень екрану або детальному опису виконаних дій виконавцем з переліченням інструментів, що використовувались під час перевірки.

8. Рекомендації по усуненню – частина, в якій аудитор надає рекомендації по усуненню проблеми чи вразливості. Тут описуються дії, які необхідно виконати або надається посилання на офіційну документацію чи ресурси, де може бути вказана ця інструкція. В випадку виявлення застарілих версій, тут надається посилання на офіційний ресурс для завантаження актуальної версії та вказується власне номер актуальної версії.

EXT-07

ID	EXT-07
Vulnerability	Plaintext credentials easily accessible
Status	Confirmed
Scope	
Risk level	Medium (CVSS 6.0 AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N)
Description	The insecure storage or transmission of user credentials, such as usernames and passwords, without proper encryption or protection. Storing or transmitting passwords in plaintext exposes sensitive information to potential unauthorized access, leading to security breaches and unauthorized access to the critical systems.
Validation description	During the system exploring the auditor found a .sh script mean to mount a file share to the system. The content of the script contains . (SCR-33). That allowed the auditor to gain further access inside the internal network (read more inside the INT-01) .
Mitigation	Provide the necessary trainings with company personal to educate and ensure the safe containment and sharing of critical information between the employers and on their workstations. Provide the necessary security policy for encrypted storing of credentials.

Рис. 2.10. Приклад карточки вразливостей

Останнім розділом, частіше за все, йдуть докази аудитора у вигляді зображень. Кожне зображення підписується індексом пов’язаної з ним вразливості (опціонально), порядковим номером та описом того, що там зображено.

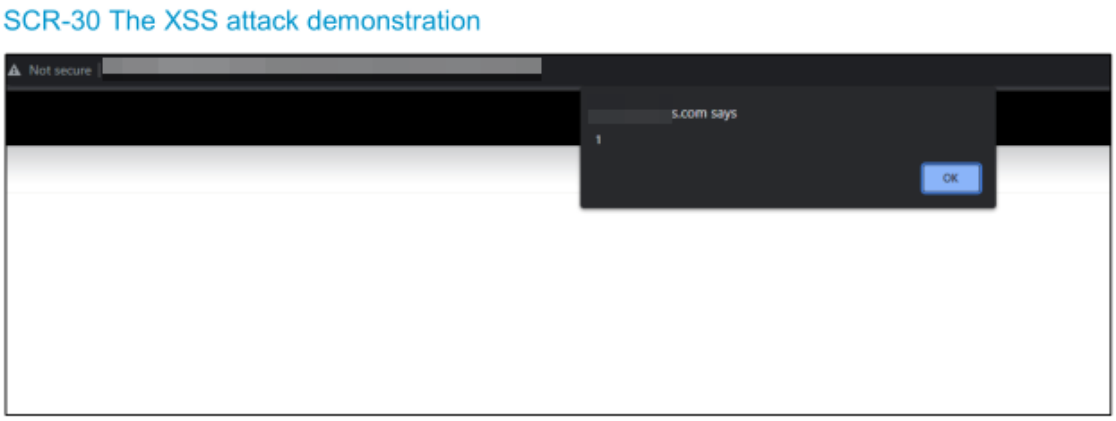


Рис. 2.11. Приклад оформлення доказу у вигляді зображення

В якості додатку до звіту можуть бути також розмішені список виявлених сервісів, додаткові форми, не зв’язані безпосередньо із змістом звіту (форми зворотного зв’язку, рекомендації щодо проведення додаткових тестувань, тощо) в залежності від організації, що виконує тестування.

Після завершення проекту, передачі та схвалення звіту замовником вся інформація по проекту, включаючи доступи, нотатки аудитора, звіт та інші дані, повинні бути зібрані та збережені захищеним способом або знищені, що оговорюється в умовах договору на виконання тестування на проникнення.

Для зберігання даних по тестуванню можна використовувати захищені носії інформації, крипто контейнери або інші дозволені договором способи.

2.6. Аналіз засобів та способів документування та нотаткування дій аудитора під час виконання тестування на проникнення

Проект по тестуванню може тривати не один тиждень і аудитору важливо не тільки прискіпливо аналізувати всі знахідки, але й відповідально зберігати свої знахідки протягом проекту.

Документування проводиться з метою збереження максимально можливої кількості інформації, що стосується проекту задля можливості в будь який момент

освіжити або нагадати аудитору про знайдені раніше зачіпки, вразливості та вектори тестування.

В процесі документування в нотатках зберігаються технічні данні вразливостей, системи, де вдалось їх проексплуатувати, докази в вигляді зображень екрану, результати спрацювання інструментів, тощо.

Також в своїх нотатках аудитор зберігає інформацію про проект у вигляді визначеного діапазону тестування, оговорених правил щодо тестування та вже виконаних дій. В деяких випадках також в нотатках може бути зібрана інформація щодо структури мережі, схема мережі та інформація, зібрана з відкритих джерел.

В рамках виконання певних видів тестування, наприклад, т. зв. Purple Teaming, нотатки можуть використовуватись для документування таймлайну виконаних аудитором дій з метою подальшого співставлення їх із спрацюваннями або не спрацюваннями механізмів захисту і реакціями команди інформаційної безпеки.

Розглянемо декілька можливих засобів та інструментів для нотаткування та документування протягом тестування.

Почнемо з виконання записів вручну. Цей спосіб, хоча й є досить непопулярним в наш час, все ще знаходить своє застосування. Його плюсом є постійна доступність. Завжди є можливість записати необхідну інформацію швидко, також для повернення до своїх записів нема необхідності вмикати електронний пристрій. Це є непоганим варіантом для тимчасового нотаткування інформації з подальшим перенесенням в електронний варіант.

Мінусом такого способу є низька надійність зберігання інформації. Записи можуть легко бути втрачені або випадково знищенні. Низька конфіденційність теж є проблемою через відсутність можливості хоч якось захистити свої нотатки від сторонніх очей без використання громіздких сховищ, типу сейфа. Неможливість зберігати зображення є проблемою для документування доказів в інформаційних системах.

В плані електронних засобів збереження інформації є декілька варіантів для використання.

Знайомим для більшості є варіант зберігання інформації в Microsoft OneNote. Ця програма вбудована в стандартний пакет Microsoft Office та підтримує можливість хмарного збереження документів. З плюсів можна відзначити простий інтуїтивно зрозумілий інтерфейс. Можливість форматування текстів, сумісність з більшістю інших додатків, можливість збереження файлів всередині документів.

До мінусів можна віднести платне розповсюдження, закритість вихідного коду та неможливість організації дерев нотаток глибше ніж на два рівні. Також Microsoft офіційно не випускали своє сімейство офісних додатків на ОС сімейства Linux, що може бути проблемою для користувачів цих систем.

Альтернативою з відкритим вихідним кодом є додаток CherryTree. Це програма для створення та збереження нотаток, що розповсюджується за ліцензією GNU General Public License та розповсюджується абсолютно безкоштовно. Додаток підтримується усіма розповсюдженими ОС та дозволяє зберігати документи, нотатки, скрипти, зображення, формули, тощо. Плюсом додатку є його незалежність від великих корпорацій, простота в використання, можливість виконання вбудованого в скрипти коду, можливість зашифрувати файл з нотатками та необмежена глибина гілок з нотатками.

До мінусів можна віднести відсутність можливості хмарного збереження документа безпосередньо з програми, дещо неінтуїтивний інтерфейс, відсутність широкої можливості форматування текстів.

Висновки до Розділу 2

Тестування на проникнення – комплексний та складний процес, що потребує плідної співпраці між замовником та виконавцем. Починаючи з моменту планування і до самого фіналу у вигляді прийняття звіту має бути налагоджений оперативний

зв’язок для швидкого вирішення можливих проблем, заминок та врахування нюансів, пов’язаних з індивідуальними особливостями вимог замовника, особливостями конфігурацій інформаційних систем та можливих форс-мажорів.

Якісне виконання тестування потребує від виконавця високих компетенцій в сфері інформаційної безпеки. Глибокого розуміння не тільки інструментарію, що використовується в тестуванні, але й комплексного розуміння систем, що піддаються тестуванню.

Також від аудитора необхідне вміння прискіпливо документувати всі виявлені знахідки, докази їх наявності, рекомендації по усуненню та грамотно описувати їх як для себе, так і в ході написання фінального звіту по тестуванню з метою повного розуміння в майбутньому замовником суті проблем та правильного їх вирішення.

Виконавець також повинен вміти якісно оцінити ризики, що та чи інша вразливість може нести системам замовника задля розумного їх використання в ході тестування та правильної оцінки їх критичності в звіті в подальшому.

З 3. РОЗРОБЛЕННЯ ТЕХНОЛОГІЇ ПРОВЕДЕНННЯ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ В КОРПОРАТИВНІЙ МЕРЕЖІ

3.1. Розроблення методології проведення тестування на проникнення на базі існуючих методологій

В рамках створення цієї методології розглядається сценарій проведення тестування на проникнення типу Black Box з необмеженим доступом до ресурсів та локації замовника з відсутністю обмежень по використанню будь-яких способів та інструментів. В разі реального використання методологія може бути видозмінена з урахуванням особливості проекту та поставлених обмежень. Протягом всього процесу тестування варто постійно вносити виявлену інформацію та виконані дії в нотатки а також вносити зміни в власний план дій.

1. Розвідка доступних для тестування активів/серверів.

Розвідка може проводитись як ззовні периметру, так і зсередини. Розглянемо обидва варіанти.

1.1 Розвідка із-за меж зовнішнього периметру.

Почати розвідку можна з використання джерел у відкритому доступі. Знаходження по запитам імен замовника в пошукових сервісах. Це дасть нам змогу визначити публічно доступні домени, субдомени та сервіси замовника а також зв’язані з ними дочірні фірми, які теж можуть входити в діапазон тестування.

Великі компанії можуть викупати собі цілі діапазони IP-адрес для створення власної автономної інформаційної системи і власного користування. Такі діапазони отримують свій ASN, який призначається організацією IANA. Потенційна інформація про ASN, така як діапазон IP-адрес, домени, що належать підприємству, може бути знайдена в публічно доступних реєстрах (наприклад реєстр RIPE NCC для європейського регіону).

Ще одним способом пошуку доменів за умови вже відомих адрес може бути реверсивний DNS пошук. Якщо компанія використовує власні потужності, то цей пошук дасть інформацію про домени, що знаходяться на цих адресах.

Знайшовши основний домен замовника, варто зайнятись пошуком доступних на ньому субдоменів. Адже за ними можуть бути такі важливі цілі, як технічні сервіси, поштові сервери, сервіси для співробітників, технічна документація, файлосховища, тощо. Існує безліч інструментів для пошуку субдоменів: від автоматичних утиліт, що проводять пошук по відкритим джерелам, закінчуючи утилітами, що проводять пошук субдоменів методом перебору по спискам з розповсюдженими варіантами назв субдоменів. Унікальним варіантом є дослідження сертифікатів SSL, в яких можуть бути згадки про всі домени та субдомени, на які розповсюджується цей сертифікат.

Для знаходження IP-адрес, маючи лише домен замовника, можна використовувати запити до реєстрів DNS або ж утиліти, що виконують це автоматично. Наприклад, WhoIs, DNSDumpster, тощо.

Корисним буде провести пошук на предмет злитих баз даних, паролей, тощо у відкритому доступі. А також пошукати публічно доступні репозиторії.

Виконання вище вказаних дій повинна дати достатньо інформації для початку безпосередньої взаємодії з системами замовника.

Валідувати, які з виявлених адрес та доменів доступні можна виконавши ICMP-запит. Ще одним варіантом є відправка TCP-запитів.

1.2 Розвідка внутрішньої мережі

Розвідка всередині мережі дещо відрізняється від зовнішньої. У аудитора зникає можливість використовувати зовнішні сервіси для знаходження адрес та доменів. Проте з’являється можливість збирати інформацію безпосередньо з трафіку всередині мережі.

Ефективним засобом збору інформації про влаштування мережі пасивним способом є прослуховування мережевого трафіку. По мережі переміщується багато технічних пакетів: TCP-трафік, ARP-запити, відповіді на них, тощо. Для збирання цієї

інформації можна використовувати такі інструменти, як TCP-dump, Wireshark, інструменти сімейства net-, тощо. Використовуючи можна полегшити збір цієї інформації.

Активним засобом збору інформації може бути пряме звернення до доменних серверів мережі.

2. Проведення сканування портів задля дослідження наявних на них сервісів.

Цей пункт ще більше розширює розуміння структури сервісів, що входять в рамки тестування. Він дозволяє зрозуміти, на яких сервісах варто зосередити увагу, розширити розуміння того, які інструменти варто використовувати та передбачити можливі шляхи обходу систем захисту інформації. В рамках цього пункту аудитор також отримує інформацію про програмне забезпечення, ОС, що використовуються на серверах та їх версії. Зазвичай сканування проводиться за декілька спроб. На першій проводиться TCP та UDP сканування по обмеженій кількості портів (зазвичай топ 1000/100 з найбільш використовуваних). На другій проводиться сканування по повному діапазону всіх мережевих портів (топ 1000 для UDP).

3. На основі знайдених сервісів проводиться пошук відомих вразливостей до них та робиться вибірка пріоритетних цілей для спроб проведення подальших атак.

Маючи повний список активних сервісів, наступним етапом варто провести додаткове дослідження задля встановлення відомих вразливостей, доступних для них експлойтів та подальшого алгоритму дій по тестуванню. Для цього можна використовувати бази даних вразливостей, такі як National Vulnerability Database, CVE, тощо.

4. Тестування знайдених сервісів.

Використовуючи знайдену інформацію, проводиться тестування виявлених сервісів. Варто зазначити, що ціллю тестування на проникнення є знаходження всіх вразливостей безпеки. Це означає, що варто перевіряти всі можливі вразливості, а не тільки ті, що дозволять просунутись далі в мережі замовника. Так сам як необхідно документувати кожну знахідку для звітування в подальшому.

4.1 Тестування з використанням автоматичних засобів.

Полегшити процес тестування можна використанням автоматичних засобів тестування. Сюди входять сканери вразливостей, фреймворки для тестування, тощо. Комплексні фреймворки, такі як metasploit, дозволяють не тільки спростити експлуатацію експлойтів на сервісах, але й налаштувати переадресацію трафіку, віддалений доступ до захоплених серверів та забезпечити постійний доступ до них.

4.2 Тестування засобами грубої сили.

Доволі часто отримати розширений доступ до сервісів можна застосувавши атаку грубої сили. Значна кількість компаній забуває змінити або нехтує рекомендаціям змінити паролі та логіни для автентифікації на мережевих пристроях, принтерах, сервісах. Це дозволяє аудитору отримати доступ до їх панелі керування або автентифікуватись з привілеями користувача на сервісах.

5. Проведення атаки методами соціальної інженерії.

Коли не вдається отримати доступ до сервісів замовника стандартними методами, корисним може бути спроба отримати доступ методами соціальної інженерії (якщо це дозволено або обумовлено умовами тестування).

Короткий алгоритм для проведення базової фішингової атаки виглядає так:

- Збір вхідних даних:
    - Вибір домену для проведення атаки;
    - Знаходження сторінки авторизації, яку можна використати в якості прикладу для фішингової сторінки;
    - Отримання списку електронних адрес співробітників.
- Технічна підготовка.
    - Пошук і купівля домену зі схожою до цільового назвою;
    - Налаштування поштового сервісу на домені для отримання можливості розсилки;
    - Налаштування віддаленого серверу з ПЗ для збору облікових даних.

- Підготовка до атаки:
    - Створення фішингового листа;
    - Створення фішингової веб-сторінки.
- Проведення атаки

Атаку рекомендовано проводити в вечірній час в другій половині тижня. Тематика листа мусить спонукати на термінову дію але бути логічною.

Для знаходження максимально схожих до оригінальних доменів можна слідувати таким порадам:

Використовуйте ключові слова. Шукайте домен зі схожими ключовими словами в назві.

Можна використати домен, що імітує назву субдомену (наприклад: www-example.com).

Домен, що має таку ж назву, але інакший домен верхнього рівня.

Використання технік заміни символів на схожі, незначної зміни їх порядку, подвоєних символів, прибирання символу або ж додавання малопомітних символів.

Це дозволить приспати увагу малоуважних жертв та з досить великою ймовірністю отримати їх облікові дані і, відповідно, доступ до сервісів.

6. Отримання доступу до виконання команд всередині цільової системи.

Використовуючи відомі вразливості на сервері/сервісі або помилки в логіці роботи програм необхідно знайти спосіб для виконання команд в середовищі операційної системи цільового серверу.

7. Дослідження цільової системи.

З використанням доступу, отриманого в попередньому пункті необхідно максимально дослідити доступні дії. Сюди входить дослідження найближчого мережевого середовища, файлової системи, рівня привілеїв, доступних для виконання програм та додатків, знаходження доступних до виконання скриптів та дослідження їх функціоналу.

8. Завантаження файлів з цільової системи.

В разі знаходження «цікавих» для дослідження файлів, що можуть містити хеші, паролі, тощо, необхідно знайти спосіб їх передачі на пристрій для детальнішого дослідження. Наприклад, створення http серверу за допомогою модуля python.

9. Ескалація привілеїв.

В залежності від операційної системи та доступних засобів, можуть бути використані різні техніки для отримання вищого рівня привілеїв. Також привілеї можуть бути підвищені як на локальний системі, так і в домені організації.

9.1 Ескалація локальних привілеїв.

Локальні привілеї можуть бути ескальовані багатьма різними способами. Основними з яких є експлуатація вразливостей, запуск shell з системними правами або виконання скриптів, що можуть запускати процеси від імені адміністратора або з root правами.

9.2 Ескалація доменних привілеїв

Ескалація доменних прав потребує або наявності профіля користувача в домені, та/або машини, що має доступ до домен-контролера. Прикладом такої дії є, наприклад, отримання т. зв. «Golden Ticket», атака, що дозволяє за допомогою знайденого на «захопленій» машині NTLM-тікета доменного адміністратор створити отримати в домені «профіль» що буде мати права адміністратора але не буде логуватись засобами захисту.

10. Постексплуатація

В цей етап входять дії, що виконуються на серверах, над якими у аудитора є максимально можливий рівень привілеїв. Основною задачею цього етапу є збір тієї інформації, що раніше не була доступна та остаточне закріплення в системі.

10.1 Збір конфіденційної інформації з систем

Використовуючи раніше отримані права в сервері, аудитор може збирати максимальну кількість інформації з сервера. Зазвичай, під час звичайних проектів це не потребує викачування великих масивів даних. Проте така активність може

проводитись з метою перевірки реакції механізмів захисту на спроби викрадення конфіденційних даних

10.2 Отримання стабільного доступу до системи.

В цьому пункті основною задачею є постійне і безперебійне забезпечення доступу для аудитора на захоплений сервер. Цього можна досягти за допомогою використання системних процесів та планувальників задач. Маскування під легітимний системний процес забезпечить невидимість для засобів захисту інформації. Використання та налаштування ж планувальника задач дозволить забезпечити регулярне створення цього самого процесу, через який аудитор зможе підключатись до захопленої системи навіть у випадку перезавантаження серверу.

11. Переадресація трафіку

В ході проведення дослідження можуть бути виявлені мережеві ресурси, доступ до яких надається виключно для обраних ресурсів і фільтрується для будь-яких сторонніх запитів. В таких випадках необхідно використовувати техніки переадресації запитів, щоб можна було використовувати проміжні захоплені машини для переадресації трафіку на такі ресурси.

12. Тестування веб-додатків

Тестування веб-додатків дещо відрізняється від процедури тестування мережі. До раніше вказаних етапів може додатись аналіз взаємодії з API, аудит коду додатку, модифікація запитів на сервер, виконання ін’єкцій в запитах на сервер та до баз даних а також тестування механізмів автентифікації на стійкість до атак грубої сили та підбору паролей.

Під час тестування на проникнення зовнішнього периметру в разі проникнення у внутрішній периметр методологію варто розпочинати з початку задля повного покриття отриманих можливостей та максимального розширення кількості знахідок.

3.2. Розроблення методології документування знахідок під час виконання тестування на проникнення

Зберігання інформації про знахідки під час тестування на проникнення є важливою роботою, що потребує від аудитора уважності, самодисципліни та прискіпливості. Саме з цих нотаток аудитор буде писати звіт по завершенню активного етапу робіт. При створені і ведені нотаток задачею аудитора є збереження максимального об'єму інформації. Дана методологія може бути змінена в залежності від особливостей проекту, специфіки задач та особистих вподобань людини, що використовує її.

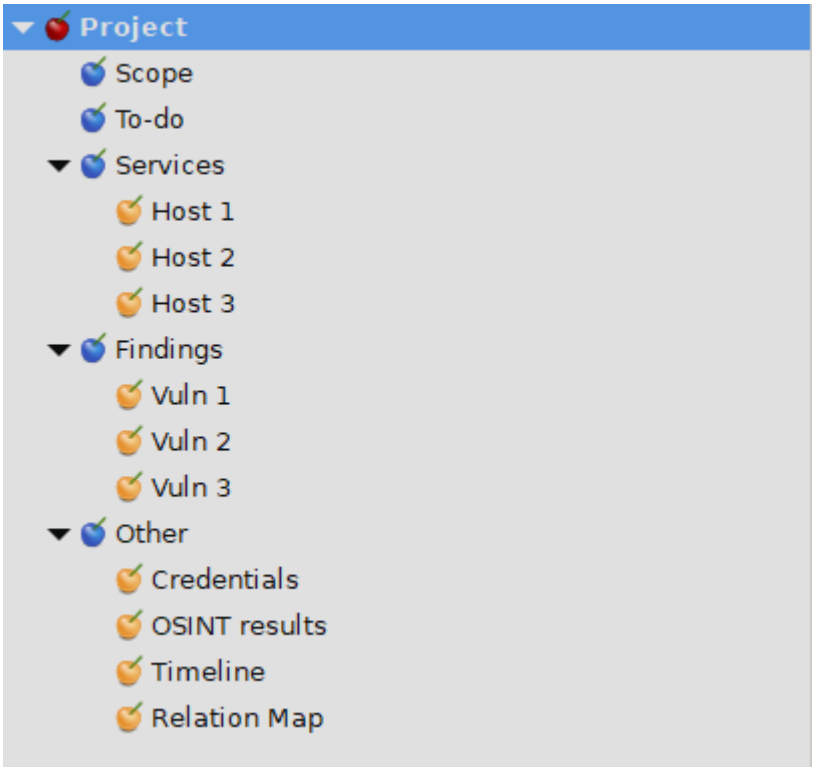


Рис. 3.1. Приклад структури нотаток під час ведення проекту по тестуванню на проникнення в ПЗ CherryTree

В нотатках аудитора обов'язково повинні зберігатись така інформація:

Загальний діапазон тестування або ж список цілей. В цій частині аудитор виписує список цілей, на який розповсюджується дозвіл на тестування. В подальшому

до цього розділу можна буде повертатись, якщо виникнуть сумніви щодо того, чи входить виявлений сервер/сервіс/домен до дозволених цілей для тестування.

Список задач. В цьому розділі аудитор на основі створеної в попередній частині або за власною методологію, створює список задач, яких він бажає або мусить досягти протягом тестування. Задачі можуть поділятись на етапи, доповнюватись по ходу тестування та видозмінюватись в залежності від знахідок протягом тестування. Використовуючи цей розділ аудитор зможе легко поставити тестування на паузу в разі необхідності і так само легко, в разі необхідності, повернутись до його проведення.

В наступному розділі, «Сервіси» рекомендовано розміщувати в окремих підрозділах виявлену інформацію по кожному окремому серверу. В разі необхідності, гілку нотаток можна розбити ще й на окремі сервіси. Тут зберігається інформація про версії програмного забезпечення, знайдені цікаві дані, зображення з екрану з сервера/сервісу, тощо. Також за допомогою видозмінювання іконок в даному розділі можна позначати сервери та сервіси, робота над якими вже завершена.

Наступний розділ, «Знахідки». В цьому розділі окремими сторінками варто виносити інформацію про знайдені вразливості. Сюди входить опис вразливості, спосіб її експлуатації, докази виявлення вразливості та сервери і сервіси, на яких було виявлено дану вразливість. На основі саме цього розділу в подальшому будуть створюватись карточки вразливостей у звіті по завершенню робіт.

В розділі «Інше» знаходиться загальна інформація, зібрана в ході проведення робіт по тестуванню. Зазвичай тут аудитор збирає ту інформацію, яку не можна однозначно віднести до якогось окремого сервісу чи яку важливо відокремити задля можливості оперативно повернутись до неї в подальшому. До такої інформації може відноситись:

Зібрані облікові дані співробітників або технічних облікових записів. Вони в подальшому можуть спрацювати і на інших серверах замовника, тому рекомендується відокремити їх в своїх нотатках.

Файли та інформація про інші інформаційні ресурси, що були знайдені на цільових серверах в ході тестування, але які не можна використати на сервері походження. До прикладу, скрипти, бази даних, персональні дані, тощо.

В разі проведення проекту з вимогою фіксування таймлайну виконаних активностей, інформація про це може також зберігатись в цьому розділі.

Мапи відносин серверів та доменів, схеми мережі, блок схеми теж рекомендується виносити в окреме місце.

В цілому, спосіб ведення нотаток є індивідуальним від виконавця до виконавця. Наведена методологія є лише одним із безліч запропонованих варіантів. Окрім зберігання записів в електронних нотатках, інформацію по ходу виконання проекту можна зберігати у вигляді блок-схем, ієрархічних мап відносин, схематичних «дерев», тощо.

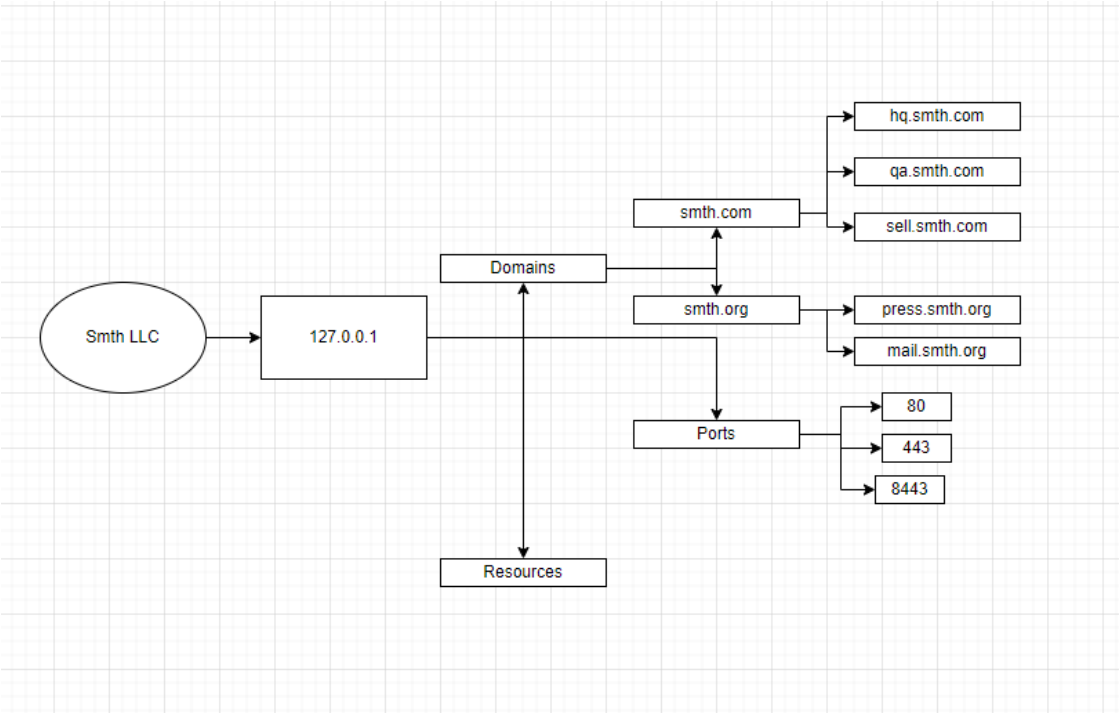


Рис. 3.2. приклад збереження інформації у вигляді mindmap

3.3. Розроблення рекомендацій щодо звітування щодо проведених робіт після завершення тестування

Якою б чудовою не була робота аудитора під час тестування на проникнення, фінальний результат буде оцінюватись за результатами, викладеними в звіті. Тому важливо приділити особливу увагу написанню звіту.

Написання звіту починається одночасно зі стартом тестування з нотаток аудитора щодо знахідок. Методологія по нотаткуванню була запропонована в попередній частині. В цій частині пропонується методологія по написанню якісного фінального звіту.

Фінальний звіт рекомендується компонувати з трьох основних частин: загальний підсумок, узагальнені дані та технічні подробиці. Зображення та докази рекомендується виносити в окремий додаток а в тексті на їх місці використовувати гіперпосилання.

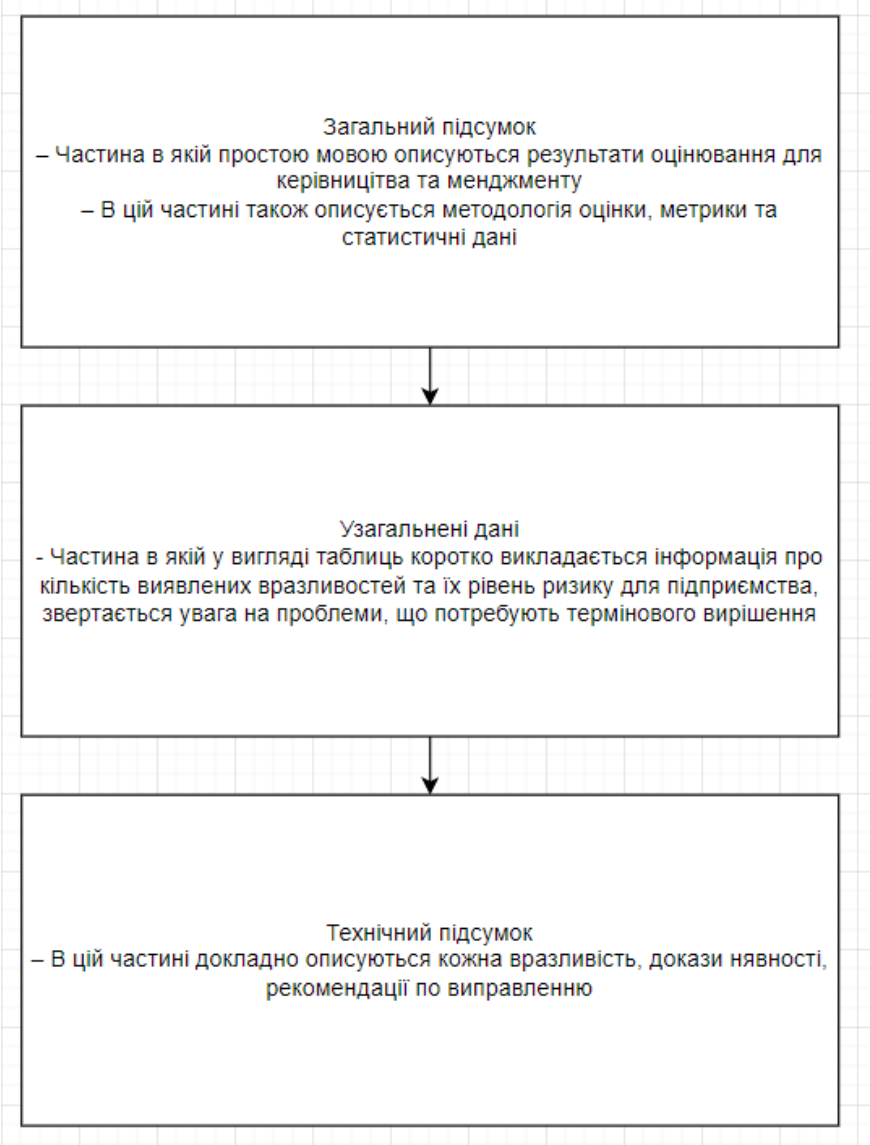


Рис. 3.3. Спрощена схема змісту звіту

Загальний підсумок. Це перша частину кожного звіту по завершення тестових робіт.

Об’єм мусить бути не більше ніж декілька сторінок.

Основною задачею цієї частини є презентувати результати тестування для людей, що не знайомі або мало знайомі з технічною частиною забезпечення безпеки. Тобто, зазвичай, керівництво або менеджмент підприємства-замовника.

В цьому розділі не рекомендується використання професійних жаргонізмів та абревіатур.

В першій частині розділу рекомендується розмістити опис проекту, себто інформацію про проект, терміни, діапазон серверів та адрес, що піддавались тестуванню а також коротко роз’яснити, яка методологія використовувалась під час тестування.

В другій частині розділу рекомендується розмістити загальний огляд результатів тестування. Сюди входить кількість виявлених вразливостей за рівнем їх ризику, загальна оцінка стану безпеки системи. Коротке згадування незначних проблем та трохи детальніший опис проблем високого та критичного рівня ризику. Також в цьому розділі можна розмістити рекомендації щодо включення додаткових серверів або ресурсів в майбутні тестування. Так само тут графічно можна продублювати кількість виявлених вразливостей за рівнем ризику. Наприкінці розділу рекомендується окремою частиною докладно описати, на основі якої методології проводилась оцінка ризиків. Коротко, обов’язкові частини цього розділу можна виділити так:

- Загальний опис проекту;
- Загальна оцінка стану безпеки;
- Кількість виявлених проблем та короткий опис їх потенційного впливу на підприємство;
- Опис методології оцінювання ризиків.

Додатково тут у вигляді графіку можна вказати кількість атак по типам, які вдалось успішно реалізувати.

Друга частина звіту, узагальнені дані. В цій частині в вигляді таблиць та опису виконаних дій рекомендується надати докладнішу інформацію про вразливості та послідовності дій, що призвели до експлуатації вразливостей.

Таблиць може бути декілька, наприклад:

Таблиця 1: виявлені вразливості, до якої будуть входити назва вразливості, вразливі ресурси, оцінка ризику.

Таблиця 2: список вразливостей, які потребують термінового усунення з вказанням рекомендацій по їх усуненню.

В залежності від цілі тестування, в цьому розділі також можуть бути таблиці з вказанням вразливостей, які треба усунути згідно вимог того, чи іншого стандарту.

Опис послідовності дій варто виконувати в формальному стилі, основний фокус опису має бути на просуванні в глибину інфраструктури замовника та експлуатації декількох найбільш критичних вразливостей. Вразливостями, що не призвели до просування або низького рівня ризику в цій частині можна нехтувати.

В другій частині дозволяється помірне використання технічних термінів та фразеології.

Третю частину звіту рекомендується присвячувати докладному опису кожної знайденої вразливості. Це можна робити у вигляді окремих підрозділів або ж таблиць у вигляді карток вразливостей.

Для кожної з вразливостей обов’язково мусять бути присутні такі пункти:

- Порядковий номер вразливості або індекс;
- Назва вразливості за однією з класифікацій (WASC, MITRE, OWASP);
- Статус вразливості;
- Список вразливих ресурсів;
- Рівень ризику вразливості з вказанням параметрів, що вплинули на оцінку
- Докладний технічний опис вразливості, наслідків її експлуатації та роз’яснення обставин, що могли вплинути на зміну рівня ризику (наприклад, вразлива система доступна тільки із внутрішньої мережі).
- Опис дій, необхідних для відтворення вразливості з вказанням використаних утиліт та параметрів. Бажано додати зображення доказів вразливості в додаток з гіперпосиланнями в основному тексті.

- Рекомендації по усуненню проблеми/вразливості. Допускається надання посилань на офіційні інформаційні сторінки, якщо вразливість була знайдена в певному продукті.

Така інформація має бути викладена для кожної вразливості незалежно від рівня ризику.

Завершити звіт можна додатками. В них можуть бути зображення з доказами, форми зворотного зв'язку, загальна таблиця виявлених сервісів, загальна таблиця взятих під контроль інформаційних ресурсів та пристроїв і серверів.

Після передачі звіту замовнику всю інформацію, що стосується тестування на проникнення обов'язково необхідно розмістити в захищеному сховищі.

Висновки до Розділу 3

В розділі було запропоновано власні варіанти методології по виконанню робіт з виконання на проникнення, збереження інформації під час виконання тестування та створенню фінального звіту за результатами виконаних робіт.

Створені методології носять рекомендаційний характер та можуть бути видозмінені під індивідуальні потреби виконавця та в залежності від особливостей виконання того чи іншого проекту.

Методології були створені з урахуванням визнаних світом робіт, таких як OWASP, NIST SP 800-115 та OSSTMM, а також з використанням знань та навичок, набутих в ході проведених досліджень, професійної діяльності і отримання сертифікації eCPPTv2.

ВИСНОВОК

Було виконано дослідження сфери тестування на проникнення. В ході дослідження було розглянуто різні методології, інструкції та рекомендації щодо проведення тестувань на проникнення. На основі проведених аналізів та досліджень було розроблено власний варіант методології проведення тестувань на дослідження в корпоративній мережі.

В першій частині було розглянуто загальну проблематику, зв’язану з відсутністю або нерегулярним проведенням аудитів безпеки та тестувань на проникнення. Означено та висвітлено основні задачі і мету проведення тестування на проникнення. В рамках цього розділу також було досліджено загально прийняті методології тестування.

В другій частині було досліджено поетапно алгоритм проведення тестування на проникнення. Для кожного етапу було проведено аналіз можливих проблем, що можуть виникнути, нюансів, пов’язаних з їх проведенням та їх впливу на фінальний результат. Окрема увага була приділена аналізу етапу підготовки до проведення тестування та етапу написання фінального звіту за результатами робіт. Проведений аналіз та доведена важливість правильного збереження інформації в ході проведення тестування.

В третьому розділі на основі проведених досліджень та аналізів а також на основі реального професійного досвіду, здобутого в ході професійної діяльності та навчання в рамках підготовки та отримання сертифікату eCPPTv2 було розроблено та викладено методологію щодо проведення тестування на проникнення в корпоративній мережі, методологію щодо збереження та нотаткування інформації, здобутої в ході виконання робіт а також методологію щодо написання фінального звіту за виконаними роботами.

Виконана робота може бути використана в ході виконання реальних робіт по тестуванню на проникнення безпеки інформаційних систем, має високу гнучкість і достатню простоту для використання малодосвідченими виконавцями тестувань.

ПЕРЕЛІК ПОСИЛАНЬ

1. Poireault K. A guide to zero-day vulnerabilities and exploits for the uninitiated. Infosecurity Magazine. URL: https://www.infosecurity-magazine.com/news-features/guide-zero-day-vulnerabilities/ (дата звернення: 28.11.2023).

2. CVE security vulnerability database. CVEdetails. URL: https://www.cvedetails.com (дата звернення: 28.11.2023).

3. Herzog P. OSSTMM 3 the open source security testing methodology manual. ISECOM. URL: https://www.isecom.org/OSSTMM.3.pdf (дата звернення: 29.11.2023).

4. Web security testing guide. OWASP.org. URL: https://owasp.org/www-project-web-security-testing-guide/stable/ (дата звернення: 29.11.2023).

5. Special Publication 800-115. Technical guide to information security testing and assessment. Вид. офіц. Gaithersburg : Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, 2008. 80 с. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf (дата звернення: 01.12.2023).

6. Reed C. 30 social engineering statistics. Firewall Times. URL: https://firewalltimes.com/social-engineering-statistics/ (date of access: 03.12.2023).

7. Tenable Nessus. Tenable. URL: https://www.tenable.com/products/nessus (дата звернення: 05.12.2023).

8. Penetration Testing. Imperva. URL: https://www.imperva.com/learn/application-security/penetration-testing/ (дата звернення: 06.12.2023).

9. brianwhelton. [Best Pen Test engagement agreement rule I've ever seen]. URL: https://community.spiceworks.com/topic/2141148-best-pen-test-engagement-agreement-rule-i-ve-ever-seen (дата звернення: 08.12.2023).

10. Web Security Testing Guide. Reporting. OWASP.org. URL: https://owasp.org/www-project-web-security-testing-guide/stable/5-Reporting/README (дата звернення: 08.12.2023).

11. Krishna A. Website penetration testing- A complete guide. getastra.com. URL: https://www.getastra.com/blog/security-audit/website-penetration-testing/ (дата звернення: 11.12.2023)

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)