Міністерство освіти і науки України
Тернопільський національний економічний університет
Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки

«ТЕСТУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ НА ПРОНИКНЕННЯ»

ОПОРНИЙ КОНСПЕКТ ЛЕКЦІЙ

для студентів спеціальності 125 «Кібербезпека»

за другим магістерським рівнем вищої освіти»

Тернопіль

ТНЕУ

2019

Опорний конспект лекцій з курсу «Тестування комп'ютерних систем на проникнення» для студентів спеціальності 125 «Кібербезпека» – Тернопіль: ТНЕУ, 2019. – 119 с.

Укладач: Яцків В.В., д.т.н., доцент

Рецензенти: Марценко С. В.., к.т.н., доцент, доцент кафедри комп'ютерних наук Тернопільського національного технічного університету ім. І. Пулюя;

Сегін А.І., к.т.н., доцент, доцент кафедри спеціалізованих комп'ютерних систем Тернопільського національного економічного університету.

Відповідальний за випуск: Яцків Василь Васильович, д.т.н., доцент, завідувач кафедри кібербезпеки

Затверджено на засіданні кафедри кібербезпеки,

протокол № 1 від 27 серпня 2019 р.)

Розглянуто та схвалено групою забезпечення спеціальності кібербезпека,

протокол №1 від 30.08. 2019 р.

Затверджено вченою радою факультету комп'ютерних інформаційних технологій, протокол №1 від 18.09.2019 р.

ЗМІСТ

ВСТУП

Тестування на проникнення використовується для пошуку недоліків у комп’ютерних системах з метою вжиття відповідних заходів безпеки для захисту даних та підтримки функціональності.

В курсі «Тестування комп’ютерних систем на проникнення» ви дізнаєтесь, якими знаннями та практичними навичками повинен володіти спеціаліст з тестування на проникнення, а також технічні та етичні обов'язки, які беруть на себе спеціалісти з тестування на проникнення. Даний курс забезпечить формування навичок необхідних для досягнення успіху у області тестування на проникнення та практичної безпеки.

Зокрема, ви познайомитеся з сучасними методами злому, які використовуються в даний час. Ви також познайомитеся з прийомами, які використовують фахівці під час тестування на проникнення для отримання інформації або встановлення бази, з якої можна запускати більш вдосконалені тести на проникнення.

Крім того, розуміння мотивацій хакерів може допомогти вам зрозуміти масштаби нападу або, можливо, навіть допомогти у виявленні деталей нападу. Насправді фахівцям з кібербезпеки потрібно думати, як хакери, щоб встановити, чому вони можуть здійснювати атаку, а потім використовувати цей досвід для тестування мережі клієнта.

Опорний конспект з курсу «Тестування комп’ютерних систем на проникнення» забезпечує уявлення про основні сучасні концепції тестування на проникнення.

1. Безпека та тестування на проникнення

Тестування на проникнення може виявити, наскільки безпеці IT-систем загрожує атака з боку хакерів, зловмисників, тощо, а також чи здатні заходи безпеки в даний час забезпечити IT безпеку.

Що таке тестування на проникнення? Тестування на проникнення це тип тестування безпеки, який використовується для перевірки безпеки програми. Він проводиться з метою виявлення ризику безпеки, який може бути присутнім у системі.

Якщо система не захищена, то будь-який зловмисник може порушити її або отримати авторизований доступ до цієї системи. Ризик безпеки, як правило, є випадковою помилкою, що виникає під час розробки та впровадження програмного забезпечення. Наприклад, помилки конфігурації, помилки оформлення, помилки програмного забезпечення тощо.

Чому потрібне тестування на проникнення? Тестування на проникнення зазвичай оцінює здатність системи захищати свої мережі, програми, кінцеві точки та користувачів від зовнішніх або внутрішніх загроз. Воно також намагається захистити засоби контролю безпеки і забезпечує лише авторизований доступ.

Тестування на проникнення має важливе значення, оскільки:

• ідентифікує середовище моделювання, тобто, як зловмисник може атакувати систему через атаку білого капелюха;

• допомагає знайти слабкі зони, де зловмисник може атакувати, щоб отримати доступ до даних і можливостей комп'ютера;

• підтримує запобігання атаці чорного капелюха і захищає вихідні дані;

• оцінює масштаби нападу на потенційний бізнес;

• надає докази того, чому важливо збільшити інвестиції в аспект безпеки технології.

Коли виконувати тестування на проникнення? Тестування на проникнення є важливою функцією, яку необхідно регулярно виконувати для забезпечення функціонування системи. На додаток до цього, вона повинна виконуватися кожного разу, коли:

• система безпеки виявляє нові загрози з боку нападників;

• ви додаєте нову мережеву інфраструктуру;

• ви оновлюєте систему або встановлюєте нове програмне забезпечення;

• ви переміщуєте свій офіс;

• ви встановлюєте нову програму / політику кінцевого користувача.

Чим корисний тест на проникнення? Тестування на проникнення дає такі переваги:

• Покращення системи управління - надає детальну інформацію про загрози безпеці. На додаток до цього, воно також класифікує ступінь вразливості і пропонує вам, який з них є більш вразливим і який менше. Таким чином, ви можете легко і точно керувати своєю системою безпеки, відповідно розподіляючи ресурси безпеки.

• Уникайте штрафів - тестування на проникнення змінює основні види діяльності вашої організації та відповідає системі аудиту. Таким чином, тестування на проникнення захищає вас від накладання штрафів.

• Захист від фінансової шкоди - просте порушення системи безпеки може завдати мільйонів збитків. Тестування на проникнення може захистити вашу організацію від таких збитків.

• Захист клієнта - порушення навіть даних одного клієнта може призвести до великих фінансових збитків, а також до пошкодження репутації. Воно захищає організації, які мають справу з клієнтами і зберігають їхні дані незмінними.

Тестування на проникнення - це комбінація методів, що розглядає різні питання систем і тестів, аналізує і дає рішення. Воно засноване на структурованій процедурі, яка здійснює покрокове тестування на проникнення.

Хто такі етичні хакери? Етичні хакери є комп'ютерними фахівцями, яким законно дозволено зламати комп'ютерну систему з метою захисту від злочинних хакерів. Етичний хакер виявляє вразливі місця і ризики системи і пропонує, як їх усунути.

Хто такі кримінальні хакери? Кримінальні хакери - це фахівці з комп'ютерного програмування, які зламують інші системи з метою крадіжки даних, крадіжки грошей, знецінення інших ресурсів, знищення даних, шантажування когось і т.д.

Що можуть зробити кримінальні хакери? Після того, як система зламана, злочинний хакер може зробити що-завгодно з цією системою.

Які навички повинні мати етичні хакери? Експертні етичні хакери мають наступні навички, щоб зламати систему етично:

• вони повинні бути надійними;

• незалежно від ризиків і вразливостей, які вони виявляють під час тестування системи, вони повинні зберігати їх у конфіденційності;

• клієнти надають конфіденційну інформацію про свою системну інфраструктуру, таку як IP-адреса, пароль і т.д. Етичні хакери повинні зберігати цю інформацію конфіденційно;

• етичні хакери повинні мати належні знання з комп'ютерного програмування, мереж і апаратних засобів;

• вони повинні мати хороші аналітичні навички для аналізу ситуації та заздалегідь передбачати ризики;

• вони повинні мати навички управління разом з терпінням, оскільки тестування на проникнення може зайняти один день, один тиждень або навіть більше.

Що роблять етичні хакери? Етичні хакери, виконуючи тестування на проникнення, в основному намагаються знайти відповіді на наступні питання:

• які слабкі сторони може використати злочинний хакер?

• що може злочинний хакер побачити на цільових системах?

• що може зробити злочинний хакер з наявною конфіденційною інформацією?

Більше того, етичний хакер зобов’язаний адекватно вирішувати вразливості та ризики, які він виявив у цільовій системі (системах). Йому потрібно пояснити і запропонувати процедури уникнення. Нарешті, підготувати заключний звіт про всі свої етичні дії, які він зробив і спостерігав під час проведення тестування на проникнення.

Типи хакерів. Хакери зазвичай поділяються на три категорії.

Чорні капелюхи (хакери). "Хакер з чорним капелюхом" - це людина, яка має спеціалізоване комп’ютерне програмне та апаратне забезпечення, і його мета полягає в тому, щоб порушити або обійти інтернет-безпеку когось іншого. Чорні капелюхи також популярні, як крекери або хакери темної сторони.

Білі капелюхи (етичні хакери). Термін «хакери в білому капелюсі» відноситься до етичного хакера, який є експертом з комп'ютерної безпеки, спеціалізується на тестуванні на проникнення та інших пов'язаних з ним методологіях тестування. Його головна роль полягає в забезпеченні безпеки інформаційної системи організації.

Сірі хакери. Термін "сірий хакер" відноситься до комп'ютерного хакера, який зламує комп'ютерну систему безпеки, чиї етичні стандарти знаходяться десь між чисто етичними і виключно шкідливими.

Тестування на проникнення дуже тісно пов'язане з етичним хакером, тому ці два терміни часто використовуються як взаємозамінні. Однак існує тонка лінія різниці між цими двома термінами. Розглянемо деякі основні поняття та фундаментальні відмінності між тестуванням на проникнення та етичним хакером.

Тестування на проникнення. Тестування на проникнення є специфічним терміном і зосереджується лише на виявленні вразливостей, ризиків і цільового середовища з метою забезпечення та прийняття контролю над системою. Іншими словами, тестування на проникнення відповідає

оборонним системам відповідної організації, що складаються з усіх комп'ютерних систем та її інфраструктури.

Етичний хакер. З іншого боку, етичний хакер є загальним терміном, який охоплює всі методи злому і інші пов'язані з ними методи комп'ютерної атаки. Таким чином, разом з виявленням недоліків і вразливостей безпеки, а також забезпеченням безпеки цільової системи, вона виходить за межі злому системи, але з дозволу на захист безпеки для майбутніх цілей. Отже, ми можемо сказати, що це узагальнюючий термін і тестування на проникнення є однією з особливостей етичного хакера.

Основні відмінності між тестуванням на проникнення та етичним хакером, наведеним у таблиці 1.1.

Таблиця 1.1 – Відмінності між тестуванням на проникнення та етичним хакером

Тестуванням на проникнення (Penetration Testing)	Етичний хакер (Ethical Hacking)
Вузький термін зосереджується на тестуванні на проникнення лише для забезпечення безпеки системи.	Комплексний термін і тестування на проникнення є однією з його особливостей.
По суті, тестер повинен мати всебічне знання, тільки про конкретну область, для якої він проводить тестування.	Етичний хакер повинен мати всебічні знання з програмного та апаратного забезпечення.
Тестер не обов'язково повинен бути хорошим автором доповіді.	Етичний хакер по суті повинен бути експертом з написання звітів.
Будь-який тестер з деякими знаннями тестування на проникнення може виконати тест на проникнення.	Він повинна бути фахівцем-експертом у цьому предметі, який має обов'язкову сертифікацію етичних хакерів, щоб бути ефективним.
Діловодство менше в порівнянні з етичним хакерством.	Потрібні детальні паперові роботи, включаючи юридичну угоду тощо.

Тестуванням на проникнення (Penetration Testing)	Етичний хакер (Ethical Hacking)
Для виконання цього типу тестування потрібно менше часу.	Етичне хакерство включає багато часу та зусиль у порівнянні з тестуванням на проникнення.
Як правило, доступність цілих комп'ютерних систем та її інфраструктури не потрібне. Доступність потрібна тільки для тієї частини, для якої тестувальник виконує ручне тестування.	Відповідно до ситуації, вона зазвичай вимагає цілого спектру доступності всіх комп'ютерних систем і його інфраструктури.

Оскільки техніки проникнення використовуються для захисту від загроз, потенційні зловмисники також швидко стають все більш і більш складними і знаходять нові слабкі місця в поточних додатках. Таким чином, певний тип тестування на проникнення недостатній для захисту вашої безпеки перевірених систем.

В деяких випадках виявляється нова лазівка у сфері безпеки, і успішний напад відбувся відразу після тестування на проникнення. Однак це не означає, що тестування на проникнення марне. Це тільки означає, що, це правда, що при ретельному тестуванні на проникнення, немає ніякої гарантії, що успішна атака не відбудеться, але, безумовно, тест значно зменшить можливість успішної атаки.

Через швидкі темпи розвитку в області інформаційних технологій, історія успіху тестування на проникнення є порівняно короткочасною. Оскільки потрібно більше захисту для систем, частіше, ніж потрібно, провести тестування на проникнення, щоб зменшити можливість успішної атаки до рівня, який оцінюється компанією.

Розглянемо основні обмеження тестування на проникнення.

Обмеження часу - як ми знаємо, тестування на проникнення не завжди визначене в часі, тим не менше, експерти тестування на проникнення виділили

фіксований час для кожного тесту. З іншого боку, зловмисники не мають часу, вони планують його через тиждень, місяць або навіть роки.

Обмеження сфери застосування - багато організацій не перевіряють все, через свої власні обмеження, включаючи обмеження ресурсів, обмеження безпеки, бюджетні обмеження тощо. Крім того, тестер має обмежену сферу застосування, і він повинен залишити багато частин систем, які можуть бути набагато вразливішим, що може бути ідеальною нішею для зловмисника.

Обмеження доступу - частіше тестери мають обмежений доступ до цільового середовища. Наприклад, якщо компанія здійснила тест на проникнення проти своїх систем DMZ з усієї мережі, але що робити, якщо зловмисники атакують через звичайний інтернет-шлюз.

Обмеження методів - існує ймовірність того, що цільова система може вийти з ладу під час тесту на проникнення, тому деякі з методів атаки, ймовірно, будуть виключені з таблиці для професійного тестера на проникнення. Наприклад, створення потоку відмови в обслуговуванні для відхилення адміністратора системи або мережі від іншого методу атаки, як правило, ідеальна тактика для зловмисних хакерів, але вона, ймовірно, виходить за межі правил залучення більшості професійних тестерів на проникнення.

Обмеження навичок тестерів на проникнення - як правило, професійні тестери на проникнення обмежені, оскільки вони мають обмежені навички незалежно від їхнього досвіду та навиків. Більшість з них орієнтовані на певну технологію і мають рідкісні знання інших галузей.

Обмеження відомих зламів - багато хто з тестерів знають лише ті звичаї, які є публічними. Фактично, їхня образна сила не так розвинена, як нападників. Зловмисники зазвичай думають далеко за межі тестувальників і виявляють недолік атаки.

Обмеження до експерименту - більшість тестерів обмежені часом і дотримуються вказівок, які вже дані їм організацією або наставниками. Вони не намагаються зробити щось нове. Вони не замислюються над даними

інструкціями. З іншого боку, зловмисники можуть вільно думати, експериментувати і створювати нові шляхи атаки.

Більше того, тестування на проникнення не може ні замінити рутинних тестів на ІТ-безпеку, ані замінити загальну політику безпеки, а тестування на проникнення доповнює встановлені процедури перевірки і виявляє нові загрози.

Зусилля на тестування на проникнення - наскільки б вони не були ретельними - не завжди можуть забезпечити вичерпне виявлення кожного випадку, коли ефективність контролю безпеки є недостатньою. Ідентифікація вразливості або ризику між сценаріями в одній області програми може не визначити всі випадки цієї вразливості, наявні в програмі.

2. Види тестування на проникнення

Розглянемо різні типи тестування на проникнення (Penetration Testing):

• тестування на проникнення – чорний ящик;

• тестування проникнення – білий ящик;

• тестування на проникнення сірий ящик.

Для кращого розуміння детально розглянемо кожен з вказаних типів.

Тестування на проникнення - чорний ящик. У тестуванні на проникнення - чорний ящик тестер не має уявлення про системи, які він збирається перевірити. Він зацікавлений зібрати інформацію про цільову мережу або систему. Наприклад, у цьому тестуванні тестер знає лише, який повинен бути очікуваний результат, і він не знає, як приходять результати. Він не розглядає ніяких програмних кодів.

Переваги тестування на проникнення - чорний ящик.

• Тестер не обов’язково повинен бути експертом, оскільки він не вимагає конкретних знань мови програмування.

• Тестер перевіряє протиріччя в реальній системі та специфікаціях.

• Тест, як правило, проводиться з точки зору користувача, а не дизайнера.

Недоліки тестування проникнення чорного ящика:

• Особливо важко розробити такі типи тестів.

• Можливо, конструктор системи вже провів тест.

• Не проводити все тестування.

Тестування на проникнення - білий ящик. Це комплексне тестування, оскільки тестувальникові було надано цілий спектр інформації про системи та / або мережі, такі як схема, вихідний код, деталі операційної системи, IP-адреса тощо. Як правило, це розглядається, як симуляція атаки з боку внутрішнього джерела. Він також відомий як структурний ящик, прозоре вікно або тестування з відкритою коробкою.

Тестування на проникнення - білий ящик, перевіряє код і проводить тестування потоку даних, тестування шляхів, тестування циклів тощо.

Переваги тестування на проникнення білий ящик.

• Забезпечує виконання всіх незалежних тестів модуля.

• Гарантує, що всі логічні рішення перевірені разом з їх істинним і помилковим значенням.

• Виявляє друкарські помилки та перевіряє синтаксис.

• Знаходить помилки, які можуть виникнути внаслідок різниці між логічним потоком програми та фактичним виконанням.

Тестування на проникнення – сірий ящик.

У цьому типі тестування тестер зазвичай надає часткову або обмежену інформацію про внутрішні деталі програм системи. Його можна розглядати як атаку зовнішнього хакера, який отримав незаконний доступ до документів мережевої інфраструктури організації.

Переваги тестування на проникнення сірий ящик.

• Оскільки тестер не вимагає доступу до вихідного коду, він не є нав’язливим та неупередженим.

• Оскільки існує чітка різниця між розробником і тестером, тому існує найменший ризик особистого конфлікту.

• Вам не потрібно надавати внутрішню інформацію про функції програми та інші операції.

Області тестування на проникнення. Тестування на проникнення зазвичай здійснюється в наступних трьох областях:

• **Тестування на проникнення мережі** – у цьому тестуванні необхідно перевірити фізичну структуру системи для виявлення вразливості та ризику, що забезпечує безпеку в мережі. У мережевому середовищі тестер ідентифікує недоліки безпеки в розробці, реалізації або роботі мережі відповідної компанії / організації. Пристроями, які тестуються, можуть бути комп'ютери, модеми або навіть пристрої віддаленого доступу, тощо.

• **Тестування на проникнення додатків** - під час цього тестування необхідно перевірити логічну структуру системи. Це симуляція атаки, розроблена з метою виявлення ефективності контролю безпеки програми

шляхом виявлення вразливості та ризику. Брандмауер та інші системи моніторингу використовуються для захисту системи безпеки, але іноді він потребує цілеспрямованого тестування, особливо коли трафіку дозволяється проходити через брандмауер.

• **Відповідь або робочий процес системи** - це третя область, яку необхідно перевірити. Соціальна інженерія збирає інформацію про взаємодію людей для отримання інформації про організацію та її комп'ютери. Доцільно перевірити здатність відповідної організації запобігти несанкціонованому доступу до її інформаційних систем. Крім того, цей тест призначений виключно для робочого процесу організації / компанії.

З цією ж метою проводяться як **ручне тестування на проникнення, так і автоматичне тестування на проникнення**. Єдина різниця між ними полягає в тому, як вони проводяться. Як випливає з назви, ручне тестування на проникнення здійснюється людьми (фахівцями цього напряму), а автоматичне тестування на проникнення здійснюється самою машиною.

Що таке ручне тестування на проникнення? Ручне тестування на проникнення - це тестування, яке здійснюють люди. У таких видах тестування вразливості і ризик машини перевіряється експертом-інженером.

Як правило, інженери з тестування виконують наступні дії (рисунок 2.1).

• **Збір даних.** Збір даних відіграє ключову роль для тестування. Можна або зібрати дані вручну, або скористатися послугами інструменту (наприклад, технікою аналізу вихідних кодів веб-сторінок і т.д.), вільно доступними в Інтернеті. Ці інструменти допомагають збирати інформацію, наприклад, назви таблиць, версії БД, бази даних, програмне забезпечення, апаратні засоби або навіть різні плагіни третіх сторін тощо.

• **Оцінка вразливості.** Як тільки дані збираються, це допомагає тестувальникам виявити слабкість безпеки та вжити відповідних заходів.

• **Фактична експлуатація.** Це типовий метод, який експерт-тестер використовує для запуску атаки на цільову систему, а також зменшує ризик атаки.

• **Підготовка звіту.** Після проникнення тестер готує заключний звіт, який описує все про систему. Нарешті, звіт аналізується, щоб вжити коригувальних заходів для захисту цільової системи.

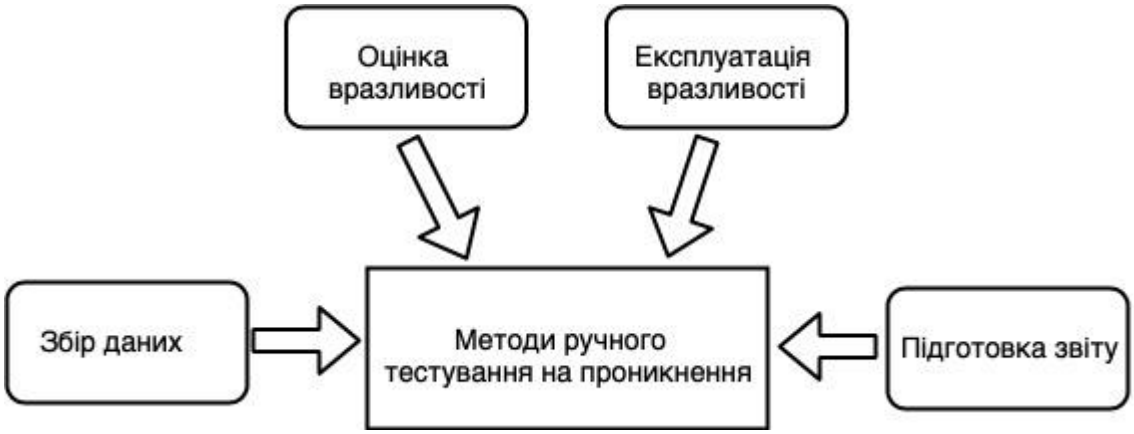

Рисунок 2.1 – Дії інженера з тестування на проникнення

Типи ручного тестування на проникнення. Ручне тестування на проникнення зазвичай класифікується за двома наступними способами.

• **Цілеспрямоване ручне тестування на проникнення** - це набагато більш цілеспрямований метод, який перевіряє конкретні вразливості та ризики. Автоматичне тестування на проникнення не може виконати це тестування; це роблять лише фахівці-люди, які вивчають специфічні вразливості додатків в межах цих доменів.

• **Комплексне ручне тестування на проникнення** - це тестування цілих систем, пов'язаних одна з одної, для виявлення всіх видів ризику та вразливостей. Проте функція цього тестування є більш ситуативною, наприклад, вивчення того, чи можуть кілька несправностей з нижчим ризиком принести більш вразливий сценарій атаки, тощо.

Що таке автоматизоване тестування на проникнення? Автоматизоване тестування на проникнення набагато швидше, ефективніше, простіше та надійніше, що автоматично перевіряє на наявність вразливістей та ризику машини. Ця технологія не вимагає жодного експертного інженера, а може бути запущена будь-якою особою, яка має найменші знання в цій галузі.

Інструментами для автоматизованого тестування на проникнення є Nessus, Metasploit, OpenVAs, backtract (серія 5), і т.д.

У таблиці нижче наведено принципову відмінність між ручним та автоматичним тестуванням на проникнення.

Таблиця 2.1 – Порівняння ручного і автоматичного тестування на проникнення

Ручне тестування проникнення	Автоматичне тестування на проникнення
Для виконання цього тесту потрібно експерт-інженер.	Воно автоматизоване, так що навіть учень може виконати тест.
Для тестування потрібні різні інструменти.	Має вбудовані інструменти, що вимагають даних ззовні.
У цьому типі тестування результати можуть варіюватися від тесту до тесту.	Він має фіксований результат.
Цей тест вимагає запам'ятовувати тестером.	Це не так.
Він є вичерпним і затратним за часом.	Це більш ефективно і швидко.
Він має додаткові переваги, тобто якщо експерт робить тест на проникнення, то він може краще аналізувати, він може подумати, що може думати хакер і де він може атакувати. Таким чином, він може підвищити безпеку відповідно.	Н може аналізувати ситуацію.
Відповідно до вимог, експерт може запускати кілька тестів.	Не може.
Для критичного стану він більш надійний.	Це не так.

Комп’ютерні системи та мережі зазвичай складаються з великої кількості пристроїв, і більшість з них відіграють важливу роль у проведенні загальних робіт відповідної системи підприємства. Незначний недолік у будь-який момент часу і в будь-якій частині цих пристроїв може завдати великої шкоди бізнесу. Тому всі вони є вразливими до ризику і повинні бути забезпечені належним чином.

3. Класифікація та цілі проникнення

3.1 Стартові точки та канали доступу для тестів на проникнення

Типовими вихідними точками або точками атаки для тестування на проникнення є брандмауери, веб-сервери, доступ до RAS точки (наприклад, модеми, точки віддаленого обслуговування) та бездротові мережі. З огляду на їх функції, як шлюз між Інтернетом та мережею компанії, брандмауери є очевидними мішенями для спроби нападу та вихідні точки для тестів на проникнення. Веб-сервери мають високий потенціал ризику через свої різноманітні функції та вразливі ситуації. Інші сервери, що пропонують послуги, доступні зовні, такі як електронна пошта, FTP та DNS, повинні бути включені в тест, як і "звичайні" робочі станції.

3.1.1 Заходи безпеки IT

Тест на проникнення повинен перевірити логічні заходи безпеки IT, такі як паролі, так і фізичні заходи, такі як системи контролю доступу. Часто випробовуються лише логічні елементи керування, оскільки це, як правило, можна робити віддалено через мережу, що робить тести менш трудомісткими, і тому, що вважається, що ймовірність атак на логічні засоби управління IT набагато більша.

3.1.2 Тестування на проникнення, аудит безпеки IT, аудит IT

"Хакери" мають на меті отримати доступ до захищених даних або зловмисно порушити обробку даних. На відміну від тестування на проникнення, метою аудиту безпеки та аудиту IT є загальне вивчення інфраструктури IT на предмет її відповідності, ефективності, тощо. Вони не обов’язково спрямовані на виявлення вразливих точок. Наприклад, тест на проникнення не передбачає перевірки, чи в разі пошкодження обладнання певні дані можуть бути відновлені за допомогою регулярної резервної копії; він лише

перевіряє, чи можна отримати доступ до таких даних. Це також можна зробити під час аудиту безпеки або аудиту IT, але зазвичай є різні точки зору характерній для тестування на проникнення.

3.2 Цілі проникнення

Для успішного тесту на проникнення, який відповідає очікуванням клієнта, абсолютно необхідним є чітке визначення цілей. Якщо цілі неможливо досягти або її неможливо досягти ефективно, тестувальник повинен повідомити клієнта на етапі підготовки та рекомендувати альтернативні процедури, такі як аудит IT або консультаційні послуги з питань IT-безпеки.

Цілі клієнта, які можуть бути досягнуті тестуванням на проникнення, можна розділити на чотири категорії:

1. Підвищення безпеки технічних систем.
2. Виявлення вразливих місць.
3. Підтвердження безпеки IT зовнішньою стороною.
4. Підвищення безпеки організаційно-кадрової інфраструктури.

Таким чином, результат тесту на проникнення IT повинен бути не лише переліком існуючих вразливих місць; в ідеалі він також повинен запропонувати конкретні рішення для їх усунення.

Розглянуто чотири цілі категорій з прикладами.

3.2.1 Підвищення безпеки технічних систем

Більшість тестів на проникнення виконані з метою підвищення безпеки технічних систем. Тести обмежуються лише технічними системами, такими як брандмауер, маршрутизатори, веб-сервери тощо, при цьому організаційна та кадрова інфраструктура не піддаються явному тестуванні. Один із прикладів – проникнення перевірка, щоб чітко перевірити, чи можуть сторонні сторони отримувати доступ до систем в локальній мережі компанії через Інтернет.

Можливими результатами тестування є непотрібні порти відкритого брандмауера або вразливі версії Інтернет-додатків та операційних систем.

3.2.2 Визначення вразливих місць

На відміну від інших трьох цілей, ідентифікація є фактичною метою тесту. Наприклад, перед об'єднанням двох локальних мереж після об'єднання компанії, нову локальну мережу можна перевірити, чи можна проникнути в неї зовні. Якщо це можна зробити в тесті на проникнення, потрібно вжити заходів щоб забезпечити інтерфейс до злиття, або дві мережі взагалі не повинні поєднуватися.

3.2.3 Підтвердження IT-безпеки зовнішньою стороною

Тест на проникнення також може бути проведений для отримання підтвердження від незалежної третьої зовнішньої сторони. Важливо зауважити, що тест на проникнення лише відображає ситуацію в певний момент часу, і тому не може дати твердження про рівень безпеки, що є дійсними в майбутньому.

Тим не менш, регулярні тести на проникнення можуть бути придатні для демонстрації підвищеної безпеки даних клієнтів у веб-магазині чи іншому інтернет-додатку.

3.2.4 Підвищення безпеки організаційної та кадрової інфраструктури

Крім тестування технічної інфраструктури, тест на проникнення може також перевірити організаційну та кадрову інфраструктуру для моніторингу процедур ескалації, наприклад, із сферою застосування та / або агресивність тестів збільшується поетапно. Методи соціальної інженерії, такі як запитуючи паролі по телефону, можна використовувати для оцінки рівня загальної безпеки, обізнаність та ефективність політики безпеки та угод з користувачами. Обсяг таких тестів повинен бути визначений заздалегідь.

3.3 Межі тестування на проникнення

Оскільки методи, які використовуються потенційними зловмисниками, швидко стають все більш досконалими, і нові слабкі місця в сучасних додатках та IT-системах повідомляються майже щодня, один єдиний тест на проникнення не може дати твердження про рівень безпеки систем, які тестуються, що буде чинним у майбутньому. У крайніх випадках нова лазівка в безпеці може означати, що успішна атака може відбутися відразу після завершення тесту на проникнення.

Однак це жодним чином не означає, що тести на проникнення марні. Ретельне тестування на проникнення не є гарантією того, що успішного нападу не відбудеться, але воно істотно знижує ймовірність успішного нападу. Через швидкий темп розвитку IT, ефект тесту на проникнення є, проте, порівняно короткочасним. Чим більше система вимагає захисту, тим частіше слід проводити тестування на проникнення, щоб знизити ймовірність успішної атаки до рівня, прийнятного для компанії.

Тест на проникнення не може замінити звичайні тести безпеки IT, а також не замінить загальну політику безпеки, тощо. Наприклад, концепція авторизації або резервного копіювання даних може бути ефективно протестована та лише іншими способами. Тест на проникнення доповнює встановлені процедури огляду та подолання нових загроз.

3.4 Класифікація

Розглянемо, які критерії можуть бути використані для опису тесту на проникнення, або що відрізняє один тест на проникнення від іншого? Відмінні особливості, такі як ступінь тестуючих систем, обережність або агресивність тестування тощо, що характеризують конкретний тест на проникнення, повинні

бути адаптовані відповідно до мети випробування для забезпечення ефективного тестування з розрахунковим ризиком. На рисунку 3.1 показана класифікація можливих тестів на проникнення. Зліва - шість критеріїв для визначення тестування на проникнення, праворуч - різні значення для критеріїв, узагальнених на компактній діаграмі дерева.

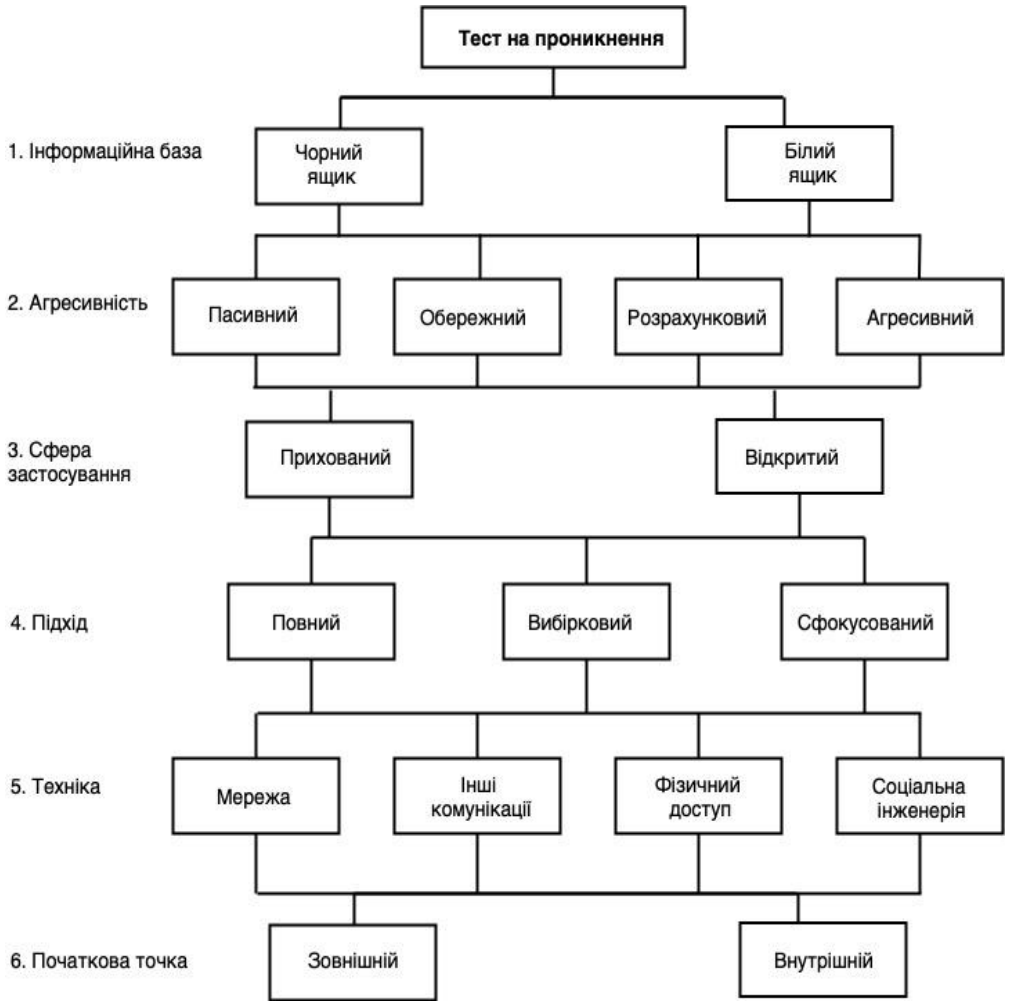

Рисунок 3.1 – Класифікація тестів на проникнення

Відповідний тест на проникнення, для досягнення цілей клієнта, повинен бути визначений на основі вищезазначених критеріїв. Слід зазначити, що не всі можливі комбінації є корисними тестами, хоча критерії в класифікації зберігалися максимально чітко. Агресивний тест, як правило, ідентифікується дуже швидко, тому не є ідеальним у поєднанні з прихованими методами. Аналогічно, явний тест на проникнення не підходить, наприклад, для

отримання конфіденційної інформації від заздалегідь попереджених працівників за допомогою методів соціальної інженерії.

Нижче розглянуто шість критеріїв та їх можливі значення:

1. Інформаційна база: Який початковий рівень знань тестера проникнення про цільову мережу чи об'єкт?

Принципова відмінність проводиться між тестуванням чорного ящика без будь-яких інсайдерських знань та тестуванням білого ящика, де тестер має інсайдерські знання:

1. Тест чорний ящик реально імітує атаку типового інтернет-хакера. Хакер повинен досліджувати необхідну інформацію в загальнодоступних базах даних або робити запити як сторонній чоловік.

2. Під час методу тестування білий ящик атака (колишнього) працівника або зовнішнього постачальника послуг з детальними знаннями в певних областях. Ступінь таких знань може варіюватися від обмежених, наприклад, як у працівника, який працював у компанії лише короткий час, до поглиблених системних знань, таких як зовнішній постачальник IT-послуг, який встановив системи, що стосуються безпеки.

2. Агресивність: наскільки агресивним є тестер на проникнення під час тестування? Для забезпечення достатньо тонкого розрізнення визначено чотири рівні агресивності:

- з найнижчим рівнем –об'єкти досліджуються лише пасивно, тобто будь-які виявлені вразливості не використовуються.

- другий рівень (обережно) – виявлені вразливості використовуються лише тоді, коли відомо, що система, яка тестується не дає результату, наприклад, використовуючи відомі паролі за замовчуванням або намагаючись отримати доступ до каталогів на веб-сервері.

- третій рівень (розрахунковий) - тестер також намагається використовувати вразливості, які можуть призвести до збоїв у роботі системи. Наприклад, це включає автоматичне випробування паролів та використання відомих переповнень буферу в точно визначених цільових системах. Перш ніж

робити такі кроки, тестер розглядає, наскільки ймовірними вони можуть бути успішними та наскільки серйозними будуть наслідки.

- Четвертий рівень (агресивний) - тестер намагається використовувати всі потенційні вразливості, наприклад переповнення буфера використовуються навіть у цільових системах, які не є чітко визначеними, або системи безпеки деактивуються шляхом навмисних атак з перевантаженням (відмова в обслуговуванні (DoS)). Тестер повинен мати на увазі, що крім систем, які тестуються, сусідні системи або компоненти мережі також можуть вийти з ладу внаслідок цих тестів.

3. Область застосування. Які системи підлягають тестуванню?

Коли вперше проводиться тестування на проникнення, доцільно провести повний тест, щоб переконатися, що в системах, які не пройшли перевірку, не пропускаються пробіли в безпеки.

Час необхідний для тесту на проникнення, як правило, безпосередньо пов'язаний із сферою досліджуваних систем. Ідентичні та майже ідентичні системи часто можуть бути досліджені в одному тесті, але як тільки з’являться різні конфігурації, з кожною системою потрібно буде розбиратися окремо:

✓ Якщо потрібно протестувати лише конкретну підмережу, систему чи послугу, для цілей цього дослідження тест на проникнення називають зосередженим. Цей тип тестування є доцільним після: наприклад, модифікація або розширення ландшафту системи. Такий тест, звичайно, може дати лише інформацію про тестовану систему; він не може надати загальна інформацію про IT-безпеку.

✓ Під час тесту з обмеженим проникненням досліджується обмежена кількість систем чи служб. Наприклад, всі системи в DMZ або системи, що містять функціональний блок, можуть бути протестовані.

✓ Повний тест охоплює всі наявні системи. Слід зазначити, що навіть у повному випробуванні певні системи, напр. аутсорсингові та зовнішньо розміщені системи, можливо, не зможуть бути випробувано.

4. Підхід: наскільки «видимою» є команда під час тестування?

Якщо, крім первинних систем безпеки, підлягають тестуванню вторинні системи (наприклад, IDS або організаційні чи кадрові структури (наприклад, процедури ескалації)), підхід до тестування повинен бути відповідно адаптований:

- ✓ Тестування на проникнення, що проводяться в системах вторинної безпеки та існуючих процедурах ескалації, повинні - принаймні на початку - бути прихованими, тобто на початковій стадії обстеження слід застосовувати лише методи, які не можна безпосередньо визначити як спроби нападу на систему.
- ✓ Якщо прихований підхід не може викликати реакцію, або випробування «білого ящика» проводиться у співпраці з особами, відповідальними за систему, явні методи, такі як сканування портів, що мають прямий зв'язок, можуть бути використані. Клієнтський персонал може бути включений до команди, яка проводить явний тест. Це особливо доцільно для висококритичних систем, оскільки, це означає, що тестери здатні швидше реагувати на несподівані проблеми.

5. Техніка. Які методи використовуються для тестування?

У звичайному тесті на проникнення системи атакуються лише через мережу. Крім того, інші типи фізичних атак та технічних засобів соціальної інженерії можуть використовуватися для нападу на системи.

Тест на проникнення на основі мережі - це нормальна процедура і імітує типову хакерську атаку. Більшість IT-мереж зараз використовують протокол TCP / IP, тому такі тести також називаються тестами на проникнення на основі IP.

Крім мереж TCP / IP, існують і інші комунікаційні мережі, які також можна використовувати для постановки атаки. До них належать телефонні та факсимільні мережі, бездротові мережі для мобільного зв'язку, наприклад заснований на IEEE 802.11 (b) і, в майбутньому, також технології Bluetooth.

В даний час такі системи безпеки, як брандмауери тощо, мають значне поширення, і конфігурації таких систем зазвичай забезпечують високий рівень

безпеки, що означає, що перемогти такі системи в результаті нападу надзвичайно важко, якщо не неможливо. Часто простіше і швидше отримати бажані або необхідні дані, обходячи ці системи під час прямої фізичної атаки. Фізичний напад може, наприклад, спричинити прямий доступ до даних на захищеній паролем робочій станції після отримання несанкціонованого доступу до будівлі та / або серверних кімнат.

Люди часто є найслабшою ланкою в ланцюжку безпеки, тому методи соціальної інженерії, які використовують неадекватні навички безпеки або недостатню обізнаність із безпекою, часто є успішними. Такі тестування доцільні після введення загальної політики безпеки, наприклад, для оцінки ступеня її впровадження та / або прийняття. Помилкові припущення щодо передбачуваної ефективності політики безпеки часто призводять до ризиків для безпеки, які, за умови точної оцінки ситуації, можуть бути пом’якшені шляхом вжиття додаткових заходів.

6. Початкова точка: звідки проводиться тест на проникнення?

Початкова точка тесту на проникнення, тобто точка, де тестер на проникнення з'єднує свій комп'ютер з мережею або звідки виникають спроби його нападу, може знаходитися як всередині, так і за межами мережі або будівлі клієнта.

Більшість хакерських атак проводиться через підключення мережі до Інтернету. Тому тест на проникнення ззовні здатний виявити та оцінити потенціал ризик такого нападу. Зазвичай брандмауер, системи в з'єднаннях DMZ та RAS досліджуються в таких тестах.

Під час тесту на проникнення зсередини тестеру зазвичай не доводиться долати міжмережеві стіни чи засоби входу для доступу до внутрішніх мереж. Тому тест зсередини може оцінити наслідки помилки в конфігурації брандмауера, успішної атаки на брандмауер або атаки осіб, які мають доступ до внутрішньої мережі.

4. Юридичні питання тестування на проникнення

Юридичні питання, які необхідно враховувати при проведенні випробувань на проникнення, можна розділити на три типи:

- юридичні питання, які можуть спонукати або мотивувати бізнес чи державний орган на проведення тестування на проникнення;

- правові норми та принципи, яких тестер повинен дотримуватися під час проведення тестів на проникнення, і які слід уточнити з клієнтом перед початком тестування;

- правові аспекти, що складають основу договору між клієнтом та тестером на проникненням.

4.1 Юридичні причини тестування на проникнення

Хоча немає законів, які вимагають від компанії чи державних органів проводити тестування на проникнення, однак є обов'язкові законодавчі положення, що стосуються:

- безпечного поводження з даними, що стосуються податкового та комерційного законодавства;

- обробка персональних даних;

- створення та організація системи внутрішнього контролю.

З метою захисту даних компанії часто вживають заходів для гарантування доступності, конфіденційності та цілісності даних або забезпечення доступу лише для уповноважених осіб.

Ці заходи включають поняття безпеки, концепції авторизації та системи брандмауера. Однак створення таких видів систем безпеки не є гарантією дотримання законних вимог. Швидше, відповідність системи правовим

вимогам та положенням повинно перевірятися для кожного конкретного випадку.

Тестування на проникнення є хорошим засобом перевірки ефективності таких заходів у певних сферах.

Найважливіші правові норми, яких слід дотримуватися при створенні та підтримці систем безпеки та дозволу, представлені нижче в контексті використання при здійсненні тестів на проникнення.

4.2 Правові рамки тестування на проникнення

Якщо під час тесту на проникнення тестер виконує дії без згоди клієнта, це може суперечити чинному законодавству.

Кримінальне право. Тестер на проникнення, як правило, не буде вчиняти кримінального злочину, оскільки він не діє з необхідними намірами - такими як незаконне збагачення. Більше того, такі дії вторгнення, зміст та обсяг яких узгоджені з клієнтом, виправдані та схваленні останнім

Точне визначення сфери дії клієнта та випробувача є визначальним. Після того, як буде визначено фактичну сферу дії, корисно отримати схвалення у вигляді окремої заяви клієнтом до початку тестування.

4.3 Важливі умови договору між тестером на проникнення та клієнтом

4.3.1 Який тип договору є контрактом на тестування на проникнення?

Тест на проникнення, як правило, є послугою за винагороду. На відміну від договору на виробництво та надання послуг, узгоджена послуга належить лише до виконання, але не має особливих економічних результатів.

Загальні положення та умови. Якщо тестер має загальні умови, вони повинні бути включені в договір. Клієнт повинен був бути проінформований про них та погодитися з їхньою чинністю.

4.3.2 Предмет договору

Окрім мети тесту на проникнення, сторони повинні визначити в договорі характер та сферу застосування інструментів та прийомів.

У контракті повинно бути чітко зазначено мета, яку переслідує організація, яка доручає виконати перевірку на проникнення.

Найпоширенішими цілями є:

- підвищення безпеки технічних систем;

- виявлення вразливості, як критерію для прийняття рішень (наприклад, щодо інвестицій або придатності продуктів),

- отримання сертифікації / підтвердження від зовнішньої третьої сторони;

- підвищення безпеки організаційно-кадрової інфраструктури.

Детальний огляд можливих цілей наведено в розділі «Цілі проникнення».

Природа тестів на проникнення. Слід звернутись до типу тесту на проникнення, який необхідно виконати. Можуть бути використані наступні критерії класифікації:

- інформаційна база (тест "чорний ящик " або "білий");

- агресивність (пасивна / скануюча до агресивної);

- сфера застосування (повна, обмежена або сфокусована);

- підхід (прихований або явний);

- техніка (мережеві, інші комунікації, фізичний доступ, соціальна інженерія);

- початкова точка (зовні або зсередини).

Створюючи такі технічні характеристики, тестер дозволяє уникнути зайвих непорозумінь та ризиків з самого початку та гарантує, що тест на проникнення підходить до потреб клієнта. Крім того, визначено сферу схвалення клієнта, яку слід отримати в якості запобіжного заходу з точки зору кримінального права.

Методи, які слід використовувати та виключати.

Окремі методи, які використовувані в тесті на проникнення, повинні бути описані більш докладно, де це можливо і доцільно. Зокрема, слід описати будь-які методи соціальної інженерії та активні тести контролю доступу, які слід використовувати.

Оскільки методи соціальної інженерії за своєю природою є проблематичними та, можливо, неетичними, доцільно визначити для них чіткі рамки (наприклад, уникати підбурювання працівників до неетичної поведінки). Активний тест контролю доступу намагається обійти заходи фізичної безпеки, що може розглядатися як злам. У цьому відношенні також необхідне пояснення обставин, за яких має проводитись тест.

Важливо також виключити атакуючі прийоми, які явно не застосовуються. Такі прийоми також повинні бути визначені в договорі із зазначенням причин їх виключення.

4.3.3 Клієнт

Зокрема, щодо затвердження, необхідного для вживання потенційно згубних заходів під час тестування, важливо, щоб договір був підписаний законним представником клієнта. Це означає, що лише особа, уповноважена представляти його, наприклад для торгової компанії генеральний менеджер, уповноважений підписант або інша особа з аналогічним індивідуальним дозволом, наприклад керівник відділу IT, може доручити виконання тесту на проникнення.

Перш ніж проводити тест на проникнення, тестувальник на проникнення повинен вимагати відповідних доказів, щоб переконатися, що представник клієнта уповноважений його представляти.

4.3.4 Тестер

Якщо тестувальник має намір взяти на себе частину випробування, у контракт має бути включено "попереднє положення". Однак, оскільки зачіпаються сфери, важливі для безпеки, клієнт зазвичай не погоджується на це

такого роду вступне застереження. Тому корисно називати субпідрядника під час укладення договору. Це гарантує, що лише ці особи мають право виконувати тестові процедури.

Призначення виконавців-учасниць особливо важливо, коли плануються нетрадиційні процедури тестування, такі як соціальна інженерія або обхід заходів фізичного забезпечення, оскільки це захищає обидві сторони та допомагає уникнути непорозумінь.

4.3.5 Письмова форма

Усі умови договору повинні бути узгоджені в письмовій формі. Крім того, сторони повинні прямо погодитися з вимогою письмово, яка повинна охоплювати всі допоміжні угоди.

4.3.6 Зобов'язання клієнта

В інтересах тестувальника на проникнення в контракті повинно бути встановлено юридичний обов'язок клієнта співпрацювати якомога детальніше. Слід враховувати такі елементи:

- ✓ Забезпечення інформації залежно від природи тесту на проникнення.

Залежно від характеру тесту на проникнення, тестер може залежати від обширної інформації від клієнта. Наприклад, для тестування білого ящика потрібна інформація про імена DNS, IP-адреси, політики безпеки, конфігурації системи, правила брандмауера, процедури ескалації тощо. Тестувальник на проникнення повинен надати клієнтові перелік необхідної інформації перед укладенням договору та домовитись про те, що вся необхідна інформація буде надана вчасно.

- ✓ Інформація від потенційно постраждалих третіх осіб.

Під час звичайного трафіку даних у загальнодоступних мережах тест на проникнення також використовує сторонні системи (наприклад, сервер зв'язку провайдера, веб-сервер основного комп'ютера). Оскільки неможливо

виключити погіршення працездатності цих систем, радимо надати попереднє повідомлення про тести на проникнення будь-якій третині особи, які можуть постраждати. Ці інформаційні обов'язки можуть бути делеговані клієнтові, оскільки він краще може оцінити, на які треті сторони можуть вплинути тести.

- ✓ Захисні заходи щодо непередбачуваної несправності системи.

Оскільки не можна повністю виключити, що системи під час тестування погіршуються таким чином, що дані втрачаються, в інтересах клієнта створюється резервне копіювання даних з високим рівнем ризику та відповідних систем, коли це вже не було зроблено під час виконання загальноприйнятих принципів комп'ютерних систем обліку (GoBS).

Резервне копіювання даних гарантує можливість відновлення даних у разі необхідності та зменшення потенційно несприятливих наслідків втрати даних.

4.3.7 Обов'язки тестера

В інтересах клієнта тестувальнику повинні бути призначені наступні зобов'язання:

- ✓ Секретність.

У ході тесту на проникнення тестувальник може отримати доступ до високочутливої інформації про вразливості в клієнтській мережі. Ця інформація не повинна надаватися третім особам, щоб звести ризик клієнта до мінімуму. Тому випробувач повинен бути зобов'язаний дотримуватися секретності стосовно інформація, що надається йому, а також інформація, яка йому стала відома під час тестування.

- ✓ Дотримання ліцензійних норм.

Тестер несе відповідальність за дотримання ліцензійних норм при використанні засобів комерційної безпеки. Оскільки роялті за використання інструментів безпеки зазвичай стягуються з клієнта, клієнту слід забезпечити чіткий розподіл цих зборів.

- ✓ Документування процедур і результатів тестування.

Характер та обсяг документації процедур тестування та результати повинні бути визначені у договорі. Тестувальник повинен бути зобов'язаний надати точну документацію про свої процедури випробувань. Це дозволяє, у разі пошкодження, простежти технікуку яку він використав. Крім того, сторони повинні погодитись із формою, у якій мають бути представлені результати (звіт, презентація, звіти та аналіз використовуваних засобів безпеки).

✓ Загальний обов’язок належної обережності. Тестер на проникнення повинен проявляти належну обережність під час виконання процедур тестування. Наприклад, було б недбало, якби тестувальник на проникнення "випадково" атакував систему невключеної третьої сторони, оскільки він переплутав ім'я DNS.

Таким чином, в контракті повинно бути передбачено, що тестувальник на проникнення повинен дотримуватися належної уваги при здійсненні своєї діяльності стосовно можливої шкоди, яку він може завдати.

4.3.8 Виконання договору

В договорі повинні бути вказані дата початку та закінчення. Тест на проникнення повинен проводитися протягом цього періоду часу. Це забезпечує те, що спроби проникнення, які трапляються після цього періоду, можуть бути чітко визначені, як реальні напади третіх сторін, таким чином, уникнути будь-яких непорозумінь. Слід зазначити, що випробувач на проникнення має право виконувати свої випробування лише в погоджений період часу.

4.3.9 Спеціальне право на припинення

Під час тестування на проникнення можуть виникнути обставини, які можуть перешкоджати процесу тестування (наприклад, аварія системи яка потребує великої ручної роботи з налагодження). Особливе право на розірвання може бути включено до договору для таких випадків. Крім того, діють загальні правила розірвання договорів на послуги.

4.3.10 Обмеження відповідальності

Коли сторони домовляються про обмеження відповідальності, вони повинні зауважити, що обмеження відповідальності може бути законодавчо погоджене лише в межах Загальних положень та умов торгівлі.

Обмеження відповідальності тестувальника за грубу недбалість і наміри та відмову від відповідальності за шкоду, спричинену дефектами чи непрямими пошкодженнями, як правило, можливі, доки вони існують не є винним порушенням значного договірного зобов'язання.

5. Загальні вимоги до тестування на проникнення

Окрім правової бази, існує низка загальних вимог, що стосуються організації, персоналу та технічних питання для проведення тестування на проникнення.

5.1 Організаційні вимоги

Наступні організаційні вимоги повинні бути роз'яснені з клієнтом напередодні планової перевірки на проникнення.

На кого, окрім клієнта, прямо чи опосередковано впливатиме тест на проникнення?

На додаток до системи клієнта, системи постачальника, які навіть можуть бути фізично розташовані в приміщеннях клієнта під час управління провайдером, часто впливають на тест на проникнення. Щоб уникнути непорозумінь, тому постачальника слід повідомити про запланований тест на проникнення. Деякі етапи тестування, наприклад DoS тести, можливо, через високу пропускну здатність вимоги або нестандартні пакети даних, також призводять до перебоїв у мережевих компонентах постачальників, і тому слід попередньо детально обговорити їх з провайдерами.

Якщо деякі функції були передані в аутсорсинг (наприклад, веб-хостинг сервера WWW), залучені системи слід виключити з тесту на проникнення. Якщо ці системи включені в тест на проникнення, необхідно отримати письмове схвалення для цього оператора системи або оператора аутсорсингу.

Тестувальник повинен зазначити, що він відповідає за безпеку IT-систем, включаючи аутсорсингові системи, наприклад. за цілісність даних бухгалтерського обліку, і що ця відповідальність не може бути простою передано постачальнику послуг аутсорсингу.

Чи належним чином було враховано ризики відповідальності? Тестер на проникнення повинен мати страхування відповідальності з достатнім покриттям, щоб убезпечити себе від можливих вимог про відшкодування

збитків третім особам. Хоча слід передбачити, щоб мінімізувати потенційні ризики для сторонніх систем перед тестуванням, збої в сторонніх системах не можуть бути повністю виключені.

Що потрібно враховувати при оцінці часу тестування? Тест на проникнення може погіршити функціональність виробничих систем. Оскільки мета тесту - виявити вразливості, але не загрожуючи впорядкованим операціям, фактичні атаки повинні мати місце за часом, погодженим обома сторонами. Це слід врахувати на етапі планування, напередодні тестування на проникнення.

Тести на проникнення часто проводяться протягом декількох днів. Слід вибирати строки, коли не виконується ні критична обробка, ні великі обсяги онлайн-замовлень, наприклад, не обробляються в цільовій системі. Термін може бути показаний на час коли атаки проводяться лише у тестах білого ящика.

З підходами до чорного ящика інформація про рівень критичності та використання системи в певний час зазвичай недоступна.

Що потрібно зробити у разі відмови системи чи інших аварійних ситуацій?

У випадку виходу з ладу системи, незважаючи на те, що дотримувались необхідних заходів під час тестування, або у випадку іншої надзвичайної ситуації, наприклад серйозні порушення системи, необхідно визначити заходи надзвичайних ситуацій.

У договорі має бути, принаймні, вказано, кого повідомити, і коли у випадку підозри чи виявлення несправності чи зриву. Крім того, слід визначити види несправностей, про які потрібно повідомити.

Можна виділити наступні "збої":

- повна відмова системи;
- частковий збій певних підсистем;
- неправильні відповіді від системи;
- значне збільшення тривалості часу реакції системи;

- контрзаходи, що вживаються у відповідь на приховану перевірку проникнення;

- напади третіх сторін на систему.

На кого з працівників клієнта впливає тест на проникнення?

Кількість працівників, які постраждали від тестування, залежатиме від обсягу та характеру тесту. Тест на проникнення, обмежений тестовою системою, зможе впливати лише на адміністраторів та користувачів системи тестування. Як і для користувачів системи, тест, який також вивчає виробничі системи, може, в крайньому випадку, також вплинути на всіх працівників, які певним чином залежать від результатів системи, які випробовуються, або перешкоджають їх роботі. Якщо в тесті на проникнення слід використовувати методи соціальної інженерії, сторони повинні домовитись про працівників, на які можуть бути націлені тестування, наскільки це допустимо.

Скільки часу та витрат потребує тест на проникнення для клієнта?

Клієнт повинен очікувати можливого пошкодження його IT-систем у результаті тесту на проникнення, що може спричинити за собою порушення в операціях. Тому необхідно зробити кроки перед тестом на проникнення, щоб звести наслідки можливих збоїв до мінімуму.

Вони можуть включати, наприклад, призначення працівника для моніторингу тесту на проникнення з точки зору клієнта, який може зупинити тестування, якщо це необхідно. Клієнт також повинен розглянути можливість створення додаткових резервних копій перед тестом на проникнення.

Необхідно також прийняти план дій у надзвичайних ситуаціях (якщо такого вже немає) та процедури ескалації, які сприяють як впорядкованому ходу дій, так і впровадженню відповідних контрзаходів.

Якщо для тестування на проникнення обрано підхід «білого ящика», додатковій інформації та професійним контактним партнерам слід забезпечити доступність тестера на проникнення.

Скільки часу та сил потребуватиме тест на проникнення?

Для того, щоб можна було оцінити, чи може постачальник послуг адекватно провести тест на проникнення, і якщо так, то приблизні витрати, які можуть бути з цим пов'язані, час і зусилля, необхідні для проведення тестування на проникнення слід спочатку оцінити кількісно. Слід враховувати такі аспекти, як мету та обсяг тесту на проникнення.

Тестер та клієнт спільно визначають характер тестування та процедури випробувань, які слід виконати відповідно до мети тесту на проникнення.

Залежно від характеру та обсягу тесту на проникнення, можливо визначити ресурси, які тестувальник на проникнення повинен використовувати (апаратне забезпечення, програмне забезпечення, відповідні працівники) до фактичного початку тестування.

Розмір інфраструктури, що підлягає тестуванню.

Розмір інфраструктури часто виражається в кількості IP-адрес, які підлягають тестуванню. Як правило, неможливо вказати час, який тестеру потрібно буде витратити на тестування на проникнення окремої системи, оскільки це залежить від моделі та конфігурації системи, досвіду та відповідальності тестера, а також від інших факторів. Іншим фактором є те, чи знаходиться система, що підлягає тестуванню, розташована в логічному сегменті, шлюз до загальнодоступної мережі захищений центральним брандмауером, чи це розділена інфраструктура з декількома різними шлюзами до публічних мереж.

Оскільки ці фактори важко оцінити, ми можемо отримати лише загальне твердження, що чим більша кількість систем і чим більша інфраструктура для тестування, тим більше часу і сил потрібно тестеру.

Складність інфраструктури, що підлягає тестуванню. Складність інфраструктури, що підлягає тестуванню, є ще одним важливим фактором, який впливає на час та зусилля, які повинен витратити тестер на проникнення. Типовими послугами, які пропонуються в Інтернеті, є пошук веб-сайтів (HTTP), завантаження (FTP) та електронна пошта. Вразливості в додатках, які підтримують ці послуги, часто відомі, оскільки такі послуги дуже поширені; їх

публікують у багатьох місцях в Інтернеті. Якщо компанія або державна влада обмежує себе такими широко розповсюдженими послугами, можна припустити інфраструктуру з низьким рівнем складності. Таким чином, кількість часу та робочої сили, що беруть участь у виконанні тесту на проникнення, повинна бути порівняно невеликою.

Якщо додатково використовуються складні рішення для електронної комерції або інтерактивні програми, знадобиться більше часу, щоб знайти вразливості, і для їх використання може знадобитися більш високий рівень знань. Це означає, що тестеру на проникнення потрібно буде передбачити більш тривалий проміжок часу та більш досвідчений персонал для проведення тестування на проникнення.

5.2 Вимоги до персоналу

Тести на проникнення повинні бути пристосовані до індивідуальної ситуації клієнта і, таким чином, не піддаються нормалізації. Тому тест на проникнення може лише певною мірою слідувати жорсткій схемі. Таким чином, тести на проникнення повинні проводити лише особи, які мають багаторічний досвід роботи в галузі IT-безпеки.

Для експертного виконання тестів на проникнення необхідні наступні навички:

- ✓ Знання системного адміністрування / операційних систем.

Ці знання необхідні для оцінки недоліків в операційних системах цільових систем, а також полегшують керування системами, які використовуються в тесті на проникнення.

- ✓ Знання TCP / IP та, якщо застосовується, інших мережевих протоколів.

Оскільки трафік даних в Інтернеті обробляється TCP / IP, що також стало стандартом у локальних мережах, поглиблене знання цього протоколу є

важливим. Знання TCP / IP тісно пов'язане з знаннями інших мереж та еталонною моделлю OSI.

- ✓ Знання мов програмування.

Щоб мати можливість експлуатувати вразливості в додатках та системах, знання мови програмування є необхідним. Незважаючи на те, що існує ряд готових інструментів, як скрипти, або з графічними інтерфейсами користувача, прогалини в безпеці, такі як переповнення буфера тощо, можна ефективно використовувати лише тоді, коли тестер має необхідні знання з програмування.

- ✓ Знання продуктів безпеки IT, таких як брандмауери, системи виявлення вторгнень.

Оскільки системи безпеки, такі як брандмауери або системи виявлення вторгнень, є надзвичайно поширеними в даний час, тестувальник на проникнення повинен знати, як працюють ці домовленості щодо безпеки, і слідкувати за останніми звітами щодо недоліків у безпеці продуктів IT-безпеки. Важливо мати огляд поширених на ринку продуктів у сфері IT-безпеки.

- ✓ Знання, як поводитися з хакерськими інструментами та сканерами на вразливість.

На додаток до деяких базових знань, досвід роботи з хакерськими інструментами та сканерами на вразливість необхідний для проведення тестів на проникнення.

Навички поводження з цими інструментами повинні отримувати через практичний досвід. З часом серед безлічі наявних інструментів деякі продукти досягли широкого розповсюдження (наприклад, nmap для сканування портів, Lophtcrack для паролів Windows).

Комерційні інструменти можуть бути використані для ефективного тестування, а безкоштовні інструменти можуть бути використані для демонстрації порівняно простого виконання таких тестів.

Ефективність тесту на проникнення сильно залежить від того, наскільки досвідчений тестер на проникнення в роботі з цими інструментами.

- ✓ Знання додатків / прикладних систем.

Багато вразливих місць розташовані в додатках, а не в програмному забезпеченні операційної системи. Вони охоплюють весь спектр прикладних систем, починаючи від недостатньо захищених макрофункцій в програмах обробки текстів до вразливості веб-браузерів через сценарії, до помилок переповнення буфера у великих системах баз даних, як приклади.

Тому тестер повинен бути знайомий з якомога більшою кількістю застосувань. Детальне знання про широко використовувані додатки є особливо важливим, оскільки ризик хакерів та зломщиків тут, як правило, особливо високий.

✓ Творчість.

Окрім високих професійних вимог, творчість є важливою якістю в тестуванні на проникнення. Оскільки кваліфікований тестер на проникнення може лише в обмеженій мірі слідувати жорсткій схемі, питання про те, як поступити в певному пункті, безсумнівно, виникне в ході тесту на проникнення, коли на перший погляд здається неможливим подальша компрометація системи. Цю проблему можна вирішити, вміло поєднуючи інформацію, отриману тестером, вразливості, які він визначив, та доступні йому інструменти та методи. Використовуючи свій інтелект, тестувальник на проникнення творчого повинен підходити для проведення "успішного" тесту, ніж тестер на проникнення, який просто спирається на результати своїх інструментів при виконанні тесту. Творчість, однак, ніколи не повинна призводити до несистемного або навіть хаотичного випробування, яке згодом не простежується.

5.3 Технічні вимоги

Перед тим, як тестувальник на проникнення може виконати випробувальні процедури, повинні бути виконані такі технічні вимоги:

✓ Доступ до публічних мереж.

Доступ до Інтернету чи загальнодоступної телефонної мережі є важливою умовою для проходження тесту на проникнення, оскільки більшість атак

здійснюються через ці канали зв'язку. Тому повинен бути доступний достатньо високий канал Інтернет-з'єднання. Тут важливо зазначити, що сканери на вразливість, зокрема, потребують високої пропускної здатності. Ефективність тестування напряму залежить від наявної пропускної здатності каналу.

- ✓ Наявність відповідних інструментів аудиту.

Тестер на проникнення повинен мати у своєму розпорядженні відповідні інструментами для проведення випробувань. Багато з цих інструментів можна безкоштовно завантажити з Інтернету. Однак такі інструменти, як сканери вразливості, часто залучають надзвичайно високі роялті (як правило, залежно від кількості IP-адрес для сканування). Для ефективного тестування потрібні «правильні» інструменти, а не велика кількість інструментів. Тестер знає ефекти та побічні ефекти інструментів і часто здатний швидко оцінити велику кількість результатів та відмежувати помилкові твердження від справжніх.

- ✓ Локальна тестова мережа.

Перед використанням справжнього тесту на проникнення різні інструменти повинні бути протестовані в локальній тестовій мережі. Такі види тестів також дозволяють тестеру на проникнення ознайомитися з хакерськими інструментами та сканерами вразливості та з результатами, які вони дають. Якщо системи тестової мережі належним чином налаштовані, вони також дозволяють перевірити вразливості в системах.

5.4 Етичні питання

Окрім вищезазначених умов, існує також ряд етичних питань, які необхідно розглянути перед початком тестування на проникнення.

Сторонам, з одного боку, слід уточнити, чи виправдано і в якій мірі використання методів соціального інженерії. Вони також повинні обговорити, чи потрібно вразливості, які були визначені як такі в тесті на проникнення, або можуть бути використані.

По-перше, проте сторони повинні чітко дати зрозуміти, що тест на проникнення може колись бути лише замовленням. Будь-яка ініціативна

поведінка, тобто запуск спроби нападу без мандату, завжди повинна вважатися нападом і підлягає відхиленню.

5.4.1 Використання методів соціальної інженерії

Далі наведено конфігурацію того, чому соціальна інженерія настільки успішна для того, щоб вирішити, чи виправдане використання таких методів у тесті на проникнення. Методи працюють тому, що всі люди мають певні характеристики або слабкі місця, які можна експлуатувати.

До них відносяться такі позитивні характеристики, як тенденція бути доброзичливими, мати почуття морального зобов'язання та бути корисними, а також менш позитивні якості, такі як опортуністичність та небажання брати на себе відповідальність.

Наприклад, майже всі працівники надають "новому начальнику" конфіденційну інформацію на його прохання, якщо він чи вона діятиме впевнено і виявляється lдоброзичливим.

Люди роблять це з готовності допомогти, з одного боку, і з почуття обов'язку, але, з іншого боку, внаслідок умовно-патогенних міркувань. Цим видам слабких місць можна протидіяти лише шляхом регулярного навчання всіх працівників. Однак можна стверджувати, що методи соціальної інженерії є успішними через недостатні або невідповідні заходи безпеки.

Якщо, наприклад, паролі видаються автоматично і настільки складні, що запам'ятати їх практично неможливо, багато користувачів записують їх у "безпечних" місцях. Або вони часто забувають свої паролі і запитують нові паролі, що також є гарною відправною точкою для соціальної інженерії.

Оскільки використання методів соціальної інженерії має прямий вплив на співробітників клієнта, оцінюючи їх надійність або обізнаність із безпекою, вони можуть викликати занепокоєння. Це може бути тим більше, коли методи соціальної інженерії виконуються без попереднього попередження і згодом пояснюються.

Навіть коли звіт про результати проникнення не містить жодної інформації та імен, і жодна особиста інформація про неналежну поведінку

певних працівників не передається усно клієнтові, ці методи все ще можуть змусити співробітників почуватись невпевнено.

Саме тому багато експертів із безпеки відмовляються від використання соціальної інженерії у тестах безпеки або лише вважають їх доцільним, коли вимоги до безпеки дуже високі. Тому використання соціальної інженерії потрібно дуже уважно розглядати.

Тестер завжди повинен інформувати клієнта про можливі наслідки соціальної інженерії та заявляти, що ця методика буде швидше за все мати , це успіх, якщо користувачі не отримують попередньої підготовки і що вона може негативно вплинути на працівників.

5.4.2 Експлуатація вразливих місць

Уразливість у додатку чи операційній системі, яка потім може бути використана для захоплення системи, як правило, буде виявлена до того, як система фактично буде порушена.

Тут тестувальник повинен розглянути питання про те, чи потрібно виконувати цей останній крок використання вразливості для того, щоб перевірити його, чи достатньо лише вказати на наявність вразливості. Це питання можна вирішити лише з огляду на визначену мету тесту та умови, що випливають із цього. Якщо тест на проникнення повинен бути максимально реалістичним та інформативним, може бути доречним не встановлювати обмежень щодо агресивності процедур тестування. Якщо, з іншого боку, уникнути можливого порушення операцій, наскільки це можливо, вразливості не слід активно використовувати.

У цьому випадку результатом тесту на проникнення було б виявлення наявних вразливостей, і жодних доказів успішного проникнення не було б надано.

6. Методика тестування на проникнення

Методика базується на структурованій процедурі проведення тестування на проникнення, яка є основою для розробки індивідуальних планів дій для конкретних випробувань на проникнення.

6.1 Вимоги до методики випробування на проникнення

Методика описує та структурує виконання тесту на проникнення замовлення на. Тест завжди повинен сприймати цілі клієнта, і непотрібно нехтувати цією перспективою.

Це означає, наприклад, окреслити етапи тестування, необхідні для досягнення цієї мети, або пояснити, чи підходить тест на проникнення взагалі для їх досягнення.

Методика також повинна включати заходи щодо дотримання законодавчих положень та дотримання умов щодо організації та персоналу для проведення тестів на проникнення.

Він повинен враховувати обмежений доступний час і повинен включати оцінку потенційного ризику або аналіз корисних вигод.

Модульний підхід, такий як OSSTMM, є доцільним для групування окремих етапів тестування, оскільки це дозволяє тематично класифікувати етапи, що беруть участь у тесті на проникнення.

Це дає тесту чітку основу, а також дозволяє тестувальнику розробити відповідний тест на проникнення шляхом вибору або виключення певних модулів.

З фінансових причин фактичний тест на проникнення зазвичай не використовує всі можливі модулі тестування. Хоча це забезпечило б повністю всебічний тест, воно також буде вкрай затратним у часі і, таким чином, не може бути погоджено ні з цілями клієнта, ні з конкретними вимогами безпеки. Коли

вимоги до безпеки особливо високі, тест повинен бути максимально вичерпним. Це означає, що всі або більшість модулів повинні бути застосовані, і всі системи клієнта повинні бути включені в тест. Якщо вимоги до безпеки низькі, певні модулі можуть бути опущені та / або перевіряти лише зовнішні системи. Фінансові міркування повинні визначати обсяг тесту на проникнення. Витрати та ризики тестувальних заходів повинні бути зважені з потенційними витратами та ризиками, які можуть виникнути у разі нападу.

6.2 П'ять фаз тесту на проникнення

Розглянемо п’ять фаз тестування на проникнення на основі викладених вище міркувань. Окремі фази проходять послідовно:

Фаза 1. Підготовка. Важко виконати очікування клієнта без ретельної підготовки, наприклад, досягнення згоди щодо цілей проникнення.

На початку тесту на проникнення повинні бути уточнені та визначені з ним цілі клієнта. Виконання тесту на проникнення без повного врахування відповідних правових положень може мати наслідки, передбачені кримінальним чи цивільним законодавством. Тому тестувальник повинен забезпечити, щоб процедури випробувань не порушували законодавчих норм чи договірних угод. Неспроможність виробничої системи також може призвести до застосування вимог внаслідок використання методів проникнення, про які не було погоджено, або ризиків, пов'язаних із використовуваними методами, про які не було відомо, саме тому процедура та її ризики повинні бути обговорені та задокументовані .

Усі узгоджені деталі повинні бути викладені у письмовій формі в договорі.

Фаза 2. Розвідка. Після визначення цілей, обсягу, процедур, надзвичайних заходів тощо з урахуванням правових та організаційних аспектів

та інших умов тестувальник може почати збирати інформацію про ціль. Ця фаза є тестом на пасивне проникнення.

Метою є отримання повного та детального огляду встановлених систем, включаючи зони, відкриті для атаки або відомі недоліки в безпеці. Залежно від кількості комп'ютерів або розміру мережі, що підлягає дослідженню, етапи тестування можуть бути дуже трудомісткими. Якщо, наприклад, мережа класу C (256 можливих IP-адрес) за брандмауером повинна бути повністю перевірена, повне сканування портів (усі 65536 порти) може зайняти кілька тижнів, залежно від налаштування. Хоча ці тривалі етапи тестування зазвичай виконуються автоматично, час, необхідний для них, все ж повинен враховуватися при плануванні. Таким чином, тест на проникнення може зайняти 20 днів, наприклад, вищезгаданий тест триватиме кілька тижнів.

Фаза 3. Аналіз інформації та ризиків; успішна, прозора та економічно ефективна процедура повинна аналізувати та оцінювати інформацію, зібрану до того, як можна провести етапи тестування для активного проникнення в систему - які часто є дуже трудомісткими.

Аналіз повинен включати визначені цілі тесту на проникнення, потенційні ризики для системи та орієнтовний час, необхідний для оцінки потенційних недоліків безпеки для наступних спроб активного проникнення.

Потім цілі на фазі 4 вибираються на основі цього аналізу. Наприклад, зі списку ідентифікованих систем тестер може вибрати тестування лише тих, які містять відомі потенційні вразливості через їх конфігурацію або ідентифіковані програми / послуги, або ті, щодо яких тестер має особливі знання.

У тесті на проникнення, для якого чітко визначено кількість цільових систем у фазі 2, цей вибір означає, що кількість цільових систем для фази 4 автоматично зменшується.

Обмеження повинні бути всебічно задокументовані та обґрунтовані, оскільки, крім бажаного підвищення ефективності, вони також призводять до зниження інформативної цінності тесту на проникнення, і клієнт повинен знати про це.

Фаза 4: Активні спроби вторгнення. Нарешті, вибрані системи активно атакуються. Ця фаза тягне за собою найвищий ризик в рамках тесту на проникнення, і її слід виконувати з належною обережністю.

Однак лише ця фаза виявляє ступінь, в якому передбачувані вразливості, виявлені на етапі розвідки, становлять реальні ризики. Цю фазу необхідно виконати, якщо потрібна перевірка потенційних вразливих місць. Для систем з дуже високими вимогами щодо доступності або цілісності потенційні ефекти повинні бути ретельно враховані перед виконанням критичних тестових процедур, таких як використання вразливостей переповнення буфера.

Під час тестування типу “білий ящик” , можливо, знадобиться встановити виправлення на критичних системах перед тим, як виконати тест, щоб запобігти відмові системи. Тест, ймовірно, не зможе знайти вразливості, але задокументує безпеку системи. На відміну від хакерської атаки, проте тест на проникнення не завершений - він буде продовжений.

Фаза 5: Остаточний аналіз а також окремі етапи тестування. Підсумковий звіт повинен містити оцінку вразливих місць у вигляді потенційних ризиків та рекомендації щодо усунення вразливих місць та ризиків. Звіт повинен гарантувати прозорість тестів та вразливості, які він розкрив. Результати та ризики для IT-безпеки повинні бути детально обговорені з клієнтом після завершення тестових процедур.

Документацію на проникнення слід складати під час фаз 1–5, а не лише як частину остаточного аналізу на фазі 5. Це забезпечує те, що етапи випробувань та результати всіх етапів є задокументованими та робить тести на проникнення прозорі та простежувані.

Незважаючи на спроби зберегти методику якомога загальнішою, на практиці можуть виникнути ситуації, які вимагають відхилень від детально описаної тут процедури.

Усі кроки, що відхиляються від методології, детально описаної тут, повинні бути документовані та обґрунтовані окремо.

6.3 Модулі для процедур тестування

Описаний вище підхід не містить явних процедур тестування, він визначає лише працездатність модулів I та E. На основі OSSTMM різні процедури тестування, які можуть бути проведені в тесті на проникнення, були згруповані в модулі.

Доступ до об'єктів тестування доступний лише у фазі 2 - "Розвідка" та на фазі 4 - "Активне вторгнення".

Модулі були розділені відповідно на два класи, I модулі для розвідки та E модулі для спроб проникнення.

Модулі були розділені таким чином, що кожен з етапів належить до однакових значень критеріїв класифікації тестування на проникнення.

Наприклад, ефективність сканування портів поділяється на модуль для прихованих сканувань портів і модуль для відкритого сканування портів, а тестування брандмауера поділяється на модулі для тестування ззовні та зсередини.

6.3.1 Модулі для розвідки

Таблиця 6.1 містить перелік розвідувальних модулів I 1 - I 22.

Таблиця 6.1 – Перелік розвідувальних модулів

№	Модуль
I 1	Аналіз опублікованих даних
I 2	Приховані запити основної мережевої інформації
I 3	Завершені запити основної мережевої інформації
I 4	Скритне сканування портів
I 5	Відкрите сканування портів
I 6	Ідентифікація програми
I 7	Ідентифікація системи
I 8	Ідентифікація прихованого маршрутизатора

№	Модуль
I 9	Ідентифікація зовнішнього маршрутизатора
I 10	Прихована ідентифікація брандмауера
I 11	Відкрита ідентифікація брандмауера
I 12	Дослідження вразливості
I 13	Ідентифікація інтерфейсу програми
I 14	Збір інформації для соціальної інженерії
I 15	Збір інформації для комп'ютерної соціальної інженерії
I 16	Збір інформації для особистої соціальної інженерії
I 17	Тестування бездротового зв'язку (лише для сканування)
I 18	Тестування телефонної системи (Ідентифікація)
I 19	Тестування системи голосової пошти (Ідентифікація)
I 20	Тестування факсимільної системи (ідентифікація)
I 21	Аналіз фізичного середовища
I 22	Ідентифікація контролю доступу

6.3.2 Модулі для активних спроб вторгнення

У таблиці 6.2 приведено перелік модулів E 1 - E 23 для активних спроб вторгнення.

Таблиця 6.2 – Список модулів для активних спроб вторгнення

№	Модуль
E 1	Прихована перевірка фактичних вразливостей
E 2	Відверта перевірка фактичних вразливостей
E 3	Завершені запити основної мережевої інформації
E 4	Приховане тестування маршрутизатора
E 5	Відкрите тестування маршрутизатора
E 6	Тест довірчих відносин між системами

№	Модуль
E 7	Тест на прихований брандмауер ззовні
E 8	Тест брандмауера ззовні
E 9	Тестування брандмауера з обох сторін
E 10	Тестування системи IDS
E 11	Перехоплення паролів
E 12	Злом пароля
E 13	Тест на сприйнятливість до відмови в обслуговуванні
E 14	Соціальна інженерія на базі комп'ютера
E 15	Пряма, особиста соціальна інженерія з фізичним доступом
E 16	Непряма, особиста соціальна інженерія без фізичного доступу
E 17	Тестування бездротового зв'язку
E 18	Тестування адміністративного доступу до телефонної системи
E 19	Тестування системи голосової пошти
E 20	Тестування адміністративних точок доступу до факсимільної системи
E 21	Тестування модему
E 22	Активний тест контролю доступу
E 23	Тест процедур ескалації

6.3.3 Розширюваність

Якщо майбутні розробки вимагають нових етапів тестування, перелік модулів може бути розширений. Усі етапи, які слід виконати в новому модулі, повинні відповідати тим самим критеріям класифікації, інакше через принцип виключення модуль не може бути інтегрований у методологію.

6.3.4 Принцип виключення

Модулі вибираються за принципом негативного виключення, а не за принципом позитивного відбору. Виходячи з обраної класифікації, модулі, які неможливо виконати через обраний підхід виключається з тестів. Якщо модуль не виключений, слід провести етапи тестування, що містяться в ньому, що

сприяє забезпеченню всебічного тесту на проникнення. Якщо модуль має бути виключений з інших причин, ці причини повинні бути викладені та задокументовані. Після того, як визначено цілі проникнення, вибирається відповідний тест за допомогою системи класифікації та з урахуванням правових та організаційних аспектів.

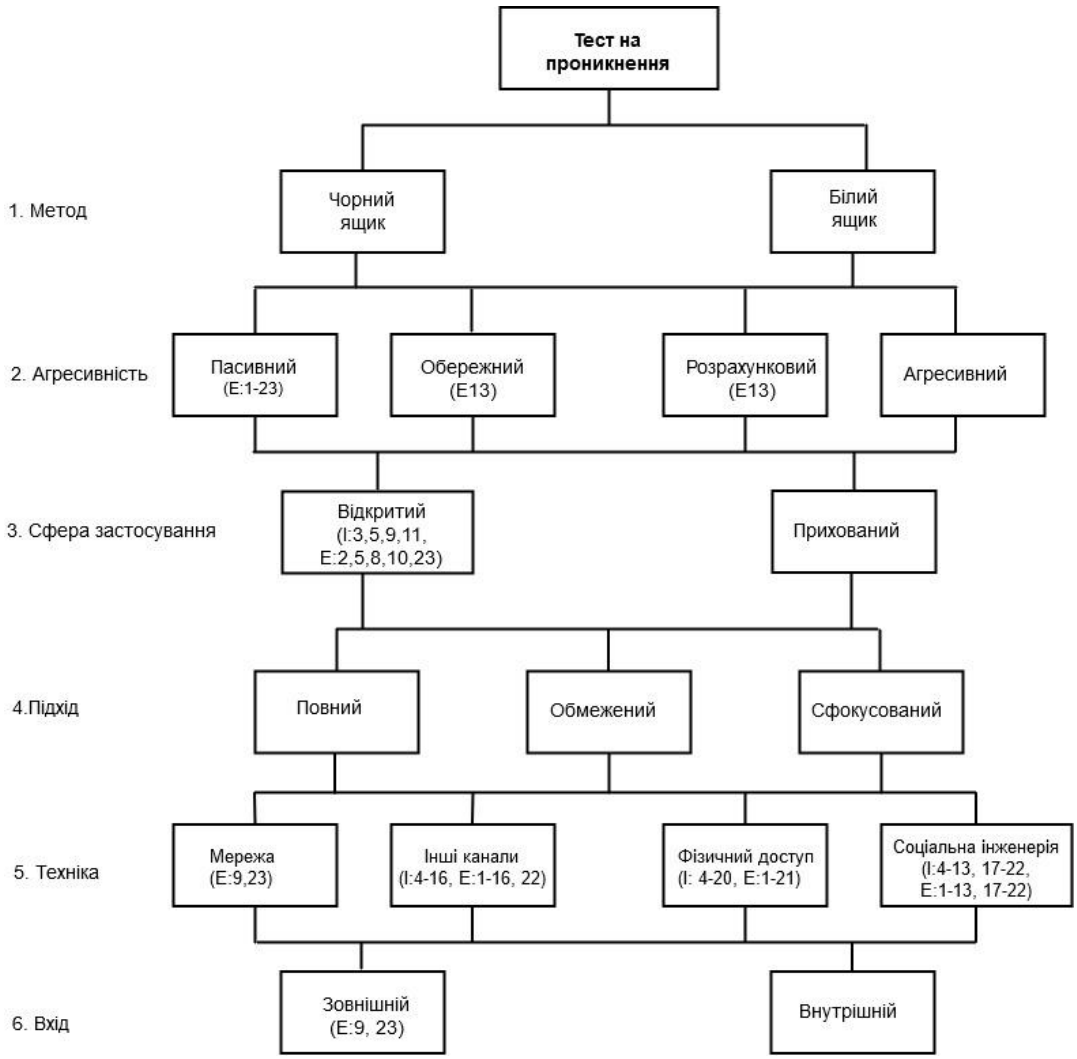

Рисунок 6.3 – Виключення модулів на основі класифікації

Потім обрана класифікація визначає за принципом виключення, які модулі для розвідки та активного проникнення неможливо виконати. Система класифікації показує, які модулі повинні бути виключені для кожного з критеріїв (рисунок 6.3).

Вибір інформаційної бази - білий або чорний - прямо не впливає на вибір модулів. Однак у рамках тестування, який залежить від наявних документів, ряд тестових процедур можна відкинути і замінити на "читання". Ця процедура проілюстрована в таблиці 6.3.

Таблиця 6.3 – Приклад принципу виключення

Критерій	Значення	Виключені I модулі	Виключені E модулі
1. Інформаційна база:	чорний ящик	-	-
2. Агресивність:	обережність	-	E13
3. Сфера застосування:	сфокусована	-	-
4. Підхід:	приховано	I 13, 5, 9, 11	E 2, 5, 8, 10, 23
5. Техніка	на основі мережі	I 14-22	E 14-23
6. Початкова точка:	ззовні	-	E 9, 23

Модулі **I 3, 5, 9, 11, 13-22** виключені, як і модулі **E 2, 5, 6, 8-10, 14-23**. Решта модулів повинні бути виконані в тесті на проникнення.

7. Виконання тестів на проникнення

У цьому розділі описано, як проводяться тести на проникнення, застосовуючи представлену вище методику. Етапи, що містяться у фазах від 1 до 5, детально пояснюються з можливими проблемами. У цьому розділі також описано на якому етапі, яку документацію слід підготувати.

7.1 Підготовка

Етап підготовки починається з визначення мети або цілей тестування на проникнення. Тестер і клієнт повинні спільно визначати цілі, щоб обидві сторони поділяли однакове розуміння цілей.

Можливі цілі тестування на проникнення - підвищити безпеку технічних систем, забезпечити IT-безпеку підтвердженою зовнішньою стороною та підвищити безпеку організаційних / кадрова інфраструктура (див. розділ 3.2). Відповідно до цих цілей, клієнт та випробувач повинні дотримуватися та обговорювати законність тесту на проникнення та організаційні, кадрові та технічні вимоги.

За допомогою класифікації, пізніше вибирається відповідний тест, використовуючи шість критеріїв інформаційної бази, агресивності, обсягу, підходу, техніки та початкової точки.

Якщо тест на проникнення проводиться вперше, тест повинен ідеально охопити всі існуючі системи, оскільки вразливості можуть залишатися в системах, які не досліджуються.

Кількість часу, який потрібно витратити на тестування, в ідеалі слід оцінювати на основі результатів а попередня оцінка вимог до захисту, застосовуючи, наприклад, методологію посібника з захисту базової лінії.

На основі обраної класифікації тестер вибирає модулі розвідки та активної спроби вторгнення, які слід проводити, виключаючи модулі, які можна виключити.

Ризики для клієнта різняться залежно від обраних модулів, і можуть варіюватися, наприклад, від відтермінування робіт з технічного обслуговування (низький ризик) до постійних збоїв IT-системи (високий ризик). Клієнт та тестер повинні обговорити ймовірність виникнення таких ризиків та їх потенційних наслідків. В результаті обговорення сторони повинні визначити необхідні заходи у надзвичайних ситуаціях для ризиків, які обидві сторони готові взяти на себе. Визначаючи заходи у надзвичайних ситуаціях, сторони повинні враховувати часові рамки, протягом яких можна проводити критичні випробування, і хто буде відповідати за необхідні заходи. Якщо вибір модулів передбачає неприйнятні ризики, потрібно буде вибрати інший тест на проникнення, наприклад. менш агресивний підхід для активних спроб вторгнення, відмови від методів соціальної інженерії або зменшення обсягу тестованих систем. У разі потреби організаційну та правову базу доведеться розглянути чи обговорити ще раз на цьому етапі.

Усі результати підготовчого етапу повинні бути записані у письмовій формі у звіті та підписані обома сторонами. Клієнт може використовувати цей звіт для моніторингу тестів на проникнення, наприклад, і він може служити керівництвом для тестера.

Крім того, в договорі має бути визначено обсяг документації, яка має бути надана після завершення тесту на проникнення. Метою документації повинно бути забезпечення можливості процес тестування на проникнення, який слід простежити.

Етап підготовки повинен завершитися детальним планом із зазначенням того, коли саме проникають компоненти, з яким рівнем інтенсивності. Також потрібно визначити етапи ескалації, тобто непередбачуваність, повинні бути розроблені заходи для чутливих систем, таких як резервне копіювання даних, альтернативні системи та які постачальники послуг повинні бути доступними.

Час тестування слід визначати приблизно, принаймні для критично важливих для бізнесу систем, наприклад, щоб уникнути порушення роботи клієнта. Ще одне рішення, яке, можливо, буде потрібно прийняти - це які функціональні відділи повинні бути поінформовані про тест.

Класифікація даних допомагає визначити інтенсивність та підхід до тестів (виробничі сервери тестуються по-різному на тестових серверах). Якщо, наприклад, кластер повинен бути протестований, сторонам доведеться вирішити чи не буде аудит краще для виявлення вразливих місць. Що стосується саморозвитку, відповідні працівники служби підтримки повинні брати участь у вирішенні необхідних та запобіжних заходів.

Нарешті, перед запуском тесту має бути зрозуміло, як будуть оброблятися результати тесту на проникнення. Позитивний та конструктивний підхід корисний для перекладу рекомендацій в напрямку вдосконалення інфраструктури безпеки IT.

7.2 Розвідка

Фаза 2: Розвідка починається з аналізу попередньої інформації. Під час тесту чорного ящика попередня інформація може містити IP-адреси або блоки IP-адрес.

Якщо детальна інформація була доступна в тесті білого ящика (наприклад, версії операційної системи, використовувані додатки тощо), тестер повинен почати з аналізу цієї інформації і, якщо необхідно, запитувати додаткову інформацію від клієнта, наприклад, описи системи, мережеві плани тощо, щоб забезпечити проведення тестування максимально ефективно.

На наступному етапі проводяться процедури тестування вибраних модулів **I**. Тестер більш-менш вільний у виборі порядку, в якому комплектуються модулі.

Тільки модуль **I 12**: "Дослідження вразливості" повинен проводитися після попередніх модулів **I**, оскільки він використовує результати цих модулів, наприклад, список доступних систем та версій програми. Отримана інформація використовується в **I 12** для ідентифікації вразливих місць в системах та додатках, при цьому публічні та приватні бази даних запитуються на відомі слабкі місця і лазівки безпеки. Ця процедура проілюстрована наступним прикладом.

Тестер визначив сервер у DMZ клієнта, потенційну ціль для тесту на проникнення, як сервер електронної пошти та виявив версію програмного забезпечення сервера електронної пошти та операційної системи сервера за допомогою пошуку банера.

За допомогою цієї інформації тестер шукає потенційні вразливості, пов’язані з цією комбінацією, в базах даних, списках розсилки та групах новин тощо. Сканери вразливості можуть виконувати деякі з цих етапів тестування автоматично, однак за допомогою незвичних комбінацій вони часто стикаються з обмежуючими факторами і не повідомляють або не виявляють наявні вразливості.

Тому вони не є заміною ручного пошуку, але вони можуть доповнити і прискорити процес. Наприкінці розвідувальної фази тестер матиме файли журналів і модулів, які генеруються сканерами вразливості, наприклад, опис систем та список потенційних вразливостей, всі вони повинні бути включені в документацію про тестування на проникнення.

7.3 Аналіз інформації / ризики

Першим кроком має бути оцінка пов'язаних ризиків. З огляду на багатство інформації, яку зазвичай отримують, важливо проаналізувати та оцінити цю інформацію, перш ніж йти далі.

Оцінка повинна включати визначені цілі, потенційні загрози для систем та передбачувану вартість оцінки недоліків безпеки. Вразливості можна оцінювати об'єктивно, а потенціал ризику можна встановити, використовуючи, наприклад, консенсус SANS-Alert Security Alens (SANS-SAC), який оновлюється щотижня. Оцінка завжди буде суб’єктивною, оскільки досвід та спеціалізація тестера, наприклад, відіграють головну роль в оцінці часу та витрат.

Після того, як загроза була оцінена, тестувальник повинен оцінити індивідуальну вартість успішної атаки, яка використовує потенційні вразливості, і порівняти їх з її шансами на успіх. Приблизний графік часу для етапів тестування може бути отриманий з часу, зазначеного в описах модуля (необхідний час: середній, високий, дуже високий). Тоді слід визначати пріоритети на основі цього порівняння.

Чим більша ймовірність успіху і чим менші необхідні час / витрати, тим вище повинен бути пріоритет. Тестувальник повинен документувати як оцінку часу / витрат, так і пріоритети, які він встановлює.

Виходячи з пріоритетів тестера, можна вибрати цілі та етапи тестування для наступного етапу, 4 фази.

Наступні кроки тестування повинні зосереджуватися насамперед на IT-системах, які після оцінки потенційних вразливих місць були оцінені як високі та середні пріоритетні, а також на тих тестових процедурах, які, швидше за все, будуть успішними. Для цього додатково вибираються модулі **E**. Письмовий список систем і модулів повинен бути доданий до документації про тестування на проникнення і обговорюватися з клієнтом до будь-яких активних спроб вторгнення.

7.4 Активні спроби вторгнення

Після того, як відповідні модулі **E**, були відібрані та визначені пріоритетні, на цьому етапі IT-системи активно застосовуються. Тестер систематично працює через спроби нападу в порядку їх пріоритетності, перш за все, найвищого пріоритету.

Цілі клієнта тестування на проникнення, як правило, є особливо критичними системами для бізнесу, тому особливу обережність вимагає проведення спроб вторгнення. Заходи щодо непередбачених ситуацій, згадані у етап підготовки абсолютно необхідний на цьому етапі. Наприклад, вони вимагають, щоб спроби вторгнення (у критичні для бізнесу системи) здійснювались поза робочим часом (тобто вночі або у вихідні дні), а також були присутні відповідальні адміністратори системи.

На етапі розвідки була визначена конкретна серверна операційна система з додатком веб-сервера в системі, яка використовується для операцій в Інтернеті та яка отримує доступ до внутрішніх даних компанії ERP система. Пошук вразливості виявив вразливість переповнення буфера для бази даних в системі ERP. Однак брандмауер перешкоджає прямому доступу до бази даних.

Тепер тестер стоїть перед завданням з'ясувати, чи може бути запущена онлайн-транзакція, яка проникає через брандмауер для використання вразливості в системі БД, маніпулюючи HTTP-зв'язком.

До тих пір, поки не будуть здійснені активні спроби проникнення, не стане зрозумілим, чи можна реально використовувати потенційні вразливості, виявлені на фазі розвідки, так що вибрані наприклад, можна проникнути в систему. Якщо клієнт просить перерахувати та перевірити потенційні вразливості, тестер і клієнт повинні ретельно зважити можливі наслідки (наприклад, час простою системи).

Документація повинна деталізувати як позитивні, тобто успішні активні спроби вторгнення, так і негативні результати, тобто невдалі спроби проникнення.

7.5 Остаточний аналіз

На цій заключній фазі результати кожного з модулів **E**, які були виконані, описуються у підсумковому звіті. Підсумковий звіт повинен містити підсумок керівництва, що описує тестові завдання, ключові результати тестування та рекомендовані дії на абстрактному рівні та розроблені рекомендації для вищого керівництва. Основний розділ підсумкового звіту повинен містити детальні позитивні та негативні результати тесту. Для вразливості результати оцінюються та визначаються пріоритети, а тестувальник описує пов'язані з цим ризики, щоб клієнт знав, які ризики мають відношення до його бізнес-операцій.

Крім того, звіт повинен містити рекомендації щодо того, як клієнт може усунути вразливості, наявні на момент тесту на проникнення. Остаточний звіт повинен також включати план дій щодо усунення вразливих місць, виходячи з пріоритетів, визначених за результатами та складених разом із клієнтом.

План дій повинен містити графік кожної критичної вразливості та називати людину та / або область, яка відповідає за її усунення.

Чутливі особисті дані, отримані під час тестування на проникнення, такі як паролі або приватні електронні листи, не повинні включатися до остаточного звіту з міркувань захисту даних; вони повинні бути передані визначеній особі, наприклад пропозиція щодо захисту даних. Однак клієнт повинен мати можливість чітко відслідковувати результати тестів, і вся інформація, зібрана на різних фазах, повинна бути включена, за адресою принаймні, як додаток до робочих документів. Це включає, наприклад, детальну інформацію про використовувані інструменти, кроки роботи (який інструмент використовувався з якими параметрами), файли журналів, час роботи (коли були здійснені напади) тощо.

Тестувальник повинен видалити будь-яке програмне забезпечення, наприклад кейлоггери, яке, можливо, було встановлено в IT-системі клієнта в ході тесту на проникнення або будь-які інші модифікації, внесені в IT-системи клієнта, і відновити систему в стані, у якому тестер отримав її перед тестуванням.

8. Тестування на проникнення інфраструктури

Тестування на проникнення інфраструктури включає всі внутрішні комп'ютерні системи, пов'язані з ними зовнішні пристрої, інтернет-мережу, тестування хмари та віртуалізацію. Незважаючи на те, що вона прихована у вашій внутрішній корпоративній мережі або від загального перегляду, завжди є можливість, що зловмисник може вплинути на вашу інфраструктуру. Отже, краще бути безпечним заздалегідь, а не пізніше.

Види тестування на проникнення інфраструктури.

Нижче наведено важливі типи тестування на проникнення інфраструктури:

• Тестування на проникнення зовнішньої інфраструктури.

• Тестування на проникнення внутрішньої інфраструктури.

• Тестування на проникнення хмари та віртуалізації.

• Тестування бездротового захисту.

Тестування зовнішньої інфраструктури. Тест на проникнення, орієнтований на зовнішню інфраструктуру, виявляє, що хакер може зробити з вашими мережами, які легко доступні через Інтернет.

У цьому тестуванні тестер зазвичай повторює ті ж атаки, які хакери можуть використовувати, знаходячи і відображаючи недоліки безпеки у вашій зовнішній інфраструктурі.

Існують різні переваги використання тестування на проникнення зовнішньої інфраструктури, зокрема:

• ідентифікує недоліки конфігурації брандмауера, які можуть бути неправильно використані;

• знаходить, як зловмисник може отримати з системи вашу інформацію;

• пропонує, як ці проблеми можуть бути виправлені;

• готує всебічний звіт, в якому висвітлюється ризик безпеки прикордонних мереж і пропонує рішення;

• забезпечує загальну ефективність і продуктивність вашого бізнесу.

Тестування на проникнення внутрішньої інфраструктури. Через незначні недоліки внутрішньої безпеки хакери незаконно вчиняють шахрайство у великих організаціях. Таким чином, при внутрішньому тестуванні на проникнення інфраструктури тестувальник може визначити можливість забезпечення та від якого співробітника ця проблема виникла.

Переваги тестування на проникнення внутрішньої інфраструктури:

• визначає, як внутрішній зловмисник може скористатися навіть незначним недоліком безпеки;

• визначає потенційний бізнес-ризик і збиток, який може завдати внутрішній зловмисник;

• покращує системи безпеки внутрішньої інфраструктури;

• готує вичерпний звіт з детальною інформацією про безпеку внутрішніх мереж, а також детальний план дій щодо його вирішення.

Тестування на проникнення хмари та віртуалізації. Оскільки ви купуєте публічний сервер або хмарний простір, це значно збільшує ризики порушення даних. Крім того, виявлення зловмисника на хмарі є стладним. Зловмисник може також придбати хостинг об'єкта Cloud, щоб отримати доступ до нових даних Cloud.

Фактично, більшість хостингів Cloud реалізована на віртуальній інфраструктурі, що викликає ризик віртуалізації, що зловмисник може легко отримати доступ.

Переваги тестування на проникнення хмари та віртуалізації:

• виявляє реальні ризики у віртуальному середовищі та пропонує методи та витрати для виправлення загроз та недоліків;

• надає керівні принципи та план дій щодо вирішення проблеми;

• покращує загальну систему захисту;

• готує комплексний звіт про систему безпеки для хмарних обчислень і віртуалізації, окреслює недоліки безпеки, причини та можливі рішення.

Тестування на проникнення бездротового захисту. Бездротова технологія вашого ноутбука та інших пристроїв забезпечує легкий і гнучкий доступ до різних мереж. Легкодоступна технологія є вразливою до унікальних ризиків; як фізична безпека не може бути використана для обмеження доступу до мережі, так як зловмисник може зламати з віддаленого місця. Таким чином, тестування бездротового проникнення безпеки необхідно для компанії / організації.

Нижче наведено причини використання бездротової технології:

• щоб знайти потенційний ризик, викликаний вашими бездротовими пристроями;

• надати керівні принципи та план дій щодо захисту від зовнішніх загроз.

• удосконалити загальну систему безпеки;

• для підготовки вичерпного звіту системи безпеки про бездротову мережу, щоб визначити недоліки безпеки, причини та можливі рішення.

Існує питання захисту найбільш критичних даних організації; отже, роль тестера на проникнення є дуже критичною, незначна помилка може спричинити ризик сторін (тестера, так і його клієнта).

Таким чином, у цій лекції розглядаються різні аспекти тестування на проникнення, включаючи його кваліфікацію, досвід та обов'язки.

Кваліфікація тестерів на проникнення. Цей тест може бути виконаний лише кваліфікованим тестером на проникнення, тому кваліфікація тестера на проникнення дуже важлива.

Як кваліфікований внутрішній експерт або кваліфікований зовнішній експерт може виконати тестування на проникнення, поки вони не є організаційно незалежними. Це означає, що тестер на проникнення повинен бути організаційно незалежним від управління цільовими системами. Наприклад, якщо стороння компанія бере участь у встановленні, обслуговуванні або підтримці цільових систем, ця сторона не може виконувати тестування на проникнення.

Ось деякі рекомендації, які допоможуть вам під час виклику тестера на проникнення.

Сертифікація. Сертифікований тестер може проводити випробування на проникнення. Сертифікація тестера на проникнення є визнанням його навичок та компетенції.

Нижче наведено важливі приклади сертифікації тестування на проникнення:

• Certified Ethical Hacker (CEH). (Сертифікований етичний хакер, CEH).

• Offensive Security Certified Professional (OSCP). Професійний сертифікований спеціаліст з безпеки (OSCP).

• CREST Penetration Testing Certifications. Сертифікати CRET тестування на проникнення.

• Communication Electronic Security Group (CESG) IT Health Check Service certification. Сертифікація служби електронної безпеки зв'язку (CESG).

• Global Information Assurance Certification (GIAC) Certifications for example, GIAC Certified Penetration Tester (GPEN), GIAC Web Application Penetration Tester (GWAPT), Advance Penetration Tester (GXPN), and GIAC Exploit Researcher // Сертифікати глобальної сертифікації інформації (GIAC), наприклад, сертифікований тест на проникнення GIAC (GPEN), тестер на проникнення веб-застосунків GIAC (GWAPT), тест на просування (GXPN), і дослідник GIAC Exploit.

Досвід минулого. Наступні питання допоможуть вам найняти ефективного тестера на проникнення:

• Скільки років досвіду тестування на проникнення?

• Чи є він незалежним тестером на проникнення або працює в організації?

• В скількох компаніях він працював у якості тестера на проникнення?

• Чи проводив він тестування на проникнення для будь-якої організації, яка має подібний розмір і сферу застосування, як ваша?

• Який досвід має тестер на проникнення? Наприклад, проведення випробувань на проникнення в мережі тощо.

• Ви також можете звернутися за посиланням від інших клієнтів, для яких він працював.

При найманні тестера на проникнення важливо оцінити досвід тестування минулого року в організації, для якої він (тестувальник) працював, оскільки це пов'язано з технологіями, спеціально розробленими ним у межах цільового середовища.

На додаток до вищезазначеного, для складних ситуацій і типових вимог клієнта, рекомендується оцінити можливість тестування та обробляти подібне середовище в його / її попередньому проекті.

Роль тестера на проникнення.

Тестер проникнення має такі ролі:

• визначення неефективного розподілу інструментів і технологій;

• тестування в системах внутрішньої безпеки;

• визначити експозиції для захисту найбільш критичних даних;

• відкрити знання про вразливі місця та ризики в інфраструктурі.

• звітність та визначення пріоритетних рекомендацій щодо виправлення ситуації для забезпечення того, щоб команда з безпеки використовувала свій час найбільш ефективним шляхом, захищаючи найбільші прогалини у сфері безпеки.

Це не обов'язково, щоб досвідчений тестер на проникнення міг написати хороший звіт, оскільки написання звіту про тестування на проникнення є мистецтвом, яке потрібно вивчити окремо.

9. Написання звітів

Написання звітів під час тестування на проникнення - це комплексне завдання, яке включає методологію, процедури, належне пояснення змісту та форми звіту, детальний приклад звіту про тестування та особистий досвід тестера. Після підготовки звіту він поширюється серед вищого керівного складу та технічної групи цільових організацій. Якщо в майбутньому виникне така потреба, цей звіт використовується як посилання.

Етапи написання звітів. Враховуючи комплексну письмову роботу, написання звітів про проникнення поділяється на наступні етапи (рисунок 9.1):

- планування звіту;
- збір інформації;
- написання першої чернетки;
- перегляд та завершення.

Рисунок 9.1 – Етапи написання звітів

Планування звіту. Планування звіту починається з цілей, які допомагають читачам зрозуміти основні моменти тестування на проникнення. У цій частині описується, чому проводиться тестування, якими є переваги

тестування, і т.д. По-друге, планування звітів також включає час, необхідний для тестування.

Основними елементами написання звіту є:

• **Цілі** - описує загальну мету та переваги тестування.

• **Час** - дуже важливим є включення часу, оскільки він дає точний статус системи. Припустимо, якщо пізніше відбудеться щось неправильне, цей звіт збереже тестера, оскільки звіт буде ілюструвати ризики та вразливості в області тестування на проникнення протягом певного періоду часу.

• **Цільова аудиторія** - звіт про тестування на проникнення також повинен включати цільову аудиторію, таку як менеджер з інформаційної безпеки, менеджер з інформаційних технологій, головний офіцер з інформаційної безпеки та технічна команда.

• **Класифікація звітів** - оскільки вона є вкрай конфіденційною і яка містить IP-адреси сервера, інформацію про додатки, вразливість, загрози, вона має бути класифікована належним чином. Однак, ця класифікація повинна проводитися на основі цільової організації, яка має політику класифікації інформації.

• **Розподіл звітів** - у обсязі робіт слід зазначити кількість копій та розподіл звітів. Слід також зазначити, що паперові копії можна контролювати шляхом друку обмеженого числа копій, прикріплених до їх номера та імені одержувача.

Збір інформації. Завдяки складним і тривалим процесам, тестеру на проникнення потрібно згадати кожен крок, щоб переконатися, що він зібрав всю інформацію на всіх етапах тестування. Поряд з методами, він також повинен згадати про системи та інструменти, результати сканування, оцінки вразливості, деталі висновків тощо.

Написання першої чернетки. Коли у тестера готові усі необхідні інструменти та інформація, він може почати перший проект. Перш за все, він повинен написати перший проект у деталях - згадуючи про всі дії, процеси та досвід.

Огляд і завершення. Після складання звіту він має бути переглянутий спочатку самим розробником, а потім його старшими наставниками або колегами, які, можливо, допомогли йому. Під час перегляду очікується, що рецензент перевірить кожну деталь доповіді та знайде будь-який недолік, який необхідно виправити.

Зміст звіту про тестування на проникнення. Нижче наведено типовий вміст звіту про тестування проникнення:

• Обсяг робіт.

• Цілі проекту.

• Припущення.

• Хронологія.

• Резюме результатів.

• Резюме рекомендацій.

- Методика.

• Планування.

• Експлуатація.

• Звітність.

- Докладні результати.

• Детальна інформація про систему.

• Інформація про сервер Windows.

• Список літератури.

• Додатки.

Швидкий розвиток Інтернету змінив спосіб життя кожного. У ці дні більшість приватних і громадських робіт залежать від Інтернету. Всі урядові таємні робочі плани та операції базуються на Інтернеті. Все це зробило життя дуже простим і легкодоступним. Але з перевагами, є також недоліки цього розвитку, тобто поява злочинних хакерів. Немає геополітичних обмежень цих злочинних хакерів, вони можуть зламати будь-яку систему з будь-якої частини світу. Вони можуть пошкодити конфіденційні дані та кредитну історію. Тому, концепція етичного хакера розвивалася, щоб захиститися від злочинних хакерів.

10. Збір інформації

Збір інформації є ретельним процесом, за допомогою якого ви знаходите інформацію, яка може бути корисною при проведенні пізніх етапів вашого тестування. Оскільки ми живемо в інформаційному віці, процес триває деякий час, але час витрачається, тому що можна знайти все, що ви хочете знати про кого-небудь або будь-яку компанію, якщо ви знайдете час, щоб скористатися правильними інструментами і задаєте правильні запитання.

Інформація, зібрана про ціль, може допомогти уточнити кроки, які будуть приведені пізніше. Під час цього процесу ви повинні намагатися використовувати стільки методів, скільки необхідно для спостереження та збору інформації про вашу мету. Ви повинні звертати особливу увагу на все, що може бути потенційно використане пізніше (хоча це вимагає певного досвіду, щоб знати, що корисно, а що ні). Зрештою, ви повинні мати можливість вибирати елементи, які можуть бути корисними пізніше в процесі тестування. Поки ви не розвинете своє "око" і не зможете ретельно виявити корисну інформацію, вивчіть, яку інформацію ви розкриваєте, і деталі, які включені.

Втрата контролю інформації. З точки зору клієнта, може бути кілька негативних результатів від збору інформації щодо їх інфраструктури та ділових операцій:

Бізнес-втрати. Якщо клієнти або постачальники виявляють, що їхня інформація або інші дані не забезпечені належним чином, вони можуть легко знищити їхню впевненість і змусити їх піти в інше місце.

Витік інформації. Це включає інформацію, яку свідомо чи випадково оприлюднюють, наприклад, інформацію про проект, дані про працівників, особисті дані, фінансову інформацію або будь-яку з багатьох можливостей.

Втрата конфіденційності. Це особливо погана ситуація, коли інформація, яка повинна бути конфіденційною, розкривається. Найбільша загроза при цьому полягає не тільки в втраті довіри, але й до юридичних наслідків.

Корпоративне шпигунство. Інформація, яка розкривається в процесі дослідження, також може бути виявлена фінансовими та іншими конкурентами, які шукають деталі про те, що робить компанія.

На щастя, або, на жаль, в залежності від обставин, для отримання інформації про цілі доступно багато ресурсів. Ця інформація чекає на те, щоб ви провели дослідження щодо цілі та поклали всю інформацію, яку ви збираєте разом, щоб намалювати фотографію своєї жертви, або у випадку тестування на проникнення, вашу мету оцінки.

Класифікація типів інформації. Як правило, при дослідженні клієнта ви прагнете зібрати якомога більше інформації з безлічі різних джерел. Ви можете розраховувати на те, щоб знайти багато інформації про ціль, у тому числі:

Технічна інформація, така як інформація про операційну систему, інформацію про мережу, наявні програми, діапазони IP-адрес і навіть інформацію про пристрої. Крім того, ви можете розраховувати на пошук веб-камер, систем сигналізації, мобільних пристроїв та багато іншого.

Адміністративна інформація, така як організаційна структура, корпоративна політика, процедури найму, деталі співробітників, телефонні довідники, інформація про постачальників та багато іншого.

Фізичні деталі, такі як дані про місцезнаходження, дані про об'єкт, дані про людей та соціальні взаємодії з окремими особами.

Очікуйте, що ви зможете переглядати деталі розташування об'єкта за допомогою простого спостереження або за допомогою ресурсів, таких як Google Street View, щоб отримати уявлення про макет області.

У цих категоріях існує величезна кількість інформації, яку необхідно виявити. Питання в тому, наскільки це корисно і скільки ви могли б оглядати. Насправді, будьте готові відчути те, що називається "інформаційним перевантаженням", де вас переповнює кількість даних, які збираються до того моменту, коли вона не може бути оброблена ефективно.

Пам'ятайте, що занадто багато інформації може бути небезпечним. Легко стати настільки захопленим тим, що виявляється, що ви в кінцевому підсумку

збираєте інформацію, яка може навіть не бути корисною. Дізнайтеся з вашого збору інформації та з досвіду, який ви отримуєте на пізніших етапах, яка інформація є найбільш корисною і яка може бути меншою.

Класифікація методів збору. Під час етапу збору інформації ви повинні мати змогу сформулювати стратегію атаки, а також зрозуміти, яку інформацію оприлюднює організація. Збір інформації зазвичай поділяється на три категорії.

Пасивні. Пасивні методи - це ті, які не взаємодіють або не залучають ціль. Не залучаючи цілі, сподіваємося, що їм недостатньо інформації або взагалі не відомо про наближення атаки.

Активний. Методи, які підпадають під цю категорію - це телефонні дзвінки компанії, довідкова служба, співробітники або інший персонал. Все, що вимагає від вас активного залучення цілі, вписується в цю категорію.

Збір відкритих вихідних даних (Open source intelligence, OSINT). Що стосується збору інформації, то відкритий або пасивний збір інформації є найменш агресивним. В основному, процес спирається на отримання інформації з тих джерел, які зазвичай є загальнодоступними і відкритими. Потенційні джерела включають газети, веб-сайти, дискусійні групи, прес-релізи, телебачення, соціальні мережі, блоги та безліч інших джерел.

Вивчення веб-присутності компанії. Хорошим місцем для початку збирання інформації про цілі є їхній власний веб-сайт. Веб-сайти представляють спосіб організації інформування громадськості про те, що вони роблять, чому вони існують, та багато інших відомостей.

Переглядаючи веб-сайт, знайдіть такі відомості, які можуть бути корисними.

Адреси електронної пошти. Слідкуйте не тільки за адресами електронної пошти в цілому, але й за будь-якою адресою, яка може привести до конкретної особи або до певного відділу. Перший тип адреси може бути корисним для орієнтації на осіб для атак соціальної інженерії, таких як фішинг, а другий - для отримання інформації про проекти або структуру відділів.

Фізичні адреси. Будь-яка фізична адреса може дати уявлення не тільки про те, де є окремі офіси, але й де можна виконувати певні функції, такі як доставка, обробка замовлення або навіть основний офіс. Крім того, якщо ви збираєтеся виконувати фізичні оцінки безпеки та проникнення, ви зможете використовувати фізичні адреси разом з програмами зіставлення або Google Street View для перегляду приміщень здалеку, щоб спланувати атаку.

Кар'єра. Багато компаній розміщують інформацію про роботу на своїх веб-сайтах як частину звичайних операцій із залучення нових працівників. Хоча така практика розміщення цієї інформації не обов'язково є поганою ідеєю, вона може стати проблемою у випадку неправильної обробки. Компанії, які публікують такі речі, як технічні завдання, можуть спокуситися розміщувати окремі елементи, такі як «досвід Active Directory» або «досвід Windows Server 2012» разом з іншими деталями. Це може здатися гарною ідеєю, щоб надати ці деталі, але пентестер може поглянути на цю інформацію і швидко визначити, яку технологію компанія має «в будинку», оскільки це єдина причина, через яку вони будуть шукати людей із зазначеним досвідом.

Інформація про продукт, проект або послугу. Хоча це не велика проблема, якщо ви збираєтеся виконувати атаку соціальної інженерії, вивчення жаргону та типів речей, які компанія робить, можуть допомогти вам переконати цільового працівника, що ви робите законні запити на інформацію.

Тепер у вас є коротка ідея про те, що шукати з веб-сайту, але проблема полягає в тому, що отримання цієї інформації з особливо великого веб-сайту може зайняти багато часу. На щастя, є способи, щоб прискорити цей процес або принаймні допомогти вам у вашому зборі інформації.

Перегляд веб-сайту в автономному режимі. Вивчення веб-сайту є чудовою ідеєю, але що, якщо ви могли б вивчити його в автономному режимі на вашому комп'ютері? Ці речі були б набагато простішими, тому що ви можете шукати файли для текстових рядків, шаблонів, різних розширень файлів і навіть вмісту, який, як вважалося, приховано в деяких випадках. Програми, які виконують цю функцію, зазвичай називаються завантажувачами веб-сайтів,

іноді також відомими як сканування веб-сайтів, і багато з них створені тільки для цієї мети. Одна з цих утиліт називається BlackWidow для платформи Windows. Ви вказуєте BlackWidow на веб-сайті, надавши адресу, і коли процес розпочнеться, програма перейде до завантаження.

Альтернативою BlackWidow є використання Wget, яка доступна як на Linux / Unix, так і на Microsoft Windows.

Вправа 10.1. Використання Wget для завантаження веб-сайту.

Wget - утиліта, яка є спільною для платформ Linux і Unix і є основним елементом встановлення за замовчуванням обох ОС. До недавнього часу не було клієнта Wget для Windows, але це було вирішено.

Завантажте весь веб-сайт у папку з тим же ім'ям на своєму комп'ютері, використовуючи це:

sudo wget -m http: // <ім'я веб-сайту> Опція –m - це дзеркало, як у “дзеркальному веб-сайті”.

Якщо ви хочете завантажити сайт повністю, можна скористатися наступним:

wget -r --level = 1 -p http: // <назва веб-сайту>

Ця команда говорить: “Завантажте всі сторінки (-r, recursive) на веб-сайті плюс один рівень (– level = 1) і отримайте всі компоненти, такі як зображення, які складають кожну сторінку (-p).”

Пошук субдоменів. Тепер давайте подивимося на іншу річ, яку потрібно враховувати під час аналізу веб-сайту: субдомени.

Субдомени - це розділ назви основного веб-сайту. Наприклад, субдомен Microsoft.com буде support.microsoft.com або beta.microsoft.com. У реальному світі вам доведеться ввести повне ім'я або натиснути посилання, щоб дістатися до цих субдоменів. Отже, чому компанія робить це як стандартну практику? Добре, вони можуть зробити це просто для того, щоб організувати їхній контент трохи краще, надаючи різні функції або відділи своїм власним підсайтом, яким вони керують. Однак, компанії можуть також через субдомен

сайти "приховати" зміст, вважаючи, що неясність через безпеку є гарною ідеєю (це не так).

Отже, як можна легко знайти ці субдомени? У вашому розпорядженні є кілька способів, але давайте подивимося на один з веб-сайтів, відомих як Netcraft. Netcraft - це веб-сайт, зараз ми будемо використовувати одну з його функцій, щоб знайти піддомени.

Вправа 10.2. Використання Netcraft для визначення піддоменів.

Для цієї вправи ви будете використовувати веб-сайт www.netcraft.com для перегляду інформації про цільовий сайт.

1. Перейдіть на веб-сайт www.netcraft.com.

2. У вікні Running box введіть www.microsoft.com.

3. Натисніть Enter.

4. Перегляньте інформацію в результатах.

Зверніть особливу увагу на інформацію про IP-адресу, ОС та веб-сервер, оскільки кожен з них буде корисним для цілі на атаку пізніше.

Пошук веб-сайтів, які більше не існують. Що б ви зробили, якщо хочете подивитися веб-сайт, який більше не існує? Або стару версію існуючого веб-сайту? За допомогою веб-сайту, відомого як Archive.org, ви можете використовувати функцію, відому як машина Wayback. За допомогою машини Wayback можна знайти архівні копії веб-сайтів, з яких ви можете вивчати та, можливо, витягувати інформацію та використовувати її. Можна знайти копії старих каталогів компанії, технічну інформацію, інформацію про проект і клієнтів, і багато іншого.

Вправа 10.3. Пошук архівованого веб-сайту за допомогою машини Wayback.

У цій вправі використаємо машину Wayback для перегляду архівованої версії веб-сайту.

1. Перейдіть на сторінку www.archive.org.

2. У вікні біля машини Wayback введіть назву веб-сайту для перегляду. Для цього введіть www.microsoft.com.

3. Натисніть огляд історії.

4. У результатах ви побачите роки у верхній частині та календарні дні під ним. Натисніть день, щоб переглянути старі версії.

Ви можете налаштувати дату, просто натиснувши рік зверху, а потім натиснувши день року, щоб переглянути веб-сайт у цей день.

Збір інформації з пошукових систем. Одна з речей, які можуть допомогти вам у пошуку корисної інформації - це ваша улюблена пошукова система. Пошукові системи показали себе незамінними джерелами для пошуку та доступу до інформації. Однак, наскільки це корисно, більшість людей використовує лише невелику частину потужності пошукової системи, просто ввівши термін і натиснувши результати. Для нас цього недостатньо, тому ви вийдете за межі цього. Пошукові системи, такі як Google і Bing, а також інші, можуть забезпечити легкий доступ до великої кількості інформації, яку важко знайти інакше. Інколи клієнт може захотіти зберігати певну інформацію в таємниці, але з правильним ноу-хау ви можете знайти цю інформацію і скористатися нею.

Пошук з Google. Ми спеціально зупинимося на пошуку Google, оскільки це, можливо, найповніша і популярна пошукова система. Злам з Google не є нічим новим; насправді, здатність робити це існує в службі протягом тривалого часу. Просто багато користувачів не знають про його присутність або як його використовувати. Завдяки зламу з Google можна витягувати інформацію таким чином, щоб отримувати такі елементи, як паролі, певні типи файлів, чутливі папки, портали входу, інформацію про конфігурацію та інші дані.

Ось оператори, які дозволяють:

– *cache* - це ключове слово, яке відображатиме версію веб-сторінки, яку Google містить у своєму кеші, замість відображення поточної версії.

Використання: ***cache***: <ім'я веб-сайту>

– *link* використовується для переліку будь-яких веб-сторінок, які містять посилання на сторінку або сайт, вказаний у запиті.

Використання: ***link***: <назва веб-сайту>

– *info* містить інформацію про перераховані сторінки.

Використання: ***info***: <назва веб-сайту>

– ***site*** обмежить пошук у вказаному місці.

Використання: **<keyword> site:**< назва веб-сайту >

– allintitle повертає сторінки з вказаними ключовими словами в назві.

Використання: allintitle: <ключ>

– allinurl повертає результати з певним запитом у URL-адресі.

Використання: allinurl: <ключ>

Якщо ви не знайшли рішення або хочете заглянути в більш просунуті запити, я пропоную вам звернутися до бази даних Google Hacking (GHDB) на сайті www.hackersforcharity.com.

Отримання сповіщень про пошукові системи. Ще однією особливістю пошукових систем, про які ви, можливо, не знаєте, але повинні враховувати, як частину пошуку інформації, є сповіщення. Повідомлення - це функція, яка є в багатьох пошукових системах, які сповіщають вас про те, що було опубліковано те, що відповідає критеріям пошуку. Розгляньте можливість використання сповіщень, щоб стежити за пошуком, коли ви працюєте над іншими аспектами вашого тесту. На рисунку 10.1 показано приклад сповіщення Google.

Вправа 10.4. Використання сповіщень Google для оповіщення про інформацію

У цій вправі ви будете проходити процес налаштування та зміни оповіщення Google.

1. Перейдіть до веб-переглядача www.google.com/alerts.

2. Введіть пошуковий запит, який бажаєте отримати. Як тільки ви введете свій пошук, з'явиться зразок попередження. Якщо результати неприйнятні, змініть свій пошук. Ви можете скористатися Google, щоб покращити або конкретизувати свій пошук, якщо це потрібно.

3. Введіть дійсну адресу електронної пошти, яку Google використовуватиме, щоб надіслати вам результати запиту. Рекомендується

створити безкоштовний обліковий запис або спеціальний обліковий запис, щоб отримати ці сповіщення, щоб полегшити їх керування. Ви повинні підтвердити цей пошук, натиснувши посилання в електронному листі, який Google надсилає вам. Тепер ваше сповіщення завершено.

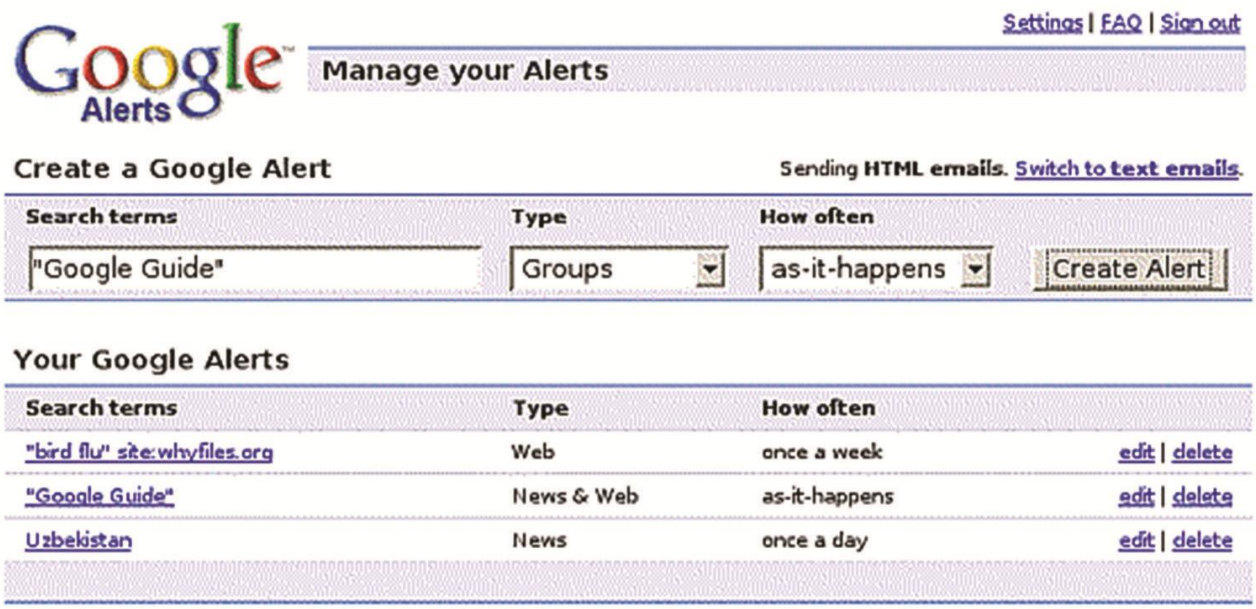

Рисунок 10.1 – Сторінка Google Alerts

Орієнтація на пошук працівників. На цьому етапі ви могли б легко зібрати багато інформації, але давайте зосередимося на одній з цих частин інформації: люди. Під час вашого пошуку, а також під час інших розслідувань, ви, мабуть, розкриєте імена осіб, які працюють за ціллю. Якщо ви це зробите, варто зробити певні дослідження щодо цих осіб, щоб вияснити, що ви можете дізнатися.

Так, ви можете використовувати Google для отримання інформації про когось, але є також набагато більше цільових ресурсів, спеціально призначених для дослідження людей, як платних, так і безкоштовних послуг. Багато з платників пропонують інформацію, яку просто збирають з інших вільних джерел, тоді як інші пропонують унікальну інформацію.

Нижче наведено кілька варіантів.

Spokeo: www.spokeo.com

Pipl: www.pipl.com

Yasni: www.yasni.com

Zabasearch: www.zabasearch.com

Intelius: www.intelius.com

ZoomInfo: www.zoominfo.com

Infospace: www.infospace.com

kgb: www.kgbpeople.com

People: www.peepdb.com

Radaris: www.radaris.com

Кожна з цих пошукових систем надає інформацію про осіб, але не лякайтеся, якщо ви не знайдете свою мету в одній з них, просто спробуйте іншу.

Також пам'ятайте, що інформація, яку ви знаходите про людину, завжди повинна бути перевірена та порівняна з іншими джерелами, щоб визначити її точність. Небажано, щоб інформація в споживчих послугах була або несвіжою, ні помилковою.

Нарешті, коли ви пробуєте скористатися переліченими тут інструментами та веб-сайтами, переконайтеся, що ви маєте дозвіл на пошук деталей іншої особи. Хоча це навряд чи відбудеться, цілком можливо, що в деяких місцях занадто цікава людина може порушити місцеві закони.

Відкриваючи місце розташування. Звичайно, люди в організації повинні створити свої офіси і робочі місця, так як ви можете дослідити це більше?

Адресна інформація повинна бути тим, що виявляється під час розслідування, це часто можна знайти на веб-сайтах. Крім того, знання фізичного розташування компанії може сприяти зусиллям з дайвінгу, соціальній інженерії та іншим зусиллям, які ще потрібно обговорити. На рисунку 10.2 показаний приклад того, що можна отримати з Google Street View.

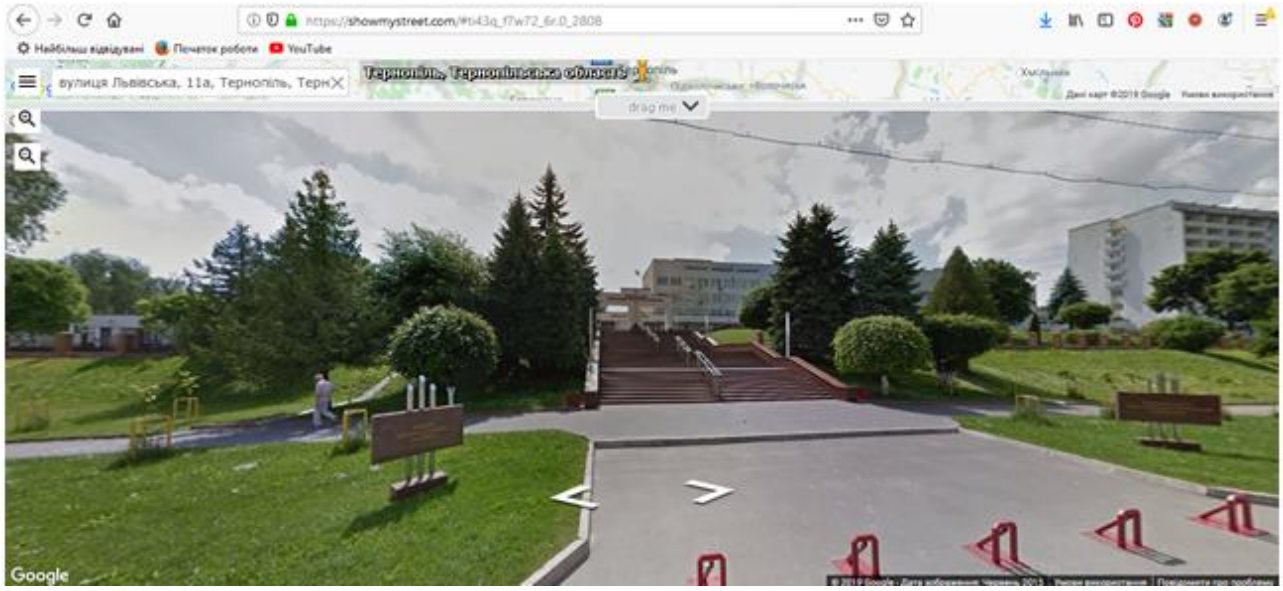

Рисунок 10.2 – Google Street View

Так, що можна зробити, якщо у вас є адреса? Як виявилося, багато веб-сайтів і технологій готові допомогти вам.

Google earth. Ця популярна утиліта для супутникових зображень доступна вже більше 12 років, і за цей час вона стала кращою, з доступом до додаткової інформації та збільшенням кількості інших даних.

Google Maps. З тієї ж причини, що і **Google earth**, **Google Maps** може надати багато інформації, включаючи інформацію про область та подібні дані.

Google Street View. Цей веб-додаток дозволяє переглядати підприємства, будинки та інші місця з точки зору автомобіля. Використовуючи цю утиліту, багато спостерігачів побачили такі деталі, як люди, входи і навіть особи, які працюють.

Webcams. Вони дуже поширені, і вони можуть надати інформацію про місця або людей. Насправді такі інструменти, як популярна пошукова система Shodan (www.shodan.io), мають можливість шукати спеціально веб-камери, а також інші пристрої.

Використання цих інструментів разом з хакером Google може дозволити вам знайти величезну кількість інформації за короткий час з мінімальними зусиллями.

Соціальні мережі. Соціальні мережі - чудовий інструмент для спілкування з друзями та сім'єю, але в неправильних руках хакери можуть бачити всі особисті та професійні стосунки, які хтось має.

Соціальні мережі стали не тільки надзвичайно плідними, але й надзвичайно цінним інструментом для збору інформації. Користувачам цих служб нормально обмінюватися інформацією, як випадково, так і навмисно. Для більшості, бажання бути в цих послугах з їхніми друзями та родиною є більш важливим, ніж будь-які потенційні витоки інформації, які можуть виникнути.

Із-за характеру цих послуг та їхньої тенденції до перекосу, до відкритості та легкості обміну інформацією, зловмисник не повинен виконувати велику кількість роботи, щоб дізнатися корисні подробиці про людей та відносини.

Очікуйте, щоб знайти всі види інформації про ці послуги, так що ви не зможете обробити все це. Зібрана інформація може бути корисною кількома способами, включаючи пошук інформації, яка може бути використана для соціальної інженерії осіб, використовуючи терміни та імена, які їм знайомі для створення почуття довіри.

Деякі з найбільш популярних сервісів соціальних мереж, які варто вивчити для отримання інформації про ціль, можуть бути ті, які вам вже знайомі:

Facebook. Найбільша соціальна мережа на планеті може похвалитися надзвичайно великою кількістю користувачів з великою кількістю груп для обміну інтересами. Крім того, Facebook використовується для входу або обміну коментарями по безлічі веб-сайтів, зробивши його ще більш доступним.

Twitter. Одним з інших надзвичайно популярних соціальних мереж є Twitter. Він має мільйони користувачів, багато з яких публікують оновлення кілька разів на день. Twitter пропонує мало безпеки, і ті функції, які він має в цій галузі, рідко використовуються. Користувачі Twitter, як правило, публікують багато інформації при цьому мало або зовсім не думаючи про значення того, що вони публікують.

Google+. Це відповідь Google на популярний Facebook. Хоча служба ще не досягла популярності Facebook, на сайті є велика кількість інформації, яку можна шукати і використовувати.

LinkedIn. Сайт є платформою соціальних мереж для шукачів роботи, і тому має історію зайнятості, контактну інформацію, навички та імена тих осіб, з якими людина може працювати або працювала.

Instagram. Це послуга, призначена для обміну фотографіями та відео з іншими, і навіть розміщувати інформацію про такі послуги, як Facebook і Tumblr. Люди часто фотографують та розміщують відео на цій службі, незважаючи на те, чи повинні вони розміщувати їх, або якщо вони становлять ризик для безпеки, перебуваючи в публічному просторі.

Tumblr. Це ще одна служба, подібна до Twitter, яка також може використовуватися для обміну інформацією, яка в деяких випадках повинна зберігатися конфіденційною.

Youtube. Хоча не розглядатися, як щось на зразок Facebook і Instagram, витрачати час на вивчення служби може виявитися корисним. Це не рідкість тикати навколо і знайти багато відео, розміщені на сайті, показуючи речі, які найкраще зберігаються в конфіденційності.

Ви знаєте, що існує декілька соціальних мереж, у яких можна шукати інформацію, кожна зі своєю вбудованою функцією пошуку, але ви можете зробити ще більше з цією інформацією? Відповідь «так» - не тільки ви можете прочитати інформацію про людей, але ви можете знайти її на основі географічних даних. Насправді, один інструмент дозволяє не лише знайти інформацію, розміщену в соціальних мережах, але й розміщувати цю інформацію на світовій карті, що показує, коли і де було розміщено інформацію. На рисунку 10.3 показано інструмент Echosec (http://app.echosec.net). Echosec - це веб-сайт, який дозволяє зосередитися на певних місцях і знаходити інформацію про повідомлення соціальних мереж, які було надіслано з цього місця. Ще більш дивовижним і потужним є той факт, що

ви можете використовувати інструмент для пошуку за конкретними іменами в Twitter і Instagram, що ще більше полегшує отримання інформації.

Рисунок 10.3 – Echosec

Щоб скористатися цією послугою, потрібно лише місце розташування та трохи часу. На рисунку 10.4 показано пошук місця в Лас-Вегас.

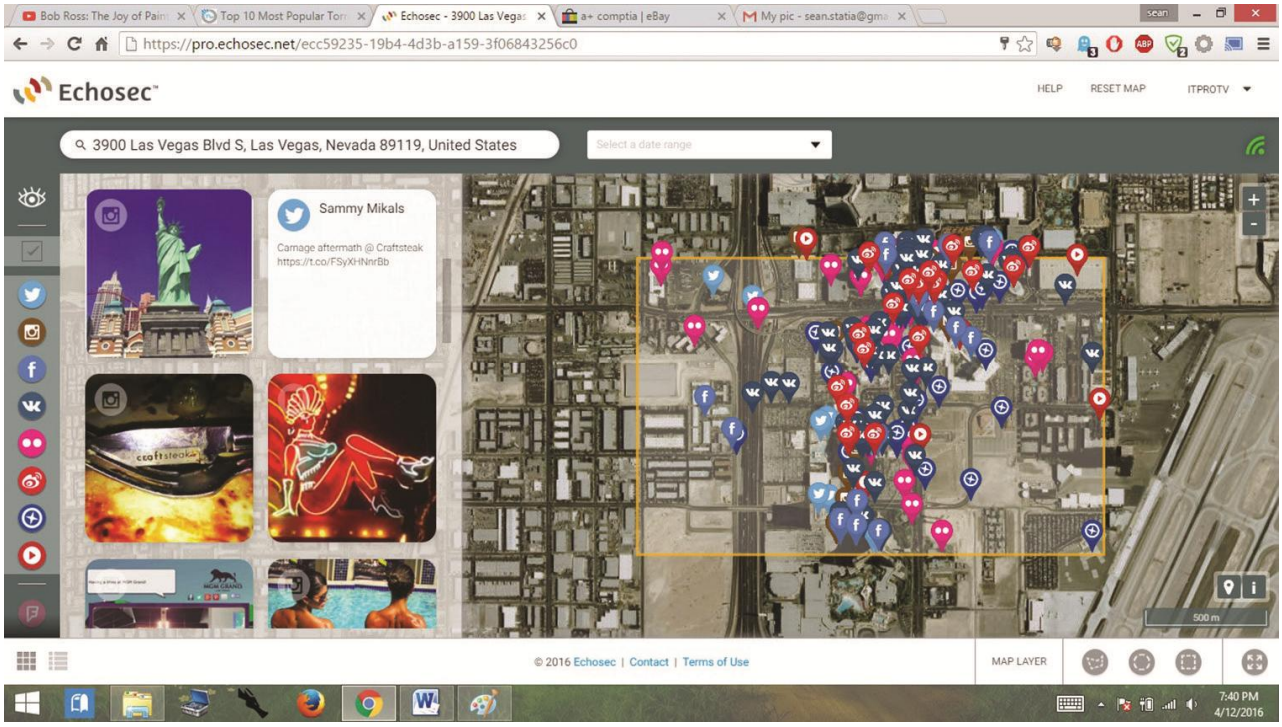

Рисунок 10.4 – Зразок пошуку в Echosec

Вправа 10.5. Використання Echosec.

Щоб скористатися програмою Echosec для перевірки повідомлень соціальних медіа, розміщених з певного місця, виконайте наведені нижче дії.

1. Перейдіть до https://app.echosec.net у веб-переглядачі.

2. Введіть адресу в поле розташування або перетягніть карту до місця розташування та налаштуйте масштаб, щоб отримати потрібне місце розташування у фокусі.

3. Натисніть кнопку "Вибрати", розташовану в нижній частині сторінки. Намалюйте вікно навколо цільової області.

4. Прокрутіть сторінку вниз, щоб переглянути результати запиту.

Через те, як деякі люди використовують соціальні медіа, можливо, іноді в результатах пошуку для цієї служби відображаються графічні зображення. Хоча це не є звичайним явищем, це траплялося час від часу.

Переглядаючи фінансові послуги. Коли ви орієнтуєтеся на певні організації, зокрема ті, які можуть публічно торгувати, є додаткові ресурси для збору інформації. Такі послуги, як Yahoo, Google, CNBC, USA Today і незліченна кількість інших, надають інформацію про компанію, яка може бути недоступною іншими засобами. Ця інформація надається для того, щоб інвесторам було легше отримувати інформацію про бізнес, а потім приймати обгрунтовані інвестиційні рішення. Однак, ця сама інформація може дати пентестеру або зловмисникові деякі приховані дорогоцінні камені інформації, які могли б просунути тест ще далі.

Щоб шукати інформацію на цих сайтах, просто перейдіть на свій вибір і введіть символ запасу, якщо він відомий, або введіть назву компанії на відповідному сайті.

Ви також можете запитати себе, коли переглядаєте ці сайти, хто є конкурентами цілі. Майже кожен діловий та інвестиційний сайт, який перераховує компанії, також скаже, хто є конкурентами компанії. Крім того, ви також можете використовувати той самий ресурс, щоб знайти сторонніх постачальників, з якими працює ціль. Чому вас цікавлять партнери компанії?

Якщо поглянути на партнера, ви можете розповісти вам про внутрішні дії вашої цілі призначення, якщо ви побачите замовлення на частину або послуги, які вони розміщують для будь-якого постачальника. У сфері безпеки ми називаємо цей висновок, або робимо припущення на основі непрямих доказів.

Під час аналізу цих ресурсів завжди слід шукати певні типи інформації, які можуть виявитися корисними, наприклад, такі.

Коли компанія почала працювати? Шукайте інформацію про розвиток компанії, яка може надати деталі майбутніх напрямків.

Як розвивалася компанія для того, щоб дати уявлення про свою бізнес-стратегію та філософію, а також корпоративну культуру?

Хто є керівниками організації? Це може дати можливість подальшого аналізу цих осіб. Іноді доступні місця розташування офісів та розподіл персоналу.

Дослідження сайтів працевлаштування. Сайти пошуку роботи можуть бути хорошими джерелами технічної та організаційної інформації. Якщо ви переглянули оголошення про вакансії, ви, без сумніву, помітили розділи об’яв і навичок. Не рідко можна знайти інформацію, наприклад, дані про інфраструктуру, інформацію про операційні системи та інші корисні дані. Пам'ятайте, що компанії, які займаються розміщенням посад, хочуть наймати кваліфікованих людей, і тому вони повинні переконатися, що вони просять належні навички - отже, їх включення в роботу.

Під час аналізу оголошень про вакансії слідкуйте за такою інформацією:

- вимоги та досвід роботи;

- профіль роботодавця;

- профіль співробітників;

- інформація про обладнання. Це надзвичайно часто зустрічається в профілях; шукайте такі ключові слова, як Cisco, Microsoft та інші, які можуть містити номери моделей або версій.

– інформація про програмне забезпечення;

– пошук електронної пошти.

Електронна пошта є інструментом, на який сьогодні покладається кожен бізнес. Для зловмисника та пентестера інформація, що передається по електронній пошті, є важливою і цінною для зловмисника, який шукає інформацію всіх типів. Для пентестера або зловмисника існує багато інструментів для виконання цієї функції.

Одним з інструментів, який корисний для збору інформації з електронної пошти, є PoliteMail. Він створює та відстежує повідомлення електронної пошти з поштового клієнта. Ця властивість може виявитися корисною, якщо ви можете отримати список електронних листів від цільової організації. Після того, як у вас є такий список, ви зможете надіслати електронний лист у список, який містить зловмисне посилання. Після того, як лист буде відкрито, PoliteMail повідомить вас про подію для кожного.

Ще одна утиліта, про яку варто згадати, - WhoReadMe. Ця програма призначена для відстеження електронних листів, але також надає таку інформацію, як ОС, тип веб-переглядача та елементи керування ActiveX, встановлені на системі жертви. Ця інформація буде надзвичайно корисною для націлювання на атаку пізніше з набагато більшою точністю.

Вилучення технічної інформації. На щастя, в сучасному світі існує безліч способів зібрати технічну інформацію про системи в організації, на яку ви орієнтуєтеся.

Whois - стара, але дуже корисна утиліта. Спочатку розроблена для операційної системи Unix утиліта стала частиною Linux і доступна, як безкоштовна для Windows. Крім того, утиліта доступна для використання на будь-якій кількості веб-сайтів, які можна знайти за допомогою простого веб-пошуку.

Whois призначений, щоб дозволити вам збирати інформацію про доменне ім'я або веб-адресу. Результати команди дадуть інформацію про власника, інформацію про IP, інформацію про DNS та інші дані, які можна використовувати.

Вправа 10.6. Робота з Whois

Щоб виконати цю вправу, потрібно завантажити Whois для Windows у http://technet.microsoft.com/en-us/sysinternals/ bb897435.aspx.

1. Після завантаження файлу розархівуйте його в папку whois на робочому столі.

2. Утримуючи клавішу Shift і клацніть правою кнопкою миші папку whois; потім виберіть Відкрити вікно команд.

Вилучення технічної інформації.

3. У командному рядку введіть whois приклад:

Whois usatoday.com

4. Перегляньте деталі результатів.

Результати, які ви побачите, включатимуть декілька ключових деталей, які можуть бути корисними. Зокрема, шукайте інформацію про адресу, номери телефонів, імена та інформацію про сервер імен. Ця інформація повинна бути відзначена для подальшого використання.

Зростає кількість власників доменів, які користуються послугами, які роблять анонімною всю інформацію (за винятком інформації про сервер імен). Ці послуги погані для вас, як пентестера, оскільки їх використання не дозволяє отримувати інформацію, а для власників доменів вони є чудовою ідеєю і їх слід рекомендувати.

Тепер ви знаєте різні шляхи, які ви можете використати, щоб зібрати інформацію про вашу ціль. Ви можете ознайомитися з веб-сайтом цілі, знайти старі версії веб-сайтів, які більше не існують, використовувати пошукові системи, націлювати співробітників на пошуки людей, знаходити інформацію про адресу та інформацію про місцезнаходження, досліджувати сайти соціальних мереж, вивчати фінансову інформацію, досліджувати робочі місця, пошук електронної пошти, витяг технічної інформації з Whois та проведення трюків соціальної інженерії.

Дослідження обов'язково повинні розглядати детальний процес ідентифікації інформації, яка може бути корисною для подальших етапів вашого тестування. Процес дослідження та розкриття деталей щодо вашої цілі

займе деякий час, але час буде добре витрачений, якщо він допоможе вам пізніше вдосконалити свої дії, щоб зробити їх більш ефективними. Крім того, майте на увазі, що інформація, яку ви знайдете, повинна бути чітко задокументована, щоб клієнт міг вирішити, чи вони виявляють занадто багато зайвого.

11. Сканування портів

Після того, як ви зібрали інформацію про свою ціль, настав час перейти до сканування. Сканування включає в себе визначення хостив (ping sweep), сканування портів і сканування вразливостей. Перелічення - це процес видобування важливої інформації з відкритих сторінок і інформації, яку ви знайшли під час сканування, наприклад, імена користувачів, обмін даними, групова інформація та багато іншого.

Сканування є досить широким терміном, це термін, що охоплює багато різних методів, які є певною формою типу сканування.

Перевірка пінгу робочих систем. Це сканування призначене для пошуку підмережі або списку IP-адрес з наміром ідентифікувати, які адреси мають системи, які працюють за нею. Ті, які визначені як такі, що знаходяться на межі, можуть бути націлені на більш конкретні дії пізніше.

Сканування портів - це форма сканування, яка спрямована на окремі IP-адреси та спрямована на виявлення відкритих і закритих портів у певній системі. Кожен з відкритих портів може мати службу, пов'язану з нею, яка може бути використана пізніше.

Сканування вразливості виявляє слабкі сторони або проблеми в середовищі та генерує звіт про свої висновки.

Кожне з цих сканувань може ефективно використовуватися самостійно, але справжня сила кожного з них дійсно сильно проявляється, коли вони об'єднані. Подумайте про це так: пошук IP-адрес, які мають робочу систему за ними, подібний до пошуку дійсного номера телефону. Маючи дійсний номер телефону, у вас є лише невелика частина інформації, але дзвінок на цей номер і з'ясування того, що знаходиться на іншому кінці проводу, ще більш корисно знати. Кожен тип сканування нагадує частину великої головоломки, яку можна зібрати, щоб отримати більш чітке уявлення про загальну мету. Чим більш чітка картина цілі, тим більш точними можуть бути подальші атаки і дії. Крім того,

подібно до головоломки, у ваших скануваннях можуть бути «дірки», і ви повинні вгадати, що там було.

Ось короткий перелік речей, про які ви зможете отримати більше інформації:

– інформація про час сканування;

– IP-адреси систем, які перетворюються на «робочі», які включають не тільки комп'ютери, а й планшети, мобільні телефони, принтери, точки бездротового доступу тощо;

– списки відкритих і закритих портів на цільових системах;

– версії операційної системи, які можна отримати у багатьох випадках під час фази сканування (але будьте обережні, оскільки спроби ідентифікувати систему можуть збільшити ваш шанс виявлення);

– MAC-адреси;

– сервісна інформація;

– дані портів;

– інша мережна інформація в залежності від ситуації.

Ви повинні очікувати, що будь-які дані, які ви збираєте під час цієї фази, будуть повноцінними і, ймовірно, вимагають справедливого або тривалого часу для розкриття та оцінки. Якщо ви раніше були уважними у зборі інформації, то в деяких випадках цей процес можна скоротити, оскільки ви можете зосередитися на певних пунктах.

Перевірка робочих систем. Якщо вам пощастило розкрити діапазони IP у фазі збору розвідувальних даних, у вас є список потенційно дійсних цілей для цього першого кроку. Для того, щоб ваше сканування було ефективним, потрібно знайти адреси, до яких додається щось, щоб вони могли бути ціллю. Один з найпростіших способів перевірити наявність живих систем - використовувати популярну функцію ping, як частину процесу, відомого як ping sweeps або ICMP scans. Pinging - це процес використання команди ping для визначення статусу даної системи, зокрема, чи відповідає вона. Якщо система відповідає команді ping, вона перебуває в режимі онлайн і може бути сканована

більш повно пізніше. Якщо немає відповіді, хост може бути фактично в автономному режимі або недоступним, і тому ви не можете отримати доступ до нього зараз. Насправді, процес pinging використовує те, що відоме як протокол керування повідомленнями Інтернету (ICMP), тому цей метод також називається скануванням ICMP. Процес працює за допомогою однієї системи для надсилання запиту ICMP ECHO до іншої системи. Якщо ця система працює, вона відповість, надіславши назад відповідь ICHO ECHO. Після отримання такої відповіді система підтвердила, що працює. Утиліта ping є корисною, тому що вона може повідомити вам не тільки про те, що система працює, але й швидкість пакетів від одного хоста до іншого, а також повертає інформацію про час життя (TTL). На рисунку 11.1 показані результати команди ping.

Pinging - це часто використовувана мережева діагностична утиліта. Однак, брандмауери та маршрутизатори досить часто блокують його на периметрі мережі, де зустрічається зовнішній світ та внутрішня мережа.

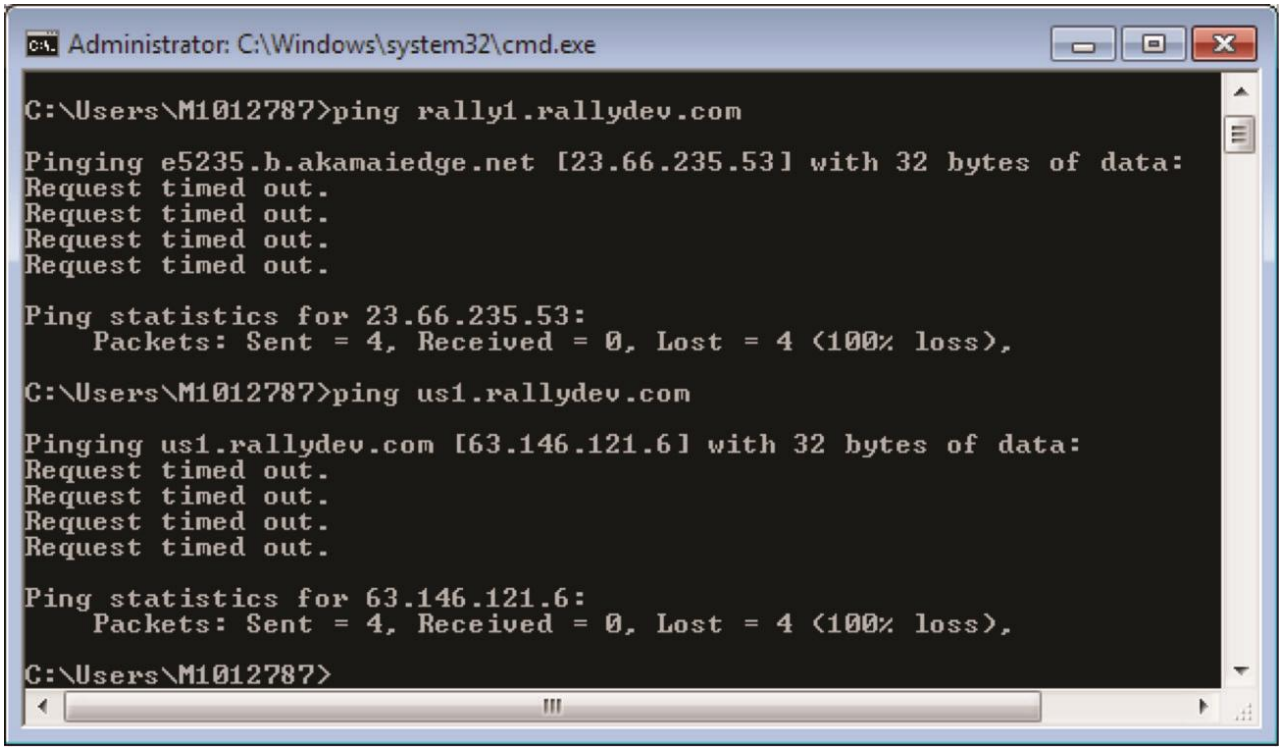

Рисунок 11.1 – Результат команди керування ping

Вправа 11.1. Використання утиліти ping.

У цій вправі ви перевірятимете, чи працює система за допомогою команди ping.

1. Відкрийте командний рядок.

2. Використовуйте формат ping <цільовий IP> або ping <цільове ім'я хоста>. Для цього виконайте команду ping www.microsoft.com.

3. Перегляд результатів.

Залежно від вашого конкретного підключення, ви повинні побачити чотири відповіді або спроби відповідей, причому всі чотири будуть успішними або один чи кілька не успішних, при цьому недоступний хост повідомлення. Якщо всі говорять про недоступність, ви маєте погану адресу / IP або систему, яка не працює.

Зверніть увагу, що, хоча ви можете використовувати ping для хоста по імені або IP-адресою, ви повинні використовувати IP в більшості випадків. Ми використовували тут лише ім'я для спрощення. На практиці, можна отримати відповідь, переглянувши IP, але не через ім'я хоста, що може привести до думки, що система недоступна, коли вона насправді працює. Однак DNS може бути недоступним за назвою, але це буде нормально працювати за допомогою IP.

Звичайно, ping - це важлива утиліта, але є й інші, які не тільки використовують команду ping. Два з інших варіантів - Angry IP і nmap. Хоча ping є гарним по відношенню до одного хоста, швидкий і легкий перегляд кількох систем за його допомогою є складним. Щоб зробити справу простішою, ви можете отримати інформацію по всій підмережі, використовуючи один з цих двох інструментів. На рисунку 11.2 показаний інтерфейс Angry IP.

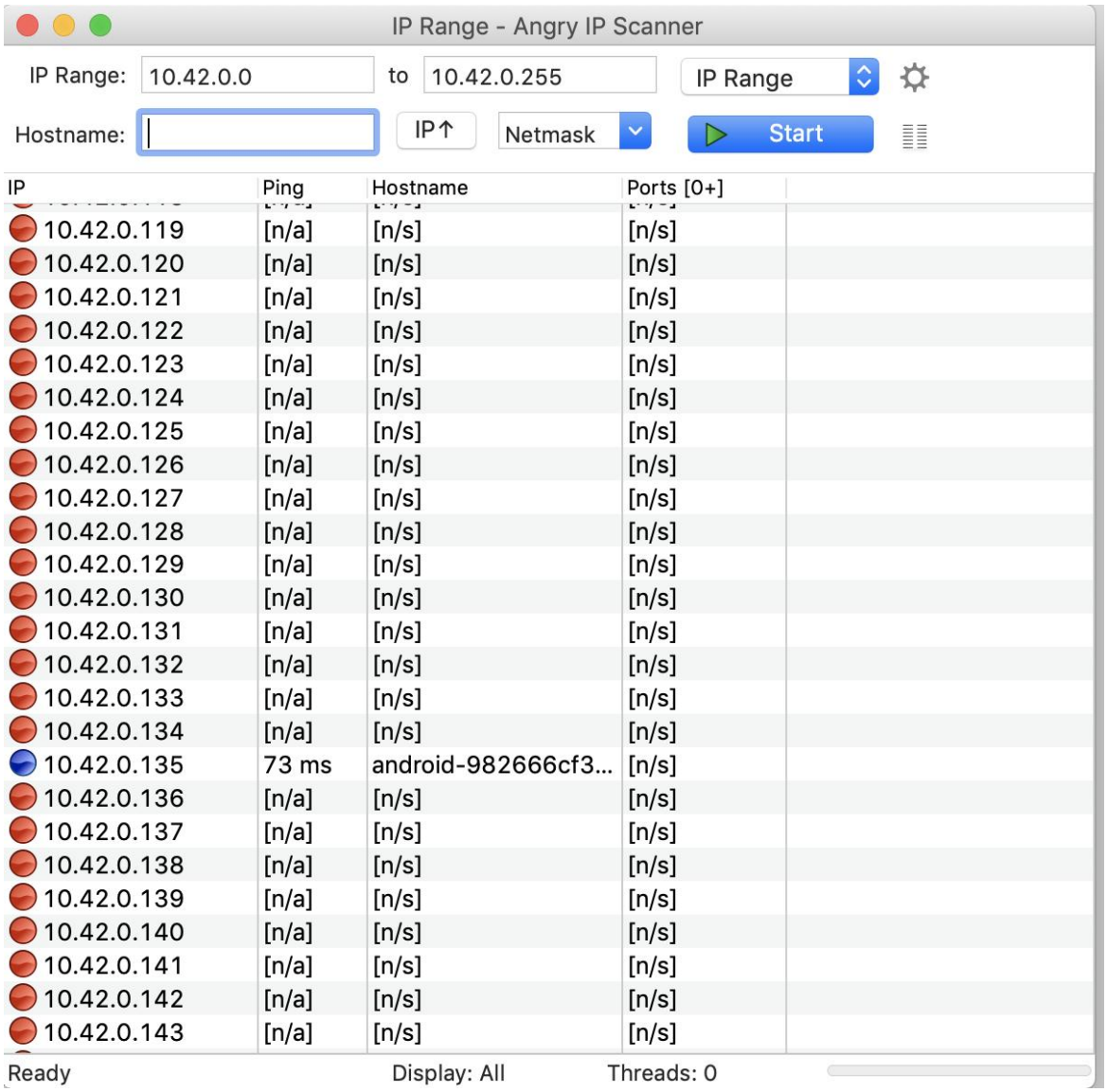

Рисунок 11.2 – AngryIP

Вправа 11.2. Використання AngryIP

У цій вправі використаємо Angry IP, щоб перевірити, чи існують декілька хостів. Щоб виконати цю вправу, перейдіть на сторінку www.angryip.org і завантажте та встановіть програму Angry IP. Після встановлення перейдіть до кроку 1.

1. Початок Angry IP.

2. У діапазоні IP, введіть початкову і кінцеву IP адресу для сканування. Найпростіший спосіб зробити це, запустити ipconfig на вашій системі і використовувати його для визначення діапазону мережі. Якщо у вас є ряд IP-адрес, які вже є зручними з вашого попереднього збору інформації, то ви

можете також використати його. Або ви можете прийняти налаштування за замовчуванням у Angry IP прямо зараз.

3. Коли готова, натисніть кнопку Пуск.

4. Через кілька секунд перевірка повинна бути завершена, і ви можете переглянути діалогове вікно, в якому вказано, скільки хостів було відсканована та скільки є робочими.

Angry IP відомий як швидкий і ефективний сканер, який може швидко виконувати розгортка ping на всьому діапазоні мережі.

Давайте перейдемо до наступного рівня, запровадивши інструмент, який ви будете використовувати, як пентестер: nmap.

Nmap або "Network Mapper" - безкоштовна утиліта, яка використовується для виявлення мережі і доступна для всіх основних операційних систем. Утиліта використовується для всього, починаючи від виконання інвентаризації мережі до аудиту безпеки, а також від систем моніторингу. Nmap може використовуватися для визначення інформації про операційну систему, брандмауер або одну з багатьох інших характеристик.

На момент підготовки лекції найновіша версія nmap 7.40 була випущена в 20 грудня 2016 року.

Nmap має як інтерфейс командного рядка, так і інтерфейс GUI, відомий як Zenmap. Ми будемо використовувати Zenmap для більшої частини того, що ми робимо, а також командний рядок, щоб ви познайомилися з обома варіантами. Якщо ви хочете повністю розблокувати потужність nmap, ви повинні використовувати командний рядок. Багато опцій nmap доступні лише з командного рядка і фактично недоступні через GUI Zenmap. На рисунках 11.3 і 11.4 показані інтерфейси nmap.

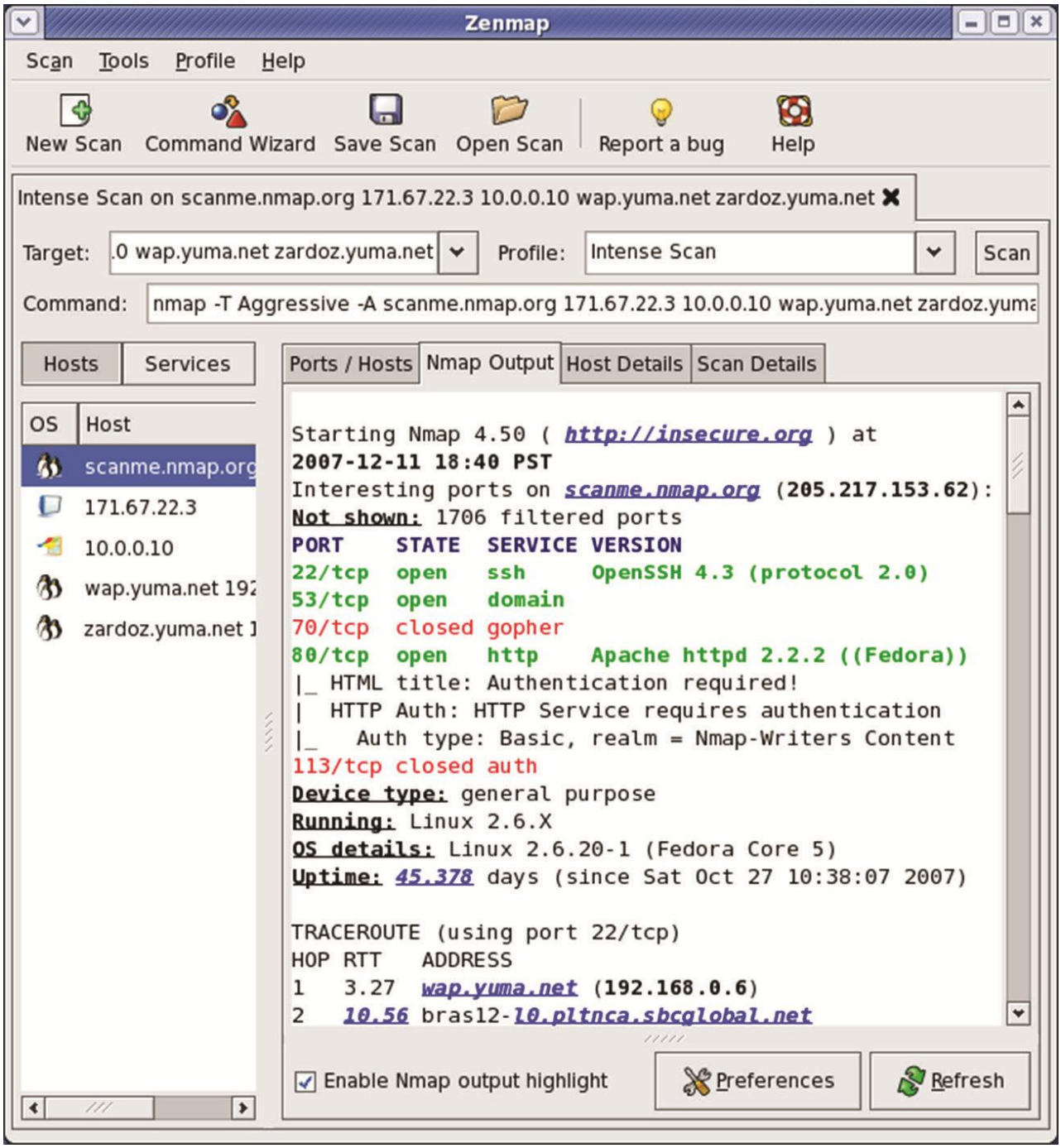

Рисунок 11. 3 – Повне сканування nmap

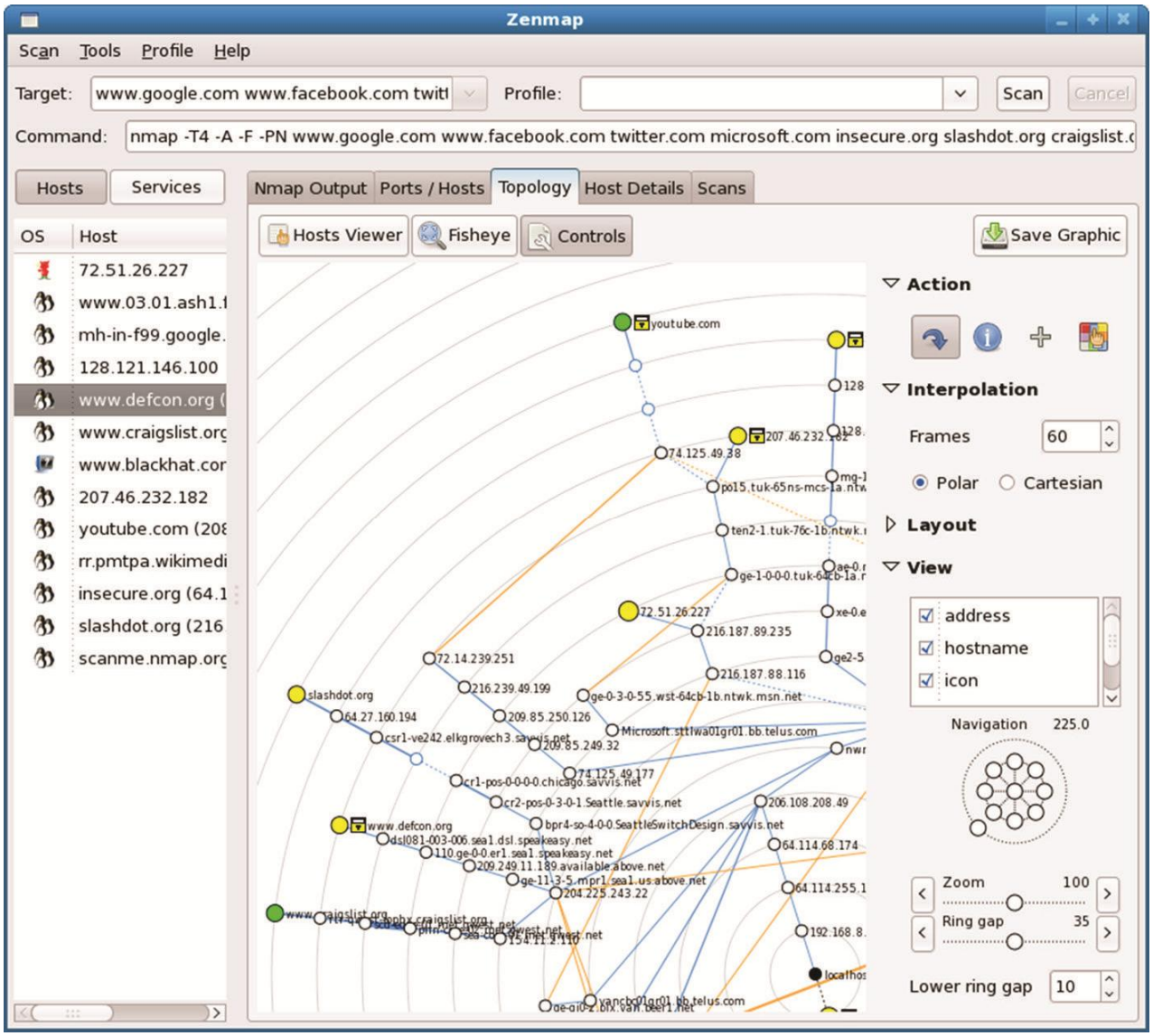

Рисунок 11.4 – Перегляд карти мережі в nmap

Вправа 11.3. Використання nmap для виконання пінгу.

У цій вправі ви будете використовувати nmap для визначення робочих хостів.

1. Відкрийте термінал.

2. У командному рядку введіть наступне:

Nmap –sP <ip адреса або діапазон>

Наприклад, у моїй мережі діапазон адрес для сканування буде виглядати так:

Nmap –sP 192.168.1.1-45

3. Натисніть Enter.

Зачекайте кілька секунд, і nmap поверне список хостів. Якщо команда успішно знайде робочий хост або хости, вона поверне повідомлення для кожної спроби про те, що IP-адреса збігається разом з MAC-адресою та постачальником мережевої карти, якщо вона зможе встановити цю інформацію.

Використовуючи nmap ви повинні пам’ятати, що команди залежать від регістру.

Крім того, перераховані тут команди, використано у ОС Windows, так само можуть використовуватися в Linux, Unix та Mac OS.

Виконання сканування портів. Після того, як ви знайшли робочі системи, настав час звернутися до більш точного дослідження цих систем через сканування портів. Простіше кажучи, сканування портів - це спосіб визначити, чи є порт «відкритим» або «закритим». Якщо порт відкритий, він може приймати з'єднання, а якщо він закритий, він не може. Сканування портів - це спосіб зворотного повороту дверних ручок на кожному порту, щоб визначити, чи можна повернути дверну ручку (і пізніше отримати доступ).

Щоб надіслати щось певній службі в системі (наприклад, веб-серверу), зверніться до IP-адреси, а потім до порту. У випадку сценарію веб-сервера, це буде виглядати так для IP-адреси 192.168.14.42, як цільової системи:

192.168.14.42:80

У цьому прикладі я звертаюся до IP-адреси, а потім підключаюся до порту 80, як зазначено після двокрапки (:). Ця комбінація IP-адреси та порту зазвичай називається сокетом або мережним сокетом. На рисунку 11.5 показана схема сокетів на двох системах зв’язку.

Є 131070 портів, доступних для використання додатками та службами, але насправді 65535 для TCP і 65535 для UDP. Якщо програма використовує протокол TCP для надсилання й отримання даних, він буде підключатися і прив'язуватися до TCP-порту. Якщо він використовує протокол UDP для надсилання та отримання даних, він буде використовувати а порт UDP.

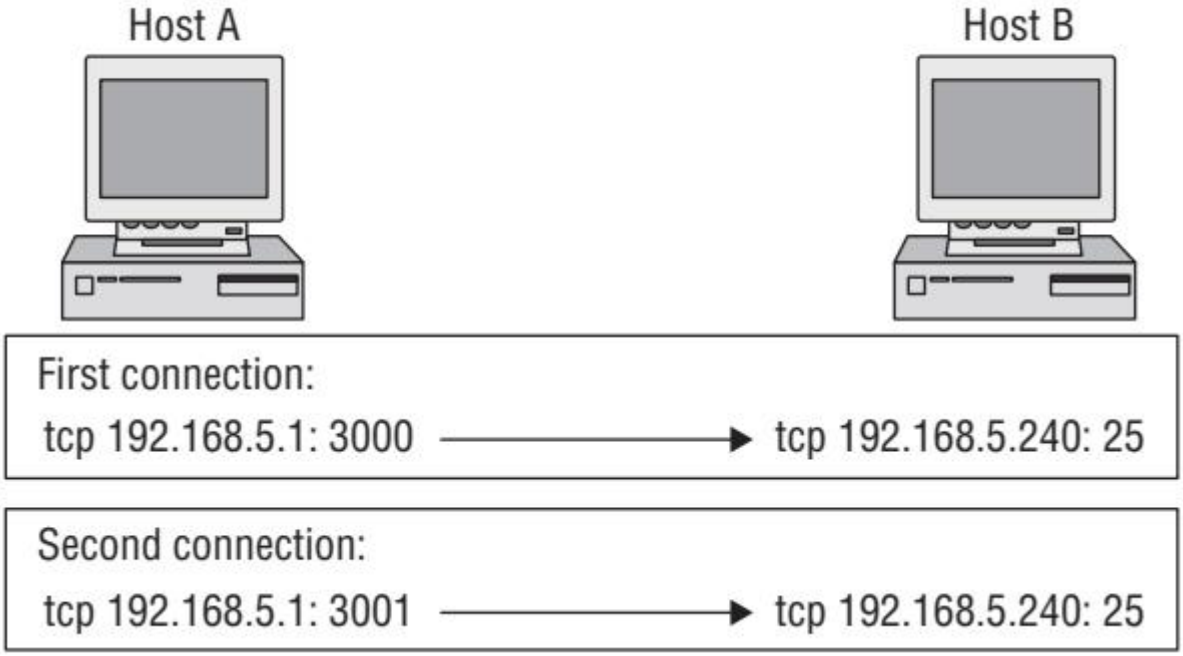

Рисунок 11.5 – Сокети двох систем

Відомі порти є найбільш поширеними для щоденних операцій і змінюються від 0–1023. У таблиці 11.1 наведено основні порти. Зареєстровані порти становлять від 1024 до 49151. Зареєстровані порти - це порти, які були ідентифіковані як такі, що використовуються іншими програмами, що працюють поза відомими портами. У таблиці 11.2 наведено перелік загальних зареєстрованих портів. Динамічні порти варіюються від 49152–65535. Вони доступні для підтримки трафіку додатків, який не був офіційно зареєстрований у попередньому діапазоні.

Таблиця 11.1 – Відомі порти

Порт	Протокол
20-21	FTP
22	SSH
23	Telnet
25	SMTP
42	WINS
53	DNS
80, 8080	HTTP

Порт	Протокол
88	Kerberos
110	POP3
111	Portmapper – Linux
123	NTP
135	RPC-DCOM
139	SMB
143	IMAP
161, 162	SNMP
389	LDAP
445	CIFS
514	Syslog
636	Secure LDAP

Таблиця 11.2 – Зареєстровані порти

Порт	Протокол
1080	Socks5
1241	Nessus Server
1433, 1434	SQL Server
1494, 2598	Citrix Applications
1521	Oracle Listener
2512, 2513	Citrix Management
3389 R	DP
6662-6667	IRC

Порти в системі можуть бути як TCP, так і UDP, і які з них можуть визначити форму сервісу. Під час сканування занотуйте номер порту, і чи це TCP або UDP, для подальшого використання. Протокол, орієнтований на з'єднання, TCP встановлює з'єднання, а потім перевіряє, що кожне повідомлення (відоме як пакет) відправляє його до призначення у правильному

порядку. Для цього TCP використовує тристороннє рукостискання, як показано на рисунку 11.6.

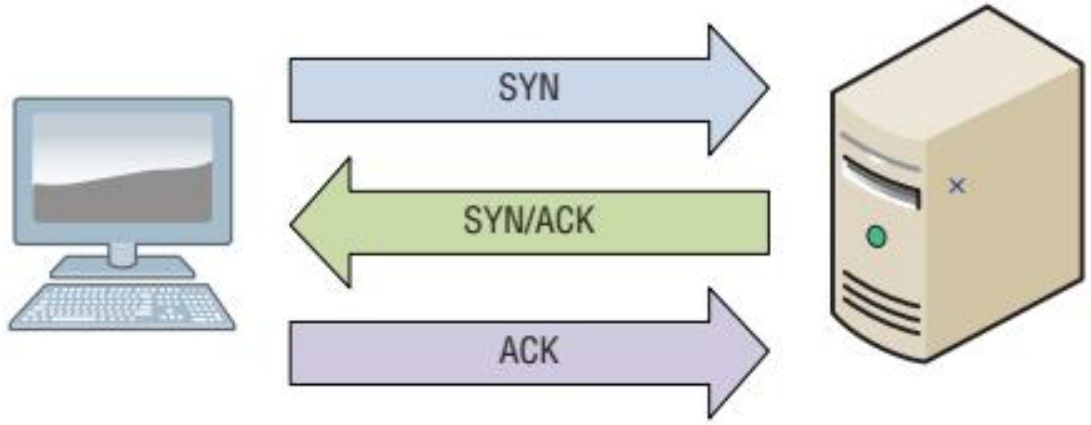

Рисунок 11.6 – Тристороннє рукостискання TheTCP

Тристороннє рукостискання взагалі не враховує безпеку. Іноді робиться помилка, думаючи, що акт визнання запиту стосується питань безпеки, але насправді це не так. Крім того, пам'ятайте, що TCP використовує тристороннє рукостискання, але UDP цього не робить.

Під час рукостискання відбуваються наступні дії:

1. **A** відправляє пакет SYN до **B** або запит на встановлення з'єднання.

2. **B** відповідає SYN-ACK або підтвердженням запиту.

3. **A** реагує назад з остаточним ACK, який служить для повного встановлення з'єднання.

На відміну від TCP, UDP надає дуже мало гарантій того, що інформація надходить до пункту призначення і робить це правильно. UDP не припускає, що вам потрібна перевірка помилок. Це те, що визначається програмою за замовчуванням або користувачем, який налаштовує програму.

UDP - це протокол без статусу. Без статусу означає, що протокол розглядає кожен запит інформації, як власну незалежну операцію. Хоча це може здаватися ресурсомістким, але це не так, тому що системам більше не потрібно відслідковувати поточні розмови і тому використовує менше пакетів даних.

Давайте зосередимося на тому, як ми використовуємо наші знання цих двох протоколів. Спочатку розглянемо сканування портів за допомогою TCP. Протокол TCP використовує прапори для інформування приймаючої сторони про те, як обробляти зв'язок. Прапори доступні в кожному TCP-пакеті і /або включені, або вимкнуті, як цього вимагає певна ситуація. У таблиці 11.3 показано деякі прапори, доступні в протоколі TCP.

Таблиця 11.3 – Різні прапори TCP

Назва	Опис
SYN	Використовується для ініціювання зв'язку між двома різними хостами, щоб полегшити зв'язок.
ACK	Використовується для підтвердження отримання пакету інформації.
URG	Стверджує, що дані, що містяться в пакеті повинні бути оброблені негайно.
PSH	Доручає системі відправлення негайно відправляти всі буферизовані дані.
PSH	Повідомляє віддаленій системі, що більше інформації не надсилатиметься. По суті це закриває зв’язок.
RST	Пакет скидання, який використовується для скидання з'єднання.

Тепер, коли ви розумієте, що таке сканування портів, розглянемо декілька різних видів сканування.

Повне сканування або сканування портів. TCP-підключення або повне відкрите сканування - це ще один спосіб сказати, що ви виконуєте тристороннє рукостискання на портах цільової системи з наміром визначити, які з них відкриті і які закриті.

Перевага використання повного сканування полягає в тому, що під час сканування ви отримуєте негайний позитивний відгук про те, що порт

відкритий або закритий. Тим не менш, є такий недолік цього типу сканування, який повертається до нашого використання тристороннього рукостискання. Пам'ятайте, що метою трьох напрямків є підтвердження того, що обидві сторони збираються спілкуватися. Якщо обидві сторони підтверджують свою присутність і беруть участь у зв'язку, то всі знають, що обидві сторони є і хто вони є. Отже, коли повні відкриті з'єднання підтверджені, у вас є дуже "шумне" з'єднання, яке можна легко виявити.

Коли це з'єднання більше не потрібно, ініціююча сторона змінить тристороннє рукостискання, з останнього кроку ACK + RST, який зриває з'єднання. На рисунку 11.7 показано, як цей процес працює для виявлення відкритого і закритого порту.

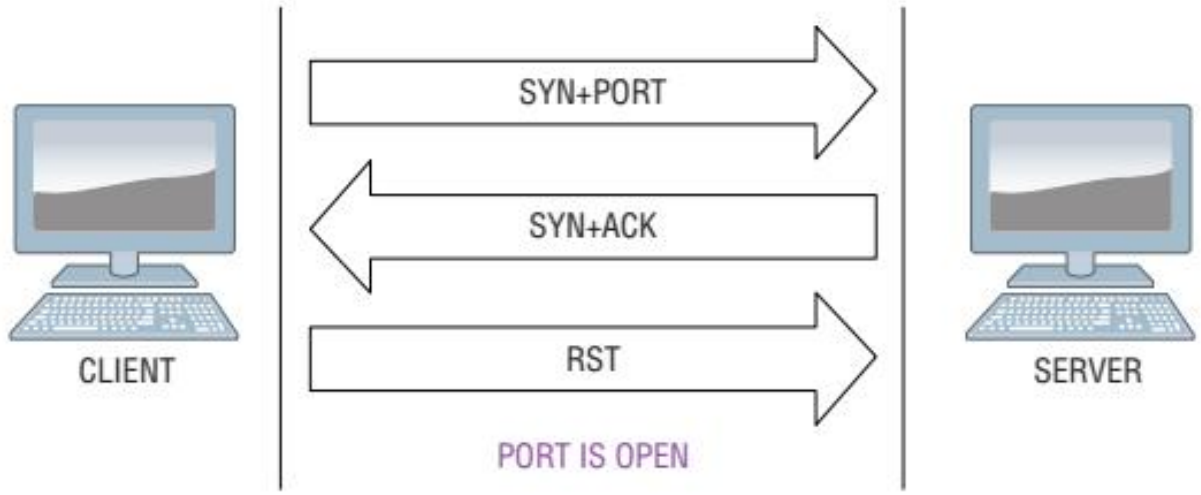

Рисунок 11.7– Закриті та відкриті відповіді порту

Для відкритого порту відповідь така, як це було б для нормального триразового рукостискання; однак, для закритого порту ви отримуєте тільки RST пакет у відповідь. Знаючи цей шаблон відповіді, можна визначити, чи є порт відкритим або закритим остаточно. Щоб виконати повне відкрите сканування в nmap, використайте наступну команду:

```
nmap –sT – v <цільова IP-адреса
```

Стелс-сканування або напіввідкрите сканування. У цьому типі сканування процес дуже схожий на повне відкрите сканування з деякими відмінностями, що робить його більш стійким. Основна відмінність цього типу сканування по відношенню до попереднього типу сканування полягає в останньому кроці. Тоді як повне відкрите сканування використовує тристороннє рукостискання, тут ми робимо тільки перші два кроки і замість цього посилаємо один пакет RST для останнього кроку, фактично закриваючи з'єднання, перш ніж воно буде повністю завершено. Чому це працює, повідомляючи нам, чи порт відкритий або закритий? Другий крок отримання SYN-ACK-пакету говорить нам, що порт відкритий - це те, що ми хочемо, не реагуючи на остаточний ACK, тому що ми лише наполовину відкрили з'єднання. Однак те, що відбувається, якщо порт закрито, так же, як і раніше. Тристороннє рукостискання починатиметься, коли сканер відправляє SYN, тільки щоб потерпілий сам повернув пакет RST, який вказує, що порт закритий і не приймає з'єднання. Рисунок 11.8 ілюструє цю технологію сканування для відкритих і закритих портів.

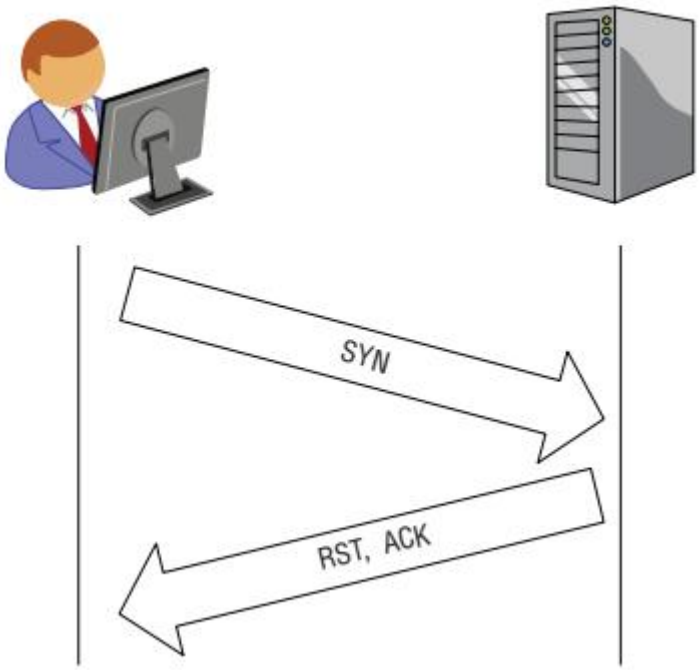

Рисунок 11.8 – Напіввідкритий проти закритих і відкритих портів

Перевагою напіввідкритого або стелс-сканування є те, що воно менш схильне до механізмів виявлення. Недоліком є те, що він менш надійний, ніж повне відкрите сканування, оскільки під час цього процесу підтвердження не отримано. У деяких випадках він також має і недолік, який у деяких випадках є трохи повільним.

Щоб виконати напіввідкрите сканування, можна скористатися наступною послідовністю:

```
nmap –sS –v <цільова IP-адреса>
```

Xmas дерево сканування. У деяких випадках цей тип сканування також відомий як пакет ялинки, пакет камікадзе, гангграма або тестовий сегмент лампи, але найпоширенішою назвою є Xmas. У цьому типі сканування встановлюються декілька прапорів, що означає, що пакет надсилається клієнту за допомогою SYN, PSH, URG і FIN все одночасно на одному і тому ж пакеті. Проблема полягає в тому, що з усіма встановленими прапорами існує нелогічна або нелегальна комбінація, що викликає проблему приймаючої системи, оскільки вона повинна визначити, що робити. У більшості сучасних систем це просто означає, що пакет ігнорується або відкидається, але в деяких системах відсутність відповіді говорить нам, що порт відкритий, тоді як один пакет RST повідомляє нам, що порт закритий. На рисунку 11.9 показаний цей процес.

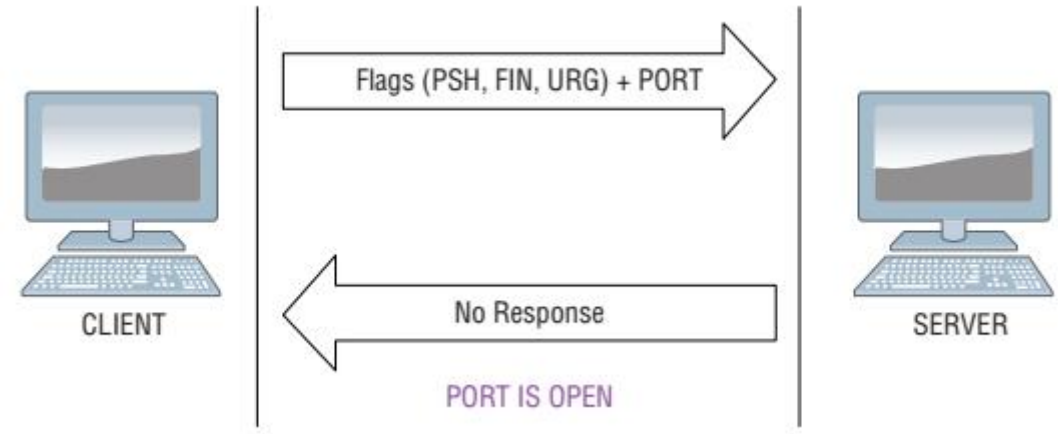

Рисунок 11.9 – Сканування Xmas

Виконання сканування Xmas дерева з nmap. У командному рядку, введіть наступну команду:

nmap –sX –v <цільова IP-адреса>

FIN Сканування. Сканування FIN відбувається, коли зловмисник посилає запити жертві з набором прапорів FIN. Подумайте про те, що відбувається, коли ви відправляєте пакет з відправленим прапором FIN: ви просите, щоб з'єднання було закрито, оскільки не було надіслано додаткової інформації. Результатом цієї дії є те, що цільова система не поверне відповідь, якщо порт закритий, але якщо порт відкритий, RST буде повернуто, подібно до нашого сканування Xmas дерева. Рисунок 11.10 ілюструє цей процес.

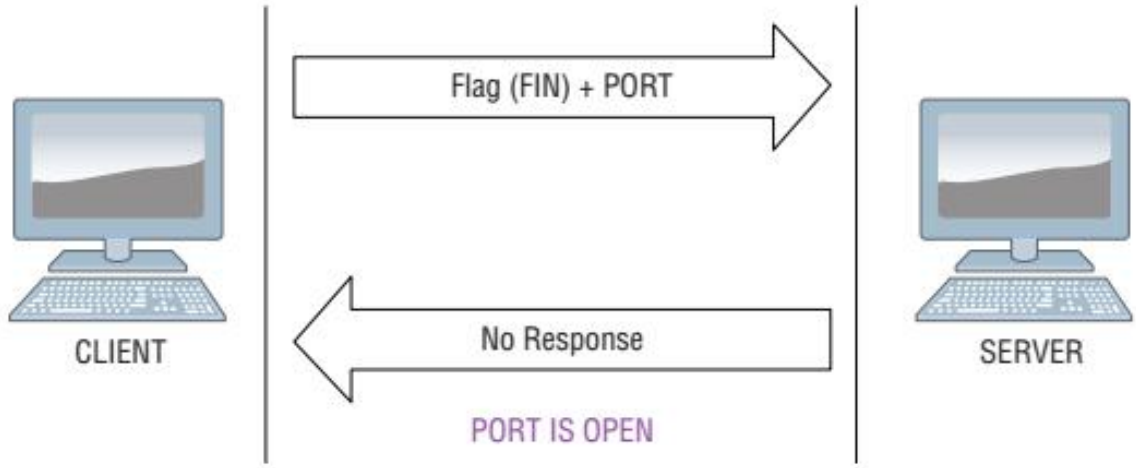

Рисунок 11.10 – Сканування FIN при закритого і відкритого порту відповідно

Сканування FIN у nmap можна виконати за допомогою наступної команди:

Nmap –sF <цільова IP-адреса>

Сканування NuLL.

Сканування NULL є ще одним цікавим скануванням, яке можна виконати, і є протилежне скануванню дерева Xmas. Щоб виконати сканування NULL, ви відправляєте пакет без встановлених прапорів, і результати

показують вам чи порт відкритий або закритий. Відкритий порт не повертає відповіді, тоді як закритий порт знову повертає RST, як показано на рисунку 11.11.

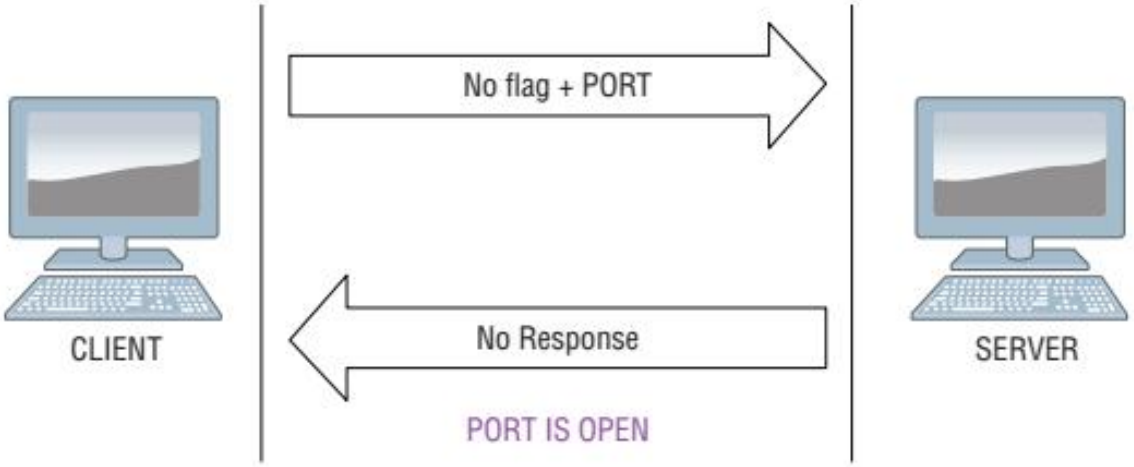

Рисунок 11.11 – Сканування NULL на закритий і відкритий порт відповідно

Для виконання NULL сканування у nmap виконайте наступну команду:

nmap –sN <цільова IP-адреса>

ACK сканування.

Іншим цікавим варіантом встановлення прапорів є сканування ACK, яке використовується для перевірки виконання будь-якої фільтрації у вигляді брандмауера. Брандмауери здійснюють фільтрацію трафіку від однієї мережі до іншої (наприклад з Інтернет до локальної мережі).

Дивлячись зі сторони, ви не можете сказати точно чи наявний брандмауер (особливо якщо здійснюється тест чорного ящика), так що вам потрібен спосіб, щоб зрозуміти це.

Одним із способів є використання сканування ACK. У цьому типі сканування пакет з набором прапорів ACK надсилається до цілі. Запит ACK, який надсилається жертві, яка не повертає відповідь, вказує, що брандмауер присутній і виконує фільтрацію, тоді як отримання RST від жертви показує, що фільтрація не виконується. На рисунку 11.12 показано сканування ACK.

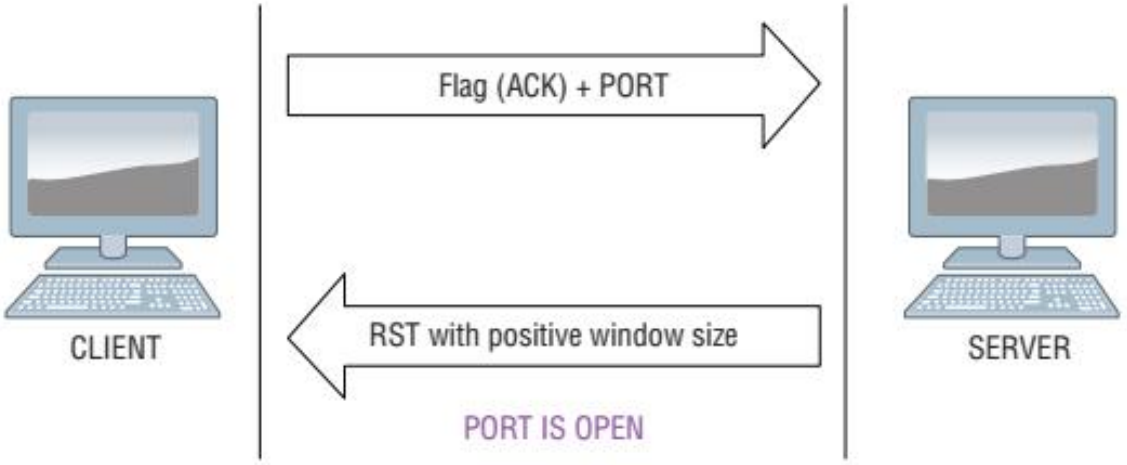

Рисунок 11. 12 – Проводиться сканування ACK

Щоб виконати сканування ACK у nmap, виконайте таку команду:

nmap –sA <цільова IP-адреса>

Ми розглянули деякі прості використання nmap, але програма набагато потужніша. Наприклад, якщо у вас є кілька цілей, ви можете ввести IP-адресу як діапазон. Наприклад, 192.168.1.1 - 200 буде сканувати всі адреси від 1 до 200. Іншим прикладом є використання 192.168.1.1/24, яка буде сканувати всю підмережу класу C.

12. Сканування вразливостей

Вразливість - це слабкість або відсутність захисту, присутня у хості, системі або програмі. Наявність вразливості являє собою потенційне місце для експлуатації або націлювання на загрозу. Розміщення та ідентифікація вразливостей у системі є одним з важливих компонентів захисту системи, але не єдиним.

Як ви знаходите всі вразливості, які існують у середовищі, особливо зі зростаючою складністю технологій? Вам можуть допомогти багато методик; деякі з них є ручними, а деякі - автоматизовані інструменти, такі як сканери уразливості.

Сканери уразливості призначені для виявлення проблем і «дірок» в операційних системах і додатках. Це робиться шляхом перевірки кодування, портів, змінних банерів і багатьох інших потенційних проблемних областей. Сканер вразливості призначений для використання багатьма законними користувачами, включаючи пентестерів, щоб з'ясувати, чи існує можливість успішної експлуатації, і що потрібно виправити, щоб зменшити або усунути область загрози. Хоча сканери уразливості зазвичай використовуються для перевірки програмних додатків, вони також можуть перевіряти всі операційні середовища, включаючи мережі та віртуальні машини.

Вступ до сканування вразливостей. Сканування вразливості - це процес, який може бути включений як частина тестування на проникнення або може бути виконаний повністю самостійно. Метою цього типу сканування є виявлення і ідентифікація вразливостей на мішені і надання інформації ініціатору сканування. При правильному та регулярному виконанні сканування вразливості може надати цінну інформацію про стан безпеки інфраструктури організації, включаючи її технічну та управлінську політику.

Багато компаній використовують сканери уразливості, оскільки можуть легко виявити багато спільних проблем безпеки. Це робиться шляхом перевірки

кодування, портів і багатьох інших аспектів цільової області, щоб виявити будь-які можливі проблеми, які зловмисник може використати на свою користь.

Сканер вразливості використовується багатьма законними користувачами, щоб з'ясувати, чи є можливість експлуатувати вразливість, і що потрібно зробити, щоб зменшити будь-яку загрозу. У той же час, хакери використовують ці сканери, щоб знати, де саме атакувати. Хоча сканери вразливості, як правило, використовуються найчастіше з програмами, вони можуть перевіряти весь комп'ютер, мережі та віртуальні машини.

У хакерів багато способів проникнення в комп'ютер, вони можуть входити через слабке кодування, через відкритий порт або через програму з легким доступом користувача. Щоб звести можливість злому до мінімуму, компанії використовують сканер вразливості. Користувач може вказати цільову область, тому програма сканує лише одну частину комп'ютера, переходячи через все в межах цієї області, щоб виявити проблеми. Деякі програми можуть автоматично виправляти дрібні помилки, хоча більшість повідомляє про проблеми.

Основними користувачами програмного забезпечення сканера вразливостей є в основному легітимні підприємства. Основні користувачі, як правило, не мають знань для правильного виправлення проблем, тому сканери уразливості зазвичай не призначені для них. Ці програми робляться більше для підприємств і великих мереж, де вразливість може спричинити пряму втрату грошей або втрату комерційної таємниці, що може бути дорогим. Пентестери, як правило, знаходять вигоду з цими утилітами, тому що вони можуть виявити вразливі місця, які можуть бути використані під час своєї роботи, і надавати інформацію для звіту клієнту. Сканер вразливостей найчастіше використовується на спеціальних програмах або веб-додатках - програмах, які залучають багато людей, які працюють одночасно, оскільки ці програми можуть становити загрозу безпеці. Сканери вразливості також створені для цілих комп'ютерів, мереж, портів, баз даних і віртуальних машин. Деякі

сканери виконуються для сканування різних цільових областей, тоді як деякі з них просто зможуть перевірити один аспект комп’ютера.

Визнання обмежень сканування вразливостей. Сканування вразливості вже давно використовувалося в інструментарії спеціаліста з безпеки. Однак, незважаючи на те, що він є цінним інструментом і продовжуватиме залишатися важливою частиною інструментарію безпеки, він також має свої обмеження, які потрібно розуміти, щоб належним чином застосувати технологію до максимального рівня. Пам'ятайте, що уразливості є постійною проблемою, яку можна пом'якшити, але необхідно проводити постійну переоцінку для того, щоб переконатися, що будь-які нові проблеми, які з'являються, розглядаються своєчасно (і принаймні відзначені, щоб відстежувати поточні проблеми безпеки в мережі). Іншим важливим моментом, який слід пам'ятати з допомогою цих сканерів, є те, що сканування з цими інструментами з боку IT-адміністратора або провайдерів безпеки не повинно приховуватися в помилковому відчутті безпеки, якщо їх сканування не виявляє проблем.

Сканери вразливості бувають різних форм, кожен з яких здатний виконувати унікальний тип сканування проти цільової системи. На нижньому кінці деякі сканери включають лише можливість перевірки конфігурації системи, включаючи виправлення та інформацію про версію програмного забезпечення. На вищому рівні сканери уразливості можуть включати в себе велику кількість потужних функцій, таких як розширені можливості звітності, функції аналізу та інші корисні можливості.

Незалежно від їхнього набору функцій та загальних можливостей, більшість сканерів використовують модель, подібну до т антивірусних пакетів. У більшості випадків сканери покладаються на використання бази даних відомих вразливостей, які необхідно регулярно оновлювати, завантажуючи нові версії бази даних з веб-сайту постачальника. Однак, необхідно застосовувати регулярні оновлення так як програмне забезпечення швидко втратить здатність виявляти нові загрози, збільшуючи таким чином ризик порушення безпеки внаслідок експлуатації непоміченого порушення. Насправді сканер, який не

регулярно оновлюється, стане по суті непридатним, якщо він не оновлюється протягом тривалого періоду часу.

Більш важливим питанням для сканерів є те, що можна отримати впевненість у собі навіть з усіма поточними оновленнями та іншими завданнями, які виконуються, щоб оновити програмне забезпечення. Деякі користувачі цих пакетів вважають, що результати звіту відображають всі вразливі місця в середовищі, і, таким чином, звіт, який розглядається означає, що це все, що можна зробити, але це не так . Фактично, сканери уразливості повідомлятимуть лише про ті елементи, які він має здатність виявляти, що залишає шанс для багатьох потенційних проблем, які потрібно пропустити. Ситуація дещо схожа на віру в те, що прогулянка навколо будівлі і пошук проблем означає, що ви знайшли всі потенційні уразливості, коли це не так, - насправді, ви могли б легко пропустити щось.

Нарешті, ще одне просте запитання пропустити зі сканерами цього типу є те, що вони тільки повинні бути використані, коли проблема згадується в статті новин або іншому джерелі. Фактично, перевірки повинні виконуватися регулярно для того, щоб правильно ловити проблеми, а також забезпечувати, щоб поточні заходи працювали над тим, щоб середовище працювало належним чином і безпечно. Залежно від того, на які вимоги відповідає ваша компанія, сканування вразливостей може потребувати виконання встановленого розкладу та перевірку. Наприклад, стандарт захисту даних промисловості платіжних карток (PCI DSS) вимагає проведення періодичних сканувань вразливостей, тому будь-яка організація, яка зберігає, обробляє або передає дані кредитної картки, повинна виконувати сканування вразливостей.

Визначення процесу сканування вразливостей. Сканування вразливостей, як правило, реалізується як один з багатьох інструментів, які допомагають організації ідентифікувати уразливості на їхній мережі та обчислювальних пристроях. Результати сканування допоможуть керівництву приймати обгрунтовані рішення щодо безпеки своїх мереж і пристроїв, прикріплених до них. Сканування вразливості може використовуватися або в невеликих

масштабах, або у великих масштабах, залежно від активів і систем, які необхідно оцінити.

Незважаючи на наявність численних інструментів, які можуть забезпечити уявлення про вразливості системи, не всі інструменти сканування мають однаковий набір функцій. Кожен інструмент сканування може або не може охоплювати той самий список вразливостей, який може оцінити інший. Таким чином, організація повинна ретельно вибирати, які сканери вони хотіли б використовувати, а потім визначити, що використання будь-якого іншого сканера уразливості повинно бути виправдано і затверджене до використання.

Будь-який інструмент сканування повинен бути здатний оцінювати інформаційні системи з центрального місця розташування і мати можливість надавати пропозиції щодо виправлення ситуації. Вона також повинна бути здатною присвоїти кожній виявленій вразливості значення важкості на основі відносної дії уразливості для ураженої одиниці.

Проведення періодичної оцінки існуючих пристроїв. В ідеалі, кожен відділ повинен бути зобов'язаний регулярно проводити оцінку своїх мережевих обчислювальних пристроїв. Принаймні, кожен відділ повинен виконувати повністю аутентифіковану перевірку за встановленим графіком (наприклад, щомісячно або щоквартально). Ці сканування повинні бути пристосовані для того, щоб оцінити унікальні потреби їхнього відділу, і вони повинні працювати проти всіх активів, які знаходяться в їх власних унікальних сферах контролю.

Прикладом можуть бути щомісячні сканування для таких мережевих обчислювальних пристроїв:

- ✓ Будь-які обчислювальні пристрої, які, як відомо, містять конфіденційні дані.
- ✓ Будь-які обчислювальні пристрої, які повинні відповідати певним нормативним вимогам.
- ✓ Всі зображення файлової системи або шаблони віртуальних машин, що використовуються, як базові зображення для створення та розгортання нових робочих станцій або серверів.

- ✓ Всі пристрої, які використовуються як сервери або використовуються для зберігання даних.
- ✓ Будь-яке обладнання мережевої інфраструктури.

Для проведення сканування слід використовувати затверджений засіб сканування вразливостей, якщо не дозволено інше.

Сканування повинні завжди виконуватись (у більшості випадків) з урахуванням унікальних потреб бізнесу. Майте на увазі, що сканування вразливостей може і буде сповільнювати мережу, а також пристрої або програми, які їм належить оцінювати. Якщо сканування виконується протягом робочого часу, слід подбати про мінімізацію потенційних порушень, які можуть бути спричинені скануванням. Сканування слід проводити не під час пікового навантаження, а також додаткове друге сканування для виявлення невідповідних клієнтів або клієнтів, які були закриті для повторного сканування.

Обчислювальні пристрої або системні адміністратори не повинні вносити зміни до мережевих обчислювальних пристроїв з єдиною метою проходження оцінки. Крім того, жоден пристрій, підключений до мережі, не повинен бути спеціально налаштований для блокування сканувань вразливості.

Вразливості на мережевих обчислювальних пристроях слід вирішувати на основі результатів та потреб бізнесу. Майте на увазі, що не всі вразливості, виявлені в механізмі сканування, мають бути вирішені.

Проведення оцінки нової системи. Жодна нова система не повинна вводитися у виробництво, поки не буде проведена оцінка вразливості та не буде розглянуто вразливості.

Кожен відділ повинен бути спрямований на проведення оцінок вразливостей у такі часи:

- ✓ Після завершення етапу встановлення та виправлення операційної системи.
- ✓ Після завершення встановлення будь-якого купленого або внутрішньо розробленого додатку.

- ✓ Перед передачею інформаційної системи у виробництво.
- ✓ Після заповнення зображення або шаблону, призначеного для розгортання декількох пристроїв.
- ✓ Після постачання інформаційних систем, що надаються постачальником, до тестування на прийом користувача, і знову до переходу у виробництво.
- ✓ Нове обладнання мережевої інфраструктури під час фази випробування та перед переходом у виробництво.

Після завершення кожної з цих оцінок вразливості всі виявлені вразливості повинні бути задокументовані та виправлені.

Розуміння того, що сканувати. Департаменти не повинні проводити нав'язливі сканування систем, які не знаходяться під їх безпосереднім контролем:

- ✓ Департаменти несуть відповідальність за те, щоб обладнання, що належить до постачальників, було обмежене в тих вразливостях, які можуть завдати шкоди підприємству.
- ✓ Постачальник повинен бути поінформований і мати дозвіл надати персонал під час сканування.
- ✓ Продавцям не дозволено проводити сканування інформаційних систем без спеціального дозволу департаменту та управління.

Мережеві обчислювальні пристрої, які викликають руйнівну поведінку в мережі, можуть бути скановані за допомогою неінструзійних методів для дослідження джерела порушення.

Зменшення ризиків. Після завершення кожної оцінки кожен відділ повинен вести документацію.

- ✓ Усіх виявлених вразливостей та пошкоджених інформаційних систем.
- ✓ Для кожної виявленої вразливості детальна інформація про те, як вразливість буде виправлена або усунена.

✓ Звіти, підготовлені інструментом сканування вразливостей підприємства, які повинні бути оцінені на предмет їх придатності до цієї документації.

Як частина щорічного процесу сканування безпеки, департаменти повинні будуть документувати сканування уразливості та зусилля з виправлення, засновані на цій документації.

Виявлені уразливості будуть усунені та / або пом'якшені на основі таких правил, як наступні приклади:

✓ Критичні уразливості будуть повністю вирішені протягом 15 календарних днів після виявлення.

✓ Висока вразливість буде повністю розглянута протягом 30 календарних днів після відкриття.

✓ Середні вразливості будуть повністю вирішені протягом 60 календарних днів після відкриття.

- Низькі вразливості будуть розглянуті протягом 90 календарних днів

після виявлення.

Вразливості вважаються усуненими, коли ризик експлуатації повністю усунуті, а подальші сканування пристрою показують, що вразливість більше не існує. Як правило, це досягається шляхом виправлення операційної системи / програмного забезпечення або оновлення програмного забезпечення.

Типи сканувань, які можна виконувати. Звичайно, сканування, яке може бути використано під час реального сканування вразливостей, різко змінюється, але ось деякі з потенційних сканувань, які використовуються в галузі.

Аутентифіковане сканування. Тип сканування, який вимагає відповідних облікових даних для автентифікації на машині для визначення наявності вразливості без спроби нав'язливого сканування.

Інформаційні системи. Програмні, апаратні та інтерфейсні компоненти, які працюють разом для виконання набору бізнес-функцій.

Внутрішня конфіденційність. Вимога підтримувати певну інформацію доступною лише для тих, хто має дозвіл на доступ до неї, і тих, хто має знати

Нав'язливе сканування. Тип сканування, який намагається визначити наявність вразливості шляхом активного виконання відомого експлуатанта.

Мережевий обчислювальний пристрій. Будь-який обчислювальний пристрій, підключений до мережі, що забезпечує засоби доступу, обробки та зберігання інформації.

Обладнання мережевої інфраструктури. Обладнання, яке забезпечує інформаційний транспорт, такі як маршрутизатори, комутатори, брандмауери та мостове обладнання; не включає в себе мережеві сервери і робочі станції, якщо такі пристрої не виконують специфічну функцію забезпечення транспорту.

Відділ. Визначена організаційна одиниця в організації, яка відповідає за забезпечення певного інформаційного активу.

Сканери вразливості є особливим типом автоматизованої утиліти, яка використовується для виявлення слабких місць в операційних системах і додатках. Це робиться шляхом перевірки кодування, портів, змінних, банерів і багатьох інших потенційних проблемних областей, які шукають проблеми. Сканер уразливості призначений для використання багатьма законними користувачами, щоб з'ясувати, чи існує можливість успішної атаки та що необхідно виправити, щоб пом'якшити проблемну область.

Хоча сканери уразливості зазвичай використовуються для перевірки програмних додатків, вони також можуть перевіряти всі операційні середовища, включаючи мережі та віртуальні машини. Сканери вразливості призначені для пошуку конкретних проблем і виявилися корисними, але є й серйозні потенційні небезпеки. Якщо вони не знайдуть жодних проблем, вони можуть помилково повідомити, що проблем немає, тому добре доповнити та перевірити результати цих тестувань.

Список використаних джерел

1. Oriyano Sean-Philip. Penetration Testing Essentials. Sybex, a Wiley brand, 2017, 363 p.

2. Baloch Rafay. Ethical hacking and penetration testing guide. Auerbach Publications, 2017, 523 p.

3. Wilhelm, Thomas. Professional penetration testing: Creating and learning in a hacking lab. Newnes, 2013, 525 p.

4. BSI - Study A Penetration Testing Model. Federal Office for Information Security, 111 p. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.html

5. Najera-Gutierrez, Gilberto, and Juned Ahmed Ansari. Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux. Packt Publishing Ltd, 2018.

6. Johansen, Gerard, et al. Kali Linux 2–Assuring Security by Penetration Testing. Packt Publishing Ltd, 2016.

7. Buchanan, Cameron, and Vivek Ramachandran. Kali Linux Wireless Penetration Testing Beginner's Guide: Master wireless testing techniques to survey and attack wireless networks with Kali Linux, including the KRACK attack. Packt Publishing Ltd, 2017.

8. Denis, Matthew, Carlos Zena, and Thaier Hayajneh. "Penetration testing: Concepts, attack methods, and defense strategies." 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT). IEEE, 2016.

9. Norman, Alan T. Computer Hacking Beginners Guide: How to Hack Wireless Network, Basic Security and Penetration Testing, Kali Linux, Your First Hack. Independently published, 2018.

10. Hertzog, Raphaël, and Jim O'Gorman. Kali Linux Revealed: Mastering the Penetration Testing Distribution. offsec Press, 2017.

11. Denis, Matthew, Carlos Zena, and Thaier Hayajneh. "Penetration testing: Concepts, attack methods, and defense strategies." 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT). IEEE, 2016.

12. Penetration Testing- A hand on introduction to hacking, Georgia Weidman, no starch press, San Francisco, 2014

13. Chu, Ge, and Alexei Lisitsa. "Penetration Testing for Internet of Things and Its Automation." 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS). IEEE, 2018.

14. https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools

15. http://www.pentest-standard.org/index.php/Exploitation

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.html

Навчально-методичне видання

Яцків Василь Васильович

«ТЕСТУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ НА ПРОНИКНЕННЯ»

ОПОРНИЙ КОНСПЕКТ ЛЕКЦІЙ

для студентів спеціальності 125 «Кібербезпека»

за другим магістерським рівнем вищої освіти»

Підписано до друку 25.09.2019
Формат 60х84 1/16. Папір офсетний.
Умов. – друк арк. 5,7. Обл.– вид. арк. 6,9
Замовне. Наклад 50 прим. Зам. 3-255

Віддруковано у ФОП Шпак В.Б.
Свідоцтво про державну реєстрацію ВО – 2№924434 від 11.12.2006р.
Свідоцтво платника податку Серія Е №897220
м. Тернопіль – 4600, вул. Просвіти, 6
тел. +(38) 0972993899
E-mail: tooums@ukr.net