Engineer

Тестування на проникнення

санкціонована атака для перевірки вразливостей на практиці

Що це таке

Тестування на проникнення (у професійному жаргоні — пентест) — це перевірка безпеки, під час якої тестувальники імітують реальні атаки, щоб знайти способи обійти захисні механізми застосунку, системи чи мережі. Технічний посібник NIST із тестування та оцінювання інформаційної безпеки, SP 800-115, зазначає, що це часто означає справжні атаки на справжні системи й дані з тими самими інструментами та техніками, якими користуються зловмисники. SP 800-53 Rev. 5, каталог заходів безпеки та приватності від NIST, у коротшому визначенні додає, що фахівці, як правило, працюють у визначених межах, і саме це відрізняє тест від нападу: він санкціонований, обмежений і письмово погоджений до того, як почнеться.

Від інших видів перевірки безпеки його відрізняє мета. Сканер вразливостей порівнює побачене з описами відомих вад і повідомляє, що там може бути. Тестувальник намагається цю ваду використати. SP 800-115 формулює різницю прямо: сканери лише перевіряють, чи може вразливість існувати, а фаза атаки під час тестування на проникнення експлуатує її, щоб підтвердити, що вона справді є. Більшість тестів шукає також комбінації, тобто слабкі місця в одній чи кількох системах, які разом дають більший доступ, ніж кожне з них окремо.

Web Security Testing Guide від OWASP (WSTG) зауважує, що цю техніку також широко називають тестуванням методом чорної скриньки або етичним хакінгом. Команда тестує ззовні, не знаючи внутрішньої будови цілі, і поводиться так, як поводився б зловмисник, хоча часто отримує один чи кілька робочих облікових записів користувача.

Кожен тест визначають два рішення. Перше — точка старту. Зовнішній тест починається поза мережею, і в команди є хіба що адреси, які входять в обсяг; внутрішній тест починається всередині, зазвичай із доступом звичайного працівника, і намагається просунутися вище через підвищення привілеїв. Друге — хто знає про тест. SP 800-115 називає відкрите тестування тестуванням «білого капелюха» (white hat): воно відбувається з відома й за згодою IT-персоналу. Приховане тестування, або тестування «чорного капелюха» (black hat), проводять без відома IT-персоналу, але з повного відома й дозволу вищого керівництва.

SP 800-115 поділяє роботу на чотири фази й у примітці додає, що це лише один із багатьох прийнятних способів її згрупувати. На етапі планування погоджують правила, документують дозвіл керівництва і визначають цілі; саме тестування починається з розвідки. Розвідка збирає відомості про ціль, сканує її та звіряє знахідки з базами даних вразливостей, як-от американською National Vulnerability Database, і з власними знаннями тестувальників. Фаза атаки, яку посібник називає серцевиною будь-якого тестування на проникнення, намагається експлуатувати кожну можливу ваду. Коли вдалий експлойт відкриває новий доступ, тестувальники повертаються до розвідки вже з нової позиції. Звітування йде паралельно з трьома іншими фазами й завершується звітом, у якому перелічено знайдені вразливості, оцінено ризик кожної та пояснено, як їх усунути. Інші методики ділять ту саму роботу інакше: Penetration Testing Execution Standard (PTES), який WSTG наводить серед своїх еталонних методологій, має сім фаз, від попередніх домовленостей до звітування.

Застосуйте поняття до рішення

Застосуйте «Що таке тестування на проникнення?» до конкретного рішення. Ми можемо пов'язати поняття із системою, яку ви створюєте або купуєте. Облікові записи, паролі й права налаштовані так, щоб доступ відповідав роботі, а звільнені втрачали його того ж дня.

Переглянути наші послуги Зв'язатися з нами →

Перевірте припущення за терміном

Використайте пояснення та пов'язані роботи, щоб сформулювати запитання для проєкту. Ми можемо перевірити припущення разом до вибору інструмента. Написала 1 000 правил RBAC для Linux-серверів — 1,000 правил доступу написано, щоб усунути вразливість

Написала 1 000 правил RBAC для Linux-серверів Зв'язатися з нами →

Чому це важливо

Звіт сканера — це перелік можливостей. Частину з них у вашому середовищі використати неможливо, а ваду, якої ніхто не описав, або таку, що виникає лише тоді, коли дві нешкідливі на вигляд слабкості використати разом, сканер не побачить. Тестування на проникнення відповідає на інше

запитання: що зловмисник може тут зробити насправді і як далеко він зайде? SP 800-115 називає, що ще воно здатне показати: наскільки система витримує реальні прийоми атак, якої кваліфікації має бути зловмисник, які додаткові контрзаходи допоможуть і чи помітять захисники атаку та чи зреагують на неї.

Тому до знахідок дослухаються навіть ті, хто ніколи не читає звітів сканерів. Знахідка, яка показує, що сторонній без облікового запису прочитав таблицю клієнтів, — це доказ, а не ймовірність. SP 800-115 описує тестування на проникнення як ітеративний процес, у якому мінімальний доступ використовують, щоб здобути більший, і добрий звіт показує цей ланцюжок крок за кроком, щоб виправлення розірвало його в найдешевшій ланці.

Той самий реалізм робить тест дорогим і ризикованим. NIST називає його трудомістким, зазначає, що він потребує глибокої експертизи, і попереджає, що під час тесту системи можуть бути пошкоджені або виведені з ладу; досвідчені тестувальники зменшують цей ризик, але цілком усунути його неможливо. Багато з того, що робить тестувальник, наприклад атаки на системи з метою їх скомпрометувати, — це дії, які власні політики організації зазвичай забороняють. Саме тому існують правила проведення тесту, англійською rules of engagement (ROE): документ, погоджений до початку тестування, що надає команді повноваження на визначені дії і ні на що понад них.

Водночас це лише одна техніка з кількох, а не остаточний вердикт. WSTG зауважує, що багато команд використовують тестування на проникнення вебзастосунків як основну техніку перевірки безпеки, і доводить, що воно не повинно бути ні основною, ні єдиною. Вебзастосунки майже завжди створюють на замовлення, тож тестувати їх ззовні — це радше дослідження, ніж пошук відомих вад у типових продуктах, а сам тест відбувається пізно в життєвому циклі розробки, коли дизайн і код уже усталені. Там, де вихідного коду немає, додає посібник, тестування на проникнення однозначно краще, ніж повна відсутність тестування.

Частота випливає з ціни. SP 800-115 припускає, що через високу вартість і можливий вплив тестувати мережу й системи організації раз на рік може бути достатньо, а між тестами регулярно проводити легше сканування. Деякі стандарти вимагають його прямо: WSTG зазначає, що PCI DSS, стандарт безпеки даних індустрії платіжних карток, має власну вимогу щодо тестування на проникнення, яка охоплює і зовнішнє, і внутрішнє тестування.

Як це виглядає на практиці

Більшу частину тестування на проникнення вирішують до того, як тестувальники торкнуться цілі. Додаток B до SP 800-115 — це шаблон правил проведення з розділами про мету й обсяг, учасників і графік, про те, як сторони спілкуються і коли тест зупиняють, які системи входять в обсяг, а які виключено, які дії дозволені й заборонені, як поводитися з тестовими даними, як звітувати про результати, а також зі сторінкою підписів. Скорочений варіант для зовнішнього тесту інтернет-магазину міг би виглядати так. Його написано для цієї статті, а назви та адреси взято з діапазонів, зарезервованих для документації.

```
ПРАВИЛА ПРОВЕДЕННЯ: зовнішній тест shop.example.com

Мета            Визначити, які вади може використати сторонній і як
                далеко веде кожна з них.
Цілі            203.0.113.10–203.0.113.20, належність перевірено в WHOIS
Виключено       203.0.113.15 (платіжний провайдер, не нам його тестувати)
                Усі сторонні сервіси, до яких звертається магазин
Акаунти         Два клієнтські акаунти й один акаунт підтримки
Графік          3–14 листопада, 19:00–06:00 CET, поза піковими годинами
                продажів
IP команди      Лише 198.51.100.7 і 198.51.100.8
Дозволено       Експлуатувати підтверджену ваду, щоб показати наслідки;
                читати дані тестових акаунтів; завантажити один позначений
                тестовий файл і видалити його наприкінці
Заборонено      Атаки на відмову в обслуговуванні; зміна чи видалення
                даних клієнтів; соціальна інженерія; фізичне проникнення
Зупинка         Збій робочого магазину, реальні дані клієнтів на екрані
                або ознаки справжнього зловмисника: зупинитися й
                зателефонувати відповідальному за безпеку
Відновлення     Лише за письмовим рішенням відповідального за безпеку
Тестові дані    Конфіденційні; лише на ноутбуках команди, видаляються
                через 30 днів після фінального звіту
Звітність       Щоденна коротка довідка про стан; фінальний звіт
                протягом десяти робочих днів
Підписи         Керівник команди тестування; директор з інформаційної
                безпеки
```

Кожен рядок відповідає на запитання, яке ставить SP 800-115. Посібник радить перед початком тестування переконатися, що кожна публічна адреса зі списку цілей належить організації, і пропонує для цього реєстраційні дані WHOIS. Він пропонує тестувати робочий сайт увечері, а не в пікові години. Він просить указати адреси, з яких працюють тестувальники, щоб адміністратори могли відрізнити тестовий трафік від справжньої атаки.

Перелік систем, яких не можна торкатися, він називає exclude list, тобто списком виключень, і каже, що правила мають містити критерії зупинки тесту та порядок його відновлення. Він також ставить запитання, що робити, якщо тестувальники натраплять на справжнього зловмисника: чи зупиняти тест, коли його можна продовжити і з чийого дозволу? Щонайменше керівник команди тестування та вище керівництво підписують документ, засвідчуючи, що розуміють обсяг тесту та його межі.

За таких правил фаза атаки йде за послідовністю, яку WSTG описує для SQL-ін'єкцій. Сканування сторінки пошуку в магазині вказує на можливу ваду. Перший доказ — помилка бази даних, коли в поле пошуку вводять одинарну лапку. Далі тестувальник надсилає спеціально підготовлені дані, які змінюють граматику SQL-запиту, і вважає ваду підтвердженою лише тоді, коли запит повертає дані, яких не мав би повертати. Якби серед цих даних була сесія акаунта підтримки, тестувальник міг би увійти як підтримка, оглянутися вже звідти, а звіт показав би весь шлях: одне неперевірене поле, одна викрадена сесія, один погляд підтримки на всі замовлення.

Такий тест доповнює інші перевірки, а не замінює їх. Стаття про безперервне сканування безпеки у межах роботи засновниці в NextMariner описує статичний аналіз, динамічне тестування живого інстансу й перевірку залежностей, що виконуються автоматично, а поряд із ними письмові аудити безпеки, зокрема модель загроз і оцінку за посібником з тестування OWASP. Сторінка пояснює й причину такого поєднання: сканери знаходять типи проблем, які хтось уже описав, а в моделі загроз називають ті, що властиві саме одній платформі.

Де виникають проблеми

Тестування без письмового дозволу. Усне «починайте» від керівника команди не покриває атак, які забороняє політика компанії, і не захищає ні тестувальників, ні тих, хто замовив тест. Спершу напишіть правила проведення, і нехай керівник команди тестування та вище керівництво підпишуть їх до того, як команда надішле перший запит.

Тестування чужих адрес. Список цілей, скопійований зі старої діаграми, може містити адреси, які тепер належать комусь іншому, а на спільних платформах поряд із вами працюють інші клієнти. Перевірте, що кожна публічна адреса в обсязі належить організації, як радить SP 800-115, і внесіть кожен сторонній сервіс до списку виключень поіменно.

Сканування, продане як тестування на проникнення. Звіт сканера з новою обкладинкою перелічує можливості, а не докази. Вимагайте підтвердження експлуатації для кожної знахідки: що зробив тестувальник, який доступ це дало і яким був би наступний крок.

Тестування на проникнення як єдина перевірка безпеки. Один тест бачить лише частину ризиків, в один момент і ззовні. WSTG відносить моделювання загроз до етапу проєктування, рецензування та аналіз вихідного коду до розробки, а тестування на проникнення до етапу тестування, що йде далі. Використовуйте все це разом, а тестуванням на проникнення підтверджуйте те, чого попередні перевірки виявити не змогли.

Відсутність правила зупинки. Якщо тестувальники виведуть з ладу робочий сервіс або знайдуть сліди справжнього зловмисника, а заздалегідь ніхто не домовився, хто зупиняє тест і хто його відновлює, людям доведеться імпровізувати під тиском. Пропишіть у правилах критерії зупинки, ланцюжок дзвінків і порядок відновлення.

Результати як звичайні дані. Звіт про тестування на проникнення — це мапа того, що може використати зловмисник, і SP 800-115 радить вважати результати тестів конфіденційними. Перш ніж почати тест, домовтеся, як знахідки збирають, передають, тримають і знищують, і обмежте коло тих, хто отримує повний звіт.

Закриття знахідок без повторного тесту. Виправлення може бути частковим або влучити не туди, де вада. WSTG називає тестування, яке намагається експлуатувати вразливості, знайдені під час попередніх перевірок, сфокусованим тестуванням на проникнення і зазначає, що воно показує, чи справді конкретні вади усунено в коді, який працює. Перш ніж закрити знахідку, повторіть початковий експлойт проти кожного виправлення.

Очікування, що прихований тест знайде все. За SP 800-115, приховане тестування з’ясовує, якої шкоди може завдати зловмисник; воно не перевіряє кожен захисний механізм і не знаходить кожну вразливість, а всередину зазвичай потрапляє через найпростіші слабкі місця. Обирайте відкритий тест, коли мета — охоплення, і прихований, коли мета — дізнатися, чи помітять атаку захисники.

Що почитати далі

- NIST SP 800-115: Technical Guide to Information Security Testing and Assessment — посібник NIST із планування та проведення перевірок безпеки, з чотирма фазами тестування на проникнення та шаблоном правил проведення.
- OWASP Web Security Testing Guide v4.2: Introduction — де місце тестування на проникнення поряд із рецензуванням і аналізом вихідного коду і чому воно не має бути єдиною технікою.
- OWASP WSTG v4.2: Penetration Testing Methodologies — короткий огляд PTES, настанов PCI DSS, PTF, NIST SP 800-115 та OSSTMM.
- NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations — каталог заходів безпеки та приватності від NIST; захід CA-8 стосується тестування на проникнення та правил його проведення.

Словник

Обирайте за фактичними умовами

Опишіть шлях розгортання, експлуатаційні ризики та чергову команду. Ми можемо визначити зміну з перевірками, шляхом відновлення та чіткою відповідальністю.

Дивитися, скільки це коштує Зв'язатися з нами →

Зробіть термінологію практичною

Запитайте, як «Що таке тестування на проникнення?» стосується вашої організації. Конкретного прикладу з поточної системи достатньо для початку розмови.

Переглянути наші послуги

welcome@engineer.company +45 50 10 61 84 Копенгаген, Данія

Візьміть цю сторінку із собою

Візитівка

Дбайливо зроблено з любов'ю — D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Авторське право © 2025 – дотепер · Engineer ApS · Усі права захищено.

Надруковано з https://engineer.company/uk/glossary/penetration-test/