

Аналіз методик співпраці між **Blue Team** та **Red Team** в галузі кібербезпеки





Вступ

В сучасному динамічному цифровому середовищі, де кібербезпека стає необхідністю для забезпечення стабільності та надійності інформаційних систем, актуальність вивчення та розуміння механізмів захисту від кіберзагроз набуває особливого значення. У цьому контексті, співпраця між Blue Team, яка забезпечує захист інформаційних систем, та Red Team, що спеціалізується на симуляції кібератак, визнається як ключовий елемент ефективного кіберзахисту.

Основні поняття та визначення

- **CIA Triad:** Три основні аспекти, які важливі для забезпечення безпеки інформації. Цей термін складається з трьох скорочень, які представляють основні принципи інформаційної безпеки: конфіденційність, цілісність, доступність. Ці три принципи є основними для розуміння та забезпечення ефективного управління безпекою інформації в організаціях.
- **Ланцюг ураження цілі:** Модель визначає необхідні кроки, які вживають атакувальники для досягнення своєї мети. Складається з семи кроків: розвідка, озброєння, доставка, експлуатація, установка, C2, шкідливі дії
- **Zero Trust:** Стратегія безпеки, яка передбачає, що жоден користувач чи пристрій не повинен автоматично вважатися надійним всередині або поза корпоративною мережею, навіть якщо вони вже отримали автентифікацію.
- **Active Directory:** Служба каталогів, яку розробляє та підтримує Microsoft, і яка використовується для управління користувачами, комп'ютерами та іншими ресурсами в корпоративних мережах, побудованих на платформах Windows Server.



Metasploit

Модульний інструменту для пентесту, побудованого на мові програмування Ruby. За допомогою інструментів у складі фреймворку можна проводити пентест заходи, виявляти вразливості в безпеці, проводити атаки та уникати виявлення.

MITRE ATT&CK

Фреймворк, який описує тактики, техніки й процеси кібератак, що використовуються зловмисниками.

OWASP

рекомендації, інструменти та ресурси для забезпечення безпеки веб-додатків, спрямована на виявлення та усунення загроз безпеці в цьому контексті.

Red Team

це команда експертів, яка виконує етичне вторгнення та симулює атаки на інформаційні системи з метою виявлення слабких місць у захисті. Основна роль Red Team полягає в тестуванні відповідності заходів безпеки, виявленні уразливостей та наданні рекомендацій для покращення рівня кіберзахисту. Ця команда використовує тактики, методи та процедури, які може використовувати реальний кіберзлочинець з метою підвищення стійкості систем до потенційних загроз. Red Team сприяє покращенню кібербезпеки шляхом імітації реальних атак та виявлення слабких місць у захисті.

Пентестінг

Проведення етичних хакерських атак для виявлення слабких місць у захисті інформаційних систем.

Аудит безпеки	Перевірка та оцінка заходів безпеки для визначення відповідності стандартам та виявлення потенційних загроз.
Розробка та тестування вразливостей	Створення нових методів атак та їхнє тестування для забезпечення кращого розуміння потенційних загроз.
Аналіз та експлуатація	Ретельний аналіз та використання вразливостей з метою вдосконалення захисту.
Створення стратегій безпеки	Розробка стратегій та рекомендацій для укріплення захисту інформаційних систем.
Симуляція атак	Імітація різних видів атак для оцінки готовності та ефективності заходів безпеки.
Дослідження та розробка інструментів	Вивчення актуальних тенденцій та розробка нових інструментів для покращення методів кіберзахисту.
Підготовка та навчання	Надання навчання та інструкцій для персоналу щодо захисту від потенційних кіберзагроз.

Blue Team

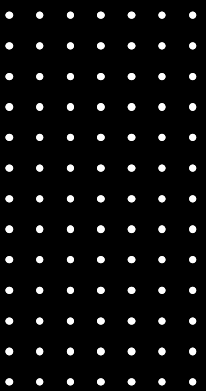
це складова оборонна частина в галузі кібербезпеки, відповідальна за захист інформаційних систем від потенційних кіберзагроз. Головна мета Blue Team - забезпечення цілісності, конфіденційності та доступності даних та ресурсів компанії. Ця команда використовує різноманітні методи та інструменти для виявлення, відстеження та запобігання кібератакам, включаючи встановлення інтрузійних систем, аналіз логів, контроль за використанням прав доступу та розробку стратегій реагування на інциденти. Blue Team грає ключову роль у створенні стійких інформаційних систем та забезпеченні їхньої безпеки в умовах постійно змінюючогося кіберзлочинства.



Моніторинг системи та виявлення загроз

Постійний моніторинг мережі та систем для виявлення аномалій та підозрілих активностей.

Відповідь на інциденти	Реагування на інциденти та швидке виправлення вразливостей під час кібератак.
Конфігурація та управління політиками безпеки	Забезпечення правильної конфігурації систем та виконання політик безпеки.
Аудит та моніторинг логів	Аналіз та моніторинг системних логів для виявлення аномалій чи невизначених подій.
Безпека корпоративних мереж	Захист корпоративних мереж від зовнішніх атак та внутрішніх загроз.
Виявлення та захист від зловживань	Виявлення та захист від неправомірного використання ресурсів та пристроїв.
Реалізація та тестування заходів безпеки	Впровадження та тестування заходів безпеки для укріплення інфраструктури.
Планування та підготовка до атак	Розробка стратегій та підготовка до можливих кібератак для забезпечення готовності команди.



Підходи до організації інфраструктури для співпраці Blue Team та Red Team



Ізольовані середовища: Red Team та Blue Team можуть працювати в ізольованих середовищах, які не пов'язані між собою. Це забезпечує максимальний захист Blue Team від атак Red Team.

Спільне середовище: Red Team та Blue Team можуть працювати в спільному середовищі. Це забезпечує більш реалістичне середовище для атак, але також підвищує ризик для Blue Team.

Гібридний підхід: Red Team та Blue Team можуть працювати в гібридному середовищі, яке включає в себе як ізольовані, так і спільні середовища. Цей підхід забезпечує найкращий баланс між безпекою та реалістичністю.



Стратегія Red Team



Penetration Testing	Кібератаки, які симулюються та налаштовуються для досягнення конкретних тестових завдань
Social Engineering	Практика психологічного обману кого-небудь для отримання конфіденційної інформації
Phishing	Практика звертання до жертви та контактування з нею за допомогою текстових повідомлень, телефону чи електронної пошти, представляючи себе як офіційна компанія
Перехоплення зв'язку	Перегляд вмісту електронних листів, телефонних розмов та інших електронних комунікацій шляхом їх перехоплення
Клонування біометрії	Процес створення магнітно-смугових карток за допомогою викрадених даних з платіжних карток з чіпами EMV

Стратегія Blue Team

- Перевірку DNS для запобігання розсилці фішингових атак;
- Використання цифрового аналізу для встановлення базового рівня мережевої активності та полегшення виявлення аномальної поведінки;
- Встановлення антивірусного програмного забезпечення на віддалених комп'ютерах та мобільних телефонах;
- Використання програмного забезпечення як засобу детекції та запобігання для систем виявлення та запобігання вторгнень, або IDS та IPS;
- Переконавання в правильності налаштування та впровадження засобів периметрової безпеки, зокрема брандмауерів та антивірусних програм.





Аналіз сучасного підходу до співпраці

Заходи червоний-проти-синього підтверджують, що системи оборони забезпечують ефективний захист від атак, для яких вони були призначені відвертати, але не здатні виявляти складні атаки. Саме такі заходи дають можливість Blue Team отримати досвід та інформацію про вразливості свого захисту, перед реальними хакерами, які шукають нестандартні шляхи прогнікнення до мережі. Зрештою, такі заходи мали б більш вагомий результат, якби учасники могли взаємодіяти більш тісно і якщо всі команди брали участь у всіх фазах заходу. Якщо б Red Team отримували би інформацію про мережу таку, як слабкі місця, які слід більш ретельно перевіряти і на яких треба фокусуватися, не витрачаючи час на «кролячі діри». Та якщо Blue Team мало дозвіл переналаштовувати свою програму після кожної успішної атаки, якість оборони швидко покращилася.

Для покращення стратегії взаємодії пропоную наступну модель: команда Blue Team використовує платформу співпраці, щоб надати Red Team доступ до сеансу обміну екраном на одній з можливо уразливих систем. Red Team може виявити помилковий позитивний результат за десять хвилин, тоді як на його розслідування витратили б години. Крім того, Blue Team зможе виявити збої в платформі оплати компанії, хоча їх не можна однозначно призначити Red Team чи чому-небудь іншому. Спільно команди вдасться виявити вразливість щодо доступності платформи, обмінюючись логами та проводячи обговорення.

- Регулярні тренування
- Автоматизація інцидент-відгуку
- Забезпечення обміну інформацією



Висновки

1. Важливість кібербезпеки: Захист кіберпростору визнається як надзвичайно важливе завдання. Для успішного вирішення цього завдання необхідно відділяти дії в межах нормативно-правових актів, дотримуватися законодавства, стандартів та використовувати новітні технології для ефективного захисту від кіберзагроз.
2. Аналіз ключових фреймворків: Ретельний аналіз ключових фреймворків та стандартів визначає надійну основу для розробки та реалізації стратегій захисту. Детальний огляд нормативних вимог та методик забезпечення безпеки сприяє комплексній безпеці кіберпростору.
3. Роль Red Team: Дослідження Red Team підкреслює важливість активного підходу у сфері кіберзахисту. Виявлення вразливостей та недоліків через проведення пенетраційних тестів та імітацію атак допомагає попереджати можливі загрози, сприяючи підвищенню загального рівня кібербезпеки.
4. Роль Blue Team: Дослідження Red Team вказує на важливість створення резистентних механізмів у відповідь на кіберзагрози. Застосування методик, таких як виявлення вразливостей та контроль доступу, свідчить про необхідність постійного удосконалення заходів для ефективного протистояння кібератакам.
5. Координація команд Red та Blue: Розгляд ролей та стратегій команд Red та Blue виявляє важливість їхньої координації. Агресивні атаки Red Team та проактивні заходи безпеки Blue Team в синергії сприяють ефективній реакції на кіберзагрози та виявленню вразливостей.
6. Експеримент з DDoS атаками: Розгляд конкретного випадку співпраці між Red та Blue team у перевірці захисту мережі від DDoS атак підкреслює важливість взаємодії між командами для подолання викликів у кібербезпеці. Застосування технологій COSSAK та D-WARD підкреслює ключову роль синергії для досягнення максимального рівня кіберзахисту.
7. Аналіз взаємодії команд: Комплексний аналіз взаємодії команд Red та Blue виявляє ключові проблеми, такі як недостатній рівень комунікації та обміну зворотнього зв'язку, що впливає на ефективність заходів у кіберзахисті.
8. Рекомендації для покращення кіберзахисту: Розроблені рекомендації базуються на глибокому аналізі проблем та можливостей. Вони наголошують на об'єднанні команд, постійному обміні інформацією та спільному розробленні стратегій захисту для досягнення вищого рівня кібербезпеки.