Особенности тестирования на проникновение. Мониторинг событий безопасности – преимущества аутсорсинга

Андрей Березов
Руководитель департамента информационной безопасности
ООО «Информационный центр»
(423) 240-48-66 доб. 7201
and@ic-dv.ru

Нормативное обоснование

С вступлением в силу новой нормативной документации требование проведения ежегодного пентеста осталось.

Положение Банка России от 17 апреля 2019 г. N 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»:

3.2. Кредитные организации должны обеспечить ежегодное тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры.

ГОСТ Р 57580.1-2017:

ЖЦ.14. Реализация контроля защищенности АС, включающего тестирование на проникновение.

ЖЦ.20. Реализация проведения ежегодного контроля защищенности АС, включающего тестирование на проникновение.

Чем **не является** пентест

Тестирование на проникновение – метод оценки безопасности компьютерных сетей средствами моделирования атаки злоумышленника. (с) Википедия

«Мы просканировали вашу сеть изнутри и снаружи разными сканерами уязвимостей – вот вам отчеты этих сканеров» – это не пентест.

Пентест не является киберучениями и противостоянием Blue Team и Red Team. Время пентеста, как правило, ограничено поэтому команда тестирования не тратит время на stealth-сканирования и «заметание следов» своей деятельности. Если службы ИТ и ИБ, осведомленные о проведении пентеста, активно противостоят команде тестирования, предполагается, что такое активное противостояние злоумышленникам осуществляется всегда.

В ходе пентеста не осуществляется поиск zero-day уязвимостей в соответствии с моделью нарушителя.

Модель нарушителя

«Вы нам вчера выдали отчет по пентесту, а сегодня появились публикации о новой страшной 0-day уязвимости. Она у нас есть, а вы в отчете не указали…»

Типичный нарушитель:

- внешний нарушитель, обладающий обширными знаниями в сфере информационных технологий и информационной безопасности, умеет проводить исследования систем общедоступными инструментами, умеет эксплуатировать общеизвестные уязвимости;
- внутренний нарушитель с непривилегированным доступом к информационной системе или без прав логического доступа (проник в КЗ и включил ноутбук в сеть);

Типичный нарушитель **не является** научно-исследовательским центром, спецслужбой какого-либо государства, организованной криминальной группировкой и **не обладает** неограниченными временными, финансовыми и интеллектуальными ресурсами.

Дорого и долго…

«Тестирование на проникновение стоит дорого, тестируют долго, а отчет всего на 30 страниц…»

Хороший пентестер – зверь редкий, востребованный и дорогой.

Стоимость пентеста формируется из человеко-часов, затрачиваемыми на пентест.

Можно сократить стоимость, сократив перечень тестируемых ресурсов, но тогда могут остаться непроверенные уязвимые места.

Большая часть работы остается «за кадром». В отчет попадают только успешно проэксплуатированные уязвимости, скомпрометированные данные, явно выявленные слабые места в системе защиты информации.

Результаты сканирований проверяются вручную. Часто осуществляется ручной анализ доступного кода веб-приложений. Анализ POST/GET-запросов. Некоторые проблемы требуют простой удачи и «угадывания» каких-либо параметров.

По запросу могут быть предоставлены все «сырые данные».

Почему нельзя обойтись анализом уязвимостей?

- большое количество ложноположительных срабатываний сканеров;
- даже если уязвимость действительно есть, ее эксплуатация может быть невозможна из-за принятых мер;
- пример: уязвимость BlueKeep имеет 2 возможных применения: уход хоста в BSOD и выполнение на хосте произвольного когда – было бы неплохо проверить что работает, а что нет именно у нас, чтобы понимать риски;
- выявление решений основанных на принципе Security Through Obscurity (например, формы авторизации на нестандартных портах);
- выявление «случайно» попавших на сайт компании конфиденциальных документов;
- выявление чувствительных данных в метаданных файлов, легально опубликованных на сайте компании;
- сканеры не реализуют сложную цепочку действий.

Пример сложной цепочки действий

- путем анализа сайта выявляем возможных пользователей (публикация информации о работниках госучреждения);
- там же узнаем некоторые личные данные возможных пользователей системы, например сконцентрируемся, например, на Иванове И.И.;
- путем анализа соцсетей узнаем, что у Иванова И.И. есть единственный ребенок - дочь Василиса 1994 года рождения;
- из метаданных файлов узнаем о наличии в системе пользователя ivanov.ii;
- находим форму удаленной авторизации пользователей на «нестандартном» порту;
- путем недолгого перебора входим в систему с учетными данными ivanov.ii/Vasilisa1994;
- отражаем в отчете.

Кто тестирует?

Качество пентеста напрямую зависит от квалификации команды тестирования.

Наша команда:

- специалисты департамента информационной безопасности (обширные знания в ИТ + практический опыт проектирования систем защиты информации);
- специалисты Security Operation Center (обширные знания в ИТ + практический опыт выявления и разбора инцидентов информационной безопасности).

+ постоянное самообучение методам и практике тестирования на проникновение;

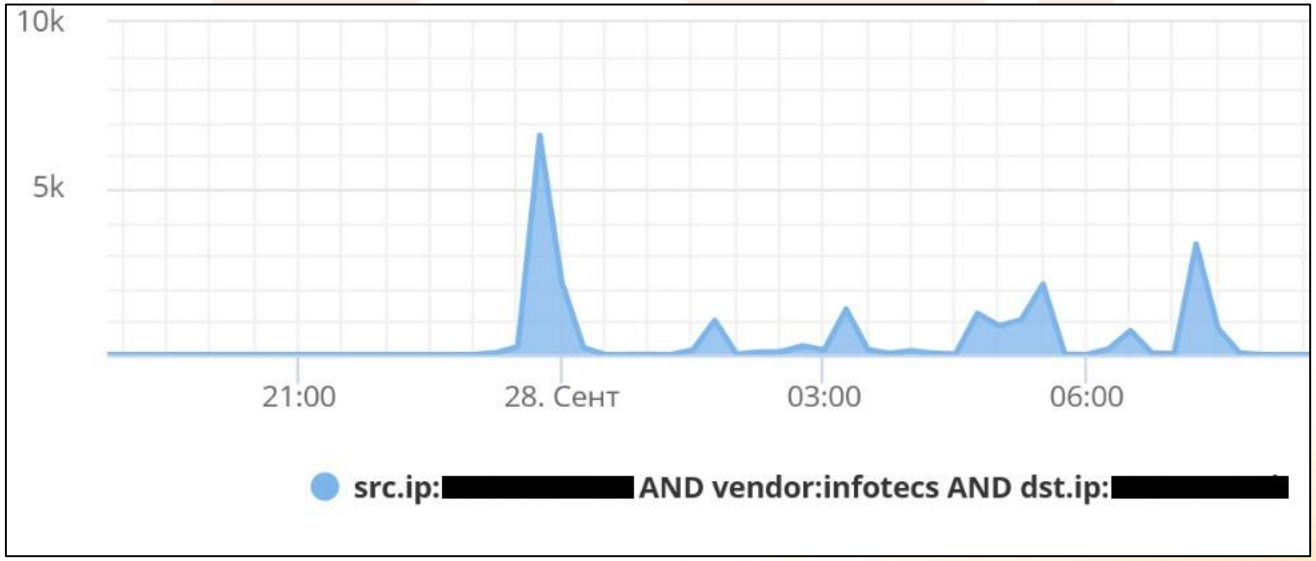
+ обучение на курсах по тестированию на проникновение (Codebe, EC-Counsil, Specialist)

+ постоянный практический опыт тестирования на проникновение.

Что в итоге дает пентест (кроме выполнения требований регулятора)?

Независимую оценку фактического уровня защищенности информационной системы.

Возможность проверки эффективности внедренных средств защиты информации, в том числе системы мониторинга событий безопасности.



Всплески EPS в SIEM во время тестирования

Мониторинг событий ИБ, нужен ли?

В соответствии с ГОСТ Р 57580.1-2017 две основные группы мер:

РИ – Обнаружение и регистрация инцидентов защиты информации.

МАС – Мониторинг и анализ событий защиты информации.

Большое количество дополнительных мер:

ЦЗИ.20 – Контроль состава разрешенного для использования ПО.

ВСА.1-8 – Контроль отсутствия (выявление) аномальной сетевой активности, связанной с …

Все указанные меры предписаны для выполнения буквой «Т», что означает техническое выполнение, только организационными мерами отделаться не получится…

Как выполнить эти требования?

Нужно развернуть Security Operation Center (SOC) в несколько «простых» шагов

1. Внедрение SIEM-системы (SIEM – Security Information and Event Management, система управления событиями безопасности).
2. Настройка пересылки событий безопасности с источников на SIEM.
3. Настройка нормализации событий безопасности в SIEM.
4. Добавление индикаторов компрометации в SIEM.
5. Написание правил корреляции событий безопасности.
6. Найм аналитиков SIEM.
7. Регистрация и анализ инцидентов.
8. Выявление огромного числа false-postive инцидентов, совершенствование правил корреляции, добавление новых источников…
9. Реагирование на инциденты.

~~10. Поиск новых аналитиков, потому что старые сбежали~~

Острее всего стоит кадровый вопрос.

Можно подключиться к внешнему SOC

Вам больше **не нужно**:

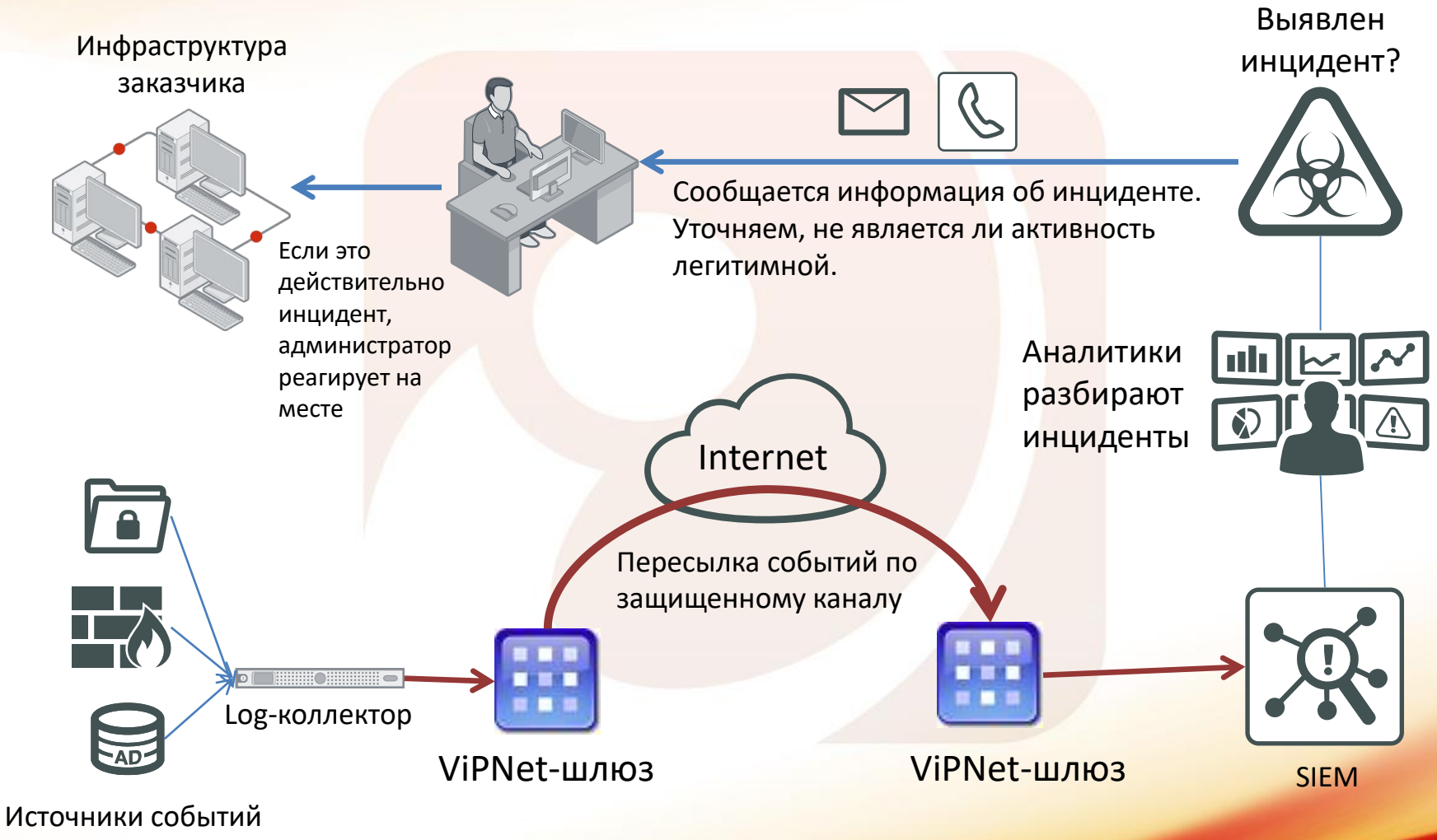
- полноценно разворачивать SIEM в своей инфраструктуре;
- осуществлять нормализацию событий ИБ;
- актуализировать индикаторы компрометации;
- писать корреляции событий;
- держать в штате собственных аналитиков;
- анализировать тысячи false-positive «инцидентов».

Вам **все еще нужно**:

- развернуть в своей инфраструктуре log-коллектор (бесплатная лицензия);
- иметь в наличии источники событий (AD, FW, IDS, Proxy и т. д.);
- следить на своей стороне за корректной работой источников и log-коллектора;
- организовать со своей стороны защищенный канал ViPNet для передачи событий ИБ до SOC;
- держать в штате администратора ИБ, реагирующего на инциденты на месте.

Стоимость мониторинга событий безопасности как услуги зависит от количества узлов и количества источников событий ИБ, но это всегда дешевле развертывания собственного SOC.

Как это работает?



Благодарю за внимание!

Андрей Березов
Руководитель департамента информационной безопасности
ООО «Информационный центр»
(423) 240-48-66 доб. 7201
E-mail: and@ic-dv.ru