Метрика поверхности атак внешнего периметра

# Постановка задачи

Представим, что мы проводим blackbox-сканирование сетевого периметра большой информационной системы (или большой организации) в рамках задачи External Attack Surface Management (EASM). По результатам сканирования мы должны дать оценку, насколько хорошо этот периметр защищен. При этом:

* Оценка должна одинаково восприниматься как специалистами по информационной безопасности «красных» и «синих» команд, а также менеджментом организации различных уровней;
* оценка должна позволять сравнивать защищенность периметров организаций и оценивать динамику защищенности периметра организации.

Какой-то единой, общепризнанной и научно обоснованной методики такой оценки не существует, и едва ли она в обозримом будущем появится. Значит, мы вынуждены опираться на экспертную оценку. Эксперт может оценить защищенность периметра в категориях “периметр А хорош”, “периметр Б плох”, “узел В сегодня лучше, чем вчера”.

Но этого недостаточно по целому ряду причин:

* Экспертные оценки субъективны (“периметр А хорош, так как я так и не сумел его пробить”, “узел В сегодня лучше, чем вчера, потому что сегодня я смог лишь подменить контент через XSS, а вчера мог получить полный контроль над ним”).
* Эксперт, как правило, оперирует дискретными показателями и не может ответить, насколько “хорош” или “плох” тот или иной периметр.

Значит. нам нужно выразить экспертную оценку количественным или качественным показателем (метрикой), и этот показатель должен удовлетворять следующим условиям:

* одинаково вычисляться любым исполнителем на одних и тех же исходных данных;
* основываться на содержательных предпосылках;
* быть правдоподобным, т.е. рассчитанный показатель не должен вызывать возражения со стороны большинства экспертов, согласных с исходными предпосылками.

# Предпосылки

Так как метрика вычисляется только по результатам blackbox сканирования, набор исходных данных, на которых можно вычислять метрики, очень ограничен. В дальнейшем, когда в нашем распоряжении будет более широкий набор средств анализа защищенности, мы сможем учитывать информацию о характере и ценности активов, их сетевую связность, точный состав программных и аппаратных средств и т.п – но пока мы можем вычислять метрики лишь на основе информации об уязвимостях сетевых сервисов.

Поэтому в качестве первого приближения под защищенностью будем понимать отсутствие уязвимостей или невозможность эксплуатации этих уязвимостей. Примерно так в своих нормативных документах трактует защищенность информационных систем ФСТЭК (информационная система может быть допущена к эксплуатации только после того, как будет подтверждено отсутствие уязвимостей или невозможность их использования для реализации угроз), но для нас это просто первый шаг к конструированию метрики.

Итак, оцениваемый показатель должен зависеть от количества и степени опасности уязвимостей, выявленных на периметре. Для степени опасности уязвимости уже есть общепринятая методика численной оценки – это базовая и временна́я оценки опасности по CVSS (CVSS Base Score и CVSS Temporal Score, описаны [здесь](https://www.first.org/cvss/v3.1/specification-document)).

Базовую оценку можно взять в базе уязвимостей, например – в [NVD](https://nvd.nist.gov/) или [БДУ](https://bdu.fstec.ru/vul) ФСТЭК. Она принимает значения от 1.6 до 10.0 с шагом 0.1 и складывается из двух экспертных оценок: оценка вреда и оценка гипотетическую возможности эксплуатации. Но как практиков нас интересует не гипотетическая, а реальная возможность эксплуатации: известны ли случаи использования уязвимости, есть ли к ней готовый эксплойт и т.п.). Для уязвимостей, отсутствующих в этих базах (например, самостоятельно найденных 0day), базовую оценку придется рассчитать самостоятельно в соответствии со спецификациями CVSS.

Реальная (в нашем понимании) возможность эксплуатации учтена в временно́й оценке опасности уязвимостей, она получается умножением базовой оценки на понижающие коэффициенты . Коэффициент E (Exploit Code Maturity) отвечает за наличие и качество эксплойта, коэффициент RC (Report Confidence) отвечает за достоверность сведений об уязвимости (подтверждена вендором, есть воспроизводимые исследования, есть частичное описание и т.п.). Коэффициент RL (Remediation Level) характеризует возможный способ устранения уязвимости (официальный патч, воркэраунд, патч отсутствует и т.п.), но так как нас интересует только сам факт наличия уязвимости и ее эксплуатабельность здесь и сейчас, этот коэффициент нам не интересен.

Уязвимости мы делим на градации степени опасности, исходя из их практической пригодности для преодоления периметра:

* Temporal Score в диапазоне от 9.5 до 10.0 (уровень опасности “Шторм”) практически гарантирует, что нарушитель может получить контроль над узлом. В эту категорию попадают уязвимости, для которых подтверждено наличие готовых инструментов эксплуатации или которые совсем не требуют каких-либо эксплойтов.
* Temporal Score в диапазоне от 9.0 до 9.4 (критический уровень опасности) говорит о том, что уязвимость с высокой вероятностью позволит нарушителю получить контроль над узлом. К неуспеху может привести только нестабильность эксплойта или техническая сложность эксплуатации, но в целом для нарушителя это не является непреодолимым препятствием.
* Temporal Score в диапазоне от 7.0 до 8.9 соответствует уязвимостям с высоким уровнем опасности. Это уязвимости, эксплуатация которых или не позволяют нарушителю пробить периметр, предоставляя ему лишь ограниченные дополнительные возможности, или требует значительных усилий, например – реверса патчей и самостоятельной разработки эксплойтов.
* Уязвимости среднего уровня (Temporal Score от 4.0 до 6.9) позволяют причинить уязвимому узлу некоторый вред, но их эксплуатация не приводит к каким-то серьезным последствиям.
* Уязвимости низкого уровня (Temporal Score до 3.9) не опасны ни в каком сочетании.

Таким образом разделение уровня опасности на градации – это взгляд на уязвимый узел глазами атакующего, исходя из того, насколько уязвимости узла полезны именно ему.

Как описать уровень защищенности узла, исходя из знания степени опасности его уязвимостей? Мы хотим оценить это состояние числом по шкале от 0 до 1000. Эту шкалу мы делим на четыре градации:

* <200 – «шторм», то есть на узле есть уязвимости, требующие немедленного устранения;
* от 201 до 500 – низкий уровень, характерный для многих слабозащищенных узлов в сети Интернет;
* от 501 до 800 – средний уровень защищенности, при котором атакующий способен добиться некоторого успеха;
* 801-1000 – отличный уровень, для достижения которого требуется целенаправленное оперативное устранение уязвимостей.

# Граничные условия

Как сконструировать метрику, с помощью которой можно было бы отобразить сведения об уязвимостях на такую шкалу? Прежде всего, нужно задать граничные условия – оценочные критерии, при выполнении которых эксперт готов согласиться, что сконструированная метрика правдоподобна. Мы остановились на следующих критериях правдоподобности:

* Наличие на узле даже единичной уязвимости уровня “шторм” делает узел беззащитным перед атакующим – его уровень защищенности должен попадать в градацию “шторм”.
* Аналогично, наличие на узле даже единичной критической уязвимости создает серьезную угрозу, и уровень защищенности узла должен быть признан низким.
* Уровень защищенности узла, на котором присутствуют уязвимости только среднего и низкого уровней опасности, должен быть признан средним
* На узле со средним уровнем защищенности допустимо появление единичных уязвимостей высокого уровня опасности. Но с ростом их числа количество переходит в качество: при превышении некоторого порогового значения уровень защищенности такого узла должен быть понижен до низкого.
* На узле с высоким уровнем защищенности недопустимо наличие уязвимостей с уровнем опасности, отличным от низкого.

Таким образом, как мы уже говорили выше, метрика – это не физическая величина, которую можно было бы обосновать научно, а лишь численное выражение мнения эксперта о том, можно ли пробить периметр путем атаки на узел с вот таким набором уязвимостей.

# Конструирование метрики

Для того, чтобы метрику можно было однозначно вычислить, ее необходимо задать в виде математической функции. Для этого нам нужно определить общий вид функции и подобрать такие ее параметры, чтобы вычисленное значение метрики соответствовало граничным условиям. Эту задачу можно решать самыми разными способами, и мы остановились на подходе, основанном на “штрафах”.

Узел, на котором отсутствуют уязвимости, мы считаем защищенным идеально – его метрика уровня защищенности равна 1000. Каждая уязвимость “штрафует” узел, снижая его уровень защищенности на некоторую величину. Но эти “штрафы” неравноценны:

* В силу граничных условий даже единичная уязвимость с уровнем опасности “средний”, “критический” или “шторм” должна понизить значение метрики до верхней границы уровней защищенности “средний”, “низкий” или “шторм” соответственно. Эти граничные условия задают минимальные значения “штрафов” для единичных уязвимостей.
* “Штраф” за несколько уязвимостей одинакового уровня опасности должен быть выше “штрафа” за единичную уязвимость. При этому уязвимостей на узле может быть бесконечно много, но в силу граничных условий суммарный “штраф” за однотипные уязвимости ограничен – значит, математическое выражение “штрафа” за однотипные уязвимости должно иметь асимптотическую верхнюю границу.

“Штрафы” с такими свойствами удобнее всего описывать с помощью гипербол, имеющих общий вид , где F – штраф за выявленные на узле уязвимости уровня опасности i, Fmax – предельный штраф за уязвимости этого уровня опасности, TS – сумма Temporary Score этих уязвимостей, а k и b – параметры, определяющие точный вид гиперболы для данного уровня опасности уязвимостей.

Гипербола – линия второго порядка, поэтому для определения параметров k и b требуется задать три ее точки, например:

* минимальное значение “штрафа” за единичную уязвимость с минимальным для данного уровня опасности значением Temporary Score;
* предельное значение “штрафа”;
* значение “штрафа” в какой-то промежуточной точке, например – при выявлении на узле пяти уязвимостей с минимальным для данного уровня опасности значением Temporary Score.



Рисунок – Так мог бы выглядеть штраф за уязвимости среднего уровня опасности

Таким образом, выявленные на узле уязвимости задают отдельные “штрафы” для каждого уровня опасности уязвимостей:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Уровень опасности | Fmin[[1]](#footnote-1) | TSmin | F(5\*TSmin) | Fmax | Формула |
| Низкий | 1 | 1.2 | 100 | 199 |  |
| Средний | 200 | 4.0 | 300 | 399 |  |
| Высокий | 400 | 7.0 | 500 | 599 |  |
| Критический | 600 | 9.0 | 700 | 799 |  |
| Шторм | 800 | 9.5 | 900 | 1000 |  |

Если смотреть на узел глазами атакующего, то наличие на нем уязвимостей определенного (например, высокого) уровня опасности делает неинтересным для нарушителя наличие уязвимостей более низких уровней опасности. В терминах метрики “штраф” за наличие уязвимостей более высокого уровня опасности “поглощает” “штрафы” за наличие уязвимостей более низких уровней опасности, и метрика уровня защищенности узла выглядит так:

Соответственно, уровень защищенности периметра равен минимальному из уровней защищенности его узлов.

# Как мы считаем временну́ю оценку уровня опасности уязвимости

Если значения оценки CVSS Base Score можно найти в базах уязвимостей, то значения Temporal Score приходится вычислять самостоятельно. Как мы уже писали выше, в спецификациях CVSS Temporal Score считается по формуле

Коэффициент RL нас не интересует, поэтому его мы считаем равным единице для всех уязвимостей.

Коэффициент E мы определяем наличию информации об экслойтах:

* E=1, если уязвимость присутствует в Known Exploited Vulnerabilities Catalog или если в фидах присутствует информация о информация о практическом применении эксплойта или если для эксплуатации уязвимости не требуется специальный эксплойт (соответствует компоненту E:H временно́го вектора CVSS);
* E=0.97, если в описаниях уязвимости есть указание на наличие эксплойта 'Exploit' (соответствует компоненту E:F временно́го вектора CVSS);
* E=0.88 в остальных случаях (соответствует компоненту E:U временно́го вектора CVSS).

Коэффициент RC мы так же определяем по описаниям уязвимости:

* E=1, если в описании уязвимости есть ссылки на бюллетени вендора (соответствует компоненту RC:C временно́го вектора CVSS);
* E=0.96, если в описании уязвимости ест ссылки только на источники, отличные от официальных сайтов вендора (соответствует компоненту RC:R временно́го вектора CVSS);
* E=0.88 в остальных случаях (соответствует компоненту RC:U временно́го вектора CVSS).

# Критика

Еще раз напомним, что, как и большинство метрик безопасности, данная метрика является лишь численным выражением экспертной оценки. Поэтому и общий вид функции, и ее параметры – это не научно обоснованные физические величины, они искусственно подобраны так, чтобы результат расчета метрики максимально соответствовал оценке эксперта.

Нетрудно заметить, что с ростом количества однотипных уязвимостей их вклад в метрику снижается. Это осознанное решение, так как метрика строится по результатам blackbox-сканирования. Увеличение количества уязвимостей, как правило, не переходит в изменение качества (за исключением уязвимостей высокого уровня опасности, что учтено в данной метрике), и оно очень быстро перестает увеличивать возможности атакующего.

По той же причине метрика не может учитывать важность активов для защищающейся стороны, сетевую связность и возможность проведения цепочек атак – blackbox-сканирование просто не дает необходимых для их учета исходных данных.

1. Минимальное значение штрафа при наличии хотя бы одной уязвимости данного уровня опасности. При отсутствии уязвимостей этого уровня опасности “штраф” за них равен нулю. [↑](#footnote-ref-1)