КОНСТРУИРОВАНИЕ МЕТРИК

на примере уровня защищенности узла

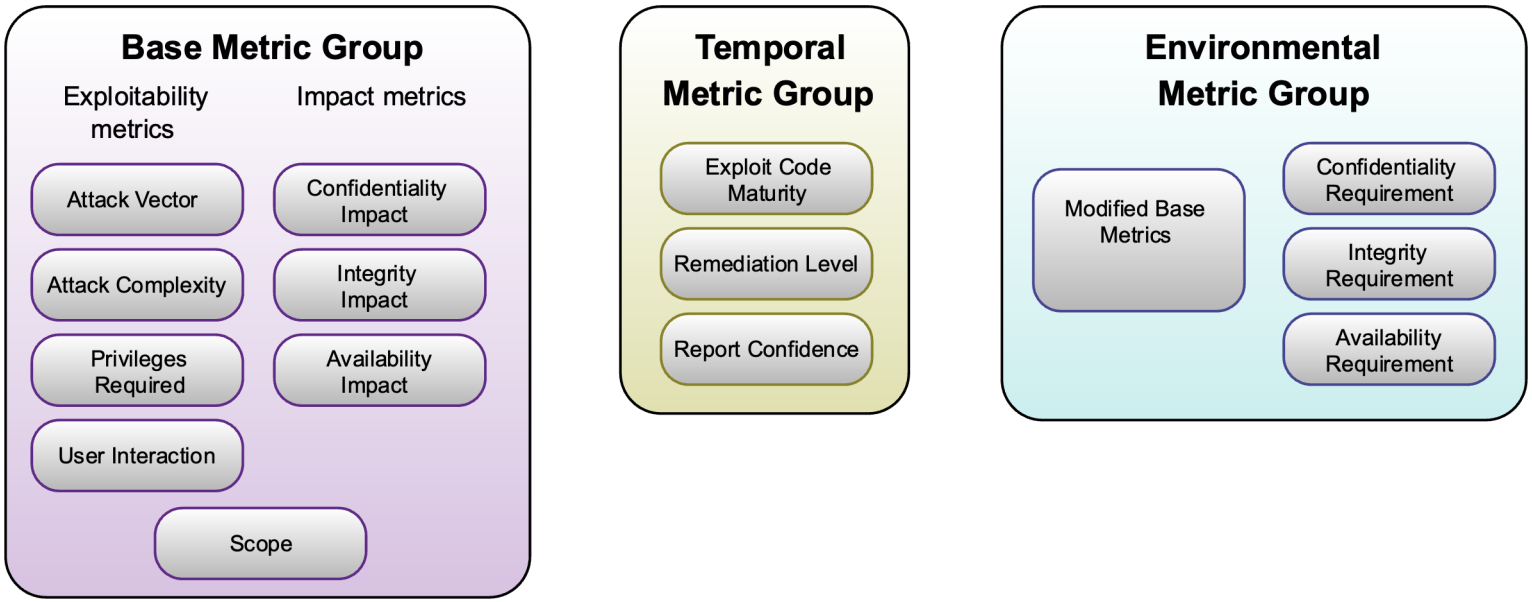
ЧТО МЫ ХОТИМ ОТ МЕТРИКИ

- Строим на основе только **blackbox**-сканирования
- Должна показывать, насколько узел уязвим к атакам
- Должна основываться на понятных предпосылках
- Автоматизироваться в рамках **External Attack Surface Management (EASM)**
- Должна быть правдоподобной
- Одинаково восприниматься экспертами «красных» и «синих» команд и менеджментом

Метрика – не научно обоснованная оценка защищенности, а лишь численное выражение экспертного мнения

СТЕПЕНЬ ОПАСНОСТИ УЯЗВИМОСТИ

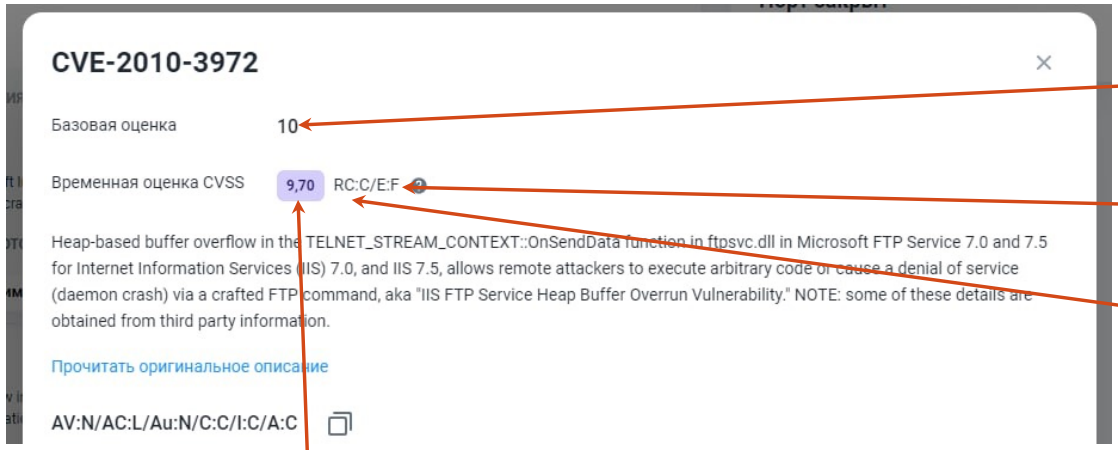
- **CVSS** – общепринятая методика оценки уровня опасности уязвимости



Подробнее – тут https://habr.com/ru/company/pt/blog/266485/

СТЕПЕНЬ ОПАСНОСТИ УЯЗВИМОСТИ

Vuln ID	Summary	CVSS Severity
CVE-2010-3972	Heap-based buffer overflow in the TELNET_STREAM_CONTEXT::OnSendData function in ftpsvc.dll in Microsoft FTP Service 7.0 and 7.5 for Internet Information Services (IIS) 7.0, and IIS 7.5, allows remote attackers to execute arbitrary code or cause a denial of service (daemon crash) via a crafted FTP command, aka "IIS FTP Service Heap Buffer Overrun Vulnerability." NOTE: some of these details are obtained from third party information. **Published:** December 23, 2010; 1:00:02 PM -0500	*V3.x:*(not available) *V2.0:* 10.0 HIGH



CVSS Base Score

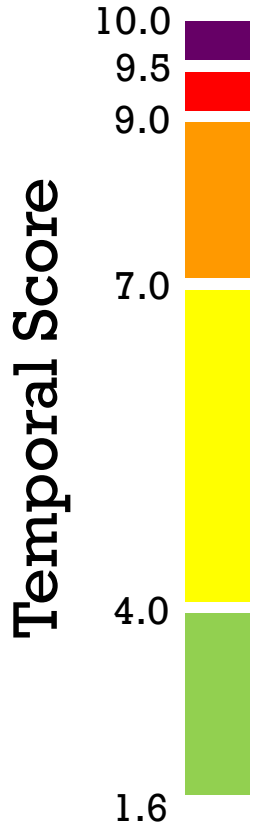
Есть ли эксплойт?

Насколько достоверны сведения?

CVSS Temporal Score = CVSS Base Score * RC * E

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

УРОВНИ ОПАСНОСТИ УЯЗВИМОСТЕЙ



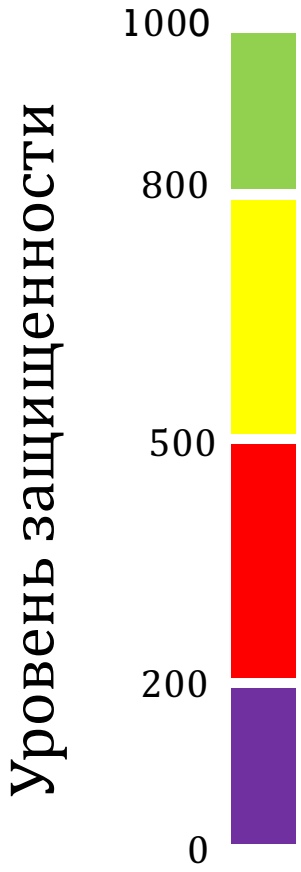
«Шторм»: можно гарантированно получить контроль над узлом
Критический: почти всегда можно получить контроль над узлом

Высокий: можно серьезно навредить узлу или получить интересные возможности

Средний: теоретически можно что-то сделать, но на практике – вряд ли

Низкий: “тоже уязвимости”

ИТОГОВАЯ МЕТРИКА



Высокий уровень: уязвимостей нет или с ними ничего нельзя сделать

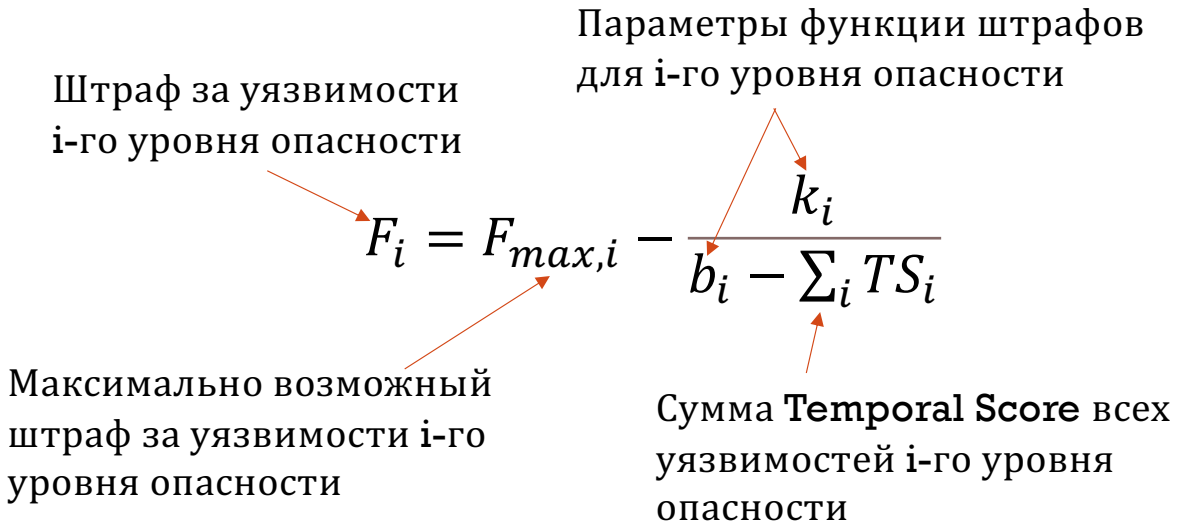
Средний уровень: атакующий может добиться какого-то заметного успеха

Низкий уровень: характерен для многих слабозащищенных узлов в сети Интернет

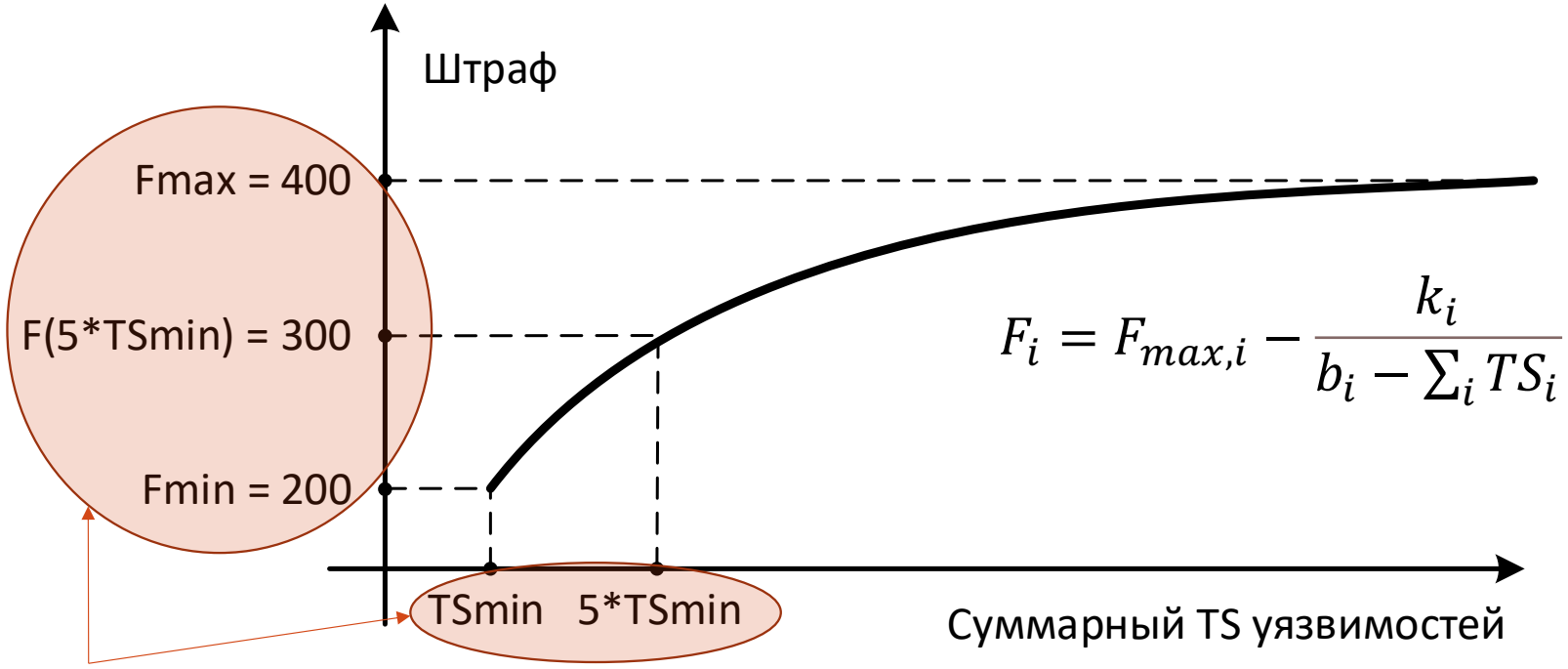
«Шторм»: есть уязвимости, требующие немедленного устранения

КАК СЧИТАЕМ

1. Делим уязвимости на группы, соответствующие уровням опасности
2. Считаем «штраф» отдельно за каждую группу уязвимостей
3. Максимальный из «штрафов» вычитаем из 1000



ФУНКЦИЯ ШТРАФОВ



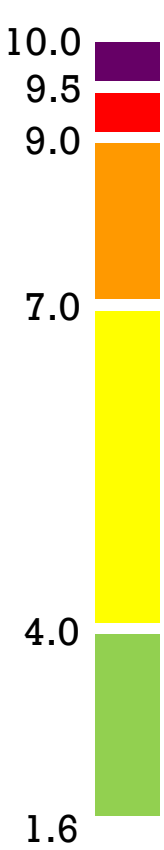
Определяют значения параметров гиперболы $F_{max,i}$, k_i и b_i

ФОРМУЛЫ ШТРАФОВ

Уровень опасности	Fmin	TSmin	F(5*TSmin)	Fmax	Формула
Низкий	1	1.2	100	199	$F_{н} = 199 - \frac{950.4}{3.6 + TS_{н}}$
Средний	200	4.0	300	399	$F_{с} = 399 - \frac{3152.16}{11.84 + TS_{с}}$
Высокий	400	7.0	500	599	$F_{в} = 599 - \frac{5516.28}{20.72 + TS_{в}}$
Критический	600	9.0	700	799	$F_{к} = 799 - \frac{7092.36}{26.64 + TS_{к}}$
Шторм	800	9.5	900	1000	$F_{ш} = 1000 - \frac{7600}{28.5 + TS_{ш}}$

$$Score = 1000 - \max(F_{ш}, F_{к}, F_{в}, F_{с}, F_{н})$$

ПРИМЕР



Уязвимости:

9.2	9.0	6.1	3.5	2.0

$$F_{\text{н}} = 199 - \frac{950.4}{3.6+3.5+2.0} = 94 \qquad F_{\text{к}} = 799 - \frac{7092.36}{26.64+9.0+9.2} = 641$$

$$F_{\text{с}} = 399 - \frac{3152.16}{11.84+6.1} = 223 \qquad F_{\text{ш}} = F_{\text{в}} = 0$$

$$Score = 1000 - \max(0, 641, 0, 223, 94) = \mathbf{359}$$