УДК 004.056

© Черноскутов А.И., Мукминов В.А.

ОЦЕНКА ДОСТОВЕРНОСТИ И ЭФФЕКТИВНОСТИ ТЕСТИРОВАНИЯ СЕТИ С ПОМОЩЬЮ СКАНЕРОВ БЕЗОПАСНОСТИ

Осуществлена проверка результатов опроса с помощью Интернета российских потребителей, проведенного на сайте www.securitylab.ru, и расчетов Учебного центра «Информзащита» по выявлению предпочтительного сканера из четырех наиболее распространенных.

В работе [1] отмечается, что в качестве одной из систем анализа защищенности сетей, занимают сканеры безопасности, позволяющие выявить ряд уязвимостей. Перед потребителями возникает вопрос выбора наиболее пригодного сканера безопасности для тестирования сети на устойчивость к взлому. Согласно опросу российских потребителей, проведенному на сайте www.securitylab.ru, степень популярности сканеров безопасности при тестировании сети на устойчивость к взлому характеризуется табл. 1.

Специалистами Учебного центра «Информзащита» [1] было проведено объемное исследование по нахождению реальных уязвимостей в сети с помощью четырех сканеров, результаты которого отражены в табл. 2.

Достоверность тестирования сети на выявление ее уязвимостей

Составим схему оценки достоверности контроля сети сканером безопасности (рис. 1).

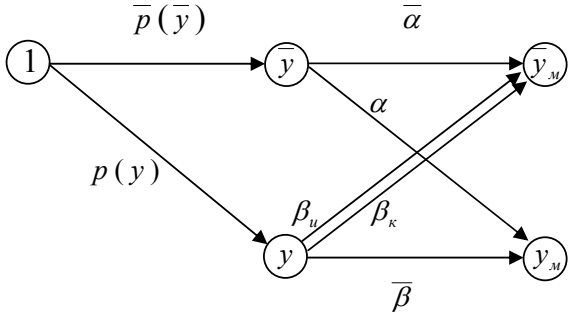

Рис.1. Схема оценки достоверности контроля сети сканером безопасности

Таблица 1

Рейтинги популярности сканеров

№ п/п	Наименование сканера	Популярность сканеров безопасности в России [%]	Рейтинг популярности
1	XSpider	42	1
2	Internet Scaner	2	4
3	Nessus	11	2
4	Retina Network Security Scaner	6	3

Примечание: Сумма в процентах популярности сканеров не составляет 100%,, так как из рассмотрения выпал ряд сканеров: LanGuard – 15%, SSS – 7% и др..

Таблица 2

Исходные данные по уязвимостям

№ п/п	Результаты сканирования	XSpider	Internet Scaner	Nessus	Retina Network
1	Найдено уязвимостей, всего	122	57	87	56
2	Ложные срабатывания (ЛС)	3	4	23	16
3	Найдено уязвимостей без ЛС	119	53	64	40
4	Пропуски уязвимостей (инструментальные)	0	15	34	30
5	Пропуски уязвимостей (конструкторские)	47	98	68	96

Черноскутов Анатолий Иванович – доктор технических наук, главный научный сотрудник 4 ЦНИИ Минобороны России;
Мукминов Владислав Аликович – заместитель начальника отдела ЦНИИ Минобороны России.

На рис. 1 введены следующие обозначения:

- *состояния*:

  $\overline{y}$ – уязвимость в сети отсутствует;

y – уязвимость в сети имеется;

$\bar{y}_м$ – мониторинг сканера – «Уязвимости нет»;

$y_м$ – мониторинг сканера – «Уязвимость есть»;

1 – исходное состояние сети перед тестированием;

• *вероятности*:

$\bar{p}\,(\bar{y})$ – вероятность отсутствия в сети уязвимости;

$p(y)$ – вероятность наличия в сети уязвимости;

$\alpha = P(y_м / \bar{y})$ – условная вероятность правильного мониторинга сканером события отсутствия в сети уязвимости;

$\alpha = P(y_м / \bar{y})$ – условная вероятность неправильного мониторинга сканером события наличия в сети уязвимости (ошибка первого рода);

$\bar{\beta} = P(y_м / y)$ – условная вероятность правильного мониторинга сканером события наличия в сети уязвимости;

$\beta_и = P(\bar{y}_м / y)$ – условная вероятность неправильного мониторинга сканером события отсутствия в сети уязвимости (инструментальная ошибка второго рода – пропуск уязвимости);

$\beta_к = P(\bar{y}_м / y)$ – условная вероятность неправильного мониторинга сканером события отсутствия в сети уязвимости (конструкторская ошибка второго рода – непредусмотрен программистами процесс контроля некоторого типа уязвимостей).

Напомним, что условные вероятности составляют полную группу событий:

$$p + \bar{p} = 1;\ \bar{\alpha} + \alpha = 1;\ \bar{\beta} + \beta_и + \beta_к = 1. \qquad (1)$$

Расчет исходных условных вероятностей для каждого сканера тестирования сети имеется в табл. 3.

Выходные показатели достоверности вычисляются по следующим формулам:

• апостериорная вероятность правильного мониторинга отсутствия в сети уязвимости, т.е. вероятность доверия к сигналу сканера: «Уязвимости нет»

$$D_{\bar{y}_м} = P(\bar{y}/\bar{y}_м) = \frac{\bar{p}\bar{\alpha}}{\bar{p}\bar{\alpha} + p(\beta_и + \beta_к)}; \qquad (2)$$

• апостериорная вероятность правильного мониторинга наличия в сети уязвимости, т.е. вероятность доверия к показанию сканера: «Уязвимость есть»

$$D_{y_м} = P(y / y_м) = \frac{p\bar{\beta}}{p\bar{\beta} + \bar{p}\alpha}; \qquad (3)$$

• априорная общая вероятность правильного мониторинга отсутствия и наличия в сети уязвимости

$$D = P(\bar{y}, \bar{y}_м) + P(y, y_м) = \bar{p}\bar{\alpha} + p\bar{\beta}. \qquad (4)$$

Значения выходных показателей достоверности тестирования сети четырьмя сканерами приведены в табл. 4 (столбцы 3, 4, 5). В столбце 6 показаны значения рейтингов этих же сканеров по результатам опроса потребителей.

В столбцах 7, 8 отражены рейтинги сканеров в соответствии с балльной системой (некоторым событиям присваивается положительный балл (+), другим– отрицательный (–) по методике [1]).

В столбце 9 демонстрируются значения рейтингов сканеров тестирования сети согласно расчетам выходных показателей достоверности по формулам (2), (3), (4). При этом первые три сканера проранжированы в соответствии с абсолютным превосходством всех показателей достоверности вышестоящего сканера в таблице над нижестоящим. Третий сканер уступает четвертому по показателю достоверности $D_{\bar{y}_м}$, но превосходит его по остальным показателям $D_{y_м}, D$.

Следует отметить разницу результатов оценки рейтингов сканеров как при опросе потребителей и при расчетах работников Учебного центра «Информзащита», так и полученную авторами статьи. Возможно, она связана с разными критериями оценки. Если авторы статьи брали в основу только показатели достоверности, то в Учебном центре была попытка оценить качество сканеров. Потребители опроса по Интернету, возможно, учитывали и другие негативные стороны сканеров.

Эффективность сканеров при тестировании сети на безопасность

Проранжируем анализируемые сканеры по эффективности тестирования сети. В качестве показателя эффективности E_i выберем отношение эффекта $Э_i$ тести-

Таблица 3

Входные показатели достоверности тестирования сети

№ п/п	Наименование сканера	$\bar{p}$	p	$\bar{\alpha}$	α	$\bar{\beta}$	$\beta_и$	$\beta_к$
1	2	3	4	5	6	7	8	9
1	XSpider	0,217	0,783	0,935	0,065	0,717	0	0,283
2	Internet Scaner	0,217	0,783	0,913	0,087	0,320	0,090	0,590
3	Nessus	0,217	0,783	0,5	0,5	0,385	0,205	0,410
4	Retina Network SS	0,217	0,783	0,652	0,348	0,241	0,181	0,578

Таблица 4

Выходные показатели достоверности тестирования сети

№ п/п	Наименование сканера	$D_{\bar{y}_м}$	$D_{y_м}$	D	Рейтинги сканеров			
					По опросу потребителей	По балльной системе		По достоверности тестирования
						(+)	(-)	
1	2	3	4	5	6	7	8	9
1	XSpider	0,424	0,975	0,764	1	1	1	1
2	Internet Scaner	0,271	0,930	0,449	4	2	1	2
3	Nessus	0,184	0,735	0,410	2	2	4	3
4	Retina Network SS	0,192	0,714	0,330	3	4	3	4

Таблица 5

Показатели эффективности тестирования сети

№ п/п	Наименование сканера	Число предотвращенных рисков / коэффициенты весомости			Общий эффект $Э$	Стоимость (USD) C, x10^3	Показатель эффективности E	Рейтинг по эффективности
		высоких	средних	низких				
1	2	3	4	5	6	7	8	9
1	XSpider	38/0.76	62/0.19	20/0.05	41.66	1.737	23.98	2
2	Internet Scaner	5/0.76	13/0.19	32/0.05	7.87	21.537	0.365	4
3	Nessus	9/0.76	13/0.19	15/0.05	10.06	б/п	$\to \infty$	1
4	Retina Network	13/0.76	33/0.19	15/0.05	16.9	7.824	2.16	3

рования i-го сканера к его затратам C_i

$$E_i = \frac{Э_i}{C_i}. \qquad (5)$$

Основными затратами для потребителя, исключая затраты на обучение операторов, служат покупные стоимости сканеров C_i, имеющиеся в [2] и приведенные в столбце 7 табл. 5. Сканер Nessus потребителям предоставляется бесплатно (б/п).

Эффект тестирования сканера безопасности, исходя из его назначения, обусловлен не только количеством выявленных уязвимостей $N_j, j =$ (столбцы 3–5 табл. 5), но и значимостью выявленных уязвимостей, следовательно, предотвращенных рисков («низких», «средних» и «высоких»), имеющихся в [1].

Методы преодоления трудностей комплексирования рисков с учетом их значимости связаны с нахождением соответствующих коэффициентов весомости W_j и указаны в литературе [3], [4]. Воспользуемся методом Саати Т.Л. [3], но вместо нахождения собственных значений матрицы применим алгоритм последовательных приближений [4], который уже на 7-м шаге позволяет получить искомые коэффициенты весомости

$$W1 \neq W_H = 0{,}05;\ W_2 \neq W_C = 0{,}19;\ W_3 \neq W4 = 0{,}76, \qquad (6)$$

показанные в столбцах 3–5 табл. 5.

Общий показатель эффекта i-го сканера определяется выражением

$$Э_i = \sum_{j=1}^{3} W_j N_j. \qquad (7)$$

Значения показателей эффекта сканеров приведены в столбце 6, а величины показателей эффективности, найденные по формуле (5), имеются в столбце 8, а рейтинги сканеров показаны в столбце 9.

В отличие от табл. 4 рейтинги сканеров снова изменились. В первую очередь, это связано с нулевой ценой сканера Nessus и со слишком дорогой ценой сканера Internet Scaner.

Литература

1. Лепихин В.Б., Гордейчик С.В. Использование сканеров безопасности в процессе тестирования сети на устойчивость к взлому. Часть 1. – М.: Учебный центр «Информзащита». – 2005. – 34 с.

2. Лепихин В.Б., Гордейчик С.В. Функциональные возможности сканеров безопасности. Часть 2. – М.: Учебный центр «Информзащита». – 2005. – 68 с.

3. Саати Т.Л. Математические модели конфликтных ситуаций. – М.: Сов. радио. – 1977.

4. Черноскутов А.И. и др. Цены на машины и оборудование на капиталистическом рынке. Выпуск 3. – М.: ВНИКИ МВЭС. – 1990. С. 1 – 109.

Материал поступил в редакцию 16. 01. 2008г.