Бизнес против pentest
или
pentest для бизнеса
или
pentest как бизнес?

Сергей Гордейчик

Positive Technologies

POSITIVE TECHNOLOGIES

Тесты на проникновение. За и против

Хакеры не будут искать всякие иньекции в ваших сайтах, им интересен компьютер генерального директора и все. Поэтому мы посылаем по почте специальную троянскую програму на машину секретарши и таким образом проводим пентест

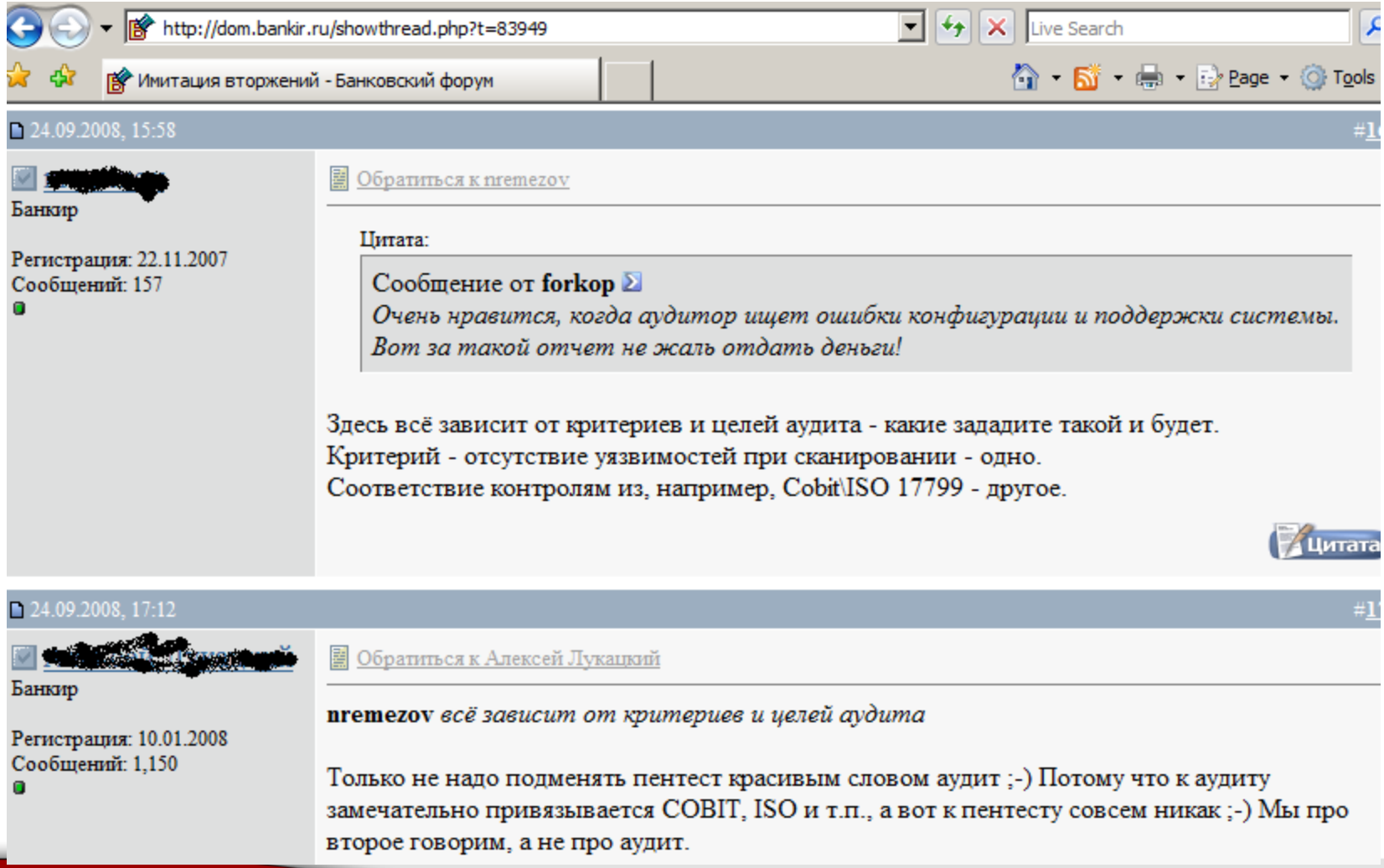
Немного о мифах

- **Цель пентеста в том, чтобы взломать**
- **Пентесты успешны на 100%**
  99%, 83,463…
- **Пентесты – это дешево**
- **Социотехника – наше все**

Pentest – что в него входит?

ВЕКТОРЫ	ТИПИЧНЫЕ ОШИБКИ	РИСК	PROB
Сетевая инфраструктура	Недостаточное сегментирование и фильтрация трафика	Средний	Высокая
Сетевые устройства	Слабые пароли, настройки, протоколы	Высокая	Средняя
Беспроводные сети	Слабое шифрование, слабые пароли, беспроводные клиенты	Высокая	Средняя
Сетевые службы и СУБД	Слабые пароли, стандартные конфигурации, patchmanagement, разграничение доступа	Высокая	Высокая
Web-приложения	Уязвимости реализации (WASC TC), слабые пароли	Высокая	Высокая
Рабочие места	Avir, patchmanagement, awarnes.	Высокая	Высокая

Pentest не аудит?



http://dom.bankir.ru/showthread.php?t=83949

Имитация вторжений - Банковский форум

24.09.2008, 15:58

[redacted]
Банкир

Регистрация: 22.11.2007
Сообщений: 157

Обратиться к nremezov

Цитата:

Сообщение от **forkop**
Очень нравится, когда аудитор ищет ошибки конфигурации и поддержки системы. Вот за такой отчет не жаль отдать деньги!

Здесь всё зависит от критериев и целей аудита - какие зададите такой и будет.
Критерий - отсутствие уязвимостей при сканировании - одно.
Соответствие контролям из, например, Cobit\ISO 17799 - другое.

Цитата

24.09.2008, 17:12

[redacted]
Банкир

Регистрация: 10.01.2008
Сообщений: 1,150

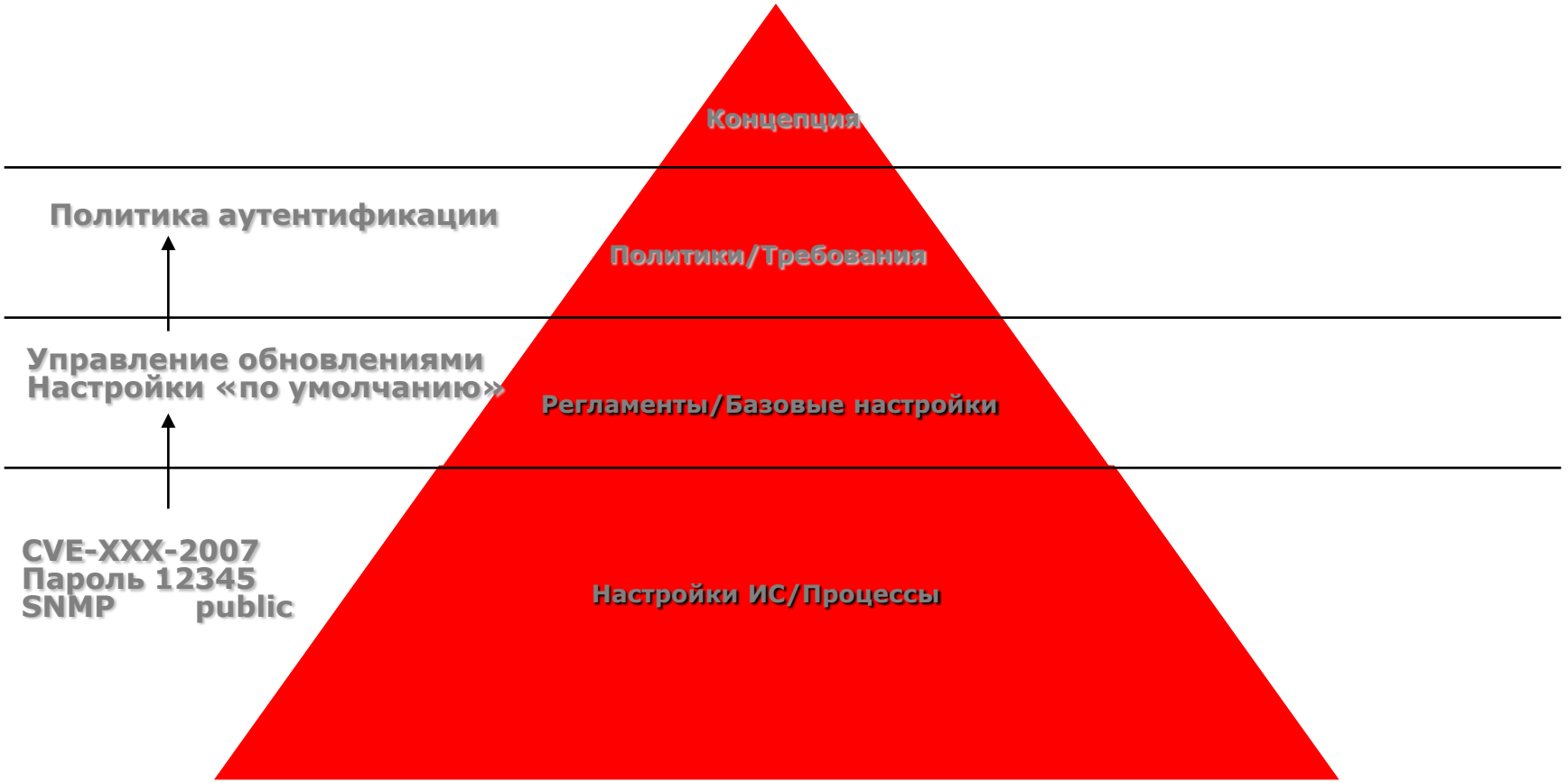
Обратиться к Алексей Лукацкий

nremezov *всё зависит от критериев и целей аудита*

Только не надо подменять пентест красивым словом аудит ;-) Потому что к аудиту замечательно привязывается COBIT, ISO и т.п., а вот к пентесту совсем никак ;-) Мы про второе говорим, а не про аудит.

Проекция на высокоуровневые процессы

Проекция на высокоуровневые процессы



Pentest – Стандарты и процессы

ЗАЩИТНЫЙ МЕХАНИЗМ	ISO/IEC 27001-2005	ISM3	PCI DSS V 1.1
Инвентаризация ресурсов	A.7.1.1	OSP-3, OSP-4	Requirement 12: Maintain a policy that addresses information security for employees and contractors
Формирование периметра сетевой безопасности	A.10.6, A.11.4	OSP-16	Requirement 1: Install and maintain a firewall configuration to protect cardholder data
Защита данных при передаче	A.10.6, A.10.8.4		Requirement 4: Encrypt transmission of cardholder data across open, public networks
Аутентификация	A.11.2	OSP-12	Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters Requirement 8: Assign a unique ID to each person with computer access
Разграничение доступа	A.8.3.3, A.11.4, A.11.5, A.11.6, A.12.4	OSP-11	Requirement 3: Protect stored cardholder data Requirement 7: Restrict access to cardholder data by business need-to-know
Управление обновлениями систем	A.12.6	OSP-5, OSP-6	Requirement 6: Develop and maintain secure systems and applications
Настройка встроенных средств безопасности	A.15.2.2	OSP-7	Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
Защита от вредоносного кода	A.10.4	OSP-17	Requirement 5: Use and regularly update anti-virus software or programs
Безопасность приложений	A.10.9, A.11.6, A.12.2, A.12.3, A.12.4, A.12.5	OSP-8	Requirement 6: Develop and maintain secure systems and applications
Повышение осведомленности сотрудников	A.8.2.2	TSP-8, TSP-9, TSP-11	Requirement 12: Maintain a policy that addresses information security for employees and contractors
Мониторинг ИБ и анализ инцидентов	A.10.10, A.13	OSP-20, OSP-22, OSP-23, OSP-24, OSP-25	Requirement 10: Track and monitor all access to network resources and cardholder data

У вас первый пентест?

- **Just for Fun**
- **Положено (Compliance)**
- **Оценка реализованных механизмов**
- **Часть процесса**
- **Произвести впечатление**

От аудита к мониторингу

- **Накопление результатов предыдущих работ**
  - **Использование таксономий (CVSS, CVE, CWE, WASC TCv2 и т.д.)**
- **Сравнение с предыдущим состоянием и мировой практикой**
  - **метрики, метрики, метрики**
- **Проекция на высокоуровневые процессы**

Pentest – Стандарты и процессы

ЗАЩИТНЫЙ МЕХАНИЗМ	ISO/IEC 27001-2005	ISM3	PCI DSS V 1.1
Инвентаризация ресурсов	A.7.1.1	OSP-3, OSP-4	Requirement 12: Maintain a policy that addresses information security for employees and contractors
Формирование периметра сетевой безопасности	A.10.6, A.11.4	OSP-16	Requirement 1: Install and maintain a firewall configuration to protect cardholder data
Защита данных при передаче	A.10.6, A.10.8.4		Requirement 4: Encrypt transmission of cardholder data across open, public networks
Аутентификация	A.11.2	OSP-12	Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters Requirement 8: Assign a unique ID to each person with computer access
Разграничение доступа	A.8.3.3, A.11.4, A.11.5, A.11.6, A.12.4	OSP-11	Requirement 3: Protect stored cardholder data Requirement 7: Restrict access to cardholder data by business need-to-know
Управление обновлениями систем	A.12.6	OSP-5, OSP-6	Requirement 6: Develop and maintain secure systems and applications
Настройка встроенных средств безопасности	A.15.2.2	OSP-7	Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
Защита от вредоносного кода	A.10.4	OSP-17	Requirement 5: Use and regularly update anti-virus software or programs
Безопасность приложений	A.10.9, A.11.6, A.12.2, A.12.3, A.12.4, A.12.5	OSP-8	Requirement 6: Develop and maintain secure systems and applications
Повышение осведомленности сотрудников	A.8.2.2	TSP-8, TSP-9, TSP-11	Requirement 12: Maintain a policy that addresses information security for employees and contractors
Мониторинг ИБ и анализ инцидентов	A.10.10, A.13	OSP-20, OSP-22, OSP-23, OSP-24, OSP-25	Requirement 10: Track and monitor all access to network resources and cardholder data

Спасибо за внимание!

Сергей Гордейчик

Positive Technologies