Этичный хакинг и тестирование на проникновение

Хеирхабаров Теймур Самедович
специалист по защите информации
admin@kb-61.com

Красноярск, 2016 г.

Кто такие хакеры?

- **Человек, наслаждающийся доскональным пониманием внутренних действий систем, компьютеров и компьютерных сетей в частности (RFC 1983).**
- Кто-либо, программирующий с энтузиазмом (даже одержимо) или любящий программировать, а не просто теоретизировать о программировании.
- Человек, способный ценить и понимать хакерские ценности.
- Человек, который силён в быстром программировании.
- Эксперт по отношению к определённой компьютерной программе или кто-либо часто работающий с ней, например «хакер Unix»;
- Эксперт или энтузиаст любого рода. Кто-либо может считаться «хакером астрономии», например.
- Кто-либо любящий интеллектуальные испытания, заключающиеся в творческом преодолении или обходе ограничений.
- **Компьютерный взломщик, злонамеренно обходящий системы компьютерной безопасности.**

WIKIPEDIA
The Free Encyclopedia

Какие бывают хакеры?

Скрипт-кидди (Script Kiddies)
Низкоквалифицированные хакеры, пытающиеся взламывать систем путём запуска готовых скриптов и утилит, не понимая принципов их работы, разработанных «настоящими» хакерами.

«Чёрные» шляпы (Black Hats)
специалисты, обладающие глубокими знаниями в области ИТ и использующие их для осуществления незаконной, вредоносной или деструктивной деятельности.

«Белые» шляпы (White Hats)
специалисты, обладающие глубокими знаниями в области ИТ и техник «Black Hats» и использующие их для защиты систем (этичные хакеры).

«Серые» шляпы (Gray Hats)
личности, использующие свои знания и навыки в области ИТ и хакерских техник в разное время как в легальных так и в нелегальных целях (сегодня «White Hat», завтра «Black Hat»).

Какие бывают хакеры?

Кибертеррористы

хакеры, использующие свои навыки в террористических целях (взлом критических систем, управляющих опасными производствами, deface для пропаганды идей и ценностей терроризма и др.).

Спонсируемые государством хакеры

хакеры, использующие свои навыки в интересах и под контролем государства.

Хактивисты

хакеры, использующие свои навыки в целях продвижения политических идей, свободы слова, защиты прав человека и обеспечения свободы информации.

Хакеры-суицидники (по Ec-Council CEH)

хакеры, стаявящие своей целью причинение огромного ущерба без каких-либо на то целей, не заботящиеся о сокрытии своих действий и не боящиеся наказания.

Хакинг и этичный хакинг

Исторически сложилось так, что в настоящее время термин «хакинг» часто употребляется именно в негативном значении. **Хакинг** – осуществление компьютерных взломов, несанкционированное проникновение в компьютерные системы с целью получения какой-либо выгоды, либо целенаправленного нарушения работоспособности систем.

Хакинг – исследование компьютерных технологий и систем с целью глубоко и досконального понимания их устройства и принципов работы, поиск недекларированных возможностей и функций.

Этичный хакинг – санкционированный владельцем системы процесс поиска уязвимостей информационной безопасности с применением методов и техник, аналогичных применяемым хакерами, в целях повышения защищенности данной системы.

Грань между этичным и неэтичным хакингом

Критерии этичности хакинга:

- есть официальное разрешение владельца системы на исследование её безопасности. Это может быть договор, публичная оферта или любая другая форма, принятая законодательством;
- результаты исследования обязательно обнародуются заказчику исследования системы или разработчикам ПО, в котором найдены уязвимости;
- в случае обнаружения уязвимости в ПО информация о ней не публикуется исследователем в открытом доступе до выпуска разработчиком патча, устраняющего уязвимость;
- результаты исследования не используются этичным хакером в целях, отличных от оценки уровня защищённости.

Продажа уязвимостей на биржах уязвимостях – это этично или нет?

Ключевая идея этичного хакинга

*«**Знай врага** и знай себя, и ты пройдёшь сотню битв без поражений»*

Сунь Цзы

Тестирование на проникновение и этичный хакинг

Термин этичный хакинг является собирательным и как правило подразумевает использование всевозможных хакерских методик во благо, будь то поиск уязвимостей в ПО, обратная инженерия прошивки какого либо устройства, фаззинг сетевого протокола или тест на проникновение. Т.е. термин не обозначает какой-то один тип исследования или деятельности.

Тестирование на проникновение – метод оценки защищённости компьютерных систем или сетей средствами моделирования атаки злоумышленника. Фактически это тестовый взлом системы. Результаты теста оформляются в виде отчёта.

Тест на проникновение и другие формы оценки защищённости

Тест на проникновение – это одна из форм оценки защищённости.

Помимо теста на проникновение есть еще другие формы:

- аудит информационной безопасности;
- анализ уязвимостей;
- аттестация информационной (автоматизированной) системы (это больше не форма анализа защищённости, а форма оценки соответствия).

Тест на проникновение != аудит информационной безопасности

Аудит (по ГОСТ 19011-2012) – систематический, независимый процесс получения **свидетельства аудита** и объективного их оценивания с целью установления степени выполнения согласованных **критерием аудита**.

Критерии аудита – совокупность политики, процедур или требований, используемых в качестве эталона, в соотношении с которыми сопоставляют свидетельства аудита, полученные при проведении аудита.

Свидетельства аудита – записи, изложение фактов или другая информация, которые связаны с критериями аудита и могут быть проверены.

При тесте на проникновение отсутствуют как таковые критерии аудита – неотъемлемый элемент понятия «Аудит».

Тест на проникновение может являться частью комплексного аудита для демонстрации на практике того, что невыполнение тех или иных требований безопасности, являющихся критериями аудита, может привести к успешной компрометации системы.

Тест на проникновение != анализ уязвимостей

Анализ уязвимостей – оценка используемого в информационных системах программного и аппаратного обеспечения на наличие известных уязвимостей без последующей попытки их эксплуатации и демонстрации возможности использования потенциальным злоумышленником.

Анализ уязвимостей	Тест на проникновение
• Поиск уязвимостей • Отчёт по результатам	• Поиск уязвимостей • Попытка их эксплуатации для проникновения в систему • Отчёт по результатам

Тест на проникновение != аттестация

Аттестация объектов информатизации – комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации.

Для некоторых категорий систем аттестация носит обязательный характер (ГИС, системы, обрабатывающие ГТ). Аттестат соответствия в таких случаях не только подтверждает соответствие некоторым требованиям, но и даёт права обрабатывать информацию определённого уровня конфиденциальности.

На практике наличие аттестата соответствия не доказывает того, что система безопасна (привет «бумажным» безопасникам ☺). Зачастую аттестация может привести к обратному эффекту, когда безопасность системы понижается. Например, в аттестованной системе есть проблемы с установкой обновлений.

Ограничения тестирования на проникновение

- Тест на проникновение не позволяет выявить всех уязвимостей. Классический аудит вкупе с анализом уязвимостей покажет больше.
- Ограничение установленной областью аудита.
- Ограничение по времени.
- Ограничение по спектру применяемых атак (никаких DDoS-атак и прочих деструктивных вещей).
- Ограничения квалификации аудитора.
- Ограничения воображения аудитора.
- Ограничение в доступных аудитору эксплойтах.

Зачем проводить тестирование на проникновение?

Оценка эффективности принятых мер безопасности для защиты от внешних и внутренних угроз.

Оценка устойчивости систем(ы) или приложения к наиболее распространённым видам внешних атак.

Внутренняя политика (тест на проникновение как инструмент воздействия).

Требование или рекомендация нормативных документов (compliance).

Зачем проводить тестирование на проникновение? Требования и рекомендации нормативных документов

Приказ ФСТЭК № 31:

XIV. Обеспечение безопасной разработки программного обеспечения (ОБР)				
ОБР.0	Разработка правил и процедур (политик) обеспечения безопасной разработки программного обеспечения	+	+	+
ОБР.1	Анализ уязвимостей и угроз безопасности информации в ходе разработки программного обеспечения	+	+	+
ОБР.2	Статический анализ кода программного обеспечения в ходе разработки программного обеспечения		+	+
ОБР.3	Ручной анализ кода программного обеспечения в ходе разработки программного обеспечения			
ОБР.4	Тестирование на проникновение в ходе разработки программного обеспечения		+	+
ОБР.5	Динамический анализ кода программного обеспечения в ходе разработки программного обеспечения		+	+
ОБР.6	Документирование процедур обеспечения безопасной разработки программного обеспечения разработчиком и представление их заказчику (оператору)	+	+	+

Зачем проводить тестирование на проникновение? Требования и рекомендации нормативных документов

Приказ ФСТЭК № 21:

«11. В случае определения в соответствии с Требованиями к защите персональных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. N1119, в качестве актуальных угроз безопасности персональных данных 1-го и 2-го типов дополнительно к мерам по обеспечению безопасности персональных данных, указанным в пункте 8 настоящего документа, могут применяться следующие меры:

проверка системного и (или) прикладного программного обеспечения, включая программный код, на отсутствие недекларированных возможностей с использованием автоматизированных средств и (или) без использования таковых;

тестирование информационной системы на проникновения;

использование в информационной системе системного и (или) прикладного программного обеспечения, разработанного с использованием методов защищенного программирования.»

Зачем проводить тестирование на проникновение? Требования и рекомендации нормативных документов

Payment Card Industry Data Security Standard (v. 3.1,April 2015):

«11.3 Implement a methodology for penetration testing…

11.3.1 Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

11.3.2 Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

11.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections. »

Зачем проводить тестирование на проникновение? Лучшие практики

CIS Critical Security Controls (бывший SANS TOP20):

15	Controlled Access Based on the Need to Know	The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.
16	Account Monitoring and Control	Actively manage the life-cycle of system and application accounts – their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.
17	Data Protection	The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.
18	Incident Response and Management	Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.
19	Secure Network Engineering	Make security an inherent attribute of the enterprise by specifying, designing, and building-in features that allow high confidence systems operations while denying or minimizing opportunities for attackers.
20	Penetration Tests and Red Team Exercises	Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

В каких случаях нет смысла проводить тест на проникновение

Если в компании не реализованы базовые контроли информационной безопасности (антивирусная защита, парольная политика, сегментирование сети, установка обновлений и др.) то тест на проникновение будет пустой тратой времени и денег! Вас гарантированно поломает компетентная команда аудиторов. Исключение составляют случаи, когда на эти самые базовые контроли не дают денег и тест на проникновение заказывается в целях выбивания бюджета.

Если в компании силами собственных специалистов никогда не проводились какие-либо проверки безопасности, то следует начать с них, а не покупать сразу тест на проникновение. Большое количество критических уязвимостей, которые могут быть эксплуатированы злоумышленниками, могут быть найдены без глубоких специальных знаний (использование бесплатных сканеров, проверка на стандартные пароли и т.д.).

Тест на проникновение надо заказывать только в случае, когда все проведенные своими силами проверки указывают на то, что система не имеет недостатков.

Тесты на проникновение и Россия

- На рынке очень мало компаний, способных оказать данную услугу качественно (мнение докладчика). Их можно пересчитать по пальцам одной руки, остальные – шарлатаны и скрипт-кидди ☺.
- Данная услуга не пользуется широким спросом. Интересна в первую очередь крупным компаниям, а также компаниям, существование которых во многом зависит от ИТ, безопасности ИТ инфраструктуры. Также услуга интересна тем, для кого периодический тест на проникновение в соответствии с какими-либо требованиями является обязательным мероприятием (в первую очередь банки, сертифицированные по PCI DSS, однако зачастую качество тестов, выполняемых в ключе требований PCI DSS оставляет желать лучшего).
- В большинстве случаев тест на проникновение выполняется внешним подрядчиком, так как компаниям дорого держать таких специалистов в штате.

Типы тестирования на проникновение

По объёму предоставляемой аудитору информации о тестируемой системе:

- чёрный ящик;
- серый ящик;
- белый ящик.

По расположению аудитора относительно сетевого периметра исследуемой системе:

- внешнее;
- внутреннее.

По степени осведомлённости персонала исследуемого объекта:

- с уведомлением администраторов тестируемого объекта;
- без уведомления администраторов тестируемого объекта;
- без уведомления администраторов и специалистов по безопасности тестируемого объекта.

Внешнее тестирование на проникновение

Тип тестирования	Описание
Тестирование внешнего периметра сети	Анализ включает только внешние IP-адреса компании, доступные из Интернет
Тестирование WEB сайтов	Анализ включает в себя только WEB-сайты и сервисы компании, доступные неограниченному кругу внешних пользователей
Тестирование специализированных приложений	Анализ включает различные приложения, доступные внешним пользователям и взаимодействующие с серверами компании
Тестирование сотрудников на устойчивость к методам социальной инженерии	Попытка получения доступа к системам компании с использованием методов социальной инженерии. Оценка уровня осведомленности сотрудников в вопросах ИБ
Тестирование беспроводных сетей	Анализ возможностей злоумышленника, находящегося в зоне радиовидимости беспроводных сетей компании, но не имеющего санкционированного к ним подключения
Имитация «утерянного» корпоративного устройства	Анализ возможностей потенциального злоумышленника, завладевшего корпоративным мобильным устройством

Внутреннее тестирование на проникновение

Тип тестирования	Описание
Тестирование внутреннего периметра	Оценка возможностей злоумышленника имеющего санкционированный ограниченный доступ к корпоративной сети, аналогичный уровню доступа рядового сотрудника или гостя, имеющего доступ только в гостевой сегмент, либо же имеющего доступ только к сетевой розетке
Тестирование отдельного компонента/системы	WEB-приложения, ERP, СУБД

В ходе внутреннего тестирования может использоваться как ноутбук аудитора, так и стандартное рабочее место заказчика теста.

При анализе отдельной системы аудитору может быть предоставлен доступ из под учётной записи с ограниченными правами, только сведения об IP-адресах серверов или код приложения.

Критерии завершения теста на проникновение

- Получение доступа во внутреннюю сеть со стороны сети Интернет
- Получения доступа в определённый сегмент сети (например, сегмент АСУТП)
- Получение высоких привилегий в основных инфраструктурных и информационных системах/сервисах (Active Directory, сетевое оборудование, СУБД, ERP и т.п.)
- Получение доступа к определённым информационным ресурсам
- Получение доступа к определённой информации (например, электронная почта директора)
- Всё, до чего удастся дотянуться за определённое время
- До первого серьёзного сбоя, вызванного действиями аудитора ☺

Этапы теста на проникновение

- Определение области обследования.
- Составление модели угроз.
- Сбор информации об объекте исследования.
- Поиск уязвимостей.
- Попытка эксплуатации обнаруженных уязвимостей.
- Получение доступа к критичным ресурсам.
- Составление отчёта.

Этапы теста на проникновение. Сбор информации об объекте исследования. Пассивные методы

- Google Hacking
- Google Cache
- WHOIS информация
- Shodan
- Wayback Machine – http://www.archive.org
- официальный сайт компании (в т.ч. и исходный код страниц сайта)
- публикации о компании и её работниках в СМИ
- сайты поиска работы
- пресс-релизы интеграторов
- закупочная документация на торговых площадках
- страницы сотрудников в социальных сетях
- блоги, форумы
- метаданные документов, выложенных на сайте компании
- поиск в мусоре (физическом) компании – Dumpster Diving

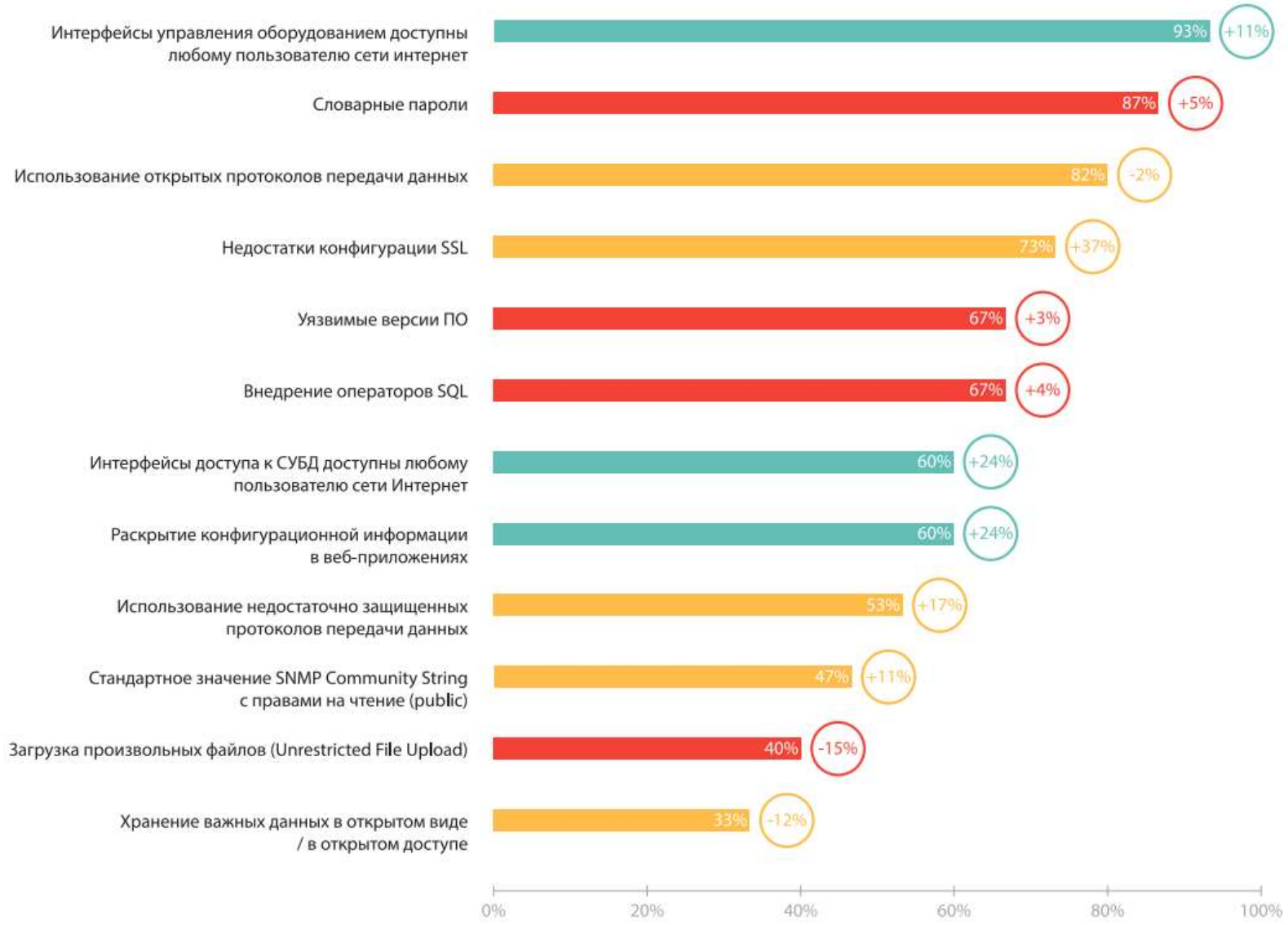
Этапы теста на проникновение. Сбор информации об объекте исследования. Активные методы

- Ping Sweep
- Fingerprint
- анализ заголовков почтовых сообщений. полученных от почтового сервера компании, попытки отправки на несуществующие адреса в домене компании и анализ возвращаемых ошибок, функции подтверждения доставки и подтверждения прочтения;
- сканирование портов
- анализ возвращаемых баннеров сетевых служб
- NetBios Enumeration
- SNMP Enumeration
- LDAP Enumeration
- NTP Enumeration
- SMTP Enumeration
- DNS Enumeration
- социальная инженерия

Этапы теста на проникновение. Поиск уязвимостей

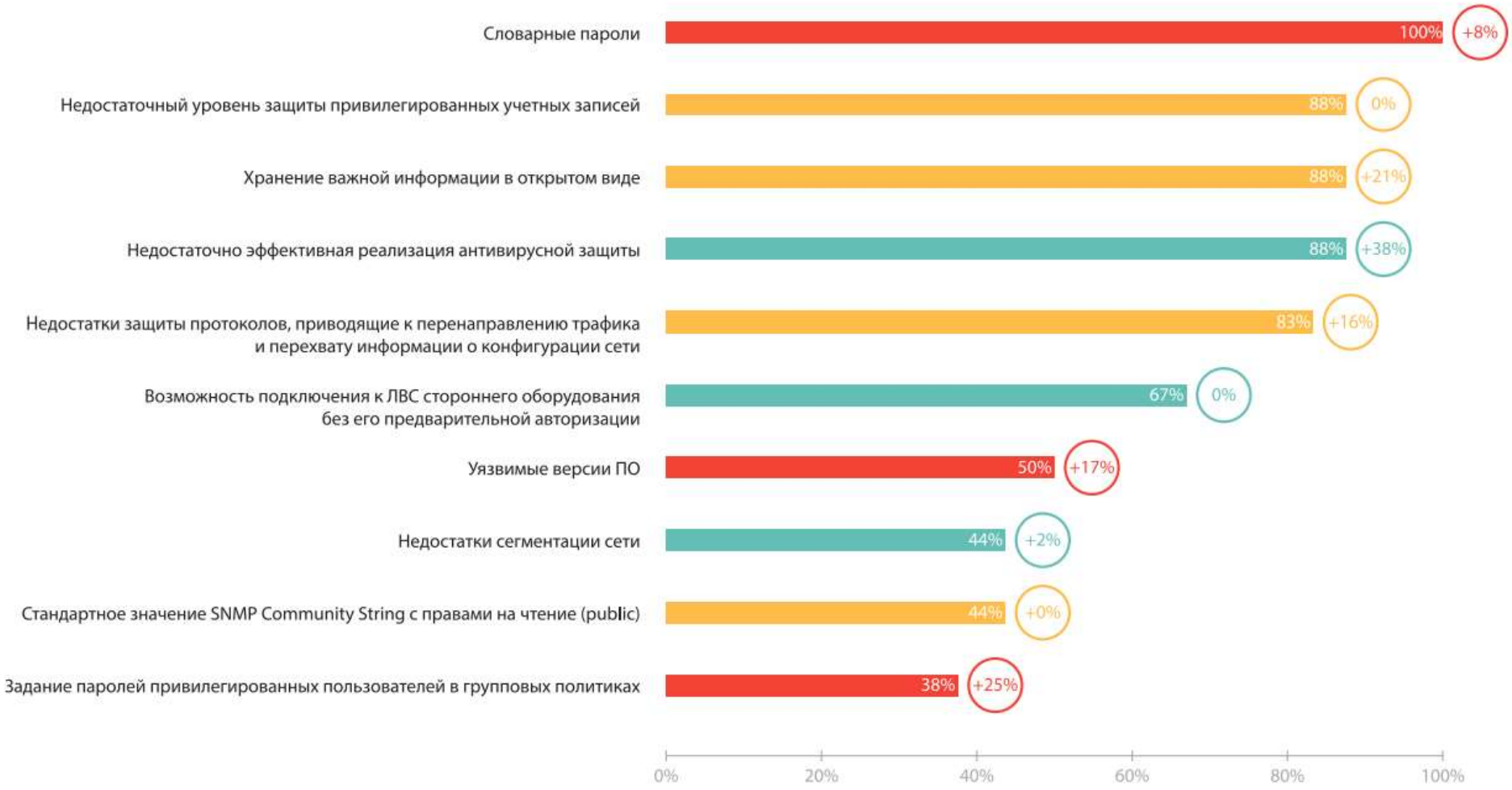
Поиск уязвимостей может проводится как вручную, так и с использование различных сканеров. Зачастую применяется оба метода.

Какие уязвимости находятся и используется чаще всего в ходе внешних тестов на проникновение



По данным компании Positive Technologies

Какие уязвимости находятся и используется чаще всего в ходе внутренних тестов на проникновение



По данным компании Positive Technologies

Применение методов социальной инженерии в ходе Тестов на проникновение

Применяемые методы:

- рассылка сообщений по электронной почте от имени внутренних сотрудников, авторитетных лиц (руководители компании, акционеры), контрагентов, гос. органов с вложенными вредоносными файлами или ссылками на вредоносный ресурс;
- вишинг, фишинг;
- подкидывание якобы утерянных носителей информации, устройств, эмулирующих клавиатуру, сопряжённых с носителем информации.

По данным компании Positive Technologies

Этапы теста на проникновение. Эксплуатация уязвимостей

Для эксплуатации уязвимостей аудитор может использовать эксплойты собственной разработки, публично доступные эксплойты, фреймворки для тестирования на проникновение.

Базы эксплойтов:

- https://www.exploit-db.com
- http://www.rapid7.com/db/
- http://ru.0day.today
- http://www.ussrback.com

Positive Technologies Exploit Explorer утилиты автоматизация поиска публично-доступных эксплойтов ро отчётам сканеров защищённости

Фреймворки для проведения тестов на проникновение:

- Metasploit;
- Cobalt Strike;
- Core Impact;
- Immunity CANVAS.

Этапы теста на проникновение. Разработка отчёта

По результатам теста на проникновение обязательно оформляется отчёт, который должен содержать:

- ✓ краткие выводы для руководства;
- ✓ описание границ исследования;
- ✓ описание методики исследования;
- ✓ перечень обнаруженных уязвимостей и недостатков с краткими рекомендациями по устранению;
- ✓ подробное описание сценариев атак, хода работ.

Примеры отчётов по результатам тестов на проникновение и рекомендации по написанию отчётов

Пример отчёта от Offensive Security (ENG):

https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf

Пример отчёта от Positive Technologies (RUS):

http://www.slideshare.net/devteev/pt-penetration-testing-report-sample

Пример отчёта от Эшелона (RUS):

http://www.slideshare.net/ucechelon/pentest-report-sample

Writing a Penetration Testing Report - SANS Institute:

https://www.sans.org/reading-room/whitepapers/bestprac/writing-penetration-testing-report-33343

The Art of Writing Penetration Test Reports:

http://resources.infosecinstitute.com/writing-penetration-testing-reports/

Методологии проведение тестов на проникновение

РС БР ИББС-2.6-2014 – Рекомендации Банка России «Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных систем» (см. приложение 3 – Рекомендации по проведению оценки защищённости);

PCI DSS Penetration Testing Guidance;

Open Source Security Testing Methodology Manual (OSSTMM);

Information System Security Assessment Framework (ISSAF);

Pen Testing Execution Standard (PTES);

NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment;

Open Web Application Security Project (OWASP) Testing Guide;

Penetration Testing Framework.

Как научиться проводить тесты на проникновение?

- ✓ Обучение по специализированным программам

- ✓ Самостоятельное обучение

- ✓ CTF

Как научиться проводить тесты на проникновение? Обучающие и сертификационные программы EC-Council

Обучающая программа	Сертификационный экзамен
Certified Ethical Hacker (CEH)	CEH, тест
Certified Security Analyst (ECSA)	ECSA, тест
-	LPT (Licensed Penetration Tester), практический, нужно взломать подготовленную организаторами систему

Для тестовых экзаменов (ECSA, CEH) в сети легко находятся дампы ответов. Можно обучиться и сдать экзамен в России. Цены обучения: CEH – 72990 для юр. лиц и 65650 для физ. лиц, ECSA – 84990 для юр. лиц и 76450 для физ. лиц (УЦ «Специалист» при МГТУ им. Н. Э. Баумана)

Как научиться проводить тесты на проникновение? Обучающие и сертификационные программы Offensive Security

Обучающая программа	Сертификационный экзамен
Penetration Testing with Kali Linux (PWK)	Offensive Security Certified Professional (OSCP)
Offensive Security Wireless Attacks (WiFu)	Offensive Security Wireless Professional (OSWP)
Cracking the Perimetr (CTP)	Offensive Security Certified Expert (OSCE)
Advanced Windows Exploitation (AWE)	Offensive Security Exploitation Expert (OSEE)
Advanced Web Attacks & Exploitation (AWAE)	Offensive Security Web Expert (OSWE)
Metasploit Unleashed (MSFU) на данный момент стал бесплатным	-

Обучение и сдача экзаменов online, кроме AWE и AWAE. Все экзамены – это практические задания. По окончанию нужно написать отчёт (на английском языке).

Как научиться проводить тесты на проникновение?
Обучающие и сертификационные программы Offensive Security

Обучающая программа	Сертификационный экзамен
SEC504: Hacker Tools, Techniques, Exploits and Incident Handling	GIAC Certified Incident Handler (GCIH)
SEC542: Web App Penetration Testing and Ethical Hacking	GIAC Web Application Penetration Tester (GWAPT)
SEC560: Network Penetration Testing and Ethical Hacking	GIAC Penetration Tester (GPEN)
SEC567: Social Engineering for Penetration Testers	-
SEC573: Python for Penetration Testers	-
SEC580: Metasploit Kung Fu for Enterprise Pen Testing	-
SEC617: Wireless Ethical Hacking, Penetration Testing, and Defenses	GIAC Assessing and Auditing Wireless Networks (GAWN)

Как научиться проводить тесты на проникновение?
Обучающие и сертификационные программы SANS

Обучающая программа	Сертификационный экзамен
SEC642: Advanced Web App Penetration Testing and Ethical Hacking	-
SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
SEC760: Advanced Exploit Development for Penetration Testers	GIAC Penetration Tester (GPEN)
SEC561: Immersive Hands-On Hacking Techniques	-
SEC575: Mobile Device Security and Ethical Hacking	GIAC Mobile Device Security Analyst (GMOB)

Как научиться проводить тесты на проникновение? Обучающие программы PentestIT

Российский стартап. Обучение дистанционное. Преимущественно практика. Предлагается несколько программ обучения:

Обучающая программа	Цена
ZERO SECURITY: A Программа для начинающих	12 000 руб.
СТАНДАРТ	30 000 руб.
ПРОФИ	60 000 руб.
ЭКСПЕРТ	100 000 руб.

https://www.pentestit.ru

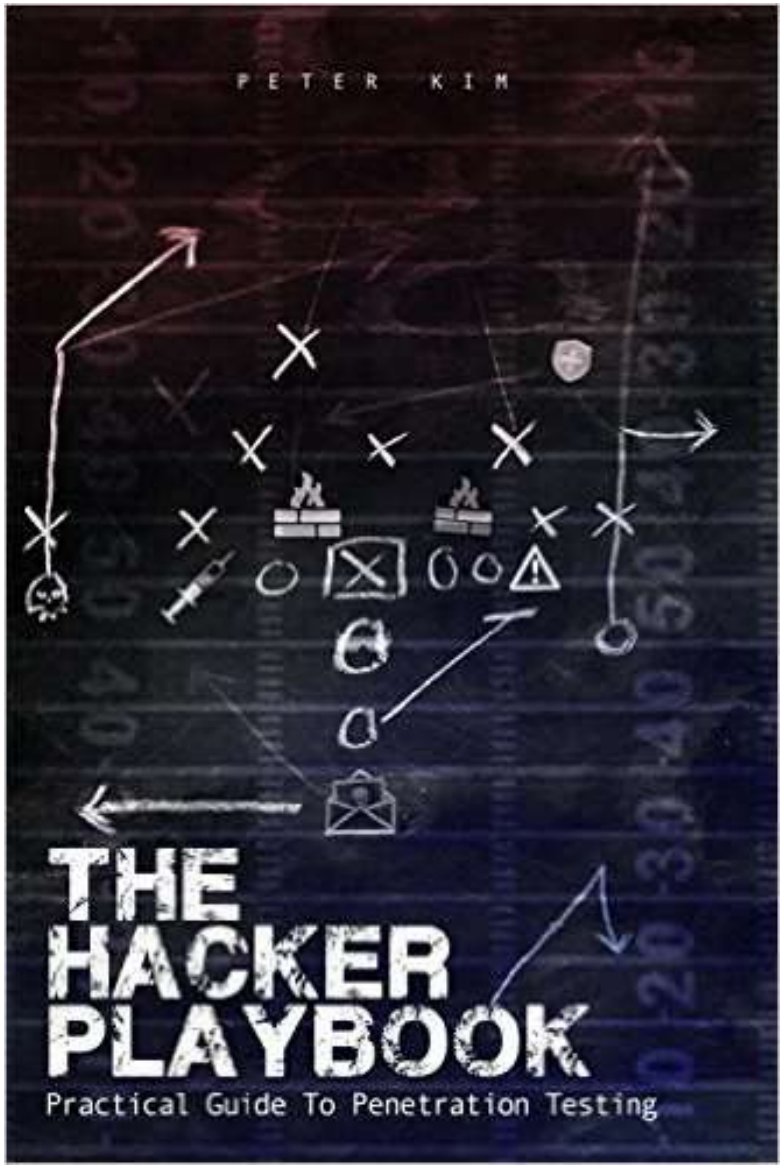
Как научиться проводить тесты на проникновение? Самостоятельное обучение

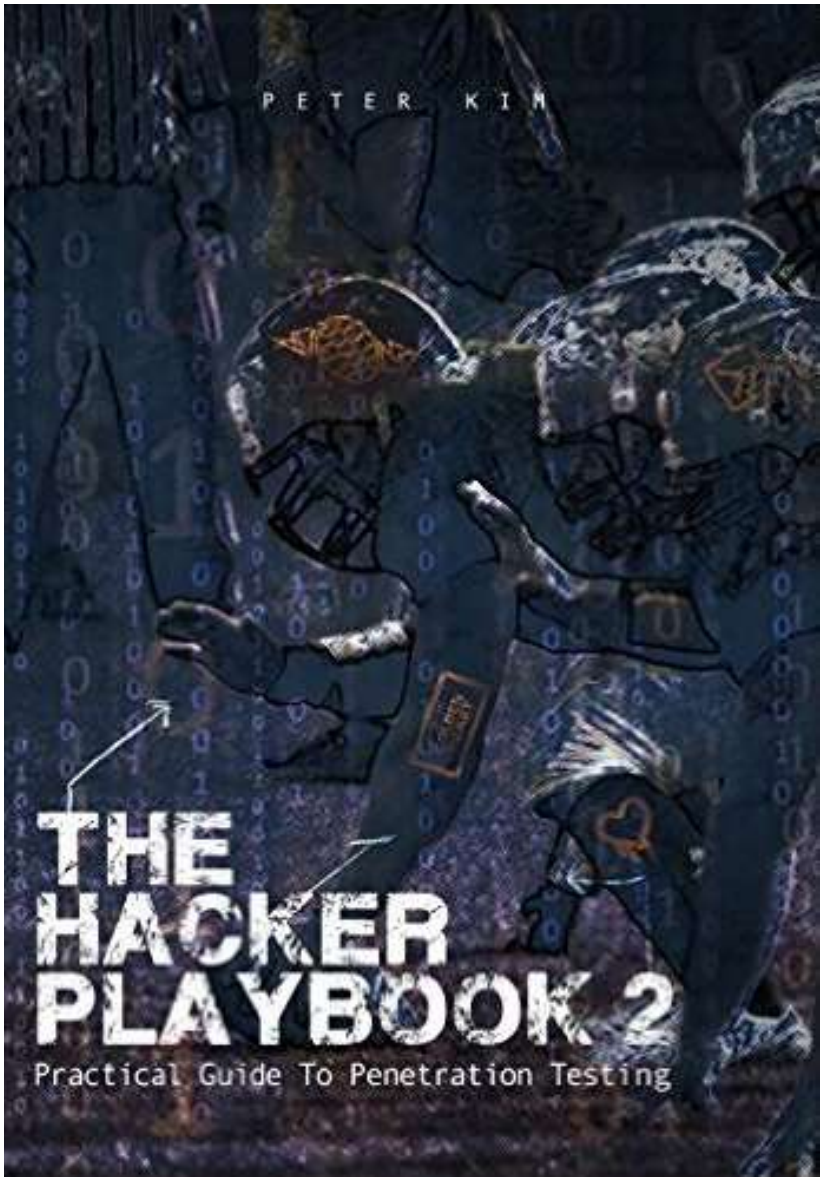
- Блоги, форумы, специализированные сайты;
- http://www.securitytube.net ;
- Offensive Computer Security Spring courses;
- Материалы многих платных обучающих курсов можно найти в сети (торренты, специализированные форумы);
- Книги на английском языке (при большом желании можно найти pdf-ки хороших книг в сети ☺);
- Специальные дистрибутивы и готовые виртуальные машины с уязвимостями (Damn Vulnerable Linux, Metasploitable, pWnOS и т.д.);
- Специализированные Online-площадки (EnigmaGroup, hACME Game, Hax.Tor, Exploit Exercises и т.д.).

Mind-карта с подборкой огромного количества online-площадок, специализированных образов, виртуальных машин и т.д. для обучения – http://www.amanhardikar.com/mindmaps/Practice.png

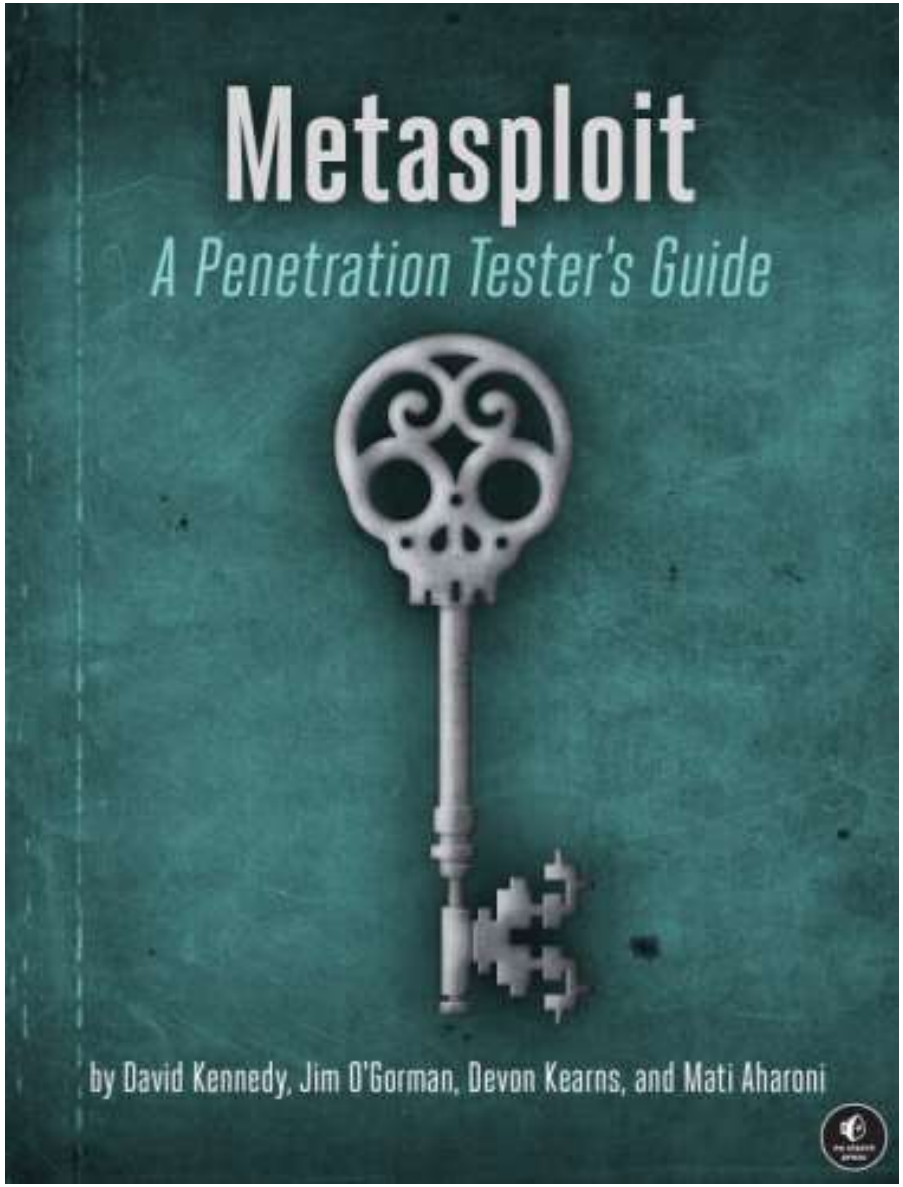
Сборник ссылок по тематике тестирование на проникновение – «The Open Penetration Testing Bookmarks Collection»

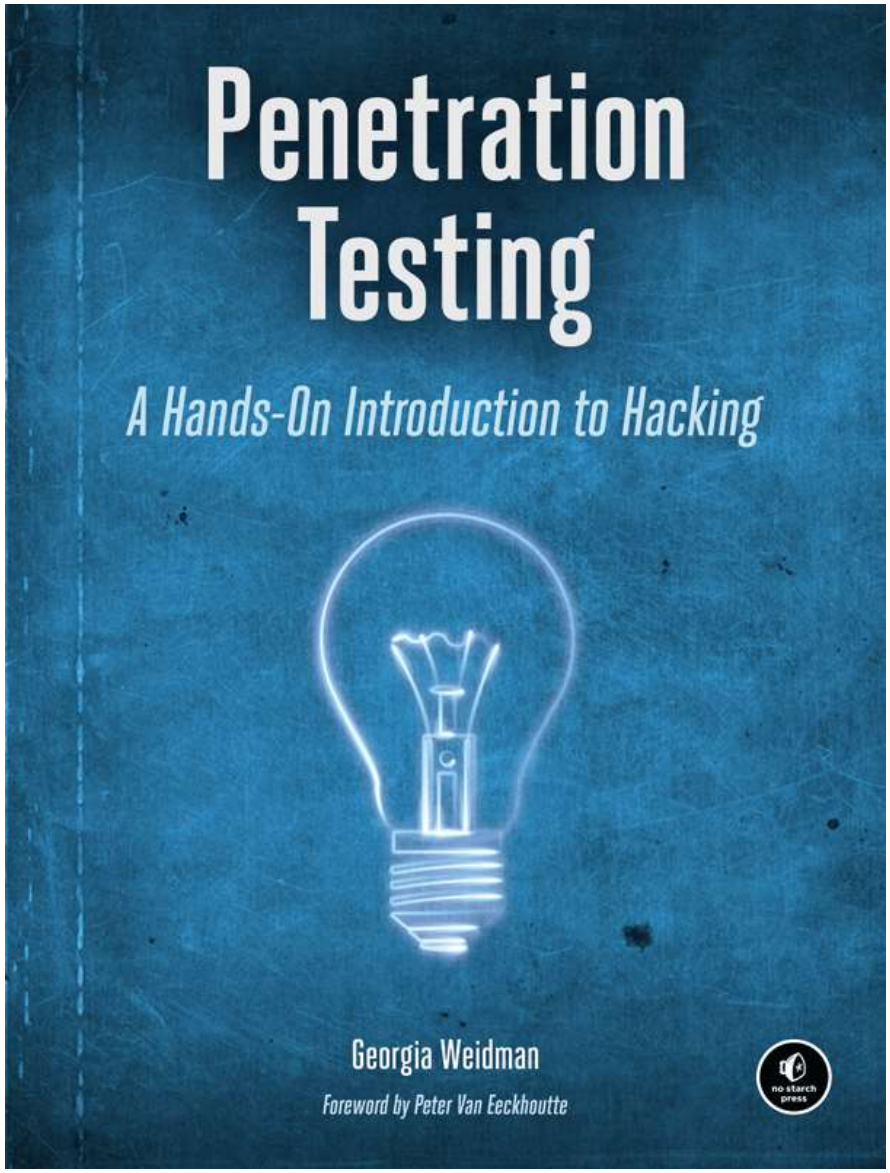
Как научиться проводить тесты на проникновение? Самостоятельное обучение. Хорошие книги



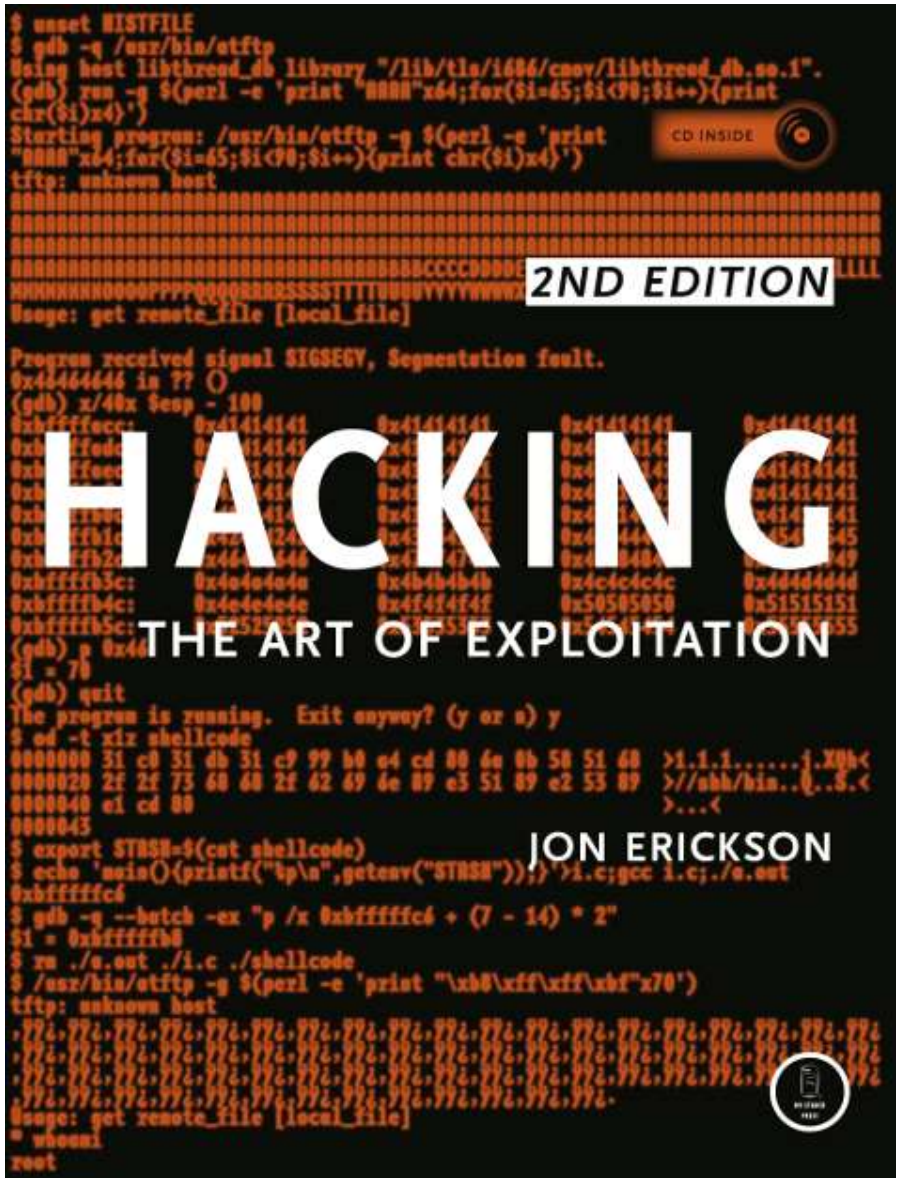


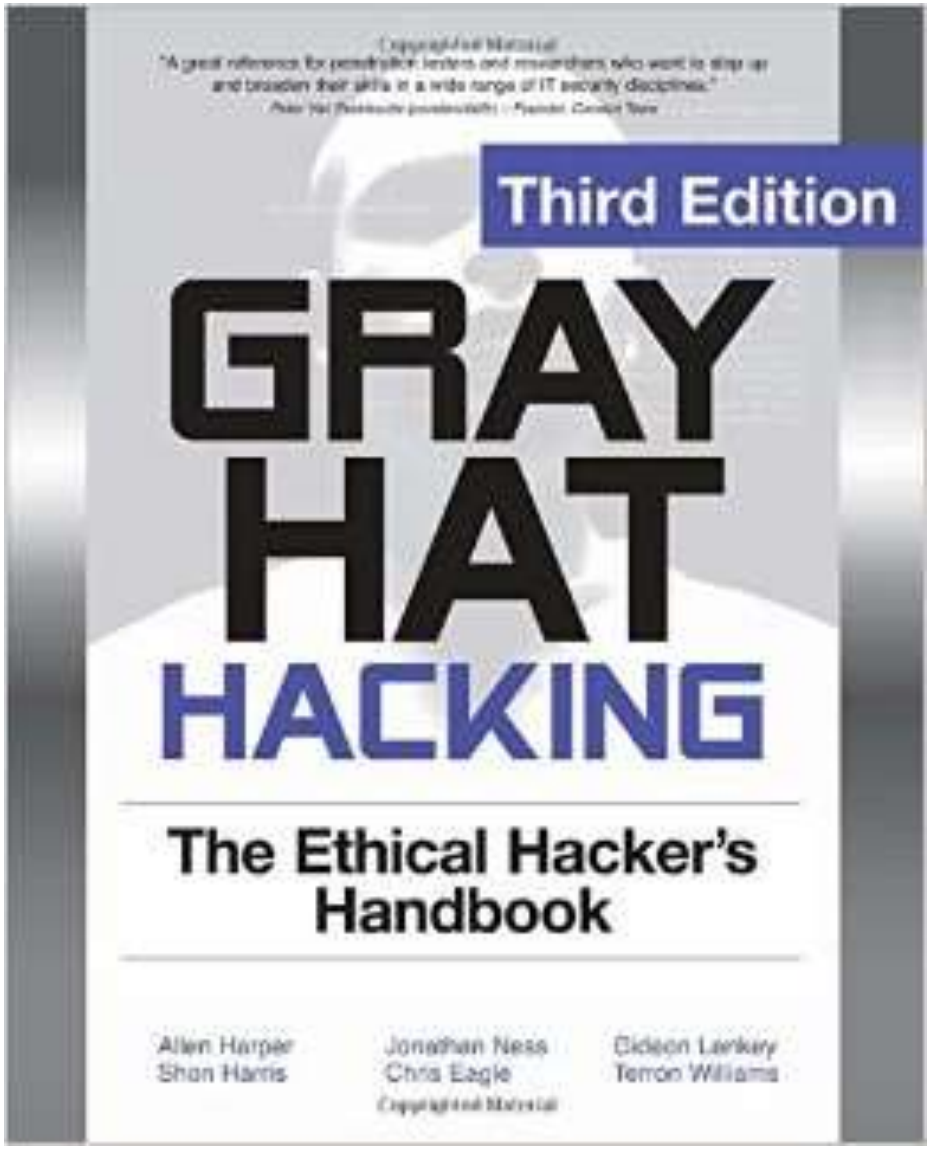
Как научиться проводить тесты на проникновение?
Самостоятельное обучение. Хорошие книги



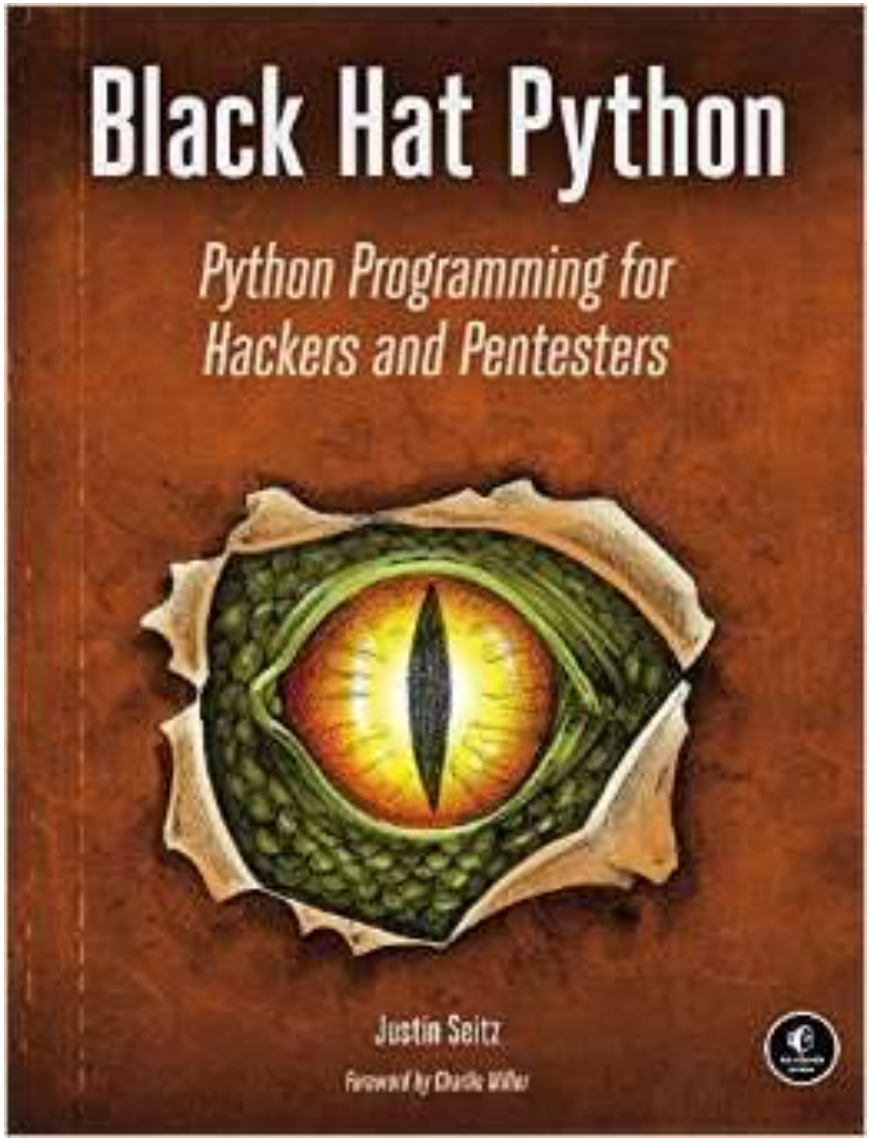


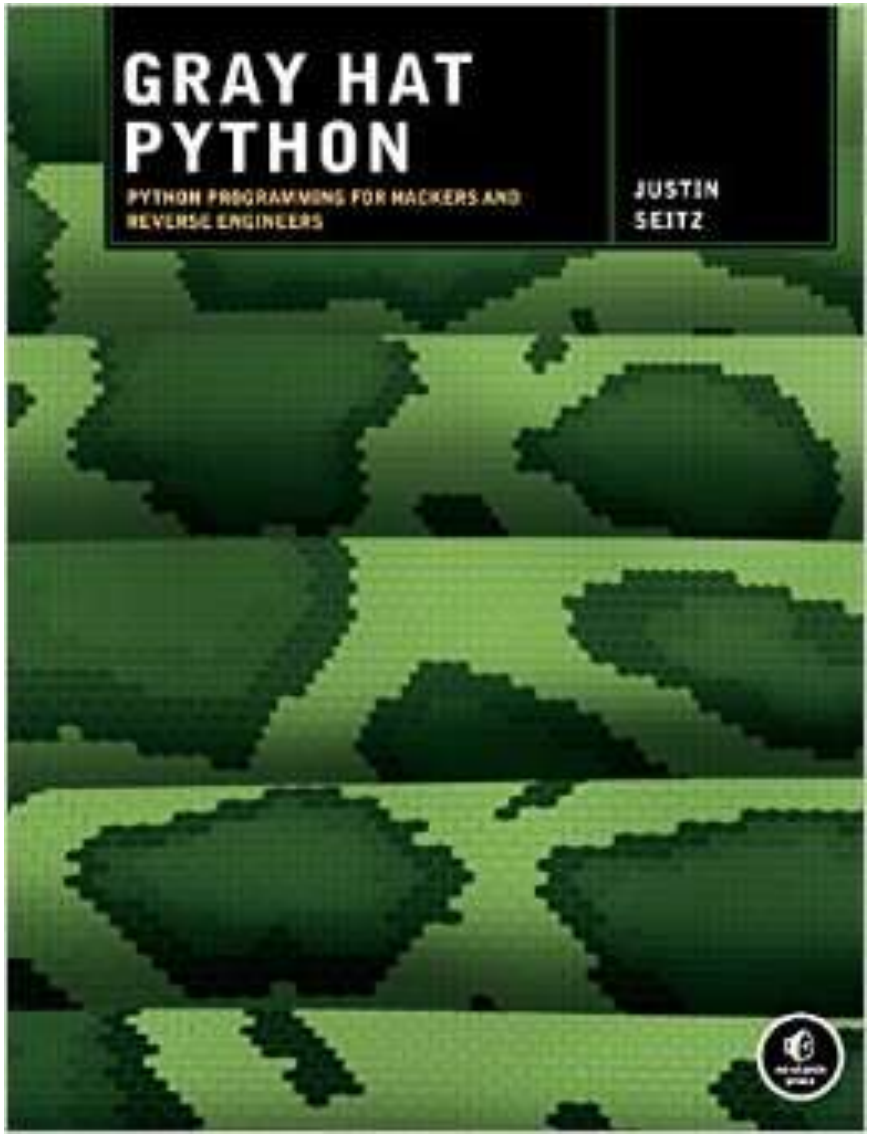
Как научиться проводить тесты на проникновение? Самостоятельное обучение. Хорошие книги



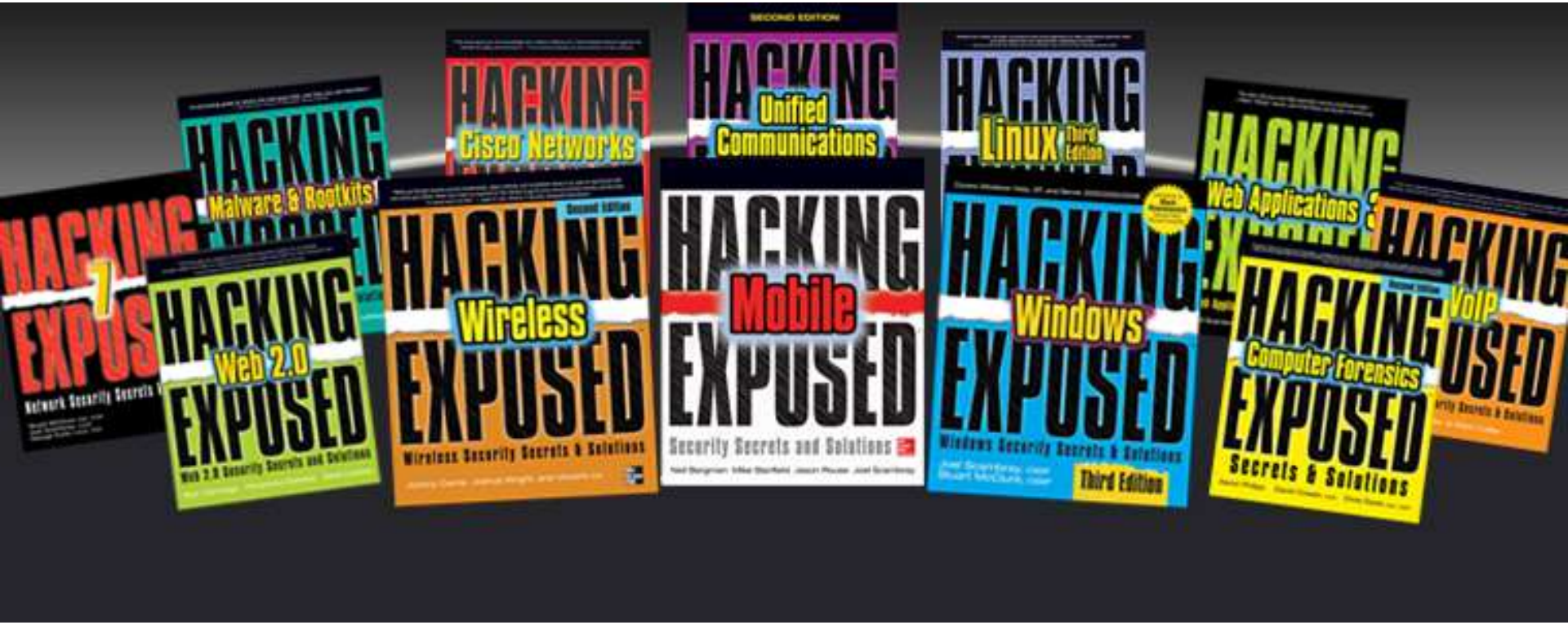


Как научиться проводить тесты на проникновение?
Самостоятельное обучение. Хорошие книги





Как научиться проводить тесты на проникновение?
Самостоятельное обучение. Хорошие книги



Как научиться проводить тесты на проникновение? CTF

Типы:

- Attack / defense CTF;
- Jeopardy CTF;
- CTF, в которых эмулируется инфраструктура реальных компаний.

Могут проводится:

- Online;
- Offline.

Виды участия:

- командные;
- индивидуальные.

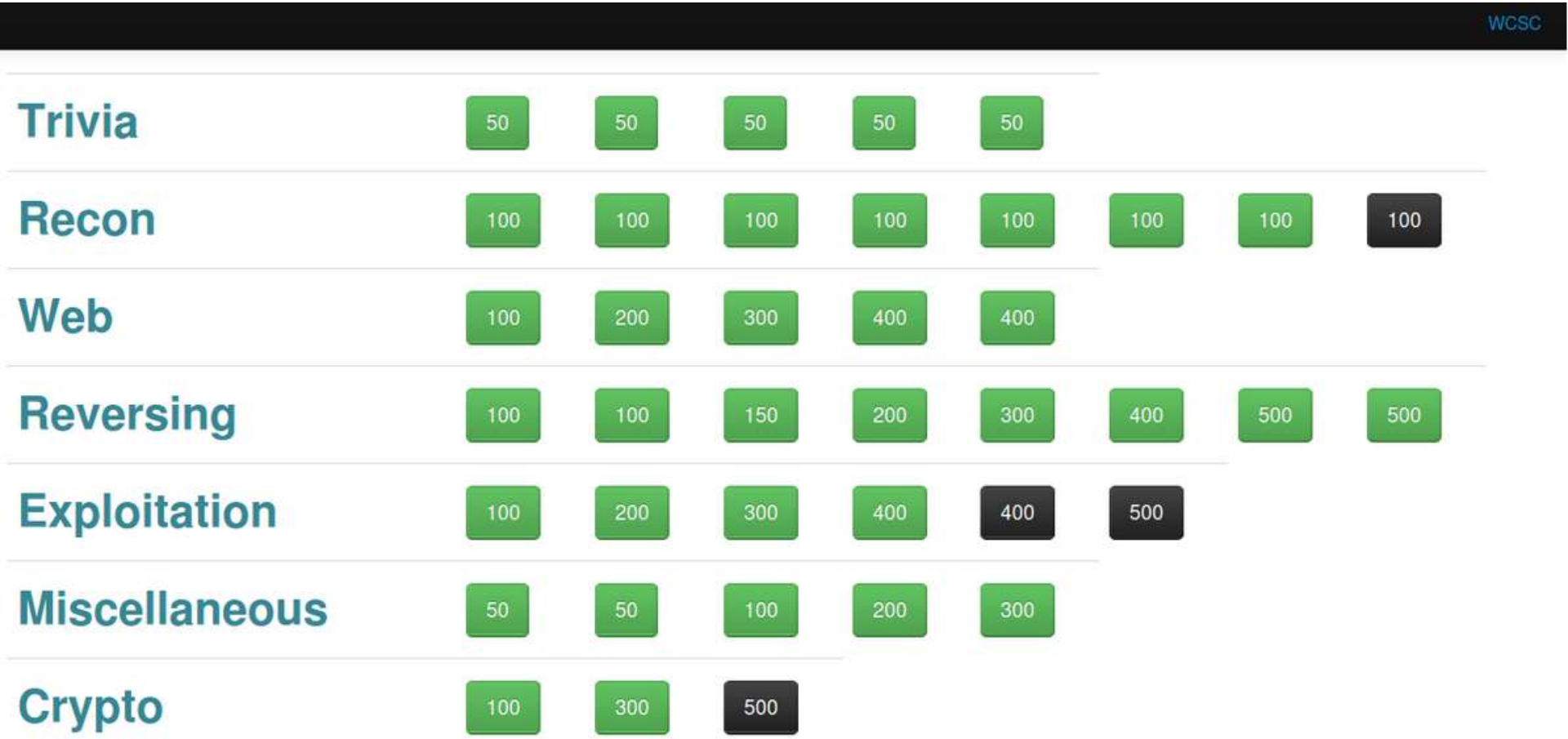
https://ctftime.org - расписание CTF-ов, рейтинги команд.

Как научиться проводить тесты на проникновение? Jeopardy CTF

Игрокам предоставляется набор заданий (тасков), к которым требуется найти ответ и отправить его. Ответом является флаг — набор символов или произвольная фраза. Каждое задание оценивается различным количеством очков, в зависимости от сложности. Обычно выделяются следующие категории:

- admin – задачи на администрирование;
- joy – различные развлекательные задачи вроде коллективной фотографии или мини-игры;
- PWN – поиск уязвимости и разработка эксплойта;
- reverse – исследование программ без исходного кода (реверс-инжиниринг) ;
- stegano – стеганография;
- ppc – задачи на программирование (professional programming and coding) ;
- crypto – криптография;
- web — задачи на веб-уязвимости, такие как SQL injection, XSS и другие.

Как научиться проводить тесты на проникновение?
Jeopardy CTF

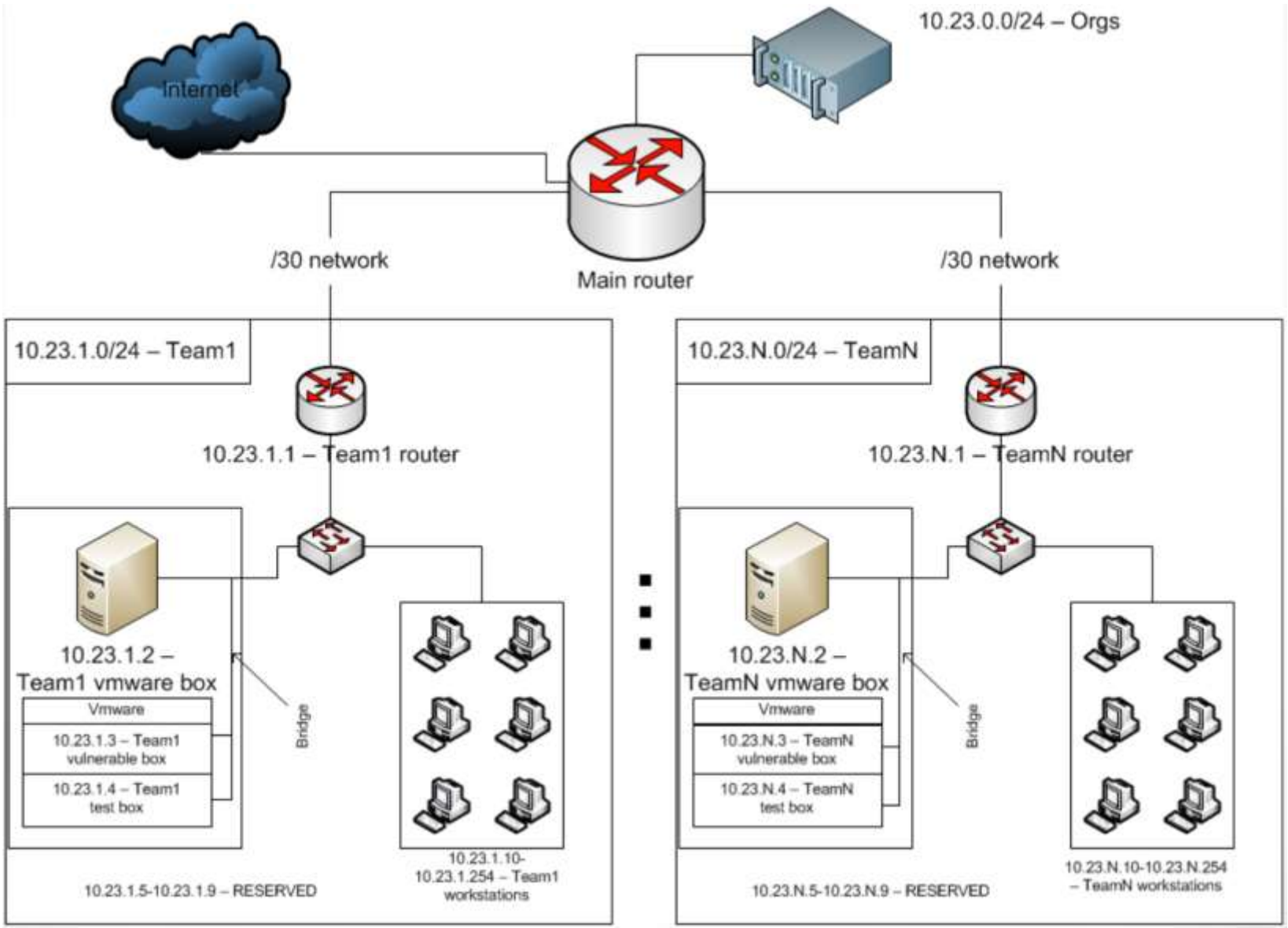


Как научиться проводить тесты на проникновение? Attack/Defense CTF

В Attack/Defense CTF каждая команда получает выделенный сервер или небольшую сеть для поддержания её функционирования и защиты. Во время игры команды получают очки за корректную работу и защиту сервисов своего сервера и за украденную информацию (флаги) с серверов противников. Флаги периодически кладутся на сервера команд специальным ботом.

Команды могут делать что угодно со своим персональным сегментом сети. Как правило, команды заняты поиском и закрытием уязвимостей в сервисах и организацией мониторинга и/или автоматической фильтрации трафика для блокирования атак других команд (исключая блокировку по признакам команд). И команды могут атаковать другие команды (кроме DDoS атак).

Как научиться проводить тесты на проникновение? Attack/Defense CTF



Как научиться проводить тесты на проникновение? CTF, эмулирующие реальную ИТ-инфраструктуру

В данного типа CTF организаторами эмулируются ИТ-инфраструктуры, близкие к инфраструктурам реальных компаний. Т.е. используются типовые для корпоративных сетей архитектуры и сетевые сервисы. Задача участников – провести тест на проникновение эмулированной инфраструктуры, попутно собирая флаги.

Примеры таких CTF:

- бесплатные лаборатории тестирования на проникновение PentestIT;
- Symantec Cyber Readiness Challenge;
- Kaspersky Industrial CTF.

Как научиться проводить тесты на проникновение? CTF, эмулирующие реальную ИТ-инфраструктуру

Спасибо за внимание!
Вопросы?