ISSN 2079-8490

Электронное научное издание
«Ученые заметки ТОГУ»
2018, Том 9, № 1, С. 307 – 312

Свидетельство
Эл № ФС 77-39676 от 05.05.2010
http://pnu.edu.ru/ru/ejournal/about/
ejournal@pnu.edu.ru

УДК 004.056

© 2018 г. **А. В. Зинкевич**, канд. техн. наук,
М. С. Михайлов
(Тихоокеанский государственный университет, Хабаровск)

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В статье описаны основные понятия тестирования на проникновение. Рассмотрены цели и задачи, механизм проведения тестирования, основные этапы и используемые техники.
Ключевые слова: тестирование на проникновение, пентест, информационная безопасность, хакер, сканирование, уязвимость, взлом, вредоносное программное обеспечение.

A. V. Zinkevich, M. S. Michaylov

AUDIT OF INFORMATION SECURITY

The article describes the basic concepts of penetration testing. The goals and tasks, the testing mechanism, the main stages and the techniques used are considered.
Keywords: penetration testing, pentest, information security, hacker, scanning, vulnerability, hacking, malware software

Введение

В наше время в мире происходит все больше инцидентов информационной безопасности, которые повысили интерес общества к теме хакерских атак. Атаки на критическую инфраструктуру, последствия которых могут оказаться катастрофичными, вирусы-шифровальщики, уже не только шифрующие файлы, но и блокирующие работу медицинского и промышленного оборудования, огромные по численности ботнеты, способные оставить без связи государства, и это только некоторые известные на сегодняшний день угрозы получившие огласку в СМИ.

Хакеры стали частью реальности. Вполне естественно, что предприятия сегодня в первую очередь вкладывают ресурсы в практическую безопасность в противоположность формальному выполнению требований регуляторов. Встает вопрос о проверке эффективности выстроенной системы защиты. Для этого существует специальная область практической информационной безопасности, как тестирование на проникновение.

Основные понятия о тестировании на проникновение

Рассмотрим практические аспекты информационной безопасности (ИБ), связанные с компьютерными атаками и непосредственной защитой от них. Для взлома в исполнении специалистов, легально имитирующих действия злоумышленников, используется термин «тестирование на проникновение» (penetration testing, пентест). За этим термином скрываются сразу несколько направлений исследования защищенности, и в каждом из них работают свои узкие специалисты.

Тестирование на проникновение — это один из видов аудита ИБ, и в этом его главное отличие от реального взлома. Злоумышленник ищет самую короткую дорогу к контролю над целевыми системами и пытается закрепиться на данном пути. А специалист-пентестер, должен досконально обследовать каждую возможную уязвимость в системе. Это позволяет понять, так ли хорошо, как мы думаем, выстроены процессы ИБ, надежны ли системы защиты, верна ли конфигурация, и понимаем ли путь, по которому предпочтет идти потенциальный злоумышленник.

Тестирование на проникновение состоит из нескольких этапов. Это сбор информации об исследуемой системе, ручное и автоматизированное сканирование на предмет уязвимостей, попытки проникновения и закрепления в системе, отчет о проведенном тестировании и рекомендации по устранению найденных уязвимостей. [2]

Таблица 1

Основные этапы тестирования на проникновение

Планирование	Согласование целей и содержания тестирования
Получение информации	Сбор открытой информации, сканирование и поиск уязвимостей
Проникновение и действия в системе	Эксплуатация найденных уязвимостей, Эскалация привилегий, Закрепление в системе
Подведение итогов тестирования и устранение уязвимостей	Предоставление отчета о найденных уязвимостях, рекомендации по их устранению

Сбор информации зависит от модели знаний о системе, которая определяет стартовую позицию пентестера. От полной информации о системе (White box) до полного ее отсутствия (Black box).

Зачастую выделяют и промежуточный вариант (Grey box), когда пентестер имитирует действия непривилегированного пользователя, имеющего некоторые данные о системе. Это может быть рядовой клерк, партнер, клиент с доступом в личный кабинет и т.п.

White box — это скорее аудит, нежели классический пентест. Применяется в том случае, когда нужно детально изучить защищенность на узком участке. Например, проверяется новый клиентский портал. Исследователю предоставляется вся информация по системе, зачастую с исходным кодом. Это помогает детально изучить безопасность системы, но едва ли имитирует реальные атаки.

Заказчики Black box пентеста хотят получить полную имитацию атаки хакера, который не обладает инсайдерской информацией о системе. Часто при данном виде тестирования проверяется не только компьютерные системы защиты, но и действия персонала, ответственного за информационную безопасность. В этом случае работы координирует руководство ИБ, а сотрудники безопасности полагают, что борются с реальными хакерами, если, конечно, вообще замечают атаку. Такие «киберучения» позволяют оценить не только наличие уязвимостей в тестируемых системах, но и зрелость ИБ персонала, уровень взаимодействия между подразделениями и другие аспекты работы ИТ-подразделения.

Модель знаний о системе сильно пересекается с понятием модели нарушителя. Кто атакует систему: внешний хакер, инсайдер, администратор? Часто это деление очень условно, так как компрометация рабочей станции рядового пользователя или партнера, с технической точки зрения, превращает внешнего хакера во внутреннего нарушителя, что существенно упрощает дальнейший взлом и закрепление в системе. [3]

Проникновение и действия в системе

На этапе проникновения в систему, специалистом, используя собранную информацию о целевой системе, предпринимаются попытки обойти защитные механизмы.

Системный взлом (System hacking) — проверка хостов и сетевой инфраструктуры на наличие уязвимостей в операционных системах и используемом программном обеспечении. После сканирования целевых систем и сборе необходимой информации пентестер лучше понимает, как злоумышленники могут проникнуть и закрепиться в системе.

Взлом системы — важный этап по многим причинам. Эта часть тестирования сопровождается постоянной угрозой обнаружения. Основная цель — оставаться в системе, до достижения целей взлома. В большинстве подобных сценариев, злоумышленники ущерб инфраструктуре не наносят, а целью является получение информации с высокой ценностью, такой как коммерческая тайна, засекреченная информация и персональные данные.

Во время сбора информации и сканирования пентестеры получили знания о моделях используемых устройств, версиях прошивок и операционных системах, установленном программном обеспечении, запущенных службах и процессах. Имеется необходимая информация чтобы понять, как работает инфраструктура, и какие факторы могут иметь ключевое значение.

Производятся обнаружение активных устройств в сети, открытых портов, и идентификация работающих служб и приложений. Имена хостов и информация об IP–адресах может быть собрана различными методами, такими как опрос DNS и WHOIS запросы, различные виды сканирования и прослушивания сети. Информацию об используемых операционных системах можно найти различными способами – с помощью протокола NetBIOS, или анализа IP пакетов.

Рассмотрим несколько наиболее популярных утилит для сканирования.

В качестве примера программного обеспечения рассмотрим «Nmap» – одну, из наиболее известных утилит, используемых для проведения сканирования.

Nmap («Network Mapper») — это утилита с открытым исходным кодом для исследования сети и проверки безопасности. Она использует «сырые» IP пакеты оригинальными способами, чтобы определить какие хосты доступны в сети, какие службы они используют и их версии, операционные системы, типы пакетных фильтров/брандмауэров и еще множество других характеристик, которые могут быть полезны при проведении тестирования на проникновение.

Интересен способ, которым Nmap производит определение операционных систем на сканируемых хостах. Утилита посылает серию TCP и UDP пакетов на удаленный хост и изучает практически каждый бит в ответах. После проведения нескольких тестов таких как TCP ISN выборки, IP ID выборки, и анализа продолжительности процедуры инициализации, Nmap сравнивает результаты со своей базой данных, состоящей из более чем тысячи известных наборов типичных результатов для различных операционных систем и, при нахождении соответствий, выводит информацию об операционной системе. Каждый набор содержит текстовое описание и классификацию операционной системы, в которой указаны название производителя, название системы, поколение, и тип устройства.

После получения необходимой информации, специалисты по тестированию на проникновение пытаются взломать систему для выявления способов возможных атак, и предотвращения реализации данных атак реальными злоумышленниками. К основным атакам относятся: попытки получения и взлома паролей, эксплуатация известных уязвимостей, эскалация привилегий, установка шпионских утилит и вредоносного программного обеспечения. Так же важным является сокрытие следов пребывания в системе и используемых инструментов.

Пароли по-прежнему широко используются потому что они дешевы и легки в эксплуатации. Грубый взлом паролей занимает большое количество времени. Чаще всего злоумышленники пользуются методами социальной инженерии для получения паролей. В данном случае безопасность зависит от бдительности пользователя.

Угадывание пароля в значительной степени наиболее эффективно и может быть выполнено, если кто-то использует легко запоминающийся пароль, например, имя домашнего питомца или один из технических паролей. Возможно, на этапе сбора информации вы узнали нужную информацию и сейчас можете ее использовать.

При проведении тестирования на проникновение важно знать, где хранятся пароли в системе. В системах семейства Microsoft Windows пароли хранятся в диспетчере учетных записей или в базе данных SAM в хешированном формате. Она может быть найдена в папке SystemRoot или system32, которая по умолчанию доступна только администраторам. [1]

При получении доступа к данной базе, есть возможность расшифровать хранящиеся в ней пароли. На сегодняшний день для этого есть пять подходов, которые с определенным успехом применяются во множестве утилит: грубый перебор, подбор по словарю, подбор по словарю с правилами или «гибридная атака», «радужные таблицы» — это особый тип словаря, который содержит цепочки паролей и криптоатаки.

Рассмотрим особенности утилиты «John the Ripper password cracker», предназначенную для вскрытия различных типов хэшей, которые применяются во множестве программного обеспечения и операционных системах. В программе реализованы возможности: брутфорса пароля, подбора по словарю и гибридная атака. А также «signle» и «external» способы подбора пароля, специфичные для этой программы.

Одной из важных особенностей данной утилиты является тот факт, что при взломе большого количества паролей одновременно, велика вероятность того, что они вскроются быстрее, чем если бы мы делали это по отдельности.

Так же упомянем утилиту «TCH Hydra», которая поддерживает огромное количество служб. Благодаря своей быстроте и надёжности она завоевала заслуженную признательность среди специалистов по тестированию на проникновение. Будучи очень мощной и гибкой, Hydra является кроссплатформенной утилитой и поддерживает множество используемых протоколов.

Одним из распространенных заблуждений является то, что если кто-то получает пароль и соответственно доступ к системе, то он может запускать приложения, устанавливать вредоносное программное обеспечение. Но это не так. Обычно этичный хакер сначала получает доступ к системе, получив имя пользователя и пароль наименее защищенной учетной записи. Это позволит получить доступ к системе, но без прав администратора.

Дальнейший взлом системы потребует уровня доступа администратора. Эскалация привилегий бывает двух видов: горизонтальная или вертикальная. В горизонтальной эскалации привилегий этичный хакер перенимает права у пользователя, уже имеющего нужные привилегии. При вертикальной эскалации привилегий этичный хакер повышает уровень привилегий учетной записи, к которой у него уже есть доступ.

Чаще всего, нужные права доступа достигаются путем использования уязвимости в приложении или операционной системе.

Когда нужный уровень доступа получен, важно помнить о том, что чем дольше находишься в системе, тем больше следов ты оставляешь, и тем проще обнаружить вторжение. Поэтому хакеру необходимо оставаться незамеченным как можно дольше.

Хакер может установить руткит, для возможности доступа к системе позже, кейлогер для сбора информации, вредоносное программное обеспечение.

Как только злоумышленник получает привилегии уровня администратора может быть нанесен большой ущерб. Поэтому цель состоит в том, чтобы быть бдительными и защищаться от эскалации привилегий. Есть несколько лучших практик, такие как двухфакторная авторизация, или запрет удаленного входа в систему.

Таблица 2

Примеры программного обеспечения, используемого на определенных этапах проведения тестирования на проникновение

Сбор данных, идентификация целевых узлов	Nmap Nslookup Net view
Поиск уязвимостей	Nessus Nikto LanScope
Эксплуатация уязвимостей	Metasploit THC Hydra Cain&Abel
Вредоносное программное обеспечение	njRAT Ghost Eye Worm

Вредоносные программы могут быть сгруппированы в пяти категориях: шпионское программное обеспечение, вирусы, черви, трояны и руткиты.

Шпионское программное обеспечение (Spyware) — это форма вредоносного ПО,

которое доставляется в систему различными методами и используется злоумышленниками для сбора информации. В его возможности входит возможность фиксации активность экрана, захват нажатий клавиш, сбор данных веб-форм, отслеживание использования Интернета, а также разрешение злоумышленнику получить несанкционированный доступ к конфиденциальным данным.

Требуется соблюдать несколько простых правил чтобы защитить вашу систему от вредоносного программного обеспечения. Быть осторожными при загрузке чего-либо. Думать, прежде чем нажимать и открывать любые вложения электронной почты. Если защитные механизмы предупреждают, что сайт, который вы собираетесь посетить имеет рискованную репутацию, не посещает сайт. А так же своевременно устанавливайте обновления для программного обеспечения и операционных систем.

При выполнении тестирования на проникновение, одно из ценных умений заключается в том, чтобы скрыть следы присутствия в системе и используемые инструменты. Файлы могут быть скрыты в альтернативных данных, потоках или с помощью стеганографии, так же, некоторые руткиты имеют функции очистки журналов, помимо обеспечения backdoor.

Отчет — критически важная часть работы специалиста по тестированию на проникновение. Заказчик работ должен получить детальное описание всех успешных и неудачных попыток проникновения, понятное описание уязвимостей и исчерпывающие рекомендации по их устранению. К последней части рационально привлекать профильных специалистов по защите информации, потому что в каждом случае следует учитывать конкретную ИТ-инфраструктуру.

Заключение

В области защиты информации, наиболее ценными и квалифицированными, считаются специалисты, обладающие практическими навыками обеспечения безопасности. Сегодня проведение тестирования на проникновение является востребованной услугой проверки безопасности инфраструктуры, результаты которой помогают достоверно оценить состояние информационной безопасности. В статье рассмотрены основные этапы аудита безопасности компьютерных систем, в частности тестирования на проникновение, такие как сбор информации, эксплуатация уязвимостей, использование вредоносного программного обеспечения и общие рекомендации противостояния описанным методам.

Список литературы

[1] Engebretson, Patrick, - The basics of hacking and penetration testing: ethical hacking and penetration testing made easy / Patrick Engebretson, 2011. – 159 с.
[2] G. Weidman, Penetration Testing: A Hands-On Introduction to Hacking / Georgia Weidman, 2014. – 495 с.
[3] Скабцов Н.В. Аудит безопасности информационных систем. – СПб.: Питер, 2018. – 272 с.

E-mail:
Зинкевич А. В. — 006526@pnu.edu.ru
Михайлов М.С. — 2011025373@pnu.edu.ru