ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ КАК МЕТОД УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

PENETRATION TESTING AS A METHOD OF INFORMATION SECURITY MANAGEMENT

A. Klyuev
A. Fajzenger
D. Yuriev

Summary. The article discusses the sets of the method that provoke a network attack, the value of which is to penetrate the secret sectors of the company, changes to data and/or theft, breach or failure to perform critical business processes.

Keywords: penetration testing, intelligence, audit, information system.

Клюев Андрей Сергеевич
Аспирант, Дальневосточный федеральный университет, г. Владивосток
kozerog1991@gmail.com
Файзенгер Алексей Аркадьевич
Аспирант, Дальневосточный федеральный университет, г. Владивосток
Юрьев Дмитрий Русланович
Аспирант, Дальневосточный федеральный университет, г. Владивосток

Аннотация. В статье рассматриваются наборы данного метода, которые провоцируют сетевые нападения, ценностью которой является — проникнуть в секретные секторы компании, изменения данных и/или кража, нарушения или сбои работы критически-важных бизнес процессов.

Ключевые слова: тестирование на проникновение, разведка, аудит, информационная система.

Тест на проникновение (penetration test или сокращенно pentest) — это один из способов продемонстрировать, в какой степени защищена ваша компания от попыток войти в её секретную инфраструктуру на ее конфиденциальные данные и различные угрозы для информации. В иностранных странах также не редка пересекаются термины под названием этический хакинг (ethical hacking).

Мероприятия такого характера являются важным для любой компании, зависящей от информации и предоставляющие услуги ее систем информационных технологий. Например, работа банковского учреждения почти полностью зависит от её функционирований процессинговой системы, а интернет магазин перестаёт совершать продажи при блокировки его веб-страницы.

Каждый день все больше ощущается взаимосвязь ИТ информации и технологий во всех компаниях и абсолютно не имеет значение её направления. Случаи с информационной безопасностью, которые часто связаны со взломами, бывают критическими или даже могут стать роковыми для многих компаний, ежегодно. О подобных инцидентах, как правило о умалчивают, что определенно реализует беспечную атмосферу для других компаний. Но бывает и так, что некоторые форс мажорные случаи попадают в СМИ на популярные новостные сайты.

Подобающее большинство компаний готовы оплачивать миллионы на приобретение разнообразных ИТ-решений и обслуживание тех самых «самолетов», которые не работают в основном даже на 30% своей производительности, но не готовы оплачивать адекватные деньги за твердость в сохранности своей компании и своего бизнеса. Информационная безопасность придерживается одного золотого правила, которое гласит, что сумма, затрачиваемая на защиту информации никогда не должна переходить выше её стоимости.

Изучение уязвимости производится специальными разработанными программами-сканерами, которые позволяют автоматически проверять сетевую площадку и веб-сайты компании на присутствие брешей. Без сомнений, такое мероприятие бывает одним из основных этапов теста на проникновение, предоставляющее найти значительное количество потенциальных изъян в системе, определить отсутствие обновлений, утилит, патчей или других проблем в защите ИТ-систем.

В отличии от злоумышленников которые пытаются навредить или войти в инфраструктуру компании, у отряда тестеров есть чётко поставленные рамки которые соглашаются и регламентируются обеими сторонами, при выполнении всех своих операций: все действия которые могут привести к сбою или навредить системе, реализуются только по заранее составленному сговору, все операции сканирования абсолютно чисты и спланированы, работа критических бизнес-процессов не нарушается, а на финальном этапе теста заказчик получает объективные отчеты о состоянии дел в его компании,

системы безопасности в терминах, понятных не только программистам, но и бизнесу.

Наличие методик разного типа выполнения тестов на проникновение не останавливает творческой составляющей, что требует от личного состава, исполняющей его, глубоких познаний в сфере ИТ-безопасности и так же — умения мыслить неординарно, применять методы социальной инженерии, анализировать и собирать информацию.

Для проведения теста на проникновения, необходимо комплексное решение которые включает в себя разные виды работ по которым согласовываются стоимость и время, за которое оно будет выполнено. В то же время, нужно согласовать дополнительные параметры такие как количество участников.

На установленной фазе можно закончить целиком проект в ином случае продолжать pentest стезёй анализа внутренних сетей (возможные подходы: белый или частично серый ящик). В аналогичной ситуации имитируются атаки с фронта инсайдера. Опциями тестирования должны быть:

Тестирование общей площади под названием сеть. Глубокая диагностика на проникновение, или же провести автоматизированное сканирование уязвимости внутренних средств компании. Показывается количество IP адресов, приложения и веб-сайты.

Исследование кода веб-страниц. Программный код проверяется на наличие уязвимостей и изъян типа SQL injection, command injection, file inclusion, DoS, на присутствие закладок добавленных несанкционированно, недостатки в архитектуре и др.

Исследованием программного кода приложения. Код диагностируется на существование изъян уязвимости типа Buffer overflow, DoS, на присутсвие закладок добавленных несанкционированное, недостатки в архитектуре и др.[12]

Аудитория устройств — мобильников. Исследование безопасности применения планшетов, смартфонов, телефонов, также устройства хранение данные такие как USB, плееров и другие мобильные устройства.

1. Немаловажно установить порядок демонстрации отчетности. Компетентные аудиторы могут предоставить доступную информацию о выполненной работе для менеджмента в чёткой и ясной форме. Из наиболее эффективных вариантов:

- Результат отчетности по окончании тестирования;
- Предоставлять отдельный отчет сразу при нахождении критической уязвимости;
- Выполнять отчеты с промежутком раз в 2–3 дня.

2. Также должны установить следующие организационные аспекты:

- Линии связи для обработки информации между заказчиком и командой тестеров. Естественно они закодированы;
- Ответственные лица со стороны исполнителя и заказчика;
- Определенный алгоритм действий в случае возникновения непредвиденных инцидентов, связанных с проведением тестирования;
- Тестирование проходит в определенных рамках (например, только в выходные дни, только безопасные проверки для определенных систем и т.д).

Каждое мероприятие по тестированию проводится только после того как подписали договора, а также подлинное соглашение о неразглашении с исполнителями. Исполнитель со своего фронта проводит явную подготовку к тесту: ставит в известность персонал, организовывает совместную работу, готовит необходимое оборудование и ПО, каналы связи и прочее.

Неотложное назначение аудиторов на этом этапе становится собирание насколько возможно огромного количества ресурсов о тестируемых процессах и о сотрудниках компании. Часто уже на в этом пункте вероятно нахождение критически-уязвимых изъян, например, забытые или «бесхозные» сервисы, не запрашивающие регистрации и предоставляющие доступ во внутреннюю сеть, опубликованная конфиденциальная информация, пароли и иная опасная информация. [12]

Даже после проникновения рассматриваются другие варианты атак, с помощью которых можно проникнуть в информационную систему (ИС).[11] Преимущества тестирования на проникновение: — позволяет эффективно продемонстрировать возможность проникновения в ИС и выявить слабые места в обеспечении информационной безопасности; — позволяет выделить критические проблемы безопасности, требующие непосредственного внимания; — позволяет выделять финансовые и материальные ресурсы на обеспечение безопасности ИС на тех участках, на которых это требуется больше всего; — тестирование подразумевает использование различных сценариев, учитывающих особенности ИС предприятия.

Поиск информации происходит в доступных источниках вручную, а также при помощи специализированных инструментов. В объем работ, как правило, входит поиск информации в таких источниках:

- Система поиска;
- Анализировать e-mail письма;
- Звонки в call-центр компании с целью получить информацию о ключевых сотрудниках компании, о структуре компании и технологиях;
- Исследование метаинформации в документации, размещенных на веб-сервисах компании и т.д.;

Как мы видим из описанного раннее, тест на проникновение — это объёмная и сложная услуга, у которой есть возможности показать текущую картину уровня ИБ систем. Результатом проведения подобного тестирования часто удивляют выше поставленных руководителей компаний-заказчиков. Практика показывает проведение тестов, связанные со слабой организацией в установке обновлений и заплаток (patch management), проникновение в хранилище сети через «бесхозные» сервисы, расположенные по соседству с критическими бизнес приложениями, несерьезные отношения к вопросам компетентности персонала в вопросах информационной безопасности, в которых 99% атак методами социальной инженерии успешно реализовываются. [11]

Свежие изъяны в системах и технологиях находят практически каждый день. В следствии, защита информации в бизнесе должна стать постоянной процедурой, а не одноразовым схождением. Отличная практика хоть раз в год проводить профилактику на тему проникновения, а в промежутки между ними организовать программы управления уязвимостями (vulnerability management) путем закупки сканера изъян и периодического самостоятельного сканирования площади сети. Такой подход обеспечивает высокую защиту от устремлённых атак, либо от направления конкурентов или других имеющих интерес персон, у которых есть определенные ресурсы (деньги, время, квалифицированных специалистов и технологии), сопоставленных с ценой самой информации.

В виду того, что тест на проверку изъян не дает сто процентной гарантии защищенность системы: есть еще различные системы защиты, одна из них 0-day уязвимости, наличие которой известно лишь определённо узкому кругу персон. Похожими так называемыми «дырами» обычно пользуется хакерская группа лиц, подобным прославившихся Anonymous. На подпольных сайтах за некую сумму есть возможность приобрести эксплойты для этих изъян, и если у злоумышленника достаточно ресурсов, взлом будет всего лишь делом времени. [11]

Для того что бы уменьшить возможность нахождения изъян системы и последствия взлома от посторонних лиц необходима организация аспекту «defense in depth» (глубокоэшелонированной защиты) и доступности высокого уровня, наладить все необходимые процессы для реализации на уменьшения угроз последствия атаки и попыток взлома. Важными элементами являются организация следующих процессов:

- Обновление и установка ПО в системах;
- Организационное управление риском для критически важных бизнес процессов и систем;
- Следить и управлять изменениями;
- Мониторить и регистрировать события влияющие на безопасность;
- Реагировать на инциденты в тех ситуациях когда обнаружен взлом;
- Расследовать инциденты (forensics) с юридическими и правильными оформлениями улик;
- Информационную безопасность– должен знать каждый работник;
- Управлять резервированием и восстановлением потерянной информации.

Для того что бы организовать безопасность своего бизнеса необходимых процессов необходимо выбрать один из подходов к реализации информационной безопасности, предлагаемые международным, а теперь и некоторыми национальными стандартами.

ЛИТЕРАТУРА

1. Серия международных стандартов ISO 27000
2. Common Vulnerability Scoring System, V3 Development Update URL: https://www.first.org/cvss (дата обращения: 12.01.2018).
3. Угрозы, уязвимости и атаки в сетях. URL: http://asher.ru/security/book/its/24 (дата обращения: 12.01.2018).
4. Систематика уязвимостей и дефектов безопасности программных ресурсов. URL: http://www.npo-echelon.ru/doc/is_taxonomy.pdf (дата обращения: 12.01.2018).
5. Buffer overflaws demystified. URL: http://www.enderunix.org/docs/eng/bofeng.txt (дата обращения: 12.01.2018).
6. Once upon a free(). URL: http://phrack.org/issues/57/9.html (дата обращения: 12.01.2018). 57
7. Core Impact Pro. Comprehensive multi-vector penetration testing. URL: http://www.coresecurity.com/core-impact-pro (дата обращения: 12.01.2018).
8. Nmap techniques for avoiding firewalls. URL: https://pentestlab.wordpress.com/2012/04/02/nmap-techniques-for-avoiding-firewalls/ (дата обращения: 12.01.208)
9. Port scanning techniques. URL: http://nmap.org/book/man-port-scanningtechniques.html (дата обращения: 12.01.2018).
10. Port scanning with Nmap. URL: http://my.safaribooksonline.com/book/networking/security/9781593272883/3dotintelligence-gathering/active_information_gathering (дата обращения: 12.01.2018)

11. [Электронный ресурс] http://auditagency.com.ua/?lang=en&p=Pentest&r=blog
12. [Электронный ресурс] https://sp123.ru/services/testirovanie-vashey-korporativnoy-informatsionnoy-sistemy/

Дальневосточный федеральный университет