УДК 004

ПЕНТЕСТ И ЕГО ОСОБЕННОСТИ

Журавлева В. В.,

студент,

Калужский государственный университет им. К. Э. Циолковского,

Калуга, Россия

Ткаченко А. Л.,

к.т.н., доцент,

Калужский государственный университет им. К. Э. Циолковского,

Калуга, Россия

Аннотация. Информационная безопасность стала одним из самых важных видов профессий на малых и крупных предприятиях. С изменением схем защиты информации сменилась и тактика мошенничества в сети. Специалисты в области информационной безопасности способны выявить уязвимости и устранить их, чтобы не допустить утечки информации. В данной статье рассматриваются основные характеристики пентеста, а именно его особенности, этапы тестирования и несколько видов методик для защиты информационной системы.

Ключевые слова: пентест, кибербезопасность, тестирование, информационная система, уязвимости.

PENTEST AND ITS FEATURES

Zhuravleva V.V.,

student,

Kaluga State University named after K.E. Tsiolkovsky,

Kaluga, Russia

Tkachenko A.L.,

Candidate of Technical Sciences, Associate Professor,

Kaluga State University named after K.E. Tsiolkovsky,

Kaluga, Russia

Annotation. Information security has become one of the most important professions in small and large enterprises. With the change in information security schemes, the tactics of fraud in the network have also changed. Information security specialists are able to identify vulnerabilities and eliminate them in order to prevent information leakage. This article discusses the main characteristics of the pentest, namely its features, testing stages and several types of techniques for protecting the information system.

Keywords: pentest, cybersecurity, testing, information system, vulnerabilities.

С появлением высоких технологий требуется все больше опыта и сноровки, чтобы справляться с наплывом встречающихся проблем. В современном мире проблема информационной безопасности является одной из самых распространенных и важных в IT-сфере [1-4]. Кибератаки, распространенные на крупных и малых предприятиях могут привести к утечке конфиденциальной информации и снижению работоспособности. Далеко не все кампании справляются с защитой своих баз, поэтому в данных ситуациях привлекают тестировщиков, главной целью которых является выявление уязвимостей через тестирование программ на проникновение.

Метод для оценки безопасности компьютерных систем посредством взлома и проникновения в базу под видом злоумышленника называется пентестом. Сценарий таков, что экспертам необходимо реализовать атаку на систему, а затем по выявленной «дыре» в защите идет ее исправление. Пентестеров еще называют «белыми» хакерами, этичными хакерами или белошляпниками. Такие хакеры действуют по закону и защищают интересы людей [5-7].

Основными этапами пентеста являются:

1) Разведка;
2) Сканирование;
3) Получение доступа;
4) Закрепление в системе;
5) Удаление следов;
6) Подготовка отчета.

Пентестеры могут заниматься тестированием в различных областях. Тест может проводиться над приложением, ПО (программное обеспечение), различными устройствами, сетью. И вследствие чего могут выявляться недочеты, например: открытые порты, неправильно настроенные протоколы, устаревшая прошивка, неправильная конфигурация, человеческий фактор и т. д.

Существует несколько методик тестирования:

1. Внутреннее тестирование. Хакер действует как сотрудник компании и пытается навредить системе изнутри.

2. Внешнее тестирование. Хакер действует на расстоянии и пытается внедриться в систему с внешней стороны.

3. Двойное слепое тестирование. Это опасный вид, при котором вовлечены 2 человека. Необходимо иметь дополнительные документы, что тестировщик работает легально.

4. Белый ящик – метод, при котором у пентестера есть знания о системе.

5. Черный ящик – метод, при котором для хакера есть только данные в открытом доступе.
6. Серый ящик – метод, при котором данные лишь частичные.

Пентестеры делятся на красных и синих. Задача одних атаковать, а других защитить. Таким образом моделируется искусственная атака на систему и защита ее в реальном времени.

Чтобы практиковаться и заниматься в дальнейшем пентестом есть несколько полезных инструментов:

1. Kali Linux – легкая ОС, содержащая 600 программ для атаки и поиска уязвимостей.
2. Metasploit – набор ПО, включающий различные программы для различного рода целей.
3. Nmap – программа для сканирования сети с любым количеством пользователей. Используется для сбора информации о портах, службах и ОС устройства.
4. Nessus – программа, которая сама найдет распространенные уязвимости в системе и сети.
5. Wireshark – программа, анализирующая трафик. В ней храниться информация о том, как устроены пакеты, передающиеся по сетевым протоколам. Так же если данные в сети не зашифрованы можно получить по ним сведения.
6. Aircrack-ng – программа для перехвата трафика в беспроводных сетях.

Пентестерам необходимо уметь и знать множество нюансов из различных отраслей. Тестировщик на проникновения должен знать:

1) Компьютерные сети, а именно каким образом функционирую сети, как найти их уязвимости, протоколы и т. д.
2) Методы атак на информационные системы. Необходимо проводить атаку и уметь защищать систему от них.

3) Знание языка программирования. В особенности очень цениться Python для пентеста.
4) Администрирование Linux.
5) Анализ вредоносного ПО. Необходимы знания о вирусах, червях, троянах. Пентестер должен знать, как создать и применить вредоносное ПО.

Подводя итог исследований, можно сделать вывод, что современные информационные системы хотя и подвержены множеству кибератак есть и люди способные им противостоять. Множество специалистов по кибербезопасности, а в их числе и пентестеры привлекаются для оценки возможных уязвимостей в системе, чтобы модернизировать защиту и улучшить работоспособность организаций.

Библиографический список:

1. Кондрашова, Н. Г. Экономическая безопасность и ее обеспечение в коммерческой организации / Н. Г. Кондрашова // Modern Economy Success. – 2021. – № 1. – С. 207-212. – EDN LKEBGG.
2. Ибрагимова, З. М. Информационная безопасность как элемент экономической безопасности / З. М. Ибрагимова, З. Б. Батчаева, А. Л. Ткаченко // Инженерный вестник Дона. – 2022. – № 11(95). – С. 26-33. – EDN AMZDZG.
3. Малюкова, Д. С. Информационные технологии в биомедицине и генетике / Д. С. Малюкова, А. Л. Ткаченко, А. В. Мазин // Modern Economy Success. – 2022. – № 1. – С. 53-57. – EDN MYAWRG.
4. Ткаченко, А. Л. Реинжиниринг бизнес-процессов туристической компании / А. Л. Ткаченко, А. А. Щеглова // Вестник Калужского университета. – 2021. – № 1(50). – С. 77-80. – EDN AMWKWN.
5. Шаурина, О. С. Информационные таможенные технологии в условиях цифровой трансформации / О. С. Шаурина, Т. В. Лесина, А. А. Мигел // Modern Economy Success. – 2021. – № 4. – С. 50-55. – EDN IXYKKT.

6. Противодействие преступности в регионе / Н. Ю. Чаусов, С. Н. Гагарина, С. В. Морозова, Н. Н. Чаусов // Вестник Калужского университета. – 2018. – № 1. – С. 109-112. – EDN WBRVVN.

Оригинальность 85%