IT

- Основные понятия ИБ для гуманитариев

Основные понятия ИБ для гуманитариев

Вы пытаетесь пройти на стройку и представляетесь вахтёру своим именем, после чего проходите внутрь. Это идентификация.

Перед тем, как пройти внутрь, вы вынуждены показать вахтёру свой паспорт. Это аутентификация.

Вы вынуждены показать одному вахтёру свой паспорт, а второму по памяти назвать его серию, номер и вспомнить, что находится на странице с номером, похожим на Кенни. Это двухэтапная аутентификация.

Вахтёр требует не только паспорт, но и водительское удостоверение. Это двухфакторная аутентификация.

Какой-то пидарас наебал вахтёра, показав ему чужие документы. Это подделка учётных данных.

Вахтёр в курсе, что его наебали, но вынужден пропустить, т.к. документы подлинные. Это имперсонация.

Вахтёр выдаёт вам на шею бейдж с персональным идентификатором. Это сессионный токен.

Вы показываете этот бейдж при входе в любую дверь. Это авторизация.

Какой-то пидарас спиздил чужой бейдж и везде его показывает. Это угон сессии.

Он же подложил вахтёру копию бейджа со своим идентификатором и дождался, пока тот не отдаст его вам. Это фиксация сессии.

Вы потоптались по только что налитому полу, не оставив в нём следов и никто кроме вас не знает, что это вообще случилось. Это приватность.

Вы потоптались по только что налитому полу, оставили в нём следы, но никто не знает, какой пидарас это сделал. Это анонимность.

Вахтёр записал в журнал дату и время вашего прихода и ухода. Это журналирование.

Вахтёр ходит за вами по пятам и записывает вообще все ваши действия. Это ретроспектируемое журналирование.

Вахтер сделал запись в журнал, что пару дней назад к ним на стройку устроился какой-то стрёмный работник с такой же фамилией, что и у вас. Это корелляция событий.

Вахтёр в ходе корелляции событий периодически жмёт кнопку, после чего начинает орать сирена, мигать красные лампочки, а весь персонал съёбывает по подвалам, откладывая кирпичи. Это SIEM.

Прораб за это наконец-таки набил вахтёру ебало. Это актуализация правил корелляции событий SIEM.

На стройке вам на голову может упасть кирпич. Это угроза.

Кирпич весит килограмм и ещё пол кирпича, ускорение свободного падения 9,80665 м/с², солнце в зените, а кирпичи могут находиться на любом из отстроенных этажей <плюс все вытекающие из этого расчёты>. Это модель угроз.

Какой-то мужик в шляпе рассказывает вам, как правильно строить модель угроз. Это Лукацкий.

Какой-то пидарас может сбросить вам кирпич на голову с верхнего этажа. Это атака.

Для этого он пройдёт на стройку, поднимется на самый верхний этаж, возьмёт в руки кирпич, прицелится и сбросит его вниз. Это эксплоит.

Ваша голова не предназначена для попадания в неё кирпича с заданным весом и ускорением. Это уязвимость.

Вы убираете со стройки все кирпичи, исключаете наличие на ней каких-то пидарасов и, на всякий случай, ещё и верхних этажей. Это защищённость.

Вы надеваете каску, чтобы хоть как-то снизить последствия попадания кирпича. Это безопасность.

У вас в правилах безопаности предписано всем носить каски, вы получили за них пушкинскую премию от регуляторов, но персонал как ходил без касок, так и продолжает ходить. Это бумажная безопасность.

Какой-то пидарас пробрался на стройку, залез на верхние этажи, убил кирпичом прораба и теперь радостно требует заплатить ему за это вознаграждение. Это багхантер.

Прораб пока ещё жив, тот пидарас кидается кирпичами во все стороны, а вахтёр уже заебался нажимать на красную кнопку. Это багхантер с анализатором защищённости.

Вы нанимаете двух прорабов, чтобы в случае смерти одного из них, работы не прекращались. Это формальная отказоустойчивость.

Вы нанимаете столько прорабов, сколько у вас кирпичей на стройке плюс ещё один. Это фактическая отказоустойчивость.

Вы покупаете устройство, кидающееся кирпичами во все стороны, на манер мячиков для тенниса. Это DAST.

Вы покупаете виртуальный симулятор, делающий всё то же самое, что и DAST, но без стройки. Это SAST.

Вы покупаете модуль обратной связи между кидающимся устройством и симулятором стройки. Это IAST.

Вы заебались покупать и обратились за помощью к сторонней компании. Та предлагает вам приобрести новейшую бетономешалку от именитого вендора, чтобы решить проблему с кирпичами. Вы в душе не ебёте, как связаны бетономешалка и кирпичи, но таки покупаете. Теперь у вас с верхних этажей могут упасть не только кирпичи, но и блядская бетономешалка, что делает проблему кирпичей не такой уж и значимой. Это -- привлечение интегратора.

Производитель бетономешалки по вашему запросу выпускает патч, оснащающий её реактивной системой торможения в воздухе. По неведомым причинам это приводит к отказу строительного крана, эпидемии гриппа среди персонала и ухудшению вязких свойств бетона. Это...

Вы наняли эксперта, чтобы тот проверил возможность проникновения на стройку, залезания на верхние этажи и сброса кирпичей на головы персонала. Это пентестер.

Пентестер не только смог убить прораба с помощью кирпича десятью разными способами, но и разрушил к ебеням весь объект, сжёг технику и заставил вахтёров сношать друг-друга. Это опытный пентестер, которому вовремя не обозначили скоуп тестирования.

Вы сделали всё мыслимое и немыслимое, чтобы упавший кирпич никого не убил, объект нельзя было разрушить, технику сжечь. И ещё пояса верности на вахтёров, чтобы наверняка. На следующий же день прораба прибивает к хуям отвалившаяся тормозная система бетономешалки...