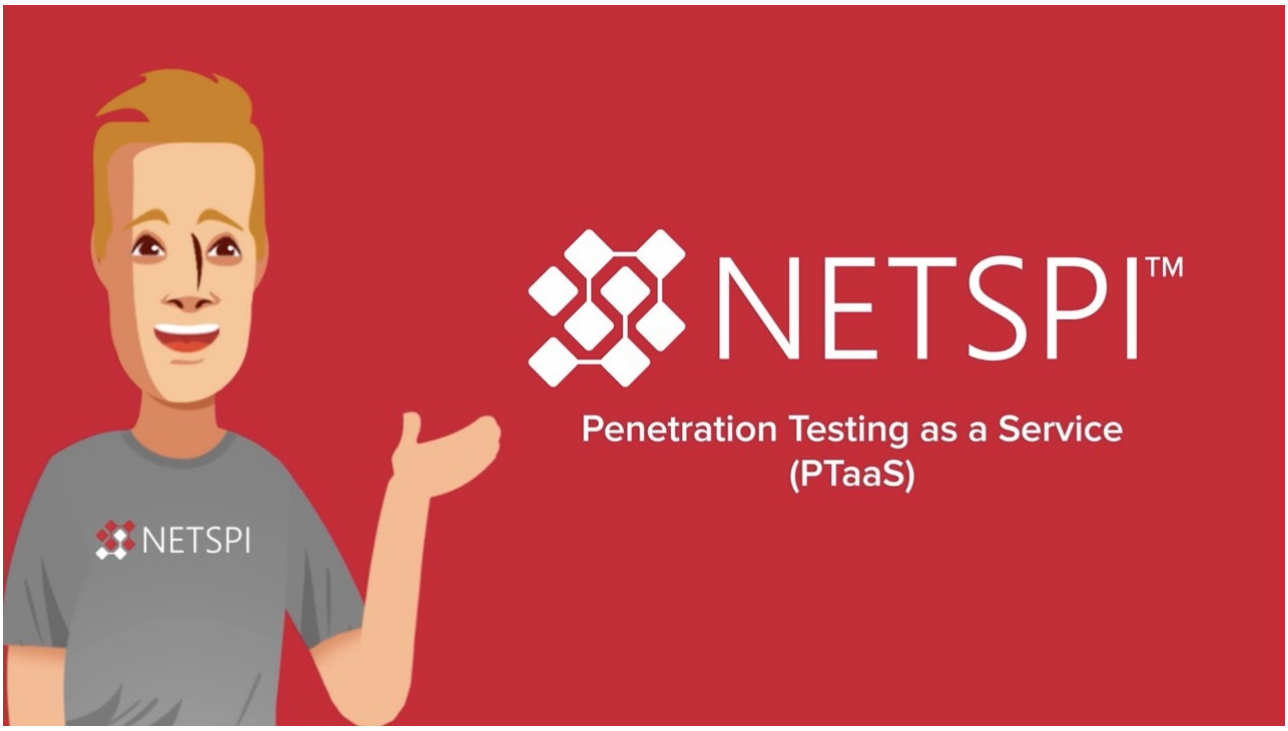
Пентест для ЦОД или "проверка на вшивость"

NetSPI* — специалист по проверке ИТ-безопасности компаний методом пентеста (англ. penetration test — тестирование на проникновение). По заказу других организаций, эта американская фирма оценивает защиту их внутренних систем и выявляет потенциальные уязвимости, которыми могут воспользоваться злоумышленники для несанкционированного доступа, в том числе физического.



В недавнем интервью Data Center Knowledge, старший консультант NetSPI Далин Макклеллан (Dalin McClellan) рассказал об одном показательном случае из практики своей компании, в котором приемы социальной инженерии позволили без особого труда попасть в строго охраняемый дата-центр. По иронии, персонал ЦОД провалил "тест на вшивость", пустив на объект якобы сотрудников по дезинсекции, а на самом деле – пентестеров NetSPI.

Проверку заказал владелец сети коллокейшн-центров. Он поставил перед NetSPI непростую задачу — не только физически попасть на территорию дата-центра, но и проникнуть в одно из помещений, из которого можно было бы получить доступ к его сетевой инфраструктуре. О реальном взломе сети речи не шло.

По словам Макклеллана, ЦОД относился к объектам высокой степени защищенности. На всех дверях имелись сканеры сетчатки и считыватели пропусков. Также, здание было оснащено пропускными вестибюлями. Пройти через них дальше можно только после того, как за посетителем закроются двери, через которые он зашел. Это значит, что пентестерам не удалось бы попасть внутрь, пристроившись за кем-то из сотрудников. Хуже того, в дата-центре находилось только два человека из персонала и один охранник, то есть посторонних немедленно бы обнаружили. Плюс, заказчик дал на выполнение задания всего семь дней, тогда как обычно пентестерам требуется несколько недель на подготовку к проникновению и сбор всевозможной информации об объекте и людях, которые там работают.

С учетом сжатых сроков клиент пошел навстречу и передал NetSPI сведения, которые они обычно выясняют самостоятельно: имена сотрудников, их контакты, список вендоров, обслуживающих объект, и время их работы. Также, заказчик предоставил другую общую информацию - как строится общение, как выглядят фирменные бланки и подписи в электронных письмах, какая терминология используется.

Узнав, что дата-центр проводит экскурсии для потенциальных клиентов, записаться на которые можно онлайн, в NetSPI поначалу хотели воспользоваться этой возможностью для проникновения. Однако, заказчик забраковал идею, заявив, что если пентестеры попадутся, то во время задержания они могут пострадать, поскольку будут иметь дело с весьма решительным сотрудником в вопросах обеспечения безопасности.

Риск для пентестеров не в новинку, но в NetSPI посчитали, что лучше не искушать судьбу.

"Мы стали просматривать список поставщиков и заметили среди партнеров широко известную в стране службу по борьбе с насекомыми и вредителями. Так совпало, что один из консультантов, с которыми мы сотрудничаем, недавно приглашал эту фирму для обработки своего дома... Мы воспользовались его электронной перепиской с этой компанией и сфабриковали свое письмо, которое выглядело так, будто один сотрудник дата-центра отвечает на сообщение коллеги″, - рассказывает Далин Макклеллан о дальнейшем развитии пентеста.

В письме говорилось, что из службы дезинсекции приедут на объект в ближайшую пятницу, и что было непросто согласовать с ними дату и все необходимое. На следующий день на это сообщение пришел ответ со словами: ″Здорово, звучит неплохо″. То есть, сотрудники дата-центра не распознали, что письмо поддельное.

В следующие пару дней пентестеры готовились к визиту в ЦОД. Макклеллан и его команда подошли к вопросу тщательно: изготовили фирменные футболки, аналогичные тем, в которых ходят настоящие дезинсекторы, взяли в аренду фургон подходящей марки, модели и цвета, заказали магнитный логотип компании и прикрепили его сбоку автомобиля. Затем съездили в магазин хозтоваров, где взяли напрокат лестницу, сумки для инструментов и другое оборудование, которым могут пользоваться специалисты по борьбе с вредителями.

"В итоге, мы выглядели вполне достоверно, хотя потратили на все про все меньше 200 долларов", – отметил Макклеллан.

[Изображение недоступно]

Охранников дата-центра заранее предупредили о предстоящем визите службы, поэтому когда мнимые дезинсекторы подъехали к воротам объекта, обнесенного 2,5-метровым забором, их пропустили, попросив лишь предъявить удостоверения личности. Пентестеры показали свои настоящие водительские права.

"Затем нас встретил парень, которому мы отправили письмо по электронной почте. Он прошел проверку на сканере сетчатки и провел нас через все здание", – продолжил Макклеллан свой рассказ.

Прямой доступ к компьютерам получить не вышло: все оборудование находилось в клетках, и сотрудник не позволил туда войти. Зато он разрешил осмотреть потолочные плиты, якобы в поисках вредителей. При желании, в этот момент лже-дезинсекторы могли бы легко установить микрофоны, видеокамеры или подключить какое-то другое устройство. Однако команда Макклеллана не стала этого делать, поскольку целью была проверка персонала, а не реальный взлом сети.

Еще около двух часов пентестеры провели в здании, обходя помещения ЦОД и заглядывая в укромные уголки.

"Когда мы наконец вышли и уже уселись в фургон, то решили пойти еще немного дальше. Мы снова дозвонились сотруднику дата-центра, с которым контактировали, и сказали, что нужно подписать кое-какие бумаги, а также поинтересовались, нет ли у них принтера, чтоб распечатать документы. Сотрудник запустил нас назад и дал данные, чтобы подключиться к их Wi-Fi-сети".

По словам консультанта NetSPI, гостевая сеть Wi-Fi была достаточно хорошо сегментирована. К примеру, не было прямого доступа к данным клиентов. Тем не менее, если бы в задачу входил реальный взлом, то это стало бы для него отправной точкой.

В гостевой сети также не было доступа к принтеру, поэтому пентестеры отправили сотруднику электронное письмо с прикрепленными к нему документами, чтобы тот открыл их и распечатал. Окажись на месте сотрудников NetSPI настоящие хакеры, они бы воспользовались этим, чтобы внедрить вредоносное ПО и впоследствии получить доступ к сети.

Однако, проверка на этом завершилась. Пентестеры связались с клиентом и сообщили ему, как все прошло, а затем собрали вещи и покинули объект, где никто так и не заподозрил неладное.

Главным выводом из этой "операции" стало то, что клиент хорошо позаботился о политике безопасности для сотрудников и клиентов, но недостаточно продумал защиту со стороны вендоров и партнеров. Среди рекомендаций, которые бы помогли исправить ситуацию, Макклеллан перечислил создание отдельной системы для отслеживания визитов поставщиков на объект с проверкой их данных, а также использование дополнительных средств безопасности электронной почты, помогающих получателю заметить признаки подделки адреса email. Кроме того, в подобных случаях сотрудникам следовало бы лично связываться с поставщиком, чтобы получить подтверждение напрямую.

[Изображение недоступно]

"Да, на это нужно потратить время. Но если речь идет о строго охраняемом объекте, где используются сканеры сетчатки и пропускные вестибюли, то, наверное, не стоит жалеть времени на проверку личности каждого, кто входит в здание", – подытожил Макклеллан.

Также, он посоветовал клиентам после таких проверок ни в коем случае не наказывать сотрудников, которые попались на удочку мошенников.

"Сразу же возникает мысль: "О, этого человека, который вам помог, надо уволить". Но на самом деле это худшее, что можно сделать. При проведении пентестов не должно быть задачи покарать. Цель таких проверок — выявить пробелы в ваших системах контроля, политиках [безопасности], процессах инструктажа, чтобы повысить защиту. Вы только что заплатили большие деньги за действительно ценное обучение своих сотрудников, которые в процессе пентеста узнали, как вести себя со злоумышленником, пытающимся проникнуть в здание. Понимание того, как подобное происходит, не приобрести, сидя за компьютером. Опыт - лучшее урок, который вы можете получить", - подчеркнул Макклеллан.

Если же компания уволит сотрудника, который только что получил очень ценный опыт, то он просто заберет этот опыт с собой на следующее место работы. "А вы не получите от этого никакой пользы", - рассудил консультант NetSPI.

На самом деле, работникам следует узнать о результатах пентеста и понять, что произошло. Сделать это нужно в уважительной форме.

"Покажите свою ориентированность на персонал. Сделайте сотрудников поборниками безопасности. Человек, [не прошедший проверку] — это наиболее обученный сотрудник вашей организации в том плане, как распознать методы социальной инженерии. Сделайте этого человека защитником фирмы, амбассадором безопасности... Как по мне, это лучший возможный исход проверки с использованием социальной инженерии".

**Для справки:*

NetSPI — лидер в области предоставления услуг пентеста и управления векторами кибератак (Attack Surface Management, ASM). Среди его партнеров — 9 из 10 ведущих банков США, три из пяти крупнейших мировых фармацевтических компаний, ведущие облачные провайдеры и множество фирм из списка Fortune 500, в том числе корпорации Hewlett Packard Enterprise и Microsoft.