пен-тестинг по обе стороны сервера

крис касперски, ака мыщъх, no-email

популярность пен-тестов отчасти вызвана абсолютным непониманием целей, стоящих перед пен-тестером, а так же методов их достижения. заказывая тест на проникновение, администратор в большинстве случаев выбрасывает деньги на ветер, не получая взамен никакой информации о реальных угрозах и дефектах системы безопасности, но чтобы понять это, нужно хотя бы на время превратиться на хакера и взглянуть на задачу с позиции атакующего. мыщъх раскрывает боевые секреты пен-тестеров, которые наверняка заинтересуют как хакеров, так и администраторов.

введение

Мыщъх долго занимался пен-тестами, хотя не здорово это афишировал. Методом проб и ошибок был выработан четкий и эффективный план действий (в количестве шести мешков драпа), позволяющий проникать внутрь защищенных сетей с минимальными усилиями и практически без отрыва от основного "делопроизводства", то есть, фактически в полном бэкграунде.

И вот теперь этот план, отшлифованный до зеркального блеска, мыщъх выносит на всеобщее обозрение.

Рисунок 1 пен-тестер за работой

сканеры безопасности

Сканеры безопасности (типа XSpider) срабатывают только в клинических случаях, когда администратор лось и идет лесом. Обычно, перед тем как заказывать тест на проникновение, клиент делает все, что только может сделать — устанавливает последнюю

версию антивируса для поиска уже внедренных руткитов, скачивает свежие заплатки, прогоняет один или несколько сканеров безопасности и только после этого приглашает пен-тестров.

Конечно, пен-тест может проводится и без ведома администратора с подачи руководства компании, что существенно упрощает задачу атакующего, вот только удаленных способов определения установленных заплаток раз два и обчелся. Практически все известные мне сканеры работают в "мягком" режиме, используя косвенные эвристические подходы (в общем случае, сводящиеся к определению версии ПО), не решаясь на прямое переполнение буферов в силу небезопасности этой операции. Запускать exploit'ы один за другим и то выгоднее!

Пен-тестер просто не может полагаться на сканеры безопасности, поскольку ему платят не за "сканирование" сети, а только за реальные проникновения! Поэтому, приходится орудовать своими лапами и хвостом, вгрызаясь в защитный периметр острыми хакерскими зубами.

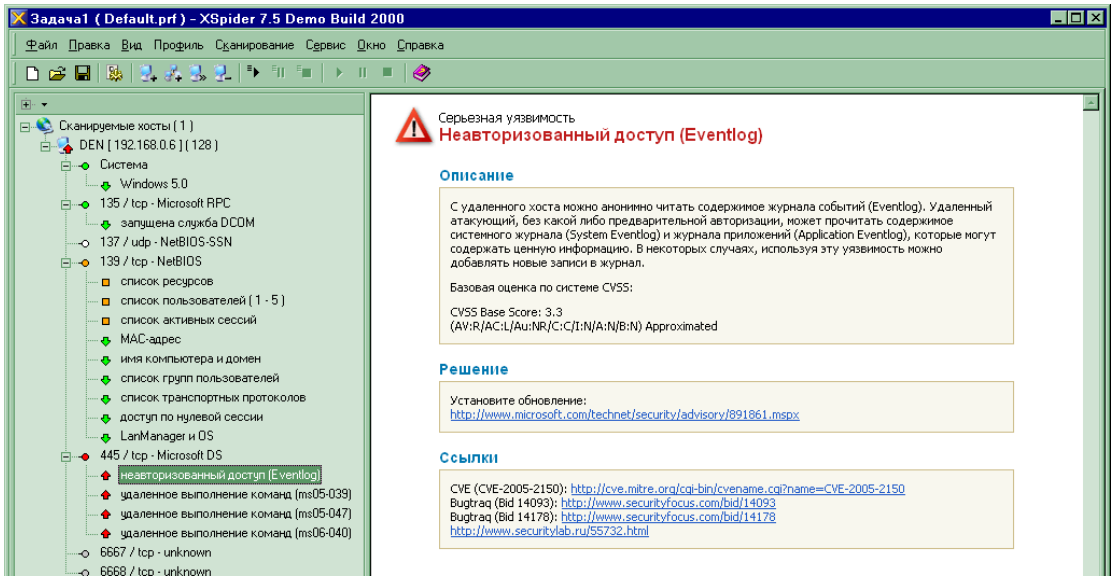

Рисунок 2 XSpider – сканер безопасности

цель определяет средства!

Security-консультанты обычно получают полный доступ ко всем уголкам сети и после тщательного анализа схемы безопасности передают администратору многостраничный отчет с перечнем явных и потенциальных дыр, а так же рекомендациями по их устранению. Обычно, Security-консультант получает деньги независимо от количества обнаруженных дыр и его труд оплачивается даже если никаких дыр он вообще не нашел, что очень даже замечательно, однако, здесь есть по меньшей мере два серьезных "но".

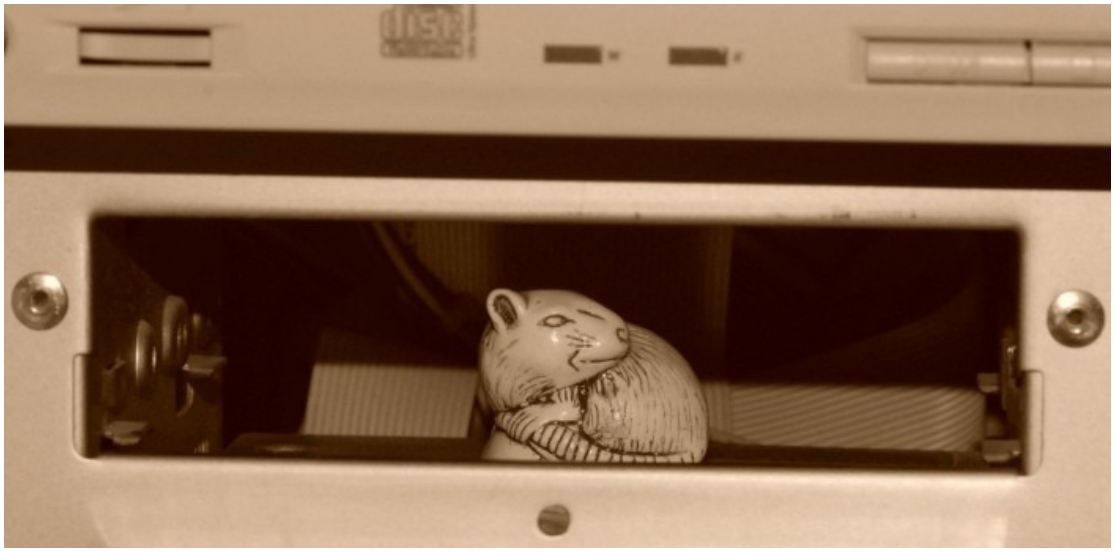

Рисунок 3 мыщъх сосредоточен в глубине норы своего одиночества

Первое — это ответственность за полноту предоставляемой информации. Заказчиком явно или неявно предполагается, что консультант найдет _все_ дыры, включая еще никому неизвестные, что невозможно по определению! Вот только заказчику этого не объяснишь и если спустя некоторое время его атакуют, то, возможно, придется сделать money back, а то и компенсировать ущерб, иначе чего доброго разъяренный заказчик может и морду побить. Следовательно, консультант должен в совершенстве владеть "пальцовкой" и выглядеть достаточно внушительно, создавая впечатление, что за спиной у него находятся могущественные силы, способные его защитить (шутка).

Второе — заказчик тоже не дурак и вероятнее всего попытается обхитрить консультанта, а поводов, чтобы не платить деньги, можно придумать много. Например, внедрить закладку в свою собственную систему безопасности, которую консультант ни за что не найдет, а потом, получив отчет, указать на нее пальцем и возмутиться, что в отчете ее нет. Естественно, это сильно упрощенная схема. На практике, заказчик обычно оставляет в системе безопасности N дыр, из которых консультант находит только K, что позволяет заказчику оценить степень полноты анализа, нижняя граница которого находится на уровне N/K. Если это соотношение окажется удручающе мало, консультант будет послан в пешее эротическое путешествие. Вердикт: администраторам — будьте бдительны и не дайте себя обмануть, консультанты – не найдетесь срубить капусты за просто так!

Пен-тестерам (за редкими исключениями) не дают никакой информации, кроме той, которую они могут получить самостоятельно через публичные источники, при этом, если пен-тестер не сможет проникнуть в систему, он не получает вообще ничего. То есть, заказчик оплачивает только реальные взломы. На первый взгляд кажется, что заказчик находится в выигрышном положении, а пен-тестеру вообще ничего не светит и лучше сразу уйти в консалтинг, на самом же деле, ситуация обстоит с точностью до наоборот!

От пен-тестера не требуется полнота анализа и он вообще ни за что не отвечает! Пен-тестер не подряжался искать _все_ дыры. Ему достаточно найти хотя бы одну, оставив в системе заранее оговоренный флаг "присутствия", доказывающий успешность ее компрометации (например, создать в непубличной директории файл с текстом "hacked") и все — кто не спрятался я не виноват! Сушите весла, господа! Пен-тестер выполняет поверхностный анализ, используя кратчайшие пути для достижения цели, не имеющие ничего общего с реальной картиной (не)безопасности системы. В то время как задача security-консультанта состоит в анализе общей защищенности, пен-тестер проникает внутрь охраняемого периметра, используя фиксированный набор шаблонных заготовок.

Ментальная ошибка заказчиков состоит в том, что они ошибочно считают, будто бы пен-тестер _ищет_ уязвимости, в то время как он действует по заранее продуманной стратегии, в которую анализ конкретных ситуаций не входит. Если принять, что защищенность системы это f(x), то вектор действий пен-тестера — это константа. Так за что же мы платим пен-тестеру деньги?!

постановка задачи

Типичный пен-тестинг начинается приблизительно так. Заказчик дает IP-адрес публичного WEB-сервера компании и требует от нас, чтобы мы забрались внутрь локальной корпоративной сети (с WEB-сервером, зачастую, никак не связанной) и… наследили там, отметив свое местопребывание. Внедрили shell или создали дисковый файл/запись в закрытой базе данных. Последние два пункта намного более предпочтительны, поскольку забраться в локальную сеть намного сложнее, чем выбраться оттуда и с shell'ом тут могут возникнуть траблы различной тяжести.

Ломать WEB-сервер смысла никакого нет, поскольку, даже если он и соединен с локальной сетью, то в 9 из 10 случаев находится в демилитаризованной зоне, огражденной брандмауэром, а это значит, что захватив контроль над WEB-сервером мы все равно не войдем внутрь сети пока не хакнем брандмауэр. Зачем это нам нужно?! Лучше атаковать непосредственно саму локальную сеть путем рассылки электронных писем с боевой начинкой или линками на "заминированные" html-страницы/файлы документов. Подробнее об этом мы поговорим ниже, а пока же рассмотрим комплекс подготовительных мероприятий, предшествующих атаке.

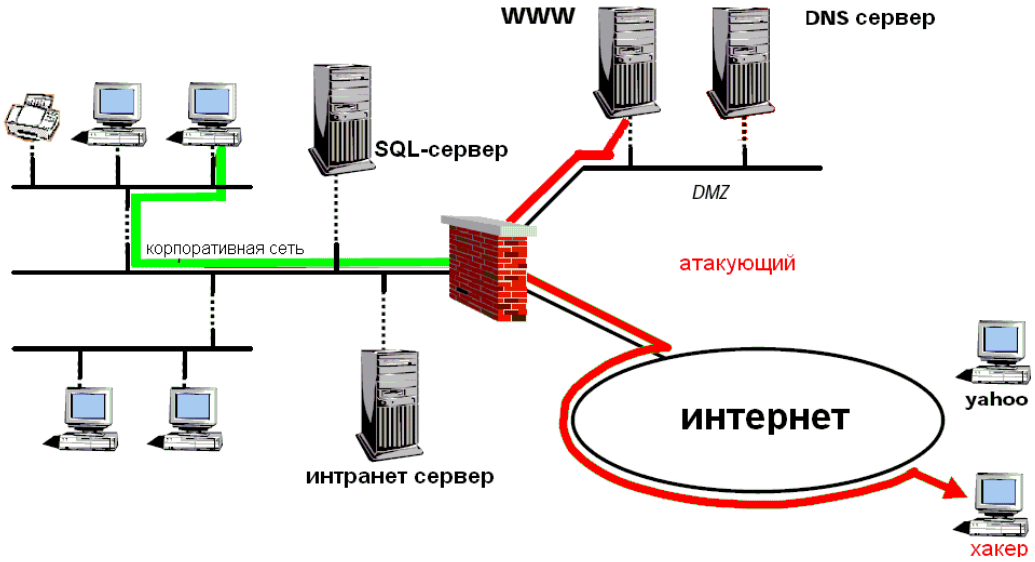

Рисунок 4 WEB-сервер в демилитаризованной зоне

Почему-то большинство заказчиков думает, что пен-тестер начинает работать только после подписания договора. Ага, щас, разбежались! Переговоры занимают достаточно длительное время, которое пен-тестер может (и должен!) использовать с пользой для дела. Во-первых, в это время администратор еще не на стреме и вероятность успешной атаки выше, во-вторых, в ходе подготовительных мероприятий пен-тестер оценивает свои шансы и если эти шансы скорее малы, чем велики, то ставит заказчика раком. Заказчик отказывается от услуг пен-тестера и обе стороны остаются довольны.

Естественно, атаковать компанию, не имея на руках бумаги, подтверждающей правомерность наших полномочий, нужно очень осторожно. Совершать противоправные действия при этом категорически недопустимо, но этого, собственного, и не требуется. Первым делом пен-тестер пытается ответить на вопросы: что это за компания? каким бизнесом она занимается? с кем сотрудничает? что за имена у ее сотрудников и партнеров? Получить эту информацию можно как с помощью социальной инженерии, выдавая себя за другое лицо (обычно высокопоставленное), так и честным путем, представившись потенциальным клиентом. Очень дотошным клиентом. И состоятельным. Короче таким, с которым компания заказчика будет вынуждена подолгу базарить, передавая его то одному, то другому сотруднику. Проще всего это сделать по телефону, но и про электронную почту забывать не следует.

Это не есть социальная инженерия, поскольку мы никого не "инженируем", а просто собираем минимально необходимую информацию для атаки — имена сотрудников, электронные адреса, названия отделов, etc. Если повезет, то удастся выяснить и личные предпочтения некоторых сотрудников (сотрудниц), например, узнать, что кто-то без ума от

группы "мама, роди меня обратно". Тогда тут же можно переслать по электронной почте "заряженный" клип или mp3 (благо, ошибки переполнения в аудио/видео плеерах встречаются в изобилии). Но это крайний случай. Будем исходить из того, что фортуна повернулась к нам задом и все девушки на фирме либо лесбиянки, либо феминистки. С мужчинами они разговаривают сугубо деловым тоном, с которого не съезжают ни при каких обстоятельствах.

Рисунок 5 мыщъх и его хвост

ударная фаза атаки

Имея на руках список электронных адресов — рассылаем на них обыкновенные (то есть ничем не начиненные) письма, на которые жертва просто обязана что-то ответить. Про бесплатные ящики типа mail.ru лучше сразу забыть — они нещадно давятся спам-фильтрами, да и выглядят несолидно. Какие проблемы в том, чтобы зарегистрировать несколько доменов третьего уровня в зоне com.ru например? Собственный сервер по современным понятиям уже давно не роскошь, особенно для IT-специалистов, коим безусловно является пен-тестер. В идеале, конечно, следовало бы порекомендовать домены второго уровня, но это совсем не обязательно.

Так же, письмо должно адресоваться конкретному лицу с указанием имени и отдела, что создаст у жертвы впечатление, что она имеет дело с "правильным" человеком. Представляться партнером (или потенциальным клиентом) компании можно и нужно, а вот выдавать себя за постороннее лицо даже имея договор о пен-тестинге на руках — слишком рискованно. К тому же в последнем случае шансы на удачную атаку не увеличиваются, а уменьшаются, поскольку, выдавать себя можно только за того, кого мы очень хорошо знаем.

Получив ответ, смотрим на заголовок письма, определяя тип и версию почтового клиента, а в ряде случаев и версию операционной системы (если используется штатный почтовый клиент по умолчанию). Соответственно, кидая жертве линк на подконтрольный нам WEB-сервер, мы определяем версию и тип браузера. Какова вероятность, что жертва кликнет по ссылке? Судя по моей практике, это происходит в 8 из 10 случаев, если используется доменный уровень в зоне типа com.ru и по меньшей мере 2-3 из 10, если это narod.ru или что-то подобное. Главное — это не домен, а мотивация. Письмо с текстом типа "а вот мы тут подготовили клевую презентацию, взгляните" – навряд ли вызовет жгучий интерес. Другое дело — "я купил ваш товар, а он оказался дефектный, в магазине мне сказали, что не гарантийная ситуация, потому

что… бла-бла-бла, и посоветовали обратится непосредственно к вам. вот фото дефекта крупным планом: [link на jpg]". Конечно, текст письма предельно упрощен, но общий смысл передан верно. Если составить письмо юридически грамотно (для чего можно воспользоваться услугами юриста), да еще упомянуть реальные имена сотрудников и отделов, то с 99,9% вероятностью они щелкнут по ссылке, что бы разобраться в ситуации. Впрочем, учитывая, что по меньшей мере в 90% случаях, почтовые клиенты настроены на автоматическое отображение внешних картинок в HTML-письмах, можно ничего не мутить. Ссылка откроется и без телодвижений со стороны жертвы.

Зная же версию почтового клиента/операционной системы/браузера – смотрим: какие в ней есть дыры (для этого достаточно зайти на security focus или любой другой подобный ресурс) и заточить. А точить можно много чего! Например, excel и word, уже давно ставшие стандартом де-факто и содержащие огромное количество дыр. Впрочем, учитывая уровень компьютерной (без)грамотности большинства сотрудников, посылки исполняемого файла во вложении зачастую оказывается вполне достаточно и его открывают, особенно если найти убедительный повод, создающий у жертвы непреодолимую мотивацию служебного или неслужебного типа.

Как показывает мой опыт, наиболее легко клюют на эту удочку пользователи со средним уровнем подготовки. Совсем уж безграмотные просто не знают, что с этим вложением делать, а достаточно продвинутые прежде чем запустить exe обязательно проконсультируются с администратором или посмеются над хакером. Уровень пользователей легко определяется в ходе предварительной разведки, после чего в ударной фазе атаки остается только позвонить по телефону войсом и сказать, что вот, типа, мы послали вам rar-архив с накладными, но мы не уверены, что все правильно упаковали и нигде не накосячили. Откройте его пожалуйста и подтвердите успешность своего заражения ;-) И ведь открывают!

Рисунок 6 мыщъх (обленившийся, растолстевший и потерявший хвост напрочь)

тузы в рукаве или честные приемы нечестной игры

На момент написания этих строк, по данным компании Secunia, в IE содержится семь незалатанных дыр, в Горящем Лисе — пять, в Опере — ни одной, да только кто же ту Оперу использует! "Незалатанных" в данном случае означает: "дыр, под которые компания-разработчик еще не выпустила заплаток безопасности", из чего следует, что вся атака сводится к заманиванию пользователя на "заминированный" сайт.

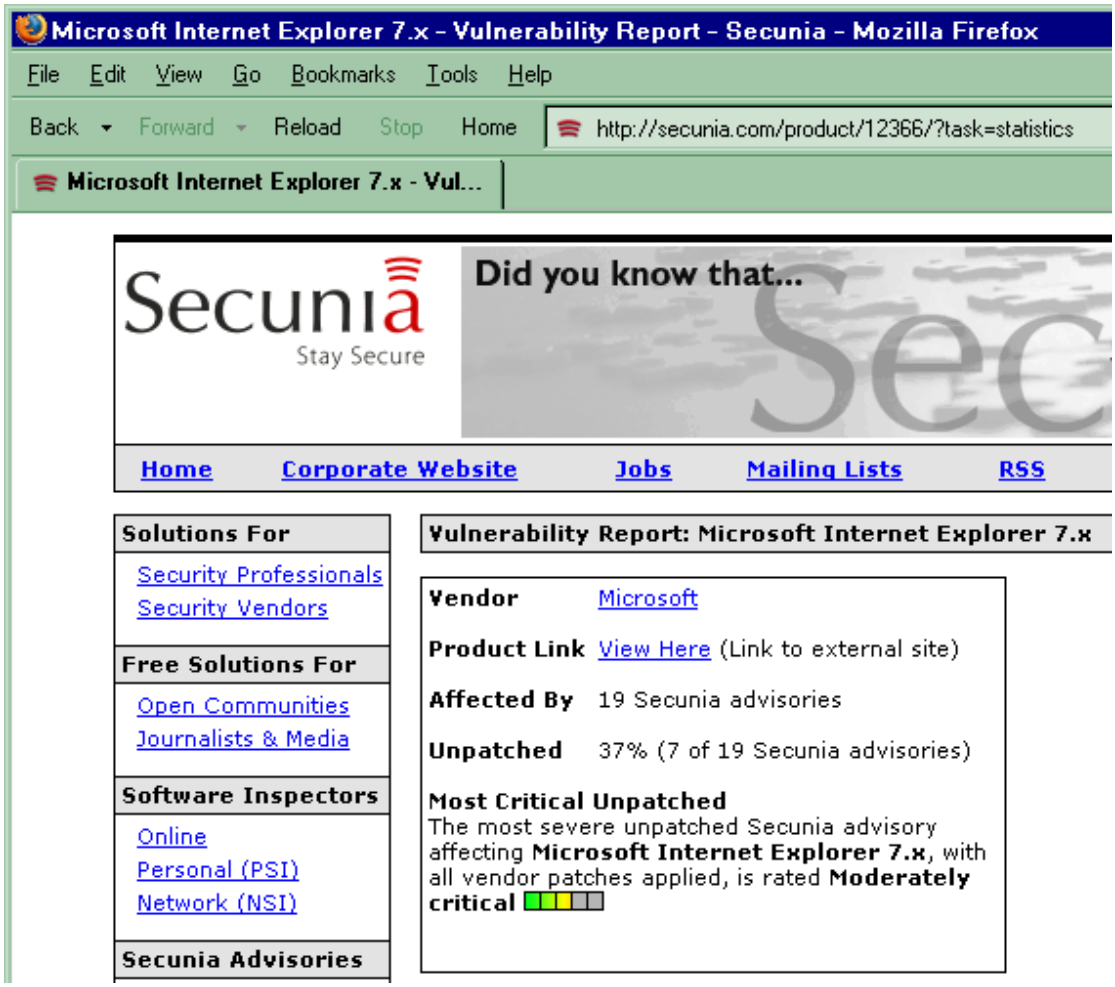

Рисунок 7 не залатанные дыры в IE

Конечно, количество незалатанных дыр не остается постоянным и в определенные моменты времени падает до нуля, существенно затрудняя атаку. Пен-тестеру остается надеяться лишь на то, что администратор забыл/поленился скачать все обновления или что целевой пользователь откроет подсунутое ему вложение.

Активность пен-тестеров хорошо коррелирует с количеством незаланных дыр, что вполне объяснимо. Действительно, зачем ломиться в закрытые дыры, если можно просто дождаться появления одной или нескольких дыр, для которых еще нет "лекарства" и тут же предложить свои услуги по проникновению. Или сначала проникнуть, а потом предложить. Это рискованно (и в ряде случаев уголовно наказуемо), но так надежнее. Как уже говорилось, переговоры с клиентом – процедура вялотекущая и пока клиент дойдет до нужной кондиции, дыру скорее всего уже успеют прикрыть или же администратор (который не лось) найдет подходящий workaround.

Вот тут меня многие спрашивают — должен ли пен-тестер вести собственные исследования на предмет поиска дыр в двоичном коде/открытых исходных текстах. Короткий ответ – пен-тестер никому ничего не должен и делает только то, что ему в кайф. Ответ подлиннее – конечно, поиск собственных дыр это хорошо. Владея дырой о которой никто не знает, можно сорвать банк и стричь корпоративных пользователей как баранов, пока источник не иссякнет (дыру не прикроют). Однако, намного более продуктивным оказываются посиделки на хакерских форумах и чтение блогов различных исследователей. Как показывает практика, средний срок реакции производителей ПО составляет один или два месяца. Это же уйма времени! Вот только, чтобы успеть прочитать блог до того, как он попадет на security focus и о нем все не узнают, нужно много читать, причем не только на английском. На английском читает толпа народу, с которыми мы вынуждены конкурировать. Знание же остальных языков (даже на уровне чтения со словарем), ставит нас все конкуренции. Кстати, производители ПО в своей массе англо-говорящие и знанием большого количества иностранных языков не обременены.

Короче, дыра — это не нора. И рыть ее не надо. Пусть роют другие, а пен-тестер снимает сливки. Когда же дыры кончаются — наступает мертвый сезон, в который работать нет никакой мазы. Зачем драть свой хвост? Достаточно просто немного подождать. Дыры появятся. Не может быть, чтобы не появились! Кстати, именно в силу этого обстоятельства, пен-тестинг не приносит стабильного дохода и дальше подработок дело не идет. Клиент тоже идет нерегулярно. То клюет косяками, то опускается на дно. Как правило, после очередной эпидемиологической вспышки, администраторы высаживаются на жуткую измену и начинают панически укреплять оборону, используя для этого все доступные средства и пен-тестинг в том числе. Но через некоторое время они успокаиваются и тогда пен-тестерам приходится прилагать большие усилия, чтобы убедить окружающих в собственной необходимости. Тут не так важны знания компьютера, как умение раскручивать клиента. То есть пен-тестер это не только (и даже не сколько!) хакер, но еще и психолог. И тут мы плавно переходим к обсуждению знаний, которыми должен обладать пен-тестер.

Рисунок 8 ежик!!!

пен-тестеры — кто они?

Бытует мнение, что пен-тестеры это высококлассные специалисты, но это не совсем так. Классные специалисты в своем большинстве чрезвычайно востребованы на рынке — их просто рвут на куски, и никто из них в здравом уме и твердой памяти не станет заниматься рабой без твердых гарантий оплаты, а пен-тестеру платят не за работу, а по факту проникновения. К тому же, быть пен-тестером много ума не надо и тут приходится конкурировать с многочисленными пионерами и голодными студентами, согласными работать в буквальном смысле за бутылку пива.

Фактически, пен-тестер это тот же киддер, осиливший ассемблер и научившийся затачивать чужие exploit'ы под нужды производственной необходимости, а в идеале — составлять свои собственные, имея на руках более или менее внятное описание дыры. Для этого достаточно знаний ассемблера и умения держать отладчик в руках. А если говорить про атаки через email, то ассемблер вообще не требуется. Узкий исследователь, специализирующий, например, на UNIX-системах, при пен-тестинге проигрывает эрудированному пионеру, проводящему все свободное (и несвободное) время за WEB-серфингом.

Конечно, это не значит, что профи не могут участвовать в пен-тестинге. Еще как могут! Но наибольшую активность в продвижении своих услуг проявляют именно пионеры, потому что для них это зачастую чуть ли не единственный способ быстрого заработка. А может ли в роли пен-тестера выступить сам администратор? Это как сказать… Разослать письма с вложениями всем сотрудникам, а затем поставить виновных по стойке смирно — нетрудно, вот только совсем не открывать никаких вложений все равно не получится. Документы для того и придумали, чтобы ими обмениваться. Кто же должен читать резюме, накладные, etc… К тому же, у администратора обычно и без того хватает проблем, чтобы поддерживать свою тушку в курсе всех новостей, касающихся безопасности. В идеале, администратор должен регулярно посещать сайты разработчиков всего используемого ПО или порталы типа Security Focus'a, чего рядовые администраторы ни хвоста не делают. Максимум — настраивают систему автоматического обновления Windows. Офис обновляют уже единицы, а про остальные программы никто и не вспоминает. Так стоит ли удивляться, что пен-тестеры плодятся как кролики?!

Рисунок 9 ежик умер!

заключение

Пен-тест это не индикатор и не лакмусовая бумажка. Успешное проникновение вовсе не признак, что администратор делает что-то не то или не так (или вообще ничего не делает, а только пьет пиво, курит сигареты и смотрит порнуху по Интернету за казенный счет). Небезопасность компьютерных сетей — фундаментальная проблема и хорошая защита это не та, которая вообще не допускает проникновения (таких защит в силу низкого качества ПО попросту нет), а та, которая позволяет "запеленговать" атакующего. Должны быть бэкапы и отлаженная схема восстановления на тот случай, если атакующий разрушит все данные до которых только успеет дотянуться. Должно быть много еще чего… И оценить степень реальной

уязвимости системы может только security-консультант, но никак не пен-тестер, полезность которого у меня вызывает бооольшие сомнения. Это я как пен-тестер говорю ;)