УДК 004

Д.Н. Колегов

Россия, Томск, НИ ТГУ

КАК СТАТЬ СПЕЦИАЛИСТОМ ПО КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Предлагается краткое содержание мотивационных лекций, проводимых для студентов первых курсов, обучающихся по специальности компьютерная безопасность в Томском государственном университете, в рамках дисциплины «Введение в специальность».

Ключевые слова: мотивация; личная эффективность; качество.

Вот уже несколько лет одной из первых лекций, читаемых первокурсникам на кафедре защиты информации и криптографии Томского государственного университета, является лекция о том, как в настоящее время стать специалистом по компьютерной безопасности.

Возможно возникает законный вопрос: зачем? Ведь разработаны подробные программы обучения, специальности аккредитованы. Неужели этого мало? Неужели это не гарантирует того, что выпускник, успешно прошедший обучение, побывавший на практике, сдавший государственный экзамен и защитивший квалификационную работу, автоматически станет специалистом по компьютерной безопасности? С нашей точки зрения, нет. И тут дело даже не в том, что ВУЗы (например, классические) часто оторваны от современных технологий и производства, не обладают преподавателями с опытом работы в практических подразделениях по компьютерной безопасности, не имеют необходимой материальной базы. Дело в том, что студентам не отвечают на два простых вопроса: “Зачем?” и “Как?”. А отвечают лишь на вопрос: “Что?”.

Зачем ему изучать конечные автоматы? Чтобы моделировать простейший светофор? А зачем ему английский? Чтобы читать топики о родном ВУЗе? Зачем изучать компьютерные сети, если большинство разработчиков часто не представляют ничего, кроме конкретного протокола, с которым они работают, или его API. А если у студента первые курсы не отбили желание стать исследователем, то как ему учиться и развиваться? Неужели достаточно только самостоятельной работы студента из наспех написанных программ по дисциплинам?

Безусловно все то, что дается в рамках специальностей по компьютерной безопасности, важно и нужно, но есть и другой более тяжелый путь, которым идут немногие студенты. Что же это за такой путь? Ничего особенного в нем нет, это всего лишь набор из нескольких пунктов, которые с нашей точки зрения очень важны и должны обязательно попасть в личный план обучения студента.

1. Личная эффективность

Предположим поставлена цель: стать специалистом по компьютерной безопасности. Для этого нужно очень много чего изучить, прочитать, попробовать на практике. И очень важно не то, что придется делать, а будет ли это делаться вообще и как будет делаться. Ввиду того, что средний человек ограничен в ресурсах и времени, возникает потребность делать это что-то эффективно. И это то, чему необходимо обучать в первую очередь. Для IT-специалистов существует очень хорошая методология Максима Дорофеева “Джедайские техники пустого инбокса”. Вот с них и следует начать.

2. Английский язык

Предположим, Вы потрясающий хакер (исследователь, багхантер), но вы не знаете язык на нужном уровне. Какие у вас возникают ограничения? Нельзя отправить заявку на CFP на Black Hat или Defcon, а если вы и сумеете написать тезисы, и их примут, то как вы будете выступать перед многонациональной аудиторией, которая, скорее всего, только мечтает выучить русский.

Точно также возникают сложности с описанием найденных вами уязвимостей, написанием научных статей, подготовкой презентаций и т.д.

Про то, что вся адекватная и современная техническая литература только на английском языке, даже говорить не стоит.

Получается, что минимально приемлемый уровень знания английского языка – это тот, что позволяет вам:

– прочитать без словаря нужную книгу (хотя бы техническую);

– просмотреть и понять любое выступление на английском;

– подготовить тезисы, статью, презентацию, описание инцидента или уязвимости;

– создать Issue на Github.com, задать или ответить на вопрос на StackOverflow, сообщить результаты ваших исследований в блоге;

– поспорить о критичности той или иной найденной вами уязвимости на HackerOne или сообщить необходимые детали команде безопасности;

– выступить самостоятельно перед англоговорящей многонациональной аудиторией на конференции с вашим выдающимся исследованием.

3. CTF

Английский язык изучен, языки программирования освоены и даже сессия, возможно, сдана на отлично. А взломать или защитить что-нибудь студент сумеет?

Вероятнее всего, нет (ну, просто по опыту общения с людьми, которые не занимаются ничем, кроме учебы). Где же тогда получить практические навыки “быстро, бесплатно и без рекламы”? Однозначно нужно пробовать сначала тренироваться, а потом играть в CTF. Почему это важно?

1. Есть возможность попробовать разные “роли”, “направления”. Ведь однозначно хороший безопасник – это не универсал, который может все, ну просто потому, что все уметь нереально и трудно, а это скорее человек с широким кругозором, разными навыками, но умеющий что-то делать особенно хорошо в определенной области.

2. Огромное количество приобретенных навыков. Только представьте, что вот вам сегодня за 8 часов необходимо разобраться в MS DOS, иначе команда проиграет, а в следующих соревнованиях научиться писать под Android. И да, может быть вы и не собираетесь быть Android-разработчиком, но может быть вы захотите стать пентестером, и тогда вам эти навыки обязательно понадобятся.

3. Очень важно быть в курсе происходящего. А CTF – это не только игры как таковые, но и невероятно большое сообщество интересных людей из других команд и организаторов. Люди – это очень важный ресурс, которые могут вам помочь новыми знаниями, навыками, информацией, стажировками и т.д.

4. В конце концов троечник, имеющий значительные результаты в CTF, более привлекателен для работодателя, чем отличник, у которого из всех 108ннтижений, это только красный диплом и ни одной пропущенной пары. А вот отличник, имеющий достижения в CTF, с широким кругозором и множеством хороших контактов из CTF-сообщества, однозначно не останется невостребованным специалистом.

4. Языки программирования

Современный специалист компьютерной безопасности должен знать несколько языков программирования. Одним из качественных наборов языков является следующий. Во-первых, один из языков типа Python или Ruby – для быстрой разработки прототипов, исследовательского программирования, реализации PoC, реализации модулей пентестерских фрэймворков (Metasploit, BeEF, Recon-ng и др.), работы с библиотеками Machine Learning. Во-вторых, язык ECMAScript (JavaScript, node.js) как основной web-язык (28 февраля 2017 года на сайте Стэнфордского университета появилось сообщение о переходе в некоторых курсах с языка Java, используемого ими с 1995 г., на язык JavaScript). В-третьих, какой-то язык со строгой типизацией (Java, C++, Go).

Минимально приемлемый уровень знания языка программирования – это тот, что позволяет вам:

– прочитать и понять код программы;

– реализовать свой собственный модуль для фрэймворка;

– найти и исправить ошибку в исходном коде;

– реализовать PoC для демонстрации наличия уязвимости;

– разработать прототип программного средства.

5. Быть в курсе происходящего

Вы знаете или учите языки программирования, активно участвуете в CTF, иногда ищите уязвимости в рамках программ Bug Bounty. Несколько часов назад Shadow Brokers опубликовали несколько zero day, а спустя 30 минут были опубликованы слайды с конференции BlackHat Russia. Как вы об этом узнаете? Через какое время вы об этом узнаете? Узнаете ли вообще?

Любой специалист должен быть в курсе последних событий, открытий, исследований, новостей в его области. Одним из эффективных средств получения этой информации является Twitter, где, подписавшись на соответствующих людей или соответствующие компании, вы сможете получать необходимую информацию.

6. Собственные исследования

Собственные исследования, как правило, начинаются на 2-3 курсе университета под названием “курсовая работа”. Очень часто ее выполняют для того, чтобы отстал научный руководитель и наконец-то поставили оценку в зачетную книжку.

Давайте перечислим, что могут дать качественные собственные исследования (речь не идет о выдающихся открытиях, номинированных на премию Алана Тьюринга):

– защита диссертации на первом или втором годе обучения в аспирантуре;

– выступления на практических и академических конференциях по компьютерной безопасности;

– зарабатывание денег путем применения результатов проведённых исследований в программах Bug Bounty;

– получение президентских и правительственных повышенных стипендий, превосходящих заработную плату многих преподавателей ВУЗов;

– признание и известность (попадание в Hall of Fame ведущих мировых компаний Google, Facebook, Microsoft, Twitter, Yandex, MailRU).

7. Bug Bounty

Участие в программах “Bug Bounty” – это уникальный фактор мотивации не только студентов, но и специалистов любого уровня. Основная идея “Bug Bounty” заключается в следующем. Заинтересованная компания публикует условия программы, направленной на поиск уязвимостей в ее информационных системах. Исследователи, которые принимают условия этой программы, ищут уязвимости, сообщают о них компании, а последняя предлагает им bounty. Это может быть денежное вознаграждение в зависимости от критичности найденной уязвимости, упоминание исследователя в своем зале славы, отправка исследователю футболки и т.п.

Участвовать в таких программах считается достаточно престижным. Многие известные исследователи являются успешными багхантерами. Более того, если ты не занимаешься собственными исследованиями, то тебе будет очень трудно конкурировать и находить интересные уязвимости.

На наш взгляд, Bug Bounty должно являться уникальным способом мотивации. Ведь фактически здесь идет речь о быстром денежном вознаграждении за проведенные практические исследования.