АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВУЗА

И. С. Макаров[1]*, Н. И. Козырева[1]

[1]Поволжский государственный университет телекоммуникаций и информатики, г. Самара, 443010, Российская Федерация

*Адрес для переписки: igor-psati@yandex.ru

Аннотация—В работе представлены результаты поиска уязвимостей информационной безопасности в результате тестирования на проникновение, проведенного в корпоративных сетях некоторых высших учебных заведений. **Предмет исследования.** Предметом исследования являются информационные ресурсы различных образовательных организаций. **Метод.** Методика и требования проведения аудиторских проверок согласно разработанному алгоритму, а также стандартам ISO27000, ISO017799, ISO15408. **Основные результаты.** Отчет по обнаруженным типичным уязвимостям характерных для вузов, а также рекомендации по их устранению. **Практическая значимость.** Результаты работы могут быть использованы для моделирования и оценки защищенности сетей и информационных систем вузов для решения задач обеспечения информационной безопасности.

Ключевые слова—информационные ресурсы вузов, тестирование на проникновение, информационная безопасность.

Информация о статье
УДК 004.056
Язык статьи – русский.
Поступила в редакцию 19.05.2021, принята к печати 20.12.2021.

Ссылка для цитирования: Макаров И. С., Козырева Н. И. Аудит информационной безопасности вуза // Информационные технологии и телекоммуникации. 2021. Том 9. № 4. С. 56–67. DOI 10.31854/2307-1303-2021-9-4-56-67.

UNIVERSITY INFORMATION SECURITY AUDIT

I. Makarov[1]*, N. Kozyreva[1]

[1]Povolzhskiy State University of Telecommunications and Informatics,
Samara, 443010, Russian Federation

*Corresponding author: igor-psati@yandex.ru

Abstract—The paper presents the results of a search for information security vulnerabilities as a result of penetration testing carried out in the corporate networks of some higher education institut. **Subject of study.** The subject of the research is the information resources of various education organizations. **Method.** Methodology and requirements for conducting audits in accordance with the developed algorithm, as well as ISO27000, ISO017799, ISO15408 standards. **Main results.** Report on the specific vulnerabilities found typical for universities, as well as recommendations for their elimination. **Practical significance.** The results of the work can be used for modeling and assessing the security of networks and information systems of universities to solve information security problems.

Keywords—information resources of universities, penetration testing, information security.

Article info
Article in Russian.
Received 19.05.2021, accepted 20.12.2021.

For citation: Makarov I., Kozyreva N.: University Information Security Audit // Telecom IT. 2021. Vol. 9. Iss. 4. pp. 56–67 (in Russian). DOI 10.31854/2307-1303-2021-9-4-56-67.

Введение

Служба ИБ практически каждого вуза регулярно сталкивается с различного вида киберугрозами. В современном мире они приобретают все большую силу и способность нанести огромный ущерб не только информационным ресурсам вуза, но и в следствии использования внешних сервисов также и информационным системам государства. Для предотвращения киберугроз специалистами по информационной безопасности разработан метод, который бы моделировал действия потенциального злоумышленника в мирных целях, т. е. использовал угрозы не для получения собственной выгоды, а для оглашения своих результатов с целью уменьшения рисков в сетевой инфраструктуре предприятия. Этот метод получил название «Тестирование на проникновение» или пентест.

Таким образом, пентест – это тестирование информационных ресурсов (ИР) на проникновение с разрешения владельца таких ресурсов. Эта процедура, в первую очередь, необходима вузу для реальной оценки состояния защищенности ИР.

Различают три вида тестирования на проникновение:

1. WhiteBox: атакующему предоставляют информацию о тестируемых компонентах информационных ресурсов компании.
2. BlackBox: информацию о тестируемых компонентах атакующему не предоставляют.
3. GreyBox: информацию об инфраструктуре компании предоставляют частично [1].

Алгоритм проведения тестирования

В ходе теста на проникновение специалист по тестированию защищенности действует как настоящий хакер: находит те уязвимости, которые легче всего использовать, эксплуатирует их и получает доступ к нужной информации. Как правило, в качестве цели выступает необходимость получить административный доступ или доступ к конкретной информации (например, данные о внебюджетной финансовой деятельности вуза, персональные данные и т. п.) [1, 2].

Ключевой особенностью тестирования на проникновение является то, что осуществляется поиск не всех имеющихся уязвимостей, а только тех, которые необходимы для достижения выбранных целей (как и в случае реального взлома), для дальнейшего осуществления так называемых целевых атак. Так как основной аспект ИБ, на который необходимо обратить в вузе это доступность, то в результате боевой эксплуатации уязвимостей на доступность, возможны негативные последствия в виде недействующих сервисов, перезагрузки серверов, как следствие – дополнительной работы у администраторов безопасности [2].

В ходе осуществления аудита ИС различных вузов был предложен типовой алгоритм проведения тестирования на проникновение, учитывающий специфику именно образовательных учреждений высшего образования, который включает в себя следующие этапы:

– получение предварительной информации о сети (в зависимости от вида проведения тестирования некоторая информация может быть получена от заказчика). Используются те же источники информации, которые доступны злоумышленникам (интернет, новости, конференции и т. д.), благодаря чему возможно построения карты ИС вуза;

– определение типов устройств, ОС, приложений по реакции на внешнее воздействие;

– поиск и идентификация уязвимостей сетевых служб и приложений;

– анализ web-ресурсов;

– эксплуатация уязвимостей;

– по согласованию может производиться проверка устойчивости внешнего периметра и открытых ресурсов на атаки типа отказа в обслуживании. Производится оценка степени устойчивости сетевых элементов и возможного ущерба при проведении наиболее вероятных сценариев подобных атак;

– анализ сетевого трафика. В случае проведения работ в сети Заказчика или при получении такой возможности в ходе эксплуатации уязвимостей проводится анализ сетевого трафика с целью получения важной информации (пароли пользователей, конфиденциальные документы и пр.);

– проверка устойчивости маршрутизации. Производится моделированием фальсификации маршрутов и проведения атаки типа отказа в обслуживании против используемых протоколов маршрутизации;

– проверка возможности получения злоумышленником несанкционированного доступа к конфиденциальной информации или информации ограниченного доступа;

– полученная в ходе анализа уязвимостей и попыток их эксплуатации информация документируется и анализируется для выработки рекомендаций по улучшению защищенности ИС [2].

Внешнее тестирование на проникновение

Моделирование действий потенциального внешнего нарушителя техническими методами представляет из себя выполнение всевозможных сценариев действий потенциального внешнего нарушителя, действующего из сети Интернет, который, используя свой опыт и имея в арсенале оборудование и ПО, находит и производит поиск и эксплуатацию уязвимостей для достижения определённых целей. Другими словами, злоумышленник проводит атаку на ресурсы компании, которые доступны из сети Интернет.

В ходе выполнения работ для выявления общедоступной информации ручной поиск файлов с применением специализированного программного обеспечения Foca. Foca представляет собой инструмент для автоматизации извлечения и анализа метаданных. Оно может вытаскивать подробную информацию о месте, где производилась фотосъёмка по сохранённым GPS данным, может извлекать данные из файлов MS Office, PDF файлов, графических файлов. Foca не взаимодействует напрямую с информационными ресурсами, производя поиск информации из открытых источников.

Указав в качестве доменного имени UUUUUU.ru программа начинает свою работу. По окончанию работы программа нашла 405 документов. После автоматического анализа Foca выявила информацию о пользователях, периферийном оборудовании программном обеспечении и т. д. (рис. 1), которая может быть использована потенциальным злоумышленником при подготовке к проведению атаки.

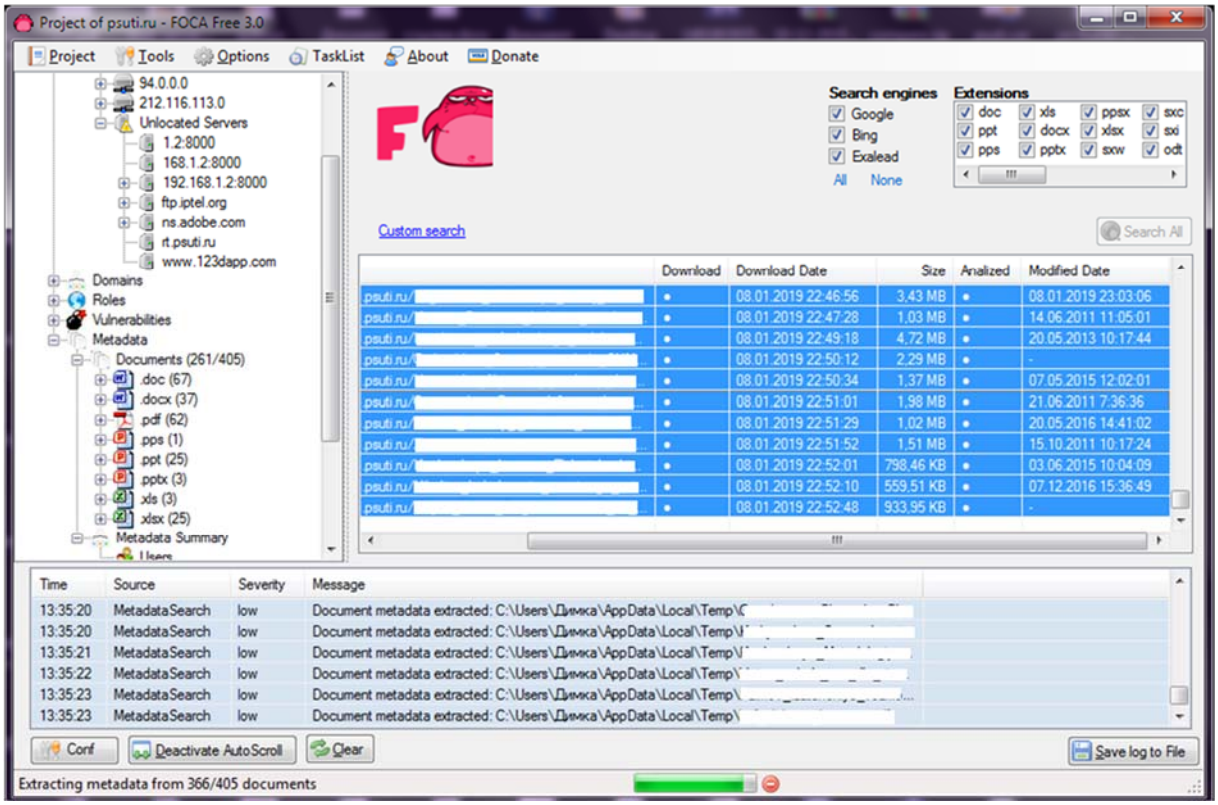

Рис. 1. Анализ полученных мета-данных

Помимо поиска и анализа мета-данных были найдены серверы, web-сайты, dns-имена.

Поиск поддоменов – неотъемлемая часть подготовки злоумышленника ко взлому. Для поиска и анализа поддоменов использовался инструмент dnsdumpster.com. После произведённого анализа информации получилась картина, представленная на рис. 2 (см. ниже).

Аналогичная процедура происходила с использованием ресурса pen-test-tools.com. Информация, полученная с использованием pentest-tools, представлена в таблице (см. ниже).

Для дальнейшего пассивного анализа системы использовалась система Shodan. Система Shodan опрашивает порты подсоединенных к сети машин и собирает выдаваемые в ответ баннеры, после чего индексирует эти баннеры на предмет последующего быстрого отыскания соответствующих устройств [3, 4]. В итоге такой обработки, вместо того, чтобы предоставлять специфический контент страниц, содержащих конкретное поисковое слово запроса, Shodan помогает отыскивать специфические узлы сети: настольные системы, серверы, маршрутизаторы, коммутаторы, веб-камеры, принтеры и т. д. (рис. 3, см. ниже).

Таблица

Полученная информация о системе

Субдомен	IP-адрес	ОС	Сервер	CMS	PageTitle
sip.UUUUUU.ru	52.112.192.75	–	RTC 7.0	–	–
ns1.UUUUUU.ru	94.25.37.18	–	–	–	–
autodiscover.UUUUUU.ru	94.25.37.24	Win	Microsoft-IIS 8.5	–	OutlookWebApp
mail.UUUUUU.ru	94.25.37.24	Win	Microsoft-IIS 8.5	–	OutlookWebApp
linux.UUUUUU.ru	94.25.37.27	–	nginx	WordPress 3.2.1	Linux-центр
tv.UUUUUU.ru	94.25.37.27	–	Apache	–	Цифровое телевидение
stud.UUUUUU.ru	94.25.37.27	–	–	–	–
veteran.UUUUUU.ru	94.25.37.27	–	nginx	–	–
radio.UUUUUU.ru	94.25.37.27	–	nginx	WordPress 3.4.1	Коллективная любительская радиостанция RC4HAA |
smc.UUUUUU.ru	94.25.37.27	–	nginx	WordPress	–
forum.UUUUUU.ru	94.25.37.27	–	nginx	–	–
vm.UUUUUU.ru	94.25.37.27	–	nginx	–	–
sso.UUUUUU.ru	94.25.37.27	–	nginx	–	–
dev.UUUUUU.ru	94.25.37.29	–	–	–	–
UUUUUU.ru	94.25.37.31	–	nginx	Drupal 7	Университет
conf.UUUUUU.ru	94.25.37.31	–	nginx	–	Конференции университета – Главная
i.UUUUUU.ru	94.25.37.31	–	nginx	Drupal 6.26	403 Forbidden
autoconfig.UUUUUU.ru	94.25.37.31	–	nginx	–	403 Forbidden
portal.UUUUUU.ru	94.25.37.31	–	nginx	–	Login
www.UUUUUU.ru	94.25.37.31	–	nginx	Drupal 7	Университет
old.UUUUUU.ru	94.25.37.31	–	nginx	–	Университет / Главная
test.UUUUUU.ru	94.25.37.31	–	nginx	–	Вход – SunRav WEB Class
phone.UUUUUU.ru	94.25.37.31	–	nginx	–	Университет – Телефонный справочник
ns3.UUUUUU.ru	94.25.37.37	–	–	–	–
git.UUUUUU.ru	94.25.37.41	–	nginx	–	SigninGitLab
vpn.UUUUUU.ru	94.25.37.45	–	–	–	–
mx.UUUUUU.ru	94.25.37.136	–	–	–	–
ns2.UUUUUU.ru	94.25.67.97	–	–	–	–

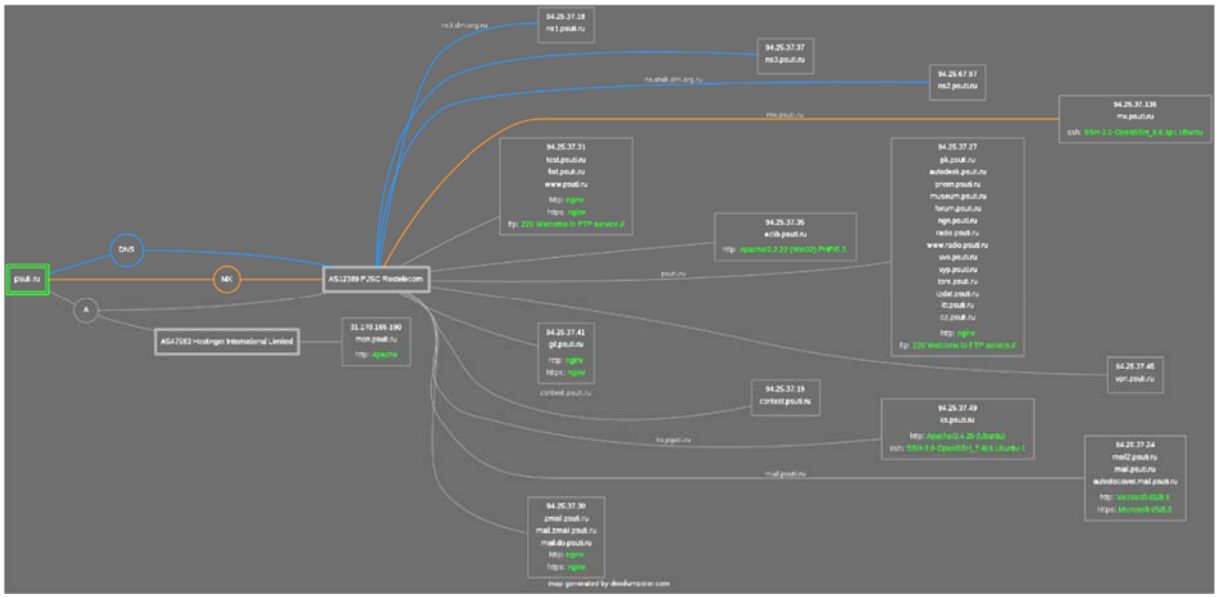

Рис. 2. Информация, полученная с помощью dnsdumpers

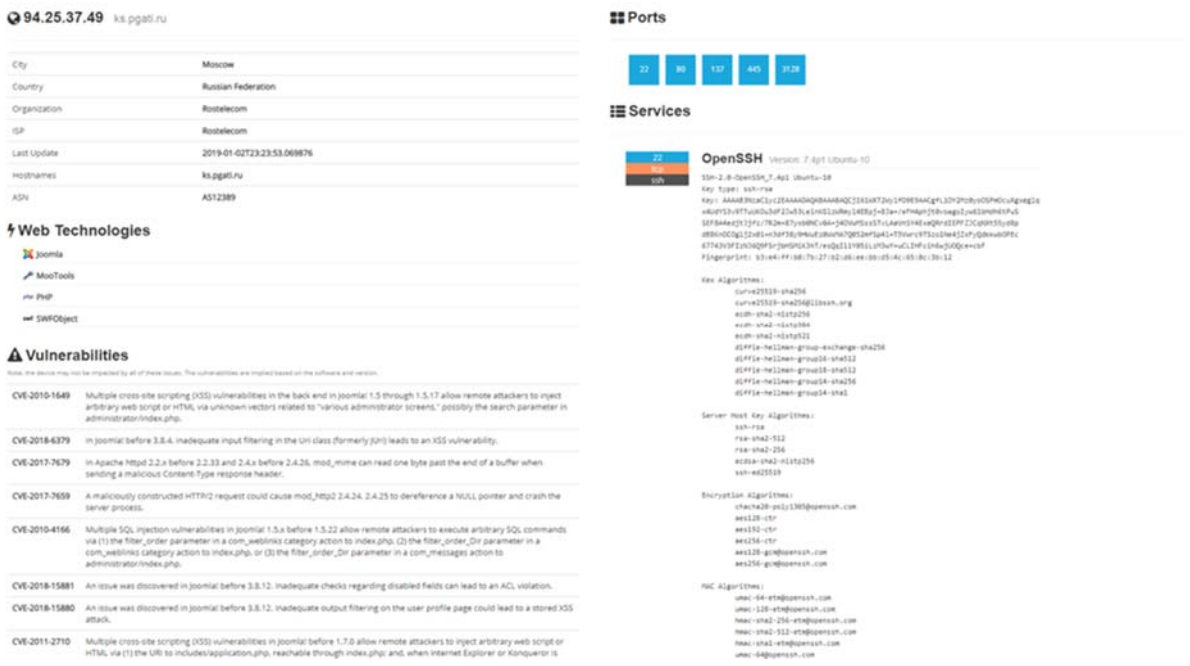

Рис. 3. Результат поиска в Shodan ресурса 94.25.37.49

Схожий функционал с Shodan имеет ситема Censys. Данная система ищет устройства, подключенные к сети Интернет и собирает данные, используя ZMap и ZGrab (сканер прикладного уровня, который работает с помощью ZMap), и сканирует адресное пространство IP [3, 4] (рис. 4).

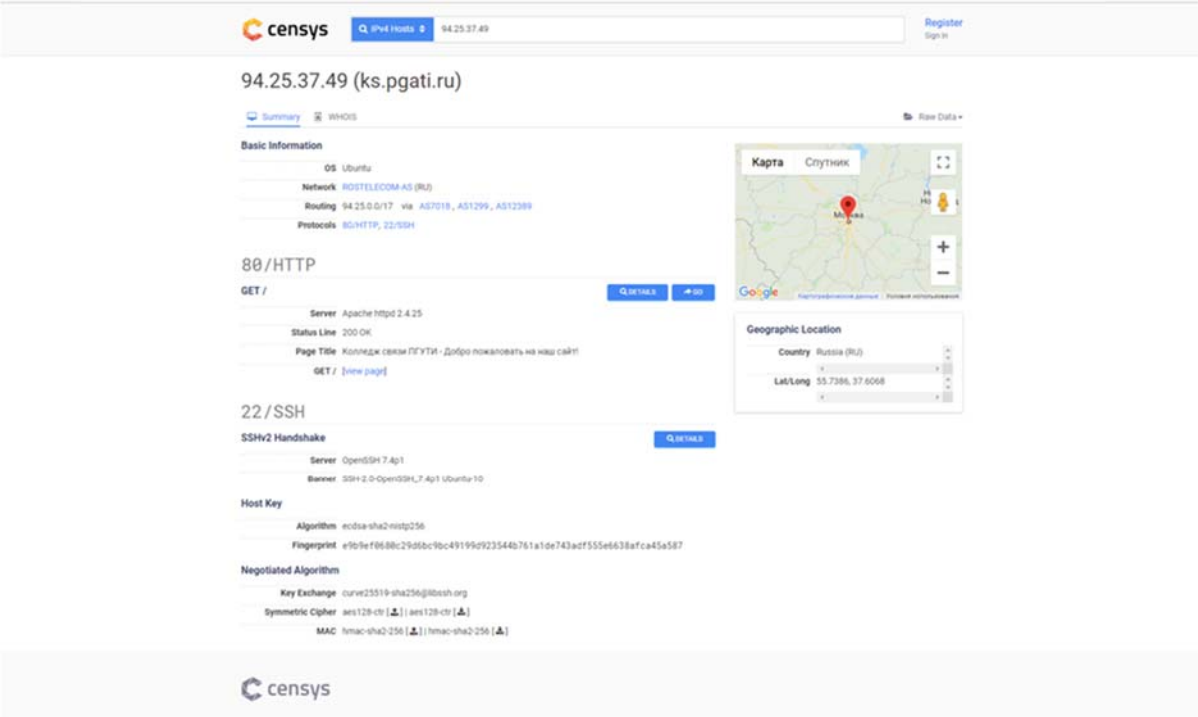

Рис. 4. Результат поиска в Censys ресурса 94.25.37.49

Взаимодействие с атакуемой системой

После проведения пассивного анализа ИР потенциальный злоумышленник может начать производить взаимодействие с ИР. В этом случае его могут зафиксировать системы обнаружения вторжений, в журнале логов сервера, WAF, и, в случае установки SIEM вся информация будет представлена в удобном для человека виде внутри SIEM-системы. В качестве поиска уязвимостей, помимо практического опыта, был использован сканер уязвимостей OpenVAS [5].

Главный сайт Университета работает на CMS Drupal. В ходе работы было установлено, что в учетной записи (УЗ) для входа в портал университета http://www.UUUUUU.ru используется стандартное имя пользователя “admin”, на что указывает успешное выполнение операции «Забыли пароль», о чём указывает информация, что дальнейшие инструкции отправлены на адрес электронной почты. Знание данной особенности даёт право потенциальному злоумышленнику на применение атаки «bruteforce» или перебор паролей по словарю.

Проанализировав интернет-ресурс было обнаружено, что студенты (и не только) могут подключиться к электронным ресурсам университета, используя номер зачётной книжки и пароль, который находится у каждого студента на титульном листе зачётной книжки. Для этого необходимо добавить сертификат и создать VPN-подключение. В качестве УЗ использовать номер зачётной книжки и пароль.

Обнаружен ресурс phone.UUUUUU.ru с подробной информацией о всех сотрудниках университета, включая ФИО, телефон, e-mail, корпус, кабинет, отдел, должность. Также, некоторые пользователи, предположительно сотрудники, оставляют личные адреса электронной почты. Эта информация может быть ис-

пользована потенциальным злоумышленником для составления списка фишинговой рассылки, фундаментом для получения информации о сотруднике из открытых источников. Помимо этого, потенциальный злоумышленник может произвести атаку типа «bruteforce» или перебор по словарю, с целью получения доступа к электронной почте сотрудника.

При анализе сайта колледжа Университета был использован сканер директорий, с помощью которого были найдены файлы .htaccess и .htpasswd.

Проанализировав доступные директории был обнаружен файл, хранящий в себе информацию о лицензионных ключах (рис. 5).

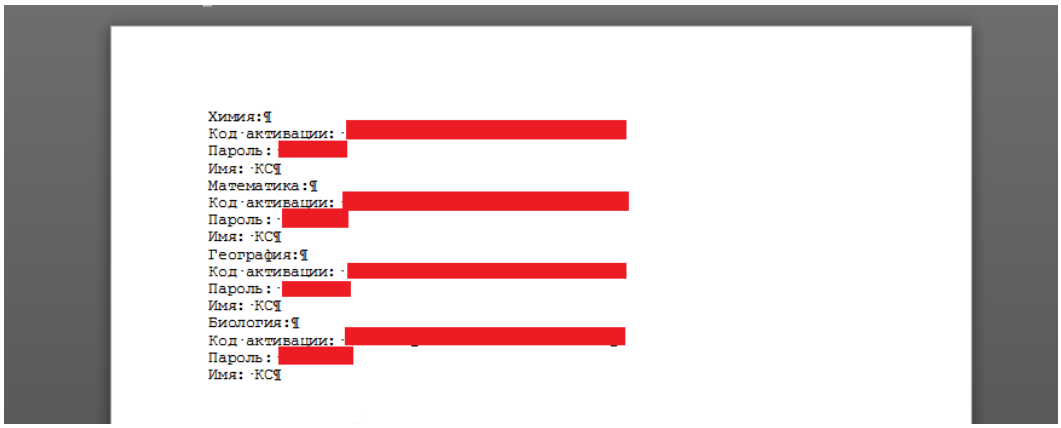

Рис. 5. Коды активации продуктов

Сайт «Конференции Университета» позволяет пройти самостоятельную регистрацию. После ввода информации об авторах, открывается окно с выбором загрузки логотипа и информационного письма. После анализа этих функций удалось выяснить, что можно произвести загрузку файла любого формата без фильтрации, т. е. любой загруженный файл попадает на сервер. Зная эту информацию, потенциальный злоумышленник может заполнить всю доступную свободную память «мусором», что сделает недоступным работу веб-ресурсов, находящихся на этом сервере. Помимо этого, потенциальный злоумышленник может произвести загрузку вируса на сервер, что вызовет заражение сервера и, возможно, заражение ПК в локальной сети университета. Еще один вектор атаки заключается в загрузке php-shell (рис. 6, см. ниже) и получения контроля над сервером, что даст потенциальному злоумышленнику возможность получить доступ ко внутренней ЛВС университета, не находясь при этом во внутреннем периметре [6].

После загрузки php-shell на сервер и его последующего запуска открываются возможности по управлению этим сервером. Дальнейшее развитие атаки подразумевает поиск ключевой информации о сервере, находящихся на нём файлов и директорий, поиск других хостов, доступность узлов ЛВС.

Поскольку на сайте электронной библиотеки Университета отсутствует система управления сайтом, то существует возможность раскрыть максимально чувствительную информацию о сервере (рис. 7, см. ниже).

Кроме того, веб-сайт позволяет раскрыть чувствительную информацию обо всех веб-ресурсах на сервере.

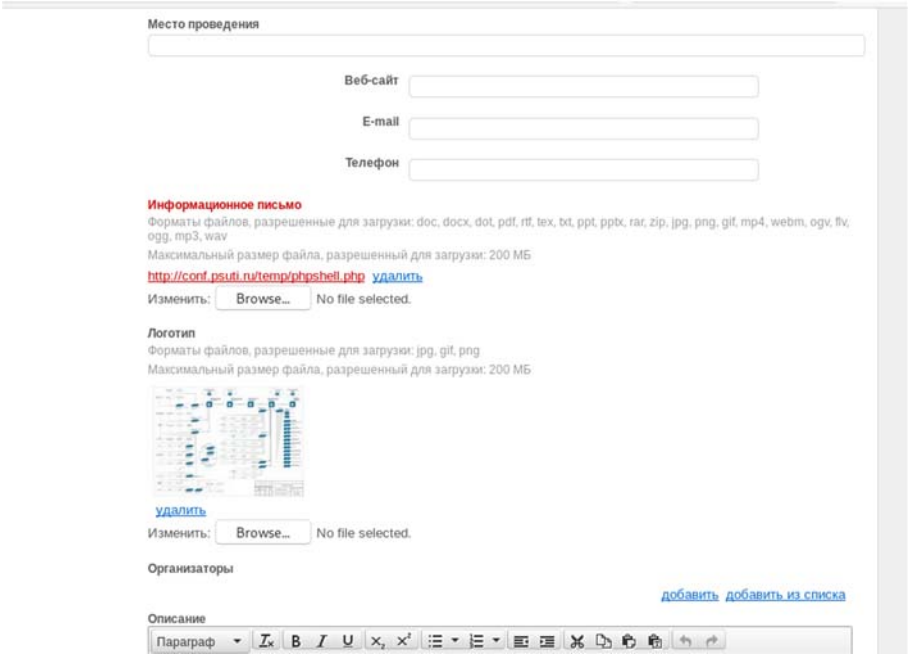

Рис. 6. Загрузка php-shell на сервер сайта conf.univer.ru

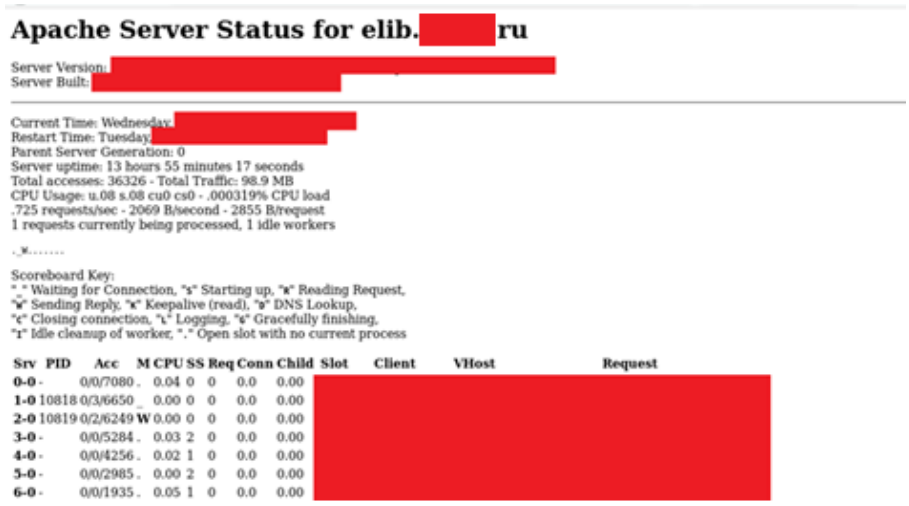

Рис. 7. Раскрытие информации о сервере

Выводы

Для обеспечения ИБ информационных систем вузов необходимо применять комплексный подход, сочетающий в себе меры различных уровней ИБ, что не всего достижимо из-за скромного финансирования и возможно недостаточной озабоченности высшего руководства вуза данной проблемой. В идеальном случае при использовании отечественных сертифицированных средств защиты информации от внутренних и внешних атак в совокупности с интеграцией механизмов безопасности в жизненный цикл информационных систем актуальность данного исследования была бы ниже, однако, к сожалению, такие идеальные варианты в результате проведенной работы не встречались (возможно, в некоторых вузах вопросам ИБ уделяется самое пристальное внимание).

Информация, собранная в результате применения разработанного алгоритма осуществления аудита ИС вузов на основе проведения тестирования на проникновение является пищей для размышления для руководителей служб ИБ вузов и показала, что потенциальный злоумышленник потенциально может завладеть сведениями о следующих уязвимостях:

- имена пользователей во внутренней системе;
- некоторое ПО, используемое во внутренних ИР;
- адреса электронной почты сотрудников;
- некоторые аппаратные сетевые компоненты;
- информация о используемых cms, ПО на веб-серверах;
- данные сотрудников, работающих в университете;
- некоторые уязвимости на ресурсах.

После активного взаимодействия с ИР вузов на внешнем периметре в некоторых случаях удавалось выяснить следующую информацию:

- использование в качестве серверных ПО ОС, которые давно не поддерживаются производителем и имеющие в открытом информацию об уязвимостях. Так же не исключен тот факт, что появятся новые и, к сожалению, производитель не сможет произвести патч для закрытия уязвимости;
- использование в cms старых версий, которые имеют множество уязвимостей, в том числе немало уязвимостей критичного уровня;
- использование слабых алгоритмов шифрования при работе протокола ssh;
- возможность использовать анонимный вход на ftp-сервер;
- использование sslv2;
- уязвимость POODLE;
- уязвимость в cms, позволяющая раскрыть LDAP информацию;
- использование старой версии сервера IIS;
- существует возможность получить контроль над сервером, не проходя никакой процедуры аутентификации;
- множество сайтов, которые раскрывают информацию о директориях;
- получение информации о чувствительных данных сервера без использования каких-либо инструментов.

Заключение

В первую очередь из любого тестирования на проникновение необходимо сделать вывод и, как минимум, принять к сведению полученную информацию и оперативно устранить найденные уязвимости и векторы атак на ИР, или, хотя бы знать слабые места в системе. После ознакомления с результатами тестирования необходимо произвести меры по устранению уязвимостей в ИР предприятия, при этом, используя, минимальные материальные ресурсы. Не стоит забывать о целесообразности применения нового архитектурного решения для предприятия, когда стоимость решения во много раз превышает стоимость хранимой информации и ресурсов в предприятии. При этом необходимо помнить о том, что информационная безопасность не строится лишь на одних архитектурных решениях. В первую очередь ИБ занимается человек. В это понятие входит не только администратор, который производит установку оборудования и ПО,

конфигурирует и настраивает сетевое оборудование, устраняет неполадки и оказывает техническую поддержку, а также каждый сотрудник организации. Так как на сегодняшний день практически каждый сотрудник, в той или иной мере, работает с сетью, использует критические ИР предприятия, имеет УЗ в ЛВС. Зачастую именно это звено оказывается наименее защищено во всей схеме ИР предприятия. Как следствие можно сделать заключение о том, что в первую очередь нужно повышать уровень ИБ среди всех сотрудников, которые так или иначе взаимодействуют или могут произвести взаимодействие с ИР компании. Данные мероприятия в дальнейшем будут способствовать сдерживанию попаданий на ИР организации со стороны злоумышленника и дальнейшей их компрометации.

Литература

1. Бондарев В. В. Анализ защищенности и мониторинг компьютерных сетей. Методы и средства : учебное пособие. Москва: МГТУ им. Н. Э. Баумана, 2017. 228 с.
2. Скабцов Н. Аудит безопасности информационных систем. СПб.: Питер, 2018. 272 с.: ил.
3. McPhee M. Mastering Kali Linux for Web Penetration Testing. Packt Publishing, 2017. 542 p.
4. Парасрам Ш., Замм А., Хериянто Т. KaliLinux. Тестирование на проникновение и безопасность. Прогресс книга, 2020. 448 с.
5. Губарева О. Ю., Жесткова А. А. Сканеры безопасности как инструменты «Пентеста» // Современные средства связи: сборник трудов XX Международной научно-технической конференции. Минск, 2015. С. 218–219.
6. Шелухин О. И., Сакалема Д. Ж., Филинова А. С. Обнаружение вторжений в компьютерные сети (сетевые аномалии): учеб. пособие. М.: Горячая линия – Телеком, 2013. 221 с.: ил.

References

1. Bondarev V. V. Analiz zashchishchennosti i monitoring komp'yuternyh setej. Metody i sredstva : uchebnoe posobie. Moskva: MGTU im. N. E. Baumana, 2017. 228 s.
2. Skabcov N. Audit bezopasnosti informacionnyh sistem. SPb.: Piter, 2018. 272 s.: il.
3. McPhee M. Mastering Kali Linux for Web Penetration Testing. Packt Publishing, 2017. 542 p.
4. Parasram S. H., Zamm A., Heriyanto T. KaliLinux. Testirovanie na proniknovenie i bezopasnost'. Progress kniga, 2020. 448 s.
5. Gubareva O. Yu., ZHestkova A. A. Skanery bezopasnosti kak instrumenty «Pentesta» // Sovremennye sredstva svyazi: sbornik trudov HKH Mezhdunarodnoj nauchno-tekhnicheskoj konferencii. Minsk, 2015. S. 218–219.
6. Sheluhin O. I., Sakalema D. Zh., Filinova A. S. Obnaruzhenie vtorzhenij v komp'yuternye seti (setevye anomalii): ucheb. posobie. M.: Goryachaya liniya – Telekom, 2013. 221 s.: il.

Макаров Игорь Сергеевич
кандидат технических наук, доцент кафедры Поволжского государственного университета телекоммуникаций и информатики,
igor-psati@yandex.ru

Makarov Igor S.
Candidate of Engineering Sciences, Associate Professor, Povolzhskiy State University of Telecommunications and Informatics,
igor-psati@yandex.ru

Козырева Надежда Ивановна
кандидат технических наук, доцент кафедры Поволжского государственного университета телекоммуникаций и информатики,
naivkozyreva@gmail.com

Kozyreva Nadezhda I.
Candidate of Engineering Sciences, Associate Professor, Povolzhskiy State University of Telecommunications and Informatics,
naivkozyreva@gmail.com