УДК 004.492.2 Вестник УрФО № 1(43) / 2022, с. 90–96

Лебедев Д.В., Гузенкова Е.А.

DOI: 10.14529/secur220111

МЕТОД ОЦЕНКИ ЭФФЕКТИВНОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ СЕТИ СИСТЕМОЙ ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ ПОСРЕДСТВОМ ПРОВЕДЕНИЯ АТАК НА УЯЗВИМУЮ СИСТЕМУ

В статье показан метод оценки эффективности использования систем предотвращения вторжений на примере комплекса для защиты сети «Континент 4». Система предотвращения вторжений представляет собой средство компьютерной и сетевой безопасности, обнаруживающее вторжения или нарушения безопасности с автоматической защитой от них.

Данный метод основывается на моделировании атак на уязвимую систему и включает в себя исследование информационной системы на наличие уязвимостей. Уязвимость представляет собой недостаток в системе, которая может использоваться для реализации угроз безопасности.

В результате данной работы был получен вывод о том, что системы предотвращения вторжений на примере комплекса «Континент 4» позволяют заблокировать многие атаки. Показанный метод позволяет определить эффективность использования систем предотвращения вторжений, а также определить объекты, требующие дополнительных мер по защите.

Ключевые слова: *информационная безопасность, программно-аппаратная защита информации, система предотвращения вторжений, система обнаружения вторжений, уязвимость, атака.*

Lebedev D.V., Guzenkova E.A.

METHOD FOR EVALUATING THE EFFECTIVENESS OF ENSURING THE SECURITY OF A COMPUTER NETWORK BY AN INTRUSION PREVENTION SYSTEM THROUGH ATTACKS ON A VULNERABLE SYSTEM

The article shows a method for evaluating the effectiveness of using intrusion prevention systems on the example of a complex for protecting the network «Continent 4». An intrusion prevention system is a computer and network security tool that detects intrusions or security breaches with automatic protection against them.

This method is based on modeling attacks on a vulnerable system and includes the study of the information system for vulnerabilities. A vulnerability is a flaw in a system that can be used to implement security threats.

As a result of this work, it was concluded that intrusion prevention systems, using the example of the complex «Continent 4», make it possible to block many attacks. The method shown makes it possible to determine the effec-

tiveness of the use of intrusion prevention systems, as well as to identify objects that require additional protection measures.

Keywords: *information security, hardware and software protection of information, intrusion prevention system, intrusion detection system, vulnerability, attack.*

Уязвимые системы являются частой проблемой, и своевременное их обновление помогает закрыть часть уязвимостей. Но существуют такие организации, которые используют неподдерживаемые устаревшие операционные системы, так как процесс обновления является невозможным или трудозатратным. Использование таких информационных ресурсов подвергает компании серьезному риску, поскольку злоумышленники могут взломать системы с помощью уязвимостей.

Для таких случаев одним из методов защиты являются системы предотвращения вторжений. Система предотвращения вторжений (IPS – Intrusion Prevention System) представляет собой средство компьютерной и сетевой безопасности, обнаруживающее вторжения или нарушения безопасности с автоматической защитой от них.

Системы предотвращения вторжений появились в результате развития нескольких независимых решений: межсетевых экранов (анализ сетевых пакетов) и систем обнаружения вторжений (анализ программ и файлов).

IPS, как правило, используют в составе межсетевого экрана следующего поколения (Next Generation Firewall).

Для проведения тестирования эффективности системы предотвращения вторжений был развернут тестовый стенд в виртуальной среде VMware, состоящий из следующих виртуальных машин:

1) Атакующий компьютер с операционной системой Kali Linux. Данная система представляет собой специально созданный дистрибутив с большим количеством программ для тестирования на проникновение.

2) Атакуемый компьютер Metasploitable 2 с умышленно уязвимой операционной системой Linux Ubuntu. Metasploitable представляет собой виртуальную машину, предназначенную для тестирования инструментов безопасности и демонстрации общих уязвимостей.

3) Система предотвращения вторжений в составе многофункционального межсетевого экрана «Континент 4».

«Континент 4» является решением класса NGFW и объединяет в себе функции межсетевого экрана, системы обнаружения и предотвращения вторжений, защиту от вредоносных веб-сайтов, виртуальной частной сети, поведенческого анализа и другие. [2]

На рисунке 1 показана схема виртуального стенда.

Для оценки эффективности системы предотвращения вторжений будет использоваться следующая последовательность действий: [1]

Рис.1. Схема виртуального стенда

1) Сканирование уязвимой защищаемой системы сканером nmap.

Nmap представляет собой утилиту для сканирования IP-сетей с целью определения открытых портов, версий программного обеспечения, операционных систем. В результате сканирования формируется список открытых портов и соответствующих им служб.

2) Сканирование уязвимой защищаемой системы сканером уязвимостей Nessus.

Nessus – программа для автоматического сканирования операционных систем с целью определения известных уязвимостей. В результате – формируется ранжированный список уязвимостей.

3) На основании сканирования системы формируется список доступных эксплойтов и атак в Metasploit (платформа для создания, тестирования и использования эксплойтов). Далее реализуются возможные атаки.

Атаки проводятся в условиях, где на атакующей машине Kali Linux указан маршрут до уязвимой системы и на межсетевом экране «Континент 4» разрешено прохождение всех сетевых пакетов. При этом активирован компонент системы предотвращения вторжений.

На рисунке 2 показано сравнение результатов сканирования сканером nmap без системы предотвращения вторжений и с активированным компонентом системы предотвращения вторжений.

На рисунке 3 показано сравнение результатов сканирования сканером Nessus без системы предот-

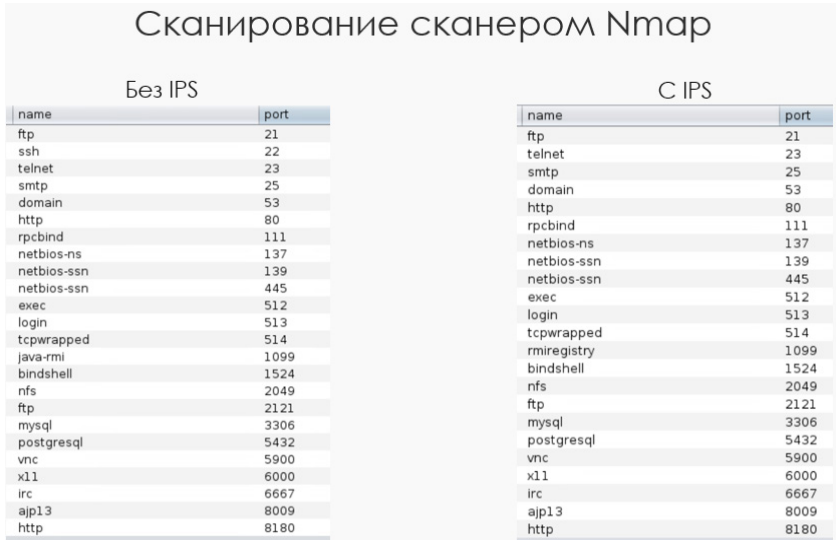


Рис. 2. Результаты сравнения сканирования сканером nmap

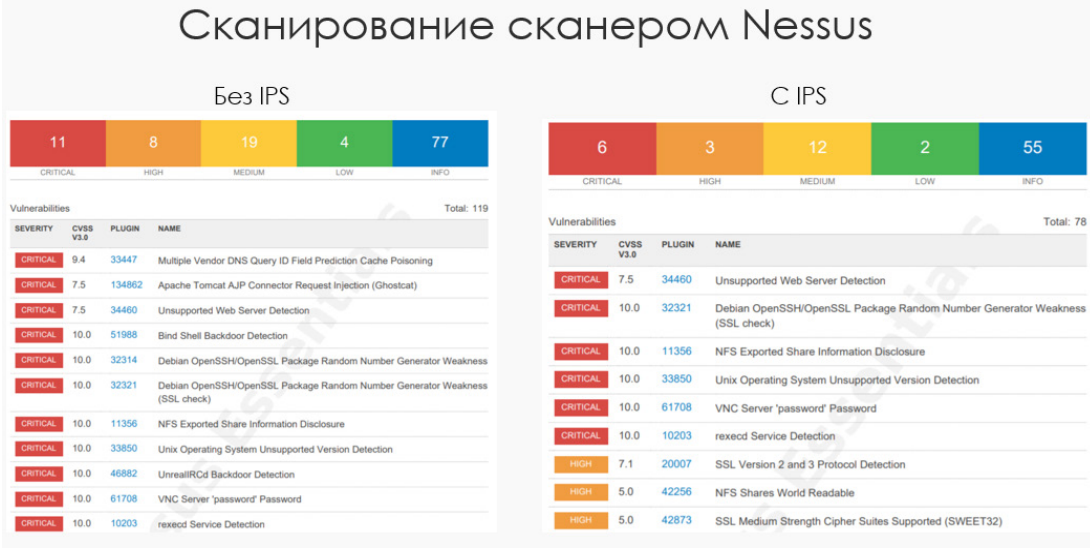


Рис. 3. Результат сравнения сканирования сканером Nessus

вращения вторжений и с активированным компонентом системы предотвращения вторжений.

При сканировании защищаемого ресурса сканерами nmap и Nessus система предотвращения вторжений сигнализировала об этом. Данные записи в журнале событий дают администратору возможность понять, что защищаемые ресурсы подвергаются сканированию, и предпринять необходимые действия для ликвидации и минимизации последствий.

Атаки на уязвимую систему осуществлялись согласно обнаруженным открытым портам, уязвимостям и сервисам в соответствии с рисунками 2 и 3. Далее описаны некоторые из проведенных атак

1) Атака на 21 порт.

2) 21 порт использует службу ftp. В Metasploitable 2 на данном порту работает ftp-сервер vsftpd.

Используя модуль сканирования в Metasploit, была проверена возможность анонимного доступа к ftp-серверу. Также был использован методом грубой силы для подбора логина и пароля (брутфорс-атака). Использование данных модулей показано на рисунке 4.

В результате было обнаружено, что на ftp-сервер возможен анонимный вход, а также подобраны пары логин/пароль.

Система предотвращения вторжений обнаружила брутфорс-атаку (рисунок 5).

Сканерами nmap и Nessus была определена используемая версию сервера. Для версии vsftpd 2.3.4 существует эксплойт, который позволяет злоумышленнику выполнить произвольный код на уязвимой системе. На рисунке 6 показан результат эксплуатации уязвимости. В результате система предотвраще-

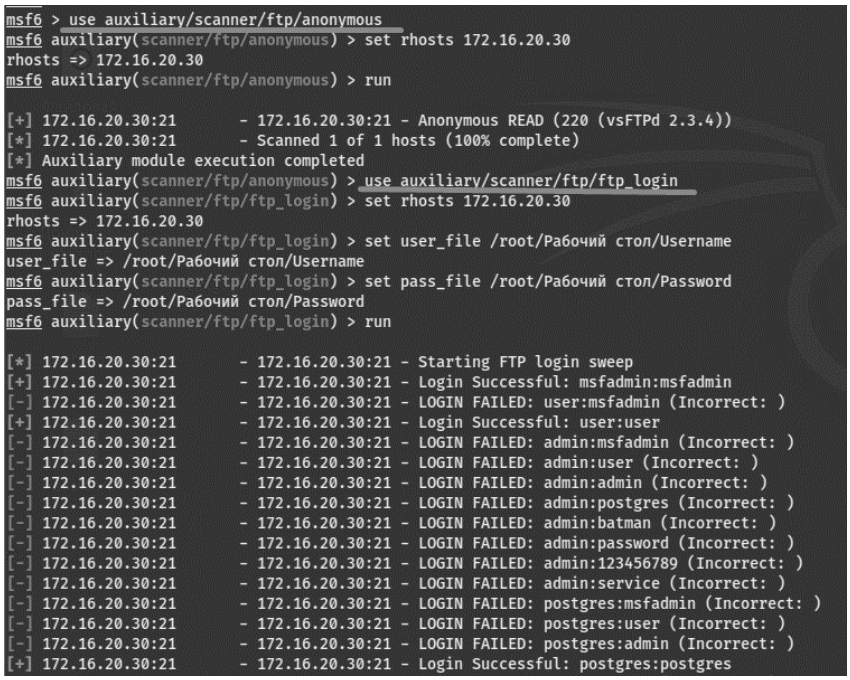


Рис.4. Результат сканирования FTP-сервера для подбора аутентификационных данных

Дата	Действие	Узел безопасности (интерф	Компонент	Адрес отправителя	Адрес получателя	Протокол / Сервис	Сигнатура / Правило (срабатываний)
15.07.2021 18:27:40.901	Блокировать	node-12345	СОВ	172.16.20.30	10.10.1.240	TCP	Potential FTP Brute-Force attempt response
15.07.2021 18:27:28.094	Блокировать	node-12345	СОВ	172.16.20.30	10.10.1.240	TCP	Potential FTP Brute-Force attempt response
15.07.2021 18:27:15.447	Блокировать	node-12345	СОВ	172.16.20.30	10.10.1.240	TCP	Potential FTP Brute-Force attempt response

Рис. 5. Обнаруженная брутфорс-атака на FTP-сервер

Рис. 6. Попытка эксплуатации уязвимости в сервере vsftpd

Дата	Действие	Узел безопасности (интерф	Компонент	Адрес отправителя	Адрес получателя	Протокол / Сервис	Сигнатура / Правило (срабатываний)
15.07.2021 18:37:56.546	Блокировать	node-12345	СОВ	172.16.20.30	10.10.1.240	TCP	id check returned root
15.07.2021 18:34:21.770	Блокировать	node-12345	СОВ	172.16.20.30	10.10.1.240	TCP	id check returned root

Рис. 7. Обнаруженная атака на FTP-сервер

ния вторжений обнаружила и заблокировала данную атаку (рисунок 7).

2) Атака на 80 порт

80 порт – порт протокола HTTP. Веб-страница Metasploitable работает на языке PHP в режиме CGI [3]. Режиме CGI описывает каким образом веб-сервер должен запускать прикладное программное обеспечение. Некоторые версии PHP в режиме CGI являются уязвимыми к эксплойту, который внедряет специальные аргументы, позволяющие предоставить доступ к системе. На рисунке 8 показано, что данный эксплойт не сработал, о чем свидетельствует запись в журнале событий в комплексе «Континент» (рисунок 9).

3) Атака на 8180 порт

Порт 8180 является альтернативным портом HTTP. В Metasploitable 2 на данном порту работает сервис Apache Tomcat. Для данного сервиса существует эксплойт, который загружает на сервер полезную нагрузку.

Атака, проведенная на уязвимый сервис (рису-

```
msf6 > use exploit/multi/http/php_cgi_arg_injection
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > set rhosts 172.16.20.30
rhosts => 172.16.20.30
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 10.10.1.240:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/php_cgi_arg_injection) >
```

Рис. 8. Атака, заблокированная системой предотвращения вторжений

Дата	Действие	Узел безопасности (интерф	Компонент	Адрес отправителя	Адрес получателя	Протокол / Сервис	Сигнатура / Правило (срабатываний)
16.07.2021 07:16:20.385	Блокировать	node-12345	СОВ	10.10.1.240	172.16.20.30	TCP	PHP //Input in HTTP POST
16.07.2021 07:16:20.384	Блокировать	node-12345	СОВ	10.10.1.240	172.16.20.30	TCP	disable_functions PHP config option in uri
16.07.2021 07:16:20.384	Блокировать	node-12345	СОВ	10.10.1.240	172.16.20.30	TCP	open_basedir PHP config option in uri
16.07.2021 07:16:20.384	Блокировать	node-12345	СОВ	10.10.1.240	172.16.20.30	TCP	auto_prepend_file PHP config option in uri
16.07.2021 07:16:20.384	Блокировать	node-12345	СОВ	10.10.1.240	172.16.20.30	TCP	safe_mode PHP config option in uri
16.07.2021 07:16:20.383	Блокировать	node-12345	СОВ	10.10.1.240	172.16.20.30	TCP	allow_url_include PHP config option in uri
16.07.2021 07:16:20.382	Блокировать	node-12345	СОВ	10.10.1.240	172.16.20.30	TCP	PHP tags in HTTP POST

Рис. 9. Заблокированная атака на PHP

```
msf6 > use exploit/multi/http/tomcat_mgr_upload
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > set rhosts 172.16.20.30
rhosts => 172.16.20.30
msf6 exploit(multi/http/tomcat_mgr_upload) > set rport 8180
rport => 8180
msf6 exploit(multi/http/tomcat_mgr_upload) > set httpusername tomcat
httpusername => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set httppassword tomcat
httppassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 10.10.1.240:4444
[*] Retrieving session ID and CSRF token...
[-] Exploit aborted due to failure: unknown: Unable to access the Tomcat Manager
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/tomcat_mgr_upload) >
```

Рис. 10. Эксплуатация уязвимости для сервиса Apache Tomcat

Дата	Действие	Узел безопасности (интерф	Компонент	Адрес отправителя	Адрес получателя	Протокол / Сервис	Сигнатура / Правило (срабатываний)
16.07.2021 08:04:08.855	Блокировать	node-12345	СОВ	10.10.1.240	172.16.20.30	TCP	Incoming Basic Auth Base64 HTTP Password detected unencrypted
16.07.2021 08:04:08.854	Блокировать	node-12345	СОВ	10.10.1.240	172.16.20.30	TCP	Outgoing Basic Auth Base64 HTTP Password detected unencrypted

Рис. 11. Заблокированная атака на Apache Tomcat

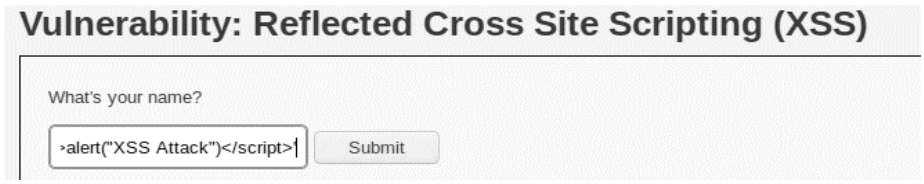


Рис. 12. Реализация XSS-атаки

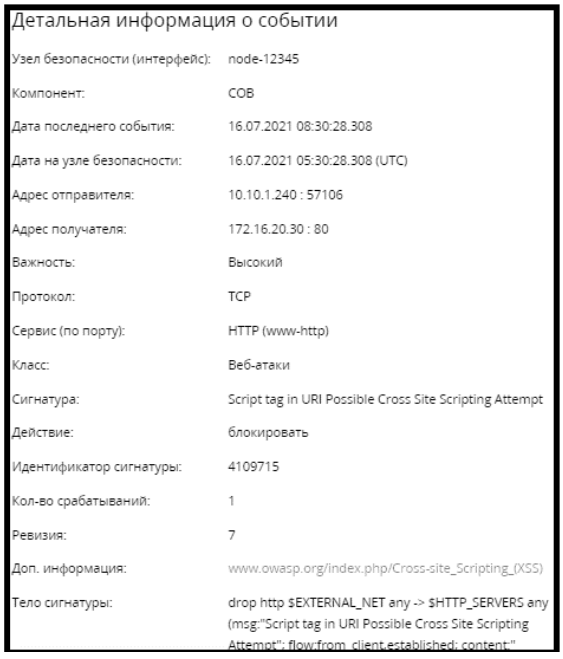
нок 10), была заблокирован системой предотвращения вторжений (рисунок 11).

4) Атака на веб-приложение

Metasploitable 2 содержит несколько уязвимых веб-приложений. Данные приложения используются для тренировки проведения веб-атак. Сервисы Mutillidae и DVWA позволяют воспроизвести атаки из OWASP top 10.

OWASP (открытый проект обеспечения безопасности веб-приложений) создал список из 10 самых опасных векторов атак на веб-приложения. Этот список получил название OWASP top 10.

Одной из атак из OWASP top 10 является XXS (межсайтовый скриптинг) [4]. Суть данной атаки заключается во внедрении вредоносного Java Script кода на исполнение в браузер пользователя. На рисунке 12 показана попытка реализации данной атаки. Система предотвращения вторжений заблокировала XSS-атаку, о чем свидетельствует запись в журнале событий на рисунке 13.


Детальная информация о событии

Узел безопасности (интерфейс):	node-12345
Компонент:	СОВ
Дата последнего события:	16.07.2021 08:30:28.308
Дата на узле безопасности:	16.07.2021 05:30:28.308 (UTC)
Адрес отправителя:	10.10.1.240 : 57106
Адрес получателя:	172.16.20.30 : 80
Важность:	Высокий
Протокол:	TCP
Сервис (по порту):	HTTP (www-http)
Класс:	Веб-атаки
Сигнатура:	Script tag in URI Possible Cross Site Scripting Attempt
Действие:	блокировать
Идентификатор сигнатуры:	4109715
Кол-во срабатываний:	1
Ревизия:	7
Доп. информация:	www.owasp.org/index.php/Cross-site_Scripting_(XSS)
Тело сигнатуры:	drop http $EXTERNAL_NET any -> $HTTP_SERVERS any (msg:"Script tag in URI Possible Cross Site Scripting Attempt"; flow:from_client,established; content:"

Рис. 13. Заблокированная XSS-атака

Таблица 1

Результат применения системы предотвращения вторжений

№	Порт (сервис)	Наименование атаки/эксплойт	Действие
1	21 (FTP)	Брутфорс-атака на FTP-сервер	Обнаружил
2	21 (FTP)	Vsftpd_234_backdoor	Заблокировал
3	22 (SSH)	Брутфорс-атака на SSH	Обнаружил
4	23 (Telnet)	Брутфорс-атака Telnet	Обнаружил
5	80 (HTTP)	Php_cgi_arg_injection	Заблокировал
6	80 (HTTP)	SQL-инъекция	Не обнаружил
7	80 (HTTP)	XSS	Заблокировал
8	139/445 (NetBIOS)	Usermap_script	Заблокировал
9	1099 (RMI Rigestry)	Java_rmi_server	Заблокировал
10	1524	Bind shell-подключение	Не обнаружил
11	3306 (MySQL)	Удаленное выполнение команд в СУБД MySQL	Обнаружил
12	5432 (PostgreSQL)	Postgres_payload	Не обнаружил
13	5900 (VNC)	Подключение через VNC	Не обнаружил
14	6667 (IRC)	Unreal_ircd_3281_backdoor	Заблокировал
15	8180 (Apache Tomcat)	Tomcat_mgr_upload	Заблокировал

В таблице 1 представлены все проведенные атаки и результаты работы системы предотвращения вторжений «Континент 4».

Система предотвращения вторжений «Континент 4» заблокировала большую часть атак (73,3%). При этом проводимые атаки являются как протокольными (доступ по SSH, Telnet, VNC), то есть блокируются межсетевым экраном, так и эксплуатирующими уязвимости программного обеспечения (эксплойты, бэкдоры и др.).

Также некоторые атаки происходили на веб-приложения (SQL-инъекция, XSS). Для обеспечения безопасности веб-приложений принято использовать межсетевой экран веб-приложений (WAF). Тем не менее сетевая система предотвращения вторжений «Континент 4» смогла обнаружить и заблокировать некоторые атаки из данной категории.

В работе был продемонстрирован метод оценки эффективности использования системы предотвращения вторжений с целью повышения общей защищенности предприятия.

Таким образом можно сделать вывод, что хоть системы предотвращения и являются необходимым компонентом эшелонированной обороны предприятия, но использование данных систем не защищает

сеть организации на 100%. Информационная безопасность должна быть комплексной, поэтому необходимо брать во внимание и другие ее факторы, такие как обновление программного обеспечения, настройка межсетевого экрана, предоставление безопасного удаленного доступа к ресурсам предприятия и т.д. Однако, показанный в работе метод, позволяет оценить общий уровень защищенности системой предотвращения вторжений и определить объекты, требующие дополнительных мер по защите.

Литература

1. Парасрам Шива, Замм Алекс, Хериянто Теди, Али Шакил, Буду Дамиан, Йохансен Джерард, Аллен Ли. Kali Linux. Тестирование на проникновение и безопасность. - 4-е изд. - СПб.: Питер, 2020. - 448 с.

2. Код безопасности. Продукты. Континент 4. [Электронный ресурс]. – Режим доступа: https://www.securitycode.ru/products/kontinent-4/, свободный. (дата обращения 24.10.2021)

3. Руководство по эксплуатации Metasploit. [Электронный ресурс]. – Режим доступа: https://docs.rapid7.com/metasploit, свободный. (дата обращения 25.10.2021)

4. OWASP. [Электронный ресурс]. – Режим доступа: https://owasp.org/, свободный. (дата обращения 30.10.2021)

References

1. Parasram Shiva, Zamm Aleks, Kheriyanto Tedi, Ali Shakil, Budu Damian, Yokhansen Dzherard, Allen Li. Kali Linux. Testirovaniye na proniknoveniye i bezopasnost'. - 4-ye izd. - SPb.: Piter, 2020. - 448 s.

2. Kod bezopasnosti. Produkty. Kontinent 4. [Elektronnyy resurs]. – Rezhim dostupa: https://www.securitycode.ru/products/kontinent-4/, svobodnyy. (data obrashcheniya 24.10.2021)/

3. Rukovodstvo po ekspluatatsii Metasploit. [Elektronnyy resurs]. – Rezhim dostupa: https://docs.rapid7.com/metasploit, svobodnyy. (data obrashcheniya 25.10.2021)/

4. OWASP. [Elektronnyy resurs]. – Rezhim dostupa: https://owasp.org/, svobodnyy. (data obrashcheniya 30.10.2021)/

ЛЕБЕДЕВ Дмитрий Валерьевич, студент кафедры информационных технологий и защиты информации, Уральский государственный университет путей сообщения. 620034, г. Екатеринбург, ул. Колмогорова, 66. E-mail: dmvlebedev@mail.ru

LEBEDEV Dmitriy Valerievich, student of the Department of Information Technology and Information Security, Ural State University of Railway Transport. 66 Kolmogorova str., Yekaterinburg, 620034. E-mail: dmvlebedev@mail.ru

ГУЗЕНКОВА Елена Алексеевна, старший преподаватель кафедры информационных технологий и защиты информации, Уральский государственный университет путей сообщения. 620034, г. Екатеринбург, ул. Колмогорова, 66. E-mail: sato-hany@ya.ru

GUZENKOVA Elena Alekseevna, Senior Lecturer of the Department of Information Technology and Information Security, Ural State University of Railway Transport. 66 Kolmogorova str., Yekaterinburg, 620034. E-mail: sato-hany@ya.ru