

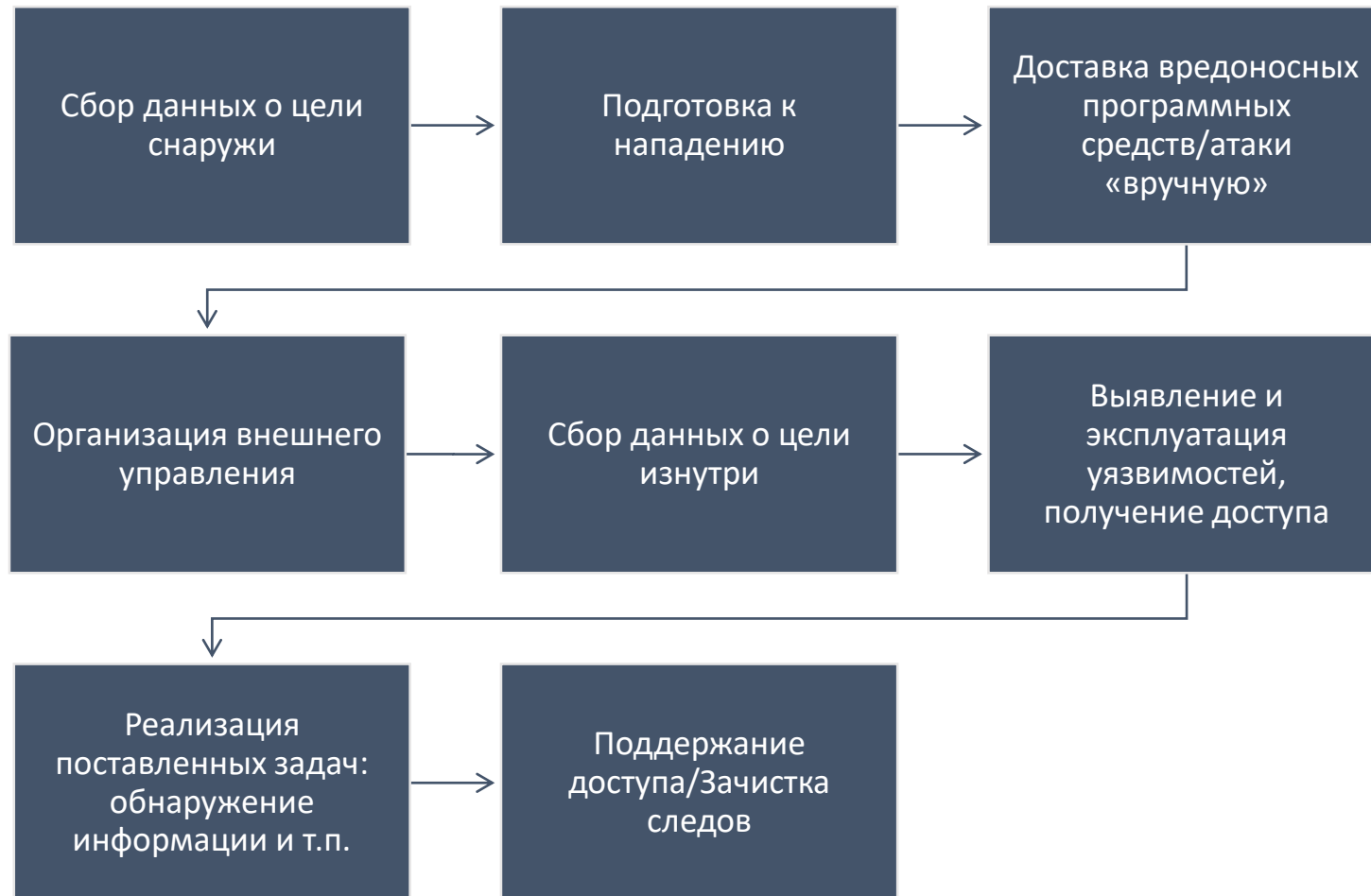
# **Подходы к тестированию защищенности. Обзор возможностей Сканер-ВС 6**

Дорофеев Александр, CISSP, CISA, CISM

# План

1. Современная кибератака
2. Подходы к тестированию защищенности
3. Сканеры уязвимостей: принципы работы и ограничения
4. Обзор возможностей Сканер-ВС 6

# Современная таргетированная атака (АРТ) = спецоперация



# MITRE ATT@CK (1)

1. Reconnaissance – сбор информации о цели снаружи
2. Resource Development – подготовка ресурсов для нападения
3. Initial Access – первоначальный доступ
4. Execution – попытка запуска вредоносного ПО
5. Persistence – организация постоянного доступа к целевой инфраструктуре
6. Privilege Escalation – повышение уровня доступа
7. Defense Evasion – обход средств защиты информации

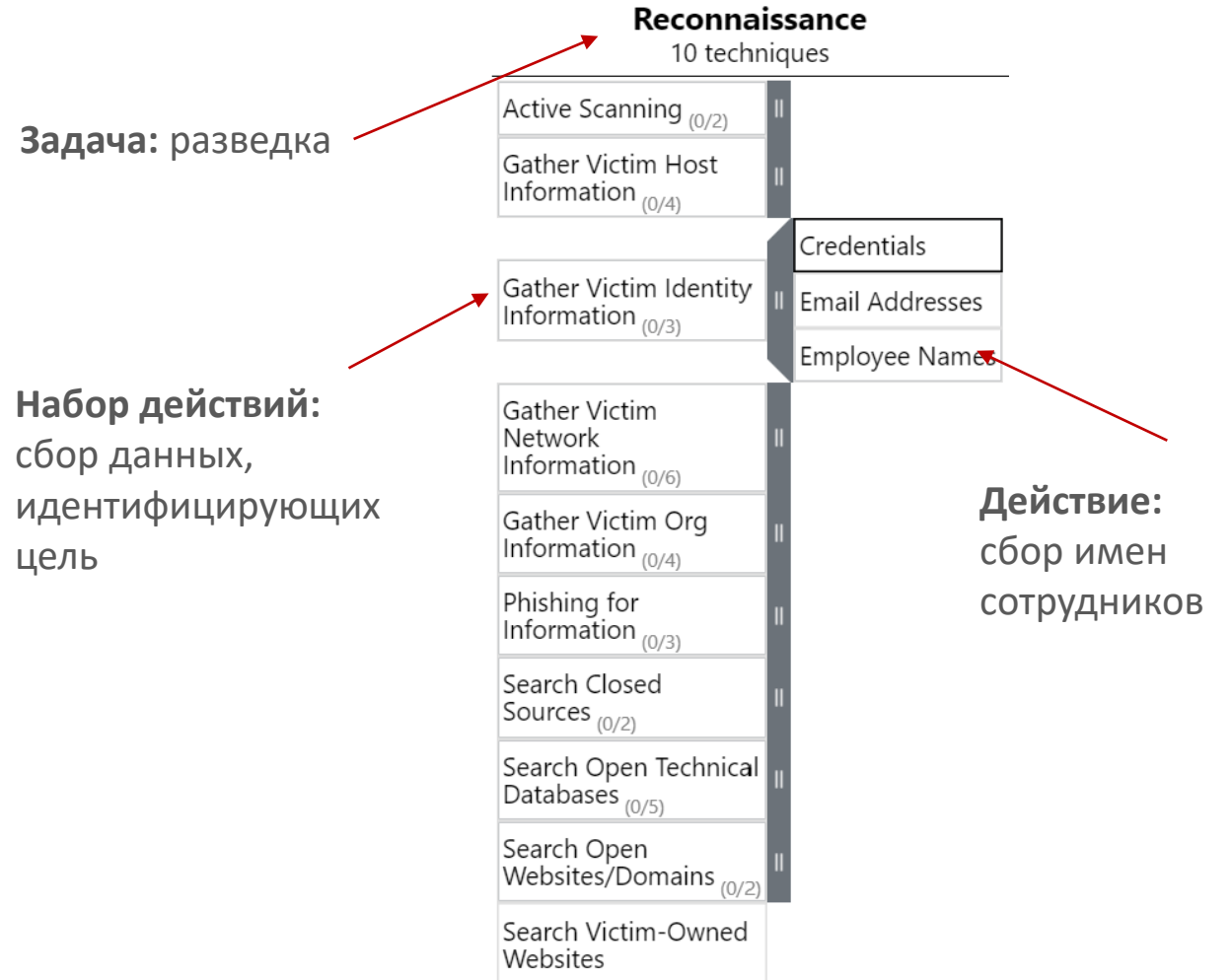
The image shows the MITRE ATT&CK Navigator interface, which is a tool for visualizing and analyzing attack techniques. The interface is divided into several columns, each representing a different category of attack techniques. The categories and their respective technique counts are as follows:

Category	Count
Reconnaissance	10 techniques
Resource Development	7 techniques
Initial Access	9 techniques
Execution	12 techniques
Persistence	19 techniques
Privilege Escalation	13 techniques
Defense Evasion	39 techniques
Credential Access	15 techniques
Discovery	27 techniques
Lateral Movement	9 techniques
Collection	17 techniques
Command and Control	16 techniques
Exfiltration	9 techniques
Impact	13 techniques

The interface also includes a search bar at the top, a legend at the bottom, and various navigation controls. The techniques are listed in a grid format, with each cell containing the technique name and a small icon representing the technique's category.

# MITRE ATT@CK (2)

8. Credential Access – получение доступа с помощью действующих учетных записей
9. Discovery – сбор информации о цели изнутри
10. Lateral Movement – перемещение внутри целевой ИТ-инфраструктуры
11. Collection – сбор интересующих данных
12. Command and Control – организация внешнего управления
13. Exfiltration – передача интересующих данных вовне
14. Impact – разрушающее воздействие на ИТ-инфраструктуру



# Приложение 11 к Методике оценки угроз ФСТЭК России

Приложение 11  
к Методике оценки угроз  
безопасности информации

Перечень основных тактик и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации

Таблица 11.1

№	Тактика	Основные техники
T1	Сбор информации о системах и сетях  Тактическая задача: нарушитель стремится получить любую техническую информацию, которая может оказаться полезной в ходе реализации угроз безопасности информации	<p>T1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций</p> <p>T1.2. Сбор информации о подключенных к публичным системам и сетям устройствах и их службах при помощи поисковых систем, включая сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений. Пример: использование поисковой системы Shodan для получения информации об определенных моделях IP-камер видеонаблюдения с возможно уязвимыми версиями прошивок</p> <p>T1.3. Пассивный сбор (прослушивание) информации о подключенных к сети устройствах с целью идентификации сетевых служб, типов и версий ПО этих служб и в некоторых случаях – идентификационной информации пользователей</p> <p>T1.4. Направленное сканирование при помощи специализированного программного обеспечения подключенных к сети устройств с целью идентификации сетевых сервисов, типов и версий программного обеспечения этих сервисов, а также с целью получения конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений. Пример: сканирование при помощи сканера шпар</p> <p>T1.5. Сбор информации о пользователях, устройствах, приложениях, а также сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений путем поиска и эксплуатации уязвимостей подключенных к сети устройств. Пример: эксплуатация уязвимости типа directory traversal публично доступного веб-сервера</p>

Продолжение таблицы 11.1

№	Тактика	Основные техники
		<p>T1.6. Сбор информации о пользователях, устройствах, приложениях, авторизуемых сервисах и вычислительной сети, путем перебора. Пример: сбор информации о почтовых адресах при помощи directoryhavestack на почтовые сервера</p> <p>T1.7. Сбор информации, предоставляемой DNS сервисами, включая DNS Hijacking</p> <p>T1.8. Сбор информации о пользователе при посещении им веб-сайта, в том числе с использованием уязвимостей программы браузера и настраиваемых модулей браузера</p> <p>T1.9. Сбор информации о пользователях, устройствах, приложениях путем поиска информации в памяти, файлах, каталогах, базах данных, прошивках устройств, репозиториях исходных кодов ПО, включая поиск паролей в исходном и хшированном виде, криптографических ключей. Пример: получение хэшей паролей из (/etc/passwd или получение паролей по умолчанию путем обратного инжиниринга прошивки устройства</p> <p>T1.10. Кража цифровых сертификатов, включая кражу физических токенов, либо неавторизованное выписывание новых сертификатов (возможно после компрометации инфраструктуры доменного регистратора или аккаунта администратора зоны на стороне жителя)</p> <p>T1.11. Сбор информации о пользователях, устройствах, приложениях, внутренней информации о компонентах систем и сетей путем применения социальной инженерии, в том числе фишинга</p> <p>T1.12. Сбор личной идентификационной информации (идентификаторы пользователей, устройства, информация об идентификации пользователей сервисами, приложениями, средствами удаленного доступа), в том числе сбор украденных личных данных сотрудников и подрядчиков на случай, если сотрудники/подрядчики используют одни и те же пароли на работе и за ее пределами</p> <p>T1.13. Сбор информации через получение доступа к системам физической безопасности и видеонаблюдения</p> <p>T1.14. Сбор информации через получение контроля над личными устройствами сотрудников (смартфонами, планшетами, ноутбуками) для скрытой прослушки и видеонаблюдения</p> <p>T1.15. Поиск и покупка баз данных идентификационной информации, скопированных паролей и ключей на специализированных нелегальных площадках</p>

Угроза несанкционированного доступа к базе данных, содержащей защищаемую информацию

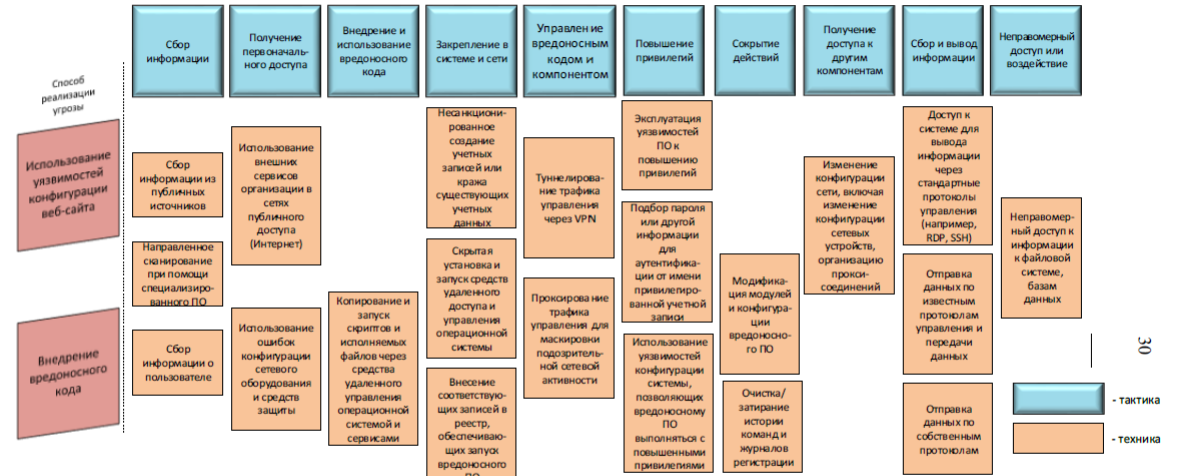


Рисунок 7. Пример сценария реализации угрозы безопасности информации

# Что можно позаимствовать у хакеров для комплексной методики анализа защищенности?

- Цели
- Приемы взлома
- Инструменты



# Цели



Административный  
доступ



Конкретные данные для  
демонстрации их  
незащищенности  
руководству



# Приемы взлома/тестирования

ИСКУССТВО  
ТЕСТИРОВАНИЯ  
НА ПРОНИКНОВЕНИЕ  
В СЕТЬ

Как взломать любую  
компанию в мире

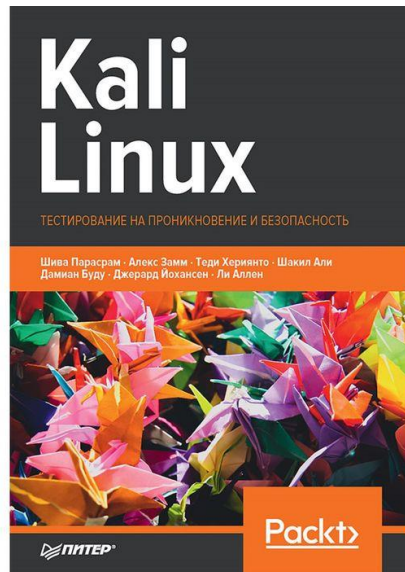


Ройс Дэвис

MANNING

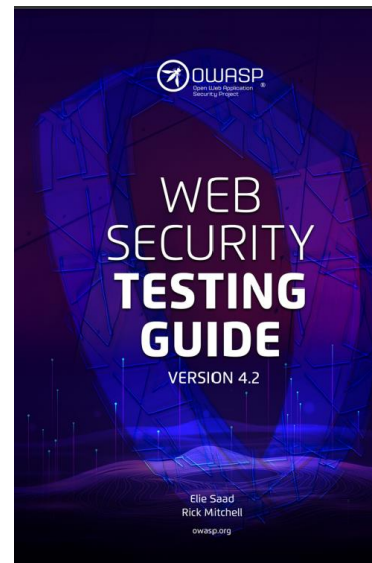
ОМК

Книги



ПИТЕР

Packt



Elie Saad  
Rick Mitchell  
owasp.org

Методики от  
профессиональных  
сообществ

NIST  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

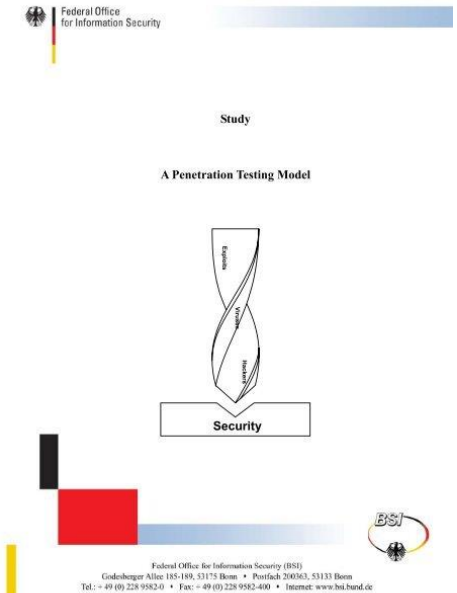
Special Publication 800-115

**Technical Guide to  
Information Security Testing  
and Assessment**

Recommendations of the National Institute  
of Standards and Technology

Karen Scarfone  
Murugiah Souppaya  
Amanda Cody  
Angela Orebaugh

Методики от организаций,  
спонсируемых государствами



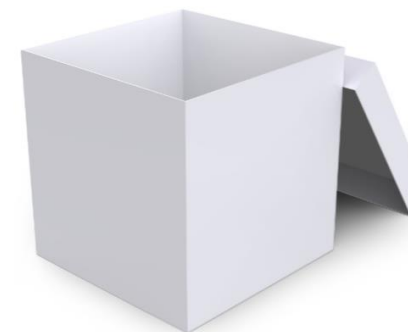
# Существующие подходы к оценке защищенности



Классический тест  
на проникновение



Сканирование на  
наличие уязвимостей



Анализ конфигурации

# Классический тест на проникновение

- Имитация действий реального злоумышленника – поиск первой уязвимости, позволяющей получить доступ к системе
- Больше искусство, чем аудит. Качество сильно зависит от уровня специалиста
- Обычный результат: несколько опасных уязвимостей
- Высокий риск нарушения доступности систем



# Сканирование

- Использование исключительно сканеров для поиска уязвимостей
- Качество сильно зависит от используемого сканера.
- Результат: множество уязвимостей различного уровня опасности
- Средний риск нарушения работоспособности систем



# Анализ конфигурации системы

- Проверка настроек систем в соответствии с рекомендуемыми вендорами или сообществами профессионалов по ИБ (NIST, Center Internet Security).
- Результат: множество уязвимостей различного уровня опасности
- Низкий риск нарушения работоспособности систем

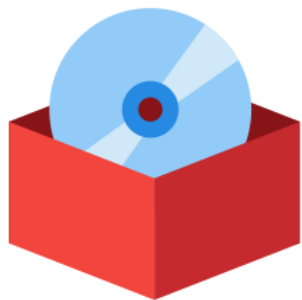


# Комплексный подход: комбинация всех подходов и приемов злоумышленников



# Инструментарий хакеров: ЭТИЧНЫХ И НЕ ОЧЕНЬ

Специалисты по тестированию защищенности



Зловреды/  
кибероружие



Хакерские  
утилиты с  
открытым  
исходным  
кодом



Утилиты  
операционн  
ой системы



Сканеры  
уязвимостей

Злоумышленники

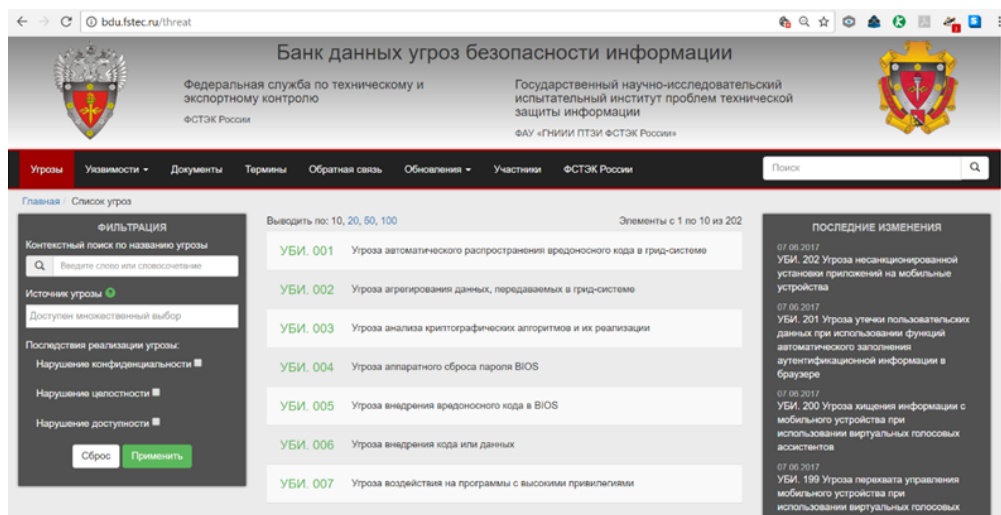
# Немного об уязвимостях (ГОСТ Р 56546-2015)

- Уязвимость - недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации
- Уязвимость может быть внесена в процессе проектирования (уязвимость архитектуры), разработки (уязвимость кода) и в процессе задания конфигурации (уязвимость конфигурации).



# Уязвимости:

## ИЗВЕСТНЫЕ



Запись об уязвимости внесена в базу данных уязвимостей и ей присвоен идентификатор (CVE, BDU)

## НУЛЕВОГО ДНЯ



Об уязвимости знает только ограниченный круг лиц, вендор ПО не знает, либо пока не успел выпустить обновление безопасности.

# Технология поиска известных уязвимостей



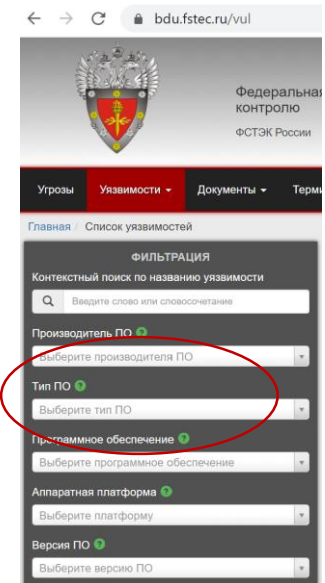
Apache HTTP Server 2.2.8



apache http server 2.2.8 vulnerabilities

Поиск в Google

Мне повезёт!



## Apache » Http Server » 2.2.8 : Security Vulnerabilities (Execute Code)

Cpe Name: cpe:/a:apache:http\_server:2.2.8

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By: CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

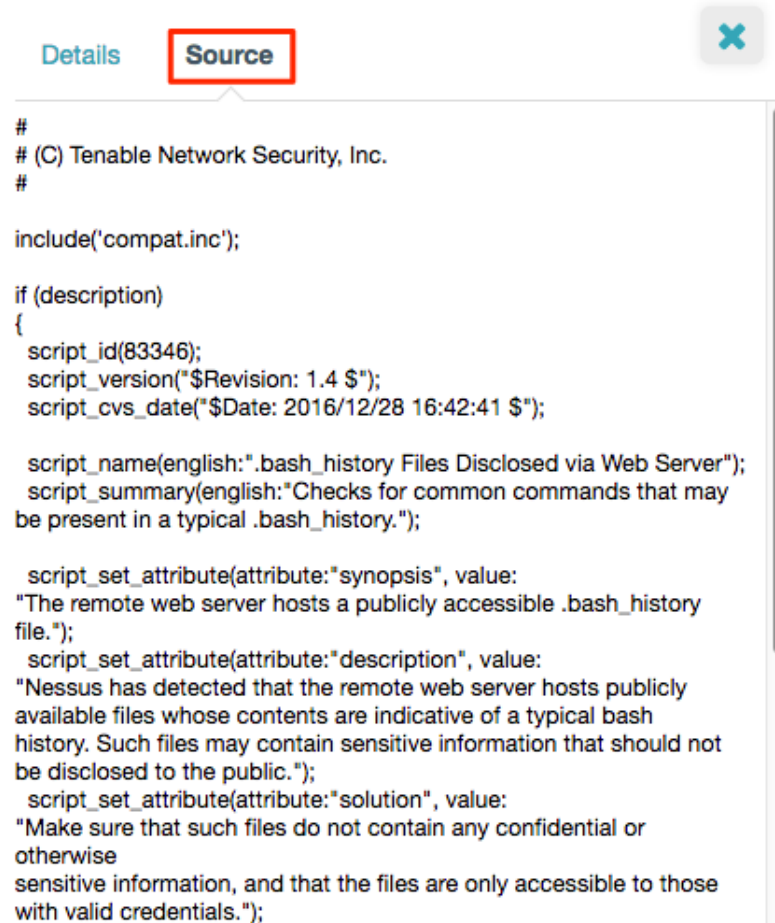
#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	<a href="#">CVE-2013-1862</a>	<a href="#">310</a>		Exec Code	2013-06-10	2017-09-18	5.1	None	Remote	High	Not required	Partial	Partial	Partial
mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary commands via an HTTP request containing an escape sequence for a terminal emulator.														
2	<a href="#">CVE-2010-0425</a>			Exec Code	2010-03-05	2018-10-30	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
modules/arch/win32/mod_isapi.c in mod_isapi in the Apache HTTP Server 2.0.37 through 2.0.63, 2.2.0 through 2.2.14, and 2.3.x before 2.3.7, when running on Windows, does not ensure that request processing is complete before calling isapi_unload for an ISAPI .dll module, which allows remote attackers to execute arbitrary code via unspecified vectors related to a crafted request, a reset packet, and "orphaned callback pointers."														

Total number of vulnerabilities : 2 Page : 1 (This Page)

# Автоматизация поиска: создания скрипта на каждую уязвимость

Nessus Attack  
Scripting Language

Nmap Scripting Engine



```
#
# (C) Tenable Network Security, Inc.
#

include('compat.inc');

if (description)
{
  script_id(83346);
  script_version("$Revision: 1.4 $");
  script_cvs_date("$Date: 2016/12/28 16:42:41 $");

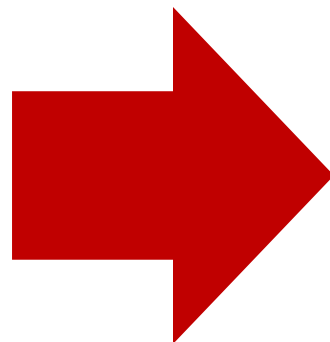
  script_name(english:".bash_history Files Disclosed via Web Server");
  script_summary(english:"Checks for common commands that may
be present in a typical .bash_history.");

  script_set_attribute(attribute:"synopsis", value:
"The remote web server hosts a publicly accessible .bash_history
file.");
  script_set_attribute(attribute:"description", value:
"Nessus has detected that the remote web server hosts publicly
available files whose contents are indicative of a typical bash
history. Such files may contain sensitive information that should not
be disclosed to the public.");
  script_set_attribute(attribute:"solution", value:
"Make sure that such files do not contain any confidential or
otherwise
sensitive information, and that the files are only accessible to those
with valid credentials.");
```

# Результат: в ходе сканирования одного узла запускаются тысячи скриптов

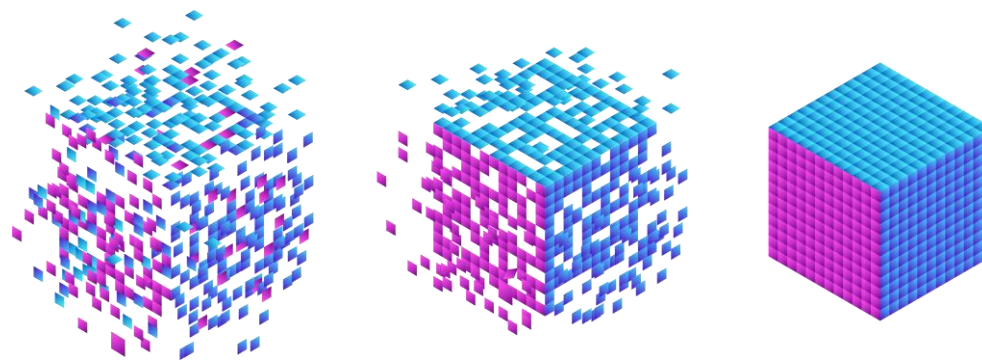
Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	<a href="#">586</a>	0.30
1-2	<a href="#">1143</a>	0.70
2-3	<a href="#">7769</a>	4.60
3-4	<a href="#">8399</a>	5.00
4-5	<a href="#">40132</a>	23.70
5-6	<a href="#">32372</a>	19.10
6-7	<a href="#">25056</a>	14.80
7-8	<a href="#">34010</a>	20.10
8-9	<a href="#">826</a>	0.50
9-10	<a href="#">19222</a>	11.30
<b>Total</b>	169515	



# Современный подход: использование агрегированной базы данных уязвимостей

- БДУ ФСТЭК России
- NIST National Vulnerability Database
- База обновлений Windows
- RHEL/CentOS Security Data
- Ubuntu CVE Tracker
- Debian GNU/Linux Security Bug Tracker
- ...



# Клиент-серверная архитектура

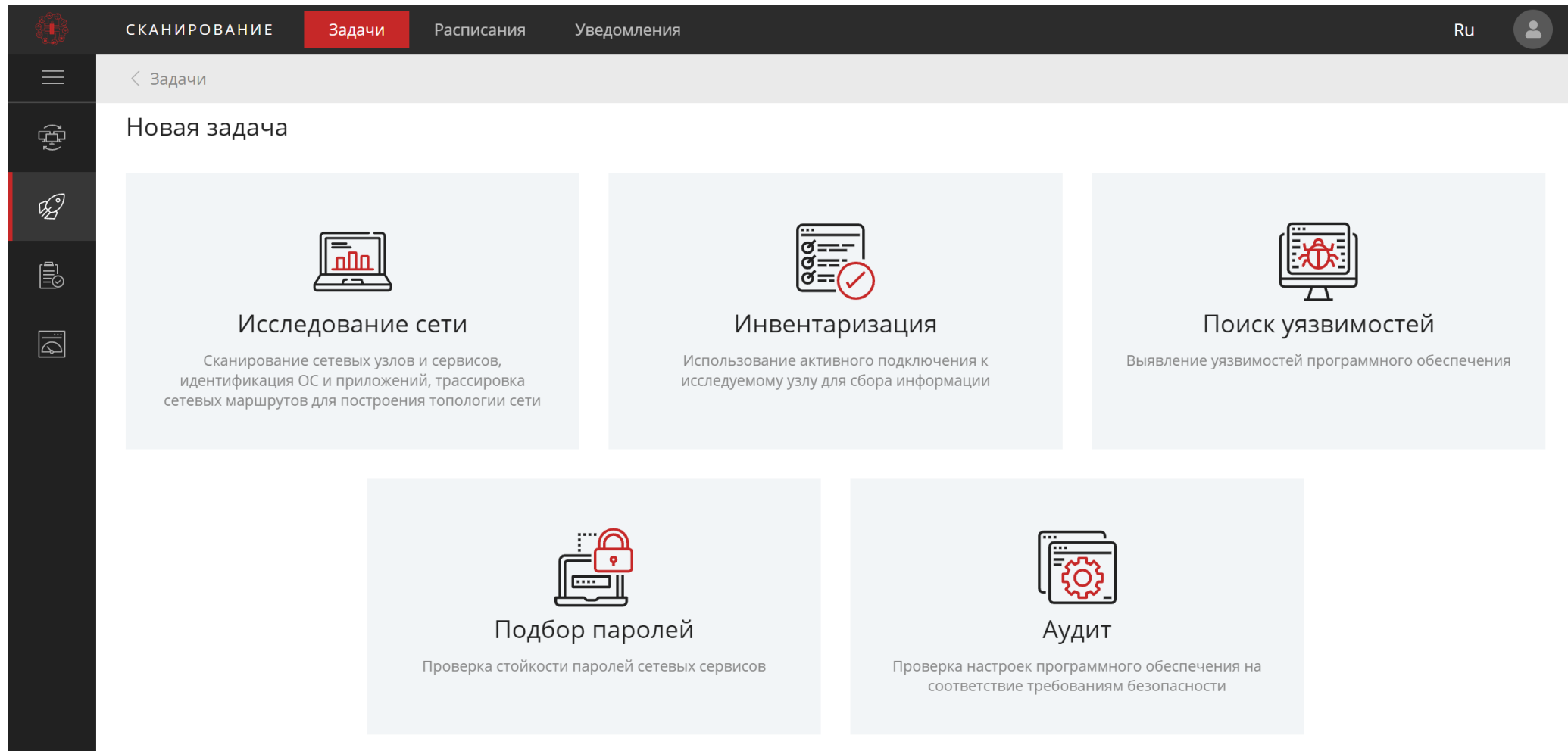


Web-браузер  
ОС: Windows/Linux



Сканер-BC 6.0  
ОС: Debian-based Linux

# Ключевой функционал



# Открытые сетевые порты

Порт	Состояние	Сервис	Продукт	Версия	CPE
21/tcp	открыт	ftp	vsftpd	2.3.4	cpe:2.3:a:vsftpd:vsftpd:2.3.4:*:*:*:*...
22/tcp	открыт	ssh	OpenSSH	4.7p1 Debian 8ubuntu1	cpe:2.3:a:openbsd:openssh:4.7p1:*:*:*...
23/tcp	открыт	telnet	Linux telnetd		cpe:2.3:o:linux:linux_kernel:*:*:*:*...
25/tcp	открыт	smtp	Postfix smtpd		cpe:2.3:a:postfix:postfix:*:*:*:*:*
53/tcp	открыт	domain	ISC BIND	9.4.2	cpe:2.3:a:isc:bind:9.4.2:*:*:*:*
80/tcp	открыт	http	Apache httpd	2.2.8	cpe:2.3:a:apache:http_server:2.2.8:*:*...
111/tcp	открыт	rpcbind		2	
139/tcp	открыт	netbios-ssn	Samba smbd	3.X - 4.X	cpe:2.3:a:samba:samba:*:*:*:*:*
445/tcp	открыт	netbios-ssn	Samba smbd	3.X - 4.X	cpe:2.3:a:samba:samba:*:*:*:*:*
512/tcp	открыт	exec	netkit-rsh rexecd		cpe:2.3:a:netkit:netkit:*:*:*:*:*
513/tcp	открыт	login	OpenBSD or Solaris rlogind		
514/tcp	открыт	shell	Netkit rshd		cpe:2.3:a:netkit:netkit_rsh:*:*:*:*...

Всего портов: 23

<https://tools.kali.org>



# Установленное ПО

<input type="checkbox"/>	Название	Вендор	Тип	Версия	Архитектура	CPE	ID учетной записи
<input type="checkbox"/>	Ubuntu 8.04		unknown	8.04	i686	cpe:2.3:a:postgresql:postgresql:...	1
<input type="checkbox"/>	adduser	Ubuntu Core Developers <ubun...	unknown	3.105ubuntu1	all		1
<input type="checkbox"/>	ant	Ubuntu Core Developers <ubun...	unknown	1.7.0-3	all	cpe:2.3:a:ant.design:ant_design:...	1
<input type="checkbox"/>	antlr	Ubuntu Core Developers <ubun...	unknown	2.7.6-10	all		1
<input type="checkbox"/>	apache2	Ubuntu Core Developers <ubun...	unknown	2.2.8-1	all		1
<input type="checkbox"/>	apache2-mpm-prefork	Ubuntu Core Developers <ubun...	unknown	2.2.8-1ubuntu0.15	i386		1
<input type="checkbox"/>	apache2-utils	Ubuntu Core Developers <ubun...	unknown	2.2.8-1ubuntu0.15	i386	cpe:2.3:a:ecryptfs:ecryptfs-utils:...	1
<input type="checkbox"/>	apache2.2-common	Ubuntu Core Developers <ubun...	unknown	2.2.8-1ubuntu0.15	i386	cpe:2.3:a:postgresql:postgresql:...	1
<input type="checkbox"/>	apparmor	Ubuntu Core Developers <ubun...	unknown	2.1+1075-0ubuntu9	i386	cpe:2.3:a:apparmor:apparmor:2:...	1
<input type="checkbox"/>	apparmor-utils	Ubuntu Core Developers <ubun...	unknown	2.1+1075-0ubuntu9	i386	cpe:2.3:a:apparmor:apparmor:2:...	1
<input type="checkbox"/>	apt	Ubuntu Core Developers <ubun...	unknown	0.7.9ubuntu17	i386	cpe:2.3:a:apt-listbugs_project:a:...	1
<input type="checkbox"/>	apt-utils	Ubuntu Core Developers <ubun...	unknown	0.7.9ubuntu17	i386	cpe:2.3:a:ecryptfs:ecryptfs-utils:...	1

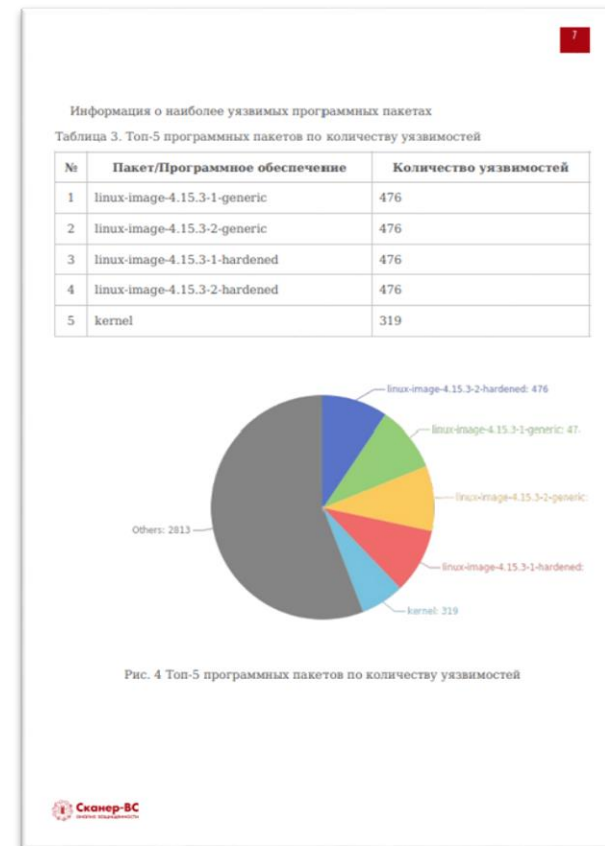
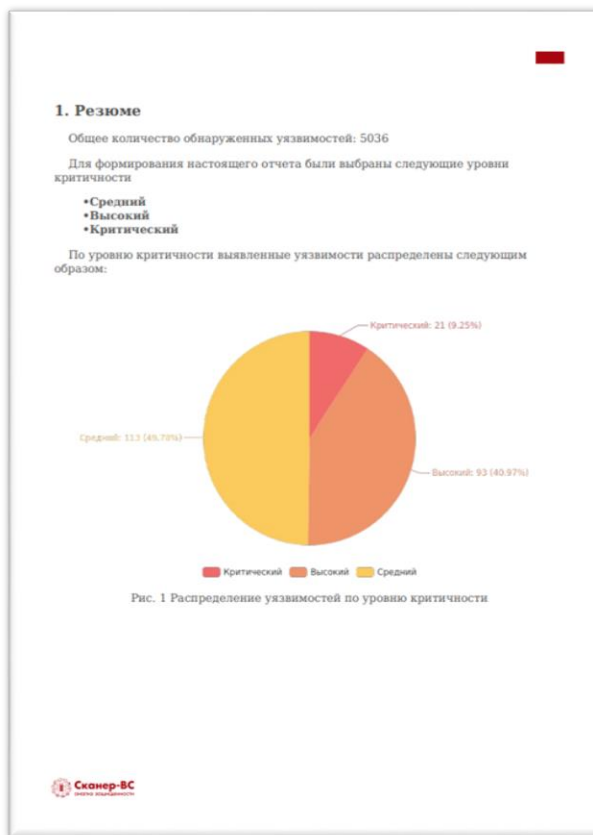
# Список обнаруженных уязвимостей

The screenshot shows a web browser window displaying the results of a security scan. The interface is in Russian and shows a list of 9 vulnerabilities for Apache Tomcat. The table includes columns for severity, CVSS scores, CVE IDs, and BDU identifiers.

Порт	Уязвимое ПО	Название	Опасность	CVSS 2.0	CVSS 3.0	CVE	BDU
0	Apache Tomcat	При расследовании ошиб...	Высокая	5	7.5	CVE-2020-17527	
0	Apache Tomcat	При использовании Арас...	Высокая	4.4	7	CVE-2020-9484	BDU:2020-03620
0	Apache Tomcat	При обслуживании ресур...	Средняя	4.3	5.9	CVE-2021-24122	
0	Apache Tomcat	При ответе на новые запр...	Высокая	5	7.5	CVE-2021-25122	BDU:2021-01807
0	Apache Tomcat	Исправление для CVE-202...	Высокая	4.4	7	CVE-2021-25329	BDU:2021-01808
0	Apache Tomcat	Уязвимость в области JND...	Средняя	5.8	6.5	CVE-2021-30640	BDU:2021-03686
0	Apache Tomcat	Apache Tomcat с 10.0.0-M1...	Средняя	5	5.3	CVE-2021-33037	BDU:2021-03688
0	Apache Tomcat	Apache Tomcat с 8.5.0 по 8...	Высокая	4.3	7.5	CVE-2021-41079	
0	Apache Tomcat			0	0		BDU:2021-06115

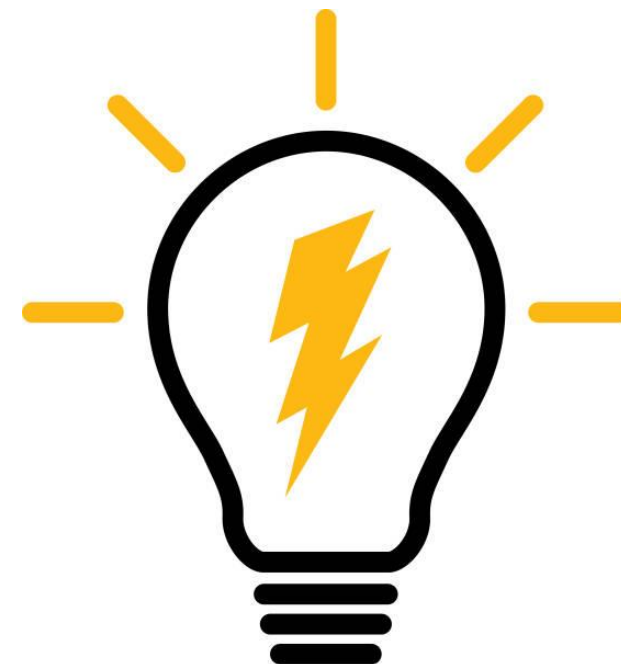
Всего уязвимостей: 9

# Отчеты с результатами сканирования



# Отличительные особенности:

- База уязвимостей, включающая все известные уязвимости (~170 тыс)
- Поддержка актуальных версий ОС: Windows, Linux
- Высокая скорость поиска уязвимостей
- Дистрибутив под Astra Linux SE
- Подбор паролей по распространенным протоколам (ftp, ssh, smtp, postgres и т.д.)

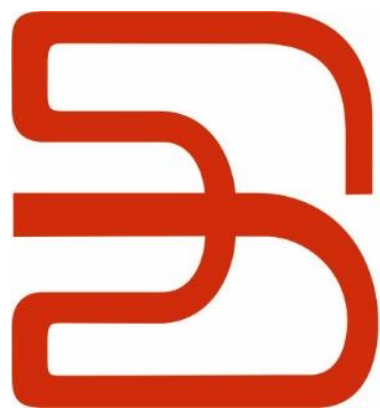


# Как получить превью-версию Сканер-ВС 6?

- [getsscanner@npo-echelon.ru](mailto:getsscanner@npo-echelon.ru) – email для получения превью-версии Сканер-ВС 6
- <https://t.me/scanervs> чат пользователей продукта
- <https://www.youtube.com/channel/UCIwZEG8EcL7tnZN4Qzjt13w>  
канал учебного центра «Эшелон» с обучающими видео

**СПАСИБО ЗА  
ВНИМАНИЕ!**

Марков Алексей Сергеевич  
д.т.н., CISSP, СЕН  
[a.markov@npo-echelon.ru](mailto:a.markov@npo-echelon.ru)



**Эшелон**

комплексная безопасность