

# Сканер уязвимостей OpenVAS.

## Поиск уязвимостей при помощи сканера.

### Уязвимости: теория

#### Причины возникновения уязвимостей

Bad coding

Архитектурная особенность

Ошибки логики работы приложения, компонента или иной сущности

Слабые настройки

#### Оценка уязвимости

### Поиск уязвимостей

#### Поиск уязвимостей по наличию обновлений

#### Поиск уязвимости при помощи сканеров

Xspider

RedCheck

Nessus

OpenVAS

Scan OVAL

### OpenVAS

#### Состав компонентов OpenVAS

OpenVAS Scanner

OpenVAS Manager

OpenVAS CLI

Greenbone Security Assistant

#### Правила для обнаружения уязвимостей

#### Установка, настройка и работа с OpenVAS в Kali Linux

Установка OpenVAS в Kali Linux

Проверка работы сервисов OpenVAS

Добавление и смена пароля пользователя

#### Практическая часть

Задание 1. Быстрое сканирование (immediate scan)

Задание 2. Задать цель вручную и провести сканирование цели

Задание 3. Создать конфиг для сканирования узла с ОС Debian Linux и просканировать узел

#### Выводы

#### Практическое задание

#### Дополнительные материалы

# Уязвимости: теория

Определимся с терминологией. Согласно ISO 27000:

- **уязвимость (vulnerability)** — это слабое место актива или меры и средства контроля и управления, которое может использовать угроза;
- **актив (asset)** — то, что имеет ценность для организации;
- **мера и средство контроля и управления (control)** — предназначены для менеджмента риска. Включает политики, процедуры, рекомендации, практические приемы или организационные структуры (административные, технические, управленческие или правовые). Под уязвимостью будем понимать слабость, эксплуатируя которую, можно реализовать угрозу.

Уязвимости можно разделить на те, что присутствуют в программных и технических компонентах, и те, которые появились вследствие несоблюдения процедур безопасности.

С каждой уязвимостью будет связана угроза: если она реализуется в системе, будут последствия.

Чем серьезнее последствия, тем выше показатель угрозы и уязвимости, приводящей к ее реализации, при их оценке. Но надо учитывать, что за угрозой могут стоять нескольких уязвимостей.

Рассмотрим, каким образом возникают уязвимости и происходит их оценка.

## Причины возникновения уязвимостей

### Bad coding

Обычная причина уязвимостей в ПО — ошибки, которые возникают при написании программ. Наиболее типичный пример — уязвимость **buffer overflow**. В «Википедии» о ней пишут так: *«Записывая данные в буфер, можно осуществить запись за его границами и изменить находящиеся там данные (в частности, адрес возврата). Если программа имеет особые привилегии — например, запущена с правами root, — злоумышленник может заменить адрес возврата на адрес шелл-кода. Это позволит ему исполнять команды в атакуемой системе с повышенными привилегиями»*.

Подобная процедура возможна в том числе потому, что в языках программирования нет встроенной защиты от переполнения буфера. Особенно это относится к C/C++, исключение — JavaScript.

### Архитектурная особенность

Часто уязвимость присутствует на аппаратном уровне: в процессоре или ОЗУ. Уязвимость **Meltdown** использует ошибку реализации спекулятивного выполнения команд в процессорах Intel и ARM. Из-за нее при спекулятивном выполнении инструкций чтения из памяти процессор игнорирует права доступа к страницам. При запуске специальной программы уязвимость позволяет локальному атакующему несанкционированно читать привилегированную память, которую использует ядро ОС.

Рассмотрим еще уязвимость **Rowhammer**, которой подвержены некоторые чипы **DDR3**. Злоумышленник может запустить программу, которая будет тысячи раз за долю секунды обращаться к конкретным рядам участков в модуле памяти. Она «постукивает по ним молотком» (hammering), пока электромагнитное излучение не проникает в соседний участок памяти. Это может изменить значения битов в нем с нулей на единицы и наоборот.

## Ошибки логики работы приложения, компонента или иной сущности

Иногда при разработке приложения авторы не учитывают особенности работы с одним из компонентов. Как в случае с уязвимостью **Sql injection**, при которой в имеющейся SQL-запрос добавляются конструкции, существенно изменяющие его логику работы. Такое нарушение в web-приложении может привести к уязвимостям: **XSS**, **CSRF**, **Clickjacking** и другим.

## Слабые настройки

Как правило, это стандартные учетные данные оборудования (логин, пароль) или те, что легко подобрать. Часто в устройстве есть предустановленная учетная запись сервиса, доступного из глобальной сети (например, **telnet**). Возможны две ситуации:

- предустановленные учетные данные — актуально для устройств сегмента **IoT**;
- слабые учетные данные — которые пользователь установил сам. Актуально всегда.

Важно не использовать подобные данные для аутентификации привилегированных пользователей.

## Оценка уязвимости

Каждая уязвимость в технических или программных решениях имеет свой рейтинг и идентификатор.

Общепринятый стандарт описания уязвимости — формат **CVE (Common Vulnerabilities and Exposures)**:

**CVE — год — номер**

Пример: **CVE-2017-0144**.

CVE поддерживает организация [MITRE](https://www.mitre.org/). На ее сайте можно посмотреть описание уязвимости и связанную с ней информацию:

CVE-ID	Идентификатор уязвимости
<b>CVE-2017-0144</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a> • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Map
Description	Описание
The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 ! 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulne described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.	
References	Ссылки
<b>Note:</b> <a href="#">References</a> are provided for the convenience of the reader to help distinguish between vulnerabilities. The list	
<ul style="list-style-type: none"><li>• EXPLOIT-DB:42030</li><li>• <a href="https://www.exploit-db.com/exploits/42030/">URL:https://www.exploit-db.com/exploits/42030/</a></li><li>• EXPLOIT-DB:42031</li><li>• <a href="https://www.exploit-db.com/exploits/42031/">URL:https://www.exploit-db.com/exploits/42031/</a></li></ul>	

Особо опасным уязвимостям присваиваются имена: уязвимость под номером CVE-2017-5754 — это Meltdown.

Чтобы оценивать уровень опасности, применяется стандарт CVSS. Каждой уязвимости присваивается вектор: для уязвимости CVE-2014-2363 это **AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H**. Также для уязвимости определяется уровень от 0 до 10. Чем выше этот показатель, тем опаснее уязвимость.

Используется две версии CVSS: 3 и 2. На рисунке — описание уязвимости CVE-2018-8349 с сайта <https://nvd.nist.gov>:

Impact	
CVSS v3.0 Severity and Metrics:	CVSS v2.0 Severity and Metrics:
Base Score: 8.8 HIGH	Base Score: 9.3 HIGH
Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H (V3 legend)	Vector: (AV:N/AC:M/Au:N/C:C/I:C/A:C) (V2 legend)
Impact Score: 5.9	Impact Subscore: 10.0
Exploitability Score: 2.8	Exploitability Subscore: 8.6
Attack Vector (AV): Network	Access Vector (AV): Network
	Access Complexity (AC): Medium

Дополнительно информацию об уязвимостях можно посмотреть на следующих ресурсах:

- [National Vulnerability Database](#);
- [Vulners.com](#);
- [БД уязвимостей ФСТЭК](#).

Информация об уязвимостях агрегируется и в описании обновлений на сайтах производителей ОС, где они были обнаружены. Обновление как мера для закрытия уязвимости — наиболее типичное решение. Например, уязвимость CVE-2018-8475 описывается на [странице Security update guide портала Microsoft](#). Здесь же можно просмотреть обновление, которое «закрывает» данную уязвимость:

Security Updates

The following software versions or editions are affected. Versions or editions that are not listed are either past their support life cycle or are not affected. To determine the support life cycle for your software version or edition, see the [Microsoft Support Lifecycle](#).

Product	Platform	Article	Download	Impact	Severity	Supersession
Windows 10 for 32-bit Systems		4457132	Ссылка на обновление: <a href="https://support.microsoft.com/ru-ru/help/4457132/windows-10-update-kb4457132">https://support.microsoft.com/ru-ru/help/4457132/windows-10-update-kb4457132</a>			
Windows 10 for x64-based Systems		KB4457132 (11 сентября 2018 г. (сборка ОС 10240.17976))				4343892
Windows 10 Version 1607 for 32-bit Systems		Имя обновления				4343887

Дата выпуска: Версия: 11 сентября 2018 г. Сборка ОС: 10240.17976

Улучшения и исправления

Следует понимать, что если уязвимость — результат действий пользователя, то в базу данных CVE она обычно не попадает. Например, если установили пароль «admin» при входе в систему.

## Поиск уязвимостей

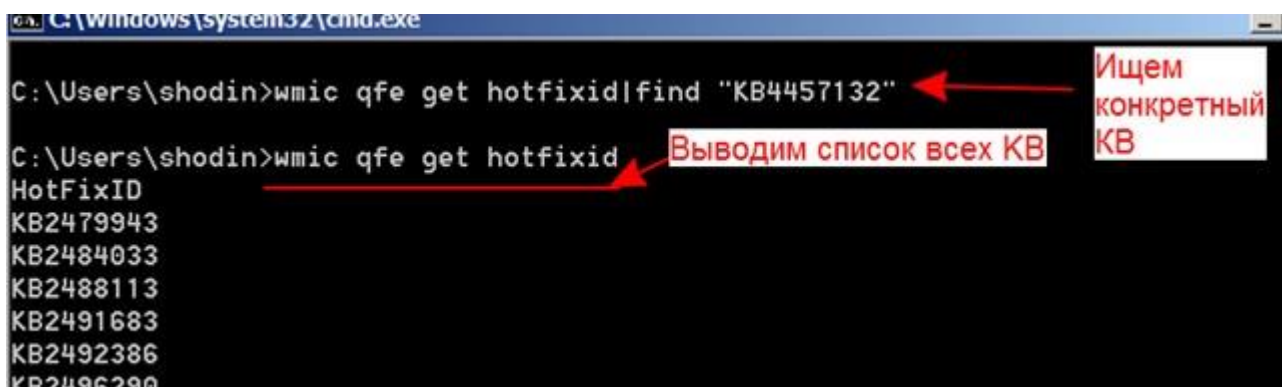
### Поиск уязвимостей по наличию обновлений

Самый простой способ обнаружить, подвержена система уязвимостям, — проверить, установлены ли обновления, которые закрывают их. Если нет — возможно, система уязвима. В Windows это можно выполнить командой:

```
wmic qfe get hotfixid
```

В этом случае выводится список всех установленных обновлений. Искать в этом перечне можно с помощью этой команды:

```
wmic qfe get hotfixid|find "KB4457132"
```



```
C:\Windows\system32\cmd.exe
C:\Users\shodin>wmic qfe get hotfixid|find "KB4457132"
C:\Users\shodin>wmic qfe get hotfixid
HotFixID
KB2479943
KB2484033
KB2488113
KB2491683
KB2492386
KB2496290
```

В системах на базе Debian Linux можно вывести список возможных обновлений и отфильтровать в них вывод по ключевому слову «security»:

```
sudo apt list --upgradable|grep security
```

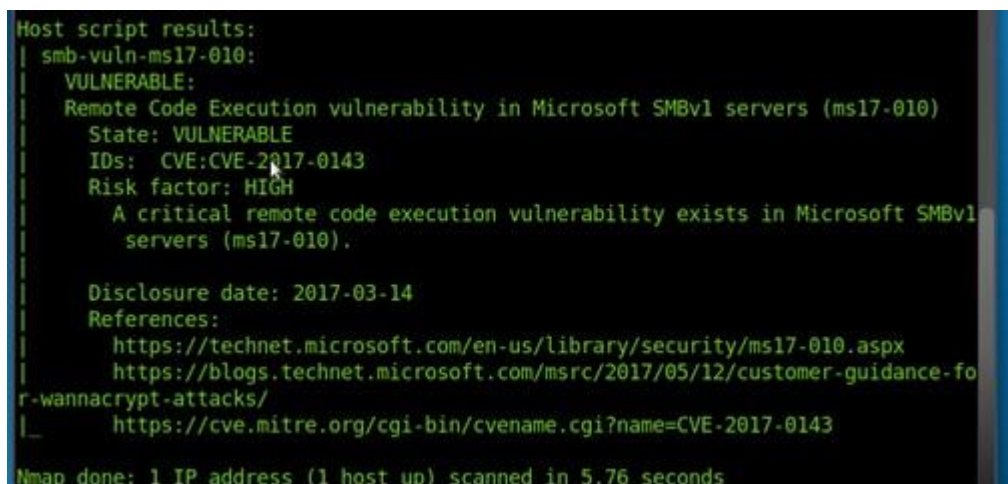
Чтобы искать уязвимость этим способом, нужно точно знать, какое обновление должно отсутствовать.

Если уязвимость серьезная, для нее может существовать плагин для сканера **nmap**. В таком случае команда следующая:

```
nmap --script smb-vuln-ms17-010.nse 192.168.56.1
```

- **--script smb-vuln-ms17-010.nse** — это имя сценария для тестирования на уязвимости;
- **192.168.56.1** — адрес тестируемого узла.

Резул



```
Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|       State: VULNERABLE
|       IDs:  CVE:CVE-2017-0143
|       Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|       servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-fo
|       r-wannacrypt-attacks/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_
Nmap done: 1 IP address (1 host up) scanned in 5.76 seconds
```

Полный список сценариев, эксплуатирующих различные уязвимости, можно посмотреть [на сайте nmap](#). Но не все уязвимости представлены в виде плагинов для сканера.

Гораздо практичнее искать уязвимости с помощью специальных программ-сканеров.

## Поиск уязвимости при помощи сканеров

Как правило, сканер содержит сценарии для поиска уязвимостей и движок, который проверяет по сценариям конечные узлы сети или локальный компьютер, если сканер не сетевой.

Стандарт при описании уязвимости — **OVAL (Open Vulnerability and Assessment Language)**, открытый язык описания и оценки уязвимостей. Он позволяет использовать один XML-файл, в котором уже описана уязвимость, метод ее определения, ссылка на патч, на CVE и многое другое. Этот формат стандартный, чтобы принимать информацию для сканеров безопасности. Официальный репозиторий правил можно [скачать с сайта OVAL](#).

Рассмотрим популярные сканеры и их функциональные возможности.

### Xspider

Разработка компании Positive Technologies с лицензией ФСТЭК. Особенности:

- контролирует изменения на сканируемых узлах и позволяет получить полную картину защищенности в динамике;
- проверяет слабость парольной защиты: выполняет оптимизированный подбор паролей практически во всех сервисах, требующих аутентификации;
- глубоко анализирует контент веб-сайтов, выявляет уязвимости в скриптах (SQLi и XSS, запуск произвольных программ);
- анализирует структуру HTTP-серверов, чтобы искать слабые места в конфигурации;
- выполняет расширенную проверку узлов под управлением Windows;
- проводит проверки на нестандартные DoS-атаки.

**Xspider** — платное решение.

### RedCheck

Разработка компании АЛТЭК-СОФТ, лицензированная ФСТЭК. Особенности:

- ищет уязвимости;
- ищет и устанавливает обновления;
- проводит инвентаризацию сети;
- контролирует целостность исполняемых файлов и служебных библиотек;
- сканирует сеть;
- подбирает пароли.

Это платный продукт.

### Nessus

Один из первых сканеров уязвимостей. Особенности:

- интегрируется с Metasploit;
- есть бесплатная версия для домашней сети и платная для корпоративной;
- экспортирует отчеты в различных форматах.

Платный продукт.

## OpenVAS

Большинство компонентов в **OpenVAS** — по лицензии GNU GPL, интегрирован в Kali Linux.

Особенности:

- интегрируется с Metasploit;
- экспортирует отчеты в различных форматах; • дает рекомендации, как устранить уязвимость;
- предустановлен в Kali linux.

Потребляете много ресурсов.

## Scan OVAL

**Scan OVAL** — утилита ФСТЭК для тестирования локального ПК на уязвимости. Особенности:

- сканирует ПК по базе данных OVAL;
- экспортирует отчеты.

Это пробная версия, сканирует только локальный ПК.

Практические рекомендации по выбору сканеров уязвимостей:

1. Сформулируйте цель сканирования — пентест или администрирование сети. Ряд сканеров оптимизированы именно для пентеста, и они, как правило, предустановлены в соответствующие ОС.
2. Определите, нужен ли сканер уязвимостей, лицензированный ФСТЭК. Это полезно, если сканирование на уязвимости будет частью процедуры, которая обеспечивает защиту конфиденциальной информации в организации (например, персональных данных).
3. Определите, как будет обрабатываться отчет об обнаруженных уязвимостях и надо ли его сохранять. Многие сканеры поддерживают экспорт результатов проверки в файл.
4. Решите, будут ли сканироваться хосты, сети и сетевые устройства. В некоторых случаях достаточно просканировать локальный хост, запустив на нем программу.

# OpenVAS

OpenVAS — это набор решений для комплексного сканирования сетевых ресурсов на уязвимости и управления найденными.

При помощи OpenVAS можно:



- искать известные уязвимости — с уже рассчитанным рейтингом CVSS по известным CVE — и получать рекомендации по их устранению;
- искать свежие уязвимости при периодических проверках;
- планировать проверки — например, проверять сервер в нерабочее время;
- создавать отчеты о результатах проверок — чтобы обосновать внедрение механизмов защиты;
- получать рекомендации по внедрению механизмов защиты.

OpenVAS — это в первую очередь сканер, который работает по правилам. Если для уязвимости нет правил NVT в базе OpenVAS, сканер ее обнаружить не сможет.

Пример отчета об обнаружении уязвимостей:


**Report: Results (277 of 278)**

ID: 43abd40f-5db4-4bae-965e-bf07838465ef  
Modified: [REDACTED]  
Created: [REDACTED]  
Owner: livedemo

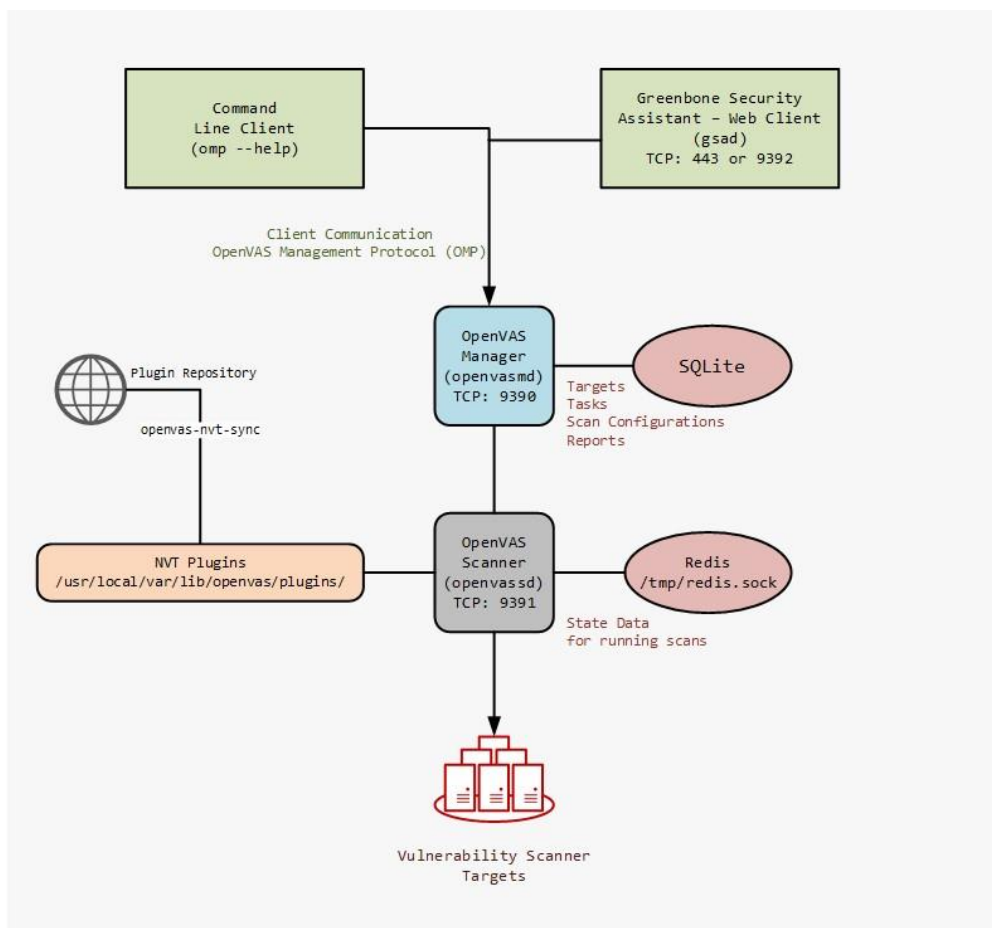
Vulnerability	Severity	QoD	Host	Location	Actions
Microsoft Windows SMB2 Negotiation Protocol Remote Code Execution Vulnerability	10.0 (Высокая)	98%	127.0.0.25	445/tcp	
Microsoft Windows SMB2 Negotiation Protocol Remote Code Execution Vulnerability	10.0 (Высокая)	98%	127.0.0.23	445/tcp	
Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote	10.0 (Высокая)	98%	127.0.0.46	445/tcp	
Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10.0 (Высокая)	98%	127.0.0.46	445/tcp	
Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote	10.0 (Высокая)	98%	127.0.0.26	445/tcp	
Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10.0 (Высокая)	98%	127.0.0.25	445/tcp	

## Состав компонентов OpenVAS

- OpenVAS Scanner;
- OpenVAS Manager;
- OpenVAS CLI;
- интерфейс **Greenbone security assistant**.

Взаимосвязи компонентов — [иллюстрация с сайта hackertarget](#):





## OpenVAS Scanner

Сервис для сканирования компонентов сети. Сканер ищет известные уязвимости по базе Network Vulnerability Tests (NVT), которая представляет обобщенную информацию о них. NVT можно считать правилами поиска уязвимостей. Основа работы сканера — конфигурационный файл **openvassd.conf**, который обычно расположен в каталоге **/usr/local/etc/openvas/**.

Управляют OpenVAS Scanner при помощи команды **openvassd**.

## OpenVAS Manager

Это основной сервис, который управляет сканером и позволяет сохранять результаты в sqlite-подобную БД. Обмениваться информацией между сканером и менеджером помогает специальный протокол **omp**. **OpenVAS Manager** выступает как прослойка между **OpenVAS Scanner** и его клиентами.

Управлять **OpenVAS Manager** можно при помощи команды **openvasmd**.

## OpenVAS CLI

Чтобы управлять этими компонентами, используется **OpenVAS CLI**. Это командная оболочка для работы сервисов OpenVAS.

OpenVAS можно управлять и из консоли: создавать задачи для сканирования, загружать отчеты о его результатах.

Протоколом **omp** управляют при помощи команды **omp**. **Greenbone**

## Security Assistant

Чтобы работать с OpenVAS было проще, используется web-интерфейс Greenbone Security Assistant. Это надстройка над **OpenVAS cli**, управлять которой можно через команду **gsad**.

## Правила для обнаружения уязвимостей

Чтобы обнаружить уязвимости, используются Network Vulnerabilities Tests (далее NVT). Это плагины — файлы вида **\*.nasl**, — написанные при помощи языка **nasl (Nessus Attack Scripting Language)**. Каждый NVT связан с уязвимостью, а у нее есть показатель рейтинга Severity. Он говорит об опасности угрозы, которую можно реализовать при помощи уязвимости.

Для одного из видов Shellshock, уязвимости CVE-2014-6278, есть NVT, который позволяет находить ее и связан с рейтингом CVSS для нее:

Name	Family	Created	Modified	Version	CVE	Severity	QoD
Cisco UCS GNU Bash Environment Variable Command Injection Vulnerability (Shellshock)	CISCO	Thu Mar 17 2016	Thu Aug 16 2018	\$Revision: 11008 \$	CVE-2014-6278	10.0	99%
Citrix XenServer Shellshock Security Update (CTX200223)	Citrix XenServer Local Security Checks	Thu Dec 18 2014	Fri Aug 24 2018	\$Revision: 11108 \$	CVE-2014-6271 CVE-2014-6277 CVE-2014-6278 CVE-2014-7169 CVE-2014-7186 CVE-2014-7187	10.0	97%
GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC) - 02	General	Wed Oct 8 2014	Sat Sep 15 2018	\$Revision: 11402 \$	CVE-2014-7169	10.0	100%
GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC) - 03	General	Wed Oct 1 2014	Sat Sep 15 2018	\$Revision: 11402 \$	CVE-2014-6278	10.0	100%
GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC) - 04	General	Wed Oct 8 2014	Sat Sep 15 2018	\$Revision: 11402 \$	CVE-2014-6277	10.0	100%
GNU Bash Off-by-one aka 'word_lineno' Buffer Overflow Vulnerability (LSC)	General	Wed Oct 1 2014	Sat Sep 15 2018	\$Revision: 11402 \$	CVE-2014-7187	10.0	50%
GNU Bash Stacked Redirects aka 'redir_stack' Memory Corruption Vulnerability (LSC)	General	Wed Oct 1 2014	Sat Sep 15 2018	\$Revision: 11402 \$	CVE-2014-7186	10.0	100%
McAfee Email Gateway - Bash Shellshock Code		Wed Jan	Fri Sep 7	\$Revision:	CVE-2014-6271 CVE-2014-6277 CVE-2014-6278		

Каждый NVT содержит следующую информацию (наиболее важные данные выделены жирным шрифтом):

- Наименование.** Обычно указывается имя NVT, например “GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC) – 04”.
- Время создания: Wed Oct 8 06:41:49 2014.
- Время изменения: Sat Sep 15 09:13:36 2018. Периодически параметры NVT переполняются и меняется показатель Severity для конкретного NVT.
- Резюме (Summary)** — описание уязвимости, с которой связан конкретный NVT: “This host is installed with GNU Bash Shell and is prone to remote command execution vulnerability”.
- Подверженное уязвимости ПО (Affected Software/OS): GNU Bash through 4.3 bash43-026.
- Количественная оценка уязвимости (Vulnerability Scoring).** Как правило, указывается в виде параметра CVSS: “CVSS base: 10.0. CVSS base vector: AV:N/AC:L/Au:N/C:C/I:C/A:C”. Чем выше оценка уязвимости по CVSS, тем она опаснее.
- Суть уязвимости (Vulnerability Insight).** Описание уязвимости и ее механизмов: “GNU bash contains a flaw that is triggered when evaluating environment variables passed from another

environment. After processing a function definition, bash continues to process trailing strings. Incomplete fix to CVE-2014-7169, CVE-2014-6271”.

8. **Метод определения уязвимости (Vulnerability Detection Method).** Описание метода определения уязвимости: “Login to the target machine with ssh credentials and check its possible to execute the commands via GNU bash shell”. Также указывается параметр качества воспроизведения уязвимости: “Quality of Detection: exploit (100 %)”.
9. **Влияние уязвимости (Impact).** Описание последствий от реализации уязвимости злоумышленником: “Successful exploitation will allow remote or local attackers to inject shell commands, allowing local privilege escalation or remote command execution depending on the application vector”.
10. **Возможное решение проблемы (Solution).** Возможные решения для найденной уязвимости.
11. Список справочных ссылок (CVE, Bugtraq ID, уведомления CERT), ссылки на заметки и переопределения, связанные с данным NVT. В разделе собрана полезная информация об уязвимости.

OpenVAS предлагает следующие возможные решения для проблем:

1. **Workaround** — есть описание конфигурации или сценария специальной установки, которое можно использовать, чтобы прикрыть уязвимость.
2. **Mitigation** — есть описание конфигурации или сценария специальной установки, которое можно использовать, чтобы снизить риск от эксплуатации уязвимости. Полностью не решает проблему с уязвимостью в затронутых продуктах.
3. **VendorFix** — есть официальное исправление от производителя затронутого продукта. Если нет специальных указаний, подразумевается, что исправление полностью устраняет уязвимость.
4. **NoneAvailable** — решение проблемы пока отсутствует. В сообщении должно быть объяснено, почему решения нет.
5. **WillNotFix** — исправления для уязвимости нет и не предвидится. Так бывает с устаревшими продуктами. В сообщении должно быть объяснено, почему решения нет в конкретном случае.

Чем полнее и актуальнее база NVT для OpenVAS, тем точнее результаты сканирования.

# Установка, настройка и администрирование OpenVAS в Kali Linux

## Установка OpenVAS в Kali Linux

OpenVAS устанавливается в Kali Linux при помощи этой команды:

```
apt-get install openvas
```

В системе появятся эти компоненты:

```
File Edit View Search Terminal Help
root@shokali:~# openvas
openvas-check-setup      openvas-portnames-update
openvas-feed-update      openvassd
openvas-manage-certs     openvas-setup
openvasmd                openvas-start
openvasmd-sqlite         openvas-stop
openvas-migrate-to-postgres
root@shokali:~# openvas
```

Далее необходимо выполнить команду **openvas-setup**. Установка проходит в три этапа:

- **Updating NVT** — обновление базы NVT;
- **Updating SCAP data** — обновление базы SCAP, которая содержит БД автоматизированного управления уязвимостями OpenSCAP (Security Content Automation Protocol);
- **Updating CERT data** — обновление сертификатов.

```
[>] Updating OpenVAS feeds
[*] [1/3] Updating: NVT Warning
Greenbone community feed server - http://feed.community.greenbone.net/
This service is hosted by Greenbone Networks - http://www.greenbone.net/

All transactions are logged.

If you have any questions, please use the Greenbone community portal.
See https://community.greenbone.net for details.

By using this service you agree to our terms and conditions.

Only one sync per time, otherwise the source ip will be temporarily blocked.

receiving incremental file list
plugin_feed_info.inc
  1,131 100%  1.08MB/s  0:00:00 (xfr#1, to-chk=0/1)

sent 43 bytes  received 1,234 bytes  510.80 bytes/sec
total size is 1,131  speedup is 0.89
[*] [2/3] Updating: Scap Data
```

В результате команды **openvas-setup** обновится база **NVT**, **scap** и сертификатов, перезапустится OpenVAS.

```
/var/run/openvasmd.pid (yet?) after start: No such file or directory
Oct 03 11:29:59 shokali systemd[1]: Started Open Vulnerability Assessment System
Manager Daemon.

[*] Opening Web UI (https://127.0.0.1:9392) in: 5... 4... 3... 2... 1...

[>] Checking for admin user

[+] Done
root@shokali:~#
```

При установке будет создан пользователь **admin**, пароль которого надо зафиксировать, так как он генерируется автоматически. В дальнейшем его можно будет изменить.

Потом автоматически откроется браузер со страницей входа в интерфейс Greenbone Security Assistance. Здесь надо ввести пароль пользователя **admin**, сгенерированный ранее. В дальнейшем запускать систему можно командой **openvas-start**.

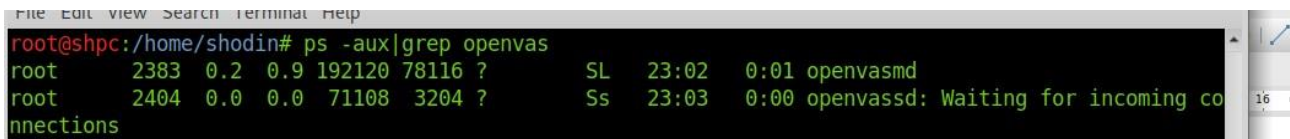
## Проверка работы сервисов OpenVAS

Для проверки необходимо проконтролировать запуск необходимых компонентов:

- OpenVAS Manager;
- интерфейс Greenbone security assistant;
- OpenVAS Scanner (опционально).

Запуск сервисов **OpenVAS manager** и **OpenVAS Scanner** можно проверить при помощи команды:

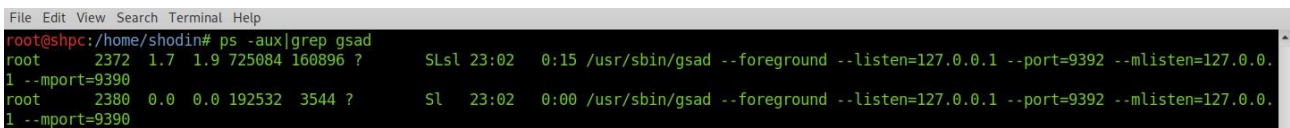
```
ps -aux|grep openvas
```



```
File Edit View Search Terminal Help
root@shpc:/home/shodin# ps -aux|grep openvas
root      2383  0.2  0.9 192120 78116 ?        SL   23:02   0:01 openvasmd
root      2404  0.0  0.0  71108  3204 ?        Ss   23:03   0:00 openvassd: Waiting for incoming co
nnections
```

Запуск сервиса **Greenbone Security Assistant** можно проверить при помощи команды:

```
ps -aux|grep gsad
```



```
File Edit View Search Terminal Help
root@shpc:/home/shodin# ps -aux|grep gsad
root      2372  1.7  1.9 725084 160896 ?        Ssl  23:02   0:15 /usr/sbin/gsad --foreground --listen=127.0.0.1 --port=9392 --mlisten=127.0.0.
1 --mport=9390
root      2380  0.0  0.0 192532  3544 ?        SL   23:02   0:00 /usr/sbin/gsad --foreground --listen=127.0.0.1 --port=9392 --mlisten=127.0.0.
1 --mport=9390
```

Если в системе запущен только OpenVAS и других сетевых сервисов нет, можно просмотреть активные сетевые соединения, которые используются компонентами. Поможет эта команда:

```
netstat -antp
```

щзут

Надо проконтролировать, что запущен **openvasmd** и интерфейс **Greenbone**. В примере интерфейс Greenbone запущен на http- и https-порты.

## Добавление и смена пароля пользователя

Сначала надо вывести список всех пользователей, чтобы узнать пользователей Openvas:

```
openvasmd -get-users
```

```
root@shokali:~# openvasmd --get-users
admin
root@shokali:~#
```

Чтобы создать нового пользователя, используется эта команда:

```
openvasmd --create-user=student
```

```
root@shokali:~# openvasmd --create-user=student
User created with password '7db58002-7ed2-409d-bd56-227276d90064'.
root@shokali:~#
```

Сменить пароль у пользователя можно при помощи такой команды:

```
openvasmd --user=student --new-password=admin123.
```

После этого необходимо перезапустить **openvas** командами **openvas-stop** и **openvas-start**. Теперь можно войти в систему с новым паролем.

## Практическая часть

Сканируя систему, злоумышленника ищет такие уязвимости, эксплуатация которых позволит ему обойти механизмы безопасности и развить атаку. Он может проводить:

- **Сканирование, которому не задаются параметры.** Цель — определить сущности, которые можно использовать, чтобы проникнуть на атакуемый узел. Как правило, при таком виде сканирования собираются сведения для более глубокого исследования: достаточно добыть информацию о версиях ОС. Или извлекается максимум информации о всех уязвимостях, если время исследования не критично.
- **Глубокое сканирование.** При этом злоумышленнику известны параметры сканирования: например, тип и версия ОС исследуемого хоста. Задача при организации такого сканирования — поиск конкретных уязвимостей (например, присущих определенной ОС).

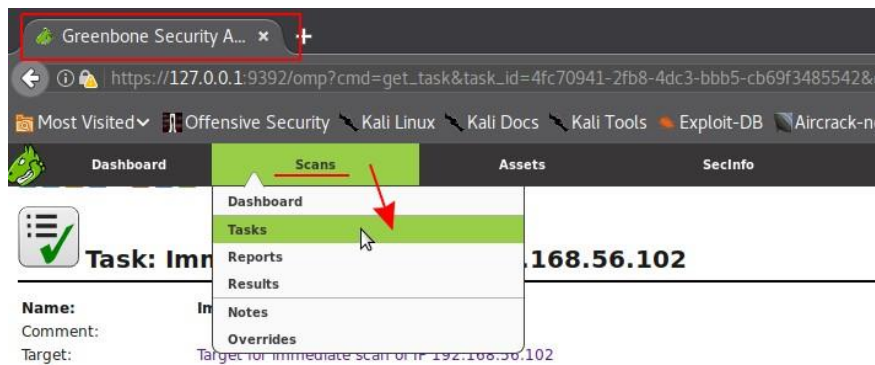
Рассмотрим способы организации этих видов сканирования.

### Задание 1. Быстрое сканирование (immediate scan)

Обычно об исследуемом узле не известно ничего, кроме его имени или адреса. Поэтому в OpenVAS есть мастер сканирования, при помощи которого можно быстро организовать исследование узла или их группы, не думая о настройках. Для этого необходимо:

Перейти в раздел **Scans — Tasks** в интерфейсе Greenbone Security Assistance.

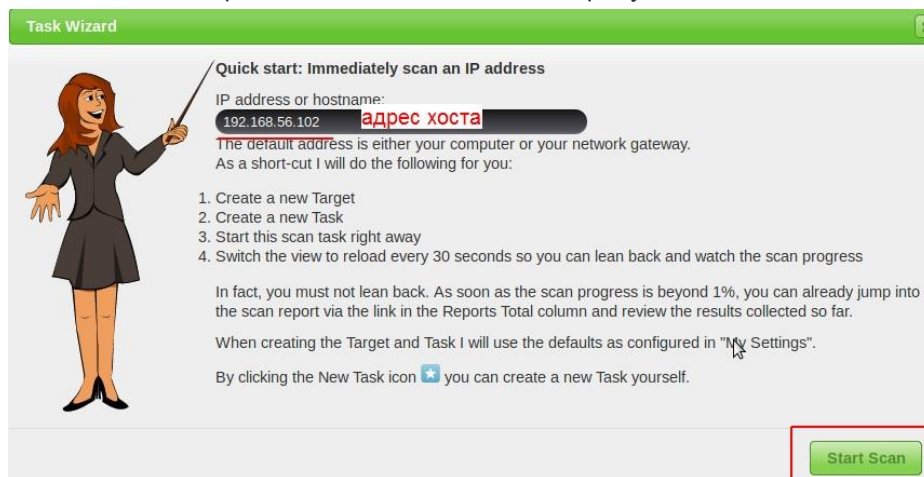




В нем запустить мастер создания задач (Task Wizard):



В открывшемся окне вводим параметры хоста и нажимаем кнопку **Start Scan**. После этого будет автоматически выполнено четыре действия, изложенных на рисунке ниже:



Остается только дождаться результатов сканирования. При данном способе сканирования задача создается с профилем **Full and fast**, в котором содержатся 47556 правил NVT для сканирования.

Сканирование может быть долгим. По его завершении можно увидеть максимальный рейтинг Severity для найденных уязвимостей, открыть задачу и посмотреть подробности:

Immediate scan of IP 192.168.56.1	Stopped at 1 %	0 (1)	date	max severity	
Immediate scan of IP 192.168.56.102	Done	1 (1)	Jul 28 2018	10.0 (High)	
Immediate scan of IP 192.168.56.104	1 %				

В подробной сводке указано общее время сканирование и предоставлены отчеты для просмотра:



**Task: Immediate scan of IP 192.168.56.102**

**Имя задачи**

**Name:** Immediate scan of IP 192.168.56.102

**Comment:**

**Target:** Target for immediate scan of IP 192.168.56.102

**Alerts:**

**Schedule:** (Next due: over)

**Add to Assets:** yes

**Apply Overrides:** yes

**Min QoD:** 70%

**Alterable Task:** no

**Auto Delete Reports:** Do not automatically delete reports

**Scanner:** OpenVAS Default (Type: OpenVAS Scanner)

**Scan Config:** Full and fast

**Order for target hosts:** N/A

**Network Source Interface:**

**Maximum concurrently executed NVTs per host:** 10

**Maximum concurrently scanned hosts:** 30

**Status:** Done

**Duration of last scan:** 43 minutes 37 seconds

**Average scan duration:** 43 minutes 37 seconds

**Reports:** 1 (Finished: 1, Last: Jul 28 2018)

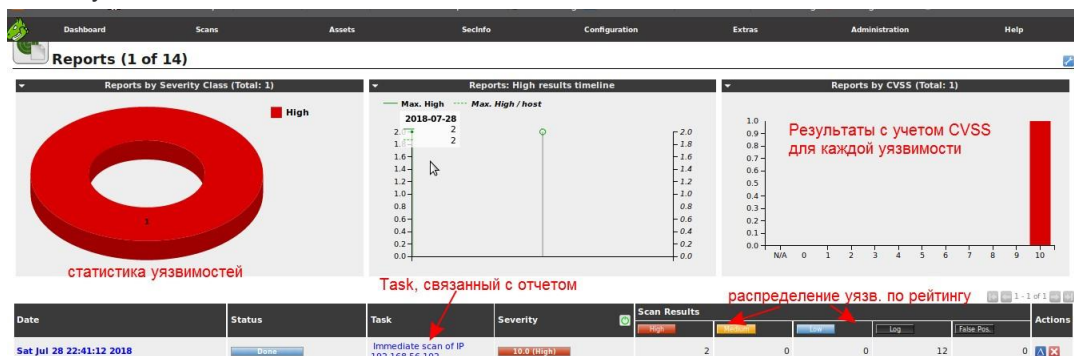
**Results:** 14

**Notes:** 0

**время сканирования**

**отчеты**

Далее по ссылке из раздела Reports можно просмотреть отчет с подробной информацией об обнаруженных уязвимостях:



По ссылке из раздела Date расположена более подробная сводка. По умолчанию отображаются уязвимости с параметром **Quality of detection** не ниже 70 %. Это можно убрать в настройках фильтра:

**Greenbone Security Assistant**

**Dashboard** **Scans** **Assets** **Secinfo** **Configuration** **Extras** **Administration** **Help**

**Filter:** **фильтр**

**по умолчанию установлен Quality of Detection в 70%**

**Report: Results (2 of 15)**

**уязвимости**

Vulnerability	Severity	QoD	Host	Location	Actions
OS End Of Life Detection	10.0 (High)	80%	192.168.56.102	general/tcp	
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95%	192.168.56.102	445/tcp	

Чтобы ознакомиться с информацией о найденной уязвимости, надо перейти по ссылке с ее именем. В открывшемся окне будет описание уязвимости и решение, которое предлагает OpenVAS:

**Result: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)**

Vulnerability	Severity	QoD	Host	Location	Actions
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95%	192.168.56.102	445/tcp	

**Summary** **Общая информация об уязвимости**

This host is missing a critical security update according to Microsoft Bulletin MS17-010.

**Vulnerability Detection Result**

Vulnerability was detected according to the Vulnerability Detection Method.

**Impact** **Описание влияния уязвимости**

Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.

Impact Level: System

**Solution** **Решение**

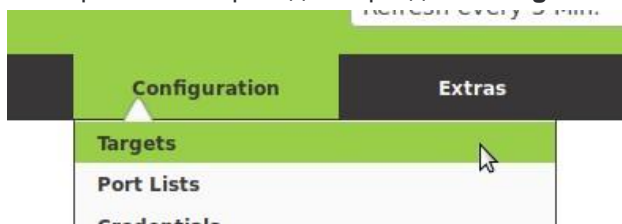
**Solution type:** VendorFix

## Задание 2. Задать цель вручную и провести сканирование цели

Заранее настроить цель сканирования полезно, если:

- о цели сканирования уже собрана информация, и это может сократить время процедуры;
- необходимо задать параметры сканирования — например, данные для подключения к хосту;
- при планировании периодических проверок ресурсов одного и того же хоста на наличие в нем уязвимостей.

Создадим новую цель для сканирования. Переходим в раздел **Configuration — Targets**:



Выбираем пиктограмму New Target:



Цель можно задать списком адресов, указать параметры сервисов, которые будем использовать при сканировании (логин/пароль для SSH).

A screenshot of the 'New Target' configuration form. The form has several sections: 'Name' (with 'Debian Web Vuln VM' entered), 'Comment', 'Hosts' (with 'Manual' selected and '192.168.56.101' entered), 'Exclude Hosts', 'Reverse Lookup Only', 'Reverse Lookup Unity', 'Port List' (with 'All IANA assigned TCP 20...' selected), 'Alive Test' (with 'Scan Config Default' selected), and 'Credentials for authenticated checks' (with fields for SSH, SMB, ESXi, and SNMP). Red arrows point to various fields with labels: 'Имя для цели' points to the Name field, 'адрес цели' points to the Hosts field, 'порты для анализа' points to the Port List field, 'как будет проверяться доступность' points to the Alive Test field, and 'данные для сервисов (логин и т.п.)' points to the Credentials fields. A 'Create' button is at the bottom right.

Цель добавится в список:

Targets (2 of 2)				
Name	Hosts	IPs	Port List	Credentials - sort by: SSH
Debian Web Vuln VM	192.168.56.101	1	All IANA assigned TCP 2012-02-10	
Target for immediate scan of IP 192.168.56.101	192.168.56.101	1	OpenVAS Default	

Когда добавили цель, можно создать новую задачу для сканирования через меню **Scans — Tasks**:



Когда добавляем задачи, выбираем созданную ранее цель. Цели подставляются из меню **Targets**. Для сканирования используются две важные настройки: сканер и его конфигурация. При создании задачи добавляется параметр QoD (в %) как фильтр для отчета. В дальнейшем фильтр можно изменить.

Когда настраиваем конфигурацию сканирования, значения берем из меню **Configuration — Scan config**. Все конфигурации, которые можно создавать самостоятельно, отличаются по количеству NVT.

Их число можно изменять при создании нового конфига, так как оно прямо влияет на время сканирования.

**Scan Configs (8 of 8)**

число NVT в конфиге

Name	Families		NVTs		Action
	Total	Trend	Total	Trend	
<b>Discovery</b> (Network Discovery scan configuration.)	22		2362		
<b>empty</b> (Empty and static configuration template.)	0		0		
<b>Full and fast</b> <span style="color: red;">имя конфига</span> (Most NVTs; optimized by using previously collected information.)	62		47549		
<b>Full and fast ultimate</b> (Most NVTs including those that can stop services/hosts; optimized by using previously collected information.)	62		47549		
<b>Full and very deep</b> (Most NVTs; don't trust previously collected information; slow.)	62		47549		

Созданную задачу можно запустить и затем проанализировать результат.

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
<b>Immediate scan of IP 192.168.56.101</b>	Done	1 (1)	Oct 4 2018	7.5 (High)		
<b>web scan</b> <span style="color: red;">Новая задача</span>	New					<span style="color: red;">ее надо запустить вручную</span>

Отметим, что отчет о сканировании с учетом примененных фильтров, например QoD ≤ 5 %, можно выгрузить в нескольких форматах, в том числе PDF.

Dashboard	Scans	Assets	Settings	Configuration	Extras	Administration	Help
PDF		Filter:		autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort=reverse=severity levels=hmlg min_qod=5 timezone=UTC			
Download filtered Report				ID: 60b54097-4b49-481e-bfe4- Modified: Thu Oct 4 19:00:04 2018 Created: Thu Oct 4 18:41:53 2018 Owner: admin			
Report: Results (64 of 64)							
Vulnerability	Severity	QoD	Host	Location			
phpMyAdmin End of Life Detection (Linux)	10.0 (High)	30%	192.168.56.101	80/tcp			
OpenSSH Multiple Vulnerabilities	8.5 (High)	30%	192.168.56.101	22/tcp			
OpenSSH Denial of Service And User Enumeration Vulnerabilities (Linux)	7.8 (High)	30%	192.168.56.101	22/tcp			
phpinfo() output accessible	7.5 (High)	80%	192.168.56.101	80/tcp			

## Задание 3. Создать конфиг для сканирования узла с ОС Debian Linux и просканировать узел

Предположим, что точно знаем тип ОС на хосте и данные для подключения к нему. В этом случае можно провести более глубокое сканирование узла, которое позволит выявить уязвимости, недоступные для внешнего сканирования. Это полезно, чтобы:

- организовать периодические проверки хоста на уязвимости;
- задать правила для поиска уязвимостей в конкретной ОС. Это сократит время сканирования.

Недостаток данного метода в том, что надо знать о хосте дополнительную информацию — как минимум тип ОС.

Создадим новый конфиг в меню **Configuration — Scan configs**:



New Scan Config

Name

Debian scan

Comment

Base

☐ Empty, static and fast
☒ Full and fast

Create

Зададим имя и шаблон конфига для основы. После этого конфиг добавится в список. Нужно прикрепить к нему NVT, которые отвечают за сканирование Debian, и убрать лишние NVT, сняв флажки. Чтобы проверить Debian, не нужны NVT для других ОС.

Из раздела **Port scan** добавим два компонента: **Nmap (NASL wrapper)** и **Ping host**. Созданный набор сохраняем.

CentOS Local Security Checks	2459 of 2459				
Citrix XenServer Local Security Checks	30 of 30				
Compliance	7 of 7				
Databases	537 of 537				
Debian Local Security Checks	2797 of 2797				
Default Accounts	214 of 214				
Denial of Service	1348 of 1348				
F5 Local Security Checks	125 of 125				
FTP	172 of 172				
Fedora Local Security Checks	10514 of 10514				
Finger abuses	6 of 6				
Firewalls	18 of 18				
FortiOS Local Security Checks	34 of 34				
FreeBSD Local Security Checks	437 of 437				
Gain a shell remotely	105 of 105				
General	4267 of 4268				
Gentoo Local Security Checks	693 of 693				
HP-UX Local Security Checks	15 of 15				

Чтобы сканировать ОС на наличие уязвимостей или неустановленных обновлений, рекомендуем задать данные для подключения — например, по **SMB** или **SSH**. Для этого переходим в раздел **Configuration — Credentials**.



Создадим новый набор данных для подключения:

The image shows a 'New Credential' form with the following fields and options:

- Name:** ssh creds *Имя*
- Comment:** (empty field)
- Type:** Username + Password *Тип данных*
- Allow insecure use:** ☒ Yes ☐ No *Разрешим небезопасную передачу*
- Auto-generate:** ☐ Yes ☒ No
- Username:** student *Имя пользователя*
- Password:** (masked with dots)
- Create:** (button)

Добавим новую задачу для сканирования (**Scans — Task — Advanced Task Wizard**) и прикрепим к ней конфиг и набор данных для подключения к SSH:



**Advanced Task Wizard**

I can help you by creating a new scan task and automatically starting it.

All you need to do is enter a name for the new task and the IP address or host name of the target, and select a scan configuration.

You can choose if you want me to run the scan immediately, schedule the task for a later date and time, or just create the task so you can run it manually later.

In order to run an authenticated scan, you have to select SSH and/or SMB credentials, but you can also run an unauthenticated scan by not selecting any credentials.

**Quick start: Create a new task**

Task Name: Debian Scan **Имя задачи**

Scan Config: Debian scan **Созданный конфиг**

Target Host(s): 192.168.56.102

Start time: ☒ Start immediately  
☐ Create Schedule  
 Monday, 8 October, 2018  
 at 20 h 40 m  
 Coordinated Universal Time  
☐ Do not start automatically

SSH Credential: ssh creds on port 22

SMB Credential: --

ESXi Credential: --

Email report to: --

**созданный набор данных для подключения**

В дальнейшем можно применять этот набор данных для подключения не только для SSH. Созданные через wizard задачи запускаются автоматически, остается дожидаться результатов сканирования.

**Report: Results (42 of 126)**

ID: 5f31ba30-12a5-4cd7-9fac-216ff1fa  
 Modified: Sat Oct 6 18:51:22 2018  
 Created: Sat Oct 6 18:27:47 2018  
 Owner: admin

Vulnerability	Severity	QoD	Host	Location	Action
Debian Security Advisory DSA 4187-1 (linux - security update)	10.0 (High)	97%	192.168.56.102	general/tcp	
Debian LTS Advisory ([SECURITY] [DLA 1500-1] openssl security update)	8.5 (High)	97%	192.168.56.102	general/tcp	
phpinfo() output accessible	7.5 (High)	80%	192.168.56.102	80/tcp	
Debian LTS Advisory ([SECURITY] [DLA 1455-1] mutt security update)	7.5 (High)	97%	192.168.56.102	general/tcp	
Debian LTS Advisory ([SECURITY] [DLA 1447-1] libidn security update)	7.5 (High)	97%	192.168.56.102	general/tcp	
Debian LTS Advisory ([SECURITY] [DLA 1397-1] php5 security update)	7.5 (High)	97%	192.168.56.102	general/tcp	
Debian LTS Advisory ([SECURITY] [DLA 1415-1] phpmyadmin security update)	7.5 (High)	97%	192.168.56.102	general/tcp	
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.	7.5 (High)	95%	192.168.56.102	80/tcp	
Debian Security Advisory DSA 4082-1 (linux - security update)	7.2 (High)	97%	192.168.56.102	general/tcp	
Debian Security Advisory DSA 4196-1 (linux - security update)	7.2 (High)	97%	192.168.56.102	general/tcp	
Debian LTS Advisory ([SECURITY] [DLA 1394-1] imagemagick security update)	6.9 (Medium)	97%	192.168.56.102	general/tcp	
Debian LTS Advisory ([SECURITY] [DLA 1411-1] tiff security update)	6.9 (Medium)	97%	192.168.56.102	general/tcp	

## Выводы

Мы рассмотрели базовые особенности сканера OpenVAS:

- изучили состав и структуру компонентов OpenVAS;
- узнали, как просканировать ОС на уязвимости;
- создали конфигурации для сканирования, при помощи которых можно расширять и сужать круг уязвимостей для обнаружения;
- научились использовать регистрационные данные, чтобы подключаться к удаленной системе и расширять зону покрытия сканирования.

Сканер можно применять шире:

- установить OpenVAS в ОС Linux, отличную от Kali Linux, и использовать его как отдельное решение для сканирования сетевых ресурсов;
- планирования с помощью OpenVAS стратегию внедрения политики безопасности и приоритизации рисков;

- использовать OpenVAS в сочетании с **metasploit**, если требуется единая платформа для анализа защищенности сети.

## Практическое задание

1. Установить OpenVAS в Kali Linux.
2. Установить систему DVL Linux в качестве виртуальной машины (ссылка для скачивания [https://sourceforge.net/projects/virtualhacking/files/os/dvl/DVL\\_1.5\\_Infectious\\_Disease.iso/download](https://sourceforge.net/projects/virtualhacking/files/os/dvl/DVL_1.5_Infectious_Disease.iso/download) , можно просто загрузиться с iso образа), настроить сетевой доступ к ней со стороны Kali Linux и просканировать систему DVL Linux на наличие уязвимостей. Формат сдачи - отчет OpenVAS в формате pdf или html.
3. \* Установить виртуальную машину на базе Windows 7 (8, 8.1 или 10), активировать сетевой доступ к общим папкам. Просканировать VM при помощи OpenVAS с использованием данных протокола SMB. Формат сдачи - отчет OpenVAS в формате pdf или html.

Задание со звездочкой\* — повышенной сложности.

## Дополнительные материалы

1. [Описание Openvas CLI.](#)
2. [Советы по настройке и использованию OpenVAS из командной строки.](#)
3. [Развертывание OpenVAS.](#)
4. [Сканирование сети \(а не отдельного узла\) в OpenVAS.](#)
5. [О развертывании и использовании OpenVAS в Windows-подобной среде.](#)
6. [Как просканировать узел на наличие уязвимости к WannaCry.](#)

## Используемая литература

1. [https://ru.wikipedia.org/wiki/Переполнение\\_буфера](https://ru.wikipedia.org/wiki/Переполнение_буфера).
2. <https://www.veracode.com/security/buffer-overflow>.
3. <https://habr.com/company/1cloud/blog/252991/>.
4. <https://habr.com/post/136046/>.
5. <https://nmap.org/nsedoc/categories/vuln.html>.
6. <https://linuxide.com/linux-how-to/install-security-updates-ubuntu/>.
7. <https://vulners.com/help>.
8. <https://www.ptsecurity.com/ru-ru/products/xspider/>.
9. <http://www.openvas.org/software.html>.



10. <https://www.kali.org/penetration-testing/openvas-vulnerability-scanning/>.
11. <http://www.irongeek.com/i.php?page=backtrack-r1-man-pages/openvasmd>.
12. <http://www.irongeek.com/i.php?page=backtrack-r1-man-pages/openvasd>.
13. <http://www.irongeek.com/i.php?page=backtrack-r1-man-pages/gsad>.
14. <https://habr.com/company/pentestit/blog/323568/>.