Как использовать Nessus для сканирования уязвимостей в Ubuntu 22.04

Nessus — это один из самых известных и широко используемых сканеров уязвимостей в мире. Разработанный компанией Tenable, Inc., Nessus предоставляет комплексное решение для обнаружения уязвимостей, позволяя организациям и индивидуальным пользователям идентифицировать и устранять потенциальные угрозы безопасности в их сетевой инфраструктуре. С его помощью можно проводить глубокий анализ безопасности, охватывая различные аспекты, от простого обнаружения уязвимостей до сложных проверок на соответствие стандартам безопасности.

Версии Nessus: Essentials, Professional, Expert

- Nessus Essentials. Бесплатная версия, предназначенная для домашних пользователей и тех, кто только начинает знакомство с областью безопасности. Эта версия предоставляет базовые функции сканирования и обнаружения уязвимостей.
- Nessus Professional. Платная версия, предназначенная для профессионалов в области безопасности и крупных организаций. Она предлагает расширенные функции, такие как возможность сканирования больших сетей, интеграция с другими системами безопасности и дополнительные инструменты для анализа и отчетности.
- Nessus Expert.Это премиальная версия, которая включает в себя все функции Professional, а также дополнительные инструменты и возможности, такие как поддержка облачного сканирования, интеграция с системами управления инцидентами безопасности и дополнительные опции настройки.

Nessus предлагает следующий набор функций для сканирования уязвимостей:

- Обнаружение уязвимостей: Nessus обнаруживает уязвимости в различных системах и приложениях на основе своей базы данных известных уязвимостей.
- Проверка на соответствие: Nessus проводит проверки на соответствие различным стандартам безопасности и регулированиям.
- Интеграция с другими системами: предоставляется возможность интеграции с системами управления инцидентами, системами управления журналами и другими инструментами безопасности.
- Облачное сканирование: Версия Nessus Expert позволяет проводить сканирование в облачных средах, таких как AWS, Azure и Google Cloud.
- Визуализация данных: Nessus включает в себя дашборды и отчеты для представления результатов сканирования.
- Регулярные обновления: Nessus обновляет свою базу данных уязвимостей для отслеживания новых угроз.
- Гибкая настройка: предоставляет опции настройки для адаптации процесса сканирования к конкретной среде.

Установка Nessus

Nessus можно установить на Ubuntu двумя способами: как docker-контейнер и как deb-пакет. Рассмотрим оба способа.

Установка Nessus на Ubuntu через Docker

1. Подготовка к установке. Прежде всего, убедитесь, что на вашей системе установлен Docker.

2. Скачивание образа. Загрузите последнюю версию образа Nessus из Docker Hub, выполнив следующую команду:

```
docker pull tenable/nessus:latest-ubuntu
```

Загрузка может занять около 10 минут.

3. Создание и запуск контейнера. После того как образ загружен, создайте и запустите контейнер с помощью следующей команды:

```
docker run --name "nessus_tw" -d -p 8834:8834 tenable/nessus:latest-ubuntu
```

Где:

- `--name "nessus_tw"` задает имя контейнера.

- `-d` указывает Docker запускать контейнер в фоновом режиме.
- `-p 8834:8834` проксирует порт 8834 из контейнера на порт 8834 хоста, делая приложение доступным на localhost:8834.

4. Запуск контейнера после остановки. Если вам потребуется запустить контейнер после его остановки, используйте команду:

```
docker start nessus_tw
```

Установка Nessus в Ubuntu как deb-пакет

> Напомним, что для загрузки установщика с сайта tenable.com на сервере должен быть запущен VPN.

1. Скачивание установочного пакета: Сначала загрузим установочный пакет для Ubuntu с помощью команды `curl`:

```
curl --request GET \
  --url 'https://www.tenable.com/downloads/api/v2/pages/nessus/files/Nessus-10.6.1-ubuntu1404_am
  --output 'Nessus-10.6.1-ubuntu1404_amd64.deb'
```

2. Установка Nessus. Установочный файл Nessus был загружен в текущую директорию. Теперь используем `dpkg` для установки Nessus на нашу машину с Ubuntu. Введите следующую команду для установки:

```
sudo dpkg -i ./Nessus-10.6.1-ubuntu1404_amd64.deb
```

3. Запуск службы Nessus. После установки необходимо запустить службу Nessusd. Введите следующую команду:

```
sudo systemctl start nessusd.service
```

4. Проверим корректность работы nessusd. Выполним `systemctl status nessusd` и убедимся, что служба запущена и работает без ошибок:

```
Active: active (running)
```

5. Доступ к Nessus через браузер. Теперь вы можете получить доступ к Nessus в вашем локальном браузере по адресу `https://localhost:8834/`

> Порт 8834 является портом по умолчанию для Nessus. В большинстве браузеров при попытке доступа к Nessus может появиться предупреждение о безопасности с предложением вернуться назад. Однако

> это полностью безопасно, и вы можете нажать на «Дополнительно» и затем продолжить работу с веб-сайтом.

Первоначальная настройка Nessus

1. Переход на страницу настройки. После запуска контейнера откройте браузер и перейдите по адресу `https://localhost:8834`. Вы увидите, что выполняется загрузка необходимых компонентов.
2. Регистрация на сайте Tenable. Пока идет загрузка необходимых компонентов, рекомендуется зарегистрироваться на официальном сайте Tenable для получения кода активации. После регистрации код будет отправлен на указанный вами электронный адрес.

> “ При регистрации необходимо использовать ящик на домене, отличном от .ru.

3. Использование мастера установки.

- Как только компоненты загрузятся, начнется процесс настройки с помощью мастера установки. Нажмите «Continue».

  a6052b12-52ba-4ed8-b4df-09a36de9685b?width=1280&height=894

- Выберите версию «Nessus Essentials».

  37a4b461-d860-4bdf-b9db-e2e497d28d99?width=1279&height=991

- Введите код активации, который был отправлен на вашу электронную почту.

  54a20a24-8ac0-4c2e-ba69-6beebc496487?width=1280&height=990

- Создайте учетную запись пользователя, указав имя и пароль.

  b8609651-970b-449d-bf55-f45784d390a0?width=1278&height=987

4. Завершение установки. Дождитесь завершения установки и загрузки всех плагинов. Как только все процессы на странице https://localhost:8834/#/settings/about/events будут завершены, установка Nessus будет полностью завершена.

Настройка сервера beeBox

После успешной установки и настройки Nessus настало время проверить его в действии. Для этого нам потребуется целевая система, которую мы будем сканировать на наличие уязвимостей. В рамках этой статьи мы решили использовать виртуальную машину bee-box.

bee-box — это специализированная виртуальная машина на базе bWAPP (buggy web application). bWAPP создано специально с уязвимостями, что позволяет специалистам по безопасности, разработчикам и студентам практиковаться в обнаружении и предотвращении угроз. В beeBox представлены следующие уязвимости:

- Injection (HTML/SQL/LDAP/SMTP/…)
- Broken Authentication & Session Management
- Cross-Site Scripting (XSS)
- Insecure Direct Object References
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross-Site Request Forgery (CSRF)
- Using Components with Known Vulnerabilities
- Unvalidated Redirects & Forwards
- XML External Entity Attacks (XXE)
- Server-Side Request Forgery (SSRF)

Это делает beeBox идеальным инструментом для демонстрации возможностей Nessus.

Установка bee-box в VirtualBox

В этом разделе мы рассмотрим процесс установки bee-box в VirtualBox версии 7.0. Отметим, что в других версиях VirtualBox процедура может незначительно отличаться.

1. Скачивание образа. Сначала скачайте образ виртуальной машины beeBox (файл bee-box_v1.6.7z) и распакуйте его.
2. Создание новой виртуальной машины. Запустите VirtualBox и нажмите кнопку «New». В разделе «Name and Operating System» укажите имя машины, выберите тип ОС Linux и версию «Oracle Linux (64-bit)».

   9f379244-c1ee-401c-9008-a4005266f4b1?width=712&height=605

3. Настройка оборудования. Выделите 1024 МБ RAM и 1 CPU.

   e796e1e5-0167-4f27-8d33-1495957eda4f?width=708&height=603

4. Выбор жесткого диска. В разделе «Hard Disk» выберите «Use an Existing Virtual Hard Disk File», затем «Add» и укажите путь к файлу `bee-box.vmdk`, который вы распаковали ранее.

ea5f0ee0-41c9-4f25-986e-391ac1d036f6?width=956&height=807

5. Настройка сети. Перед запуском машины перейдите в «Settings» -> «Network» и измените «Attached to» с «NAT» на «Bridged Adapter».

334e7edc-4ab5-4dee-901d-29761064f1af?width=946&height=437

6. Запуск виртуальной машины. Нажмите «Start» для запуска.

7. Настройка раскладки клавиатуры. После загрузки рабочего стола кликните на «USA» в верхнем меню, выберите «Keyboard Preferences», затем «Layouts» и в «Keyboard model» укажите «IBM Rapid Access II».

79c158a5-bf6a-4d33-8125-04ab67bae973?width=512&height=555

8. Получение IP-адреса. Откройте терминал и введите команду ip a для определения IP-адреса виртуальной машины. Затем обратитесь к этому IP с вашей основной машины, чтобы убедиться в доступности приложения.

5caaa196-7dab-420b-abc9-fff7323c70c9?width=660&height=461

Сканирование с использованием Nessus

Общие параметры Nessus

Перед тем как приступить к использованию Nessus, важно ознакомиться с его интерфейсом и настройками. Главный экран программы разделен на две основные вкладки: «Scans» и «Settings». Для начала давайте подробно рассмотрим раздел «Settings».

About:

- Overview. Этот подраздел предоставляет общую информацию о вашей установке Nessus, включая версию, детали лицензии и другую ключевую информацию.
- License Utilization. Здесь отображаются все IP-адреса, которые были просканированы. В бесплатной версии доступно сканирование до 16 хостов. Хосты, которые не сканировались в течение 90 дней, автоматически освобождаются из лицензии.
- Software Update. Позволяет настроить автоматическое обновление или запустить процесс обновления вручную.
- Encryption Password. Здесь можно установить пароль для шифрования данных Nessus. Если вы решите установить пароль, то вам необходимо запомнить его, так как без него восстановление данных будет невозможно.

- Events. Этот подраздел позволяет просматривать историю обновлений и другие ключевые события.

Advanced Settings:

- Этот раздел содержит дополнительные настройки Nessus. Хотя мы не будем подробно рассматривать каждую из них в этой статье, вы можете найти подробную информацию о каждой настройке на официальном сайте.

Proxy Server:

- Если ваша сеть требует использование прокси-сервера для доступа к интернету или целевым серверам, вы можете настроить параметры прокси в этом разделе.

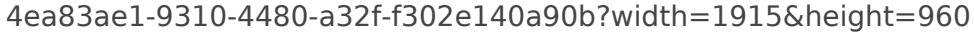
SMTP Server:

- Здесь можно настроить параметры SMTP-сервера, чтобы Nessus мог отправлять уведомления по электронной почте о результатах сканирования и других важных событиях.

Запуск базового сканирования

Теперь перейдем во вкладку Scans. Перед тем как приступить к использованию Nessus для сканирования уязвимостей, необходимо правильно настроить параметры сканирования. Это обеспечит максимальную эффективность и точность в обнаружении уязвимостей.

На главном экране нажмем на кнопку New Scan и попадем в мастер создания сканирования.



Выбор типа сканирования. Для нашего примера выберем Basic Network Scan.

Общие настройки

- General. Задайте имя, описание, выберите папку для результатов и в Targets укажите IP-адрес виртуальной машины bee-box.

- Schedule. Здесь можно настроить периодичность сканирования (опционально).
- Notifications. Укажите почтовые адреса для уведомлений. Для работы этой функции необходимо настроить подключение к SMTP-серверу в настройках.

Детальные настройки

- Discovery. Тут мы можем выбрать тип сканирования — common ports (4700 часто используемых портов, исходя из документации), all ports (все порты) или выбрать Custom с тонкой настройкой сканирования портов. В примере выберем common

ports.

- Assessment. Можем выбрать способ обнаружения уязвимостей. В примере выберем «Scan for all web vulnerabilities» для более быстрого выполнения сканирования. Вы также можете выбрать Custom. Все параметры доступные в настройке описаны в официальной документации.

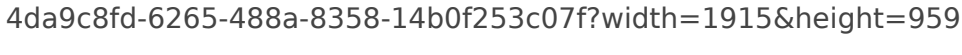
- Report. Настройте параметры формирования отчета (опционально). В примере ничего изменять не будем.

- Advanced. можно настроить скорость выполнения сканирования. При выборе ручной настройки, можно включить/отключить дебаг для плагинов. Подробнее про каждый пункт вы можете прочитать в документации. В примере установим значение в Default.

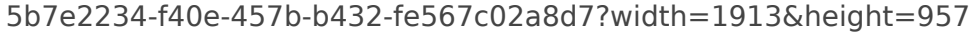
Дополнительные настройки

Помимо основных настроек сверху вы можете увидеть две вкладки — Credentials и Plugins.

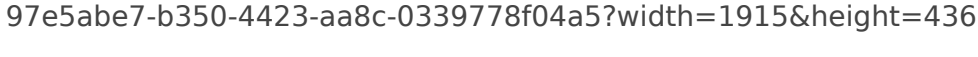
- Credentials. Вы можете установить данные для подключения к сервисам, запущенным на сканируемом хосте (например, для поиска уязвимостей, для которых необходим не привилегированный доступ).



- Plugins. Можем увидеть список плагинов, которые будут использоваться при сканировании. При выборе других типов сканирования, например, advanced scans, у вас будет возможность включать и отключать нужные плагины.



Завершение настройки и запуск сканирования. Нажмите **save**, затем вернитесь на главную страницу и нажмите **Launch** для запуска сканирования (находится рядом с крестиком).



Теперь сканирование запущено. За ходом выполнения вы можете наблюдать, нажав на созданный скан.

Просмотр результатов сканирования

После завершения сканирования для анализа результатов перейдите к выбранному сканированию.

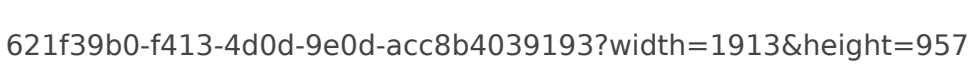
Центральная часть экрана представляет собой таблицу с детальной информацией о найденных уязвимостях:

- Severity: Отражает степень серьезности угрозы, основываясь на метрике CVSS.
- CVSS: Значение метрики CVSSv2, которое указывает на риск уязвимости.
- VPR: Альтернативная метрика от Tenable, предоставляющая дополнительную оценку риска.
- Name: Название обнаруженной уязвимости.
- Family: Категория или группа, к которой относится уязвимость.
- Count: Количество экземпляров данной уязвимости.

Важно отметить, что некоторые уязвимости могут быть объединены в группу «Mixed». Чтобы изменить это поведение, перейдите в Settings -> Advanced и установите параметр Use Mixed Vulnerability Groups в значение «No».

Слева от таблицы представлена информация о целевом хосте, а также диаграмма, демонстрирующая распределение обнаруженных уязвимостей по степени их серьезности.

Для детального изучения конкретной уязвимости, просто кликните по ее названию. Возьмем для примера уязвимость «Drupal Database Abstraction API SQLi».



В основной части экрана будет представлено:

- Описание уязвимости: Краткое описание проблемы и версии ПО, в которой она была устранена.
- Детали обнаружения: Отчеты о найденной уязвимости и методах ее устранения.
- Технические детали: В данном случае, это SQL-запрос, который использовался для выявления уязвимости.

В левой части экрана представлена дополнительная информация:

- Информация о плагине: Описание плагина, который обнаружил уязвимость.
- Рейтинги VPR и CVSS: Оценки серьезности уязвимости по различным метрикам.
- Данные об эксплуатации: Информация о возможности эксплуатации уязвимости.
- Ссылки: Полезные ссылки на ресурсы, такие как exploit-db, nist.gov и другие, где можно узнать больше о данной уязвимости.

Заключение

В этом гайде мы подробно рассмотрели процесс установки, настройки и использования Nessus для сканирования уязвимостей. Nessus — это мощное автоматизированное средство, но его эффективность напрямую зависит от корректной настройки. Однако стоит помнить, что для обеспечения полноценной безопасности сети и системы нельзя полагаться исключительно на автоматизированные инструменты. Комплексный подход и постоянное обучение в области безопасности — ключ к надежной защите.

Источник

Revision #1
Created 2023-11-25 17:56:16 UTC by odiljonov
Updated 2023-11-25 17:57:13 UTC by odiljonov