МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НЕФТИ И ГАЗА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ) ИМЕНИ
И.М. ГУБКИНА

ФАКУЛЬТЕТ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ТОПЛИВНО-
ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА
КАФЕДРА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ДИСЦИПЛИНА:
«БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ»

Статья

на тему:

«Развёртывание и настройка Tenable Nessus на базе ОС Альт»

Выполнили: студенты группы КИ-21-02
Копанев Олег Олегович
Лужнов Александр Олегович
Проверил: старший преподаватель
Павловский Владимир Владимирович

Москва, 2024

Введение

В современных информационных системах важнейшими аспектами обеспечения безопасности являются обнаружение и устранение уязвимостей. Одним из наиболее эффективных средств для управления уязвимостями является Tennable Nessus, который позволяет проводить глубокий анализ защищенности систем и выявлять потенциальные угрозы.

Однако для эффективного использования Nessus необходимо правильно настроить его окружение. В данной статье мы рассмотрим процесс развёртывания и настройки Tenable Nessus на базе отечественной операционной системы Альт. Этот дистрибутив, разработанный компанией "Базальт СПО", становится всё более популярным благодаря своей безопасности, стабильности и совместимости с требованиями российского законодательства.

Версии Nessus

Компания Tebable предлагает несколько решений, предназначенных для разных задач и бюджетов. В таблице 1 приведено сравнение версий, которое направлено для помощи в выборе подходящей версии.

Функция/ Характеристика	**Nessus Essentials**	**Nessus Professional**	**Nessus Expert**
Назначение	Бесплатная версия для обучения и тестов	Профессиональная версия для организаций	Расширенная версия для экспертов
Количество сканирований уязвимостей	Ограниченное	Неограниченное	Неограниченное
Оценка уязвимостей (CVSS v4, EPSS, VPR)	Нет	Да	Да

Аудит конфигураций и соответствия нормам	Нет	Да	Да
Использование в любой среде	Нет	Да	Да
Настраиваемые отчёты	Нет	Да	Да
Поддержка сообщества	Да	Да	Да
Расширенная поддержка	Нет	Опционально	Опционально
Обучение по запросу	Нет	Опционально	Опционально
Сканирование веб-приложений	Нет	Да (5 FQDN с возможностью расширения)	Да (5 FQDN с возможностью расширения)
Сканирование внешней поверхности атак	Нет	Да	Да
Сканирование облачной инфраструктуры	Нет	Да	Да
Цена	Бесплатно	250€/год	814,93 €/год

Таблица 1 – сравнение версий Nessus

Исходя из данных в таблице можно охарактеризовать каждую версию следующим образом:

- Nessus Essentials – это базовая версия, которая предназначена для небольших команд и индивидуальных специалистов по безопасности. Она бесплатная, но с ней вы будете ограничены в количестве IP-адресов, которые можно сканировать. Этот инструмент идеально подходит для студентов, любителей и малых предприятий, которые хотят получить общее представление о своих сетевых уязвимостях и начать с основ кибербезопасности.

- Nessus Professional – это более продвинутая и коммерческая версия, которая предназначена для специалистов по информационной безопасности, а также малых и средних предприятий. Она предоставляет расширенные возможности сканирования, включая более обширную библиотеку плагинов, которые позволяют обнаруживать более широкий спектр уязвимостей.

  Эта версия поддерживает более сложные сценарии сканирования, автоматизацию и интеграцию с другими инструментами безопасности. В целом, она обеспечивает глубокий анализ уязвимостей и рекомендации по их устранению.

- Nessus Expert – наиболее мощная версия ПО, которая предлагает полный набор функций для крупных организаций и специалистов с высокими требованиями к безопасности. Помимо функций, которые и так доступны в версии Professional, Nessus Expert включает в себя дополнительные инструменты для управления облачной безопасностью, а также возможности для работы с инфраструктурами DevOps. Она позволяет организациям проводить глубокий анализ безопасности не только традиционных сетей, но и современных облачных и контейнерных сред.

  Версия Expert идеально подходит для крупных предприятий и организаций, которым необходимо управлять безопасностью в масштабах и комплексности их инфраструктур.

В данной исследовательской работе была выбрана версия Nessus Essentials 10.8.3 (#10) LINUX для проведения эксперимента. Несмотря на ограниченный функционал по сравнению с профессиональными инструментами, эта версия идеально подходит для тестирования решений и сканирования небольших сетей, а также является абсолютно бесплатной.

В качестве платформы для тестирования сканера уязвимостей был выбран отечественный дистрибутив ОС Альт последней версии ALT Workstation 10.4. В этой части будет приведено его краткое описание.

ОС Альт – это отечественная операционная система, разрабатываемая компанией «Базальт СПО». Дистрибутивы данной операционной системы подходят для образовательных, корпоративных и даже государственных задач. Данная операционная система обладает высокой стабильностью и безопасностью, а так же полностью соответствует требованиям Российского законодательства, включая наличие сертификатов ФСБ и ФСТЭК.

Главные особенности ОС Альт:

1. Российская разработка и поддержка.

   ОС Альт полностью разрабатывается и поддерживается российской компанией, что полностью удовлетворяет требованиям импортозамещения в корпоративных и государственных структурах.
2. Безопасность и сертификация.

   Дистрибутив ОС Альт один из немногих имеет сертификаты безопасности ФСТЭК. Поэтому организации часто выбирают его для использования в автоматизированных системах обработки информации.
3. Богатая система репозиториев:

   ОС Альт обладает большим набором репозиториев программного обеспечения, причем многие из них адаптированы под российских пользователей. В целях безопасности рекомендуется использовать только официальные репозитории.
4. Инструменты безопасности:

   ОС Альт обладает большим набором средств для обеспечения безопасности. Среди них много инструментов как настройки, так и мониторинга. Как пример можно привести SELinux и набор утилит для контроля целостности системы.

Преимущества использования ОС Альт:

- Совместимость с российскими технологиями и ПО: ОС Альт разрабатывается с упором на интегрирование с отечественными решениями и стандартами.
- Ориентация на информационную безопасность: ОС Альт имеет мощные встроенные решения для обеспечения защиты данных и предотвращения утечек.
- Долгосрочная поддержка и стабильность: разработчики ОС Альт регулярно обновляют саму операционную систему и дистрибутивы, чтобы она удовлетворяла современным требованиям и оставалась удобной для пользователей.

Процесс установки Nessus Essentials на ОС Альт начинается с перехода на официальный сайт Tenable Nessus для загрузки. На странице загрузки необходимо выбрать последнюю доступную версию Nessus и соответствующую платформу. Однако стоить отметить, что Tenable Nessus не предоставляет официальный пакет для ОС Альт. Поскольку ОС Альт использует RPM-пакеты, аналогичные тем, что применяются в Red Hat Enterprise Linux (RHEL), рекомендуется выбрать версию для RHEL 8. Эта версия наиболее совместима с архитектурой ОС Альт, которая использует RPM как систему управления пакетами. В связи с этим целесообразно выбирать Linux-RHEL 8 - x86_64 в качестве платформы перед началом установки пакета.

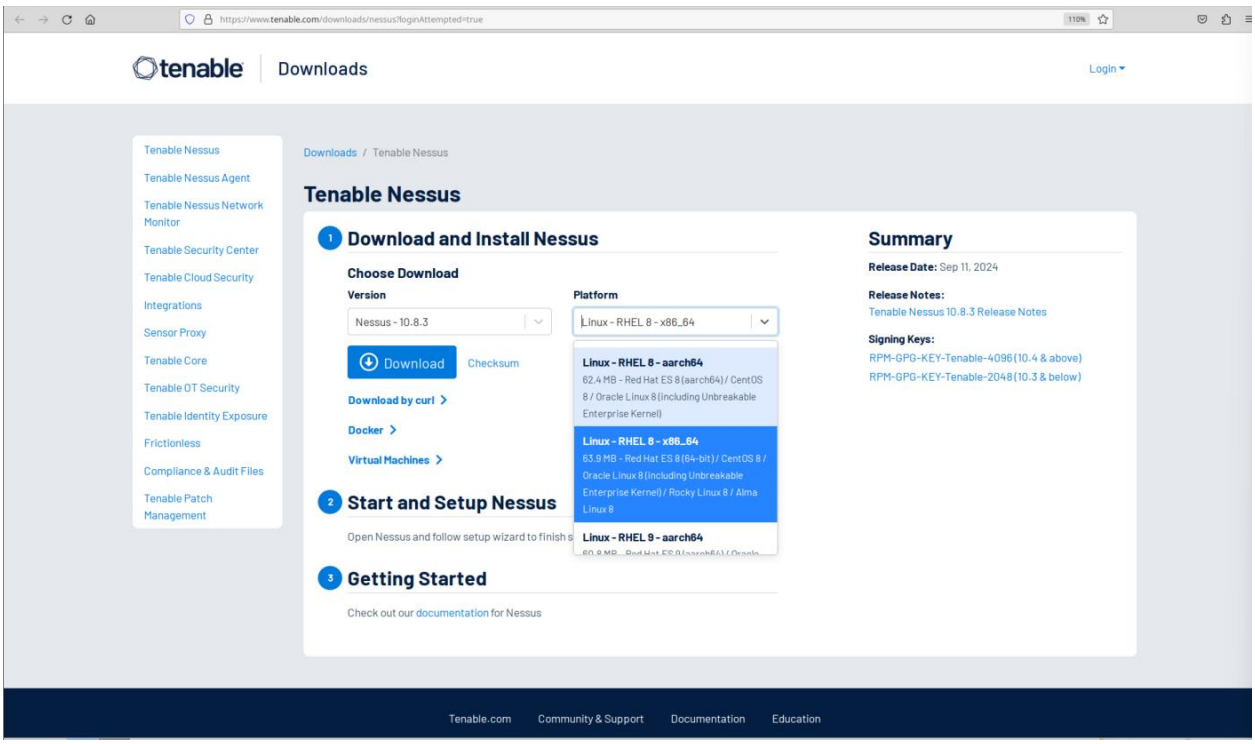

Рисунок 1 – выбор версии и платформы для ОС Альт

Для установки пакетов в форме .rpm, необходимо предварительно убедиться в наличии всех необходимых зависимостей. В данной цели следует обновить информацию о доступных пакетах и установить пакеты, отвечающие за работу с .rpm, а также инструменты, которые обеспечивать совместимость с системой.

После выполнения предыдущего шага, следует перейти в каталог загрузок и произвести установку Nessus. Для этого необходимо выполнить установку пакета, после чего активировать службу Nessus. Также в завершении необходимо проверить статус, установленной службы.

Настройка Nessus

После проверки корректности работы сервиса можно продолжить настройку Nessus. Для этого необходимо выполнить следующие шаги:

1. Открыть веб-браузер и перейти к Nessus, который работает по протоколу HTTPS на порту 8834, введя адрес: https://localhost:8834/.
2. Дождаться завершения компиляции плагинов.

3. После завершения выбрать версию Nessus Essentials.
4. Для работы с Nessus Essentials требуется ключ активации, который можно получить, указав имя и адрес электронной почты. Важно отметить, что активационный код можно получить только при использовании зарубежных почтовых сервисов.
5. На указанный адрес будет отправлено письмо с ключом активации
6. Создать аккаунт администратора, задав логин и пароль для входа в систему.
7. После создания аккаунта Nessus начнет загружать плагины.
8. Войти в систему под аккаунтом администратора

После выполнения этих шагов сканер Nessus будет готов к использованию.

Настройка сервера beeBox

Для проверки функционирования нашего сканера безопасности необходимо настроить сервер beeBox, основанный на версии Ubuntu 8,04, который будет использоваться для сканирования на наличие уязвимостей. BeeBox представляет собой виртуальную машину, основанную на bWAPP (buggy web application) - учебное приложении с преднамеренно встроенными уязвимостями, предназначенном для обучения в области кибербезопасности.

В beeBox реализованы различные уязвимсоти, включая:

1. Атаки с использованием внешних сущностей XML (XXE)
2. Инъекции (HTML, SQL, LDAP и другие)
3. Использование компонентов с известными уязвимостями
4. Межсайтовая подделка запроса (CSRF)
5. Межсайтовый скриптинг (XSS)
6. Нарушение аутентификации и управления сессиями

7. Недостаточная проверка объектов
8. Неправильная конфигурация безопасности
9. Отсутствие контроля доступа на уровне функции
10. Утечка конфиденциальной информации

Хотя установка и конфигурация виртуальной машины beeBox будет рассмотрена кратко, следует отметить несколько ключевых моментов, необходимых для успешного запуска и проведения эксперимента:

1. Виртуальной машине следует выделить не менее 1024 МБ RAM и 1 CPU, чтобы обеспечить ее запуск.
2. При конфигурации сети необходимо добавить порт внутренней сети для объединения с ОС Альт в одну подсеть.
3. После запуска виртуальной машины следует выпролнить команду, указанную в листинге 1, для изменения раскладки клавиатуры на американскую (QWERTY), так как исходная раскладка непригодна для работы.
4. Назначить статический IP-адрес для созданного порта и проверить соединение между двумя машинами. Листинг 1 - изменение раскладки клавиатуры на американскую

```
setxkbmap us
```

Настройка beeBox окончена.

Общие параметры Nessus

При подготовке к сканированию с использованием Nessus, важно изучить пользовательский интерфейс и доступные настройки программы. Главный

экран интерфейса разделен на две основные вкладки: “Сканирование” и “Настройки”, что обеспечивает эффективное управление функционалом.

В разделе “Настройки (Settings)” выделяются следующие категории:

1. Обзор (About):

Общая информация (Overview): Данный раздел предоставляет сведения о текущей установки Nessus, включая версию программного обеспечения, условия лицензирования и другие важные аспекты.

Использование лицензии (License Utilization): В этом разделе отображаются все IP-адреса, которые были сканированы.

Обновления программного обеспечения (Software Update): Данный раздел позволяет пользователю настраивать автоматические обновления или выполнять их вручную.

Пароль шифрования (Encryption Password): Здесь можно установаить пароль для шифрования данных Nessus. Важно запомнить пароль, поскольку его отсутствие затруднить восстановление данных.

События (Events): В этом разделе пользователю предоставляется возможность отслеживать историю обновлений и другие значимые события.\

2. Расширенные настройки (Advanced Settings): Данный раздел включает дополнительные параметры конфигурации Nessus. Несмотря на то, что настоящая работа не предполагает детального рассмотрения этих эффектов, подробная информация может быть найдена на официальном сайте.

Прокси-сервер (Proxy Server): Если в вашей сети требуется использование прокси для доступа в интернет или к целевым серверам, соответствующие параметры можно настроить в этом разделе.

SMTP-сервер: В этом разделе возможно настроить параметры SMTP-сервера, что позволит Nessus отправлять уведомления по электронной почте о результатах сканирования и других важных событиях.

Запуск тестового сканирования

Теперь необходимо перейти к вкладке “Сканирование (Scans)”. Перед использованием Nessus для обнаружения уязвимостей следует правильно настроить параметры сканирования. На главном экране следует нажать на кнопку “Новое сканирование”, что откроет мастер создания сканирования

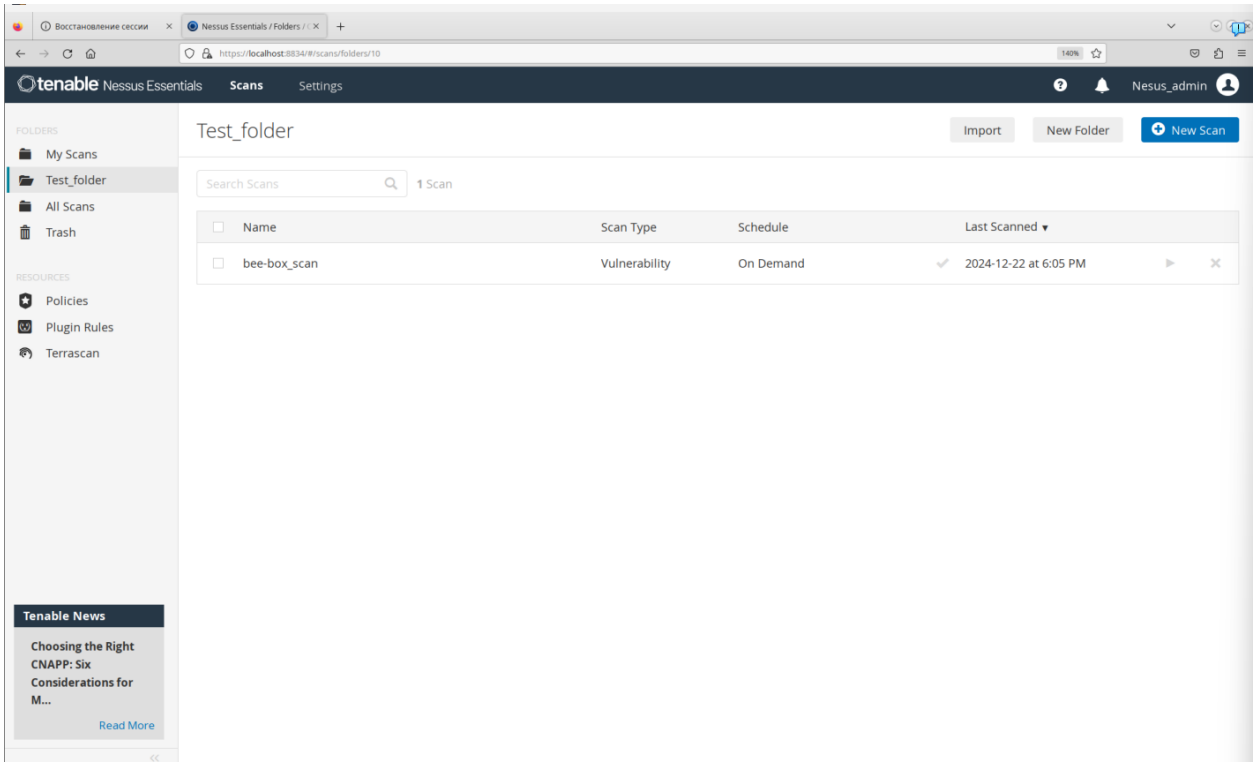

Рисунок 2 – мастер сканирования Tenable Nessus

Для примера выберем Basic Network Scan.

Далее необходимо провести общие настройки.

- General. Здесь можно задать имя, описание, выберать папку для результатов и в Targets указать IP-адрес виртуальной машины bee-box (рисунок 3).

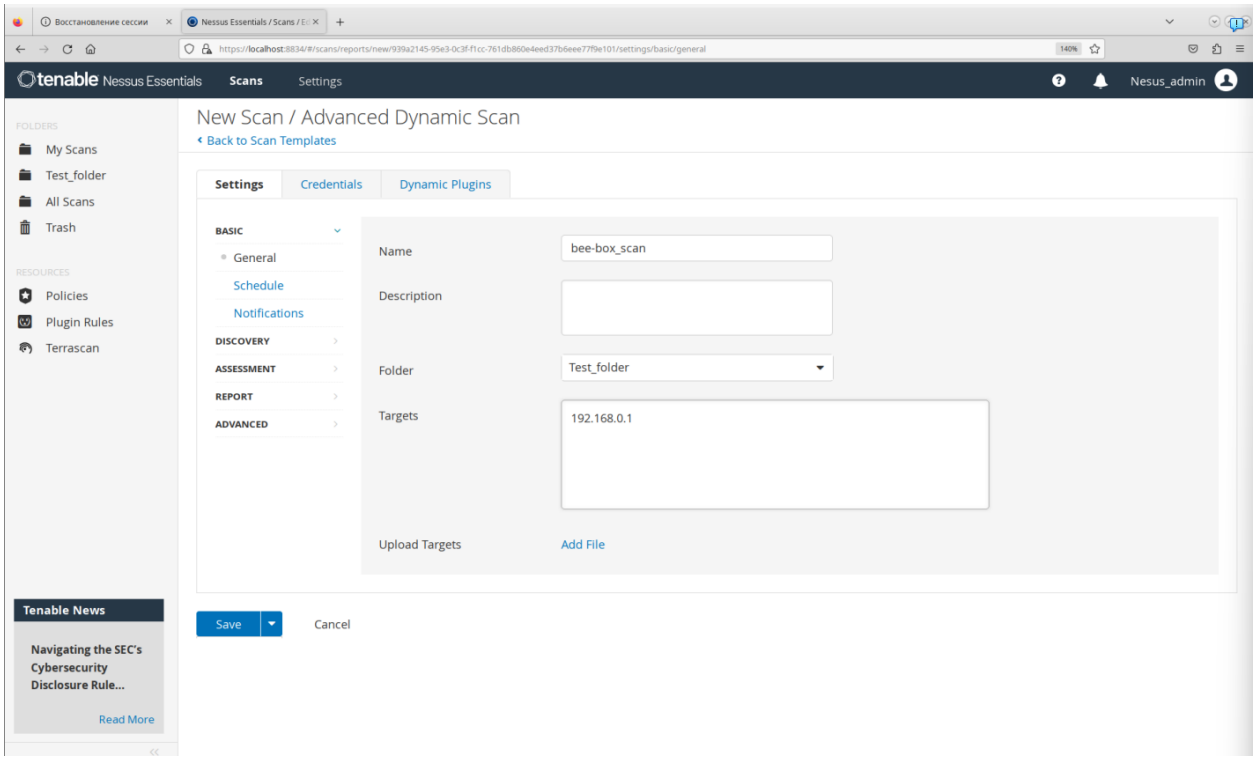

Рисунок 3 – основные настройки сканирования

“Расписание и уведомления (Schedule, Notifications)”

В рамках настройки сканирования в Nessus можно задать расписание, которое позволяет установить периодичность сканирования по желанию пользователя.

Дополнительно имеется возможность настроить уведомления, указав адреса электронной почты для отправки уведомлений. Для корректной работы этой функции необходимо предварительно настроить подключение к SMTP-серверу.

Подобные настройки

В параметрах выделяются следующие аспекты:

1. Обнаружение (Discovery): В данном разделе можно выбрать тип сканирования, включая опции для сканирования общих портов (4700 часто используемых портов), всех портов или настроить сканирование по индивидуальным параметрам. В рассматриваемом примере выбран вариант сканирования общих портов.
2. Оценка (Assessment): Здесь задан метод обнаружения уязвимостей.

3. Отчет (Report): Предоставляется возможность конфигурации параметров формирования отчета в зависимости от требований пользователя.
4. Дополнительно (Advanced): Этот раздел позволяет настроить скорость выполнения сканирования. В текущей примере установлены значения по умолчанию.

Дополнительные настройки

Помимо основных настроек, в интерфейсе Nessus доступны две дополнительные вкладки - “Учетные данные и Плагины (Credentials, Plugins)”:

1. Учетные данные (Credentials): Этот раздел позволяет установить данные для подключения к сервисам, запущенным на сканируемом хосте, что необходимо для идентификации уязвимостей, которые требуют не привилегированный доступ.
2. Плагины (Plugins): Здесь представлен список плагинов, которые будут задействованы при сканировании. При выборе других типов сканирования, таких как расширенные сканы, существует возможность включать или отключать необходимые плагины.

По завершении настройки следует сохранить изменения, нажав кнопку “Save”, после чего возвращаемся на главную страницу и нажимаем “Launch” для начала сканирования. Процесс выполнения можно отслеживать, выбрав созданный скан.

Просмотр результатов сканирования

По окончании проверки пользователю доступны результаты, представленные на рисунке 4.

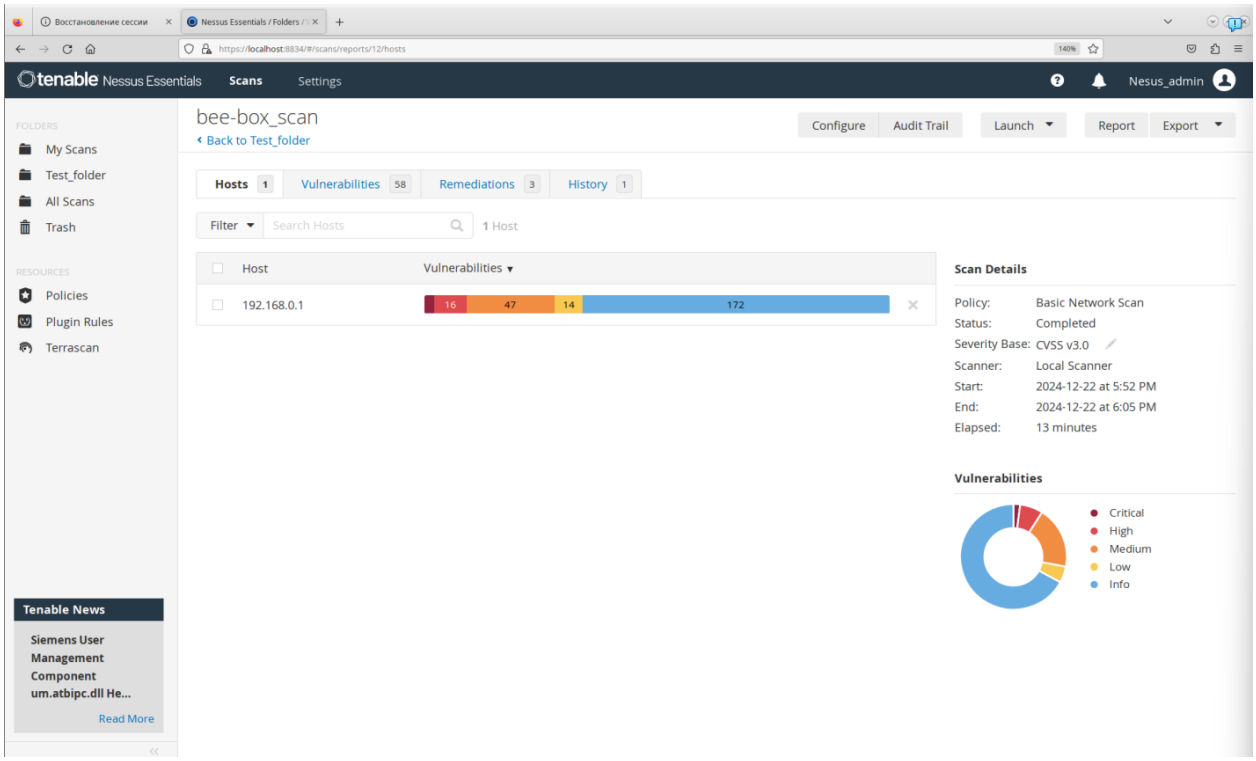

Рисунок 4 – результат сканирования

Теперь рассмотрим подробнее, что представляют из себя результаты сканирования (рисунок 5).

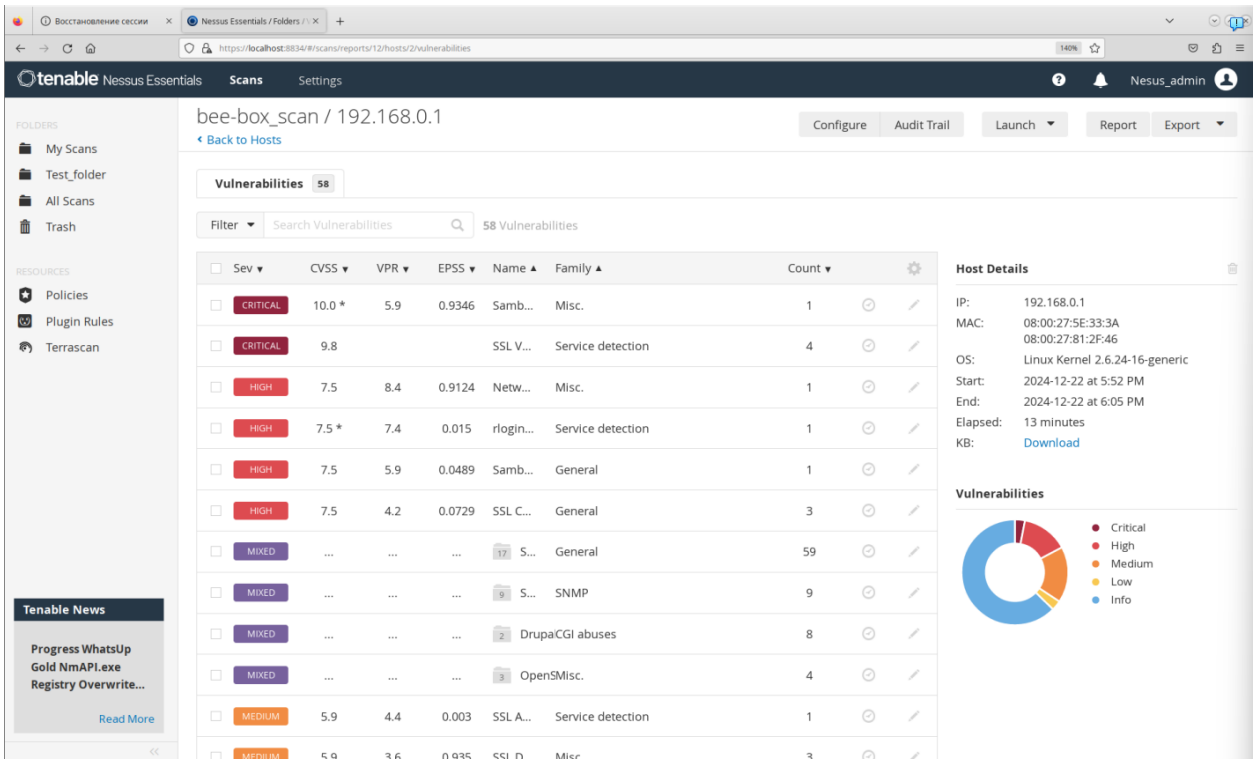

Рисунок 5 – подробные результаты сканирования

Центральная часть интерфейса Nessus представляет собой таблицу, содержащую детальную информацию о выявленных уязвимостях, включающую следующие ключевые параметры:

1. Severity: Указывает на степень серьезности угрозы, основанные на метрике CVSS (Common Vulnerability Scoring System)
2. CVSS: Значение метрики CVSSv2, отражающие риск, связанный с указанной уязвимостью.
3. VPR: Альтернативная метрика, которая предоставляет дополнительную оценку уровня риска.
4. Name: Название обнаруженной уязвимости.
5. Family: Категория или группа, к которой принадлежит данная уязвимость.
6. Count: Общее количество экземпляров данной уязвимости.

Следует отметить, что некоторые уязвимости могут быть объединены в категорию “Mixed”. Для изменения данного поведения пользователь может перейти в настройки и, выбрав раздел Advanced, установить параметр Use Mixed Vulnerability Groups в положении “No”.

Слева от таблицы представлена информация о целевом хосте, а также график, который демонстрирует распределение обнаруженных уязвимостей по степени их серьезности.

Для более детального изучения конкретной уязвимости достаточно кликнуть на ее название. Например, анализируя уязвимость “Samba ‘AndX’ Request Heap-Based Buffer Overflow” (см. Рисунок 6), можно получить более подробную информацию о ее характеристиках и последствиях.

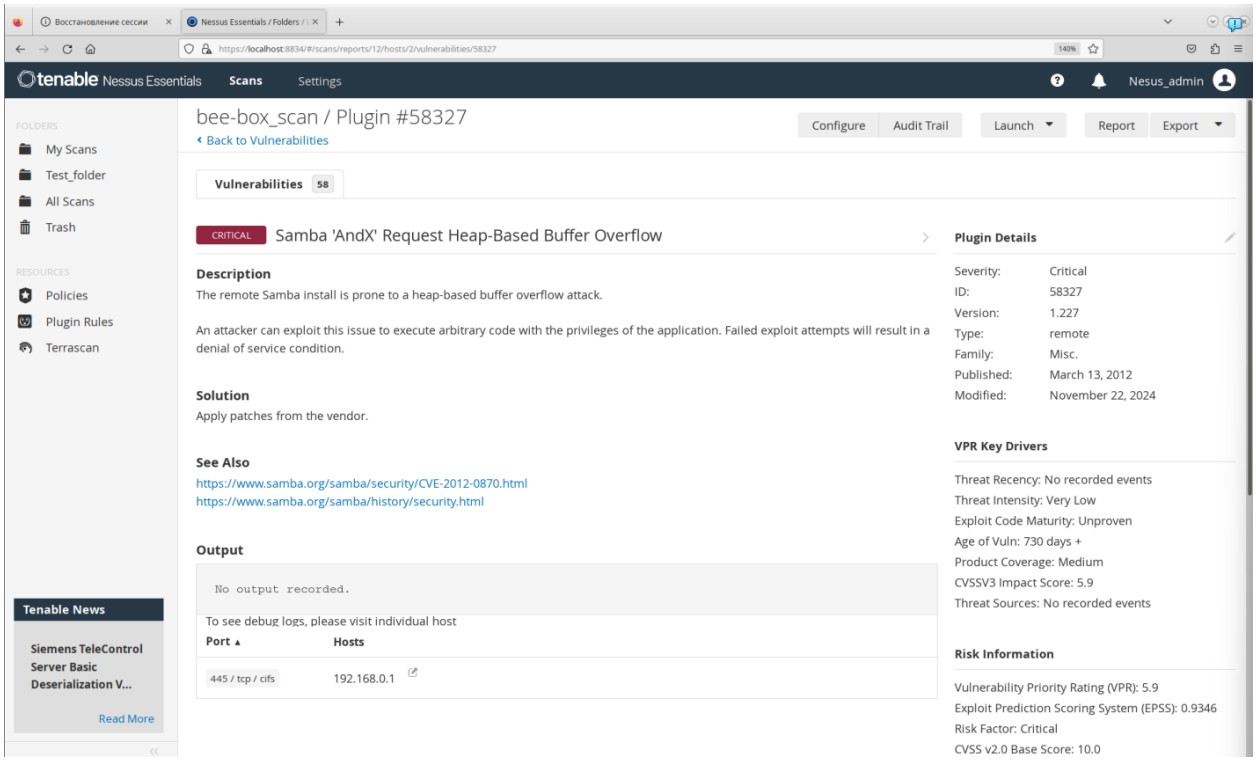

Рисунок 6 – описание уязвимости уязвимость «Samba 'AndX' Request Heap-Based Buffer Overflow»

В основной части экрана 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.

Подробный список обнаруженных уязвимостей, степени их критичности, описание и способы решения представлены в таблице 2.

Название	CVSS	Описание	Методы решения
Samba 'AndX' Request Heap-Based Buffer Overflow	10.0	Удалённая установка Samba уязвима к атаке переполнения буфера в куче. Злоумышленник может использовать эту уязвимость для выполнения произвольного кода с привилегиями приложения. Неудачные попытки эксплуатации приведут к отказу в обслуживании.	Необходимо обновить Samba до последней версии.
SSL Version 2 and 3 Protocol Detection	9.8	Удалённый сервис принимает соединения, зашифрованные с использованием SSL 2.0 и/или SSL 3.0. Эти версии имеют криптографические уязвимости, позволяющие атаки "человек посередине" или дешифрование данных. Кроме того, возможна эксплуатация для даунгрейда соединений.	Необходимо отключить SSL 2.0 и 3.0, изучив документацию приложения. Используйте TLS 1.2 или выше с утверждёнными наборами шифров.
Network Time Protocol Daemon (ntpd) monlist Command Enabled DoS	7.5	Версия ntpd на удалённом хосте имеет включённую команду monlist, что позволяет злоумышленникам проводить разведку или атаки на отказ в обслуживании (DoS/DDoS).	Если используется NTP из проекта Network Time Protocol, необходимо обновить NTP до версии 4.2.7-p26 или выше. Либо добавьте строку disable monitor в файл конфигурации

			ntp.conf и перезапустите сервис.
rlogin Service Detection	7.5	Сервис rlogin передаёт данные в открытом виде, что делает возможным перехват логинов и паролей. Также злоумышленники могут обойти аутентификацию в определённых условиях.	Необходимо закомментировать строку 'login' в файле /etc/inetd.conf и перезапустить процесс inetd. Либо отключите rlogin и используйте SSH.
Samba Badlock Vulnerability	7.5	Уязвимость в протоколах SAM и LSAD из-за неправильной аутентификации в Samba позволяет злоумышленникам проводить атаки "человек посередине" и выполнять произвольные сетевые вызовы Samba.	Необходимо обновить Samba до версии 4.2.11 / 4.3.8 / 4.4.2 или выше.
SSL Certificate Signed Using Weak Hashing Algorithm	6.0	SSL-сертификат использует слабый хэш-алгоритм (например, MD5 или SHA1), что позволяет злоумышленникам подделать сертификат.	Необходимо обратиться к Центру сертификации для перевыпуска SSL-сертификата.
SSL Medium Strength Cipher Suites Supported (SWEET32)	7.5	Удалённый хост поддерживает шифры средней силы, которые уязвимы для атак, особенно если злоумышленник находится в одной сети.	Необходимо настроить приложение для исключения использования шифров средней силы.
SNMP Agent Default	7.5	Удалённый SNMP-сервер использует стандартное имя сообщества (public), что может быть использовано	Необходимо отключить SNMP, если он не

Community Name (public)		злоумышленниками для разведки или изменения настроек.	используется, или сменить имя сообщества на нестандартное.
Drupal Database Abstraction API SQLi	7.5	Версия Drupal уязвима из-за ошибки в API абстракции базы данных, что позволяет SQL-инъекцию. Это может привести к повышению привилегий или удалённому выполнению кода.	Необходимо обновить Drupal до версии 7.32 или выше.
OpenSSL Heartbeat Information Disclosure (Heartbleed)	6.0	Уязвимость OpenSSL (Heartbleed) позволяет злоумышленнику читать до 64КБ памяти сервера, включая конфиденциальные данные.	Необходимо обновить OpenSSL до версии 1.0.1g или выше, либо перекомпилировать его с флагом -DOPENSSL_NO_HEARTBEATS.
SSL Anonymous Cipher Suites Supported	5.9	Использование анонимных SSL-шифров позволяет шифровать трафик без проверки подлинности, делая возможными атаки "man in thee middle".	Необходимо настроить приложение для исключения использования анонимных шифров.
SSL DROWN Attack Vulnerability	5.9	Поддержка SSLv2 делает хост уязвимым к атаке DROWN, позволяющей дешифровать TLS-соединения.	Необходимо отключить SSLv2 и использовать современные криптографические алгоритмы.
X Server Detection	2.6	Сервер X11 передаёт данные в открытом виде, что позволяет злоумышленникам перехватывать трафик.	Необходимо ограничить доступ к порту. Если X11 не используется, отключите

			поддержку TCP (-nolisten tcp).
ICMP Timestamp Request Remote Date Disclosure	2.1	Хост отвечает на ICMP-запросы времени, что может быть использовано для обхода протоколов аутентификации, зависящих от времени.	Необходимо отфильтровать ICMP-запросы времени (13) и ответы (14).

Таблица 2 – список обнаруженных уязвимостей

Заключение

В данной статье была рассмотрена процедура установки и настройки Tenable Nessus на базе ОС Альт, а также основные аспекты работы с этим инструментом для сканирования уязвимостей. Несмотря на ограниченную функциональность бесплатной версии Nessus Essentials, она является отличным инструментом для проведения тестирования и обучения в области информационной безопасности. ОС Альт, благодаря своей совместимости с RPM-пакетами и стабильности, является хорошей платформой для использования Nessus.

Таким образом, настройка Tenable Nessus на платформе ОС Альт позволяет эффективно проводить анализ уязвимостей и обеспечивать безопасность информационных систем. Применение таких инструментов, как Nessus, является важным шагом в борьбе с киберугрозами и обеспечивает высокий уровень защиты для организаций и специалистов по безопасности.

Список использованных источников

1. Уймин, А. Г. Разработка методики тестирования системы безопасности автоматизированных систем управления технологическими процессами на основе корпоративного стандарта / А. Г. Уймин // Автоматизация и информатизация ТЭК. – 2024. – № 5(610). – С. 59-65. – EDN VSLWIA.
2. Киргизбаев С. П., Киргизбаев В. П., Бутин А. А. Применение сканеров уязвимостей для обнаружения потенциальных угроз информации в корпоративной Сети и анализа её защищенности //Информационные технологии и математическое моделирование в управлении сложными системами. – 2023. – №. 4. – С. 20.
3. Плетнев Д. А. и др. НОВЫЕ ВЫЗОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МАЛОГО И СРЕДНЕГО БИЗНЕСА //Вестник Челябинского государственного университета. – 2022. – №. 11 (469). – С. 177-181.
4. Караванов И. В., Трещев И. А. АНАЛИЗ УЯЗВИМОСТЕЙ КАТЕГОРИИ A5 OWASP С ПОМОЩЬЮ BWAPP И BEE-BOX //МОЛОДЕЖЬ И НАУКА: АКТУАЛЬНЫЕ ПРОБЛЕМЫ ФУНДАМЕНТАЛЬНЫХ И ПРИКЛАДНЫХ ИССЛЕДОВАНИЙ. – 2023. – С. 286-289.
5. Мунтян М. М., Сидоркина И. Г. Алгоритм интеграции сканеров уязвимостей с системами мониторинга рисков информационной безопасности и представления результатов сканирования в формализованном виде. – 2023.
6. Pulkkinen H. Safe security scanning of a production state automation system : дис. – 2023.
7. Zafar A. A. Improving internal vulnerability scanning and optimal positioning of the vulnerability scanner in. – 2023.