Этап 1. Заочный.

Задание для проведения заочного этапа Всероссийского хакатона по программированию «Обучаюсь. Проектирую. Программирую. Будущее»: Направление Информационная безопасность.

Содержание конкурсного задания:

1. ВВЕДЕНИЕ

Большинство инфраструктурных решений в качестве серверной платформы используют операционные системы на базе открытого исходного кода. Умение работать с подобными системами становится крайне важным навыком для тех, кто планирует стать профессиональным специалистом в области информационных технологий: программистами, системными администраторами, специалистами в области информационной безопасности, и пр.

Представленные далее конкурсные задания соответствуют базовой практике настройки ряда защитных механизмов серверной инфраструктуры.

Представленные задания не покрывают весь спектр мероприятий по защите серверных систем. Вместе с тем, продемонстрированные знания и навыки работы с механизмами защиты в системе на базе открытого исходного кода позволят осуществить отбор (определение) команд для участия в Подготовительном этапе в соответствии с Положением о Всероссийском хакатоне по программированию «Обучаюсь. Проектирую. Программирую. Будущее».

2. УСЛОВИЯ И ФОРМЫ УЧАСТИЯ

Условия и формы участия определяются в соответствии с Положением о Всероссийском хакатоне по программированию «Обучаюсь. Проектирую. Программирую. Будущее»

3. ЗАДАНИЕ ДЛЯ КОНКУРСА

Содержанием конкурсного задания являются работы по базовой пусконаладке сервера на базе операционной системы Linux. Конкурсное задание выполняется участниками на основе предоставленного образа виртуальной машины (далее – Сервер).

В рамках легенды конкурсного здания вы – специалист по информационной безопасности нефтегазовой компании, после переезда управляющего офиса компании вам предстоит настроить сервер совместного доступа к корпоративным ресурсам (файлы, веб-сервер) в части предоставления прав доступа, минимизации источников угроз состояния защищенности Сервера.

Доступ к виртуальной машине можно получить по аккаунту **root**:**Pa$$w0rd2023**.

Историю введенных в консоль команд (вызывается командой history) очищать запрещается.

На серверных операционных системах графическое окружение рабочего стола обычно не используется, в том числе для уменьшения поверхности атак. Для решения заданий удаление графического окружения не требуется.

Задания предоставлены не по порядку. Порядок выполнения определяется участниками.

3.1. Добавить пользователей согласно списку

A. Вам необходимо добавить на Сервер аккаунты работников компании согласно списку:

	Должность	**Логин пользователя**
1	Генеральный директор	vladimirgrishin
2	Главный бухгалтер	yaroslavmakarov
3	Бухгалтер	romanparamonov
4	Финансовый директор	sergejcherkasov
5	Финансист	zaharbondarev
6	Руководитель ИТ службы	evaandreeva
7	Специалист по ИТ	itadmin
8	Главный юрист	madinaivanova
9	Юрист	aleksejantonov
10	Директор по информационной безопасности	nikolajvolkov
11	Специалист по информационной безопасности	ibadmin
12	Помощник генерального директора	kiranovikova
13	Маркетолог	artyomcherkasov
14	Директор по производству	maksimvorobev
15	Главный геолог	daniilavdeev
16	Геолог	elisejignatov
17	Главный геофизик	mariyazhuravleva
18	Геофизик	maksimserebryakov
19	Архивариус	daniilbirykov

Используйте для пользователей следующий пароль (без кавычек): “**Pa$$w0rd2023**”.

При добавлении аккаунтов пользователей система помимо пароля просит указать дополнительную информацию о пользователе. Игнорируйте эти запросы, нажимая клавишу Enter.

Б. Для генерального директора задайте пароль (без кавычек): “**SupersafePa$$2023**”, а для Директора по информационной безопасности задайте пароль (без кавычек): “**P@$$w0rd2@0)2@3#**”

В. Для усиления безопасности следует отказаться от использования аккаунта **root** в повседневных задачах. Отключите учетную запись **root** для входа по протоколу **ssh**.

Г. Добавьте аккаунты **ibadmin** и **itadmin** в группу sudo для выполнения команд от имени суперпользователя.

Д. Маркетолог компании, Артем Черкасов, идет на повышение и переходит на работу в дочерний филиал компании. Следует настроить автоматическую блокировку его аккаунта с 01 октября 2023 года.

3.2. Создать систему папок для общего использования и предоставить доступ

Для организации работы с корпоративными материалами необходимо создать на Сервере структуру папок согласно матрице доступа. Папки необходимо разместить по адресу: “**/home/share**”. Используйте в качестве инструмента ACL (Access control lists – листы контроля доступа). Для удобства предоставления доступа добавляйте пользователей с одинаковым уровнем доступа в общие группы.

Матрица доступа

Должность и логин	finance	finance/director	finance/shared	finance/department	accountant	accountant/chief	accountant/shared	accountant/department	library	library/main	lawyer	lawyer/chief	lawyer/shared	lawyer/department	projects	projects /shared	projects department	Shared
Генеральный директор - vladimirgrishin	RX	RWX	RWX	RX	RX	RWX	RWX	RX	RX	RX	RX	RWX	RWX	RX	RX	RWX	RX	RWX
Главный бухгалтер - yaroslavmakarov	RX	RX	RWX	RX	RX	RWX	RWX	RWX	RX	RX	RX	0	RWX	0	RX	0	0	RWX
Бухгалтер - romanparamonov	RX	0	RWX	0	RX	0	RWX	RWX	RX	RX	RX	0	RWX	0	RX	0	0	RWX
Финансовый директор - sergejcherkasov	RX	RWX	RWX	RWX	RX	R	RWX	R	RX	RX	RX	0	RWX	0	RX	0	0	RWX
Финансист - zaharbondarev	RX	0	RWX	RWX	RX	0	RWX	0	RX	RX	RX	0	RWX	0	RX	0	0	RWX
Руководитель ИТ службы - evaandreeva	RX	0	RWX	0	RX	0	RWX	0	RX	RX	RX	0	RWX	RX	RX	0	0	RWX
Специалист по ИТ - itadmin	RX	0	RWX	0	RX	0	RWX	0	RX	RX	RX	0	RWX	RX	RX	RWX	RWX	RWX
Главный юрист - madinaivanova	RX	0	RWX	0	RX	0	RWX	0	RX	RX	RX	RWX	RWX	RWX	RX	0	0	RWX
Юрист - aleksejantonov	RX	0	RWX	0	RX	0	RWX	0	RX	RX	RX	0	RWX	RWX	RX	0	0	RWX

Должность и логин	finance	finance/director	finance/shared	finance/department	accountant	accountant/chief	accountant/shared	accountant/department	library	library/main	lawyer	lawyer/chief	lawyer/shared	lawyer/department	projects	projects /shared	projects department	Shared
Директор по информ. без-сти - nikolajvolkov	RX	0	RWX	0	RX	0	RWX	0	RX	RX	RX	0	RWX	0	RX	RWX	RWX	RWX
Специалист по информ. без-сти - ibadmin	RX	0	RWX	0	RX	0	RWX	0	RX	RX	RX	0	RWX	0	RX	RWX	RWX	RWX
Помощник ген.директора - kiranovikova	RX	0	RWX	0	RX	0	RWX	0	RX	RX	RX	0	RWX	0	RX	0	0	RWX
Маркетолог - artyomcherkasov	RX	0	RWX	0	RX	0	RWX	0	RX	RX	RX	0	RWX	0	RX	0	0	RWX
Директор по производству - maksimvorobev	RX	0	RWX	0	RX	0	RWX	0	RX	RX	RX	0	RWX	0	RX	RWX	RWX	RWX
Главный геолог - daniilavdeev	RX	0	RWX	0	RX	0	RWX	0	RX	RX	RX	0	RWX	0	RX	RWX	RWX	RWX
Геолог - elisejignatov	RX	0	RWX	0	RX	0	RWX	0	RX	RX	RX	0	RWX	0	RX	RWX	RWX	RWX
Главный геофизик - mariyazhuravleva	RX	0	RWX	0	RX	0	RWX	0	RX	RX	RX	0	RWX	0	RX	RWX	RWX	RWX
Геофизик - maksimserebryakov	RX	0	RWX	0	RX	0	RWX	0	RX	RX	RX	0	RWX	0	RX	RWX	RWX	RWX

R - Read – **Чтение**, **W** - Write – **Запись**, **X** - eXecute – **Выполнение**, **0** - **Нет доступа**

3.3. Настроить парольную политику на сервере

Для усиления защиты аккаунтов вам предстоит настроить набор требований для формирования единой парольной политики и защиты от перебора паролей.

А. К устанавливаемым на аккаунтах сервера паролям настройте требования, чтобы допускались к установке пароли, состоящие из:
   a. не менее 11 символов;
   b. букв в ВЕРХНЕМ и нижнем регистрах;
   c. цифр;
   d. спецсимволов.

Б. Установите минимальное количество дней до истечения действия пароля -10 дней, а также максимальное - 120 дней.

В. Необходимо установить количество неудачных попыток входа пользователя для защиты от перебора паролей равное 10 попыткам.

3.4. Настроить межсетевой экран

Одним из важнейших мер обеспечения безопасности сети является настройка межсетевого экрана (далее МСЭ). Вам необходимо провести аудит и настройку МСЭ на Сервере. МСЭ может быть настроен с помощью iptables непосредственно или с помощью ufw. Ufw уже предустановлен на Сервере.

А. Вам необходимо проверить текущий статус процесса МСЭ на предмет его активности. При необходимости его следует запустить.

Б. На Сервере уже установлены веб-сервер для организации внутреннего корпоративного портала, а также OpenSSH сервер, для удаленного доступа и управления сервером. Вам необходимо в МСЭ разрешить доступ портам по умолчанию для протоколов: http, https, pop3, smtp и ssh. Подключение через протокол TCP.

В. Проверьте конфигурацию МСЭ, определите текущие правила доступа на Сервер через сеть. Если запрет на внешние подключения к серверу по умолчанию отсутствует, запрет необходимо установить принудительно.

3.5. Уменьшение поверхности для атак

Для уменьшения возможных точек компрометации рекомендуется удалить неиспользуемые программы и сервисы. Важно отказаться от использования известных небезопасных сервисов.

По результатам аудита известно о наличии на Сервере двух сервисов: первый предназначен для организации обмена файлами

между компьютерами через порт 21 (по умолчанию), а второй для создания интерактивного соединения между удаленными компьютерами. Его современный аналог - протокол ssh. Из-за низкого уровня безопасности их использование не планируется. Вам необходимо найти и удалить эти сервисы.

4. КРИТЕРИИ ОЦЕНКИ

Каждый критерий оценивается по 10-бальной шкале.

1. Соответствие проекта техническому заданию: проект представляет из себя продукт, определённый заданием.

2. Работоспособность проекта: сам продукт, его ветки и модули работают и выполняют свои функции.

3. Инструменты и технологии, используемые при реализации проекта: полнота настроек и параметров проекта.

5. ТЕХНИЧЕСКИЕ ПАРАМЕТРЫ ИНФРАСТРУКТУРЫ

Выполнение конкурсных заданий осуществляется на основе преднастроенной виртуальной машины. Инструкция по настройке можно скачать по адресам ниже.

Виртуальную машину, инструкции и полезные материалы можно скачать по адресам:

А. Основной: https://disk.yandex.ru/d/UhRBYWuVZehKPA

Б. Резервный: https://disk.yandex.ru/d/M-DEfGHvYqFvtg

Рекомендуемая форма представления результата:

1. Папка с виртуальной машиной: в заархивированном виде в формате zip (допускается многотомный архив), в формате OVA записанная на физический носитель информации или через сеть интернет;
2. Видеозапись экрана компьютера с демонстрацией реализованного функционала в формате *.mp4 или *.avi, с выводом: списков пользователей, групп с пользователями, настроек доступа к папкам через вывод команды getfacl, установленную парольную политику, правила МСЭ, список программ и сервисов, демонстрация вывода команды history;
3. Файл-обследование виртуальной машины по результатам выполнения скрипта в формате txt.

Возможно предоставить результат по одной из форм представления результатов.

Достаточность предоставленных результатов и необходимость предоставления дополнительных материалов (в другой форме) определяется экспертной комиссией.

Конфигурации для виртуальной машины:

Минимум:1 процессорное ядро, 1 ГБ оперативной памяти;

Рекомендуется: 2 процессорных ядра, 2 ГБ оперативной памяти.

Для работы виртуальной машины требуется установить программу-гипервизор – VirtualBox версии 7.0.10 и дополнительный пакет расширений VirtualBox Extension Pack 7.0.10.

Ссылки на загрузку VirtualBox:
https://download.virtualbox.org/virtualbox/7.0.10/VirtualBox-7.0.10-158379-Win.exe

Ссылки на загрузку VirtualBox Extension Pack:
https://download.virtualbox.org/virtualbox/7.0.10/Oracle_VM_VirtualBox_Extension_Pack-7.0.10.vbox-extpack