ТИПОВОЕ КОНКУРСНОЕ ЗАДАНИЕ

ДЛЯ РЕГИОНАЛЬНЫХ ЧЕМПИОНАТОВ

чемпионатного цикла 2021/2022

компетенции

«КОРПОРАТИВНАЯ ЗАЩИТА ОТ ВНУТРЕННИХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

для основной возрастной категории
16-22 года

Конкурсное задание включает в себя следующие разделы:

1. **Форма участия в конкурсе**: Индивидуальный конкурс

2. **Общее время на выполнение задания:** до 22 ч.

3. **Задание для конкурса**

Содержанием конкурсного задания являются применение на практике систем корпоративной защиты от внутренних угроз. Участники соревнований получают описание модели организации, включая описание её организационной структуры, информации, циркулирующей внутри периметра безопасности, информационной инфраструктуры, каналов связи, видов трафика, списков пользователей.

Конкурсное задание имеет несколько модулей, выполняемых последовательно.

Конкурс включает исследование организации с целью защиты от внутренних угроз, настройку и проверку специализированного программного обеспечения, разработку и применение политик информационной безопасности, контроль информационных потоков, анализ выявленных инцидентов и подготовку отчётов.

Окончательные аспекты критериев оценки уточняются членами жюри. Оценка производится как в отношении работы модулей, так и в отношении процесса выполнения конкурсной работы. Если участник конкурса не выполняет требования техники безопасности, конфликтен, не владеет техниками управления стрессом и разрешения конфликтных ситуаций, подвергает опасности себя или других конкурсантов, такой участник может быть отстранен от конкурса.

Время и детали конкурсного задания в зависимости от конкурсных условий могут быть изменены членами жюри.

Конкурсное задание должно выполняться помодульно. Оценка также происходит от модуля к модулю.

Если участник закончил выполнение модуля досрочно, он должен расписаться в ведомости времени напротив соответствующей информационной записи «Участник №__ закончил выполнение модуля __».

4. Модули задания и необходимое время

Таблица 1.

Наименование модуля		Соревновательный день (С1, С2, С3)	Время на задание
A	Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз	С1	3-4 часа
B	Отчетность и нормативно-правовое обеспечение корпоративной безопасности	С1	3 часа
C	Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз	С2	3-4 часов
D	Технологии защиты и анализа сетевого трафика	С2	3-5 часов
E	Технологии защиты узла и агентского мониторинга	С3	2-3 часа
F	Предотвращение инцидентов и управление событиями информационной безопасности	С3	3 часа

Модули с описанием работ

Модуль А: Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз

Технологии этого модуля: DLP-системы, системы защиты сетей и систем
Время на выполнение: 3-4 часа

Пример задания

Задание на установку, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз

Установите сервер безопасности InfoWatch Traffic Monitor в виртуальной среде VMWare Workstation. Сервер и СУБД должны быть установлены на одной виртуальной машине со следующими параметрами:

- виртуальный диск размером 80 – 100 ГБ в динамическом режиме;
- 2 процессора, 2 логических ядра;
- 8ГБ ОЗУ.

Параметры IWTM для установки: версия - Enterprise, СУБД - PostgreSQL.
Все дистрибутивы находятся в каталоге с дистрибутивами.
Настройки сетевых интерфейсов указаны в дополнительных сведениях к заданию.
При установке IWTM задайте следующий пароль суперпользователя: xxXX1234

Измените пароль офицера безопасности для доступа к веб-интерфейсу IWTM на: xxXX4321
Активируйте лицензию, которая находится в каталоге с дистрибутивами.
Для интеграции с Active Directory необходимо получить информацию о пользователях и компьютерах компании «Домен локал» с помощью LDAP-синхронизации.

Задание на установку и настройку InfoWatch Device Monitor
Введите машину, на которую будет установлен сервер IWDM в домен и выполните аутентификацию от имени пользователя, указанного в дополнительных сведениях к заданию.
Установить базу данных PostgreSQL с паролем суперпользователя xxXX1234.
Установить InfoWatch Device Monitor с параметрами по умолчанию, в качестве базы данных использовать ранее установленную базу данных PostgreSQL.
При установке необходимо настроить пользователя для доступа к консоли управления: officer с паролем xxXX1234.
После установки использовать доменного пользователя для входа в консоль управления (dmadmin).
Синхронизируйте IWDM с Active Directory (компьютеры и пользователи) и свяжите IWDM с вашим InfoWatch Traffic Monitor.

Задание на установку InfoWatch Device Monitor Agent
Необходимо создать доменных пользователей для клиентских машин. Ввести виртуальную машину нарушителя в домен и войти в систему от ранее созданного доменного пользователя.
Установите InfoWatch Device Monitor Agent на виртуальные машины-нарушителя

- На 1-ю пользовательскую машину – с помощью задачи первичного распространения (без формирования пакета установки) в Device Monitor Server.

Зафиксируйте выполнение задачи скриншотом (1 на создание задачи, 1 на успешное выполнение).

- На 2-ю пользовательскую машину – с помощью групповых политик домена. Политика должна применяться только на конкретную машину. Зафиксируйте выполнение скриншотами.

Задание на установку и настройку подсистемы Crawler
Необходимо установить и настроить подсистему Crawler на Windows Server IWMD.

Создайте общий доступ только на каталог c:\data\share на Windows Server IWDM с правами чтения и записи для всех.
Настройте Crawler на автоматическое ежедневное сканирование только ранее созданного каталога вашего Windows Server и зафиксируйте выполнение задания скриншотом настройки crawler в web-консоли IWTM.

Модуль B: Отчетность и нормативно-правовое обеспечение корпоративной безопасности

Технологии этого модуля: программное обеспечение для создания текстовых документов (например, MS World)

Время на выполнение: 3 часа

Пример задания

Конкурсанту необходимо провести обследование и анализ структуры организации (как главного объекта защиты) на основании представленного описания и выполнить задания:

1.1. Задание на сводки DLP. Создайте в сводке «Чемпионат» 2 виджета:

- Выборка по событиям краулера за последнюю неделю
- Выборка по политикам с технологиями: графические объекты, печати, эталонные документы за последние 3 дня

1.2. Задание на отчеты.

- Создайте отчет в разделе «Отчеты», назвав его «Региональный» и добавьте 2 виджета:
- Отобразить всех пользователей, занимающихся не относящейся к работе деятельностью (по тегам или другим критериям из задания на политики)
- Вычислить топ-нарушителей среди всех сотрудников компании и вывести отчет по нарушениям только по самому активному отправителю.

1.3. В компании (ООО Demo.lab) происходят утечки данных, нарушение трудовой дисциплины и непрофильное использование рабочих ресурсов и времени. Директор рассержен и просит произвести образцово-показательные действия с наиболее несознательными сотрудниками. На основании зафиксированных в DLP-системе действий сотрудников, необходимо разработать и корректно оформить полный пакет документов (за подписью руководителя организации) для осуществления дисциплинарного взыскания (выговор или другой вид взыскания). Приложите к пакету документов полный перечень документов, который должны был принят в организации ДО факта нарушения для законного осуществления

вышеперечисленных действий. Список должен быть достаточен для осуществления правомерного и законного взыскания и не содержать лишних документов, не относящихся к этому вопросу.

1.4. Подготовить отчет об обнаруженных атаках согласно прилагаемому в дополнительных файлах шаблону. Название файла – Отчет об известной атаке.docx

1.5. На основании представленного описания, определите типы циркулирующих данных с точки зрения категорий информации ограниченного доступа (с учетом допущения 2 – см. ниже), представляющих важность для деятельности компании и подлежащих защите, и каналы передачи этих данных.

1.6. Определите перечень нормативно-правовых актов и регуляторных документов РФ, которые могут относить данные, циркулирующие в организации (см. п. 1.1) к категориям информации ограниченного доступа. Приведите максимально подробный перечень по каждому типу информации.

Результаты выполнения пунктов 1.1. и 1.2. оформите в виде таблицы:

Тип (категория) информации ограниченного доступа	Информация ограниченного доступа (из п. 1.1.)	Подразделения, которые участвуют в обработке данных и имеют к ним доступ	Каналы передачи данных	Регулирующие нормативно-правовые акты

1.7. Составьте перечень основных угроз (рисков) от внутренних утечек информации ограниченного доступа для организации и оцените объём потенциальных финансовых потерь для каждой угрозы (в рублях).

Используйте при расчётах методические рекомендации ФСТЭК или профильные ГОСТ, например «Методику определения угроз безопасности информации в информационных системах». Разрешается использовать альтернативные модели со ссылкой на источник.

По итогам расчётов оцените приоритеты: представьте перечень угроз в порядке снижения важности для организации, т.е. по снижению уровня потенциальных финансовых потерь.

Результат выполнения пункта 1.3. оформите в виде таблицы:

Основные угрозы/риски	Объём потенциальных финансовых потерь для каждой угрозы (в рублях)

1.8. Определите типы и возможности потенциальных внутренних нарушителей.

Результат выполнения пункта 1.4. оформите в виде таблицы:

Тип нарушителя	Характеристика имеющихся прав доступа	Способы реализации угроз воздействия на информацию ограниченного доступа	Характер воздействия

1.9. Подготовьте план организационных мероприятий по усилению защиты конфиденциальной информации, отвечающий теории и практике применения законодательства РФ.

Результат выполнения пункта 1.5. оформите в виде таблицы:

Организационно-методические документы по защите конфиденциальной информации	Организационно-режимные мероприятия

1.10. На основе конкурсного задания, подготовьте предложения по усилению контроля циркулирующих в организации (а также передаваемых за пределы организации) данных с использованием существующей DLP-системы с целью предотвращения утечек информации ограниченного доступа или других инцидентов информационной безопасности. Разработайте не менее 2-х политик для DLP-системы Infowatch, учитывающих специфику и направление деятельности организации, согласно представленному выше описанию.

Конкурсант готовит отчёт в формате.docx, суммирующий итоги исследования организации. Графические иллюстрации (при наличии) должны быть внутри документа.

Итоговый документ должен быть сдан на USB носителе (в корневом каталоге) под названием Модуль_2_Аудит_<Фамилия участника>.docx

Главный эксперт распечатывает документ и отдаёт участнику на проверку на 5 минут. После чего участник обязан расписаться на документе и сдать бумажную копию Главному эксперту. Работа не принимается к оценке без наличия печатной копии с подписью конкурсанта.

Задание считается выполненным при условии подписанного отчета и устного доклада участника об окончании работ.

Модуль С: Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз.

Технологии этого модуля: DLP-система, корпоративная система защиты информации от внутренних угроз

Время на выполнение: 3-5 часа

Пример задания

Создайте в системе InfoWatch Traffic Monitor политики безопасности согласно нижеперечисленным заданиям.

- Политики должны автоматически блокировать трафик и/или предупреждать о нарушении в соответствии с заданием.
- Некоторые политики должны быть созданы с нуля, некоторые могут быть сделаны путём модификации существующих в системе.
- Для некоторых политик необходима работа с разными разделами консоли управления TM: категориями и терминами, технологиями, объектами защиты и т. п. Способ, которым создана корректная политика, оставлен на усмотрение самого экзаменуемого.
- При выявлении уязвимости DLP-система должна автоматически устанавливать уровень угрозы в соответствии с заданием (если в задании это не указано явно, участник должен самостоятельно задать уровень угрозы при разработке политики).
- Списки сотрудников, занимаемые позиции и отделы сотрудников (HR, Accounting и др.) представлены в разделе «Персоны» Infowatch Traffic Monitor по результатам LDAP-синхронизации с AD-сервером компании

- После создания всех политик будет запущен автоматический «генератор трафика», который передаст на InfoWatch Traffic Monitor поток данных, содержащих как утечки, так и легальную информацию.
- При правильной настройке политики InfoWatch Traffic Monitor должны автоматически выявить (или блокировать) и маркировать инциденты безопасности. Не должно быть ложных срабатываний, т. к. легальные события не должны маркироваться как вредоносные. Не должно быть неправильной маркировки. Должны быть выявлены все инциденты безопасности.
- Внимание! Необходимо называть политики/объекты/категории и прочие объекты в соответствии с номером и названием задания, например «Задание 1», «Политика 4», «Политика 10», «Объект 1». Без верно названных объектов проверка вашего задания может стать невозможной. При выполнении задания учитывайте, что совместно с созданными могут срабатывать стандартные политики, что необходимо предотвратить.
- В комплексных заданиях необходимо пользоваться объектами защиты.
- Задания можно выполнять в любом порядке.
- Проверьте синхронизацию времени на всех системах, т. к. расхождение во времени между системами может повлиять на актуальность событий.
- Для некоторых политик могут понадобиться дополнительные файлы, которые можно найти в папке «Additional files» в общей папке из дополнительных сведений.
- Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). В этом случае необходимо протоколировать свои результаты с помощью двух скриншотов для каждого задания (скриншот заданной политики и скриншот ее работы). Для некоторых заданий необходимо после фиксации результатов в виде скриншотов удалить заданную политику, что будет оговорено отдельно в тексте задания.
- Все скриншоты необходимо сохранить на рабочем столе в папке.

  Формат названия скриншотов политик:

  Пример 1 для сохранения скриншота созданной политики: CP-1.jpg

  где CP – сокращение от англ. creating a policy,

  1 – номер задания

  Пример 2 для сохранения скриншота работающей политики: PW-1.jpg

  где PW – сокращение от англ. policy work,

  1 – номер задания.

Пример 3 для сохранения нескольких скриншотов одной работающей политики:

PW-1-2.jpg

где PW – сокращение от англ. policy work,

1 – номер задания;

2 – номер скриншота для задания 1.

При проверке политик стоит учитывать, что нарушителем могут являться не только указанные в задании пользователи, а еще и виртуальная машина с агентом мониторинга (для проверки сработки политик). Необходимо учитывать данное условие при разработке и проверке политик.

Задание 1

Создайте локальную группу пользователей «Подозрительные» в Traffic Monitor. Добавьте в нее пользователя домена виртуальной клиентской машины.

Подтвердите выполнение задания скриншотами.

Задание 2

Для работы системы необходимо настроить периметр компании:

- Почтовый домен: demo.lab.
- Список веб ресурсов (необходимо создать новый список ресурсов, назвав его «Доверенные домены»): worldskills.moscow, worldskills.ru, new.guap.ru.
- Необходимо создать новый список ресурсов, назвав его «Доверенные».
- Группа персон: пользователи домена.
- Исключить из перехвата почту генерального директора.

Подтвердите выполнение задания скриншотами.

Задание 3

Для недавно нанятого аудитора компании необходимо создать пользователя системы IWTM с правами доступа только на чтение и выполнение отчетов, сводок и событий, а также на просмотр каталога локальных и доменных пользователей.

Логин: newauditor, пароль: xxXX1234

Подтвердите выполнение задания скриншотами настройки прав пользователя.

Задание 4

В связи с постоянными проблемами при организации очередного чемпионата WorldSkills (Корпоративный Чемпионат), совет директоров решил контролировать передачу информации о WorldSkills и межвузовском чемпионате за пределы компании. В связи с этим необходимо создать политику в InfoWatch Traffic Monitor

на правило передачи текстовых данных за пределы компании (на адрес вне домена), содержащих слова «ВорлдСкиллз», «WorldSkills», «Региональные» и «Reg2021».

Необходимо учесть, что в словах могут содержаться комбинации латиницы и кириллицы, а также стоять или не стоять пробел между словами, например: «Ворлд Skills», «Reg 2021». Ложных срабатываний быть не должно (например, просто на Рег или Skills).

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 4

Проверить работоспособность.

Модуль D: Технологии защиты и анализа сетевого трафика.

Технологии этого модуля: технологии защиты сетевого трафика VPN VipNET, PKI-системы (ViPNet УЦ, Publication Service и др.)

Время на выполнение: 3-4 часа

Пример задания

Задание 1.1. Установка ПО ViPNet Administrator для создания защищённой сети:

- Установить и настроить рабочее место администратора VipNet: центр управления сетью (серверное и клиентское приложение ЦУС), Удостоверяющий и ключевой центр (УКЦ).

Если были произведены изменения паролей, IP-адресов и так далее, необходимо отразить это в отчете.

Задание 1.2. Установка ПО ViPNet Coordinator и ПО VipNet Client на соответствующие виртуальные машины:

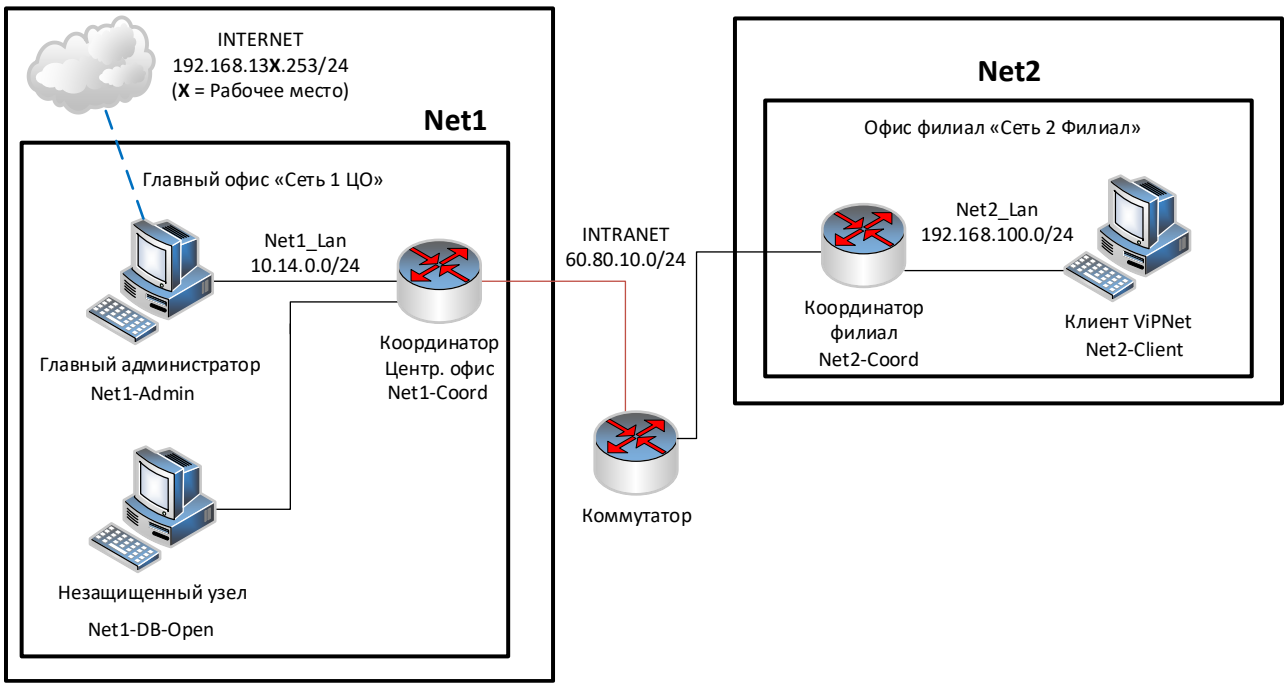
- На компьютере на Net1-Admin (ЦО) установить ПО ViPNet Client (Windows), рабочее место администратора;
- На компьютере на Net1-Coord (ЦО) установить ПО ViPNet Coordinator (Windows);
- На компьютере на Net2-Coord (Филиал) установить ПО ViPNet Coordinator (Windows);
- На ВМ на Net2-Client (филиал) установить ПО ViPNet Client, рабочее место пользователя;

Необходим скриншот первого запуска приложения.

Задание 2. Защита локально-вычислительной сети предприятия с применением ПО ViPNet

Необходимо использовать рабочее место администратора (созданное ранее) для создания структуры защищенной сети, развернуть с помощью технологии виртуальных машин сеть предприятия и настроить необходимые АРМ в соответствии с заданными ролями.

Схема сети, которую требуется создать, приведена ниже.



В итоге выполнения задания должны быть развернуты и настроены следующие сетевые узлы защищенной сети (см. таблицу).

Таблица 1 Узлы защищенной сети если УКЦ и ЦУС на одной машине.

Вирт. машина	Название сетевого узла	ПО VipNet	ОС сетевого узла	Имя пользователя сетевого узла, уровень полномочий
Net1-Admin (ЦО)	Главный администратор (VM)	ViPNet Administrator (ЦУС клиент и сервер + УКЦ) ViPNet Client	ОС Windows Server	Admin

Вирт. машина	Название сетевого узла	ПО VipNet	ОС сетевого узла	Имя пользователя сетевого узла, уровень полномочий
Net1-Coord (ЦО)	Координатор Центр Офис (VM)	ViPNet Coordinator	ОС Windows 10	CoordinatorOffice
Net2-Coord (Филиал)	Координатор Филиал (VM)	ViPNet Coordinator	ОС Windows 10	CoordinatorSub
Net2-Client (филиал)	Пользователь_2 Филиал (VM)	ViPNet Client	ОС Windows 10	User2

Связи между узлами необходимо настроить самостоятельно.

Таблица 2. Схема связей пользователей

Схема связей пользователей	**Coordinator Office**	**Admin**	**Coordinator Subsidiary**	**User2**
CoordinatorOffice	×	*	*	
Admin	*	×		*
CoordinatorSub	*		×	*
User2		*	*	×

Модуль Е: Технологии защиты узла и агентского мониторинга

Технологии этого модуля: Агентский монитор DLP, средства защиты узла, групповые политики ОС Active Directory

Время на выполнение: 2 часа

Пример задания

Задания выполняются с помощью компонентов DLP системы InfoWatch.

Все сценарии заданий (где применимо) необходимо воспроизвести и зафиксировать результат.

Необходимо убедиться в корректном отображении результата в сводках событий.

Называйте созданные вами разделы/политики/группы и т. д. в соответствии с заданием, например «Политика 1» или «Политика 1-2» и т. д.

Для некоторых политик могут понадобиться дополнительные файлы, которые можно найти на диске “D” хост-машины.

Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). В этом случае необходимо протоколировать свои результаты с помощью двух скриншотов для каждого задания (скриншот заданной политики и скриншот ее работы). Для некоторых заданий необходимо после фиксации результатов в виде скриншотов удалить заданную политику, что будет оговорено отдельно в тексте задания.

Все скриншоты необходимо сохранить на рабочем столе в папке «Модуль 5».

Формат названия скриншотов политик:

Пример 1 для сохранения скриншота созданной политики: CP-1.jpg

где CP – сокращение от англ. creating a policy,

1 – номер задания

Пример 2 для сохранения скриншота работающей политики: PW-1.jpg

где PW – сокращение от англ. policy work,

1 – номер задания.

Пример 3 для сохранения нескольких скриншотов одной работающей политики:

PW-1-2.jpg

где PW – сокращение от англ. policy work,

1 – номер задания;

2 – номер скриншота для задания 1.

Задание 1

Необходимо установить (сменить) пароль для удаления Device Monitor Agent всех виртуальных машин нарушителей с помощью средств DeviceMonitor Server (удаленно). Пароль: xxXX1357.

Проверить работоспособность и зафиксировать выполнение скриншотом

Задание 2

Необходимо создать новую политику (кроме политики на устройства по умолчанию), назвав ее «Региональные2021», применить ее к группе компьютеров по умолчанию.

Последующие правила по заданиям должны быть добавлены в эту политику.

Зафиксировать выполнение скриншотом.

Задание 3

Для удобства работы офицера безопасности необходимо установить дополнительную консоль управления IWDM на хост-машину (компьютер с виртуальными машинами) для удаленного доступа к серверу IWDM.

Проверить работоспособность, зафиксировать выполнение скриншотом запущенной консоли на хост-машине.

Задание 4

Необходимо запретить пользоваться Microsoft Paint, а также Paint 3D (при наличии), так как участились случаи подделки печатей компании.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Пример заданий на групповые политики

Групповая политика 1:

С помощью редактора групповой политики запретить доступ к реестру. Выполнение задания подтвердить скриншотами.

Групповая политика 2:

Защита RDP-сессии с помощью SSL/TLS. создайте групповую политику, которая будет применять шифрование при подключении по RDP. Выполнение задания подтвердить скриншотами.

Групповая политика 3:

С помощью редактора групповой политики Настройте запрет установки программ для пользователей. Выполнение задания подтвердить скриншотами.

Модуль F: Предотвращение инцидентов и управление событиями информационной безопасности

Технологии этого модуля: подсистемы отчетов и сводок DLP/VPN, средства детектирования и предотвращения вторжений (IDS/IPS), системы менеджмента событий информационной безопасности (SIEM), текстовые редакторы и электронные таблицы

Время на выполнение: 3 часа

Пример заданий

Задание 1

1. Развернуть ViPNet IDS VA из OVA образа в среде VirtualBox или VMWare Workstation, но сетевые интерфейсы настроены не до конца.
    a. Использовать один сетевой интерфейса как…., другой для …..
    b. Активировать лицензию
    c. Настроить добавить нового администратора системы с полным доступом, а также создать ограниченную учетную запись.
    d. Настроить сетевые интерфейсы управления и перехвата в соответствии с рис. 1.
    e. Загрузить и применить актуальные сигнатуры.
2. Развернуть ViPNet TIAS из OVA образа в среде VirtualBox или VMWare Workstation.
3. Подключить установленный ранее IDS VA в качестве сенсора.

Зафиксировать выполнение задания скриншотами.

Задание 2. Базовая работа с правилами ViPNet IDS VA

1. Создать и применить пользовательское правило ViPNet IDS VA обнаружения попыток доступа к сетевым папкам ноутбука. Проверить выполнение с помощью ПК и ноутбука.
2. Создать и применить пользовательское правило обнаружение ping пакетов. Проверить выполнение с помощью ПК и ноутбука.
3. Провести детектирование трафика согласно указанным правилам с помощью IDS-VA

Зафиксировать выполнение задания (правила и обнаруженные события в IDS) скриншотами.

Задание 3 Проверка системы на выявление известной атаки: IDS+TIAS

1. Самостоятельно, с помощью утилит Kali Linux имитировать атаку (на выбор участника) на уязвимую виртуальную машину с Win10 или Win7
2. Зафиксировать детектирование атаки с помощью IDS-VA: вкладка *События*
3. Зафиксировать детектирование атаки с помощью TIAS: вкладки *События* и *Инциденты*
4. Подготовить отчет об обнаруженной атаке согласно прилагаемому в дополнительных файлах шаблону. Название файла – *Отчет об известной атаке.docx*

5. Критерии оценки

Таблица 2.

Критерий		Баллы		
		Судейские аспекты	Объективная оценка	Общая оценка
A	Организация работы и управление		5,00	5,00
B	Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз		15,00	15,00
C	Отчетность и нормативно-правовое обеспечение корпоративной безопасности	5,00	2,00	7,00
D	Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз		20,00	20,00
E	Технологии анализа и защиты сетевого трафика		25,00	25,00
F	Технологии защиты узла и агентского мониторинга		17,00	17,00
G	Предотвращение инцидентов и управление событиями информационной безопасности		11,00	11,00
Итого		5	95	100