Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Безопасность компьютерных систем (продвинутый уровень)

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Оценочные материалы
по дисциплине
Технологии проактивной защиты информационных систем

Москва
2022

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Поляк Р.И. Идентификатор: Rbc0e923e-PoliakRI-10208dd2	Р.И. Поляк
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

ОБЩАЯ ЧАСТЬ

Оценочные материалы по дисциплине предназначены для оценки: достижения обучающимися запланированных результатов обучения по дисциплине, этапа формирования запланированных компетенций и уровня освоения дисциплины.

Оценочные материалы по дисциплине включают оценочные средства для проведения мероприятий текущего контроля успеваемости и промежуточной аттестации.

Формируемые у обучающегося компетенции:

1. ПК-2 Готов к внедрению систем защиты информации автоматизированных систем
   ПК-2.3 Внедряет организационные меры по защите информации в автоматизированных системах

и включает:

для текущего контроля успеваемости:

Форма реализации: Выполнение задания

1. Анализ угроз безопасности с использованием технологий проактивного поиска, обнаружения событий в сети и сбора событий с конечных устройств на основе ОС Windows. (Отчет)
2. Изучение технологий эвристического детектирования и поведенческого анализа в контролируемой изолированной среде на основе ОС Windows (Отчет)
3. Разработка архитектуры системы проактивной защиты в организации (Контрольная работа)
4. Разработка модели безопасности компьютерной системы (Кейс (решение конкретных производственных ситуаций))
5. Разработка плана осведомленности по вопросам ИБ (Отчет)

Форма реализации: Компьютерное задание

1. Практика интеграции IDS/IPS в компьютерную сеть (Лабораторная работа)
2. Практика применения технологии настройки защищенной виртуальной машины (Лабораторная работа)
3. Разработка эвристических алгоритмов с помощью Yara (Лабораторная работа)

Форма реализации: Письменная работа

1. Разработка корреляционных правил при использовании SIEM систем (Отчет)

БРС дисциплины

6 семестр

Раздел дисциплины	Веса контрольных мероприятий, %								
	Индекс КМ:	КМ-1	КМ-1	КМ-2	КМ-2	КМ-3	КМ-3	КМ-3	КМ-4	КМ-4
	Срок КМ:	4	4	8	8	12	12	12	15	15
Введение										
Тема 1. Введение в проактивную защиту			+							
Проактивная защита конечных устройств (endpoint protection)										

Тема 2. Организация проактивной защиты на базе защитных механизмов, встроенных в ОС (Windows, Linux).				+	+				
Тема 3. Технологии виртуализации в задачах проактивной защиты.	+			+	+				
Тема 4. Технологии эвристического детектирования и поведенческого анализа			+	+	+	+			
Тема 5. Решения класса endpoint protection.			+	+	+	+			
Проактивная защита сетевого периметра (network protection)									
Тема 6. Технологии мониторинга и обнаружения событий в сети.			+			+	+		+
Тема 7. Введение в threat hunting.			+			+			+
Тема 8. Технология Threat Intelligence.			+			+			+
Тема 9. Основы построения защищённых компьютерных сетей.									+
Тема 10. Решения для защиты компьютерных сетей									+
Совершенствование проактивной защиты в ИС									
Тема 11. Перспективные технологии проактивной защиты.								+	
Тема 12. Организационные меры проактивной защиты.								+	
Вес КМ:	10	10	15	10	10	10	10	10	15

$Общая часть/Для промежуточной аттестации$

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ

I. Оценочные средства для оценки запланированных результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Индекс компетенции	Индикатор	Запланированные результаты обучения по дисциплине	Контрольная точка
ПК-2	ПК-2.З$_{ПК-2}$ Внедряет организационные меры по защите информации в автоматизированных системах	Знать: основные понятия и назначение технологий проактивной защиты, в т.ч. использующие перспективные технологии проактивной защиты основные виды, назначение и принцип работы современных средств защиты информации, использующих проактивные технологии и технологии реализации моделей безопасности компьютерных систем технологию создания правил, детектирующих угрозы безопасности современных компьютерных систем Уметь: выбирать и применять средства защиты	Изучение технологий эвристического детектирования и поведенческого анализа в контролируемой изолированной среде на основе ОС Windows (Отчет) Анализ угроз безопасности с использованием технологий проактивного поиска, обнаружения событий в сети и сбора событий с конечных устройств на основе ОС Windows. (Отчет) Разработка архитектуры системы проактивной защиты в организации (Контрольная работа) Разработка модели безопасности компьютерной системы (Кейс (решение конкретных производственных ситуаций)) Практика применения технологии настройки защищенной виртуальной машины (Лабораторная работа) Разработка эвристических алгоритмов с помощью Yara (Лабораторная работа) Разработка корреляционных правил при использовании SIEM систем (Отчет) Практика интеграции IDS/IPS в компьютерную сеть (Лабораторная работа) Разработка плана осведомленности по вопросам ИБ (Отчет)

		информации, использующих проактивные технологии, для нейтрализации угроз безопасности современных компьютерных систем анализировать причины нарушения функционирования средств защиты информации, использующих проактивные технологии внедрять организационные меры политик обновления системного и прикладного ПО, резервного копирования и управления уязвимостями применять навыки интеграции средств защиты информации, использующих проактивные технологии и автоматизации их настроек при выявлении угроз безопасности современных компьютерных систем применять навыки администрирования средств защиты информации, использующих проактивные технологии	

		применять инструменты создания правил, детектирующих угрозы безопасности	

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Практика применения технологии настройки защищенной виртуальной машины

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Лабораторная работа
Вес контрольного мероприятия в БРС: 10
Процедура проведения контрольного мероприятия: Проверка задания преподавателем

Краткое содержание задания:

Поведенческий анализ файлов в среде Cuckoo sandbox

Для выполнения данного задания понадобится ВМ с Windows из прошлого раздела + доп. ВМ с ОС Debian или Ubuntu

Ход работы:

1. Установить cuckoo sandbox, согласно инструкции https://cuckoo.sh/docs/installation/index.html . В качестве гостевой машины использовать ВМ с Windows из прошлого раздела
2. Проверить корректность установки (критических ошибок в host машине быть не должно)
3. Запустить cuckoo https://cuckoo.sh/docs/usage/start.html
4. Загрузить в cuckoo утилиту Mimikatz на анализ
5. Дождаться окончания анализа и изучить результат
6. Описать функционал программы по результатам анализа.
7. Сделать вывод по данной части задания

Контрольные вопросы/задания:

Уметь: применять навыки администрирования средств защиты информации, использующих проактивные технологии	1.Виртуализация в информационной безопасности 2.Порядок настройки защищенной виртуальной машины

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-1. Разработка модели безопасности компьютерной системы

Формы реализации: Выполнение задания
Тип контрольного мероприятия: Кейс (решение конкретных производственных ситуаций)
Вес контрольного мероприятия в БРС: 10
Процедура проведения контрольного мероприятия: Проверка задания преподавателем

Краткое содержание задания:

По модели Белла-ЛаПадуллы
Пусть имеется мандатная система доступа Σ(v0,Q, FT), в которой решетка уровней безопасности ΛL является линейной и имеет три уровня – *l1, l2, l3; l1>l2> l3; l1>l3*.
Пусть имеется следующая система субъектов (пользователей) доступа:
u1 – администратор системы;
u2 – руководитель предприятия;
u3 – делопроизводитель;
u4 – user, т.е. рядовой непривилегированный пользователь.
Пусть имеется следующая система объектов доступа:
o1 – системное ПО;
o2 – документ "Стратегия выхода предприятия на новые рынки сбыта продукции";
o3 – документ "Приказ о поощрении работников по случаю Дня Предприятия";
o4 – АИС "Борей" (прием, обработка и исполнение заказов клиентов) (ПО и БД).
Задача № 1. Обосновать и составить систему уровней допусков пользователей, грифов секретности объектов доступа и матрицу доступа A[*u,o*] .
Задача № 2. Составить и обосновать систему допусков и грифов секретности для двух состояний системы:
Состояние I – Подготовка (разработка) документа *o2*.
Состояние II – Документ *o2* утвержден и введен в действие.

Контрольные вопросы/задания:

Уметь: анализировать причины нарушения функционирования средств защиты информации, использующих проактивные технологии	1.Дискреционный контроль доступа Windows. Дескриптор безопасности и разрешения 2.Мандатный контроль целостности. Стандартная политика. Примеры использования. 3.Основная концепция безопасности. Разграничение прав доступа. Основные правила и модели

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-2. Разработка эвристических алгоритмов с помощью Yara

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Лабораторная работа
Вес контрольного мероприятия в БРС: 15
Процедура проведения контрольного мероприятия: Проверка задания преподавателем

Краткое содержание задания:

Детектирование угроз с помощью Yara-эвристик

Третья часть задания выполняется в подготовленной виртуальной машине (ВМ) с ОС Windows, полученной в ходе выполнения первой части данного задания

Документация по yara - https://yara.readthedocs.io/en/latest/

Ход работы:

1. Для создания правил следует использовать установленные на ВМ инструменты. Такие как hex редактор, strings…
2. Создать yara правило для детектирования след. файла https://support.kaspersky.ru/downloads/eicar/eicar.zip
3. Создать yara правило для детектирования утилиты Mimikatz
4. Создать yara правило для детектирования doc, xls, pdf документов (Любые, на свой выбор)
5. Создать yara правило для детектирования pe, elf файлов (Любые, на свой выбор)
6. Создать yara правило для детектирования группы файлов***** (одного расширения и схожие по параметрам, которые Вы должны определить сами. Любые, на свой выбор)
7. Используя созданные yara правила просканировать файловую систему ВМ. Созданные правила должны детектировать только те файлы, для детекта которых они написаны (включая группы файлов).
8. В случае выявления FP срабатываний, исправить их. Все FP отразить в отчете и описать процесс их устранения
9. Сделать вывод по данной части задания

Примечание: после создания каждого yara правила проверить его работоспособность.

Контрольные вопросы/задания:

Уметь: применять инструменты создания правил, детектирующих угрозы безопасности	1.Язык Yara. Синтаксис. Принцип написания детектирующих правил. 2.Детектирование исполняемых файлов (PE, ELF) с помощью эвристических алгоритмов

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-2. Изучение технологий эвристического детектирования и поведенческого анализа в контролируемой изолированной среде на основе ОС Windows

Формы реализации: Выполнение задания
Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 10
Процедура проведения контрольного мероприятия: Проверка задания преподавателем

Краткое содержание задания:

Изучение основных компонентов архитектуры безопасности ОС Windows
Задание выполняется в виртуальной машине (ВМ) с ОС Windows
Ход работы:

1. Установить VirtualBox https://www.virtualbox.org/wiki/Downloads
2. Скачать ВМ ОС Windows 10 для Virtual Box. https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/
3. Импортировать ВМ в virtual box
4. Запустить ВМ. (Данные для входа - IEUser:Passw0rd!)
5. По-умолчанию, виртаульная машина уже должна иметь активированную 90 дневную пробную лицензию. В случае неоднократного появления сообщения о необходимости проведения процедуры активании, необходимо выполнить следующее: «Откройте cmd.exe и активируйте 90-дневную лицензию, введя slmgr / ato»
6. Сделать снэпшот текущего состояния ВМ
7. Установить необходимый софт (https://github.com/fireeye/flare-vm). Данные программы понадобятся позже, при выполнении 3 части ДЗ-1 и ДЗ-2.
8. Скачать Process Explorer (https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer)
9. Сделать снэпшот текущего состояния ВМ
10. Запустить Process Explorer от имени администратора (есть в , изучить программу.
11. Найти все компоненты безопасности ОС Windows о которых шла речь во время лекционных и практических занятий (указать названия компонентов и путь к файлам. Сделать в виде таблицы)
12. Изучить процесс lsass.exe. Перечислить и описать компоненты процесса
13. Скачать утилиту Mimikatz (https://github.com/gentilkiwi/mimikatz/releases). При необходимости, отключить Windows Defender.
14. Запустить утилиту mimikatz от имени администратора (https://github.com/gentilkiwi/mimikatz/releases) и выполнить следующие команды
15. Проанализировать полученные данные и записать их в отчет
16. Запустить cmd.exe от имени администратора и выполнить следующую команду: «**reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1**»
17. Перезагрузить ВМ
18. Повторить п.14
19. Проанализировать полученные данные, сравнить их с данными, полученными из п.15 и записать результат в отчет.
20. Ответить на вопрос: «Почему был получен пароль пользователя в открытом виде и с проблемой какого компонента безопасности это связано?»
21. Исправить проблему в компоненте безопасности Windows (для необходимо внести соответствующие изменения в системный реестр).
22. Повторить п.17
23. Сделать вывод по данной части задания

Доп. Задание (со звездочкой):

Скомпилировать Mimikatz таким образом, чтобы скачивание, перемещение в ФС и запуск не детектировался Windows Defender’ом.

Контрольные вопросы/задания:

Знать: основные понятия и назначение технологий проактивной защиты, в т.ч. использующие перспективные технологии проактивной защиты	1.Проактивная защиты информационных систем. Достоинства и недостатки. Отличия от реактивных методов 2.ОС Linux. Подсистемы безопасности. краткое описание и примеры использования 3.Подсистемы безопасности ОС Windows

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-3. Разработка архитектуры системы проактивной защиты в организации

Формы реализации: Выполнение задания
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 10
Процедура проведения контрольного мероприятия: Проверка задания преподавателем

Краткое содержание задания:
Построение системы проактивной защиты на базе SIEM Qradar

Требования
Windows 7/8/8.1/10 x64
Virtualbox
CPU 4 Core, 16 Gb RAM
CentOS 7.5 (Окружение GNOME)
https://developer.ibm.com/qradar/wp-content/uploads/sites/89/2018/08/b_qradar_community_edition.pdf
Задачи контрольной работы
1. Развернуть SIEM Qradar CE
2. Настроить отправку событий журналов безопасности Windows (из созданной ВМ в 1 ДЗ) в SIEM систему (На отлично, настроить отправку журналов sysmon)
3. Сделать парсинг событий Windows security events (в кол-ве достаточном, для выполнения данной части ДЗ)
4. Написать правила корреляции:
Запуск teamviewer

Использование mimikatz (не только запуск!!!)
Детектирование любой атаки из матрицы Mitre / Kill Chain

Контрольные вопросы/задания:

Знать: основные виды, назначение и принцип работы современных средств защиты информации, использующих проактивные технологии и технологии реализации моделей безопасности компьютерных систем	1.SIEM системы. Основные механизмы и решаемые задачи. 2.SIEM системы. Типовая архитектура.

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-3. Анализ угроз безопасности с использованием технологий проактивного поиска, обнаружения событий в сети и сбора событий с конечных устройств на основе ОС Windows.

Формы реализации: Выполнение задания
Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 10
Процедура проведения контрольного мероприятия: Проверка задания преподавателем

Краткое содержание задания:
Изучение возможностей SIEM-системы IBM Qradar
Вводная информация
Допускается выполнение ДЗ-2 в группах по 5 человек.
Изучение возможностей SIEM-системы IBM Qradar
Полезные ссылки:
https://developer.ibm.com/qradar/ce/
https://developer.ibm.com/qradar/wp-content/uploads/sites/89/2020/02/b_qradar_community_edition_7.3.3GA_v1.0.pdf
https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/com.ibm.dsm.doc/b_dsm_guide.pdf?origURL=SS42VS_DSM/b_dsm_guide.pdf
https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.3/com.ibm.qradar.doc/b_qradar_gs_guide.pdf
https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.3/com.ibm.qradar.doc/b_qradar_users_guide.pdf

https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
https://ibm.ent.box.com/s/ich0yyiw54y0ek6s9a66xvtjku8e42rc/file/619638909365
https://attack.mitre.org/

Задачи:

1. Установить SIEM Qradar CE в ВМ на основе CentOS
2. Изучить интерфейс и основные компоненты SIEM Qradar CE
3. Настроить отправку событий журналов безопасности Windows Sysmon (из созданной ВМ в 1 ДЗ) в SIEM систему.
4. Сделать парсинг событий Windows security events (в кол-ве, достаточном, для выполнения данной части ДЗ)
5. Написать правило корреляции на запуск Remote Access Tool (RAT).

№ варианта	**Название RAT**
1	TeamViewer
2	AmmyAdmin
3	AnyDesk
4	VNC
5	LogMeIn

Дополнительно ответить на вопрос: чем может быть опасен RAT в корпоративной сети.

6. Написать правило корреляции на использование mimikatz на хосте (не только запуск!!!).
7. (На оценку отлично) Детектирование любой техники из матрицы Mitre ATT&CK до этапа Command and Control. **У команд не должно быть пересечений в выбранных техниках!!!**
8. Подготовить выводы и сделать схему получившейся инфраструктуры.

Контрольные вопросы/задания:

Знать: технологию создания правил, детектирующих угрозы безопасности современных компьютерных систем	1.Технологии сбора событий (winlogbeat, auditbeat, auditd). 2. Sysmon. Назначение. Виды событий. 3.Технологии хранения и анализа событий (ELK stack).

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-3. Разработка корреляционных правил при использовании SIEM систем

Формы реализации: Письменная работа
Тип контрольного мероприятия: Отчет

Вес контрольного мероприятия в БРС: 10
Процедура проведения контрольного мероприятия: Проверка задания преподавателем

Краткое содержание задания:

1 Вариант.

Разработка программы (скрипта) для обогащения IP фидов.

Необходимо написать скрипт, которому на вход подаешь IPv4 адрес. На выходе получаешь JSON с обогащенной информацией. Полученный JSON должен содержать следующее:

1. Whois информацию (страна, хостер, hostname (если есть)…)
2. Детекты антивирусных движков, наличие в black листах. Отобразить в виде бинарного значения (к примеру, «clean или malicious» или «clean или blacklisted»). Если присутствуют детекты по IP, отдельным полем отобразить названия движков в виде списка (К примеру “detect_engines” : “Kaspersky, ESET, Symantec”
3. Разрешается использовать вложенный json

В качестве основного источника данных для обогащения рекомендуется использовать https://developers.virustotal.com/v3.0/reference#overview

ЯП – любой на выбор. Интерфейс – консольный, с help информацией.

2 Вариант

Разработка модели для обогащения IP фидов.

Необходимо разработать модель обогащения IP open source фидов. За основу взять IP фид с https://threatfeeds.io (1 любой, на выбор) и проработать процесс обогащения. От простого IP до полноценного IP фида. Для этого нужно:

1. Выявить необходимые для фида данные (исходя из контекста фида) – какой информацией обогащать, сколько внешних источников использовать и т.д. К примеру, если фид по малваре, то необходимо, как минимум, обогащать вердиктами антивирусных движков.
2. Определить структуру обогащенных фидов (json или csv, поля и их название и т.д.)
3. Полученные данные структурировать и отобразить в visio в виде схемы.

Обязательно указать пример обогащенного IP фида со всеми полями и их описанием (делается руками по заданной модели). На схеме должны быть указаны взаимосвязи с внешними источниками для обогащения.

Контрольные вопросы/задания:

Уметь: выбирать и применять средства защиты информации, использующих проактивные технологии, для нейтрализации угроз безопасности современных компьютерных систем	1.Threat Intelligence. Фиды. Обогащение и анализ. Привести примеры. 2.Порядок сбора и аккумуляция данных. 3.Обогащение и анализ полученных данных.

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60

Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-4. Разработка плана осведомленности по вопросам ИБ

Формы реализации: Выполнение задания
Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 10
Процедура проведения контрольного мероприятия: Проверка задания преподавателем

Краткое содержание задания:

В организации рекомендуется разработать программу и план регулярного обучения и повышения осведомленности в области информационной безопасности.
Программу и план обучения и повышения осведомленности необходимо разработать по следующим основным направлениям:
- повышение осведомленности работников организации по вопросам исполнения регламента обнаружения событий ИБ и оповещения о них, в том числе по составу событий ИБ;
- повышение осведомленности представителей внешних организаций и клиентов организации, использующих информационную инфраструктуру организации, о порядке и процедурах информирования организации об обнаруженных инцидентах ИБ;
- обучение и повышение осведомленности членов ГРИИБ и работников организации, привлекаемых к реагированию на инциденты ИБ, по вопросам сбора, фиксации и документирования информации об инцидентах ИБ, использования классификатора инцидентов ИБ;
- обучение и повышение осведомленности членов ГРИИБ и работников организации, привлекаемых к реагированию на инциденты ИБ, с целью приобретения знаний по технической эксплуатации информационной инфраструктуры организации, позволяющих осуществить оперативное закрытие инцидентов ИБ;
- обучение работников подразделений информатизации организациипо вопросам эксплуатации технических средств;
- обучение работников службы ИБ организации по вопросам контроля эксплуатации технических средств.
Рекомендуется ознакомление работников организации с процедурой информирования о событиях ИБ, а также о необходимости незамедлительного сообщения об обнаруженных событиях ИБ оператору-диспетчеру ГРИИБ. В процедуры ознакомления рекомендуется включать:
- перечень или описание событий ИБ, о которых требуется сообщать;
- форму сообщения о событиях ИБ, включая детали, существенные для классификации инцидента ИБ, и описание действий по реагированию (например, о типе несоответствия или нарушения, возникновениях неправильных срабатываний, появлении сообщений на экране, нетипичном поведении);
- способы первичного документирования информации о событиях ИБ;
- рекомендации по поведению в случае явных нарушений ИБ, например о выполнении или, наоборот, запрете каких-либо действий, кроме немедленного оповещения оператора-диспетчера ГРИИБ.

Контрольные вопросы/задания:

Уметь: внедрять организационные меры политик обновления системного и прикладного ПО, резервного копирования и управления уязвимостями	1.Порядок разработки основного содержания программы повышения осведомленности в области информационной безопасности 2.Порядок разработки основного содержания плана повышения осведомленности в области информационной безопасности в организации

Описание шкалы оценивания:

Оценка: зачтено
Описание характеристики выполнения знания:

Оценка: не зачтено
Описание характеристики выполнения знания:

КМ-4. Практика интеграции IDS/IPS в компьютерную сеть

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Лабораторная работа
Вес контрольного мероприятия в БРС: 15
Процедура проведения контрольного мероприятия: Проверка задания преподавателем

Краткое содержание задания:

Разработка демо-платформы Threat Hunting на основе ELK stack
Полезные ссылки:
https://www.elastic.co/elastic-stack
https://www.elastic.co/beats
Задачи:
1. Развернуть Elastic stack последней версии в виртуальной машине Unix (Debian или Ubuntu)
2. Изучить компоненты Elastic stack, включить в отчет их краткое описание.
3. Изучить агенты сбора событий с источников (beats), выбрать и обосновать выбор агентов для сбора событий с ВМ и создания системы проактивного поиска угроз
4. Создать hunt для детектирования (На выбор):
Техники Remote Access Tool (RAT) - https://attack.mitre.org/techniques/T1219/
Техники Credential dumping - https://attack.mitre.org/techniques/T1003/
(На оценку отлично) Suspicious powershell - https://attack.mitre.org/techniques/T1086/
5. Добавить функционал детектирования по threat intelligence фидам.

Контрольные вопросы/задания:

Уметь: применять навыки интеграции средств защиты информации, использующих проактивные технологии и автоматизации их настроек при выявлении угроз безопасности современных компьютерных систем	1.Техники Threat Hunting. Визуализации и агрегации 2.Техники Threat Hunting. Машинное обучение 3.Источники информации и гипотез в Threat Hunting

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

6 семестр

Форма промежуточной аттестации: Зачет с оценкой

Пример билета

НИУ МЭИ	ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №1 Кафедра *Безопасности и информационных технологий* Дисциплина «Технологии проактивной защиты информационных систем» **Инженерно-экономический институт**	*Утверждаю:* *Зав. каф. БИТ* *А.Ю.Невский* *Протокол НМК ИЭБ*
1. ОС Linux. Подсистемы безопасности. краткое описание и примеры использования. 2. Threat Hunting. Источники информации и гипотез. 3. Практическое задание № 3		

Процедура проведения

Проверка преподавателем письменного ответа на вопросы билета

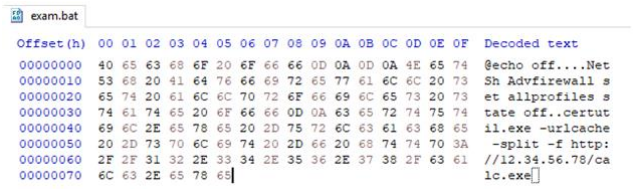
I. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины

1. Компетенция/Индикатор: ПК-2.З$_{ПК-2}$ Внедряет организационные меры по защите информации в автоматизированных системах

Вопросы, задания

1.Проактивная защиты информационных систем. Достоинства и недостатки. Отличия от реактивных методов.
2.Модели безопасности компьютерных систем. Дискреционная и мандатная политики.
3.ОС Linux. Основные компоненты архитектуры и их назначение. Принцип работы ядра.
4.ОС Linux. Подсистемы безопасности. краткое описание и примеры использования.
5.Архитектура ОС Windows.
6.Подсистемы безопасности ОС Windows.
7.Монитор состояния защиты (SRM). Взаимодействие с LSASS.
8.Active Directory. Домены. База данных. Управление учётными записями.
9.Сервис проверки подлинности локальной системы безопасности. Принцип работы. База политик.
10.Основные компоненты LSASS. Краткое описание и назначение.
11.Процесс входа пользователя в систему. Виды аутентификации пользователя.
12.Принцип работы протокола NTLM.
13.Принцип работы протокола Kerberos.
14.Управление доступом в ОС Windows.
15.Идентификаторы безопасности. Описание структуры. Привести пример идентификатору уровня «администратора домена» и уровня «Гость».
16.Токены доступа. Структура и применение.
17.Механизм олицетворения. Уровни привилегий.
18.Привилегии объектов и субъектов. Виды привилегий и их краткое описание.
19.Дискреционный контроль доступа Windows. Списки контроля доступа и определение прав.
20.Дискреционный контроль доступа Windows. Дескриптор безопасности и разрешения.
21.Мандатный контроль целостности. Уровни целостности.
22.Мандатный контроль целостности. Стандартная политика. Примеры использования.

23.User Account Control. Принцип работы. Примеры использования.
24.Основная концепция безопасности. Контроль доступа к ресурсам ОС.
25.Основная концепция безопасности. Разграничение прав доступа. Основные правила и модели.
26.Виртуализация. Основные преимущества. Виртуальные машины.
27.Виды виртуализации.
28.Виртуализация в информационной безопасности.
29.Технология песочниц. Применение и модели изоляции.
30.Технология песочниц. Принципы детектирования приложений песочницей.
31.Технология песочниц. Cuckoo sandbox. Архитектура и принцип работы.
32.Эвристические алгоритмы детектирования угроз.
33.Язык Yara. Синтаксис. Принцип написания детектирующих правил.
34.Поведенческий анализ. Блокиратор HIPS.
35.Эмуляция кода. Процесс детектирования. Собираемые артефакты.
36.Стандартные журналы событий ОС. Основные события безопасности. Виды журналов. Краткое описание назначения.
37.Sysmon. Назначение. Виды событий.
38.Threat Intelligence. Понятие, задачи и этапы. Примеры использования.
39.Threat Intelligence. Фиды. Сбор и аккумуляция данных. Привести примеры.
40.Threat Intelligence. Фиды. Обогащение и анализ. Привести примеры.
41.Мониторинг информационной безопасности. Виды мониторинга.
42.Системы мониторинга производительности и доступности. Их функции. Привести примеры.
43.SIEM системы. Основные механизмы и решаемые задачи. Примеры SIEM систем.
44.SIEM системы. Типовая архитектура.
45.SIEM системы. Применяемые методы и средства.
46.Межсетевой экран. Функции.
47.Межсетевой экран нового поколения (NGFW). Принцип работы. Отличия от классического межсетевого экрана. Примеры NGFW.
48.Межсетевой экран нового поколения (NGFW). Технологии внедрения в корпоративную сеть.
49.Фильтрация сетевого трафика. Списки контроля доступа.
50.Репутационные технологии. Преимущества и недостатки. Примеры использования.
51.Репутационные технологии. Whitelisting.
52.Репутационные технологии. Web, Email, File репутация.
53.Threat Hunting. Отличия от классического подхода по обнаружению угроз.
54.Threat Hunting. Источники информации и гипотез.
55.Threat Hunting. Процесс проверки гипотез. Привести пример.
56.Техники Threat Hunting. Базовый поиск.
57.Техники Threat Hunting. Статический анализ.
58.Техники Threat Hunting. Визуализации и агрегации.
59.Техники Threat Hunting. Машинное обучение.
60.Оценка эффективности защиты периметра сети.
61.Повышение осведомлённости сотрудников в области ИБ.
62.Политика обновления системного и прикладного ПО.
63.Политика резервного копирования.
64.Управление уязвимостями.
65.Data Science в ИБ. Основные задачи.
66.Data Science в ИБ. Применение. Привести примеры.
67.**Практическое задание №1**
Детектирование файлов с помощью Yara-правил.

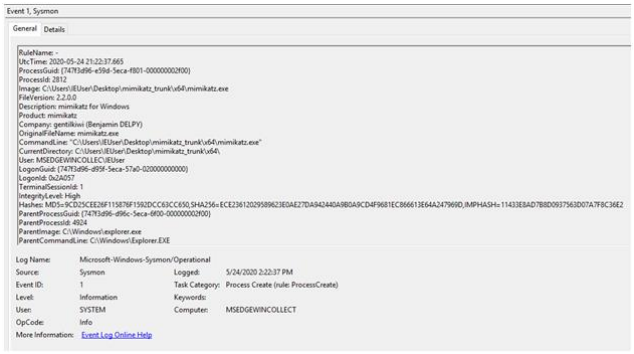


Дано шестнадцатеричное представление .bat файла. Необходимо:

1. Кратко описать функционал файла;
2. Создать детектирующее правило на языке Yara.

68.**Практическое задание №2**

Создание модели данных события 1 журнала Sysmon для дальнейшей обработки SIEM системой.



По данным из рисунка 1 сформировать модель данных, минимально необходимою для последующей обработки SIEM системой. Модель отобразить в виде следующей таблицы.

Название переменной	Регулярное выражение
cmd	CommandLine:\s*\”(.{0,})\”
…	…

Для описания значений переменных необходимо использовать язык регулярных выражений. Для переменных, имеющих постоянный паттерн, необходимо использовать точные регулярные выражения.

69.**Практическое задание №3**

Обогащение индикатора компрометации

Дан следующий индикатор компрометации:

hxxp://www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com

Необходимо:

1. Определить тип индикатора компрометации (IP адрес, хэш и т.д.);
2. Обогатить индикатор дополнительными данными. Критерий успешного выполнения – однозначная интерпретация индикатора системами безопасности и специалистами ИБ;
3. Обогащённый индикатор представить в виде структурированного массива;

Для обогащения необходимо использовать актуальные данные из открытых источников.

Материалы для проверки остаточных знаний

1.Проактивные технологии защиты.

Ответы:

-

Верный ответ: Проактивные технологии защиты – совокупность технологий и методов, используемых в программном и программно-аппаратном обеспечении,

основной целью которых, в отличие от реактивных (сигнатурных) технологий, является предотвращение реализации угроз ИБ.

2.Метод обнаружения, основанный на сигнатурах (реактивных технологиях).

Ответы:

-

Верный ответ: Обнаружение, основанное на сигнатурах — метод работы антивирусов и систем обнаружения вторжений, при котором программа, просматривая файл или пакет, обращается к базе данных с известными вирусами, составленному авторами СЗИ.

3.Недостатки реактивных методов защиты.

Ответы:

-

Верный ответ: 1. Слабая эффективность против угроз типа 0-day; 2. Необходимость постоянного обновления базы знаний (банка данных об известных угрозах); 3. Для детектирования угрозы необходимо процедура сканирования / реагирования, которая отнимает достаточно много времени и ресурсов.

4.Понятие проактивной защиты.

Ответы:

-

Верный ответ: Проактивные технологии защиты – совокупность технологий и методов, используемых в программном и программно-аппаратном обеспечении, основной целью которых, в отличие от реактивных (сигнатурных) технологий, является предотвращение реализации угроз ИБ.

5.Понятие термина **kill chain** или ***убийственная цепочка.***

Ответы:

-

Верный ответ: Термин kill chain или убийственная цепочка получил широкое распространение после публикации доклада "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains" компанией Lockheed Martin, специализирующаяся в области авиастроения и авиакосмической техники, в котором среди прочего описывается последовательность шагов злоумышленника, осуществляющего незаконное проникновение (взлом) в информационную систему. Разведка. Исследование, идентификация и выбор целевой системы для взлома. Вооружение. Оснащение тулзами и malware для совершения нападения Доставка. Донесение вредоносного контента до целевой системы. Заражение. Запуск вредоносного кода или эксплуатация уязвимости системы. Инсталляция. Открытие удаленного доступа и другие действия с зараженной системой. Получение управления. Управление зараженной системой. Выполнение действий. Сбор, кража, отправка данных, шифрование файлов, подмена и удаление данных.

6.Технологии проактивной защиты.

Ответы:

-

Верный ответ: 1. Эвристический анализ; 2. Эмуляция кода; 3. Поведенческий анализ; 4. Sandboxing (Песочница) — ограничение привилегий выполнения; 5. Виртуализация рабочего окружения; 6. Защита на основе политик; 7. «Белые списки» (Whitelisting); 8. Threat Hunting etc.

7.Технологии проактивной защиты - эвристического анализа.

Ответы:

-

Верный ответ: Технология эвристического анализа заключается в обнаружении путем анализа кода реализуемого приложения, макроса или скрипта участков

вредоносного кода. Это не самая эффективная технология, так как большое количество срабатываний очень чувствительного анализатора ложно, а набор техник, который используется авторами вредоносного ПО достаточно широк.

8.Технологии проактивной защиты - эмуляции кода.

Ответы:

-

Верный ответ: Технология эмуляции кода реализуется путем запуска приложения в среде эмуляции и эмулирует поведение центрального процессора или ОС. Недостаток данной технологии в её большом объеме во времени и ресурсах компьютера пользователя.

9.Технологии проактивной защиты - анализа поведения.

Ответы:

-

Верный ответ: Технология анализа поведения реализуется как перехват набора важнейших системных функций или установка т.н. мини-фильтров. При ней отслеживается вся активность пользователя в системе. Технологией поведенческого анализа оценивается как единичное действие, так и вся цепочка действий.

10.Технология проактивной защиты - Песочница.

Верный ответ: Технология Песочницы реализована на базе принципа ограничения активности потенциально вредоносных приложений с тем, чтобы лишить их возможности нанесения вреда системе пользователя.

11.Технология проактивной защиты - виртуализации рабочего окружения.

Ответы:

-

Верный ответ: Технологию виртуализации рабочего окружения осуществляет системный драйвер, используя перехват всех запросов на запись на жесткий диск с выполнением записи в специальную дисковую область – буфер вместо записи на реальный жесткий диск. Однако, технология виртуализации рабочего окружения не гарантирует защиту от вредоносных программ, цель которых кража конфиденциальных данных, так как не запрещает доступ на чтение к жесткому диску.

12.Компонента безопасности Windows - процедура регистрации (Logon Processes),

Ответы:

-

Верный ответ: Процедура регистрации (Logon Processes), которая обрабатывает запросы пользователей на вход в систему. Она включают в себя начальную интерактивную процедуру, отображающую начальный диалог с пользователем на экране, и удаленные процедуры входа, которые позволяют удаленным пользователям получить доступ с рабочей станции сети к серверным процессам Windows NT. Процесс Winlogon реализован в файле Winlogon.exe и выполняется как процесс пользовательского режима. Стандартная библиотека аутентификации Gina реализована в файле Msgina.dll.

13.Компонента безопасности Windows - Подсистема локальной авторизации (Local Security Authority, *LSA*).

Ответы:

-

Верный ответ: Подсистема локальной авторизации (Local Security Authority, LSA) система которая гарантирует, что пользователь имеет разрешение на доступ в систему. Этот компонент - центральный для системы защиты Windows NT. Он порождает маркеры доступа, управляет локальной политикой безопасности и предоставляет интерактивным пользователям аутентификационные услуги. LSA также контролирует политику аудита и ведет журнал, в котором сохраняются

сообщения, порождаемые диспетчером доступа. Основная часть функциональности реализована в Lsasrv.dll.

14.Компонента безопасности Windows - Менеджер учета (Security *Account Manager*, SAM).

Ответы:

-

Верный ответ: Менеджер учета (Security Account Manager, SAM), который управляет базой данных учета пользователей. Эта база данных содержит информацию обо всех пользователях и группах пользователей. Данная служба реализована в Samsrv.dll и выполняется в процессе Lsass.

15.Компонента безопасности Windows - Диспетчер доступа (Security Reference Monitor, *SRM*).

Ответы:

-

Верный ответ: Диспетчер доступа (Security Reference Monitor, SRM), проверяющий, имеет ли пользователь право на доступ к объекту и на выполнение тех действий, которые он пытается совершить. Этот компонент обеспечивает легализацию доступа и политику аудита, определяемые LSA. Он предоставляет услуги для программ супервизорного и пользовательского режимов, чтобы гарантировать, что пользователи и процессы, осуществляющие попытки доступа к объекту, имеют необходимые права. Данный компонент также порождает сообщения службы аудита, когда это необходимо. Это компонент исполнительной системы: Ntoskrnl.exe.

16.Монитор безопасности (Security Reference Monitor, SRM).

Ответы:

-

Верный ответ: Монитор безопасности (Security Reference Monitor, SRM) проверяет, имеет ли пользователь достаточные права для доступа к объекту. В отличие от других компонентов системы безопасности он работает в режиме ядра. Компоненты ядра и пользовательские процессы обращаются к Монитору безопасности, чтобы выяснить, имеют ли право пользователи и процессы получить доступ к объекту. SRM хранит в себе весь код, ответственный за подтверждение доступа, и это единственная копия данного кода для любой системы Windows. Благодаря этому все проверки выполняются одинаково для всех объектов в системе.

17.Подсистема проверки подлинности локальной системы безопасности (LSASS).

Ответы:

-

Верный ответ: Сервис проверки подлинности локальной системы безопасности (англ. Local Security Authority Subsystem Service, LSASS) — часть операционной системы Windows, отвечающая за авторизацию локальных пользователей отдельного компьютера. Сервис является критическим, так как без него вход в систему для локальных пользователей (не зарегистрированных в домене) невозможен в принципе.

18.Взаимодействие SRM и LSASS.

Ответы:

-

Верный ответ: SRM, выполняемый в режиме ядра, и LSASS, работающий в пользовательском режиме, взаимодействуют по механизму LPC (см. главу 3). При инициализации системы SRM создает порт SeRmCommandPort, к которому подключается LSASS. Процесс Lsass при запуске создает LPC-порт SeLsaCommandPort. К этому порту подключается SRM. В результате формируются закрытые коммуникационные порты. SRM создает раздел общей памяти для

передачи сообщений длиннее 256 байтов и передает его описатель при запросе на соединение. После соединения SRM и LSASS на этапе инициализации системы они больше не прослушивают свои порты. Поэтому никакой пользовательский процесс не сможет подключиться к одному из этих портов.

19.Active Directory и домены Windows.

Ответы:

-

Верный ответ: Active Directory («Активный каталог», AD) — службы каталогов корпорации Microsoft для операционных систем семейства Windows Server. Первоначально создавалась, как LDAP-совместимая реализация службы каталогов, однако, начиная с Windows Server 2008, включает возможности интеграции с другими службами авторизации, выполняя для них интегрирующую и объединяющую роль. Позволяет администраторам использовать групповые политики для обеспечения единообразия настройки пользовательской рабочей среды, разворачивать программное обеспечение на множестве компьютеров через групповые политики или посредством System Center Configuration Manager (ранее — Microsoft Systems Management Server), устанавливать обновления операционной системы, прикладного и серверного программного обеспечения на всех компьютерах в сети, используя Службу обновления Windows Server. Хранит данные и настройки среды в централизованной базе данных.

20.Понятие Winlogon.

Ответы:

-

Верный ответ: Winlogon - это доверенный процесс, отвечающий за управление взаимодействием с пользователем, связанным с безопасностью. Он координирует вход в систему, запускает первый процесс пользователя при входе в систему, обрабатывает выход из системы и управляет различными другими операциями, относящимися к безопасности, включая запуск LogonUI для ввода паролей при входе в систему, изменение паролей и Блокировка и разблокировка рабочей станции Процесс Winlogon должен гарантировать, что операции, относящиеся к безопасности, не видны другим активным процессам. Например, Winlogon гарантирует, что ненадежный процесс не сможет получить контроль над рабочим столом во время одной из этих операций и, таким образом, получить доступ к паролю.

21.Что называется разграничением доступа.

Ответы:

-

Верный ответ: Разграничением доступа субъектов к объектам является совокупность правил, определяющая для каждой тройки субъект—объект—метод, разрешен ли доступ данного субъекта к данному объекту по данному методу. При избирательном разграничении доступа возможность доступа определена однозначно для каждой тройки субъект—объект—метод, при полномочном разграничении доступа ситуация несколько сложнее.

22.Правила разграничения доступа должны удовлетворять следующим требованиям: **…..**

Ответы:

-

Верный ответ: Правила разграничения доступа должны удовлетворять следующим требованиям. 1. Соответствовать аналогичным правилам, принятым в организации, в которой установлена ОС. Иными словами, если согласно правилам организации доступ пользователя к некоторой информации считается несанкционированным, этот доступ должен быть ему запрещен. 2. Не должны допускать разрушающие воздействия субъектов доступа на ОС, выражающиеся в несанкционированном

изменении, удалении или другом воздействии на объекты, жизненно важные для нормальной работы ОС. 3. Любой объект доступа должен иметь владельца. Недопустимо присутствие ничейных объектов — объектов, не имеющих владельца. 4. Не допускать присутствия недоступных объектов — объектов, к которым не может обратиться ни один субъект доступа ни по одному методу доступа. 5. Не допускать утечки конфиденциальной информации.

23.Какие существуют модели разграничения доступа.

Ответы:

-

Верный ответ: Существуют две основные модели разграничения доступа: - избирательное (дискреционное) разграничение доступа; - полномочное (мандатное) разграничение доступа.

24.Как формулируется система правил *дискреционного* разграничения доступа (discretionaryaccesscontrol).

Ответы:

-

Верный ответ: Система правил избирательного или дискреционного разграничения доступа (discretionaryaccesscontrol) формулируется следующим образом: Для любого объекта операционной системы существует владелец. Владелец объекта может произвольно ограничивать доступ других субъектов к данному объекту. Для каждой тройки субъект – объект - метод возможность доступа определена однозначно. Существует хотя бы один привилегированный пользователь (администратор), имеющий возможность обратиться к любому объекту по любому методу доступа. Это не означает, что этот пользователь может игнорировать разграничение доступа к объектам и поэтому является суперпользователем. Не всегда для реализации возможности доступа к объекту операционной системы администратору достаточно просто обратиться к объекту. Например, в Windows NT администратор для обращения к чужому (принадлежащему другому субъекту) объекту должен вначале объявить себя владельцем этого объекта, использовав привилегию администратора объявлять себя владельцем любого объекта, затем дать себе необходимые права, и только после этого администратор может обратиться к объекту. При этом использование администратором своей привилегии не остается незамеченным для прежнего владельца объекта.

25.Мандатное разграничение доступа.

Ответы:

-

Верный ответ: Мандатное (полномочное) разграничение доступа заключается в том, что все объекты могут иметь уровни секретности, а все субъекты делятся на группы, образующие иерархию в соответствии с уровнем допуска к информации.

26.Каковы правила разграничения доступа в мандатной модели доступа.

Ответы:

-

Верный ответ: Правила разграничения доступа в мандатной модели формулируются следующим образом. 1. Для любого объекта ОС существует владелец. 2. Владелец объекта может произвольно ограничивать доступ других субъектов к данному объекту. 3. Для каждой четверки субъект—объект—метод—процесс возможность доступа определена однозначно в каждый момент времени. При изменении состояния процесса со временем возможность предоставления доступа также может измениться. Вместе с тем, в каждый момент времени возможность доступа определена однозначно. Поскольку права процесса на доступ к объекту меняются с течением времени, они должны проверяться не только при открытии объекта, но и перед выполнением над объектом таких операций, как чтение и запись. 4.

Существует хотя бы один привилегированный пользователь (администратор), имеющий возможность удалить любой объект. 5. В множестве объектов выделяется множество объектов полномочного разграничения доступа. Каждый объект полномочного разграничения доступа имеет гриф секретности. Чем выше числовое значение грифа секретности, тем секретнее объект. Нулевое значение грифа секретности означает, что объект несекретен. Если объект не является объектом полномочного разграничения доступа или если объект несекретен, администратор может обратиться к нему по любому методу, как и в предыдущей модели разграничения доступа. 6. Каждый субъект доступа имеет уровень допуска. Чем выше числовое значение уровня допуска, тем больший допуск имеет субъект. Нулевое значение уровня допуска означает, что субъект не имеет допуска. Обычно ненулевое значение допуска назначается только субъектам-пользователям и не назначается субъектам, от имени которых выполняются системные процессы. 7. Доступ субъекта к объекту должен быть запрещен независимо от состояния матрицы доступа, если: • объект является объектом полномочного разграничения доступа; • гриф секретности объекта строго выше уровня допуска субъекта, обращающегося к нему; • субъект открывает объект в режиме, допускающем чтение информации. Это правило называют правилом NRU (Not Read Up — не читать выше). 8. Каждый процесс ОС имеет уровень конфиденциальности, равный максимуму из грифов секретности объектов, открытых процессом на протяжении своего существования. Уровень конфиденциальности фактически представляет собой гриф секретности информации, хранящейся в оперативной памяти процесса. 9. Доступ субъекта к объекту должен быть запрещен независимо от состояния матрицы доступа, если: • объект является объектом полномочного разграничения доступа; • гриф секретности объекта строго ниже уровня конфиденциальности процесса, обращающегося к нему; • субъект собирается записывать в объект информацию, Это правило предотвращает утечку секретной информации; его называют правило NWD (Not Write Down — не записывать ниже). 10. Понизить гриф секретности объекта полномочного разграничения доступа может только субъект, который: • имеет доступ к объекту согласно правилу 7; • обладает специальной привилегией, позволяющей ему понижать грифы секретности объектов. При использовании данной модели разграничения доступа существенно страдает производительность ОС, поскольку права доступа к объекту должны проверяться не только при открытии объекта, но и при каждой операции чтение/запись. Кроме того, эта модель создает пользователям определенные неудобства: если уровень конфиденциальности процесса строго выше нуля, то вся информация в памяти процесса фактически является секретной и не может быть записана в несекретный объект. Если процесс одновременно работает с двумя объектами, только один из которых является секретным, то он не может записывать информацию из памяти во второй объект. Эта проблема решается посредством использования специального программного интерфейса API для работы с памятью. Области памяти, выделяемые процессам, могут быть описаны как объекты полномочного разграничения доступа, после чего им могут назначаться грифы секретности. При чтении секретного файла процесс должен считать содержимое такого файла в секретную область памяти, используя для этого функции ОС, гарантирующие невозможность утечки информации. Для работы с секретной областью памяти процесс также должен использовать специальные функции. Поскольку утечка информации из секретных областей памяти в память процесса невозможна, считывание процессом секретной информации в секретные области памяти не отражается на уровне конфиденциальности процесса. Если же процесс считывает секретную информацию в область памяти, не описанную как объект полномочного разграничения доступа, повышается уровень конфиденциальности процесса.

27.Подсистемы безопасности ОС Linux.

Ответы:

-

Верный ответ: POSIX ACL - Разграничение прав доступа к файлам на основе их атрибутов (Discretionary Access Control, DAC). Sudo - Выполнение программ от своего и/или чужого имени. Chroot - Операция, ограничивающая доступ процесса к файловой системе, изменяя ее корень в контексте процесса. PAM - Подключаемые модули аутентификации. SELinux - Реализация системы принудительного контроля доступа (Mandatory Access Control, MAC), основанная на политиках и контекстах безопасности. AppArmor - Система упреждающей защиты, основанная на политиках безопасности (профилях). PolicyKit - Средство контроля системных привилегий.

28.Подсистемы безопасности ОС Windows.

Ответы:

-

Верный ответ: Ядром подсистемы безопасности является локальная служба безопасности (Local Security Authority, LSA), размещающаяся в файле lsass.exe. Стандартный провайдер аутентификации размещается в файле msgina.dll и в качестве аутентифицирующей информации использует пароли пользователей.

29.Виртуализация что это ….

Ответы:

-

Верный ответ: Виртуализация — предоставление набора вычислительных ресурсов или их логического объединения, абстрагированное от аппаратной реализации, и обеспечивающее при этом логическую изоляцию друг от друга вычислительных процессов, выполняемых на одном физическом ресурсе.

30.Преимущества виртуализации.

Ответы:

-

Верный ответ: Эффективное использование вычислительных ресурсов. Сокращение расходов на инфраструктуру. Снижение затрат на программное обеспечение. Повышение гибкости и скорости реагирования системы. Несовместимые приложения могут работать на одном компьютере. Повышение доступности приложений и обеспечение непрерывности работы предприятия. Возможности легкой архивации. Повышение управляемости инфраструктуры. Безопасность.

31.Виртуализация приложений.

Ответы:

-

Верный ответ: Виртуализация приложений - это тип виртуализации, при котором происходит изоляция приложения от ресурсов операционной системы. Основной принцип виртуализации приложений заключается в том, что само приложение физически выполняется на локальной машине, но при этом оно не имеет доступ ни к драйверам, ни к реестру, ни к файловой системе, все эти ресурсы эмулируются.

32.Виртуализация представлений (рабочих мест).

Ответы:

-

Верный ответ: Виртуализация представлений подразумевает эмуляцию интерфейса пользователя, т.е. пользователь видит приложение и работает с ним на своём терминале, хотя на самом деле приложение выполняется на удалённом сервере, а пользователю передаётся лишь картинка удалённого приложения.

33.Понятие песочница.

Ответы:

-

Верный ответ: Песочница – механизм для безопасного исполнения программ. Песочницы часто используют для запуска непроверенного кода из неизвестных источников и обнаружения вирусов и закладок.

34.Антивирусные песочницы. Модели изоляции.

Ответы:

-

Верный ответ: Изоляция на основе полной виртуализации. Использование любой виртуальной машины в качестве защитного слоя над гостевой операционной системой, где установлен браузер и иные потенциально опасные программы, через которые пользователь может заразиться, даёт достаточно высокий уровень защиты основной рабочей системы. Изоляция на основе частичной виртуализации файловой системы и реестра. Совсем необязательно таскать с собой движок виртуальной машины, можно подпихивать процессам в песочнице дубликаты объектов файловой системы и реестра, помещая в песочницу приложения на рабочей машине пользователя. Попытка модификации данных объектов приведёт к изменению лишь их копий внутри песочницы, реальные данные не пострадают. Контроль прав не даёт возможности атаковать основную систему изнутри песочницы через интерфейсы операционной системы. Изоляция на основе правил. Все попытки изменения объектов файловой системы и реестра не виртуализируются, но рассматриваются с точки зрения набора внутренних правил средства защиты. Чем полнее и точнее такой набор, тем большую защиту от заражения основной системы предоставляет программа. То есть, этот подход представляет собой некий компромисс между удобством обмена данными между процессами внутри песочницы и реальной системой и уровнем защиты от зловредных модификаций. Контроль прав не даёт возможности атаковать основную систему изнутри песочницы через интерфейсы операционной системы.

35.Назначение системы для автоматического исследования вредоносного ПО **Cuckoo Sandbox.**

Ответы:

-

Верный ответ: Cuckoo Sandbox — система для автоматического исследования вредоносного ПО, эксплоитов, вредоносных скриптов, документов, архивов и ссылок. Система способна проверять документы pdf, doc, xls, rtf, скрипты Python, JS, DLL библиотеки, бинарники, jar и многое другое.

36. Функционал системы Cuckoo Sandbox.

Ответы:

-

Верный ответ: Мониторинг вызовов win32 API функций; Дамп сетевой активности; Дамп и анализ памяти; Создание скриншотов в ходе выполнения анализа; Сохранение копий всех созданных файлов и загруженных в процессе проверки; Трассировка инструкций, выполняемых вредоносным процессом; Создание удобного отчета в json, mmdef, maec, html-форматах; Абсолютная изолированность среды, в которой производится запуск вредоносных программ.

37.Сигнатурный метод обнаружения это ….

Ответы:

-

Верный ответ: Сигнатурные методы обнаружения - точные методы обнаружения, основанные на сравнении файла/сетевого пакета с известными образцами.

38.Эвристические методы обнаружения это ….

Ответы:

-

Верный ответ: Эвристические методы - нечеткие методы обнаружения, которые позволяют с определенной вероятностью предположить, что файл / сетевой пакет является вредоносным.

39.YARA правила это ….

Ответы:

-

Верный ответ: YARA правила - это способ выявления вредоносных программ (или других файлов) путем создания правил, которые описывают определенные характеристики объекта.

40.Мониторингом информационной безопасности или мониторингом событий безопасности, называется ….

Ответы:

-

Верный ответ: Мониторингом информационной безопасности или мониторингом событий безопасности, называется сбор и анализ информации для выявления подозрительного поведения или несанкционированных изменений систем в сети и определения типов поведения, в отношении которых требуется выпуск уведомлений и выполнение соответствующих действий.

41.Источники мониторинга информационной безопасности.

Ответы:

-

Верный ответ: Мониторинг событий производится на основе данных, полученных из различных источников, к которым относятся: • IDS/IPS-системы; • средства антивирусной защиты; • журналы событий; • сканеры уязвимостей; • DLP-системы; • сетевое оборудование; • прочие источники.

42.Системы мониторинга производительности и доступности это …

Ответы:

-

Верный ответ: Системы мониторинга производительности могут использоваться как отдельно, так и являться одним из источников событий для системы управления событиями (SIEM). Такие системы предназначены для отслеживания состояния функционирования разнообразных сервисов сети и ее узлов (серверов, сетевого оборудования, приложений и других), в том числе подсистем ИБ, на основе различных критериев производительности и доступности.

43.Функции систем мониторинга производительности и доступности.

Ответы:

-

Верный ответ: 1. Сбор и агрегация разнообразных данных; 2. Анализ и корреляция собранных данных для определения или упреждения достижения пороговых значений показателей производительности и доступности; 3. Автоматизированное выполнение заранее запрограммированных тестов; 4. Автоматизированное реагирование системы; 5. Генерации оповещений (уведомлений) о выявленных отклонениях в производительности и доступности систем; 6. Визуализация собираемых данных в виде диаграмм; 7. Хранение собранных данных в базе данных.

44.Системы управления событиями и инцидентами информационной безопасности (SIEM) это …

Ответы:

-

Верный ответ: Система мониторинга событий информационной безопасности предназначена для автоматизации процесса сбора и анализа информации о событиях безопасности, поступающих из различных источников. В качестве таких источников

могут выступать средства защиты информации, общесистемное и прикладное ПО, телекоммуникационное обеспечение и др.

45.Основные задачи SIEM-систем.

Ответы:

-

Верный ответ: 1. Оперативное обнаружение атак и нарушений политики ИБ; 2. Соотнесение в режиме реального времени событий от разных устройств, выявление инцидентов ИБ и их приоритезация; 3. Автоматическое реагирование на инциденты; 4. Формирование базы знаний по инцидентам; 5. Проведение аудитов и расследований инцидентов; 6. Оценка уровня угроз для отдельных корпоративных ресурсов.

46.Механизмы SIEM систем.

Ответы:

-

Верный ответ: Нормализация заключается в приведении собранных из различных источников аудита данных о событиях к единому виду и формату, "понятному" системе и необходимому для дальнейшего анализа и хранения. Фильтрация событий используется для отсеивания избыточных и ненужных для дальнейшего анализа событий. Классификация устанавливает атрибуты события в соответствии с его происхождением, типом и т.п. Механизм агрегации объединяет несколько схожих событий в одно по определенным параметрам или признакам. Корреляция событий позволяет выявлять взаимосвязь между разнородными событиями от различных устройств, приложений и систем безопасности, что позволяет не только обнаруживать атаки на корпоративную информационную систему, но и выявлять нарушения требований и политик безопасности. Приоритезация - это процесс автоматического выставления значимости и критичности произошедшего события или группы событий на основании как предустановленных в системе правил, так и на основании критериев, разработанных администраторами системы. В простейшем случае порядок обработки событий осуществляется именно в порядке перечисления данных механизмов.

47.Типовая структура SIEM-систем.

Ответы:

-

Верный ответ: 1. Агенты – устанавливаются на информационную систему и передают данные с нее на сервер, в состав агентов могут включаться модули для преобразования данных; 2. Сервер-коллектор – собирает события от множества источников; 3. Сервер-коррелятор – собирает и обрабатывает информацию от коллекторов и агентов; 4. Сервер баз данных – хранит журналы событий.

48.Технология Threat Intelligence это …

Ответы:

-

Верный ответ: Threat Intelligence (TI, киберразведка) – знание (включая процесс его получения) об угрозах и нарушителях, обеспечивающее понимание методов, используемых злоумышленниками для нанесения ущерба, и способов противодействия им. TI оперирует не только и не столько статической информацией об отдельных уязвимостях и угрозах, сколько более динамичной и имеющей практическое значение информацией об источниках угроз, признаках компрометации (объединяющих разрозненные сведения в единое целое), вредоносных доменах и IP-адресах, взаимосвязях и т.п.

49.Задачи технологии Threat Intelligence.

Ответы:

-

Верный ответ: 1. Разведка и сбор данных об уязвимостях и угрозах. TI должна быть интегрирована в систему защиты и должна предоставлять возможность централизованного сбора информации из открытых и закрытых источников об уязвимостях и угрозах. 2. Аналитика. TI должна анализировать и накапливать базу знаний по обнаружению, раскрытию, разработке и выдаче рекомендаций по реагированию на угрозы.

50.Задачи технологии Threat Intelligence.

Ответы:

-

Верный ответ: 1. Обмен данными. TI также должна предоставлять возможность обмена полученными данными в режиме реального времени. Аналитическая информация должна мгновенно распространяться в стандартизированном формате как внутренним, так и внешним средствам защиты. 2. Оперативное оповещение. TI должна оперативно оповещать об атаках и угрозах в любой конечной точке, используя единую стандартизированную базу с классифицированными данными.

51.Этапы применения технологии Threat Intelligence.

Ответы:

-

Верный ответ: 1. Этап планирования - где устанавливаются цели, требования к получаемой информации и расставляются приоритеты. 2. Этап сбора включает в себя различные этапы деятельности по сбору информации для удовлетворения поставленных на первом этапе целей. Кроме собственных источников информации, на этом этапе используются и данные провайдеров. 3. Этап обработки собранных исходных данных, где они интерпретируются, транслируются и унифицируются. 4. Этап подготовки данных, который включает в себя процесс уточнения и слияния информации, обработанной на предыдущем этапе. 5. Заключительный этап - этап распространения информации конечным потребителям, в роли которых могут выступать как внешние потребители, так и собственные подразделения ИБ в филиалах, дочерних и зависимых бизнес-единицах компании.

52.Какие бывают фиды?

Ответы:

-

Верный ответ: 1. IP и DNS-адреса вредоносных сайтов, спамеров, входных узлов Tor, анонимайзеров, открытых прокси… ; 2. Заголовки E-mail; 3. URL и URI; 4. Хеши и пути файлов; 5. CVE-записи; 6. Правила CIDR; 7. Репутация файлов, узлов, сайтов; 8. Ключи реестра; 9. Индикаторы компрометации (IoC); 10. Whois данные; 11. GeoIP – географическая информация об IP-адресе; 12. Статистическая и поведенческая информация – техники, тактики и процедуры проведения атак.

53.Какие инструменты используются для классификации данных из фидов.

Ответы:

-

Верный ответ: Для классификации данных из фидов используются следующие инструменты: 1. Теги; 2. Таксономии – набор библиотек, классифицированных по процессам проведения атаки, распространения угроз, обмена данными и др. Например, ENISA, CSSA, VERIS, Diamond Model, Kill Chain, CIRCL, MISP имеют свои таксономии; 3. Кластеризация – набор библиотек, классифицированных по статическим признакам угроз и атак. Например, секторы экономики; используемые инструменты и эксплоиты; TTP (Tacticks, Techniques & Procedures), этапы и методы проникновения, эксплуатации и закрепления в системе, основанные на ATT&CK Matrix.

54.Технологии репутации.

Ответы:

-

Верный ответ: 1. Whitelisting – белые списки программного обеспечения; 2. Web reputation – репутация веб-сайтов; 3. Email reputation – репутация отправителя электронной почты; 4. File reputation – репутация файла.

55.Технология репутации Whitelisting.

Ответы:

-

Верный ответ: Whitelisting - избирательный запуск программ, на основе составления «белого списка» безопасных и желательных приложений. Все остальные приложения блокируются. "Белые списки" программ (Application Whitelisting, AWL) являются эффективным методом предотвращения вирусного заражения, в первую очередь вирусов-шифровальщиков.

56.Технология репутации Web Reputation.

Ответы:

-

Верный ответ: Технология репутации Web Reputation это технология, которая: 1. Отслеживает надежность веб-сайтов и веб-страниц, используя сведения о репутации доменов, содержащиеся в одной из крупнейших в мире баз данных. 2. Оценивает репутацию веб-доменов и отдельных страниц, а также ссылок на веб-сайтах (поскольку законные сайты периодически частично взламываются). 3. Блокирует доступ пользователей к сомнительным или зараженным сайтам.

57.Технология репутации Email Reputation.

Ответы:

-

Верный ответ: Технология репутации Email Reputation это технология, которая: 1. Проверяет IP-адреса по базе данных, содержащей сведения об их репутации. 2. Оценивает репутацию отправителей почтовых сообщений в режиме реального времени. 3. Постоянно анализирует IP-адреса, переоценивая репутацию. 4. Блокирует вредоносные почтовые сообщения и угрозы (например, «зомби») в «облачной» среде до их проникновения в систему.

58.Технология репутации File Reputation.

Верный ответ: Технология File Reputation это технология, которая: 1. Проверяет репутацию всех файлов по «облачной» базе данных, прежде чем предоставить пользователям доступ к ним. 2. Минимизирует время задержки при проверке благодаря использованию высокопроизводительных сетей для доставки содержимого и локальных серверов кэширования. 3. Использует архитектуру «облако — клиент», чтобы уменьшить размер файла локальной антивирусной базы данных и таким образом свести к минимуму угрозу увеличения объемов (большое количество создаваемых за день угроз).

59.Преимущества репутационных технологий.

Ответы:

-

Верный ответ: 1. Скорость реакции. 2. Скрытая логика принятия решений. 3. Выявление не только новых недетектируемых угроз, но и источников их распространения. 4. Полнота выявляемых угроз. 5. Минимизация ложных срабатываний. Как показывает практика, уровень ложных срабатываний при детектировании с помощью репутации, как минимум в 100 раз ниже обычного сигнатурного детектирования 6. Простота автоматизации процессов детектирования

60.Недостатки репутационных технологий.

Ответы:

-

Верный ответ: 1. Сложность реализации и поддержания технологии; 2. Необходимость постоянно пересматривать репутационные списки; 3. Зависимость технологии от внешних источников (для пополнения базы).

61.Технологии построения защищенных компьютерных сетей.

Ответы:

-

Верный ответ: 1. Межсетевой экран (Firewall vs Next Generation FireWall); 2. Демилитаризованная зона (demilitarized zone или DMZ); 3. Список контроля доступа (Access Control List или ACL).

62.Межсетевой экран, сетевой экран.

Ответы:

-

Верный ответ: Межсетевой экран, сетевой экран — программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами.

63.Функции межсетевого экрана.

Ответы:

-

Верный ответ: Каждый из фильтров предназначен для интерпретации отдельных правил фильтрации путем выполнения следующих действий: 1. Анализ информации по заданным в интерпретируемых правилах критериям, например по адресам получателя и отправителя или по типу приложения, для которого эта информация предназначена. 2. Принятие на основе интерпретируемых правил одного из следующих решений: - не пропустить данные; - обработать данные от имени получателя и возвратить результат отправителю; - передать данные на следующий фильтр для продолжения анализа; - пропустить данные, игнорируя следующие фильтры. 3. Правила фильтрации могут задавать и дополнительные действия, которые относятся к функциям посредничества, например преобразование данных, регистрацию событий и др. Соответственно, правила фильтрации определяют перечень - - условий, по которым осуществляется: - разрешение или запрещение дальнейшей передачи данных; - выполнение дополнительных защитных функций. 4. В качестве критериев анализа информационного потока могут использоваться следующие параметры: - служебные поля пакетов сообщений, содержащие сетевые адреса, идентификаторы, адреса интерфейсов, номера портов и другие значимые данные; - непосредственное содержимое пакетов сообщений, проверяемое, например, на наличие компьютерных вирусов; - внешние характеристики потока информации, например временные, частотные характеристики, объем данных и т. д.

64.Межсетевые экраны нового поколения (NGFW) – это …

Ответы:

-

Верный ответ: Межсетевые экраны нового поколения (NGFW) – это устройства, в которых проводится глубокая проверка пакетов (выходящая за рамки порт/протокол), с возможностью инспектировать и блокировать трафик уровня приложения, включающие в себя встроенные системы предотвращения вторжений и интеллектуальную обработку трафика на основе интеграции с внешними системами.

65. Демилитаризованная зона (demilitarized zone или DMZ).

Ответы:

-

Верный ответ: DMZ (ДМЗ) - сокращение от demilitarized zone (демилитаризованная зона) – область в сети, системы в которой отделены от основной сети; смысл создания такого сегмента заключается в том, чтобы отделить системы, к которым осуществляют доступ пользователи интернета, от систем, с которыми работают

только сотрудники организации. Цель ДМЗ — добавить дополнительный уровень безопасности в локальной сети, позволяющий минимизировать ущерб в случае атаки на один из общедоступных сервисов: внешний злоумышленник имеет прямой доступ только к оборудованию в ДМЗ.

66.Список контроля доступа (Access Control List или ACL).

Ответы:

-

Верный ответ: Access Control List или ACL — список контроля доступа, который определяет, кто или что может получать доступ к конкретному объекту, и какие именно операции разрешено или запрещено этому субъекту проводить над объектом. ACL — это набор текстовых выражений, которые что-то разрешают, либо что-то запрещают. Обычно ACL разрешает или запрещает IP-пакеты, но помимо всего прочего он может заглядывать внутрь IP-пакета, просматривать тип пакета, TCP и UDP порты. Также ACL существует для различных сетевых протоколов (IP, IPX, AppleTalk и так далее). В основном применение списков доступа рассматривают с точки зрения пакетной фильтрации, то есть пакетная фильтрация необходима в тех ситуациях, когда у вас стоит оборудование на границе Интернет и вашей частной сети и нужно отфильтровать ненужный трафик. Вы размещаете ACL на входящем направлении и блокируете избыточные виды трафика.

67.Технология Threat Hunting.

Ответы:

-

Верный ответ: Threat Hunting — процесс проактивного и итеративного поиска и обнаружения advanced угроз, которые невозможно обнаружить традиционными средствами защиты. К продвинутым угрозам относятся, например, такие атаки, как APT, атаки на 0-day уязвимости и т.д. TH – это процесс проверки гипотез. Это преимущественно ручной процесс с элементами автоматизации, в рамках которого аналитик, опираясь на свои знания и квалификацию, просеивают большие объемы информации в поисках признаков компрометации, соответствующих первоначально определенной гипотезе о присутствии определённой угрозы.

68.Составляющие технологии Threat Hunting.

Ответы:

-

Верный ответ: 1. Данные (что?), в том числе и Big Data. Всевозможные потоки трафика, информация о ранее проведенных APT, аналитика, данные о пользовательской активности, сетевые данные, информация от сотрудников, информация в даркнете и многое другое. 2. Технологии (как?) обработки этих данных – все возможные способы обработки этих данных, включая Machine Learning. 3. Люди (кто?) – те, кто обладает большим опытом анализа разнообразных атак, развитой интуицией и способностью обнаружить атаку. Обычно это аналитики информационной безопасности, которые должны иметь способность генерировать гипотезы и находить им подтверждение. Они — основное звено процесса.

69.Источники информации Threat Hunting.

Ответы:

-

Верный ответ: Типовыми источниками практически в любой инфраструктуре будут данные от средств защиты: DLP, SIEM, IDS/IPS, WAF/FW, EDR. Также типовыми источниками информации будут являться всевозможные индикаторы компрометации, сервисы Threat Intelligence, данные CERT и OSINT. Дополнительно можно использовать информацию из даркнета (например, внезапно есть заказ на взлом почтового ящика руководителя организации, или своей активностью засветился кандидат на должность сетевого инженера), информацию, полученную от

HR (отзывы о кандидате с прошлого места работы), информацию от службы безопасности (например, результаты проверки контрагента).

70.Процесс проверки гипотез с использованием технологии Threat Hunting.

Ответы:

-

Верный ответ: Этап 1: TI Farm. На этом этапе необходимо выделить объекты (путем их анализа совместно со всеми данными об угрозах) с присвоением им меток их характеристик. Это файл, URL, MD5, процесс, утилита, событие. Проводя их через системы Threat Intelligence, необходимо навесить метки. То есть этот сайт был замечен в CNC в таком-то году, эта MD5 была связана с такой-то малварой, эта MD5 качалась с сайта, который раздавал малвары. Этап 2: Cases. На втором этапе смотрим на взаимодействие между этими объектами и выявляем взаимосвязи между всеми этими объектами. Получаем промаркированные системы, которые делают что-то нехорошее. Этап 3: Аналитик. На третьем этапе дело передается опытному аналитику, имеющему огромный опыт анализа, он и выносит вердикт. Он разбирает до байтов, что, откуда, как, зачем и почему делает этот код. Это тело было зловредом, этот компьютер был заражен. Раскрывает связи между объектами, проверяет результаты прогона через песочницу.Результаты работы аналитика передаются далее. Digital Forensics исследует образы, Malware Analysis исследует найденные «тела», а команда Incident Response может выехать на место и исследовать что-то уже там. Итогом работы будет подтвержденная гипотеза, выявленная атака и пути противодействия ей.

71.Техники Threat Hunting. Базовый поиск.

Ответы:

-

Верный ответ: Базовый поиск – это наиболее часто используемая техника в Threat Hunting. Этот метод подразумевает использование специализированных запросов, которые возвращают некоторые результаты поиска. Из-за сложности формализации задачи по поиску неизвестной угрозы не всегда возможно однозначно указать, что ищет аналитик, когда начинает поиск. По этой причине область поиска не должна быть ни слишком широкой, охватывающей множество факторов и выдающей обилие результатов, ни слишком узкой, так как появляется высокая вероятность упустить потенциальные угрозы, которые не были включены в поиск.

72.Машинное обучение в технологии Threat Hunting.

Ответы:

-

Верный ответ: Алгоритмы машинного обучения (Data Mining), в качестве еще одной техники Threat Hunting, успешно применимы при фильтрации спама, обнаружении вредоносного трафика и детектировании мошеннических действий. Успешно внедренные в процесс ханкинга алгоритмы способны существенно повысить эффективность защиты информации. Указанные алгоритмы можно внедрять в средства защиты информации, которые требуют серьезной ресурсной и организационной подготовки, как в IT, так и в ИБ-секторе.

73.Организационные меры проактивной защиты.

Ответы:

-

Верный ответ: 1. Оценка эффективности защиты периметра сети. 2. Повышение осведомлённости сотрудников в области ИБ. 3. Политика обновления системного и прикладного ПО. 4. Политика резервного копирования. 5. Управление уязвимостями

74.Организационная мера проактивной защиты - оценка эффективности защиты периметра сети.

Ответы:

-

Верный ответ: Аудит и анализ защищенности — это комплексные решения, которые помогают организациям определять уязвимости находят слабые места в сети, проводят проверки соответствия стандартам и тестирования на проникновения. Анализ защищённости сети включает в себя: - Обнаружение ресурсов сетевого периметра, уязвимых для атак через интернет; - Оценка уровня критичности уязвимостей и их воздействия на бизнес; - Осуществление сканирования веб-приложений; - Возможность проверки на использование найденных уязвимостей; - Проверка соответствия защиты периметра требованиям безопасности; - Осуществление мониторинга процесса устранения уязвимостей; - Определение закрытой информации в системах или документах; - Анализ тенденций в области проблем безопасности.

75.Организационная мера проактивной защиты - повышение осведомленности сотрудников в области ИБ.

Ответы:

-

Верный ответ: Минимальной и необходимой мерой является повышение осведомленности сотрудников в области ИБ в области знания принципов работы с файлами и почтой: - не открывать файлы с двойным расширением: настроить для пользователей отображение расширений, чтобы идентифицировать вредоносные файлы с двойными расширениями (например, 1CRecord.xlsx.scr); - не включать макросы в недоверенных документах Microsoft Office; - проверять адреса отправителей почтовых сообщений; - не открывать ссылки на веб-страницы, почтовые вложения от неизвестных отправителей.

76.Политика обновления системного и прикладного ПО.

Ответы:

-

Верный ответ: Patch Management – это процесс управления обновлениями программного обеспечения (ПО), без которого вряд ли обходится хоть одна современная компания, думающая о безопасности своей ИТ-инфраструктуры.Обновления или патчи — это дополнительное программное средство, которое применяется для исправления обнаруженных дефектов в программном обеспечении или изменения его функционала. Существуют 2 типа обновлений: 1. для операционных систем и серверного ПО, которые применяются для поддержки надлежащего уровня безопасности и устранения дыр в защите; 2. для прикладного ПО (например, Microsoft Office, Adobe Acrobat или клиентские части бизнес-приложений), которые необходимы для решения возникших проблем с часто используемыми или важными библиотеками и другими частями исходного кода.

77.Политика резервного копирования.

Ответы:

-

Верный ответ: Политика резервного копирования определяет, каким образом осуществляется резервное копирование данных. Зачастую эти требования включаются в политику безопасности организации. Задачи резервного копирования: 1. Выделение целевых данных. 2. Сохранение указанных данных для последующего восстановления. 3. Восстановление сохранённых данных. 4. Обеспечение устойчивости хранимых данных к изменению и уничтожению. 5. Разграничение доступа к хранимым данным. 6. Обеспечение контроля системы и процесса резервного копирования.

78.Управление уязвимостями.

Ответы:

-

Верный ответ: Уязвимость – это характеристика, которая может быть использована нарушителем при проведении атаки на ИТактив и привести к реализации угрозы. Процесс управления уязвимостями – циклические действия, направленные обнаружение и классификацию уязвимостей, а также на их устранение или снижение последствий их эксплуатации.

79.Создание программы осведомлённости.

Ответы:

-

Верный ответ: Планирование: – Определите ответственных за создание и реализацию программы; – Определите цели и задачи программы; – Определите роли (категории вашей целевой аудитории). Разным ролям потребуется разное обучение в разном объеме, например, все сотрудники, IT-персонал, менеджмент, внешние исполнители и т.п.; – Для каждой категории целевой аудитории определите актуальный набор мероприятий (курсы, тренинги, рассылки …); – Определите способы взаимодействия с аудиторией (семинары, тренинги, мультимедиа курсы, рассылки, бюллетени безопасности, постеры и т.п.); – Определите метрики для анализа эффективности программы – Разработайте план реализации программы и план мероприятий по проверке/тестированию знаний. Внедрение: – Разработайте/приобретите материалы для реализации программы; – Выберите необходимые инструменты для реализации; – Проводите мероприятия в соответствии с программой; – Проводите мероприятия по тестированию осведомленности. Анализ: – Анализируйте результаты и показатели эффективности; – Доводите результаты и получайте обратную связь менеджмента компании; – Получайте обратную связь от аудитории, вовлеченной в обучение (полезность, качество материалов, рекомендуемые изменения и т.п.). Совершенствование: – Развивайте свою систему в соответствии с полученными показателями эффективности, результатами тестирования (проверки знаний) и по результатам обратной связи; – Анализируйте ландшафт угроз и дополняйте свою программу обучения новыми материалами; – Анализируйте новые требования и вносите изменения в программу обучения; – Развивайте свою программу с учетом долгосрочных бизнес-целями компании.

II. Описание шкалы оценивания

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Работа выполнена в рамках "продвинутого" уровня. Ответы даны верно, четко сформулированные особенности практических решений

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Работа выполнена в рамках "базового" уровня. Большинство ответов даны верно. В части материала есть незначительные недостатки

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Работа выполнена в рамках "порогового" уровня. Основная часть задания выполнена верно. на вопросы углубленного уровня

III. Правила выставления итоговой оценки по курсу