CCNA Cybersecurity Operations v1.1. Общий объем и последовательность изучения

Последнее обновление 14 марта 2019 г.

Введение

Перед современными организациями стоит сложная задача быстрого обнаружения нарушений кибербезопасности и эффективного реагирования на события безопасности. Группы людей в центрах мониторинга и управления безопасностью (SOC) управляют системами безопасности и защищают свою организацию, своевременно обнаруживая и нейтрализуя угрозы кибербезопасности. Курс CCNA Cybersecurity Operations подготавливает слушателей к началу работы в качестве аналитиков по кибербезопасности младшего уровня в центрах мониторинга и управления безопасностью (SOC).

Целевая аудитория

Курс Cisco CCNA® Cybersecurity Operations v1.1 (CyberOps) предназначен для студентов Сетевой академии Cisco®, ориентированных на получение первоначальных навыков для работы в качестве аналитиков по безопасности. Курс ориентирован в первую очередь на студентов технологических факультетов высших учебных заведений и ИТ-специалистов, желающих получить работу в центре мониторинга и управления безопасностью (SOC).

Предварительная подготовка

Студенты курса CCNA Cybersecurity Operations должны обладать следующими знаниями и навыками:

- навыки работы с ПК и использования Интернета;
- базовые знания систем Windows и Linux;
- основные принципы организации сетей;
- понимание двоичной и шестнадцатеричной систем счисления;
- знание основных принципов программирования;
- знакомство с базовыми запросами SQL.

Целевые сертификации

Этот курс соответствует требованиям сертификации CCNA Cyber Ops. Для получения сертификации CCNA Cyber Ops слушателям необходимо сдать экзамены 210–250 SECFND и 210–255 SECOPS.

Описание учебного плана

В курсе имеется много функций, помогающих студентам понять следующие концепции.

- Насыщенное мультимедийное содержание, включая интерактивные задания, видео, игры и контрольные работы, обеспечивает разные стили обучения, стимулирует интерес к учебе и улучшает запоминание материала

- Виртуальные среды позволяют моделировать реальные ситуации с развитием угроз кибербезопасности и предоставляют «белым» хакерам возможности для мониторинга безопасности, анализа и устранения угроз.
- Практические лабораторные занятия помогают студентам развивать критическое мышление и навыки решения сложных задач.
- Новаторская система аттестаций обеспечивает немедленную обратную связь для оценки знаний и приобретенных навыков.
- Технические принципы объясняются языком, который доступен студентам всех уровней, а встроенные интерактивные задания облегчают понимание содержимого и способствуют укреплению знакомства с материалом
- Учебный план побуждает студентов задуматься о дополнительном образовании в сфере ИТ, но в нем также придается особое значение применению навыков и практическому опыту
- Задания Cisco Packet Tracer разработаны для выполнения в программе Packet Tracer версии не ниже 7.0.

Цели учебного плана

Курс CCNA Cybersecurity Operations v1.1 охватывает знания и навыки, необходимые для успешного выполнения задач и обязанностей аналитика по безопасности младшего уровня в Центре мониторинга и управления безопасностью (SOC).

После прохождения курса *CCNA Cybersecurity Operations v1.1* студенты смогут выполнять следующие задачи:

- установить виртуальную машину, чтобы создать безопасную среду для проведения и анализа мероприятий кибербезопасности;
- рассказать, какую роль выполняет на предприятии аналитик по кибербезопасности;
- рассказать о функциях и характеристиках операционной системы Windows, служащих для поддержки анализа кибербезопасности;
- рассказать о функциях и характеристиках операционной системы Linux;
- анализировать работу сетевых протоколов и служб;
- объяснить принципы работы сетевой инфраструктуры;
- классифицировать различные типы сетевых атак;
- использовать средства сетевого мониторинга для определения атак на сетевые протоколы и службы;
- применять различные способы предотвращения несанкционированного доступа к компьютерным сетям, хостам и данным;
- рассказать о роли шифрования для мониторинга сетевой безопасности;
- рассказать о способах определения уязвимостей оконечных устройств и атаках на них;
- оценивать предупреждения безопасности сети;
- анализировать данные о вторжении в сеть для определения скомпрометированных хостов и уязвимостей;
- применять модели реагирования для устранения инцидентов безопасности.

Требования к лабораторным работам с использованием виртуальной машины

В этом курсе одна виртуальная машина (ВМ) используется для выполнения множества лабораторных работ до главы 10 включительно. В главе 11 добавляются еще три виртуальные машины. Также доступен вариант с одной виртуальной машиной для компьютеров студентов или лабораторных работ, которые не соответствуют следующим требованиям:

- хост-компьютер с 64-разрядным процессором, не менее 8 ГБ ОЗУ и 45 ГБ свободного дискового пространства (как определить, оснащен ли хост-компьютер 64-разрядным процессором, см. по ссылке https://www.computerhope.com/issues/ch001121.htm).
- Последняя версия Oracle VirtualBox: http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html
- Интернет-подключение
- Пять виртуальных машин, перечисленных в таблице ниже.

Таблица 1. Требования виртуальной машины

Виртуальная машина	RAM	Дисковое пространство	Имя пользователя	Пароль
Виртуальная машина рабочей станции CyberOps	1 ГБ	7 ГБ	analyst	cyberops
Kali	1 ГБ	10 ГБ	корневой	cyberops
Metasploitable	512 МБ	8 ГБ	msfadmin	msfadmin
Security Onion	4 ГБ	10 ГБ	analyst	cyberops
Security Onion (альтернативная)*	3 ГБ	10 ГБ	analyst	cyberops

*Для выполнения лабораторных работ 12.4.1.1 и 12.4.1.2 из главы 12 можно использовать только одну альтернативную виртуальную машину Security Onion.

Для того чтобы процесс обучения каждого студента был оптимальным, рекомендуется организовать в классе от 12 до 15 рабочих мест и обеспечить отдельный компьютер каждому студенту. На одном лабораторном компьютере не должно совместно работать больше двух студентов при выполнении лабораторных работ. Для некоторых лабораторных работ потребуется, чтобы компьютеры студентов были подключены к локальной сети.

Описание курса

Таблица 2. Cybersecurity Operations v1.1. Описание курса

Глава/Раздел	Цели/задачи
Глава 1. Кибербезопасность и центр мониторинга и управления безопасностью	**рассказать, какую роль выполняет на предприятии аналитик по кибербезопасности;**
1.1. Опасность	Объясните, почему сети и данные подвергаются атакам.
1.2. Борцы с киберпреступностью	Объясните, как подготовиться к работе в сфере информационной безопасности.

Глава 2. Операционная система Windows	**Расскажите о функциях и характеристиках операционной системы Windows, служащих для поддержки анализа кибербезопасности.**
2.1. Обзор ОС Windows	Объясните принципы работы операционной системы Windows.
2.2. Администрирование Windows	Объясните, как обеспечить защиту оконечных устройств, работающих под управлением ОС Windows.
Глава 3. Операционная система Linux	**Описание функций и характеристика операционной системы Linux.**
3.1. Работа с Linux	Выполните базовые операции в оболочке Linux.
3.2. Администрирование Linux	Выполните основные задачи администрирования Linux.
3.3. Клиенты Linux	Выполните основные задачи, связанные с информационной безопасностью, на хосте под управлением ОС Linux.
Глава 4. Сетевые протоколы и службы	**Анализ работы сетевых протоколов и служб.**
4.1. Сетевые протоколы	Объясните использование протоколов для сетевых операций.
4.2. Ethernet и протокол IP	Разъяснение использования протоколов Ethernet и IP для передачи данных по сети.
4.3. Проверка подключения	Использовать типичные утилиты для проверки и тестирования сетевого подключения.
4.4. Протокол разрешения адресов (ARP)	Объяснить, как протокол разрешения адресов (ARP) позволяет передавать данные по сети.
4.5. Транспортный уровень и сетевые сервисы	Описание того, как протоколы транспортного уровня и сетевые службы обеспечивают функционирование сети.
4.6. Сетевые сервисы	Объясните, как сетевые сервисы обеспечивают функционирование сети.
Глава 5. Сетевая инфраструктура	**Разъяснение принципов работы сетевой инфраструктуры.**
5.1. Сетевые устройства связи	Объясните, как сетевые устройства обеспечивают обмен данными по проводной и беспроводной сети.
5.2. Инфраструктура обеспечения сетевой безопасности	Объясните, как устройства и службы используются для обеспечения безопасности сети.
5.3. Представления сети	Объясните, каким образом представляются сети и сетевые топологии.
Глава 6. Принципы обеспечения безопасности сети	**Классификация различных типов сетевых атак.**
6.1. Хакеры и их инструменты	Объясните, как происходят атаки на сети.
6.2. Распространенные угрозы и атаки	Расскажите о различных видах угроз и атак.
Глава 7. Сетевые атаки. Углубленный разбор	**Использование средств сетевого мониторинга для определения атак на сетевые протоколы и службы.**

7.1. Изучение работы сети	Объяснение мониторинга сетевого трафика.
7.2. Атаки на базовые функции	Рассказ об уязвимостях TCP/IP, позволяющих проведение сетевых атак.
7.3. Атаки на то, что мы делаем	Описание уязвимости к атакам распространенных сетевых приложений и служб.
Глава 8. Защита сети	**Применение различных способов предотвращения несанкционированного доступа к компьютерным сетям, хостам и данным.**
8.1. Объяснение принципов защиты	Описание подходов к защите безопасности сети.
8.2. Контроль доступа	Описание управления доступом как способа защиты сети.
8.3. Межсетевые экраны и предотвращение вторжений	Описание использования межсетевых экранов и других устройств для предотвращения вторжений в сеть.
8.4. Фильтрация содержимого	Описание использования фильтрации содержимого для предотвращения попадания нежелательных данных в сеть.
8.5. Аналитика угроз	Использование различных источников аналитики для обнаружения текущих угроз безопасности.
Глава 9. Криптография и инфраструктура общих ключей	**Объяснение роли шифрования для мониторинга сетевой безопасности.**
9.1. Криптография	Использование средств шифрования и расшифровки данных.
9.2. Криптография с общими ключами	Объяснение того, как инфраструктура открытых ключей (PKI) поддерживает сетевую безопасность.
Глава 10. Защита и анализ оконечных устройств	**Объяснение способов определения уязвимостей оконечных устройств и атак на них.**
10.1. Защита оконечных устройств	Использование инструментальных средств для формирования отчета об анализе вредоносного ПО.
10.2. Оценка уязвимостей оконечных устройств	Классификация данных оценки уязвимостей оконечного устройства.
Глава 11. Мониторинг безопасности	**Оценка предупреждений о безопасности сети.**
11.1. Технологии и протоколы	Объясните, как технологии обеспечения безопасности влияют на мониторинг безопасности.
11.2. Файлы журналов	Описание типов файлов журналов, используемых в мониторинге безопасности.
Глава 12. Анализ данных вторжений	**Выполнение анализа данных о вторжении в сеть для определения скомпрометированных хостов и уязвимостей.**
12.1. Сбор данных	Описание сбора данных, связанных с безопасностью.
12.2. Подготовка данных	Систематизация различных файлов журналов при подготовке к анализу данных о вторжении.
12.3. Анализ данных	Анализ данных о вторжении для определения источника атаки.

Глава 13. Реагирование на инциденты и их обработка	**Описание процесса обработки инцидентов безопасности группами CSIRT.**
13.1. Модели реагирования на инциденты	Применение моделей реагирования на инциденты к событию вторжения.
13.2. Группы CSIRT и NIST 800-61r2	Применение к событию информационной безопасности стандартов, указанных в NIST 800-61r2.
13.3. Действия на основе прецедентов	Изоляция злоумышленника и составление плана реагирование на инциденты по набору журналов.

Россия, 115054, Москва,
бизнес-центр «Риверсайд Тауэрс»,
Космодамианская наб., д. 52, стр. 1, 4 этаж
Телефон: +7 (495) 961 1410, факс: +7 (495) 961 1469
www.cisco.ru, www.cisco.com

Россия, 197198, Санкт-Петербург,
бизнес-центр «Арена Холл»,
пр. Добролюбова, д. 16, лит. А, корп. 2
Телефон: +7 (812) 313 6230, факс: +7 (812) 313 6280
www.cisco.ru, www.cisco.com

Украина, 03038, Киев,
бизнес-центр «Горизонт Парк»,
ул. Николая Гринченко, 4В
Телефон: +38 (044) 391 3600, факс: +38 (044) 391 3601
www.cisco.ua, www.cisco.com

Беларусь, 220034, Минск,
бизнес-центр «Виктория Плаза»,
ул. Платонова, д. 1Б, 3 п., 2 этаж.
Телефон: +375 (17) 269 1691, факс: +375 (17) 269 1699
www.cisco.ru

Казахстан, 050059, Алматы,
бизнес-центр «Самал Тауэрс»,
ул. О. Жолдасбекова, 97, блок А2, 14 этаж
Телефон: +7 (727) 244 2101, факс: +7 (727) 244 2102

Азербайджан, AZ1010, Баку,
ул. Низами, 90А, Лэндмарк здание III, 3-й этаж
Телефон: +994-12-437-48-20, факс: +994-12-437 4821

Узбекистан, 100000, Ташкент,
бизнес центр INCONEL, ул. Пушкина, 75, офис 605
Телефон: +998-71-140-4460, факс: +998-71-140 4465