МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

“Ярославский государственный университет им. П.Г. Демидова”

УТВЕРЖДАЮ

Ректор
А.И.Русаков
(подпись)
«__» _____ 2021 г.

ПРОГРАММА КУРСОВ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Сети связи и системы коммутации:

программа «CCNA Cybersecurity»

Ярославль, 2021

1. Цель реализации программы

дать практические знания и навыки, необходимые для успешного выполнения задач и обязанностей аналитика по безопасности младшего уровня в Центре мониторинга и управления безопасностью (SOC).

2. Планируемые результаты обучения

- знать методы установки виртуальной машины и создания безопасной среды;
- знать современные методы анализа работы сетевых протоколов и служб;
- знать средства сетевого мониторинга для определения атак на сетевые протоколы и службы;
- владеть технологиями анализа работы сетевых протоколов и служб;
- владеть способами реагирования для устранения инцидентов безопасности;
- владеть средствами анализа данных о вторжении в сеть.

3. Содержание программы

УЧЕБНЫЙ ПЛАН
курсов повышения квалификации
«Сети связи и системы коммутации: программа «CCNA Cybersecurity»
(наименование)

Категория слушателей: лица желающие получить образование IT-специалиста
Срок обучения: 2 месяца (72 часа)
Форма обучения: с применением дистанционных технологий без отрыва от работы

№ п/п	Наименование разделов и дисциплин	Общая трудоемкость, ч.	В том числе						Сам. раб.	Формы контроля
			Аудиторные занятия, ч.			Дистанционное обучение, ч.				
			Всего	из них		Всего	из них			
				лекции	практика		лекции	практика		
1.	Кибербезопасность и центр мониторинга и управления безопасностью	5						1	4	
2.	Операционная система	6						1	5	
3.	Операционная система Linux	6						1	5	
4.	Сетевые протоколы и службы	5						1	4	
5.	Сетевая инфраструктура	5						1	4	
6.	Принципы обеспечения безопасности сети	6						1	5	
7.	Сетевые атаки. Углубленный разбор	6						1	5	
8.	Защита сети	6						1	5	
9.	Криптография и инфраструктура общих ключей	5						1	4	
10.	Защита и анализ оконечных устройств	6						1	5	

11.	Мониторинг безопасности	**6**						**1**	**5**	
12.	Анализ данных вторжений	**5**						**1**	**4**	
13.	Реагирование на инциденты и их обработка	**5**						**1**	**4**	
	Итоговая аттестация:									Экзамен (тест)
	Итого	**72**						**13**	**59**	

УЧЕБНАЯ ПРОГРАММА

курсов повышения квалификации

«Сети связи и системы коммутации: программа «CCNA Cybersecurity»

Тема 1. Кибербезопасность и центр мониторинга и управления безопасностью.

В теме представлено описание почему сети и данные подвергаются атакам. Также рассказывается как подготовиться к работе в сфере информационной безопасности.

Тема 2. Операционная система Windows.

Данный модуль посвящен принципам работы операционной системы Windows. Так же рассматривается модели обеспечения защиты оконечных устройств, работающих под управлением ОС Windows.

Тема 3. Операционная система Linux.

В главе рассматриваются основные модели администрирования ОС Linux. Так же даются навыки выполнения базовых операций в оболочке Linux. Слушатели также знакомятся с основными задачами, связанными с информационной безопасностью, на хосте под управлением ОС Linux.

Тема 4. Сетевые протоколы и службы.

В главе подробно рассматриваются Ethernet и протокол IP и разъясняется методы использования протоколов Ethernet и IP для передачи данных по сети. Так же разбираются типичные утилиты для проверки и тестирования сетевого подключения.

Тема 5. Сетевая инфраструктура.

В теме объясняют, как сетевые устройства обеспечивают обмен данными по проводной и беспроводной сети. Так же разбираются как устройства и службы используются для обеспечения безопасности сети.

Тема 6. Принципы обеспечения безопасности сети.

Объясняются как происходят атаки на сети и какие виды угроз существуют.

Тема 7. Сетевые атаки. Углубленный разбор.

В главе подробно изучается принципы работы сети. Рассматриваются атаки на базовые функции и рассказывается об уязвимостях TCP/IP, позволяющих проведение сетевых атак.

Тема 8. Защита сети.

Объяснение принципов защиты сети и описание подходов к защите безопасности сети. Разбираются методы контроля доступа и описание управления доступом как способа защиты сети.

Тема 9. Криптография и инфраструктура общих ключей.

В главе подробно рассматриваются различные архитектуры и особенности проектирования, защиты, эксплуатации корпоративных сетей, а также поиска и устранения неполадок. Она охватывает особенности создания глобальных сетей (WAN) и применения механизмов качества обслуживания (QoS) для защиты удаленного доступа. Слушатели также знакомятся с понятиями программно-определяемой сети, виртуализации и автоматизации, то есть основами цифровых сетей.

Тема 10. Защита и анализ оконечных устройств.

В главе подробно рассматриваются различные архитектуры и особенности проектирования, защиты, эксплуатации корпоративных сетей, а также поиска и устранения неполадок. Она охватывает особенности создания глобальных сетей (WAN) и применения механизмов качества обслуживания (QoS) для защиты удаленного доступа. Слушатели также знакомятся с понятиями программно-определяемой сети, виртуализации и автоматизации, то есть основами цифровых сетей.

Тема 11. Мониторинг безопасности.

В главе подробно рассматриваются различные архитектуры и особенности проектирования, защиты, эксплуатации корпоративных сетей, а также поиска и устранения неполадок. Она охватывает особенности создания глобальных сетей (WAN) и применения механизмов качества обслуживания (QoS) для защиты удаленного доступа. Слушатели также знакомятся с понятиями программно-определяемой сети, виртуализации и автоматизации, то есть основами цифровых сетей.

Тема 12. Анализ данных вторжений.

В главе подробно рассматриваются различные архитектуры и особенности проектирования, защиты, эксплуатации корпоративных сетей, а также поиска и устранения неполадок. Она охватывает особенности создания глобальных сетей (WAN) и применения механизмов качества обслуживания (QoS) для защиты удаленного доступа. Слушатели также знакомятся с понятиями программно-определяемой сети, виртуализации и автоматизации, то есть основами цифровых сетей.

Тема 13. Реагирование на инциденты и их обработка.

Модели реагирования на инциденты, а также применение моделей реагирования на инциденты к событию вторжения. Как применять событию информационной безопасности стандартов, указанных в NIST 800-61r2.

4. Условия реализации программы

Условия организации и проведения учебных занятий:

- наличие рабочих столов из расчета не менее 0,48 кв.м. на каждого слушателя, причем за каждым отдельно стоящим столом должны работать не более 1 слушателя;
- обеспечение техники для проведения обучения (проектор, ноутбук или компьютер, экран, колонки), прочим оборудованием и принадлежностями необходимыми для учебного процесса.

4.1 Структурная матрица используемого технологического и учебно-методического обеспечения

Номер раздела	Технологическое обеспечение		Учебно-методическое обеспечение дисциплины												
			Средства лекционного преподавания				Учебная литература для слушателей				Электронные ресурсы				
													Электронные копии		
	Традиционные технологии	Инновационные технологии	Раздаточный материал	Материалы для мультимедийных средств	Мультимедийные презентации	Другие средства	Конспект лекций	Учебные пособия	Методические указания	Другая учебная литература	Мультимедийные презентации	Другие электронные ресурсы	лекций	методических указаний	других электронных ресурсов
1	+	+		+	+					+	+		+		
2	+	+		+	+					+	+		+		
3	+	+		+	+					+	+		+		

4.2 Перечень литературы и методических материалов.

3.2.1 Основная литература

1. Cisco Security Agent. – Издательство Cisco Press, 2006 – 456 с.
2. CCNA (Cisco Certified Network Associate). Учебное руководство. – Издательство: Лори, 2002 – 741 с.
3. Cisco CCNA Routing and Switching 200-120 Official Cert Guide. – Издательство: Cisco Press, 2013 – 1758 с.

4.3 Техническое обеспечение

Мультимедийный проектор, аппаратура для проведения видеотренинга.

5. Формы аттестации, оценочные материалы

Оценка качества освоения программы осуществляется в виде тестирования в электроной форме на основе стобальной системы оценок по основным разделам программы. Тестирование считается пройденным при наличии 90% правильных ответов

1. ABC Company just purchased three new routers to start their company network. Which items are needed to establish a terminal session between a PC and the router for the initial configuration? (Choose three.)

a. straight-through cable.
b. terminal emulation software. +
c. rollover cable. +
d. RJ-45 to DB-9 connector+
e. V.35 cable.

2. Which of the following descriptions are true regarding the management connections on a Cisco router? (Choose three.)

a. They are non-network connections.+
b. They are used to connect the router to the rest of the production network.
c. They are synchronous serial ports.
d. They are used for initial router configuration.+
e. They are asynchronous serial ports. +
g. They are accessed using their assigned IP address.

3. What contains the instructions that a router uses to control the flow of traffic through its interfaces?

a. packet configuration.
b. configuration files+
c. flash memory.
d. internal components.

4. Which of the following describes the function of a WAN?

a. connects peripherals in a single location.
b. connects multiple networks in a single building.
c. provides connectivity on a LAN.
d. provides connectivity over a large geographic area.+

5. An internetwork must include which of the following? (Choose three.)

a. switching.+
b. static addressing.
c. IETF standardization.
d. dynamic or static routing.+
e. consistent end-to-end addressing.+

6. Which basic components do a router and a standard desktop PC have in common? (Choose three.)

a. JR-Admin cannot issue any command because the privilege level does not match one of those defined.
b. JR-Admin can issue debug and reload commands.
c. JR-Admin can issue only ping commands.+
d. JR-Admin can issue ping and reload commands
e. R-Admin can issue show, ping, and reload commands.

7. Which recommended security practice prevents attackers from performing password recovery on a Cisco IOS router for the purpose of gaining access to the privileged EXEC mode?

a. Keep a secure copy of the router Cisco IOS image and router configuration file as a backup.
b. Disable all unused ports and interfaces to reduce the number of ways that the router can be accessed.+
c. Configure secure administrative control to ensure that only authorized personnel can access the router.
d. Locate the router in a secure locked room that is accessible only to authorized personnel.
e. Provision the router with the maximum amount of memory possible.

8. Which three options can be configured by Cisco AutoSecure? (Choose three.)

a. CBAC
b. SNMP
c. Syslog+
d. security banner+
e. interface IP address
f. enable secret password+

9. Refer to the exhibit. Based on the output of the show running-config command, which type of view is SUPPORT?

a. secret view, with a level 5 encrypted password
b. root view, with a level 5 encrypted secret password+
c. superview, containing SHOWVIEW and VERIFYVIEW views
d. CLI view, containing SHOWVIEW and VERIFYVIEW commands

10. Which three services on a router does Cisco SDM One-Step Lockdown enable? (Choose three.)

a. SNMP
b. TCP intercepts+
c. SSH access to the router+
d. Cisco Discovery Protocol
e. password encryption service+
f. firewall on all outside interfaces

11. An administrator defined a local user account with a secret password on router R1 for use with SSH. Which three additional steps are required to configure R1 to accept only encrypted SSH connections? (Choose three.)

a. configure the IP domain name on the router+
b. enable inbound vty Telnet sessions+
c. generate the SSH keys
d. configure DNS on the router
e. enable inbound vty SSH sessions
f. generate two-way pre-shared keys+

12. Which statement describes the operation of the Cisco SDM Security Audit wizard?

a. The wizard configures a router to prevent unauthorized access.
b. The wizard compares a router configuration against recommended settings.+
c. The wizard monitors network data and logs possible unauthorized or malicious traffic.
d. The wizard logs the effectiveness of network security measures for baseline comparisons.

13. An administrator needs to create a user account with custom access to most privileged EXEC commands. Which privilege command is used to create this custom account?

a. privilege exec level 0
b. privilege exec level 1+
c. privilege exec level 2
d. privilege exec level 15
e.

14. Which three areas of router security must be maintained to secure an edge router at the network perimeter? (Choose three.)

a. flash security
b. physical security+
c. operating system security
d. remote access security
e. router hardening
f. zone isolation

15. Which service is enabled on a Cisco router by default that can reveal significant information about the router and potentially make it more vulnerable to attack?

a. HTTP
b. CDP
c. FTP+
d. NTP
e. TFTP

16. Which two operations are required to implement Cisco SDM One-Step Lockdown? (Choose two.)

a. Choose the One-Step Lockdown feature.
b. Apply the documented network policies.+
c. Deliver the configuration changes to the router.+
d. Compare the router configuration against recommended settings.
e. Select the Firewall and ACL task on the SDM Configuration screen.

17. Which statement matches the CLI commands to the SDM wizard that performs similar configuration functions?

a. aaa configuration commands and the SDM Basic Firewall wizard
b. auto secure privileged EXEC command and the SDM One-Step Lockdown wizard
c. class-maps, policy-maps, and service-policy configuration commands and the SDM IPS wizard+
d. setup privileged EXEC command and the SDM Security Audit wizard

7. Составители программы

Бизин О.Е., начальник 5 отдела УЦИ