ОБРАЗОВАТЕЛЬНОЕ ЧАСТНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ "ЦЕНТР ОБУЧЕНИЯ "СПЕЦИАЛИСТ" УНЦ ПРИ МГТУ ИМ. Н.Э. БАУМАНА
(ОЧУ ДПО «СПЕЦИАЛИСТ»)
123242, город Москва, улица Зоологическая, дом 11, строение 2, этаж 2, помещение №I, комната №12,
ИНН 7701168244, ОГРН 1127799002990

Утверждаю:
Директор ОЧУ ДПО «Специалист»

_____/Д.Ю.Звезлочкин/
«17» января 2022 года

Дополнительная профессиональная программа профессиональной переподготовки «Linux. Уровень 3. Обеспечение безопасности систем, сервисов и сетей»

город Москва

Программа «Linux. Уровень 3. Обеспечение безопасности систем, сервисов и сетей» разработана в соответствии с требованиями Профессионального Стандарта

Повышение квалификации слушателей, осуществляемое в соответствии с программой, проводится с использованием модульного принципа построения учебного плана с применением различных образовательных технологий, в том числе дистанционных образовательных технологий и электронного обучения в соответствии с законодательством об образовании.

Дополнительная профессиональная программа повышения квалификации, разработана образовательной организацией в соответствии с законодательством Российской Федерации, включает все модули, указанные в учебном плане.

Содержание оценочных и методических материалов определяется образовательной организацией самостоятельно с учетом положений законодательства об образовании Российской Федерации.

Структура дополнительной профессиональной программы соответствует действующим нормативно-правовым актам:

- ФЗ №273 «Об образовании в Российской Федерации», приказу Минобрнауки России от 1 июля 2013 г.;
- Приказ Министерства образования и науки Российской Федерации от 1 июля 2013 г. N 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам».

Объем дополнительной профессиональной программы вне зависимости от применяемых образовательных технологий, должен быть не менее 16 академических часов. Сроки ее освоения определяются образовательной организацией самостоятельно.

Формы обучения слушателей (очная, очно-заочная, заочная) определяются образовательной организацией самостоятельно.

К освоению дополнительных профессиональных программ допускаются:

- лица, имеющие среднее профессиональное и (или) высшее образование;
- лица, получающие среднее профессиональное и (или) высшее образование.

Для определения структуры дополнительной профессиональной программы и трудоемкости ее освоения может применяться система зачетных единиц. Количество зачетных единиц по дополнительной профессиональной программе устанавливается организацией.

Образовательная деятельность слушателей предусматривает следующие виды учебных занятий и учебных работ: лекции, практические и семинарские занятия, лабораторные работы, круглые столы, мастер-классы, мастерские, деловые игры, ролевые игры, тренинги, семинары по обмену опытом, выездные занятия, консультации, выполнение аттестационной, дипломной, проектной работы и другие виды учебных занятий и учебных работ, определенные учебным планом.

Правила внутреннего распорядка обучающихся регулируются лицензией на осуществление образовательной деятельности № 039441 (бланк серия СР77Л01 № 0010312, регистрационный номер лицензии Л035-01298-77/00182700), от 20.06.2018 года "Центр обучения "Специалист" УНЦ при МГТУ им Н.Э. Баумана", а также другими локальными актами организации, регулирующими образовательную деятельность.

Аннотация. Курс позволит получить ключевые знания по обеспечению комплексной безопасности сетевой инфраструктуры, что значительно уменьшит риск взлома сетей и сервисов предприятия и минимизировать последствия такого взлома. Уникальной особенностью курса являются лабораторные работы, которые дадут возможность слушателям побывать по обе стороны «баррикад» - в роли хакеров и в роли администраторов безопасности сети. Слушатели будут производить сканирования и, даже, реальные «взломы» своих систем и перехваты конфиденциальной информации, чтобы, впоследствии, научиться защищать системы от таких действий.

Цель программы: программа повышения квалификации направлена на совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации. Цель курса – предоставить слушателям комплекс знаний и практических навыков для работы системным администратором Linux.

Совершенствуемые компетенции

№	Компетенция	Направление подготовки
		ФГОС ВО ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 09.03.02 «ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ» (УРОВЕНЬ БАКАЛАВРИАТА)
		Код компетенции
1	Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности	ОПК-1
2	Способен использовать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности	ОПК-2
3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3
4	Способен участвовать в разработке технической документации, связанной с профессиональной деятельностью с использованием стандартов, норм и правил;	ОПК-4
5	Способен инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем	ОПК-5
6	Способен разрабатывать алгоритмы и программы, пригодные для практического применения в области информационных систем и технологий	ОПК-6
7	Способен осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем	ОПК-7
8	Способен применять математические модели, методы и средства проектирования информационных и автоматизированных систем	ОПК-8

Совершенствуемые компетенции

Совершенствуемые компетенции в соответствии с трудовыми фикциями профессионального стандарта 06.016 «Руководитель проектов в области информационных технологий» утвержден Приказом Министерства труда и социальной защиты Российской Федерации от 18.11.2014 № 893н

Совершенствуемые и/или формируемые компетенции	**Направление подготовки** **ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ** **Трудовые функции (код)** **«Руководитель проектов в области информационных технологий»**
А6 Управление проектами в области ИТ на основе полученных планов проектов в условиях, когда проект не выходит за пределы утвержденных параметров	A/01.6 Идентификация конфигурации ИС в соответствии с полученным планом A/02.6 Ведение отчетности по статусу конфигурации ИС в соответствии с полученным планом A/03.6 Аудит конфигураций ИС в соответствии с полученным планом A/04.6 Организация репозитория проекта в области ИТ в соответствии с полученным планом A/05.6 Проверка реализации запросов на изменение (верификация) в соответствии с полученным планом A/06.6 Организация заключения договоров в проектах в соответствии с полученным заданием A/07.6 Мониторинг выполнения договоров в проектах в области ИТ в соответствии с полученным планом A/08.6 Организация заключения дополнительных соглашений к договорам в соответствии с полученным заданием A/09.6 Регистрация запросов заказчика в соответствии с установленными регламентами A/10.6 Согласование документации в соответствии с установленными регламентами A/11.6 Управление распространением документации в соответствии с установленными регламентами A/12.6 Контроль хранения документации в соответствии с установленными регламентами A/13.6 Сбор информации для инициации проекта в соответствии с полученным заданием A/14.6 Планирование проекта в соответствии с полученным заданием

	A/15.6 Организация исполнения работ проекта в соответствии с полученным планом A/16.6 Мониторинг и управление работами проекта в соответствии с установленными регламентами A/17.6 Общее управление изменениями в проектах в соответствии с полученным заданием A/18.6 Завершение проекта в соответствии с полученным заданием A/19.6 Подготовка к выбору поставщиков в проектах в области ИТ в соответствии с полученным заданием A/20.6 Исполнение закупок в ИТ-проектах в соответствии с полученным заданием A/21.6 Обеспечение качества в проектах в области ИТ в соответствии с установленными регламентами A/22.6 Организация приемо-сдаточных испытаний (валидация) в проектах малого и среднего уровня сложности в области ИТ в соответствии с установленными регламентами A/23.6 Организация выполнения работ по выявлению требований в соответствии с полученным планом A/24.6 Организация выполнения работ по анализу требований в соответствии с полученным планом A/25.6 Согласование требований в соответствии с полученными планами A/26.6 Реализация мер по неразглашению информации, полученной от заказчика A/27.6 Идентификация заинтересованных сторон проекта в области ИТ в соответствии с полученным заданием A/28.6 Распространение информации в проектах в области ИТ в соответствии с полученным заданием A/29.6 Идентификация рисков проектов в области ИТ в соответствии с полученным заданием A/30.6 Анализ рисков в проектах в области ИТ в соответствии с полученным заданием

После окончания обучения Слушатель будет знать:

- Принципы по обеспечению комплексной безопасности сетевой инфраструктуры, что позволит значительно уменьшить риск взлома сетей и сервисов предприятия или минимизировать последствия такого взлома

- Процесс сканирования и «взлома» систем, пути перехвата конфиденциальной информации для выработки стратегии защиты системы от таких действий
- Уязвимости некоторых распространенных решений, альтернативные и безопасные решения
- Комплексная безопасность сетевой инфраструктуры средствами Linux, функции специалиста по информационной безопасности

После окончания обучения Слушатель будет уметь:

- Выбрать правильную, с точки зрения безопасности, конфигурацию сети
- Безопасным способом связать в единую сеть несколько филиалов
- Безопасным способом предоставить доступ к сетевым ресурсам предприятия удаленным пользователям
- Использовать сканеры безопасности для оценки безопасности систем, сервисов и сетей
- Использовать средства аудита состояния систем с точки зрения безопасности
- Использовать механизмы защиты систем от вредоносных действий пользователей и скомпрометированного ПО
- Осуществлять настройку сервисов сети предприятия с точки зрения безопасности и конфиденциальности данных
- Осуществлять активную защиту периметра сети с помощью систем IDS и IPS

Учебный план

Категория слушателей: Курс предназначен для системных администраторов, которым требуется обеспечить комплексную безопасность сетевой инфраструктуры средствами Linux, а также для тех, кто планирует освоить смежную компетенцию специалиста по информационной безопасности.

Уровень образования: дополнительное профессиональное образование: повышение квалификации/ профессиональная переподготовка.

Требования к предварительной подготовке: Успешное окончание курса Linux. Уровень 2. Администрирование сервисов и сетей или эквивалентная подготовка.

Срок обучения: 24 академических часов в группе с преподавателем, 12 академических часов самостоятельных занятий в аудитории (СРС).

Форма обучения: очная, очно-заочная, заочная. По желанию слушателя форма обучения может быть изменена и/или дополнена.

Режим занятий: утренний, дневной, вечерний, группы выходного дня, онлайн

Документ, выдаваемый после завершения обучения:
Удостоверение о повышении квалификации;
Свидетельство о прохождении курсов.

№	Наименование модулей	Кол-во часов	Виды учебных занятий			Форма контроля
			Лекции	Практические занятия	СРС	
1	Периметры безопасности и размещение сервисов в сети предприятия	4	2	2	2	Лабораторная работа

2	Анализ информационных систем предприятия с точки зрения безопасности	4	2	2	2	Лабораторная работа
3	Защита систем предприятия на уровне ОС	4	2	2	2	Лабораторная работа
4	Защита сервисов предприятия	4	2	2	2	Лабораторная работа
5	Защита сети предприятия	4	2	2	2	Лабораторная работа
6	Использование VPN в сети предприятия	4	2	2	2	Лабораторная работа
	ИТОГО	24			12	
	Итоговая аттестация	Тестирование				

Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

Количество аудиторных занятий при очно-заочной форме обучения составляет 20-25% от общего количества часов.

Календарный учебный график

Календарный учебный график формируется при осуществлении обучения в течение всего календарного года. По мере набора групп слушателей по программе составляется календарный график, учитывающий объемы лекций, практики, самоподготовки.

Неделя обучения	1	2	3	4	5	6	7	Итого часов
	пн	вт	ср	чт	пт	сб	вс	
1 неделя	8	8	8ИА					24
СРС	2	2	2	2	2	2		12
Итого:								24/12
Примечание: ИА – Итоговая аттестация (тестирование)								

Учебная программа

Наименование	Виды учебных занятий	Содержание
Модуль 1. Периметры безопасности и размещение сервисов в сети предприятия	Лекция	Обзор моделей безопасности и обязанностей администратора безопасности компьютерной сети
	Лекция	Выбор конфигурации сети предприятия
	Лекция	Разделение сервисов сети предприятия с точки зрения аудитории

	Лабораторная работа	Развертывание шлюза и сетей предприятия: - Настройка шлюза для подключения сети предприятия к Internet - Развертывание сетей предприятия (DMZ, MGMT, LAN) - Развертывание сервисов в сетях предприятия
Модуль 2. Анализ информационных систем предприятия с точки зрения безопасности	Лекция	Методы анализа безопасности сети и сервисов предприятия
	Лабораторная работа	Использование сканеров безопасности: - Оценка безопасности систем и сервисов с помощью сканеров Nmap и OpenVAS - Оценка безопасности передачи информации по сети с помощью сканера Ettercap - Аудит учетных данных (John the Ripper) - Аудит целостности систем (Tripwire, AIDE, OSSEC) - Аудит закладок (rkhunter, chkrootkit) - Аудит системных событий Linux (auditd)
Модуль 3. Защита систем предприятия на уровне ОС	Лекция	Обзор технологий, повышающих безопасность систем на уровне ОС
	Лекция	Аудит состояния систем с точки зрения безопасности
	Лабораторная работа	Аудит состояния и защита систем предприятия: - Использование списков доступа POSIX ACL - Использование системного вызова Chroot - Использование механизмов мандатного доступа сервисов к объектам системы Linux LSM, AppArmor, SELinux - Использование технологии изоляции сервисов Linux namespaces/cgroup/Docker/LXC - Использование технологий Linux Hardened/PaX/grsecurity
Модуль 4. Защита сервисов предприятия	Лекция	Методы защиты сетевых сервисов от вредоносных действий

	Лабораторная работа	Защита сетевых сервисов предприятия: - Настройка сервисов с точки зрения безопасности (сокрытие «баннеров», отключение небезопасных опций, ограничение попыток входа и т.д.) - Ограничения привилегий учетных записей пользователей сервисов Замена устаревших сервисов (ftp/sftp, inetd/xinetd) - Развертывание Удостоверяющего центра (УЦ) Certificate of Authority (CA) предприятия - Защита конфиденциальной информации, передаваемой сервисам с использованием протоколов SSL/TLS - Использование PKI для управления идентификацией и конфиденциальности пользователей - Использование технологий Honeynet и Honeypot (portsentry) - Защита информации компании с использованием шифрования блочных устройств (dm-crypt) - Использование специальных решений для защиты сервисов (dhcdrop)
Модуль 5. Защита сети предприятия	Лекция	Обзор решений пассивной и активной защиты периметра сети предприятия
	Лабораторная работа	Защита периметра сети предприятия: - Использование возможностей пакетных фильтров для активной защиты периметра сети - Использование систем обнаружения вторжений (IDS) Snort для предупреждения о попытках вторжения - Использование решений защиты от вторжений (IPS) Snort/Snortsam/Fail2Ban для активной защиты периметра сети
Модуль 6. Использование VPN в сети предприятия	Лекция	Варианты организации сетей VPN
	Лабораторная работа	Управление доступом к внутренним ресурсам сети предприятия: - Использование SSH туннелей для организации VPN - Использование Proxy сервера Squid в качестве WebVPN

		- Использование OpenVPN для подключения филиалов и пользователей к сети предприятия

Организационно-педагогические условия

Соблюдение требований к кадровым условиям реализации дополнительной профессиональной программы:

а) преподавательский состав образовательной организации, обеспечивающий образовательный процесс, обладает высшим образованием и стажем преподавания по изучаемой тематике не менее 1 года и (или) практической работы в областях знаний, предусмотренных модулями программы, не менее 3 (трех) лет;

б) образовательной организацией наряду с традиционными лекционно-семинарскими занятиями применяются современные эффективные методики преподавания с применением интерактивных форм обучения, аудиовизуальных средств, информационно-телекоммуникационных ресурсов и наглядных учебных пособий.

Соблюдение требований к материально-техническому и учебно-методическому обеспечению дополнительной профессиональной программы:

а) образовательная организация располагает необходимой материально-технической базой, включая современные аудитории, библиотеку, аудиовизуальные средства обучения, мультимедийную аппаратуру, оргтехнику, копировальные аппараты. Материальная база соответствует санитарным и техническим нормам и правилам и обеспечивает проведение всех видов практической и дисциплинарной подготовки слушателей, предусмотренных учебным планом реализуемой дополнительной профессиональной программы.

б) в случае применения электронного обучения, дистанционных образовательных технологий каждый обучающийся в течение всего периода обучения обеспечивается индивидуальным неограниченным доступом к электронной информационно образовательной среде, содержащей все электронные образовательные ресурсы, перечисленные в модулях дополнительной профессиональной программы.

Формы аттестации и оценочные материалы

Образовательная организация несет ответственность за качество подготовки слушателей и реализацию дополнительной профессиональной программы в полном объеме в соответствии с учебным планом.

Оценка качества освоения слушателями программы курса включает текущий контроль успеваемости и промежуточную аттестацию.

Слушатели, успешно освоившие программу курса и прошедшие промежуточную аттестацию, получают удостоверение о повышении квалификации, а также допускаются к освоению следующего курса, входящего в состав дипломной программы (ДПП подготовки).

Слушателям, не прошедшим промежуточной аттестации или получившим на промежуточной аттестации неудовлетворительные результаты, а также лицам, освоившим часть курса и (или) отчисленные из образовательной организации, выдается справка об обучении или о периоде обучения по образцу, самостоятельно устанавливаемому образовательной организацией.

К итоговой аттестации по ДПП переподготовки допускаются только те слушатели, которые сдали промежуточную аттестацию по всем курсам (включая данный), входящим в дипломную программу (ДПП переподготовки).

Промежуточная аттестация проводится по форме выполнения задания в соответствии с учебным планом. Результаты промежуточной аттестации заносятся в соответствующие документы. Результаты промежуточной аттестации слушателей ДПП выставляются по двух бальной шкале («зачтено»/ «не зачтено»). «Зачтено» выставляется,

если слушатель набирает не менее 70% баллов (правильных ответов и/или выполненных заданий).

Учебно-методическое обеспечение и информационное обеспечение программы (литература)

Нормативно-правовые документы, дополнительная литература: авторские наработки преподавателя.

Материально-технические условия реализации программы: чехол одноразовый на наушник, файл-вкладыш А4, тетрадь, ручка

Текущая аттестация (выполнение практических/лабораторных работ по модулям)

Лабораторные работы по первому модулю:

Развертывание шлюза и сетей предприятия:

- Настройка шлюза для подключения сети предприятия к Internet
- Развертывание сетей предприятия (DMZ, MGMT, LAN)
- Развертывание сервисов в сетях предприятия

Лабораторные работы по второму модулю:

Использование сканеров безопасности:

- Оценка безопасности систем и сервисов с помощью сканеров Nmap и OpenVAS
- Оценка безопасности передачи информации по сети с помощью сканера Ettercap
- Аудит учетных данных (John the Ripper)
- Аудит целостности систем (Tripwire, AIDE, OSSEC)
- Аудит закладок (rkhunter, chkrootkit)
- Аудит системных событий Linux (auditd)

Лабораторные работы по третьему модулю:

Аудит состояния и защита систем предприятия:

- Использование списков доступа POSIX ACL
- Использование системного вызова Chroot
- Использование механизмов мандатного доступа сервисов к объектам системы Linux LSM, AppArmor, SELinux
- Использование технологии изоляции сервисов Linux namespaces/cgroup/Docker/LXC
- Использование технологий Linux Hardened/PaX/grsecurity

Лабораторные работы по четвертому модулю:

Защита сетевых сервисов предприятия:

- Настройка сервисов с точки зрения безопасности (сокрытие «баннеров», отключение небезопасных опций, ограничение попыток входа и т.д.)
- Ограничения привилегий учетных записей пользователей сервисов

Замена устаревших сервисов (ftp/sftp, inetd/xinetd)

- Развертывание Удостоверяющего центра (УЦ) Certificate of Authority (CA) предприятия
- Защита конфиденциальной информации, передаваемой сервисам с использованием протоколов SSL/TLS
- Использование PKI для управления идентификацией и конфиденциальности пользователей
- Использование технологий Honeynet и Honeypot (portsentry)
- Защита информации компании с использованием шифрования блочных устройств (dm-crypt)
- Использование специальных решений для защиты сервисов (dhcdrop)

Лабораторные работы по пятому модулю:

Защита периметра сети предприятия:

- Использование возможностей пакетных фильтров для активной защиты периметра сети

- Использование систем обнаружения вторжений (IDS) Snort для предупреждения о попытках вторжения
- Использование решений защиты от вторжений (IPS) Snort/Snortsam/Fail2Ban для активной защиты периметра сети

Лабораторные работы по шестому модулю:

Управление доступом к внутренним ресурсам сети предприятия:
- Использование SSH туннелей для организации VPN
- Использование Proxy сервера Squid в качестве WebVPN
- Использование OpenVPN для подключения филиалов и пользователей к сети предприятия

Итоговая аттестация по курсу (тестирование):

Аттестация проводится в виде теста на последнем занятии или на основании оценок практических работ, выполняемых во время обучения на курсе. Для успешной сдачи теста Вам нужно правильно ответить на 25 вопросов из 30.

Вопрос 1

Назовите атрибут, который может не играть роли при использовании PKI в корпоративной переписке по электронной почте?
Выберите один ответ:
Имя владельца
Подпись
Период действия
Адрес электронной почты
Имя компании

Вопрос 2

Для какого протокола необходим серверный SSL сертификат?
Выберите один ответ:
ftps
sftp
scp
ftp

Вопрос 3

В поле shell учетной записи пользователя допустимо использовать
Выберите один ответ:
только командный интерпретатор
любую программу

Вопрос 4

Для защиты сервиса от подбора учетных данных можно использовать решение
Выберите один ответ:
tcpwrap
fail2ban
portsentry

Вопрос 5

Авторитетный DNS сервер, отвечающий за домен предприятия, следует расположить
Выберите один ответ:
в сети DMZ
в локальной сети
в managment сети

Вопрос 6
Систему мониторинга оборудования предприятия следует расположить
Выберите один ответ:
в сети DMZ
в локальной сети
в managment сети

Вопрос 7
Выберите верное утверждение: разрешено устанавливать соединения
Выберите один ответ:
из сети DMZ в сеть WAN
из сети DMZ в сеть LAN
из сети WAN в сеть LAN

Вопрос 8
Почтовый сервер предприятия следует расположить
Выберите один ответ:
в сети DMZ
в локальной сети
в managment сети

Вопрос 9
Какая из перечисленных технологий позволяет реализовать принудительный контроль доступа?
Выберите один ответ:
UNIX права доступа
UNIX ACL
FreeBSD MAC

Вопрос 10
Какая из перечисленных технологий не использует namespaces?
Выберите один ответ:
chroot
LXC
Docker

Вопрос 11
Какой режим профиля AppArmor используется для ограничения приложения?
Выберите один ответ:
complain
enforce
disable

Вопрос 12

Какая из перечисленных технологий используется для изоляции процессов?
Выберите один ответ:
namespaces
cgroup

Вопрос 13

Какой модуль пакета netfilter позволяет ограничивать количество одновременных соединений?
Выберите один ответ:
persist table
conntrack
iptables

Вопрос 14
Выберите наиболее точную формулировку: сервис snort предназначен для
Выберите один ответ:
анализа трафика и протоколирования нарушений
анализа журналов и блокировки нарушителей

Вопрос 15
Какой элемент конфигурации пакета pf позволяет ограничивать количество одновременных соединений?
Выберите один ответ:
persist table
conntrack
max-src-conn-rate

Вопрос 16
Какой пакет используется для поиска изменений в системе?
Выберите один ответ:
tripwire
openvas
tcpdump
auditd

Вопрос 17
Какой пакет используется для сканирования открытых портов системы?
Выберите один ответ:
nmap
ettercap
john the ripper
chkrootkit

Вопрос 18
Какой пакет используется для взлома паролей?
Выберите один ответ:
nmap
ettercap
john the ripper
chkrootkit

Вопрос 19
Какой пакет используется для сканирования системы на наличие уязвимостей?
Выберите один ответ:
tripwire
openvas
tcpdump
auditd

Вопрос 20
Какой из пакетов не годится для предоставления авторизованного доступа к внутренним ресурсам сети предприятия?
Выберите один ответ:
OpenVPN
OpenSSH
OpenSSL

Вопрос 21
В каком файле конфигурации определяется соответствие между именем службы и номером порта и протоколом?
Выберите один ответ:
/etc/shells
/etc/protocols
/etc/services

Вопрос 22
Выберите наиболее точную формулировку: сервис fail2ban предназначен для
Выберите один ответ:
анализа трафика и блокировки нарушителей
анализа журналов и блокировки нарушителей
анализа журналов и выполнения настроенных действий

Вопрос 23
Какую из перечисленных технологий безопаснее использовать для реализации VPS?
Выберите один ответ:
chroot
FreeBSD MAC
FreeBSD Jail

Вопрос 24
Выберите верное утверждение: для создания цифровой подписи используется
Выберите один ответ:
закрытый ключ
открытый ключ
сессионный ключ

Вопрос 25
Выберите верное утверждение: для шифрования трафика в SSL/TLS используется
Выберите один ответ:
закрытый ключ
открытый ключ
сессионный ключ

Вопрос 26
Назовите атрибут, который может не играть роли при проверке серверного сертификата?
Выберите один ответ:
FQDN
Подпись
Период действия
Адрес электронной почты

Вопрос 27
Какой атрибут не содержится в запросе на сертификат?

Выберите один ответ:
Имя владельца
Период действия
Код страны

Вопрос 28
Какая из перечисленных технологий не использует LSM?
Выберите один ответ:
AppArmor
FreeBSD MAC
SELinux

Вопрос 29
Какая из перечисленных технологий позволяет реализовать принудительный контроль доступа?
Выберите один ответ:
UNIX права доступа
UNIX ACL
Linux LSM

Вопрос 30
Рекурсивный кэширующий DNS сервер предприятия следует расположить
Выберите один ответ:
в сети DMZ
в локальной сети
в managment сети