Образовательное частное учреждение
Дополнительного профессионального образования «Центр компьютерного обучения «Специалист» Учебно-научного центра при МГТУ им. Н.Э. Баумана»
(ОЧУ «Специалист»)

123242, город Москва, улица Зоологическая, дом 11, строение 2, помещение I, комната 11

ИНН 7701257303, ОГРН 1037739408189

Утверждаю:
Директор ОЧУ «Специалист»

_____/Т.С.Григорьева/
«01» июня 2018 года

Дополнительная профессиональная программа повышения квалификации

«Linux (CentOS/Debian)/FreeBSD. Уровень 3. Обеспечение безопасности систем, сервисов и сетей»

город Москва

Программа разработана в соответствии с приказом 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".

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 требованиям Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам, утвержденного приказом Минобрнауки России от 1 июля 2013 г. N 499.

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.

Аннотация. Материал курса позволяет получить ключевые знания по обеспечению комплексной безопасности сетевой инфраструктуры, что позволит значительно уменьшить риск взлома сетей и сервисов предприятия или минимизировать последствия такого взлома. Уникальной особенность курса являются лабораторные работы, позволяющие слушателям побывать по обе стороны «баррикад» - в роли хакеров и в роли администраторов безопасности сети. На занятиях слушатели будут производить сканирования и, даже, реальные «взломы» своих систем и перехваты конфиденциальной информации, чтобы, впоследствии, научиться защищать системы от таких действий. Будет продемонстрирована уязвимость некоторых распространенных решений и предложены альтернативные и безопасные решения. Все лабораторные работы максимально адаптированы под реальные условия, и легко могут быть перенесены в настоящую сеть предприятия. Курс предназначен для системных администраторов, которым требуется обеспечить комплексную безопасность сетевой инфраструктуры средствами UNIX (Linux/FreeBSD), а также для тех, кто планирует освоить смежную

компетенцию специалиста по информационной безопасности.

1. Цель программы:

В результате прохождения обучения предоставить слушателю комплекс знаний и практических навыков работы в UNIX (Linux/FreeBSD).

1.1. Планируемый результат обучения:

Лица, успешно освоившие программу, должны овладеть следующими компетенциями: управление проектами в области ИТ на основе полученных планов проектов в условиях, когда проект не выходит за пределы утвержденных параметров

1.2. Совершенствуемые компетенции

№	Компетенция	Направление подготовки ФГОС ВО ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 09.03.02 «ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ» (УРОВЕНЬ БАКАЛАВРИАТА)
		Код компетенции
1	способностью участвовать в работах по доводке и освоению информационных технологий в ходе внедрения и эксплуатации информационных систем	ПК-15
2	способностью к инсталляции, отладке программных и настройке технических средств для ввода информационных систем в опытную и промышленную эксплуатацию	ПК-28
3	способностью поддерживать работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества	ПК-30
4	способностью обеспечивать безопасность и целостность данных информационных систем и технологий	ПК-31
5	способностью адаптировать приложения к изменяющимся условиям функционирования	ПК-32
6	способностью выбирать и оценивать способ реализации информационных систем и устройств (программно-, аппаратно- или программно-аппаратно-) для решения поставленной задачи	ПК-37

1.3. Совершенствуемые компетенции в соответствии с трудовыми фикциями профессионального стандарта «РУКОВОДИТЕЛЬ ПРОЕКТОВ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ», утвержденного приказом Минтруда и социальной защиты РФ от 18 ноября 2014 г. N 893н

№	Компетенция	Направление подготовки
		ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ «Руководитель проектов в области информационных технологий» Утвержден приказом Минтруда России от 18.11.2014 N

		893н» (Зарегистрировано в Минюсте России 09.12.2014 N 35117) Наименование вида ПД: Менеджмент проектов в области информационных технологий (ИТ)
		Трудовые функции (код)
1	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 информационной системы (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/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

1.4. Планируемые результаты обучения

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 UNIX (Linux/FreeBSD), 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

2. Категория слушателей

Курс предназначен для системных администраторов, которым требуется обеспечить комплексную безопасность сетевой инфраструктуры средствами UNIX (Linux/FreeBSD), а также для тех, кто планирует освоить смежную компетенцию специалиста по информационной безопасности.

2.1. Требования к предварительной подготовке:

Требуемая подготовка: Linux (Ubuntu). Уровень 2. Администрирование сервисов и сетей или FreeBSD. Уровень 2. Администрирование сервисов и сетей, или эквивалентная подготовка.

Связь с другими программами и курсами (ДПП):
Linux (Ubuntu). Уровень 2. Администрирование сервисов и сетей
FreeBSD. Уровень 2. Администрирование сервисов и сетей,
CEH. Этичный хакинг и тестирование на проникновение

1.7. Срок обучения: 36 академических часов, в том числе 24 аудиторных, **СРС -** 12 час.
1.8. Форма обучения: очная. По желанию слушателя форма обучения может быть изменена и/или дополнена.
1.9. Режим занятий: дневной, вечерний, группы выходного дня.

2.2. Учебный план курса

№	Наименование модулей	Академические часы	Форма

п/п	по программе	Общая трудоемкость	В том числе			ПА [1]
			Аудиторные		СРС	
			Лекций	Практических занятий		
1	**Модуль 1. Периметры безопасности и размещение сервисов в сети предприятия**	6	2	2	2	Лабораторная работа
2	**Модуль 2. Анализ информационных систем предприятия с точки зрения безопасности**	6	2	2	2	Лабораторная работа
3	**Модуль 3. Защита систем предприятия на уровне ОС**	6	2	2	2	Лабораторная работа
4	**Модуль 4. Защита сервисов предприятия**	6	2	2	2	Лабораторная работа
5	**Модуль 5. Защита сети предприятия**	6	2	2	2	Лабораторная работа
6	**Модуль 6. Использование VPN для соединения сетей филиалов предприятия и удаленных пользователей**	6	2	2	2	Лабораторная работа
	ИТОГО:	**36**	12	12	**12**	
6	Итоговая аттестация	Тест				

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.

Практические занятия включают в себя, в частности, анализ ситуаций, выполнение практических заданий.

3. 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, выезды на объекты.

Неделя обучения	1	2	3	4	5	6	7	Итого часов
	пн	вт	ср	чт	пт	сб	вс	
1 неделя	0	4	0	4	0	0	0	8
СРС	0	2	0	2	0	0	0	4

[1] ПА – промежуточная аттестация

2 неделя	0	4	0	4	0	0	0	8
СРС	0	2	0	2	0	0	0	4
2 неделя	0	4	0	4ИА	0	0	0	8
СРС	0	2	0	2	0	0	0	4
Итого:	**0**	**18**	**0**	**18**	**0**	**0**	**0**	**36**
Примечание: ИА – Итоговая аттестация (тест)								

4. Рабочая программа

Модуль 1. Периметры безопасности и размещение сервисов в сети предприятия

- Обзор моделей безопасности и обязанностей администратора безопасности компьютерной сети.
- Выбор конфигурации сети предприятия
- Разделение сервисов сети предприятия с точки зрения аудитории, для которой они предназначены.
- Основные сети предприятия (DMZ, MGMT, INTERNAL)

Модуль 2. Анализ информационных систем предприятия с точки зрения безопасности

- Методы анализа безопасности сети и сервисов предприятия

Модуль 3. Защита систем предприятия на уровне ОС

- Обзор технологий повышающих безопасность систем на уровне ОС
- Аудит состояния систем с точки зрения безопасности

Модуль 4. Защита сервисов предприятия

- Методы защиты сервисов от вредоносных действий

Модуль 5. Защита сети предприятия

- Использование решений для пассивной и активной защиты периметра сети от сканирования и вторжений

Модуль 6. Использование VPN для соединения сетей филиалов предприятия и удаленных пользователей

- Варианты организации сетей VPN

5. 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.

6. 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 дополнительной профессиональной программы слушателей включает текущий контроль успеваемости, промежуточную и итоговую аттестацию.

Промежуточная аттестация по данному курсу проводится в форме выполнения практических работ и устного опроса, к итоговой аттестации допускаются слушатели, выполнившие все практические работы.

Результаты итоговой аттестации слушателей ДПП в соответствии с формой итоговой аттестации, установленной учебным планом, выставляются по двух бальной шкале («зачтено»/«не зачтено»), правильное выполнение не менее 80% заданий – «зачтено».

Слушателям, успешно освоившим дополнительную профессиональную программу и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации.

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

Итоговая аттестация проводится по форме выполнения задания в соответствии с учебным планом. Результаты итоговой аттестации заносятся в соответствующие документы.

7. <u>Промежуточная аттестация:</u>

№п/п	***Тематика практического занятия***	***Форма ПА***
Модуль 1.	**Лабораторные работы: Настройка стенда.** • Настройка шлюза для подключения сети предприятия к Internet • Развертывание сетей предприятия • Развертывание сервисов в соответствующих сетях	Лабораторная работа

	предприятия	
Модуль 2.	**Лабораторные работы: Использование сканеров безопасности** • Оценка безопасности систем и сервисов с помощью сканеров Nmap и Nessus • Оценка безопасности передаваемой по сети конфиденциальной информации с помощью сканера Ettercap	Лабораторная работа
Модуль 3.	**Лабораторные работы: Аудит состояния и защита систем от вредоносных действий пользователей и скомпроментированного ПО** • Аудит состояния систем с использованием штатных средств, пакета Tripwire и систем обнаружения rootkit • Защита систем на основе управления привилегиями процессов • Защита систем на основе механизмов мандатного доступа сервисов к объектам системы с использованием технологий MAC (FreeBSD) и AppArmor (Ubuntu) • Защита систем с использованием системного вызова Chroot для сервисов • Защита систем с использованием технологии изоляции сервисов в выделенном окружении Jail (FreeBSD) и LXC/OpenVZ (Ubuntu) • Использование технологии Linux PaX, grSecurity, SELinux и подобных, для защиты систем	Лабораторная работа
Модуль 4.	**Лабораторные работы: Защита сервисов предприятия развернутых в начале курса** • 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 • Защита информации компании с использованием шифрования блочных устройств (шифрование дисков) • Защита конфиденциальной информации передаваемой сервисам с использованием протоколов SSL/TLS • Использование PKI для управления	Лабораторная работа

	идентификацией и повышения конфиденциальности пользователей • Использование сервис ориентированных решений для защиты, на примере сервера DHCP	
Модуль 5.	**Лабораторные работы: Усиление защиты периметра сети предприятия развернутой в начале курса** • Использование возможностей пакетных фильтров для активной защиты периметра сети • Использование систем обнаружения вторжений (IDS) Snort для предупреждения о попытках вторжения • Использование решения защиты от вторжений (IPS) Snort/Snortsam для активной защиты периметра сети	Лабораторная работа
Модуль 6.	**Лабораторные работы: Предоставление доступа к внутренним ресурсам компании** • Использование протокола SSH для организации VPN • Использование Proxy сервера Squid для организации WebVPN • OpenVPN для организации VPN	Лабораторная работа

8. Итоговая аттестация (выполнение заданий):

Модуль 1. Развертывание сети и сервисов предприятия

Теория

- Информационная безопасность
- STRIDE is a system developed by Microsoft for thinking about computer security threats
- Demilitarized Zone — демилитаризованная зона, ДМЗ

Лабораторные работы

Сценарий: 192.168.X/24 - «белая» DMZ сеть, 192.168.100+X - «серая» LAN сеть

```
route -p add 192.168.0.0 mask 255.255.0.0 10.N.M.252
```

1.1 Настройка систем Gate и Сервер

- Настройка стендов слушателей
- Адаптер 3 - Виртуальный адаптер хоста (eth2/em2)
- Подключаемся putty к server и gate к адресам 192.168.X.Y

Debian/Ubuntu

```
root@gate:~# cat /etc/network/interfaces

...

auto eth2

iface eth2 inet static

        address 192.168.100+X.1

        netmask 255.255.255.0
```

FreeBSD

```
# cat /etc/rc.conf

...

ifconfig_em2="192.168.100+X.1/24"

...
```

1.2 Настройка системы Lan

- 64 бита для Docker
- Общие файлы конфигурации

Debian/Ubuntu

```
root@localhost:~# cat /etc/hostname

lan.corpX.un

root@localhost:~# cat /etc/network/interfaces

auto lo

iface lo inet loopback



auto eth0

iface eth0 inet static
```

```
        address 192.168.100+X.10

        netmask 255.255.255.0

        gateway 192.168.100+X.1

root@localhost:~# init 6
```

FreeBSD

```
# cat /etc/rc.conf

hostname="lan.corpX.un"

ifconfig_em0="192.168.100+X.10/24"

defaultrouter=192.168.100+X.1



keyrate="fast"

sshd_enable=yes

# init 6
```

1.3 Подключение сети предприятия к Internet

- Назначаем host системе на интерфейсе «VirtualBox Host-Only Network» ip address 192.168.100+X.20/24 и подключаемся putty к lan
- Настраиваем доступ в Internet из сети LAN (Трансляция на основе адреса отправителя)
- Тестируем

```
lan# apt update



lan# pkg update -f



lan# pkg install pkg
```

- Копируем ключи ssh с системы lan на gate и server (Аутентификация с использованием ключей ssh)

1.4 План размещения сервисов в сети предприятия

Сервис DNS

Уже развернут у провайдера

Сервис EMAIL

Будет развернут на системе server

Сервис DHCP

Разворачиваем на системе gate в сети LAN (можно не разворачивать, назначив клиенту 101-й адрес статически)

- Сервис DHCP Установка
- Сервис DHCP Стандартная настройка (поправить интерфейс, сеть и DNS)
- Проверка конфигурации и запуск
- Запуск системы client1

Файловый сервис

Будет развернут на системе lan

Сервис WWW

Сценарий: внешний корпоративный сайт на server

- Сервис INETD
- Web сервер на shell

Модуль 2. Анализ информационных систем предприятия с точки зрения безопасности

Теория

- Аудит информационной безопасности
- Nmap
- Kali Linux - Advanced Penetration Testing Linux Distribution
- OpenVAS
- Видео урок: Аудит системных событий в Linux/FreeBSD

Лабораторные работы

2.1 Сканеры безопасности систем

Сценарий: сканирование портов сервисов системы server, находим web сервер

- Утилита nmap

Сценарий: определяем «вручную» нет ли уязвимости directory traversal

```
gate.isp.un$ curl --path-as-is http://server.corpX.un/../../../etc/passwd



gate.isp.un$ fetch -o - http://server.corpX.un/../../../etc/passwd
```

```
gate.isp.un$ telnet server.corpX.un 80

GET /../../../etc/passwd HTTP/1.1



GET /../../../etc/shadow HTTP/1.1



GET /../../../etc/master.passwd HTTP/1.1
```

Сценарий: автоматизированный поиск уязвимостей

- Сервис OpenVAS (https://openvas.isp.un/)

2.2 Сканеры безопасности сети

Сценарий: перехват учетных данных при обновлении пользователем user1 веб информации на server по протоколу ftp

- Управление учетными записями в Linux, Управление учетными записями в FreeBSD
- Сервер ftp
- Утилита ettercap
- tcpdump

2.3 Аудит систем

Проверка стойкости паролей

- John the Ripper password cracker
- An online password cracking service
- Утилита john

Проверка целостности системы

Сценарий: находим модифицированное ПО (можно изменить код web сервера)

- Утилита tripwire
- Видео Урок: Tripware - мониторинг и предупреждения об изменениях файлов в системе

Проверка системы на наличие закладок

- Безопасность сервера FreeBSD: проверка на rootkit
- Scanning CentOS 7 Server for Malware
- Утилита rkhunter (В Debian: не работает, устанавливает exim)
- Утилита chkrootkit

Аудит системных событий

Сценарий: фиксируем обращения к файлам базы данных учетных записей со стороны процессов с EUID=user1. Можно тестировать из shell или запустить www сервер на server с правами user1

- Система FreeBSD Audit
- Система Linux Auditing
- Видео урок: Аудит системных событий в Linux/FreeBSD

Модуль 3. Защита систем предприятия

Теория

- Гугл для хакера
- Computer Security Resource Center National Vulnerability Database Keyword Search: Apache 2.4.18
- Вызов Chroot
- Песочница безопасность
- Handbook: Защита FreeBSD
- OpenBSD - ОС ориентированная на безопасность
- Переполнение буфера
- Выход из Chroot
- GRSecurity
- Hardened Gentoo

Лабораторные работы

3.1 Обновление систем

- Управление ПО в Linux
- Обновление системы и базового ПО в FreeBSD
- Обновление дополнительного ПО в FreeBSD

3.2 Управление привилегиями сервисов

Система безопасности UNIX

Сценарий: Запуск www сервера с правами пользователя user1 не позволит получить через него доступ к /etc/shadow (linux) или /etc/master.passwd (freebsd)

- Система безопасности UNIX
- Сервис INETD

POSIX ACL

Сценарий: с помощью POSIX ACL запрещаем пользователю user1 читать файл /etc/passwd

- POSIX ACL

3.3 Изоляция сервисов

Модули Linux LSM и FreeBSD MAC

Сценарий: ограничения, накладываемые политиками на www сервер на server не позволят получить через него доступ к любым файлам, кроме разрешенных даже в случае запуска его с правами root

- Модуль AppArmor

- Модули MAC
- Модуль SELinux
- Видео Урок: FreeBSD MAC and Linux AppArmor

Изоляция сервисов в файловой системе

Сценарий: запуск www сервера на server в chroot позволит получить через него доступ только к файлам, которые мы скопировали в chroot окружение

- Команда chroot

Изоляция сервисов в выделенном окружении

Сценарий: переносим www хостинг в контейнер

- Технология jail
- Технология namespaces
- Технология cgroup
- Технология LXC
- Установка и запуск сервера Apache на www
- Технология Docker (Разворачивать на lan, поскольку правила, добавленные docker-ce в netfilter блокируют LXC подключенный к bridge)
- Linux (Перемещение учетных записей), FreeBSD (Перемещение учетных записей)

3.4 Усиление системы с помощью специальных средств

- Linux Hardened
- Видео урок: Использование GRSecurity

Модуль 4. Защита сервисов предприятия

Теория

- Шифрование
- Криптосистема с открытым ключом
- Центр сертификации
- Аутентификация
- Privacy-enhanced Electronic Mail

Лабораторные работы

4.1 Ограничения учетных записей пользователей сервисов

Сценарий: разворачиваем на server, MTA для домена server.corpX.un, IMAP без SSL. Учетные записи почтовых пользователей не должны иметь shell, предоставляющий командную строку

- Настройка MTA
- Управление учетными записями в Linux, Управление учетными записями в FreeBSD
- UA mail
- Сервер dovecot
- В linux (Изменение атрибутов учетной записи)
- В freebsd (Изменение атрибутов учетной записи)

4.2 Скрытие баннеров сервисов

Сценарий: заменяем банеры сервисов SMTP, IMAP, FTP, HTTP, CIFS, SSH

- Сервис SMTP (Сокрытие названия сервиса)
- Сервис IMAP (Сокрытие названия сервиса)
- Сервис FTP (Сокрытие названия/версии сервиса)
- Сервис HTTP (Сокрытие версии сервиса)

```
gate# curl -I http://www.corpX.un/
```

- Сервис CIFS (Публичный каталог доступный на запись, Сокрытие названия/версии сервиса)
- Сервис SSH (OpenSSH Hide Version Number From Clients)

4.3 Замена устаревших сервисов

Сценарий: для хостинга на www используем SFTP вместо FTP

- SSH вместо FTP (SFTP)
- Использование домашних каталогов

Сценарий: защита web сервера от DoS атак (демонстрирует преподаватель на CentOS вместе с SElinux)

- Сервис XINETD

4.4 Шифрование трафика

Подготовка стенда

- Локализация временной зоны
- Сервис NTP для FreeBSD систем gate, server, lan

Использование самоподписанных цифровых сертификатов

Сценарий: замена сервиса HTTP на HTTPS на server (демонстрирует преподаватель)

- Использование алгоритмов с открытым ключем
- Создание самоподписанного сертификата для системы server
- Поддержка протокола HTTPS для системы server

Использование PKI

Сценарий:

1. развертывание корпоративного CA (на lan)
2. замена HTTP на HTTPS (на www)
3. замена IMAP на IMAPS (на server)
4. в client-ах добавляем сертификат CA в корневые центры сертификации

- Установка и запуск сервера Apache на lan
- Создание центра сертификации на lan (удалить index.html)
- Создание сертификата сервиса, подписанного CA для www
- Поддержка протокола HTTPS для www
- Использование сертификатов для шифрования трафика IMAPS на server (демонстрирует преподаватель)

4.5 Аутентификация и Авторизация доступа к сервису

- Управление идентификацией в сетях UNIX и Windows
- Видео урок: Использование одноразовых паролей OPIE
- Видео урок: SSH SSO

Задание: создание пользовательских сертификатов

- Создание пользовательского сертификата, подписанного CA
- Оформление сертификата и ключа в формате PKS#12 с парольной защитой

```
lan# cp user* /disk2/



lan# chown -R games /disk2
```

Сценарий: использование пользовательских сертификатов на server и для электронной подписи

- Thunderbird (подделку писем удобнее показать в старой версии)

Сценарий: использование пользовательских сертификатов для доступа по https на www

- Управление доступом к HTTP серверу на основе сертификатов
- Использование директивы Redirect
- CGI интерфейс сервера

Сценарий: использование пользовательских сертификатов для доступа по imaps на server

- Аутентификация на основе пользовательских сертификатов в протоколе IMAP

4.6 Ограничение доступа к сетевым сервисам

Статичное, с использованием специальных средств

Сценарий: разрешаем подключение к gate только из DMZ

- Сервис Tcpwrap

Статичное, с использованием средств встроенных в сервис

- Публичный каталог доступный на запись
- Ограничение доступа к DNS серверу
- Настройка MTA на релеинг почты из LAN
- Управление доступом к HTTP серверу на основе сетевых адресов
- Установка, настройка и запуск пакета SQUID

Адаптивное, с использование специальных средств

- Защита почты от вирусов и SPAMa
- Антивирусная защита web трафика SQUID

Сценарий: препятствуем попыткам сканирования системы server

- Сервис Portsentry
- Видео урок: Honeypot из tcpwrap и portsentry

Сценарий: блокируем атаки на сервис SSH на server

- Сервис Fail2ban

4.7 Шифрование контента

Сценарий: размещаем данные пользователей на шифрованном разделе для сервера SAMBA

- Создаем раздел, без файловой системы (Добавление дисков в Linux, Добавление дисков в FreeBSD)
- Использование шифрованных разделов в Linux, Использование шифрованных разделов в FreeBSD
- Установка сервера SAMBA
- Публичный каталог доступный на запись
- Убираем сервисы smbd и nmbd из автозагрузки (Управление сервисами в Linux, Управление сервисами в FreeBSD)

4.8 Специальные решения

Сценарий: защита LAN от посторонних сервисов DHCP

- DHCP, TFTP, DNS, SNTP и Syslog для Windows
- DHCP snooping
- Поиск и подавление посторонних DHCP серверов

Модуль 5. Защита сети предприятия

Теория

- Межсетевой экран
- еще один способ блокировать ssh bruteforce роботов
- Система обнаружения вторжений
- Система предотвращения вторжений

Лабораторные работы

5.1 Пакетные фильтры

Сценарий: защита сервиса ssh на server от bruteforce

- Конфигурация для защиты от bruteforce (атакуем server через putty с host системы)

5.2 Системы IDS и IPS

Сценарий: фиксируем атаки на server из WAN, проверять с gate.isp.un

- Сервис SNORT на gate (указать правильный интерфейс)

Сценарий: блокируем атаки на server из WAN, проверять с client1, переместив его в WAN (демонстрирует преподаватель на FreeBSD)

- Сервис SNORTSAM
- Сервис BARNYARD2
- Интеграция fail2ban и snort

Модуль 6. Использование VPN для соединения сетей филиалов предприятия и удаленных пользователей

Теория

- Virtual Private Network — виртуальная частная сеть

Лабораторные работы

6.1 Использование сервиса SSH

SSH вместо VPN (привязка к порту клиента)

Сценарий: Отключаем на host системе VirtualBox Host-Only Network адаптер и, используя доступность LAN с server, осуществляем доступ по HTTP в систему LAN через учетную запись user1 системы server

- Добавляем учетную запись user1 в linux (Добавление учетной записи), в freebsd (Добавление учетной записи)
- SSH вместо VPN (привязка к порту клиента)

SSH вместо VPN (привязка к порту сервера)

Сценарий: отключаем доступность LAN с server (и других систем, имеющих туда маршрут), осуществляем доступ по RDP в сеть LAN через учетную запись user1 системы server с использованием ssh соединения между lan и server

- Настройка Firewall (Конфигурация для шлюза WAN - LAN - DMZ)
- Назначаем host системе на интерфейсе «VirtualBox Host-Only Network» ip address 192.168.100+X.20/24 и подключаемся putty к lan
- SSH вместо VPN (привязка к порту сервера), использовать Bitvise SSH Client (Tunnelier)

6.2 Пакет OpenVPN

Сценарий: требуется предоставить авторизованный доступ внешних пользователей к любым LAN сервисам компании, например - CIFS

- Инициализация списка отозванных сертификатов

```
lan# scp /etc/ssl/openssl.cnf gate:/etc/ssl/



lan# scp /var/www/html/ca.crt gate:



lan# scp /var/www/html/ca.crl gate:
```

- Создание сертификата сервиса, подписанного CA для gate
- Пакет OpenVPN
- Настройка client/server конфигурации
- Отзыв сертификатов

Сценарий: требуется объединить сети филиалов

- Пакет OpenVPN
- Настройка peer2peer конфигурации