Тестовое задание для диагностического тестирования по дисциплине:

Безопасность сетевых технологий, 3 семестр

Код, направление подготовки	11.04.02. Инфокоммуникационные технологии и системы связи
Направленность (профиль)	Корпоративные инфокоммуникационные системы и сети
Форма обучения	Очная
Кафедра-разработчик	Радиоэлектроники и электроэнергетики
Выпускающая кафедра	Радиоэлектроники и электроэнергетики

№№ пп	Проверяемая компетенция	Задание	Варианты ответов	Тип сложности вопроса
1.	**ПК-1, ПК-2, ПК-3, ПК-4**	Какое из перечисленных средств применяется для диагностики уязвимостей серверов?	1) Access Control List 2) Сканер XSpider 3) Intrusion Detection System 4) SNMP-сервер 5) Межсетевой экран	**низкий**
2.	**ПК-1, ПК-2, ПК-3, ПК-4**	Вы настраиваете на сервере службу синхронизации времени с серверами точного времени в Интернете по протоколу NTP и обнаруживаете, что запросы не пропускаются наружу межсетевым экраном. Какие изменения необходимо внести в настройку межсетевого экрана для обеспечения работоспособности службы синхронизации времени?	1) Разрешить исходящие пакеты на 123 порт UDP 2) Разрешить исходящие пакеты на 119 порт TCP 3) Разрешить исходящие пакеты на 161 порт UDP 4) Разрешить исходящие пакеты на 110 порт TCP 5) Разрешить исходящие пакеты на 79 порт UDP	**низкий**
3.	**ПК-1, ПК-2, ПК-3, ПК-4**	Какое из приведенных ниже утверждений о приватных адресах является ложным?	1) Приватные адреса могут быть свободно использованы в любой	**низкий**

			локальной сети 2) FTP-сервер с приватным адресом может быть доступен из Интернет только в пассивном режиме 3) Пакеты с приватными адресами не пропускаются маршрутизаторами 4) WEB-сервер с приватным адресом может быть доступен из Интернет 5) SMTP-сервер с приватным адресом может быть доступен из Интернет	
4.	**ПК-1, ПК-2, ПК-3, ПК-4**	Межсетевой экран зарегистрировал большое число приходящих из Интернета SYN пакетов с IP-адресом источника из Вашей сети. Какому из перечисленных типов атак подверглась ваша сеть?	1) Land 2) TearDrop 3) Smurf 4) SYN flood 5) Brute force	**низкий**
5.	**ПК-1, ПК-2, ПК-3, ПК-4**	Какая из перечисленных утилит Unix для решения разнообразных проблем, связанных с TCP/IP, позволяет захватывать проходящие через сетевой интерфейс пакеты, выделять из них по определенным правилам только интересующие в данный момент и выводить их на экран либо записывать в файл для последующего анализа?	1) net view 2) netstat 3) tcpdump 4) nbtstat 5) trafshow	**низкий**
6.	**ПК-1, ПК-2, ПК-3, ПК-4**	Какой способ защиты из перечисленных следует применить для защиты от атаки Ping flood из Интернета?	1) Запретить на межсетевом экране прохождение UDP пакетов 2) Ограничить очередь ICMP пакетов 3) Удалить на клиентских компьютерах файл ping.exe 4) Запретить на межсетевом экране прохождение пакетов с адресом источника равным адресу приемника 5) Запретить выполнение команды ping непривилегированным пользователям	**средний**

7.	**ПК-1, ПК-2, ПК-3, ПК-4**	Ваш сервер был подвергнут smurf атаке. Какие изменения необходимо внести в конфигурацию межсетевого экрана для защиты сервера от атак подобного типа?	1) Запретить прохождение пакетов с установленным флагом SYN 2) Запретить прохождение пакетов с одновременно установленными флагами FIN и SYN 3) Запретить прохождение широковещательных ICMP запросов 4) Запретить прохождение фрагментированных пакетов 5) Ограничить очередь пакетов с установленным флагом SYN	**средний**
8.	**ПК-1, ПК-2, ПК-3, ПК-4**	Ваш сервер был подвергнут Land атаке из Интернета. Какие изменения необходимо внести в конфигурацию межсетевого экрана для защиты от атак подобного типа?	1) Запретить прохождение широковещательных ICMP пакетов 2) Запретить прохождение пакетов с одновременно установленными флагами SYN и ACK 3) Запретить прохождение пакетов из Интернета с адресом источника из вашей сети 4) Запретить прохождение пакетов с одновременно установленными флагами SYN и FIN 5) Запретить прохождение широковещательных UDP пакетов	**средний**
9.	**ПК-1, ПК-2, ПК-3, ПК-4**	Ваш DNS сервер подвергся атаке из сети 172.36.0.0/16. Какие изменения необходимо внести в файл named.conf, чтобы запретить обработку DNS запросов из этой сети?	1) options blackhole 172.36.0.0/16; 2) options deny-query 172.36.0.0/16; 3) options forwarders 172.36.0.0/16; 4) options query-source 172.36.0.0/16; 5) options transfer-source 172.36.0.0/16;	**средний**

10.	**ПК-1, ПК-2, ПК-3, ПК-4**	Связь между локальными сетями головного офиса и филиала компании организована посредством Интернет. Злоумышленник прослушивает проходящие пакеты на маршрутизаторе провайдера с целью сбора конфиденциальной информации. Какие меры необходимо предпринять системному администратору для защиты от данного вида атаки?	1) Задействовать IDS (Intrusion Detection System) 2) Активировать EFS (Encrypted File System) 3) Использовать маршрутизацию от источника для обхода маршрутизатора злоумышленника 4) При помощи межсетевого экрана заблокировать все порты, кроме 80 и 8080 5) Настроить VPN - соединение между головным офисом и филиалом	**средний**
11.	**ПК-1, ПК-2, ПК-3, ПК-4**	Ваш веб-сервер был подвергнут DoS - атаке. Выполнив на сервере команду netstat, Вы обнаруживаете большое число TCP соединений в состоянии SYN_RECV. Какому из перечисленных типов атак был подвергнут сервер?	1) Переполнение буфера 2) Brute force 3) Syn flood 4) Фрагментация пакетов 5) Smurf	**средний**
12.	**ПК-1, ПК-2, ПК-3, ПК-4**	Необходимо настроить межсетевой экран таким образом, чтобы разрешить доступ из Интернета к вашему DNS серверу для передачи зоны на вторичный DNS сервер. Какие изменения необходимо внести в конфигурацию межсетевого экрана для выполнения поставленной задачи?	1) Разрешить прохождение пакетов на TCP порт23 2) Разрешить прохождение пакетов на TCP порт 53 3) Разрешить прохождение пакетов на TCP порт 113 4) Разрешить прохождение пакетов на UDP порт 53 5) Разрешить прохождение пакетов на IP порт 23	**средний**
13.	**ПК-1, ПК-2, ПК-3, ПК-4**	Межсетевой экран, установленный на сервере, зарегистрировал большое количество широковещательных ICMP запросов. Какому из перечисленных типов атак был подвергнут сервер?	1) smurf 2) SYN flood 3) Скрытое сканирование портов 4) Brute Force 5) Buffer Overflow	**средний**
14.	**ПК-1, ПК-2, ПК-3, ПК-4**	Межсетевой экран, установленный на сервере, зарегистрировал большое число пакетов с одновременно установленными флагами SYN и FIN. Какое из утверждений относительно данной ситуации	1) Сервер подвергся SYN flood атаке 2) Сервер функционирует в обычном режиме 3) Сервер подвергся скрытому	**средний**

		является верным?	сканированию портов 4) Сервер подвергся Brute Force атаке 5) Сервер подвергся smurf атаке	
15.	**ПК-1, ПК-2, ПК-3, ПК-4**	Что произойдет, если у межсетевого экрана прикладного уровня будут отсутствовать модули для работы с каким-либо протоколом?	1) трафик по этому протоколу будет проходить без фильтрации 2) трафик по протоколу не пройдет 3) будет использоваться другой протокол	**средний**
16.	**ПК-1, ПК-2, ПК-3, ПК-4**	Необходимо запретить доступ к консоли сервера локальной сети извне. Какие изменения необходимо внести в настройку межсетевого экрана для решения поставленной задачи?	1) Запретить входящие пакеты на порты 137-139 TCP и UDP 2) Запретить входящие пакеты на порты 22 и 23 TCP 3) Запретить входящие пакеты на порт 21 TCP 4) Запретить входящие пакеты на порт 25 TCP 5) Запретить входящие пакеты на порт 389 TCP и UDP	**высокий**

17.	**ПК-1, ПК-2, ПК-3, ПК-4**	`zone "domain.ru" in {`
		`type master;`
		`file "domain.ru";`
		`};`
		Из соображений безопасности необходимо запретить передачу зоны domain.ru на любые сервера, кроме вторичного DNS сервера с IP-адресом 192.168.0.1.
		Какая из строк, помещаемая в блок описания зоны файла named.conf, позволит решить поставленную задачу?
			1) allow-query 192.168.0.1;
			2) allow-transfer 192.168.0.1;
			3) forwarders 192.168.0.1;
			4) allow-update 192.168.0.1;
			5) transfers-out 192.168.0.1;
				высокий

18.	**ПК-1, ПК-2, ПК-3, ПК-4**	Если web-сервер компании расположен между двумя экранами, первый отделяет его от внутренней сети, а второй от внешней, то через сколько экранов пойдет запрос сотрудника компании к внешнему web-серверу?	1) 2 2) 1 3) 0	**высокий**
19.	**ПК-1, ПК-2, ПК-3, ПК-4**	Что необходимо сделать злоумышленнику чтобы украсть данные передаваемые по VPN соединению?	1) захватить весь сеанс соединения 2) захватить часть передаваемых данных 3) иметь большие вычислительные мощности для дешифровки трафика	**высокий**

			4) просто подключиться к соединению VPN	
20.	**ПК-1, ПК-2, ПК-3, ПК-4**	Какой тип атаки был использован Кевином Митником для проникновения в Центр суперкомпьютеров в Сан-Диего?	1) имитация IP-адреса 2) перенаправление трафика 3) переполнение буфера	**высокий**