

УТВЕРЖДАЮ

Начальник 27 кафедры

ПОЛКОВНИК

С. Войцеховский

« ____ » _____ 2022 г.

Практическое занятие № 10

по учебной дисциплине

«Защита информации»

на тему:

«Работа с средством анализа защищённости XSpider»

Рассмотрено и одобрено

на заседании кафедры № 27

« ____ » _____ 202_ г. протокол № ____

Санкт-Петербург
2022

I. ТЕМА И ЦЕЛЬ ПРАКТИЧЕСКОГО ЗАНЯТИЯ

Тема практического занятия: «Работа с средством анализа защищённости XSpider».

Учебная цель:

выработать практические умения и приобрести практические навыки по:
осуществлению поиска и обнаружения уязвимостей АС.
составлению отчёта о результатах сканирования.

Время - 180 мин.

Место – аудитория (класс) по расписанию занятий.

Учебно-материальное и методическое обеспечение

1. Лабораторные установки – персональные ЭВМ с установленным на них программным обеспечением.
2. Электронный практикум по ЗИ.
3. Учебно-методические материалы.

II. УЧЕБНЫЕ ВОПРОСЫ И РАСЧЕТ ВРЕМЕНИ

№ п\п	Учебные вопросы	Время, мин.
1.	Вступительная часть. Контрольный опрос.	10
2.	Учебные вопросы. ОСНОВНАЯ ЧАСТЬ: 1. Работа со сканером безопасности «XSPIDER». 2. Работа с CGI сканером «XSPIDER». 3. Работа с TCP сервисами «XSPIDER». 4. Перенаправление данных через TCP порт «XSPIDER». 5. Работа с UDP датаграммами IP пакетами «XSPIDER». 6. Составление отчёта о ходе выполнения предыдущих заданий и его защита.	 25 25 25 25 25 55
3.	Заключительная часть. Задание и методические указания курсантам на самостоятельную подготовку	5

III. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПРЕПОДАВАТЕЛЮ ПРИ ПРОВЕДЕНИИ ПРАКТИЧЕСКОГО ЗАНЯТИЯ

Во вступительной части преподавателю объявить тему занятия, его цели, учебные вопросы, порядок его проведения, отметить практическую значимость для пользователя ПК знание антивирусной защиты, используемую литературу.

Проверку готовности слушателей к занятию осуществить проверкой наличия у них рабочих тетрадей, а также постановкой контрольных вопросов по знанию материала предыдущего группового занятия.

Отработку учебных вопросов осуществлять путем выполнения заданий, выдаваемых всей группе.

При отработке первого вопроса основное внимание обратить на приобретение курсантами первоначальных практических навыков в работе со сканером безопасности.

При отработке второго вопроса прививать практические навыки в самостоятельной работе с CGI сканером.

При отработке третьего вопроса прививать практические навыки в самостоятельной работе с TCP сканером.

При отработке четвертого вопроса прививать практические навыки в самостоятельной работе с TCP сканером при перенаправлении данных.

При отработке пятого вопроса прививать практические навыки в самостоятельной работе с UDP датаграммами IP пакетами.

В заключительной части занятия оценить работу учебной группы в целом, подвести итоги занятия, выставить оценки слушателям, ответить на возникшие вопросы. Сформулировать задание на самоподготовку и объявить тему следующего занятия.

III. УЧЕБНЫЕ МАТЕРИАЛЫ

Вступительная часть

Товарищи курсанты, целью сегодняшнего занятия является - приобретение первоначальных практических навыков работы со сканером безопасности «XSPIDER».

Итак, тема сегодняшнего практического занятия - " Работа с средством анализа защищённости XSpider".

Для достижения поставленных учебных целей вам требуется отработать шесть учебных вопросов занятия:

1. Работа со сканером безопасности «XSPIDER».
2. Работа с CGI сканером «XSPIDER».
3. Работа с TCP сервисами «XSPIDER».
4. Перенаправление данных через TCP порт «XSPIDER».
5. Работа с UDP датаграммами IP пакетами «XSPIDER».
6. Составление отчёта о ходе выполнения предыдущих заданий.

Порядок проведения занятия будет следующий - сначала вы ответите на ряд контрольных вопросов, что позволит оценить вашу теоретическую готовность к занятию, а затем в рамках рассматриваемых вопросов занятия

вы будете исполнять задания с использованием ПЭВМ. Ваша работа будет оцениваться на местах.

Контрольные вопросы до начала занятия.

Вопрос № 1: Какие средства анализа защищенности Вы знаете?

Вопрос № 2: Каков принцип работы средств анализа защищенности?

1. Задание на практическое занятие

1.1. Изучить п.4 настоящего задания.

1.2. Осуществить поиск уязвимостей на ПЭВМ в соответствии с п. 5 задания.

1.3. Составить отчет о результатах сканирования.

2. Подготовка к работе

Подготовка к работе проводится в часы самоподготовки. В ходе её каждый курсант обязан:

2.1. Изучить настоящее задание.

3. Выполнение работы

3.1. В классе ПЭВМ курсанты самостоятельно под руководством преподавателя выполняют п. 5 настоящего задания.

3.2. При выполнении работы задания выполняются последовательно.

3.3. В ходе практической работы запрещается вносить изменения, удалять или добавлять какие-либо компоненты, в настройки и параметры операционной системы.

4. Теоретические сведения

Общие сведения

Средство анализа защищённости XSpider 7.5

Вам предлагается выделить две задачи по обеспечению информационной безопасности, поскольку в известной мере ими можно заниматься независимо. Или не заниматься.

Задача, которая стоит перед всеми Информационно-Вычислительными Центрами, имеющими выход в глобальную Сеть, — это обеспечение защиты от внешних атак. Глобальный доступ к информации имеет обратную негативную сторону — канал связи с глобальным скопищем сетевых мерзавцев. От их атак никто не застрахован, но можно сделать все их атаки безуспешными.

Задача, которая стоит чаще всего перед специалистами по компьютерной безопасности достаточно больших (или достаточно серьезных) организаций — это обеспечение внутренней информационной безопасности. Она актуальна в том случае, когда часть сотрудников в определенных ситуациях и по отношению к определенным ресурсам рассматриваются как посторонние. Другими словами, когда внутри вашей сети не всем все можно. На самом деле, это актуально всегда, но подобной строгостью зачастую пренебрегают. Во многих случаях это проходит

относительно безболезненно, но надо всегда задумываться над вероятностью и степенью возможного ущерба.

Что нужно для внешней защиты

Тут возможны два варианта. Первый, наиболее распространенный, реализуется, если внутри сети организации нет публичных (доступных из Интернет) серверов, а локальные машины не имеют глобальных IP-адресов — используется технология типа NAT (Network Address Translation). В этом случае из внешнего мира получить прямую связь с компьютерами локальной сети невозможно, и они находятся вне досягаемости для посторонних. Но всегда имеется хотя бы один компьютер, который обеспечивает связь всей сети с внешним миром (шлюз), который обязан иметь внешний адрес и является потенциально уязвимым. Если его удастся "сломать", то не исключено, что после этого взломщик сможет получить доступ и к компьютерам внутренней сети. В этом случае все внимание надо сосредоточить на защите внешнего периметра сети, который в простейшем случае представлен единственным сервером.

Самое простое решение состоит из двух шагов: 1) установить и настроить должным образом на сервере сетевой экран (firewall) и 2) постоянно следить за уязвимостями на этом компьютере. Если это делать аккуратно, то можно чувствовать себя в безопасности. Обратите внимание на пункт 2, он является вторым только по порядку, но не по важности. Без его выполнения вся работа по пункту 1 может оказаться бесполезной. Чтобы так не случилось, как раз и стоит использовать сканер безопасности (об этом чуть позже).

Если в вашей сети имеются компьютеры с глобальными IP-адресами, то обеспечение безопасности становится более трудоемким — пристального внимания требуют все подобные хосты.

Что нужно для защиты внутренней

При необходимости обеспечить внутреннюю безопасность ситуация еще более усложняется. В предельном случае все внутренние компьютеры должны рассматриваться как потенциально уязвимые со всеми вытекающими последствиями: отслеживанием их конфигурации и постоянным мониторингом уязвимостей. К счастью, эту задачу, хороший сканер безопасности позволяет сильно упростить и в значительной степени автоматизировать.

Кроме того, тут сразу возникает еще как минимум пара задач: 1) создание грамотной архитектуры внутренней сети (кроме единовременного повышения защищенности она к тому же позволяет минимизировать усилия на дальнейшее обеспечение безопасности) и 2) разработка и соблюдение так называемой политики (или нескольких политик) безопасности, то есть набора правил, касающихся различных вопросов работы сети (создание и модификация паролей, регламент доступа к тем или иным ресурсам). Первый пункт можно сделать, что называется, "за раз", а вот вторым надо заниматься постоянно, и именно он оказывается, как правило, самым тяжелым —

главным образом, в организационном плане. Самое неприятное, что его реализацию невозможно в значительной степени автоматизировать.

Но, несмотря на то, что достичь идеально работающей архитектуры и политики безопасности достаточно трудно, можно построить сеть с очень высокой степенью защищенности. В этих обстоятельствах ключевым оказывается опять-таки постоянный мониторинг уязвимостей отдельных компьютеров. В принципе, даже далекая от идеала сеть, в которой каждый отдельный компьютер является неуязвимым, может рассматриваться как хорошо защищенная. Другими словами, грамотное решение задачи аудита сетевой безопасности (которая хорошо автоматизируется) позволяет в значительной степени компенсировать недоработки в тех областях, где решение проблем более трудоемко или затруднено по тем или иным причинам.

Особенности XSpider7

XSpider 7 сильно отличается от примитивного сканера сетевой безопасности, который просто выполняет сканирование и показывает результаты (приблизительно таким был XSpider версии 6.x, что не мешало ему занимать первые места в рейтингах благодаря отличному качеству работы сканирующего ядра).

Центральной концепцией XSpider 7 является "Задача". Она включает в себя прежде всего набор проверяемых хостов. В Задачу имеет смысл объединять хосты, которые следует проверять сходным образом (ничто не мешает иметь в Задаче и всего один хост). Как только Задача сформирована, ей можно присвоить Профиль — набор настроек, которые определяют нюансы сканирования. Если вы этого не сделаете, ничего страшного — будет использоваться Профиль по умолчанию. Самое приятное, что выполнение Задачи можно автоматизировать, то есть присвоить ей расписание, по которому она будет выполняться без вашего вмешательства. Кроме того, для каждой Задачи хранится полная история всех сканирований. Результаты любого из них вы можете загрузить и работать с ними, как со "свежими". Это удобно и для анализа развития ситуации, и для того, чтобы случайно не потерять какие-то результаты работы.

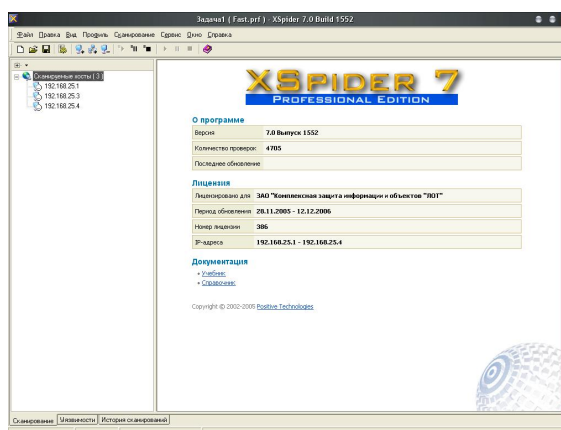


Рис 1. Задача

Когда создается рабочее окно XSpider — это окно текущей Задачи. Создание нового окна создает новую Задачу со стандартным именем, которое при сохранении Задачи лучше заменить на что-то более внятное. Задачи, как файлы, можно открывать, сохранять и т.п. Собственно, каждой Задаче и соответствует файл на диске, находящийся по умолчанию в стандартном каталоге XSpider (Tasks).

Одновременно XSpider 7 может обрабатывать много Задач, каждая из которых может содержать много хостов. Единственное, о чем вам при этом стоит беспокоиться — пропускная способность канала, связывающего XSpider с проверяемыми компьютерами. Скорость и надежность проверки может сильно падать, если канал перегружен. Учитывая, что трафик, создаваемый XSpider на один хост, невелик, то перегрузка канала возможна либо при очень большом (сотни) числе **ОДНОВРЕМЕННО** сканируемых хостов, либо, если канал очень узкий. Регулировать максимальное число проверяемых хостов на одну Задачу можно через настройки. То есть, даже если в Задаче, скажем, 100 хостов, вы можете указать, что одновременно должны сканироваться 50. При этом остальные будут стоять в очереди и проверяться последовательно.

По результату каждого сканирования XSpider может сгенерировать отчет, причем в автоматическом режиме они могут доставляться вам по email (или выкладываться на доступный сетевой диск). Если один раз потратить время на грамотную настройку режима автоматической работы, то потом достаточно будет только регулярно проверять свой почтовый ящик, чтобы отслеживать безопасность всей сети (или сетей).

Также заслуживают признания эвристические алгоритмы, использующиеся XSpider 7. Он не только занимается простым перебором уязвимостей из базы, но и выполняет дополнительный анализ по ходу работы, исходя из особенностей текущей ситуации. Благодаря этому, XSpider 7 может иногда обнаружить специфическую уязвимость, информация о которой еще не была опубликована. Хотя, конечно, случается это нечасто.

Пересканирование отдельных сервисов

После того как сканирование завершилось вы можете при необходимости провести повторное сканирование отдельных сервисов. Это может быть полезно в некоторых особых ситуациях, например, для подтверждения наличия DoS-уязвимости. Иногда, при плохом качестве связи с проверяемым хостом возможно ложное определение DoS-уязвимости (когда связь с хостом прервалась случайно, а XSpider сделал вывод, что прошла DoS-атака). В этом случае можно провести повторное сканирование соответствующего сервиса и при повторном обнаружении уязвимости более уверенно сделать вывод о ее наличии.


Сохранение результатов

Если сразу после завершения сканирования вы попытаетесь закрыть окно XSpider, то он выдаст диалог с предложением сохранить результаты. Конечно, это не то предложение, от которого вы не сможете отказаться, но сохранять результаты своего труда — это хорошая практика.

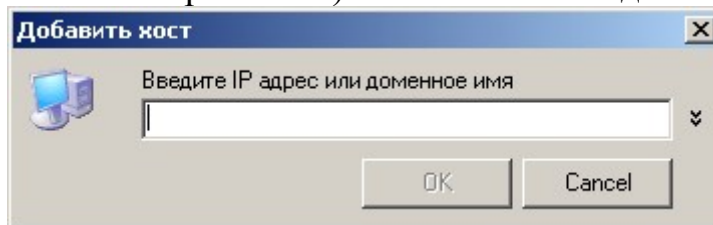
Результаты сохраняются в специальный файл задачи, который вы потом можете загружать, смотреть предыдущие результаты, создавать по ним отчеты и запускать новые сканирования для того же списка хостов.


IV.ЗАДАНИЯ И МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ИХ ВЫПОЛНЕНИЮ

Ход работы

 Сразу после запуска XSpider на экране появляется рабочее окно программы. В его тулбаре нажимаем кнопку (добавить хост) или нажимаем клавишу Insert или выполняем команду меню Правка/Добавить хост. В появившемся окне задаем IP-адрес (указанный в полученном задании). Введенный хост появится в списке слева.


Если нужно добавить несколько хостов, то ситуация усложняется ненамного. Как и прежде, нажимаем ту же кнопку тулбара (или Insert на клавиатуре, можно также через меню). В появившемся диалоге




 Если необходимо добавить целый диапазон хостов для сканирования, то проще всего воспользоваться специальной кнопкой (или командой меню Правка/Добавить диапазон). В этом случае, конечно, хосты нужно задавать в виде IP-адресов. Максимальный диапазон адресов ограничен сетью класса C (254 адреса):



Запуск сканирования

 Нажимаем кнопку тулбара "Сканирование всех хостов" или Ctrl+R на клавиатуре или выбираем соответствующую команду из меню Сканирование. Сканирование началось.

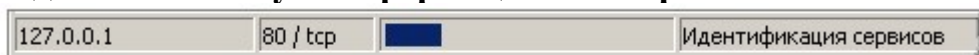
 Эта кнопка подразумевает сканирование одного или нескольких выделенных хостов.

Во время сканирования



В процессе сканирования каждый из сканируемых хостов отображается иконкой, обозначающей одно из нескольких состояний хоста: ожидающий проверки, проверяемый, приостановленный, прерванный.

Кроме того, по строке статуса в нижней части окна программы можно получить дополнительную информацию о выбранном хосте:



В строке указывается IP-адрес проверяемого хоста, текущий порт, общая степень завершенности и краткое текстовое описание текущей операции.

Наконец, о том, что имеется активное сканирование можно судить по анимированной иконке программы в правом нижнем углу экрана, если вы, конечно, не передвинули панель задач Windows в нестандартное место, как это делают некоторые эстеты (конечно, анимированная иконка будет и в этом случае, просто находиться она будет в другом углу).

Во время сканирования вы можете управлять как процессом в целом, так и отдельными хостами. Вы можете приостановить или прервать сканирование всех или некоторых выбранных хостов.



Приостановить сканирование можно при помощи кнопок "Приостановить все" и "Приостановить выделенные". В любой момент вы можете продолжить работу всех или некоторых из приостановленных процессов кнопками старта точно так же, как запускали сканирование. Сканирование в состоянии паузы рассматривается Xspider как активное. Например, если вы попытаетесь закрыть окно программы в момент, когда сканирование всех хостов приостановлено, то вам это не удастся и вы получите предупреждение о том, что сканирование не завершено.

У вас может возникнуть вопрос: а зачем вообще нужна возможность приостанавливать сканирование. В обычной ситуации это, как правило, не требуется, но может иногда оказаться удобным. Например, если вам стало известно, что один из хостов временно недоступен, то его сканирование можно приостановить и затем возобновить.



Иначе ведут себя кнопки прерывания сканирования. Они также останавливают сканирование на текущей стадии, но продолжить его уже нельзя — можно только начать с самого начала. При попытке повторно запустить сканирование вы получите предупреждение, что сканирование будет начато с нуля, а все "добытые" до этого данные по хосту (хостам) будут отброшены. Поэтому прежде чем выполнять вашу команду на прерывание XSpider всегда на всякий случай спрашивает подтверждения.

Прерывать сканирование имеет смысл, если вы решили, что уже получили всю интересующую вас информацию и дальнейшее сканирование бессмысленно.

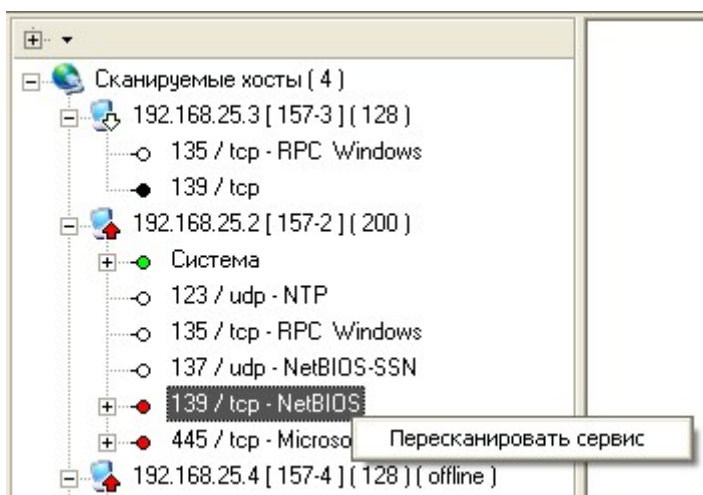
Подчеркнем еще раз, что при штатной организации аудита безопасности вам, как правило, не понадобится пользоваться командами приостановки и

прерывания сканирования — они могут потребоваться в нестандартных ситуациях.



И последнее замечание. Иногда процесс запуска, приостановки или прерывания сканирования может занять заметное время (до нескольких секунд). Это бывает при плохой связи или в случае очень медленного ответа хоста. В этих случаях вы можете успеть заметить небольшую красную стрелочку, которой помечается значок хоста. Она обозначает, что идет процесс смены режима, во время которого команды управления сканированием недоступны.

Пересканирование отдельных сервисов



После того как сканирование завершилось, вы можете при необходимости провести повторное сканирование отдельных сервисов. Для этого на требуемый сервис надо нажать правую клавишу мыши и выбрать команду «Пересканировать сервис».

Это может быть полезно в некоторых особых ситуациях, например, для подтверждения наличия DoS-уязвимости. Иногда, при плохом качестве связи с проверяемым хостом возможно ложное определение DoS-уязвимости (когда связь с хостом прервалась случайно, а XSpider сделал вывод, что прошла DoS-атака). В этом случае можно провести повторное сканирование соответствующего сервиса и при повторном обнаружении уязвимости более уверенно сделать вывод о ее наличии.

5. Поиск уязвимостей на ПЭВМ

Задание № 1.

Осуществить поиск уязвимостей на ПЭВМ с IP-адресом **192.168.25.1**, с помощью сканера безопасности «XSpider7.0». В ходе поиска уязвимостей создать Задачу (согласно терминологии касающейся данного сканера) и присвоить ей имя содержащее Фамилию старшего расчёта и номера учебной группы.

Во время поиска осуществить:

1. Сканирование хоста с указанным IP-адресом (используя стандартный профиль)
2. Пересканирование отдельных сервисов содержащих уязвимости
3. Создать собственный профиль, максимально оптимизированный для используемого типа локальной сети Вычислительных Машин.
4. Пересканировать указанную ПЭВМ используя созданный пользовательский профиль.

Задание № 2.

Осуществить поиск уязвимостей на ПЭВМ с IP-адресом **192.168.25.2**, с помощью сканера безопасности «XSpider7.0». В ходе поиска уязвимостей создать Задачу (согласно терминологии касающейся данного сканера) и присвоить ей имя содержащее Фамилию старшего расчёта и номера учебной группы.

Во время поиска осуществить:

1. Сканирование хоста с указанным IP-адресом (используя стандартный профиль)
2. Пересканирование отдельных сервисов содержащих уязвимости
3. Создать собственный профиль, максимально оптимизированный для используемого типа локальной сети Вычислительных Машин.
4. Пересканировать указанную ПЭВМ используя созданный пользовательский профиль.

Задание № 3.

Осуществить поиск уязвимостей на ПЭВМ с IP-адресом **192.168.25.3**, с помощью сканера безопасности «XSpider7.0». В ходе поиска уязвимостей создать Задачу (согласно терминологии касающейся данного сканера) и присвоить ей имя содержащее Фамилию старшего расчёта и номера учебной группы.

Во время поиска осуществить:

1. Сканирование хоста с указанным IP-адресом (используя стандартный профиль)
2. Пересканирование отдельных сервисов содержащих уязвимости
3. Создать собственный профиль, максимально оптимизированный для используемого типа локальной сети Вычислительных Машин.
4. Пересканировать указанную ПЭВМ используя созданный пользовательский профиль.

Задание № 4.

Осуществить поиск уязвимостей на ПЭВМ с IP-адресом **192.168.25.4**, с помощью сканера безопасности «XSpider7.0». В ходе поиска уязвимостей создать Задачу (согласно терминологии касающейся данного сканера) и присвоить ей имя содержащее Фамилию старшего расчёта и номера учебной группы.

Во время поиска осуществить:

1. Сканирование хоста с указанным IP-адресом (используя стандартный профиль)
2. Пересканирование отдельных сервисов содержащих уязвимости

3. Создать собственный профиль, максимально оптимизированный для используемого типа локальной сети Вычислительных Машин.

4. Пересканировать указанную ПЭВМ используя созданный пользовательский профиль.

Задание № 5.

Осуществить поиск уязвимостей на ПЭВМ с диапазоном IP-адресов **192.168.25.1-192.168.25.4**, с помощью сканера безопасности «XSpider7.0». В ходе поиска уязвимостей создать Задачу (согласно терминологии касающейся данного сканера) и присвоить ей имя содержащее Фамилию старшего расчёта и номера учебной группы.

Во время поиска осуществить:

1. Сканирование хостов с указанными IP-адресами (используя стандартный профиль)

2. Пересканирование отдельных сервисов содержащих уязвимости

3. Выбрать наиболее уязвимую машину из указанного диапазона (указать в отчёте)

4. Создать собственный профиль, максимально оптимизированный для используемого типа локальной сети Вычислительных Машин.

5. Пересканировать указанную наиболее уязвимую ПЭВМ используя созданный пользовательский профиль.

Задание № 6.

Осуществить поиск уязвимостей на ПЭВМ выполнив самосканирование. Для этого машине на которой выполняется работа, необходимо задать IP-адрес **192.168.25.1**. И с помощью сканера безопасности «XSpider7.0» выполнить сканирование данного адреса (можно с отключённым проводом локальной сети). В ходе поиска уязвимостей создать Задачу (согласно терминологии касающейся данного сканера) и присвоить ей имя содержащее Фамилию старшего расчёта и номера учебной группы.

Во время поиска осуществить:

1. Сканирование хоста с указанным IP-адресом (используя стандартный профиль)

2. Пересканирование отдельных сервисов содержащих уязвимости

3. Создать собственный профиль, выполняющий все базовые проверки и сканирование всего диапазона портов. Увеличить в 3 раза количество одновременно открываемых потоков по сравнению с профилем, используемым по умолчанию.

4. Пересканировать ПЭВМ используя созданный пользовательский профиль.

6. Отчетность по работе

По выполнению работы каждый курсант должен представить отчет. Отчет должен содержать:

- название практического занятия;
- текст индивидуального задания;
- цель работы;
- результаты проделанной работы;
- Выводы.

В процессе выполнения индивидуального задания или после завершения его выполнения преподаватель проводит собеседование с каждым курсантом по теме выполненной работы, проверяя также практические навыки, приобретенные в ходе занятия. Отчетный материал предоставляется преподавателю, а результаты защищаются.

7. Заключительная часть

В заключительной части подводятся итоги проделанной работы, дается краткая оценка действиям участников, прослеживается связь с теоретическими положениями и перспективой на будущую деятельность.

8.Задание и методические указания курсантам на самостоятельную подготовку:

1. Изучить по конспекту лекций систему контроля целостности Aide операционной системы MC BC 3.0.
2. Быть готовыми к настройке и работе с системой контроля целостности Aide в ОС MC BC 3.0.

V. ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. Эксплуатационный документ «Руководство пользователя XSpider», конспект лекций/
2. Информационная безопасность: – учебное пособие / В.М.Зима, СПб.: ВКА имени А.Ф.Можайского, 2017 с.
3. Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем. Ч.2. Сетевые ОС и принципы обеспечения информационной безопасности в сетях / С.И. Макаренко, А.А. Ковальский, С.А. Краснов СПб.: Научные технологии 2020.

Доцент 27 кафедры
к.т.н.
подполковник

С. Краснов

« ____ » _____ 20__ г.