



Кафедра информатики
и информационных технологий

Б1.О.22 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Лабораторные работы. Методы и средства защиты информации

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

Направление подготовки
09.03.03 Прикладная информатика

Квалификация (степень) выпускника
бакалавр

Уфа 2021

Рекомендовано к изданию методической комиссией экономического факультета (протокол № 8 от 25.03.2021 г.)

Составитель: доцент, к.ф.-м.н. Шамсутдинова Т.М.

Рецензент: ст. преподаватель Прокофьева С.В.

Ответственный за выпуск: зав. кафедрой ИИТ, д.т.н., Беляева А.С.

г.Уфа, БГАУ, Кафедра информатики и информационных технологий

СОДЕРЖАНИЕ

Лабораторная работа № 1

Компьютерные вирусы и противовирусная защита

Лабораторная работа № 2

Моделирование технической разведки по исходным данным для объекта информатизации

Лабораторная работа №3

Понятие дискреционной модели политики безопасности

Лабораторная работа №4

Количественная оценка стойкости парольной защиты

Лабораторная работа №5

Защита от копирования. Привязка к аппаратному обеспечению. Использование реестра

Лабораторная работа №6

Анализ безопасности систем с использованием сканеров уязвимостей

Лабораторная работа №7

Изучение механизмов работы и вариантов совместного применения межсетевого экрана и сетевого сканера на примере ПО Agnitum Outpost и XSpider

Библиографический список

Лабораторная работа № 1

Компьютерные вирусы и противовирусная защита

Цель работы: Освоение программных средств защиты персонального компьютера от вредоносных программ

Подготовка к выполнению работы: Используя интернет-источники, изучите теоретический материал о компьютерных вирусах. Данные систематизируйте в виде таблицы 1.

Таблица 1. Пример таблицы для включения в отчет

№ №	Название группы вирусов	Разновидности	Механизм порчи информации	Рекомендуемые средства защиты
1	Черви	1..... 2..... 3.....		
2	Трояны			
3	Баннеры			
4	Спам			
5	Фишинг			
6	Ложные антивирусы			
7	Потенциально нежелательные программы			
8	Spyware			

1

Ход работы:

1. Изучить установленное на компьютерах антивирусное программное обеспечение;
2. Произвести настройку антивирусного программного обеспечения;
3. Произвести выборочное сканирование файла;
4. Поместить любой файл в карантин;
5. Добавить планировщику задачу на запуск внешнего приложения;
6. Включить защиту электронной почты и доступа в интернет.
7. Заполнить таблицу 1 с описанием видов компьютерных вирусов.

Контрольные вопросы:

1. Какие основные признаки у зараженного вирусом компьютера?
2. Компьютер заразился вирусом, хотя антивирусное ПО установлено. В чем может быть причина?
3. Можно ли устанавливать больше одного антивируса на компьютер, почему?
4. Чем отличается сигнатурный метод защиты от эвристического, перечислите основные достоинства и недостатки каждого метода.
5. Опишите облачный метод защиты, перечислите преимущества и недостатки.
6. Какая ответственность предусмотрена законодательством РФ за распространение троянских или вредоносных программ?

Лабораторная работа № 2

Моделирование технической разведки по исходным данным для объекта информатизации

Цель работы: Приобрести практические навыки в определении степени защищенности объекта информатизации путем моделирования возможных действий технических разведок. Научиться определять потенциальные и реальные каналы утечки информации.

Теоретическая часть

Для того чтобы построить эффективную систему информационной безопасности, необходимо в первую очередь определить потенциальные и реальные угрозы технического проникновения на защищаемый объект, возможные каналы для несанкционированного доступа и утечки защищаемой информации.

Данная работа базируется на знании природы возникновения технических каналов утечки информации и методов ведения технической разведки. Правильное определение потенциальных угроз на предпроектном этапе построения системы защиты позволит в дальнейшем выбрать наиболее оптимальные меры и средства защиты.

При выявлении технических каналов утечки информации необходимо рассматривать всю совокупность элементов защиты, включающую основное оборудование технических средств обработки информации, соединительные линии, распределительные и коммутационные устройства, системы электропитания, системы вентиляции и т.п.

Наряду с основными техническими средствами, непосредственно связанными с обработкой и передачей конфиденциальной информации, необходимо учитывать и вспомогательные технические средства и системы (ВТСС), такие, как технические средства открытой телефонной, факсимильной, громкоговорящей связи, системы охранной и пожарной сигнализации, электрификации, радиофикации, часофикации, электробытовые приборы и др. Наибольшее внимание следует уделить вспомогательным средствам, имеющие линии, выходящие за пределы контролируемой зоны.

В качестве каналов утечки больше внимания следует уделить вспомогательным средствам, имеющим линии, выходящие за пределы контролируемой зоны, а также посторонним проводам и кабелям, проходящим через помещения, где установлены основные и вспомогательные технические средства, металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции.

При оценке защищенности помещений от утечки речевой информации необходимо учитывать возможность ее прослушивания, как из соседних помещений, так и с улицы. Следует проводить оценку возможности ведения разведки с использованием лазерных микрофонов. Интерес могут вызывать каналы утечки за

счет вибраций, возникающих под давлением акустических волн, в твердых телах (ограждениях, трубах и т.п.).

Оценка защищенности объекта включает в себя анализ режима работы и охраны объекта, с целью моделирования действий по скрытному проникновению на них (неконтролируемому пребыванию) посторонних лиц. Режим работы специалистов сторонних организаций, приобретение, установка и ремонт мебели, оргтехники и т.п. Т.е. всю совокупность условий, позволяющих внедрить на объект специальные закладные устройства перехвата информации (микропередатчики, возможность установки миниатюрных микрофонов с подключением к внешним линиям и т.д.). А также определение наиболее эффективных, для использования на разных уровнях проникновения, средств технической разведки.

Большое, а иногда решающее, значение при оценке угрозы может иметь знание наиболее вероятного противника, его финансовых и оперативных возможностей, знание личностных качеств постоянного персонала, временных работников и другая дополнительная информация.

Определение потенциальных и реальных ТКУИ

Ниже приведена примерная характеристика защищаемого объекта (исходные данные).

1. Защищаемое помещение расположено на четвертом этаже 7-этажного здания. Все здание принадлежит одной организации:
 - Сверху расположены служебные помещения.
 - Снизу расположены технические помещения (туалет, электрощитовая).
 - Со стороны стены Б расположена приемная.
 - Со стороны стены Г расположен общий коридор.Стороны А и В выходят на улицы с интенсивным пешеходным и транспортным движением. Окна помещения оборудованы шторами, смотрят на жилой дом, расположенный на расстоянии 30 метров.
2. Из мебели в помещении установлены рабочий и журнальный столы, стулья, подставки под: телефоны, ПЭВМ и телевизор.
3. Из основных технических средств в помещении установлен телефон внутренней конфиденциальной связи, ПЭВМ включенная в локальную сеть.
4. Из вспомогательных технических средств в помещении установлен телефон ГТС, телевизор, радиотрансляционный приемник. Помещение оборудовано системой пожарной и охранной сигнализации, линии которых выходят на пульт дежурного охранника. Помещение электрифицировано (освещение, питание оборудования).
5. Помещение оборудовано системой вытяжной вентиляции, короб которой проложен вдоль коридора и поднимается на крышу здания. Радиаторы отопления установлены вдоль стены А. Трубы отопления спускаются в подвал.

6. Режим работы учреждения предусматривает свободное передвижение сотрудников и посетителей в рабочее время. В ночное время помещение закрывается на ключ, сдается под охрану дежурному. Системы связи обслуживаются штатным сотрудником. Системы жизнеобеспечения (отопление, канализация) обслуживаются по заявке приходящим сотрудником.

7. Доступ штатных сотрудников к служебной информации не разграничен.

Схема объекта представлена на рис 1.

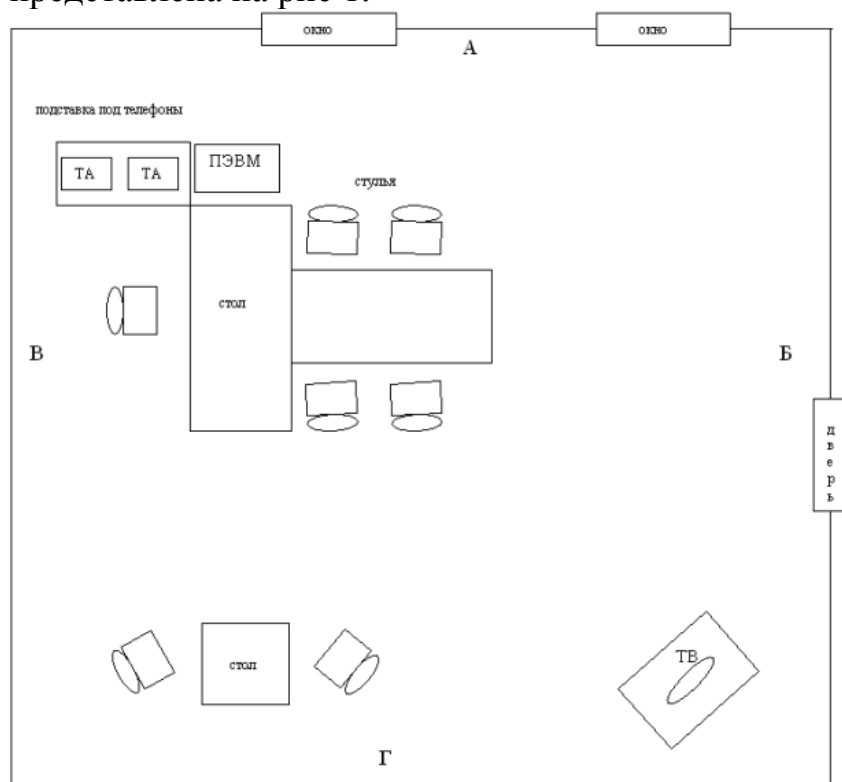


Рисунок 1. Схема объекта

В качестве примера представим порядок рассуждения защищенности объекта со стороны окон. При определении вероятности существования каналов утечки, в случае недостаточности исходных данных, допущено использование оговорок типа "если.... то....".

1. Просмотр помещения со стороны улицы, ввиду того, что помещение находится на 4 этаже, не возможен. Так как возможен просмотр помещения извне, со стороны жилого дома с помощью оптических приборов, существует потенциальный канал утечки видовой информации. Однако, если организационными мероприятиями (соответствующим инструктажем ответственных лиц) введено обязательное зашторивание окон во время проведения совещаний, работы с документами и т.п., то реального визуального оптического канала утечки информации нет. В качестве дополнительных мер можно ввести периодический контроль за соблюдением сотрудниками правила зашторивания, а также поставить тонированные или рифленые стекла.
2. Так как возможно прослушивание помещения, со стороны улицы и жилого дома, через открытые окна и форточки с помощью направленных микрофо-

нов, существует потенциальный канал утечки акустической информации. Однако, если организационными мероприятиями введено обязательное закрытие окон и форточек во время проведения совещаний, реального акустического канала утечки информации нет.

В качестве дополнительной меры можно установить кондиционер или приобрести генератор белого шума и включать его во время проведения совещаний.

В заключение первого этапа можно предложить установку стекол с рифленной поверхностью и кондиционера. Решение представляется оптимальным, т.к. акустический и визуально оптический каналы устраняются при минимальных финансовых затратах. Также, в дальнейшем, обеспечивается удобство эксплуатации объекта и исключается негативный человеческий фактор.

При оценке вероятности использования технической разведкой потенциальных каналов утечки информации следует принимать во внимание окружающую обстановку, с точки зрения возможности по организации и ведению технической разведки, а именно:

- скрытное размещение поста перехвата (для прослушивания и просмотра помещения) на улице с интенсивным движением затруднительно, т.к. подозрительные лица, транспортные средства и т.п. привлекают к себе внимание, легко визуально обнаруживаются;
- скрытное размещение поста перехвата (для прослушивания и просмотра помещения, установки лазерного микрофона) в жилом здании, если, например, арендовать квартиру с окнами расположенными напротив окон защищаемого помещения, вполне реализуемо.

Необходимо, если имеется такая возможность, проверить благонадежность (лояльность) жильцов в квартирах, потенциально пригодных для организации поста перехвата (сдаются ли квартиры, проживают ли в квартирах потенциальные конкуренты, имеются ли лица бывшие в конфликте с законом и т.п.). Возможно организации постов перехвата на технических этажах и т.п.

В случае получения в ходе проверки положительных данных можно заключить, что защитные мероприятия не требуются вообще. С точки зрения защиты от случайных утечек, например прослушивания, можно заключить, что улица с интенсивным автомобильным и пешеходным движением создает достаточно сильную акустическую помеху, за которой разговоры случайными прохожими различаться не будут. При необходимости в этом можно убедиться экспериментально.

В случае получения в ходе проверки отрицательных или неоднозначных данных оптимальным остается вариант указанный в заключение первого этапа.

Самостоятельная часть работы

В самостоятельной части работы предлагается:

- выявить оставшиеся, потенциально возможные каналы утечки информации (с учетом исходных данных, используя, при необходимости оговорки);
- смоделировать возможные действия технических разведок, определить реальные каналы утечки информации;
- доказать целесообразность и предложить проведение тех или иных защитных мероприятий.

Примечание: При определении вероятности существования каналов утечки, в случае недостаточности исходных данных, допускается использовать оговорку типа "если.... то....".

Контрольные вопросы:

- 1) Перечислите основные принципы организационной защиты информации, опишите их;
- 2) Какие виды структурных подразделений могут создаваться на предприятиях для организации работ по защите информации;
- 3) Какие технические средства используют для оценки защищенности выделенных помещений.
- 4) Дать определения понятий:
 - конфиденциальная информация;
 - канал утечки информации;
 - организационная защита;
 - вспомогательные технические средства и системы;
 - защищенность информации, несанкционированный доступ;
 - технические каналы утечки информации;
 - средства защиты информации.

Лабораторная работа № 3

Понятие дискреционной модели политики безопасности

Цель работы: ознакомиться с проблемами реализации политик безопасности в компьютерных системах на примере дискреционной модели.

Теоретические сведения

Под политикой безопасности понимают набор норм, правил и практических приемов, регулирующих управление, защиту и распределение ценной информации. Политика безопасности задает механизмы управления доступом к объекту, определяет как разрешенные, так и запрещенные доступы.

Политика безопасности реализуется посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты. Для конкретной организации политика безопасности должна носить индивидуальный характер и зависеть от конкретной технологии обработки информации и используемых программных и технических средств.

Политика безопасности определяется способом управления доступом, который задаёт порядок доступа к объектам системы. Различают два основных вида политики безопасности: избирательную и полномочную.

Избирательная политика безопасности основана на избирательном способе управления доступом. Избирательное (или дискреционное) управление доступом характеризуется заданным администратором множеством разрешенных отношений доступа (например, в виде троек объект – субъект – тип доступа). Обычно для описания свойств избирательного управления доступом применяют математическую модель на основе матрицы доступа.

Матрица доступа представляет собой матрицу, в которой столбец соответствует объекту системы, а строка – субъекту. На пересечении столбца и строки матрицы указывается тип разрешенного доступа субъекта к объекту. Обычно выделяют такие типы доступа субъекта к объекту, как «доступ на чтение», «доступ на запись», «доступ на исполнение» и т.п. Матрица доступа является самым простым подходом к моделированию систем управления доступом. Однако она служит основой для сложных моделей, более адекватно описывающих реальные автоматизированные системы обработки информации (АСОИ).

Избирательная политика безопасности широко применяется в АСОИ коммерческого сектора, так как её реализация соответствует требованиям коммерческих организаций по разграничению доступа и подотчетности, а также имеет приемлемую стоимость.

Полномочная политика безопасности основана на полномочном (мандатном) способе управления доступом. Полномочное (или мандатное) управление доступом характеризуется совокупностью правил предоставления доступа, определенных на множестве атрибутов безопасности субъектов и объектов, например, в зависимости от метки конфиденциальности информации и уровня допуска пользователя. Полномочное управление доступом подразумевает, что:

- 1) все субъекты и объекты системы однозначно идентифицированы;

2) каждому объекту системы присвоена метка конфиденциальности информации, определяющая ценность содержащейся в нем информации;

3) каждому субъекту системы присвоен определенный уровень допуска, определяющий максимальное значение метки конфиденциальности информации объектов, к которым субъект имеет доступ.

Чем важнее объект, тем выше его метка конфиденциальности. Поэтому наиболее защищенными оказываются объекты с наиболее высокими значениями метки конфиденциальности.

Основное назначение полномочной политики безопасности – регулирование доступа субъектов системы к объектам с различными уровнями конфиденциальности, предотвращение утечки информации с верхних уровней должностной иерархии на нижние, а также блокирование возможных проникновений с нижних уровней на верхние.

При выборе и реализации политики безопасности в компьютерной системе, как правило, работают следующие шаги:

1. В информационную структуру вносится структура ценностей (определяется ценность информации) и проводится анализ угроз и рисков для информации и информационного обмена.

2. Определяются правила использования для любого информационного процесса, права доступа к элементам информации с учетом данной оценки ценностей.

Реализация политики безопасности должна быть четко продумана. Результатом ошибочного или бездумного определения правил политики безопасности, как правило, является разрушение ценности информации без нарушения политики.

Дискреционная политика безопасности

Пусть O – множество объектов, U – множество пользователей, S – множество действий пользователей над объектами. Тогда дискреционная политика определяет отображение $O \rightarrow U$ (объектов на пользователей-субъектов). В соответствии с данным отображением, каждый объект $O_j \in O$ объявляется собственностью соответствующего пользователя $U_k \in U$, который может выполнять над ними определенную совокупность действий $S_i \in S$, в которую могут входить несколько элементарных действий (чтение, запись, модификация и т.д.). Пользователь, являющийся собственником объекта, иногда имеет право передавать часть или все права другим пользователям (обладание администраторскими правами).

Указанные права доступа пользователей-субъектов к объектам компьютерной системы записываются в виде так называемой матрицы доступа. На пересечении i -й строки и j -ого столбца данной матрицы располагается элемент S_{ij} – множество разрешенных действий j -ого пользователя над i -м объектом.

Пример. Пусть имеем множество из трёх пользователей {Администратор, Гость, Пользователь_1} и множество из четырёх объектов {Файл_1, Файл_2, CD-RW, Дисковод}. Множество возможных действий включает следующие: {Чтение, Запись, Передача прав другому пользователю}. Действие «Полные права» разрешает выполнение всех трёх действий, действие «Запрет» запрещает выполнение

всех перечисленных действий. В данном случае, матрица доступа, описывающая дискреционную политику безопасности, может выглядеть следующим образом.

Таблица 1. Пример матрицы доступа

Объект / Субъект	Файл_1	Файл_2	CD-RW	Дисковод
1. Администратор	Полные права	Полные права	Полные права	Полные права
2. Гость	Запрет	Чтение	Чтение	Запрет
3. Пользователь_1	Чтение, передача прав	Чтение, запись	Полные права	Запрет

Например, Пользователь_1 имеет права на чтение и запись в Файл_2. Передавать же свои права другому пользователю он не может.

Пользователь, обладающий правами передачи своих прав доступа к объекту другому пользователю, может сделать это. При этом, пользователь, передающий права, может указать непосредственно, какие из своих прав он передает другому.

Например, если Пользователь_1 передает право доступа к Файлу_1 на чтение пользователю Гость, то у пользователя Гость появляется право чтения из Файла_1.

Задание на лабораторную работу

Пусть множество S возможных операций над объектами компьютерной системы задано следующим образом: $S = \{\text{«Доступ на чтение»}, \text{«Доступ на запись»}, \text{«Передача прав»}\}$.

1. Получить данные о количестве пользователей и объектов компьютерной системы из табл. 2, соответственно варианту.

2. Реализовать программный модуль, создающий матрицу доступа пользователей к объектам компьютерной системы. Реализация данного модуля подразумевает следующее:

2.1. Необходимо выбрать идентификаторы пользователей, которые будут использоваться при их входе в компьютерную систему (по одному идентификатору для каждого пользователя, количество пользователей указано для варианта). Например, множество из трёх идентификаторов пользователей {Ivan, Sergey, Boris}. Один из данных идентификаторов должен соответствовать администратору компьютерной системы (пользователю, обладающему полными правами доступа ко всем объектам).

2.2. Реализовать программное заполнение матрицы доступа, содержащей количество пользователей и объектов, соответственно Вашему варианту.

2.2.1. При заполнении матрицы доступа необходимо учитывать, что один из пользователей должен являться администратором системы (допустим, Ivan). Для него права доступа ко всем объектам должны быть выставлены как полные.

2.2.2. Права остальных пользователей для доступа к объектам компьютерной системы должны заполняться случайным образом с помощью датчика случайных чисел. При заполнении матрицы доступа необходимо учитывать, что пользователь может иметь несколько прав доступа к некоторому объекту компьютерной системы, иметь полные права, либо совсем не иметь прав.

2.2.3. Разработать алгоритм (либо реализовать программный модуль), демонстрирующий работу в дискреционной модели политики безопасности.

3. Данный модуль должен выполнять следующие функции:

3.1. При запуске модуля должен запрашиваться идентификатор пользователя (проводится идентификация пользователя), при успешной идентификации пользователя должен осуществляться вход в систему, при неуспешной – выводиться соответствующее сообщение.

3.2. При входе в систему после успешной идентификации пользователя на экране должен распечатываться список всех объектов системы с указанием перечня всех доступных прав доступа идентифицированного пользователя к данным объектам. Вывод можно осуществить, например, следующим образом:

```
User: Boris
```

```
Идентификация прошла успешно, добро пожаловать в систему
```

```
Перечень Ваших прав:
```

```
Объект1: Чтение
```

```
Объект2: Запрет
```

```
Объект3: Чтение, Запись
```

```
Объект4: Полные права
```

```
Жду ваших указаний >
```

3.3. После вывода на экран перечня прав доступа пользователя к объектам компьютерной системы, необходимо организовать ожидание указаний пользователя на осуществление действий над объектами в компьютерной системе. После получения команды от пользователя, на экран необходимо вывести сообщение об успешности либо не успешности операции. При выполнении операции передачи прав (grant) должна модифицироваться матрица доступа. Программа должна поддерживать операцию выхода из системы (quit), после которой запрашивается идентификатор пользователя. Диалог можно организовать, например, так:

```
Жду ваших указаний > read
```

```
Над каким объектом производится операция? 1
```

```
Операция прошла успешно
```

```
Жду ваших указаний > write
```

```
Над каким объектом производится операция? 2
```

```
Отказ в выполнении операции. У Вас нет прав для ее осуществления
```

```
Жду ваших указаний > grant
```

```
Право на какой объект передается? 3
```

```
Отказ в выполнении операции. У Вас нет прав для ее осуществления
```

Жду ваших указаний > grant
 Право на какой объект передается? 4
 Какое право передается? read
 Какому пользователю передается право? Ivan
 Операция прошла успешно
 Жду ваших указаний > quit
 Работа пользователя Boris завершена. До свидания.
 User:

4. Выполнить тестирование разработанной программы, продемонстрировав реализованную модель дискреционной политики безопасности.

5. Оформить отчет по лабораторной работе.

Таблица 2. Варианты заданий

Вариант	Количество субъектов доступа (пользователей)	Количество объектов доступа
1	3	3
2	4	4
3	5	4
4	6	5
5	7	6
6	8	3
7	9	4
8	10	4
9	3	5
10	4	6

Контрольные вопросы

1. Что понимается под политикой безопасности в компьютерной системе?
2. В чем заключается модель дискреционной политики безопасности в компьютерной системе?
3. Что понимается под матрицей доступа в дискреционной политике безопасности? Что хранится в данной матрице?
4. Какие действия производятся над матрицей доступа в том случае, когда один субъект передает другому субъекту свои права доступа к объекту компьютерной системы?

Лабораторная работа № 4

Количественная оценка стойкости парольной защиты

Цель работы: реализация простейшего генератора паролей, обладающего требуемой стойкостью к взлому.

Теоретические сведения

Подсистемы идентификации и аутентификации пользователя играют важную роль в системах защиты информации.

Стойкость подсистемы идентификации и аутентификации пользователя в системе защиты информации (СЗИ) во многом определяет устойчивость к взлому самой СЗИ. Данная стойкость определяется гарантией того, что злоумышленник не сможет пройти аутентификацию, присвоив чужой идентификатор или украв его.

Парольные системы идентификации/аутентификации являются одними из основных и наиболее распространенных в СЗИ методами пользовательской аутентификации. В данном случае информацией, аутентифицирующей пользователя, является некоторый секретный пароль, известный только легальному пользователю.

Парольная аутентификация пользователя, как правило, передний край обороны СЗИ. В связи с этим модуль аутентификации по паролю наиболее часто подвергается атакам со стороны злоумышленника. Цель последнего в данном случае – подобрать аутентифицирующую информацию (пароль) легального пользователя.

Методы парольной аутентификации пользователя наиболее просты и при несоблюдении определенных требований к выбору пароля являются достаточно уязвимыми.

Основными минимальными требованиями к выбору пароля и к подсистеме парольной аутентификации пользователя являются следующие.

К паролю:

- 1) минимальная длина пароля должна быть не менее 6 символов;
- 2) пароль должен состоять из различных групп символов (малые и большие латинские буквы, цифры, специальные символы ‘(’, ‘)’, ‘#’ и т.д.);
- 3) в качестве пароля не должны использоваться реальные слова, имена, фамилии и т.д.

К подсистеме парольной аутентификации:

- 1) администратор СЗИ должен устанавливать максимальный срок действия пароля, после чего, пароль следует сменить;
- 2) в подсистеме парольной аутентификации необходимо установить ограничение числа попыток ввода пароля (как правило, не более трёх);
- 3) в подсистеме парольной аутентификации требуется установить временную задержку в случае ввода неправильного пароля.

Как правило, для генерирования паролей в СЗИ, удовлетворяющих перечисленным требованиям к паролям, используются программы – автоматические генераторы паролей пользователей.

При выполнении перечисленных требований к паролям и к подсистеме парольной аутентификации единственно возможным методом взлома данной подсистемы злоумышленником является прямой перебор паролей (brute forcing). В данном случае, оценка стойкости парольной защиты осуществляется следующим образом.

Количественная оценка стойкости парольной защиты

Пусть A – мощность алфавита паролей (количество символов, которые могут быть использованы при составлении пароля: если пароль состоит только из малых английских букв, то $A = 26$), L – длина пароля, $S = A^L$ – число всевозможных паролей длины L , которые можно составить из символов алфавита A , V – скорость перебора паролей злоумышленником, T – максимальный срок действия пароля.

Тогда, вероятность P подбора пароля злоумышленником в течение срока его действия T определяется по следующей формуле:

$$P = (V \cdot T) / S = (V \cdot T) / A^L.$$

Эту формулу можно использовать в обратную сторону для решения следующей задачи.

Задача. Определить минимальные мощность алфавита паролей A и длину паролей L , обеспечивающих вероятность подбора пароля злоумышленником не более заданной P , при скорости подбора паролей V , максимальном сроке действия пароля T .

Данная задача имеет неоднозначное решение. При исходных данных V , T , P однозначно можно определить лишь нижнюю границу S^* числа всевозможных паролей. Целочисленное значение нижней границы вычисляется по формуле

$$S^* = [V \cdot P / T], \quad (1)$$

где $[]$ – целая часть числа, взятая с округлением вверх.

После определения нижней границы S^* необходимо выбрать такие A и L для формирования $S = A^L$, чтобы выполнялось следующее неравенство:

$$S^* \leq S = A^L. \quad (2)$$

При выборе S , удовлетворяющего неравенству (2), вероятность подбора пароля злоумышленника (при заданных V и T) будет меньше, чем заданная P .

Следует отметить, что при осуществлении вычислений по формулам (1) и (2), величины должны быть приведены к одним размерностям.

Пример. Исходные данные: $P = 10^{-6}$, $T = 7$ дней = 1 неделя, $V = 10$ (паролей / минуту) = $10 \cdot 60 \cdot 24 \cdot 7 = 100800$ паролей в неделю. Тогда, $S^* = [(100800 \cdot 1) / 10^{-6}] = 108 \cdot 10^8$.

Условию $S^* \leq A^L$ удовлетворяют, например, такие комбинации A и L , как $A = 26$, $L = 8$ (пароль состоит из восьми малых символов английского алфавита), $A = 36$, $L = 6$ (пароль состоит из шести символов, среди которых могут быть малые латинские буквы и произвольные цифры).

Задание на лабораторную работу

1. В табл. 3 найти для указанного варианта значения характеристик P , V , T .
2. Вычислить по формуле (1) нижнюю границу S^* для заданных P , V , T .
3. Выбрать некоторый алфавит с мощностью A и получить минимальную длину пароля L , при котором выполняется условие (2).
4. Реализовать программу (алгоритм) для генерации паролей пользователей. Программа должна формировать случайную последовательность символов длины L , при этом должен использоваться алфавит из A символов.

Примеры кодов символов:

- Коды английских символов : «A» = 65, ..., «Z» = 90, «a» = 97, ..., «z» = 122.
- Коды цифр : «0» = 48, «9» = 57.
- «!» = 33, «“» = 34, «#» = 35, «\$» = 36, «%» = 37, «&» = 38, «'» = 39.
- Коды русских символов : «А» – 128, ... «Я» – 159, «а» – 160, ..., «п» – 175, «р» – 224, ..., «я» – 239.

Таблица 3. Варианты заданий

Вариант	P	V	T
1	10^{-4}	15 паролей/мин	2 недели
2	10^{-5}	3 паролей/мин	10 дней
3	10^{-6}	10 паролей/мин	5 дней
4	10^{-7}	11 паролей/мин	6 дней
5	10^{-4}	100 паролей/день	12 дней
6	10^{-5}	10 паролей/день	1 месяц
7	10^{-6}	20 паролей/мин	3 недели
8	10^{-7}	15 паролей/мин	20 дней
9	10^{-4}	3 паролей/мин	15 дней
10	10^{-5}	10 паролей/мин	1 неделя

Контрольные вопросы

1. Чем определяется стойкость подсистемы идентификации и аутентификации?
2. Перечислить минимальные требования к выбору пароля.
3. Перечислить минимальные требования к подсистеме парольной аутентификации.
4. Как определить вероятность подбора пароля злоумышленником в течение срока его действия?
5. Выбором каких параметров можно повлиять на уменьшение вероятности подбора пароля злоумышленником при заданной скорости подбора пароля злоумышленником и заданном сроке действия пароля?

Лабораторная работа №5

Защита от копирования. Привязка к аппаратному обеспечению. Использование реестра

Цель работы: ознакомиться с возможностями «привязки» к характеристикам компьютера.

Теоретические сведения

В качестве анализируемых характеристик компьютера могут использоваться:

1. Информация об используемой операционной системе
2. Имя пользователя;
3. Имя компьютера;
4. Наличие звуковой карты;
5. Наличие подключенных принтера, сканера и т.д;
6. Дата создания BIOS;
7. Серийный номер диска;
8. Характеристики процессора.

Для получения подобных характеристик в операционной системе Windows используются API-функции и информация из реестра.

API-функции

API сокращенно Application Programming Interface (интерфейс прикладного программирования). API – набор функций, которые операционная система предоставляет программисту. API обеспечивает относительно простой путь для программистов для использования полных функциональных возможностей аппаратных средств или операционной системы.

32-разрядные версии Windows обычно используют один и тот же набор функций API, хотя имеются некоторые различия между платформами.

Почти все функции, которые составляют Windows API, находятся внутри DLL (Dynamic Link Library). Эти dll-файлы находятся в системной папке Windows. Существует свыше 1000 функций API, которые условно делятся на четыре основные категории:

- 1) работа с приложениями – запуск и закрытие приложений, обработка команд меню, перемещения и изменения размера окон;
- 2) графика – создание изображений;
- 3) системная информация – определение текущего диска, объема памяти, имя текущего пользователя и т.д.
- 4) работа с реестром – манипуляции с реестром Windows.

Реестр Windows

Реестр – база данных операционной системы, содержащая конфигурационные сведения. По замыслу Microsoft реестр должен был полностью заменить файлы ini, которые были оставлены только для совместимости со старыми программами, ориентированными на более ранние версии операционной системы.

Переход от ini файлов к реестру произошел по той причине, что на эти файлы накладывается ряд серьезных ограничений, и главное из них состоит в том, что предельный размер такого файла составляет 64Кб.

Предупреждение: никогда не удаляйте или не меняйте информацию в реестре, если Вы не уверены что это именно то, что нужно. В противном случае некорректное изменение данных может привести к сбоям в работе Windows и, в лучшем случае, информацию придется восстанавливать из резервной копии.

Реестр имеет следующую структуру:

1) HKEY_CLASSES_ROOT. В этом разделе содержится информация о зарегистрированных в Windows типах файлов, что позволяет открывать их по двойному щелчку мыши, а также информация для OLE и операций drag-and-drop;

2) HKEY_CURRENT_USER. Здесь содержатся настройки оболочки пользователя (например, Рабочего стола, меню "Пуск", ...), вошедшего в Windows. Они дублируют содержимое подраздела HKEY_USER\name, где name – имя пользователя, вошедшего в Windows. Если на компьютере работает один пользователь и используется обычный вход в Windows, то значения раздела берутся из подраздела HKEY_USERS\DEFAULT;

3) HKEY_LOCAL_MACHINE. Этот раздел содержит информацию, относящуюся к компьютеру: драйверы, установленное программное обеспечение и его настройки;

4) HKEY_USERS. Содержит настройки оболочки Windows для всех пользователей. Как было сказано выше, именно из этого раздела информация копируется в раздел HKEY_CURRENT_USER. Все изменения в HKCU (сокращенное название раздела HKEY_CURRENT_USER) автоматически переносятся в HKU;

5) HKEY_CURRENT_CONFIG. В этом разделе содержится информация о конфигурации устройств Plug&Play и сведения о конфигурации компьютера с переменным составом аппаратных средств;

6) HKEY_DYN_DATA. Здесь хранятся динамические данные о состоянии различных устройств, установленных на компьютере пользователя. Именно сведения этой ветви отображаются в окне "Свойства: Система" на вкладке "Устройства", вызываемого из Панели управления. Данные этого раздела изменяются самой операционной системой, так что редактировать что-либо вручную не рекомендуется.

Примеры процедур и функций, определяющих параметры компьютера

Определение версии операционной системы

```
BOOL DisplaySystemVersion()
{
    OSVERSIONINFOEX osv;
    BOOL bOsVersionInfoEx;
    ZeroMemory(&osv, sizeof(OSVERSIONINFOEX));
    osv.dwOSVersionInfoSize = sizeof(OSVERSIONINFOEX);
    if( !(bOsVersionInfoEx = GetVersionEx ((OSVERSIONINFO *) &osv)) )
    {
        osv.dwOSVersionInfoSize = sizeof (OSVERSIONINFO);
        if (! GetVersionEx ( (OSVERSIONINFO *) &osv) )
    }
```

```

        return FALSE;
    }

    switch (osvi.dwPlatformId)
    {
        case VER_PLATFORM_WIN32_NT:
            if ( osvi.dwMajorVersion <= 4 )
                printf("Microsoft Windows NT ");
            if ( osvi.dwMajorVersion == 5 && osvi.dwMinorVersion == 0 )
                printf ("Microsoft Windows 2000 ");
            if( bOsVersionInfoEx )
            {
                if ( osvi.wProductType == VER_NT_WORKSTATION )
                {
                    if ( osvi.dwMajorVersion == 5 && osvi.dwMinorVersion
== 1 )
                        printf ("Microsoft Windows XP ");

                    if( osvi.wSuiteMask & VER_SUITE_PERSONAL )
                        printf ( "Home Edition " );
                    else
                        printf ( "Professional " );
                }
                else if ( osvi.wProductType == VER_NT_SERVER )
                {
                    if ( osvi.dwMajorVersion == 5 && osvi.dwMinorVersion
== 2 )
                        printf ("Microsoft Windows .NET ");

                    if( osvi.wSuiteMask & VER_SUITE_DATACENTER )
                        printf ( "DataCenter Server " );
                    else if( osvi.wSuiteMask & VER_SUITE_ENTERPRISE )
                        if( osvi.dwMajorVersion == 4 )
                            printf ("Advanced Server " );
                        else
                            printf ( "Enterprise Server " );
                    else if ( osvi.wSuiteMask == VER_SUITE_BLADE )
                        printf ( "Web Server " );
                    else
                        printf ( "Server " );
                }
            }
        else
        {
            HKEY hKey;
            char szProductType[BUFSIZE];
            DWORD dwBufLen=BUFSIZE;
            LONG lRet;
            lRet = RegOpenKeyEx( HKEY_LOCAL_MACHINE,
                "SYSTEM\\CurrentControlSet\\Control\\ProductOptions",
                0, KEY_QUERY_VALUE, &hKey );

```

```

    if( lRet != ERROR_SUCCESS )
        return FALSE;
    lRet = RegQueryValueEx( hKey, "ProductType", NULL, NULL,
        (LPBYTE) szProductType, &dwBufLen);
    if( (lRet != ERROR_SUCCESS) || (dwBufLen > BUFSIZE) )
        return FALSE;
    RegCloseKey( hKey );
    if ( lstrcmpi( "WINNT", szProductType) == 0 )
        printf( "Professional " );
    if ( lstrcmpi( "LANMANNT", szProductType) == 0 )
        printf( "Server " );
    if ( lstrcmpi( "SERVERNT", szProductType) == 0 )
        printf( "Advanced Server " );
}
if ( osvi.dwMajorVersion <= 4 )
{
    printf ("version %d.%d %s (Build %d)\n",
        osvi.dwMajorVersion,
        osvi.dwMinorVersion,
        osvi.szCSDVersion,
        osvi.dwBuildNumber & 0xFFFF);
}
else
{
    printf ("%s (Build %d)\n",
        osvi.szCSDVersion,
        osvi.dwBuildNumber & 0xFFFF);
}
break;
case VER_PLATFORM_WIN32_WINDOWS:
    if (osvi.dwMajorVersion == 4 && osvi.dwMinorVersion == 0)
    {
        printf ("Microsoft Windows 95 ");
        if ( osvi.szCSDVersion[1] == 'C' || osvi.szCSDVersion[1]
== 'B' )
            printf("OSR2 " );
    }
    if (osvi.dwMajorVersion == 4 && osvi.dwMinorVersion == 10)
    {
        printf ("Microsoft Windows 98 ");
        if ( osvi.szCSDVersion[1] == 'A' )
            printf("SE " );
    }
    if (osvi.dwMajorVersion == 4 && osvi.dwMinorVersion == 90)
    {
        printf ("Microsoft Windows Millennium Edition ");
    }
    break;
}
return TRUE;
}

```

Определение серийного номера раздела диска

```
TCHAR    szVolName[256];
DWORD    dwNum;
DWORD    dwMaxComSize;
DWORD    dwFlags;
TCHAR    szFS[256];
BOOL     bRes;
bRes = GetVolumeInformation ( "c:\\", szVolName, sizeof(szVolName),
&dwNum, &dwMaxComSize, &dwFlags, szFS, sizeof(szFS));
```

Определение имени компьютера

```
const int WSVer = 0x101;
WSADATA wsaData;
char Buf[128];
if (WSAStartup(WSVer, &wsaData) == 0)
{
    gethostname(&Buf[0], 128);
    MessageBox(0, Buf, 0, 0);
    WSACleanup;
}
```

Определение имени пользователя

```
char buffer[UNLEN+1];
DWORD size;
size=sizeof(buffer);
GetUserName(buffer, &size);
```

Определение версии BIOS

```
LPSTR GetSystemBiosVersion()
{
    HKEY hKey;
    LONG Res1, Res2;
    DWORD cData=255;
    TCHAR SystemBiosVersion[255]={'\0'};

    Res1=RegOpenKeyEx(HKEY_LOCAL_MACHINE, "HARDWARE\\DESCRIPTION\\System",
    NULL, KEY_QUERY_VALUE, &hKey);
    if (Res1==ERROR_SUCCESS)
    {
        Res2=RegQueryValueEx(hKey, "SystemBiosVersion", NULL, NULL, ...
        (LPBYTE) SystemBiosVersion, &cData);
        if (Res2==ERROR_SUCCESS)
        {
            for (const char* p = SystemBiosVersion; *p; p +=
strlen(p)+1)
            {
                printf("%s\n", p);
            }

            return SystemBiosVersion;
        }
        else
        {

```

```

        MessageBox(NULL, "RegQueryValueEx:
SystemBiosVersion", "ERROR", MB_OK);
        return NULL;
    }
}
else
{
    MessageBox(NULL, "RegOpenKeyEx:
SystemBiosVersion", "ERROR", MB_OK);
    return NULL;
}
RegCloseKey(hKey);
}

```

Определение частоты процессора (способ №1)

```

double CPUSpeed(void)
{
    DWORD dwTimerHi, dwTimerLo;
    asm
    {
        DW 0x310F
        mov dwTimerLo, EAX
        mov dwTimerHi, EDX
    }
    Sleep (500);
    asm
    {
        DW 0x310F
        sub EAX, dwTimerLo
        sub EDX, dwTimerHi
        mov dwTimerLo, EAX
        mov dwTimerHi, EDX
    }
    return dwTimerLo/(1000.0*500);
}

```

Задание на лабораторную работу

Описать API-функции, реализующие привязку к компьютеру, используя совокупность характеристик:

- 1) Серийный номер раздела жесткого диска, MAC-адрес сетевой карты
- 2) Информация из реестра, тактовая частота процессора
- 3) Версия операционной системы, MAC-адрес сетевой карты
- 4) Имя пользователя, серийный номер раздела жесткого диска
- 5) Название компьютера, информация из реестра
- 6) Версия БИОС, имя пользователя
- 7) Серийный номер раздела жесткого диска, имя пользователя
- 8) Имя пользователя, тактовая частота процессора
- 9) MAC-адрес сетевой карты, тактовая частота процессора

Контрольные вопросы

1. Что понимается под «привязкой» к компьютеру?
2. Какие характеристики обычно используются для идентификации компьютера?
3. Перечислите основные API-функции для определения индивидуальных характеристик компьютера.
4. Что представляет собой реестр Windows?
5. Какую структуру имеет реестр?

Лабораторная работа 6

Анализ безопасности систем с использованием сканеров уязвимостей

Цель работы – изучить принципы анализа безопасности систем с использованием сканеров уязвимостей.

Теоретические сведения

1 Уязвимость информационных систем

В компьютерной безопасности термин «уязвимость» (англ. vulnerability) используется для обозначения недостатка в системе, используя который можно намеренно нарушить её целостность и вызвать неправильную работу. Уязвимость может быть результатом ошибок программного кода, недостатков, допущенных при проектировании системы, ненадежных паролей, вирусов и других вредоносных программ, скриптовых и SQL-инъекций и др.

Сканеры уязвимостей – это программные или аппаратные средства, служащие для осуществления диагностики и мониторинга сетевых компьютеров, позволяющее сканировать сети, компьютеры и приложения на предмет обнаружения возможных проблем в системе безопасности, оценивать и устранять уязвимости.

Примеры сканеров уязвимостей:

Nessus Professional	https://www.tenable.com/products/nessus/nessus-professional/evaluate
XSpider	https://www.ptsecurity.com/ru-ru/products/xspider/
OpenVAS	http://www.openvas.org/
IBM® Security AppScan и др.	https://www.ibm.com/security/application-security/appscan

2 Пример применения сканера анализа уязвимостей

Рассмотрим анализ уязвимости на примере использования пакета Nessus Professional.

Nessus® Professional – это прикладное решение для оценки уязвимостей безопасности, включая проблемы с конфигурацией и с вредоносным ПО, которое злоумышленники могут использовать для проникновения в сеть. Используется для автоматического поиска известных изъянов в защите информационных систем. Программа способна обнаружить наиболее часто встречающиеся виды уязвимостей, например:

- наличие уязвимых версий служб или доменов;
- ошибки в конфигурации (например, отсутствие необходимости авторизации на smtp-сервере);
- наличие слабых паролей и др.

Программа имеет клиент-серверную архитектуру. Прежде всего, используется для сканирования портов и определяет использующие их сервисы. Также проводится проверка сервисов по базе уязвимостей. Для тестирования уязвимостей используются специальные плагины.

Имеется бесплатная демоверсия системы с временным ограничением.

Инструкции по установке программы:

Для демоверсии программы требуется регистрация, при этом необходимо указать свой e-mail для получения кода активации.

Далее будет предложено выбрать тип и разрядность вашей системы; при этом поддерживаются Windows Server, MacOS, Linux, FreeBSD и др.

Например:

[Nessus-7.0.3-x64.msi](#)

Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, 7, 8, 10, Server 2016 (64-bit)

Nessus построен на клиент-серверной архитектуре. После завершения установки откроется браузер, установленный по умолчанию. Если сервер был задан как localhost, то браузер и будет выступать в роли клиента. Если при этом будет выдаваться сообщение: «Your connection is not secure» («Ваше соединение не безопасно»), то следует добавить исключения для подключения Nessus по порту 8834.

Далее необходимо создать учетную запись. Именно ее нужно будет указывать для входа в Nessus.

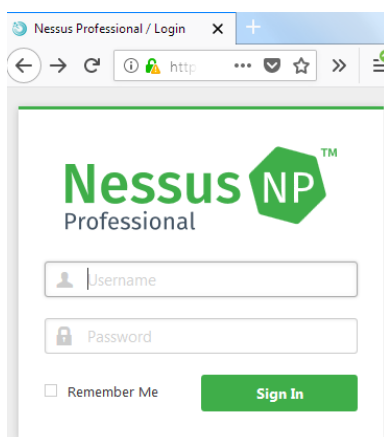


Рисунок 1 - Вход в систему

После ввода вашего логина и пароля будет необходимо активировать продукт – ввести код активации из полученного ранее по электронной почте письма. После этого Nessus начнет загружать все актуальные обновления и плагины, необходимые для поиска уязвимостей в сети.

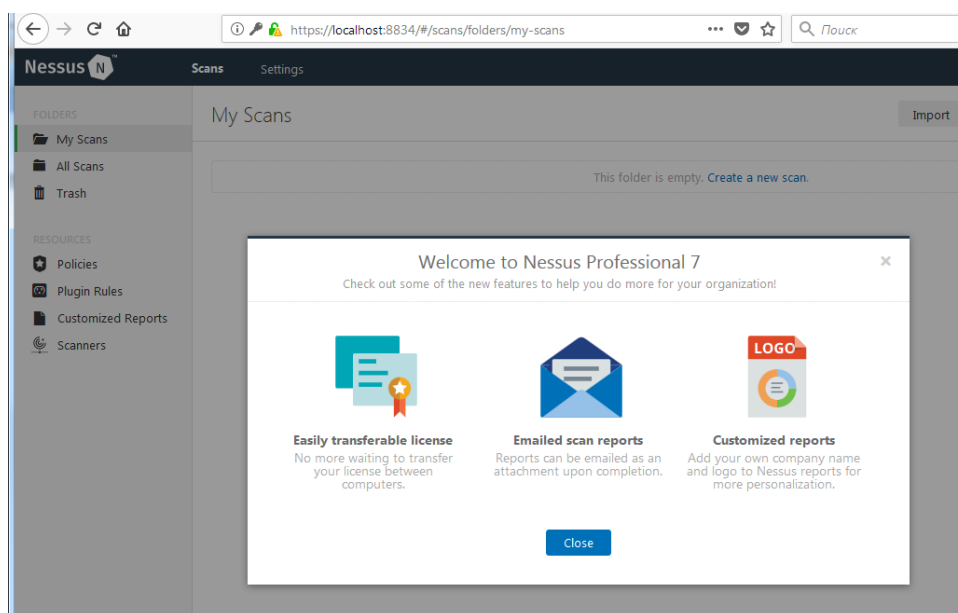


Рисунок 2 - Вид программного окна

Затем вы сможете выбрать требуемый тип сканирования. На соответствующей странице содержатся разнообразные актуальные модели угроз.

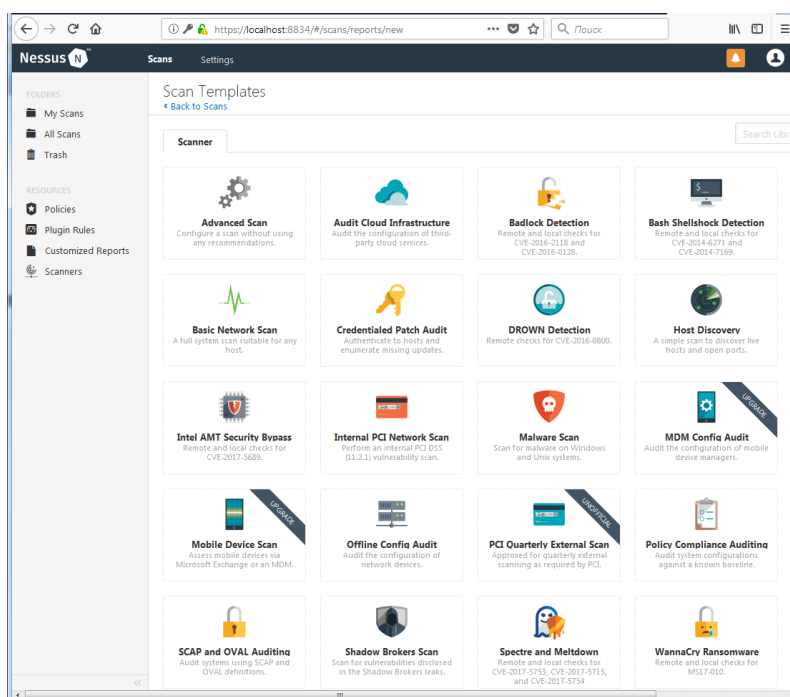


Рисунок 3 - Выбор видов сканирования

Выберем нужный вариант сканирования:



Advanced Scan

Configure a scan without using any recommendations.

Расширенное сканирование.
Настройки сканирования без каких-либо рекомендаций.



Audit Cloud Infrastructure

Audit the configuration of third-party cloud services.

Аудит облачной инфраструктуры.
Аудит конфигурации сторонних облачных сервисов.



Badlock Detection

Remote and local checks for CVE-2016-2118 and CVE-2016-0128.

Обнаружение уязвимости Badlock.
Удаленные и локальные проверки для CVE-2016-2118 и CVE-2016-0128.



Bash Shellshock Detection

Remote and local checks for CVE-2014-6271 and CVE-2014-7169.

Обнаружение уязвимости Shellshock Bash.
Удаленные и локальные проверки для CVE-2014-6271 и CVE-2014-7169.



Basic Network Scan

A full system scan suitable for any host.

Основное сетевое сканирование.
Полное сканирование системы, подходящее для любого хоста.



Credentialed Patch Audit

Authenticate to hosts and enumerate missing updates.

Аутентификация с проверкой подлинности.
Аутентификация хостов и перечисление отсутствующих обновлений.



DROWN Detection

Remote checks for CVE-2016-0800.

Обнаружение уязвимости DROWN.
Удаленные проверки для CVE-2016-0800.



Host Discovery

A simple scan to discover live hosts and open ports.

Исследование хоста.
Простое сканирование для обнаружения активных хостов и открытых портов.



Intel AMT Security Bypass

Remote and local checks for CVE-2017-5689.

Обход безопасности Intel AMT.
Удаленные и локальные проверки для CVE-2017-5689.



Internal PCI Network Scan

Perform an internal PCI DSS (11.2.1) vulnerability scan.

Внутреннее сканирование сети PCI.
Выполнение внутренней проверки уязвимости PCI DSS (11.2.1).



Malware Scan

Scan for malware on Windows and Unix systems.

Сканирование вредоносных программ.
Сканирование вредоносных программ в системах Windows и Unix.



MDM Config Audit

Audit the configuration of mobile device managers.

Аудит MDM Config.
Аудит конфигурации менеджеров мобильных устройств.



Mobile Device Scan

Assess mobile devices via Microsoft Exchange or an MDM.

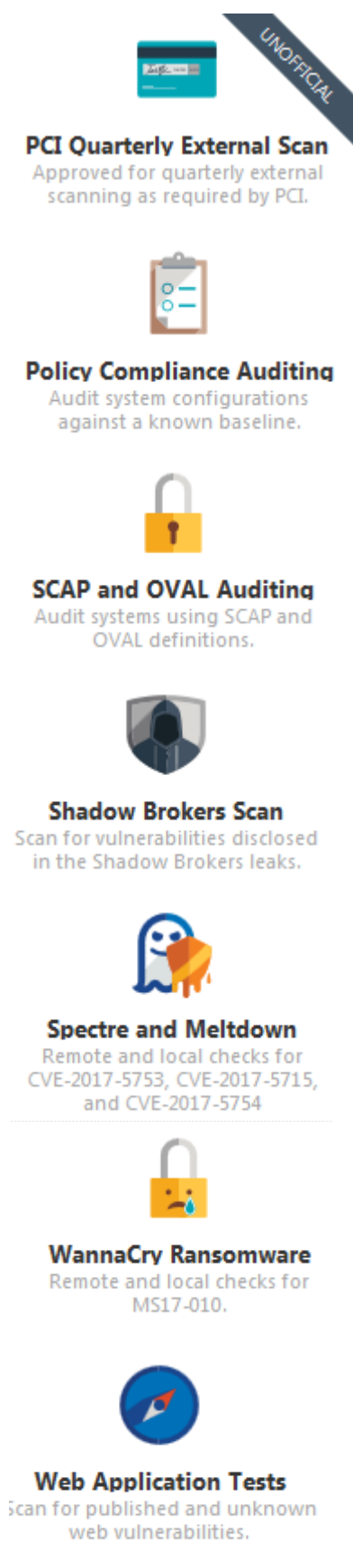
Сканирование мобильных устройств.
Оценка мобильных устройств через Microsoft Exchange или MDM.



Offline Config Audit

Audit the configuration of network devices.

Аудит автономной конфигурации.
Аудит конфигурации сетевых устройств



PCI Quarterly External Scan.
Доступно для ежеквартального внешнего сканирования, как требуется PCI.

Проверка соответствия нормативным требованиям.
Аудит конфигурации системы с учетом известного базового уровня.

Аудит SCAP и OVAL.
Системы аудита с использованием определений SCAP и OVAL.

Сканирование «теневых брокеров».
Сканирование уязвимостей, обнаруженных в утечках Shadow Brokers.

Уязвимости Spectre и Meltdown.
Удаленные и локальные проверки для CVE-2017-5753, CVE-2017-5715 и CVE-2017-5754

Уязвимость WannaCry «Вымогатели».
Удаленные и локальные проверки для MS17-010.

Тестирование веб-приложений.
Сканирование опубликованных и неизвестных уязвимостей в Интернете.

По результатам сканирования получаем список выявленных проблем и связанные с ними риски. Риски имеют цветовую кодировку. Нажимаем

"vulnerabilities" в верхнем меню, чтобы отобразить все уязвимости, обнаруженные в сети.

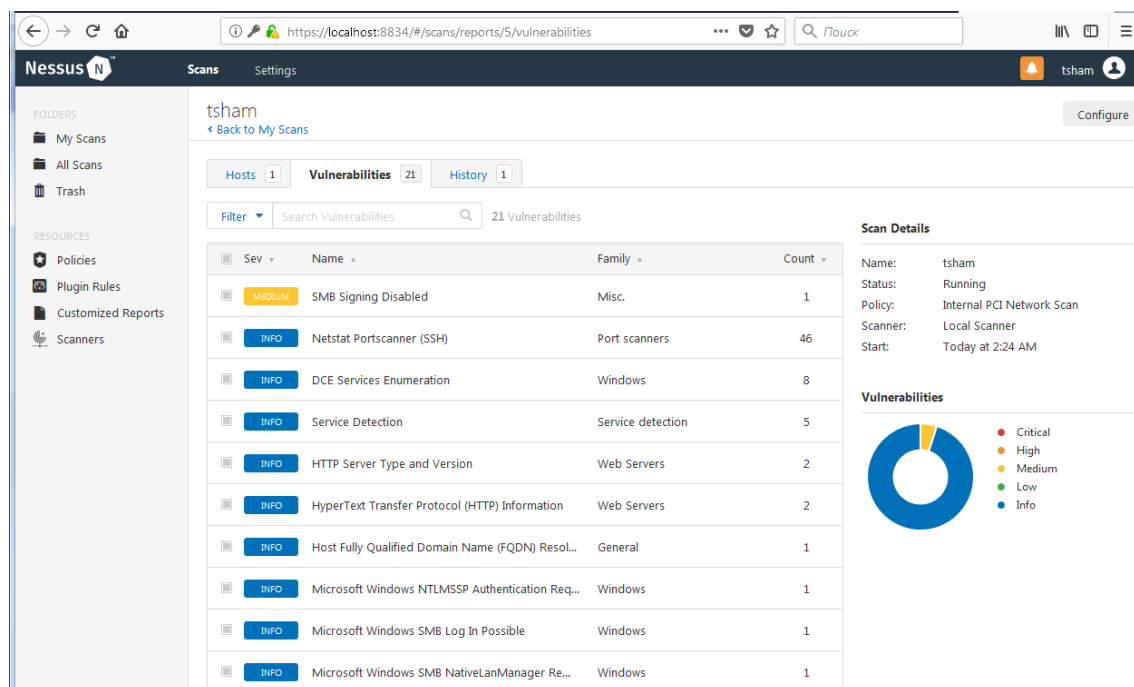


Рисунок 4 - Отчет о результатах сканирования и выявленных проблемах

Если кликнуть по конкретной уязвимости, то получим более детальную информацию.

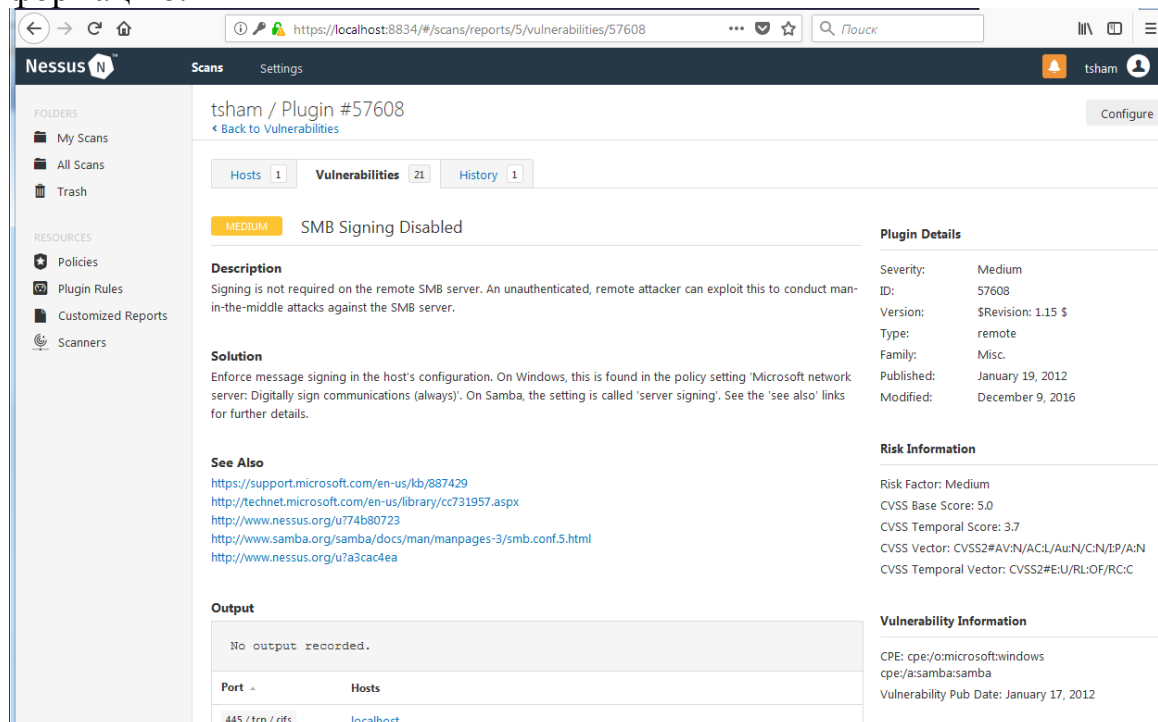


Рисунок 5 - Детализация уязвимости

Помимо описания уязвимости, в детализации присутствует также и способ ее исправления и устранения (раздел Solution – «Решение»).

2 Порядок выполнения работы:

2.1 С использованием одного из сканеров уязвимостей провести анализ безопасности компьютеров сети.

Выявить проблемы безопасности, рассмотреть вопросы их решения.

2.2 Оформить отчет по данной работе.

Отчет по лабораторной работе должен содержать:

- результат анализа уязвимости сети, проведенного с использованием сканера уязвимостей. Для выполнения задания можно использовать либо пакет Nessus Professional, либо имеющееся у вас соответствующее программное обеспечение подобного класса;

- ответы на контрольные вопросы из пункта 3.

3 Вопросы для самоконтроля знаний

- 1) Что понимают под уязвимостью информационной системы?
- 2) Назовите виды и примеры компьютерных уязвимостей.
- 3) Охарактеризуйте понятие «сканер уязвимости».
- 4) Перечислите примеры сканеров сетевой уязвимости.
- 5) Что понимают под удаленной сетевой атакой? Приведите классификацию сетевых атак.

Лабораторная работа №7

Изучение механизмов работы и вариантов совместного применения межсетевого экрана и сетевого сканера на примере ПО Agnitum Outpost и XSpider

Цель работы:

- 1) Изучение механизмов работы средств обеспечения и поддержки сетевой защиты – брандмауэра и сетевого сканера;
- 2) Практическое ознакомление с работой сетевого сканера XSpider и межсетевого экрана «Outpost»;
- 3) Изучение работы рассматриваемых систем в «совместном» режиме для защиты и тестирования рабочих станций на наличие уязвимостей.

Подготовка к выполнению работы: Подготовить для включения в отчет о лабораторной работе определения понятий:

1. Адаптивная безопасность сети
2. Межсетевой экран, *Сканеры уязвимостей, Бэкдор*
3. "Имитация атак" (exploit check)

1 Теоретические сведения.

Среди угроз безопасности информации значительное место занимает автоматическое внедрение в компьютеры программных закладок, способных скрыто отслеживать и передавать злоумышленнику данные о функционировании компьютера, обрабатываемой на нем информации, а также о всей компании в целом. Кроме того, проблемы компьютерным сетям предприятий создают факты проникновения компьютерных хулиганов, которые, взломав систему сетевой защиты компании, могут завладеть конфиденциальной информацией или нанести физический вред оборудованию, используя специализированное вредоносное ПО.

Подобные ситуации возникают из-за уязвимостей в системе корпоративной защиты компании, в основном связанные с открытыми портами неиспользуемых сервисов, работающих вхолостую. Как правило, через «дыры» в данных сервисах осуществляется большая часть удачных атак извне, которые, зачастую, кончаются потерей компанией секретных данных.

Необходимо отметить, что на сегодняшний день работы по проникновению злоумышленников через «дыры» в защите на 90% автоматизированы. Поэтому, «самостоятельное» появление вредоносного ПО на вашем компьютере, которое встречается сегодня очень часто, связано в большинстве случаев с наличием непреднамеренных лазеек в неиспользуемых, а значит, не обновляющихся, службах.

Тем не менее, при использовании специальных средств защиты, подобных нежелательных событий можно, как правило, избежать.

Основными средствами защиты на сегодняшний день являются две категории специализированных программ:

- Межсетевые экраны (брандмауэры, FireWall, МСЭ);
- Сканеры (сканеры открытых портов и сервисов).

Следует сказать, что брандмауэр – основной механизм в сети программной и аппаратной защиты рабочих станций и серверов от атак извне и изнутри.

Сканер – это вспомогательный программный инструмент, позволяющий провести групповое тестирование параметров хостов сети, а также определить наличие и правильность настройки в них МСЭ.

Эти два класса систем в комплексе позволяют построить эффективную эшелонированную систему защиты компании, значительно снизив тем самым вероятность вторжения в сеть злоумышленников.

2 Архитектура firewall

Firewall — это шлюз сети, снабженный правилами защиты. Он может быть аппаратным или программным. В соответствии с заложенными правилами обрабатывается каждый пакет, проходящий наружу или внутрь сети, причем процедура обработки может быть задана для каждого правила. Производители программ и машин, реализующих firewall-технологии, обеспечивают различные способы задания правил и процедур. Обычно firewall создает контрольные записи, детализирующие причину и обстоятельства возникновения внештатных ситуаций. Анализируя такие контрольные записи, администраторы часто могут обнаружить источники атаки и способы ее проведения.

2.1 Фильтрация пакетов (packet filtering firewalls)

Каждый IP-пакет проверяется на совпадение заложенной в нем информации с допустимыми правилами, записанными в firewall.

Параметры, которые могут проверяться:

- физический интерфейс движения пакета;
- адрес, с которого пришел пакет (источник);
- адрес, куда идет пакет (получатель);
- тип пакета (TCP, UDP, ICMP);
- порт источника;
- порт получателя.

Механизм фильтрации пакетов не имеет дела с их содержанием. Это позволяет использовать непосредственно ядро операционной системы для задания правил. В сущности, создаются два списка: отрицание (deny) и разрешение (permit). Все пакеты должны пройти проверку по всем пунктам этого списка. Далее используются следующие методы:

- если никакое правило соответствия не найдено, то удалить пакет из сети;
- если соответствующее правило найдено в списке разрешений, то пропустить пакет;
- если соответствующее правило найдено в списке отрицаний, то удалить пакет из сети.

В дополнение к этому firewall, основанный на фильтрации пакетов, может изменять адреса источников пакетов, выходящих наружу, чтобы скрыть тем самым топологию сети (метод address translation), плюс осуществляет условное и безусловное перенаправление пакетов на другие хосты. Отметим преимущества firewall, основанного на фильтрации пакетов:

- фильтрация пакетов работает быстрее других firewall-технологий, потому что используется меньшее количество проверок;
- этот метод легко реализуем аппаратно;
- одно-единственное правило может стать ключевым при защите всей сети;
- фильтры не требуют специальной конфигурации компьютера;
- метод address translation позволяет скрыть реальные адреса компьютеров в сети.

Однако имеются и недостатки:

- нет проверки содержимого пакетов, что не дает возможности, например, контролировать, что передается по FTP. В этом смысле application layer и circuit level firewall гораздо практичнее;
- нет информации о том, какой процесс или программа работали с этим пакетом, и сведений о сессии работы;
- работа ведется с ограниченной информацией пакета;
- в силу «низкоуровневости» метода не учитывается особенность передаваемых данных;
- слабо защищен сам компьютер, на котором запущен firewall, то есть предмет атаки может стать сам этот компьютер;
- нет возможности сигнализировать о внештатных ситуациях или выполнять при их возникновении какие-либо действия;
- возможно, что большой объем правил будет тормозить проверку.

2.2 Firewall цепного уровня (circuit level firewalls)

Поскольку при передаче большой порции информации она разбивается на маленькие пакеты, целый фрагмент состоит из нескольких пакетов (из цепи пакетов). Firewall цепного уровня проверяет целостность всей цепи, а также то, что она вся идет от одного источника к одному получателю, и информация о цепи внутри пакетов (а она там есть при использовании TCP) совпадает с реально проходящими пакетами. Причем цепь вначале собирается на компьютере, где установлен firewall, а затем отправляется получателю. Поскольку первый пакет цепи содержит информацию о всей цепи, то при попадании первого пакета создается таблица, которая удаляется лишь после полного прохождения цепи. Содержание таблицы следующее:

- уникальный идентификатор сессии передачи, который используется для контроля;
- состояние сессии передачи: установлено, передано или закрыто;

- информация о последовательности пакетов;
- адрес источника цепи;
- адрес получателя цепи;
- физический интерфейс, используемый для получения цепи;
- физический интерфейс, используемый для отправления цепи.

Эта информация применяется для проверки допустимости передачи цепи.

Правила проверки, как и в случае фильтрации пакетов, задаются в виде таблиц в ядре. Основные **преимущества firewall цепного уровня**:

- firewall цепного уровня быстрее программного, так как производит меньше проверок;
- firewall цепного уровня позволяет легко защитить сеть, запрещая соединения между определенными адресами внешней и внутренней сети;
- возможно скрытие внутренней топологии сети.

Недостатки firewall цепного уровня:

- нет проверки пакетов на программном уровне;
- слабые возможности записи информации о нештатных ситуациях, кроме информации о сессии передачи;
- нет проверки передаваемых данных;
- трудно проверить разрешение или отрицание передачи пакетов.

2.3 Firewall программного уровня

Помимо целостности цепей, правильности адресов и портов, проверяются также сами данные, передаваемые в пакетах. Это позволяет проверять целостность данных и отслеживать передачу таких сведений, как пароли. Вместе с firewall программного уровня используется проху-сервис, который кэширует информацию для более быстрой ее обработки. При этом возникают такие новые возможности, как, например, фильтрация URL и установление подлинности пользователей. Все соединения внутренней сети с внешним миром происходят через проху, который является шлюзом. У проху две части: сервер и клиент. Сервер принимает запросы, например на telnet-соединение из внутренней сети с внешней, обрабатывает их, то есть проверяет на допустимость передачи данных, а клиент работает с внешним компьютером от имени реального клиента. Естественно, вначале все пакеты проходят проверку на нижних уровнях. **Достоинства проху:**

- понимает и обрабатывает протоколы высокого уровня типа HTTP и FTP;
- сохраняет полную информацию о сессии передачи данных как низкого, так и высокого уровня;
- возможен запрет доступа к некоторым сетевым сервисам;
- есть возможность управления пакетами данных;
- есть сокрытие внутренних адресов и топологии сети, так как проху является фильтром;
- остается видимость прямого соединения сетей;
- проху может перенаправлять запросы сетевых сервисов на другие компьютеры;

- есть возможность кэширования http-объектов, фильтрации URL и установления подлинности пользователей;
- возможно создание подробных отчетных записей для администратора.

Недостатки проху:

- требует изменения сетевого стека на машине, где стоит firewall;
- нельзя напрямую запустить сетевые сервисы на машине, где стоит firewall, так как проху перехватывает работу портов;
- неминуемо замедляет работу, потому все данные обрабатываются дважды: «родной» программой и собственно проху;
- так как проху должен уметь работать с данными какой-либо программы, то для каждой программы нужен свой проху;
- нет проху для UDP и RPC;
- иногда необходима специальная настройка клиента для работы с проху;
- проху не защищен от ошибок в самой системе, а его работа сильно зависит от наличия последних;
- корректность работы проху напрямую связана с правильностью обработки сетевого стека;
- использование проху может требовать дополнительных паролей, что неудобно для пользователей.

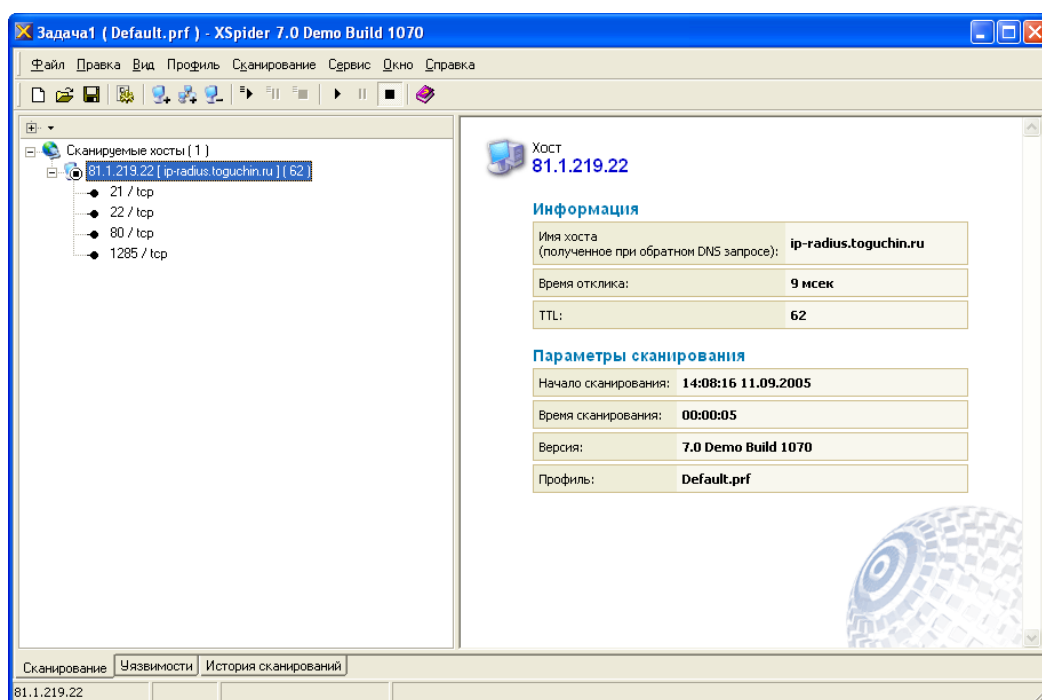


Рисунок 1.Главное окно сканера Xspider

4. Порядок выполнения работы.

Условия выполнения лабораторной работы. Данная работа должна выполняться в присутствии администратора компьютерного класса или уполномоченно-

го им лица, которому предоставляются права на осуществление следующих действий в операционных системах Windows XP– 7, работающих как в сетевом режиме, так и в одиночном режиме:

- 1) права на установку программного обеспечения;
- 2) права на работу как в составе рабочей группы или домена Windows, так и в составе локального администратора рабочей станции;
- 3) права на предоставление учетной записи учащимся, позволяющей установку ПО.

Лабораторная работа проводится в двух вариантах:

1. Автономный.

В компьютерном классе должны находиться не менее 2-х машин, объединенных в сеть. На первой устанавливается *сетевой сканер* или *межсетевой экран*. В случае установки МСЭ вторая машина используется для тестирования защиты первой от ICMP пакетов с помощью стандартной утилиты *ping*. При «автономном» тестировании сканера вторая машина будет использоваться в качестве исследуемого объекта.

2. Совместный.

В компьютерном классе должны находиться также не менее 2-х машин, объединенных в сеть. На части из них устанавливается *сканер*, на остальных – МСЭ. При этом для проверки защиты рабочей станции от ICMP пакетов с помощью МСЭ (а также для тестирования сканера) будет использоваться сетевой сканер.

Порядок работы

Работа будет проходить в два этапа. Первый этап предназначен для изучения работы XSpider, Outpost и WindowsXP в «автономном» режиме. Второй этап – для изучения работы в совместном режиме. На каждом этапе студенты делятся на две группы, одна из которых будет работать с МСЭ, вторая – со сканером или псевдосканером (утилитой ping).

Действия, общие для двух этапов:

- 1) Взять из папки файлы (предоставляется преподавателем) установки сканера XSpider и МСЭ Agnitum Outpost;
- 2) На каждом рабочем месте выполнить установку сканера и МСЭ;
- 3) При установке Outpost соглашаться со всеми вопросами. По окончании установки – перезагрузить машину;
- 4) Перед началом работы перевести установленный МСЭ в режим разрешения. Открыть Outpost -> меню «Параметры» -> «Политики» -> выбрать режим «Разрешать»;
- 5) Узнать имя и IP-адрес своего рабочего компьютера: «Пуск» -> «Выполнить» -> “cmd” -> “ipconfig /all”;

Этап 1. Автономный режим. Каждый студент из группы 1 должен работать в паре со студентом из группы 2.

Группа 1:

- 1) Запустить пинг компьютера-соседа из группы 2: «Пуск» -> «Выполнить» -> “cmd” -> “ping ip-addr -t”; (утилита ping располагается в C:\windows\system32)
- 2) Смотреть на ответные пинг-пакеты.
- 3) Фиксировать моменты, когда ответные пакеты пропадают и появляются.
- 4) Сравнить данные с моментами изменения конфигурации МСЭ напарником

Группа 2:

- 1) Открыть Outpost;
- 2) Зайти в меню «Параметры» -> «Системные» -> «ICMP параметры» -> отключить/включить эхо-запросы и ответы;
- 3) Проверить состояние ответов на ping-запросы у напарника;
- 4) Повторить п.1-2 несколько раз.

Поменяться ролями и повторить вышеуказанные пункты.

Этап 2. Совместный режим. Каждый студент из группы 1 должен работать в паре со студентом из группы 2.

Группа 1:

1. Запустить утилиту сканирования сети XSpider;
2. В меню «Правка» выбрать «Добавить хост»;
3. Введите IP-адрес хоста напарника;
4. Узнать у напарника текущий режим работы МСЭ;

В меню «Сканирование» выберите «Старт все»;

Начнется попытка XSpider сканировать указанный хост. В случае, если на целевом хосте отключены ICMP-ответы, то сканирование происходить не будет без установки в XSpider специальной опции: меню «Профиль» -> «Редактировать текущий» -> «Поиск хостов» -> поставить галочку «Сканировать не отвечающие хосты».

Сбросить флаг «Сканировать не отвечающие хосты» для возврата XSpider в первоначальную конфигурацию.

Группа 2:

1. Открыть Outpost;
2. Зайти в меню «Параметры» -> «Системные» -> «ICMP параметры» -> отключить/включить эхо-запросы и ответы;
3. Проверить, как работает XSpider у напарника;

4. Повторить п.1-2 несколько раз для двух режимов XSSpider – требующего ICMP-ответа и не требующего.

Поменяться ролями и повторить вышеуказанные пункты.

Контрольные вопросы:

1. Опишите утилиту ping, методы и случаи ее применения.
2. Описать данные, полученные о компьютере с помощью XSSpider
3. Какого типа уязвимости были найдены?
4. Как можно предотвратить появление таких уязвимостей с помощью изученных средств?
5. Какие еще сканеры и МСЭ вы знаете? Какие между ними и изученными отличия?

Библиографический список

- 1) Партыка, Т. Л. Информационная безопасность [Текст] : учебное пособие для студентов учреждений среднего профессионального образования, обучающихся по специальностям информатики и вычислительной техники / Т. Л. Партыка, И. И. Попов. - 5-е изд., перераб. и доп. - Москва : ФОРУМ, 2016. - 431 с.
- 2) Баранова, Е. К. Информационная безопасность и защита информации [Текст] : учебное пособие для студентов, обучающихся по направлению "Прикладная информатика" / Е. К. Баранова, А. В. Бабаш. - 3-е изд., перераб. и доп. - Москва : РИОР : ИНФРА-М, 2016. - 321 с.
- 3) Федотова, Е.Л. Информационные технологии в науке и образовании [Текст] : учебное пособие для магистров, обучающихся по спец.: 552800 "Информатика и вычислительная техника", 540600 "Педагогика" / Е. Л. Федотова, А. А. Федотов. - Москва : ФОРУМ : ИНФРА-М, 2015. - 334 с.
- 4) Платонов, В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей [Текст] : учеб. пособие для студ. вузов, обуч. по спец. 090102 "Компьютерная безопасность", 090105 "Комплексное обеспечение информационной безопасности автоматизированных систем" : допущено УМО по образованию / В. В. Платонов. - М. : Академия, 2006. - 239 с.
- 5) Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей [Текст] : учеб. пособие для студ. учреждений среднего проф. образования, обуч. по спец. 2200 "Информатика и вычислительная техника" / В. Ф. Шаньгин. - М. : ФОРУМ : ИНФРА-М, 2008. - 415 с.