

Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

№ 7 (110)/2002

Анализ защищенности корпоративных автоматизированных систем



ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ

Анализ защищенности корпоративных автоматизированных систем

Александр Астахов
CISA

СОДЕРЖАНИЕ

Введение	3
Понятие защищенности АС	3
Нормативная база анализа защищенности.....	4
ISO 15408: Common Criteria for Information Technology Security Evaluation	
ISO 17799: Code of Practice for Information Security Management	
РД Гостехкомиссии России	
РД «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации»	
РД «АС. Защита от НСД к информации. Классификация АС и требования по защите информации»	
РД «СВТ. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации»	
Методика анализа защищенности.....	8
Исходные данные по обследуемой АС	
Анализ конфигурации средств защиты внешнего периметра АВС	
Методы тестирования системы защиты	
Средства анализа защищенности	11
Средства анализа параметров защиты (Security Benchmarks)	
Сетевые сканеры	
Средства контроля защищенности системного уровня	
Выводы.....	27
Ссылки на Web-ресурсы	

Введение

При создании информационной инфраструктуры корпоративной автоматизированной системы (АС) на базе современных компьютерных сетей неизбежно возникает вопрос о защищенности этой инфраструктуры от угроз безопасности информации. Насколько адекватны реализованные в АС механизмы безопасности существующим рискам? Можно ли доверять этой АС обработку (хранение, передачу) конфиденциальной информации? Имеются ли в текущей конфигурации АС ошибки, позволяющие потенциальным злоумышленникам обойти механизмы контроля доступа? Содержит ли установленное в АС программное обеспечение (ПО) уязвимости, которые могут быть использованы для взлома защиты? Как оценить уровень защищенности АС и как определить является ли он достаточным в данной среде функционирования? Какие контрмеры позволят реально повысить уровень защищенности АС? На какие критерии оценки защищенности следует ориентироваться и какие показатели защищенности использовать?

Таковыми вопросами рано или поздно задаются все специалисты ИТ-отделов, отделов защиты информации и других подразделений, отвечающих за эксплуатацию и сопровождение АС. Ответы на эти вопросы далеко неочевидны. Анализ защищенности АС от угроз безопасности информации — работа сложная. Умение оценивать и управлять рисками, знание типовых угроз и уязвимостей, критериев и подходов к анализу защищенности, владение методами анализа и специализированным инструментарием, знание различных программно-аппаратных платформ, используемых в современных компьютерных сетях — вот далеко не полный перечень профессиональных качеств, которыми должны обладать специалисты, проводящие работы по анализу защищенности АС.

Анализ защищенности является основным элементом таких взаимно пересекающихся видов работ как аттестация, аудит и обследование безопасности АС.

В настоящей статье обобщается существующий опыт проведения работ по анализу защищенности, дается обзор наиболее значимых стандартов в этой области, описываются методы анализа и используемый программный инструментарий.

Изложенный здесь подход не претендует ни на уникальность, ни на всеобъемлемость. С одной стороны, описываемые методы и программные средства анализа защищенности являются достаточно распространенными и уже давно с успехом используются на практике. С другой стороны, вполне возможно получение таких же (либо еще более убедительных) результатов с использованием других методов и средств.

Понятие защищенности АС

Защищенность является одним из важнейших показателей эффективности функционирования АС, наряду с такими показателями как *надежность, отказоустойчивость, производительность* и т. п.

Под защищенностью АС будем понимать степень адекватности реализованных в ней механизмов защиты информации существующим в данной среде функционирования рискам, связанным с осуществлением угроз безопасности информации.

Под угрозами безопасности информации традиционно понимается возможность нарушения таких свойств информации, как конфиденциальность, целостность и доступность.

На практике всегда существует большое количество неподдающихся точной оценке возможных путей осуществления угроз безопасности в отношении ресурсов АС. В идеале каждый путь осуществления угрозы должен быть перекрыт соответствующим механизмом защиты. Данное условие является **первым фактором**, определяю-

щим защищенность АС. Вторым фактором является прочность существующих механизмов защиты, характеризующаяся степенью сопротивляемости этих механизмов попыткам их обхода либо преодоления. Третьим фактором является величина ущерба, наносимого владельцу АС в случае успешного осуществления угроз безопасности.

На практике получение точных значений приведенных характеристик затруднено, т. к. понятия угрозы, ущерба и сопротивляемости механизма защиты трудноформализуемы. Например, оценку ущерба в результате НСД к информации политического и военного характера точно определить вообще невозможно, а определение вероятности осуществления угрозы не может базироваться на статистическом анализе. Оценка степени сопротивляемости механизмов защиты всегда является субъективной.

Описанный в настоящей работе подход позволяет получать качественные оценки уровня защищенности АС путем сопоставления свойств и параметров АС с многократно опробованными на практике и стандартизированными критериями оценки защищенности.

Нормативная база анализа защищенности

Наиболее значимыми нормативными документами в области информационной безопасности, определяющими критерии для оценки защищенности АС, и требования, предъявляемые к механизмам защиты, являются:

1. Общие критерии оценки безопасности ИТ (The Common Criteria for Information Technology Security Evaluation/ISO 15408).
2. Практические правила управления информационной безопасностью (Code of practice for Information Security Management/ISO 17799).

Кроме этого, в нашей стране первостепенное значение имеют Руководящие документы (РД) Гостехкомиссии России. В других странах их место занимают соответствующие национальные стандарты (там, где они есть).

ISO 15408: Common Criteria for Information Technology Security Evaluation

Наиболее полно критерии для оценки механизмов безопасности программно-технического уровня представлены в международном стандарте ISO 15408: Common Criteria for Information Technology Security Evaluation (Общие критерии оценки безопасности информационных технологий), принятом в 1999 году.

Общие критерии оценки безопасности информационных технологий (далее «Общие критерии») определяют функциональные требования безопасности (security functional requirements) и требования к адекватности реализации функций безопасности (security assurance requirements).

При проведении работ по анализу защищенности АС, а также средств вычислительной техники (СВТ) «Общие критерии» целесообразно использовать в качестве основных критериев, позволяющих оценить уровень защищенности АС (СВТ) с точки зрения полноты реализованных в ней функций безопасности и надежности реализации этих функций.

Хотя применимость «Общих критериев» ограничивается механизмами безопасности программно-технического уровня, в них содержится определенный набор требований к механизмам безопасности организационного уровня и требований по физической защите, которые непосред-

ственно связаны с описываемыми функциями безопасности.

Первая часть «Общих критериев» содержит определение общих понятий, концепции, описание модели и методики проведения оценки безопасности ИТ. В ней вводится понятийный аппарат, и определяются принципы формализации предметной области.

Требования к функциональности средств защиты приводятся во **второй части** «Общих критериев» и могут быть непосредственно использованы при анализе защищенности для оценки полноты реализованных в АС (СБТ) функций безопасности.

Третья часть «Общих критериев» содержит классы требований гарантированности оценки, включая класс требований по анализу уязвимостей средств и механизмов защиты под названием AVA: Vulnerability Assessment. Данный класс требований определяет методы, которые должны использоваться для предупреждения, выявления и ликвидации следующих типов уязвимостей:

- Наличие побочных каналов утечки информации;
- Ошибки в конфигурации либо неправильное использование системы, приводящее к переходу в небезопасное состояние;
- Недостаточная надежность (стойкость) механизмов безопасности, реализующих соответствующие функции безопасности;
- Наличие уязвимостей («дыр») в средствах защиты информации, дающих возможность пользователям получать НСД к информации в обход существующих механизмов защиты.

Соответствующие требования гарантированности оценки содержатся в следующих четырех семействах требований:

- Семейство AVA_CCA: Covert Channel Analysis (Анализ каналов утечки информации);
- Семейство AVA_MSU: Misuse (Ошибки в конфигурации либо неправильное использование системы, приводящее к переходу системы в небезопасное состояние);
- Семейство AVA_SOF: Strength of TOE Security Functions (Стойкость функций безопасности, обеспечиваемая их реализацией);
- Семейство AVA_VLA: Vulnerability Analysis (Анализ уязвимостей).

При проведении работ по аудиту безопасности перечисленные семейства требований могут использоваться в качестве руководства и критериев для анализа уязвимостей АС (СБТ).

ISO 17799: Code of Practice for Information Security Management

Наиболее полно критерии для оценки механизмов безопасности организационного уровня представлены в международном стандарте ISO 17799: Code of Practice for Information Security Management (Практические правила управления информационной безопасностью), принятом в 2000 году. ISO 17799 является ни чем иным, как международной версией британского стандарта BS 7799.

ISO 17799 содержит практические правила по управлению информационной безопасностью и может использоваться в качестве критериев для оценки механизмов безопасности организационного уровня, включая административные, процедурные и физические меры защиты.

Практические правила разбиты на следующие 10 разделов:

1. Политика безопасности;
2. Организация защиты;
3. Классификация ресурсов и их контроль;
4. Безопасность персонала;
5. Физическая безопасность;
6. Администрирование компьютерных систем и вычислительных сетей;
7. Управление доступом;
8. Разработка и сопровождение информационных систем;
9. Планирование бесперебойной работы организации;
10. Контроль выполнения требований политики безопасности.

В этих разделах содержится описание механизмов безопасности организационного уровня, реализуемых в настоящее время в правительственных и коммерческих организациях во многих странах мира.

Десять средств контроля, предлагаемых в ISO 17799 (они обозначены как ключевые), считаются особенно важными. **Под средствами контроля в данном контексте понимаются механизмы управления информационной безопасностью организации.**

При использовании некоторых из средств контроля, например, шифрования данных, может потребоваться оценка рисков, чтобы определить нужны ли они и каким образом их следует реализовывать. Для обеспечения более высокого уровня защиты особенно ценных ресурсов или оказания противодействия особенно серьезным угрозам безопасности в ряде случаев могут потребоваться более сильные средства контроля, которые выходят за рамки ISO 17799.

Десять ключевых средств контроля, перечисленные ниже, представляют собой либо обязательные требования, например, требования действующего законодательства, либо считаются основными структурными элементами информационной безопасности, например, обучение правилам безопасности. Эти средства контроля актуальны для всех организаций и сред функционирования АС и составляют основу системы управления информационной безопасностью. Они служат в качестве основного руководства для организаций, приступающих к реализации средств управления информационной безопасностью.

Ключевыми являются следующие средства контроля:

- Документ о политике информационной безопасности;
- Распределение обязанностей по обеспечению информационной безопасности;
- Обучение и подготовка персонала к поддержанию режима информационной безопасности;
- Уведомление о случаях нарушения защиты;
- Средства защиты от вирусов;
- Планирование бесперебойной работы организации;
- Контроль над копированием программного обеспечения, защищенного законом об авторском праве;
- Защита документации организации;
- Защита данных;
- Контроль соответствия политике безопасности.

Процедура аудита безопасности АС включает в себя проверку наличия перечисленных ключевых средств контроля, оценку полноты и правильности их реализации, а также анализ их адекватности рискам, существующим в данной среде функционирования. Составной частью работ по аудиту безопасности АС также является анализ и управление рисками.

РД Гостехкомиссии России

В общем случае в нашей стране при решении задач защиты информации должно обеспечиваться соблюдение следующих указов Президента, федеральных законов, постановлений Правительства Российской Федерации, РД Гостехкомиссии России и других нормативных документов:

- Доктрина информационной безопасности Российской Федерации;
- Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфи-

денциального характера»;

- Закон Российской Федерации «Об информации, информатизации и защите информации» от 20.02.95 N 24-ФЗ;
- Закон Российской Федерации «О связи» от 16.02.95 N 15-ФЗ;
- Закон Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных» от 23.09.92 N3523-1;
- Закон Российской Федерации «Об участии в международном информационном обмене» от 04.07.96 N 85-ФЗ;
- Постановление Правительства Российской Федерации «О лицензировании отдельных видов деятельности» от 16.09.98г;
- Закон Российской Федерации «О государственной тайне» от 21 июля 1993 г;
- ГОСТ Р 51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении».
- Руководящий документ «Положение по аттестации объектов информатизации по требованиям безопасности информации» (Утверждено Председателем Гостехкомиссии России 25.11.1994 г.);
- Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация АС и требования к защите информации» (Гостехкомиссия России, 1997);
- «Положение о сертификации средств защиты информации по требованиям безопасности информации» (Постановление Правительства РФ № 608, 1995 г.);
- Руководящий документ «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации» (Гостехкомиссия России, 1992 г.);
- Руководящий документ «Концепция защиты средств вычислительной техники от НСД к информации» (Гостехкомиссия России, 1992 г.);
- Руководящий документ «Защита от НСД к информации. Термины и определения» (Гостехкомиссия России, 1992 г.);
- Руководящий документ «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в АС и СВТ» (Гостехкомиссия России, 1992 г.);
- Руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели за-

щищенности от НСД к информации» (Гостехкомиссия России, 1997 г.);

- Руководящий документ «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей» (Гостехкомиссия России, 1999 г.);
- Руководящий документ «Специальные требования и рекомендации по технической защите конфиденциальной информации» (Гостехкомиссия России, 2001г.).

РД Гостехкомиссии России составляют основу нормативной базы в области защиты от НСД к информации в нашей стране. Наиболее значимые из них, определяющие критерии для оценки защищенности АС (СВТ), рассматриваются ниже.

Критерии для оценки механизмов защиты программно-технического уровня, используемые при анализе защищенности АС и СВТ, выражены в РД Гостехкомиссии РФ «АС. Защита от НСД к информации. Классификация АС и требования по защите информации» и «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации».

РД «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации»

РД «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации» устанавливает классификацию СВТ по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований. (Основным «источником вдохновения» при разработке этого документа послужила знаменитая американская «Оранжевая книга»). Устанавливается семь классов защищенности СВТ от НСД к информации. Самый низкий класс седьмой, самый высокий — первый. Классы подразделяются на четыре группы, отличающиеся уровнем защиты:

- **Первая группа** содержит только один седьмой класс, к которому относят все СВТ, не удовлетворяющие требованиям более высоких классов;
- **Вторая группа** характеризуется дискреционной защитой и содержит шестой и пятый классы;
- **Третья группа** характеризуется мандатной защитой и содержит четвертый, третий и второй классы;

- **Четвертая группа** характеризуется верифицированной защитой и содержит только первый класс.

РД «АС. Защита от НСД к информации. Классификация АС и требования по защите информации»

РД «АС. Защита от НСД к информации. Классификация АС и требования по защите информации» устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов. К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

- наличие в АС информации различного уровня конфиденциальности;
- уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
- режим обработки данных в АС — коллективный или индивидуальный.

Устанавливается девять классов защищенности АС от НСД к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности и конфиденциальности информации и, следовательно, иерархия классов защищенности АС.

РД «СВТ. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации»

При анализе системы защиты внешнего периметра корпоративной сети в качестве основных критериев целесообразно использовать РД «СВТ. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации». Данный документ определяет показатели защищенности межсетевых экранов (МЭ). Каждый показатель защищенности представляет собой набор требований безопасности, характеризующих определенную область функционирования МЭ. Всего выделяется пять показателей защищенности:

1. Управление доступом;
2. Идентификация и аутентификация;
3. Регистрация событий и оповещение;
4. Контроль целостности;
5. Восстановление работоспособности.

На основании показателей защищенности определяются следующие пять классов защищенности МЭ:

1. Простейшие фильтрующие маршрутизаторы — **5 класс**;
2. Пакетные фильтры сетевого уровня — **4 класс**;
3. Простейшие МЭ прикладного уровня — **3 класс**;
4. МЭ базового уровня — **2 класс**;
5. Продвинутое МЭ — **1 класс**.

МЭ первого класса защищенности могут использоваться в АС класса 1А, обрабатывающих информацию «Особой важности». Второму классу защищенности МЭ соответствует класс защищенности АС 1Б, предназначенный для обработки «совершенно секретной» информации и т.п.

Методика анализа защищенности

В настоящее время не существует каких-либо стандартизированных методик анализа защищенности АС, поэтому в конкретных ситуациях алгоритмы действий аудиторов могут существенно различаться. Однако типовую методику анализа защищенности корпоративной сети предложить все-таки возможно. И хотя данная методика не претендует на всеобщность, ее эффективность многократно проверена на практике.

Типовая методика включает использование следующих методов:

- Изучение исходных данных по АС;
- Оценка рисков, связанных с осуществлением угроз безопасности в отношении ресурсов АС;
- Анализ механизмов безопасности организационного уровня, политики безопасности организации и организационно-распорядительной документации по обеспечению режима информационной безопасности и оценка их соответствия требованиям существующих нормативных документов, а также их адекватности существующим рискам;
- Ручной анализ конфигурационных файлов маршрутизаторов, МЭ и прокси-серверов, осуществляющих управление межсетевыми взаимодействиями, почтовых и DNS серверов, а также других критических элементов сетевой инфраструктуры;
- Сканирование внешних сетевых адресов ЛВС из сети Интернет;
- Сканирование ресурсов ЛВС изнутри;
- Анализ конфигурации серверов и рабочих станций ЛВС при помощи специализированных программных средств.

Перечисленные методы исследования предполагают использование как активного, так и пассивного тестирования системы защиты. Активное тестирование системы защиты заключается в эмуляции действий потенциального злоумышленника по преодолению механизмов защиты. Пассивное тестирование предполагает анализ конфигурации ОС и приложений по шаблонам с использованием списков проверки. Тестирование может производиться вручную либо с использованием специализированных программных средств.

Исходные данные по обследуемой АС

В соответствии с требованиями РД Гостехкомиссии при проведении работ по аттестации безопасности АС, включающих в себя предварительное

обследование и анализ защищенности объекта информатизации, заказчиком работ должны быть предоставлены следующие исходные данные:

1. Полное и точное наименование объекта информатизации и его назначение.
2. Характер (научно-техническая, экономическая, производственная, финансовая, военная, политическая) информации и уровень секретности (конфиденциальности) обрабатываемой информации определен (в соответствии с какими перечнями (государственным, отраслевым, ведомственным, предприятия).
3. Организационная структура объекта информатизации.
4. Перечень помещений, состав комплекса технических средств (основных и вспомогательных), входящих в объект информатизации, в которых (на которых) обрабатывается указанная информация.
5. Особенности и схема расположения объекта информатизации с указанием границ контролируемой зоны.
6. Структура программного обеспечения (общесистемного и прикладного), используемого на аттестуемом объекте информатизации и предназначенного для обработки защищаемой информации, используемые протоколы обмена информацией.
7. Общая функциональная схема объекта информатизации, включая схему информационных потоков и режимы обработки защищаемой информации.
8. Наличие и характер взаимодействия с другими объектами информатизации.
9. Состав и структура системы защиты информации на аттестуемом объекте информатизации.
10. Перечень технических и программных средств в защищенном исполнении, средств защиты и контроля, используемых на аттестуемом объекте информатизации и имеющих соответствующий сертификат, предписание на эксплуатацию.
11. Сведения о разработчиках системы защиты информации, наличие у сторонних разработчиков (по отношению к предприятию, на котором расположен аттестуемый объект информатизации) лицензий на проведение подобных работ.
12. Наличие на объекте информатизации (на предприятии, на котором расположен объект информатизации) службы безопасности информации, службы администратора (автоматизированной системы, сети, баз данных).
13. Наличие и основные характеристики физической защиты объекта информатизации

(помещений, где обрабатывается защищаемая информация и хранятся информационные носители).

14. Наличие и готовность проектной и эксплуатационной документации на объект информатизации **и другие исходные данные по аттестуемому объекту информатизации, влияющие на безопасность информации.**

Опыт показывает, что перечисленных исходных данных явно недостаточно для выполнения работ по анализу защищенности АС, и приведенный в РД Гостехкомиссии список нуждается в расширении и конкретизации. Пункт 14 приведенного списка предполагает предоставление других исходных данных по объекту информатизации, влияющих на безопасность информации. Как раз эти «дополнительные» данные и являются наиболее значимыми для оценки текущего положения дел с обеспечением безопасности АС. Их список включает следующие виды документов:

Дополнительная документация:

1. Нормативно-распорядительная документация по проведению регламентных работ.
2. Нормативно-распорядительная документация по обеспечению политики безопасности.
3. Должностные инструкции для администраторов, инженеров технической поддержки, службы безопасности.
4. Процедуры и планы предотвращения и реагирования на попытки НСД к информационным ресурсам.
5. Схема топологии корпоративной сети с указанием IP-адресов и структурная схема.
6. Данные по структуре информационных ресурсов с указанием степени критичности или конфиденциальности каждого ресурса.
7. Размещение информационных ресурсов в корпоративной сети.
8. Схема организационной структуры пользователей.
9. Схема организационной структуры обслуживающих подразделений.
10. Схемы размещения линий передачи данных.
11. Схемы и характеристики систем электропитания и заземления объектов АС.
12. Данные по используемым системам сетевого управления и мониторинга.

Проектная документация:

1. Функциональные схемы.
2. Описание автоматизированных функций.
3. Описание основных технических решений.

Эксплуатационная документация:

Руководства пользователей и администраторов используемых программных и технических средств защиты информации (СЗИ) (в случае необходимости).

Анализ конфигурации средств защиты внешнего периметра АВС

При анализе конфигурации средств защиты внешнего периметра АВС и управления межсетевыми взаимодействиями особое внимание обращается на следующие аспекты, определяемые их конфигурацией:

- Настройка правил разграничения доступа (правил фильтрации сетевых пакетов) на МЭ и маршрутизаторах;
- Используемые схемы и настройка параметров аутентификации;
- Настройка параметров системы регистрации событий;
- Использование механизмов, обеспечивающих сокрытие топологии защищаемой сети, включающих в себя трансляцию сетевых адресов (NAT), маскердинг и использование системы split DNS;
- Настройка механизмов оповещения об атаках и реагирования;
- Наличие и работоспособность средств контроля целостности;
- Версии используемого ПО и наличие установленных пакетов программных коррекций.

Методы тестирования системы защиты

Тестирование системы защиты АС проводится с целью проверки эффективности используемых в ней механизмов защиты, их устойчивости в отношении возможных атак, а также с целью поиска уязвимостей в защите. Традиционно используются два основных метода тестирования:

- тестирование по методу «черного ящика»;
- тестирование по методу «белого ящика».

Тестирование по методу «черного ящика» предполагает отсутствие у тестирующей стороны каких-либо специальных знаний о конфигурации и внутренней структуре объекта испытаний. При этом против объекта испытаний реализуются все известные типы атак и проверяется устойчивость системы защиты в отношении этих атак. Используемые методы тестирования эмулируют действия потенциальных злоумышленников, пытающихся взломать систему защиты. Основным средством тестирования в данном случае являются се-

тевые сканеры, располагающие базами данных известных уязвимостей.

Метод «белого ящика» предполагает составление программы тестирования на основании знаний о структуре и конфигурации объекта испытаний. В ходе тестирования проверяются наличие и работоспособность механизмов безопасности, соответствие состава и конфигурации системы защиты требованиям безопасности и существующим рисками. Выводы о наличии уязвимостей делаются на основании анализа конфигурации используемых средств защиты и системного ПО, а затем проверяются на практике. Основным инструментом анализа в данном случае являются программные агенты средств анализа защищенности системного уровня, рассматриваемые ниже.

Средства анализа защищенности

Арсенал программных средств, используемых для анализа защищенности АС достаточно широк. Причем во многих случаях свободно распространяемые программные продукты ничем не уступают коммерческим. Достаточно сравнить некоммерческий сканер NESSUS с его коммерческими аналогами.

Удобным и мощным средством анализа защищенности ОС является рассматриваемый ниже, свободно распространяемый программный продукт CIS Windows 2000 Level I Scoring Tool, а также аналогичные средства разработчиков ОС, предоставляемые бесплатно, такие как ASET для ОС Solaris или MBSA (Microsoft Security Baseline Analyzer) для ОС Windows 2000.

Одним из методов автоматизации процессов анализа и контроля защищенности распределенных компьютерных систем является использование технологии интеллектуальных программных агентов. Система защиты строится на архитектуре консоль/менеджер/агент. На каждую из контролируемых систем устанавливается программный агент, который и выполняет соответствующие настройки ПО и проверяет их правильность, контролирует целостность файлов, своевременность установки пакетов программных коррекций, а также выполняет другие полезные задачи по контролю защищенности АС. (Управление агентами осуществляется по сети программной менеджером.) Менеджеры являются центральными компонентами подобных систем. Они посылают управляющие команды всем агентам контролируемого ими домена и сохраняют все данные, полученные от агентов в центральной базе данных. Администратор управляет менеджерами при помощи графической консоли, позволяющей выбирать, настраивать и создавать политики безопасности, анализировать изменения состояния системы, осуществлять ранжирование уязвимостей и т. п. Все взаимодействия между агентами, менеджерами и управляющей консолью осуществляются по защищенному клиент-серверному протоколу. Такой подход был использован при построении комплексной системы управления безопасностью организации Symantec ESM.

Другим широко используемым методом анализа защищенности является активное тестирование механизмов защиты путем эмуляции действий злоумышленника по осуществлению попыток сетевого вторжения в АС. Для этих целей применяются сетевые сканеры, эмулирующие дейст-

вия потенциальных нарушителей. В основе работы сетевых сканеров лежит база данных, содержащая описание известных уязвимостей ОС, МЭ, маршрутизаторов и сетевых сервисов, а также алгоритмов осуществления попыток вторжения (сценариев атак). Рассматриваемые ниже сетевые сканеры Nessus и Symantec NetRecon являются достойными представителями данного класса программных средств анализа защищенности.

Таким образом, программные средства анализа защищенности условно можно разделить на два класса. Первый класс, к которому принадлежат сетевые сканеры, иногда называют средствами анализа защищенности сетевого уровня. Второй класс, к которому относятся все остальные рассмотренные здесь средства, иногда называют средствами анализа защищенности системного уровня. Данные классы средств имеют свои достоинства и недостатки, а на практике взаимно дополняют друг друга.

Для функционирования сетевого сканера необходим только один компьютер, имеющий сетевой доступ к анализируемым системам, поэтому в отличие от продуктов, построенных на технологии программных агентов, нет необходимости устанавливать в каждой анализируемой системе своего агента (своего для каждой ОС).

К недостаткам сетевых сканеров можно отнести большие временные затраты, необходимые для сканирования всех сетевых компьютеров из одной системы, и создание большой нагрузки на сеть. Кроме того, в общем случае трудно отличить сеанс сканирования от действительных попыток осуществления атак. Сетевыми сканерами также с успехом пользуются злоумышленники.

Системы анализа защищенности, построенные на интеллектуальных программных агентах, являются потенциально более мощным средством, чем сетевые сканеры. Однако, несмотря на все свои достоинства, использование программных агентов не может заменить сетевого сканирования, поэтому эти средства лучше применять совместно. Кроме того, сканеры являются более простым, доступным, дешевым и, во многих случаях, более эффективным средством анализа защищенности.

Средства анализа параметров защиты (Security Benchmarks)

Уровень защищенности компьютерных систем от угроз безопасности определяется многими факторами. При этом одним из определяющих факторов является адекватность конфигурации системного и прикладного ПО, средств защиты инфор-

мации и активного сетевого оборудования существующим рискам. Перечисленные компоненты АС имеют сотни параметров, значения которых оказывают влияние на защищенности системы, что делает их ручной анализ трудновыполнимой задачей. Поэтому в современных АС для анализа конфигурационных параметров системного и прикладного ПО, технических средств и средств защиты информации зачастую используются специализированные программные средства.

Анализ параметров защиты осуществляется по шаблонам, содержащим списки параметров и их значений, которые должны быть установлены для обеспечения необходимого уровня защищенности. Различные шаблоны определяют конфигурации для различных программно-технических средств.

Относительно коммерческих корпоративных сетей, подключенных к сети Интернет, можно говорить о некотором базовом уровне защищенности, который в большинстве случаев можно признать достаточным. Разработка спецификаций (шаблонов) для конфигурации наиболее распространенных системных программных средств, позволяющих обеспечить базовый уровень защищенности, в настоящее время осуществляется представителями международного сообщества в лице организаций и частных лиц, профессионально занимающихся вопросами информационной безопасности и аудита АС, под эгидой международной организации Центр Безопасности Интернет (Center of Internet Security). На данный момент закончены, либо находятся в разработке следующие спецификации (Security Benchmarks):

- **Solaris** (Level-1)
- **Windows 2000** (Level-1)
- **CISCO IOS Router** (Level-1/Level-2)
- **Linux** (Level-1)
- **HP-UX** (Level-1)
- **AIX** (Level-1)
- **Check Point FW-1/VPN-1** (Level-2)
- **Apache Web Server** (Level-2)
- **Windows NT** (Level-1)
- **Windows 2000 Bastion Host** (Level-2)
- **Windows 2000 Workstation** (Level-2)
- **Windows IIS5 Web Server** (Level-2)

В приведенном списке спецификации первого уровня (Level-1) определяют базовый (минимальный) уровень защиты, который требуется обеспечить для большинства систем, имеющих подключения к Интернет. Спецификации второго уровня (Level-2) определяют продвинутый уровень защиты, необходимый для систем, в которых предъявляются повышенные требования по безопасности.

Перечисленные спецификации являются результатом обобщения мирового опыта обеспечения информационной безопасности.

Для анализа конфигурации компонентов АС на соответствие этим спецификациям используются специализированные тестовые программные средства (CIS-certified scoring tools).

В качестве примера рассмотрим спецификацию базового уровня защиты для ОС MS Windows 2000 и соответствующий программный инструментарий для анализа конфигурации ОС.

Windows 2000 Security Benchmark

CIS Windows 2000 Security Benchmark является программой, позволяющей осуществлять проверку соответствия настроек ОС MS Windows 2000 минимальному набору требований безопасности, определяющих базовый уровень защищенности, который в общем случае является достаточным для коммерческих систем. Требования к базовому уровню защищенности ОС Windows 2000 были выработаны в результате обобщения практического опыта. Свой вклад в разработку этих спецификаций внесли такие организации, как SANS Institute, Center for Internet Security, US NSA и US DoD.

В состав инструментария CIS Windows 2000 Security Benchmark входит шаблон политики безопасности (cis.inf), позволяющий осуществлять сравнение текущих настроек ОС с эталонными и производить автоматическую переконфигурацию ОС для обеспечения соответствия базовому уровню защищенности, задаваемому данным шаблоном.

CIS Windows 2000 Security Benchmark позволяет осуществлять количественную оценку текущего уровня защищенности анализируемой ОС по 10-бальной шкале. Уровень 0 соответствует минимальному уровню защищенности (после установки ОС ее уровень защищенности как раз и будет равен 0). Уровень 10 является максимальным и означает полное соответствие анализируемой системы требованиям базового уровня защищенности для коммерческих систем.

Все проверки, выполняемые при анализе системы, делятся на 3 категории:

1. Service Packs and Hotfixes (Пакеты обновлений и программные коррективы);
2. Account and Audit Policies (Политика управления пользовательскими бюджетами и политика аудита безопасности);
3. Security Options (Опции безопасности).

Первая категория включает проверку установки последних пакетов обновлений (Service Packs) и текущих программных коррекций (Hotfixes) от Microsoft.

Рис. 1. Windows 2000 Level 1 Security Scoring Tool

Вторая категория включает проверки параметров политики безопасности по управлению пользовательскими бюджетами (включая политику управления паролями) и осуществлению аудита безопасности.

Третья категория включает проверки всех остальных параметров безопасности ОС, не относящиеся к первым двум категориям, включая запрет анонимных сессий (NULL sessions), правила выделения внешних устройств, параметры защиты протокола TCP/IP, установки прав доступа к системным объектам и т.п.

Для проверки наличия установленных текущих программных коррекций используется утилита MS Network Security Hotfix Checker (HFNetCheck), которая автоматически скачивается с сайта Microsoft и устанавливается во время осуществления проверок. Подробную информа-

цию об этой утилите можно получить по адресу: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/hfnetchk.asp>.

Используя список недостающих программных коррекций (Hotfixes), сгенерированный утилитой HFNetCheck, следует осуществить поиск и установку этих коррекций. Для этого используется Microsoft Security Bulletin Search Web-сайт: (<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/Default.asp>).

Для осуществления мониторинга установки необходимых программных коррекций, помимо утилит Microsoft, можно использовать более мощные средства третьих фирм, например, программу UpdateExpert, разработки St. Bernard Software (www.stbernard.com).

Для настройки ОС с использованием шаблона CIS.INF используется Security Configuration and Analysis Snap-In — стандартное средство ОС



Рис. 2. Список недостающих программных коррекций

Windows 2000 для осуществления анализа и настройки параметров безопасности ОС.

Порядок подключения данного средства к MMC (Microsoft Management Console), загрузки шаблона, его использования для анализа и изменения конфигурации ОС описывается в «CIS Win2K Level 1 Implementation Guide», входящем в комплект программной документации, которая содержит также подробное описание всех производимых проверок и соответствующих параметров настройки ОС.

Сетевые сканеры

Основным фактором, определяющим защищенность АС от угроз безопасности, является наличие в АС уязвимостей защиты. Уязвимости защиты могут быть обусловлены как ошибками в конфигурации компонентов АС, так и другими причинами, в число которых входят ошибки и программные закладки в коде ПО, отсутствие механизмов безопасности, их неправильное использование, либо их

неадекватность существующим рискам, а также уязвимости, обусловленные человеческим фактором. Наличие уязвимостей в системе защиты АС, в конечном счете, приводит к успешному осуществлению атак, использующих эти уязвимости.

Сетевые сканеры являются, пожалуй, наиболее доступными и широко используемыми средствами анализа защищенности. Основной принцип их функционирования заключается в эмуляции действий потенциального злоумышленника по осуществлению сетевых атак. Поиск уязвимостей путем имитации возможных атак является одним из наиболее эффективных способов анализа защищенности АС, который дополняет результаты анализа конфигурации по шаблонам, выполняемый локально с использованием шаблонов (списков проверки). Сканер является необходимым инструментом в арсенале любого администратора либо аудитора безопасности АС.

Современные сканеры способны обнаруживать сотни уязвимостей сетевых ресурсов, представляющих те или иные виды сетевых сервисов. Их

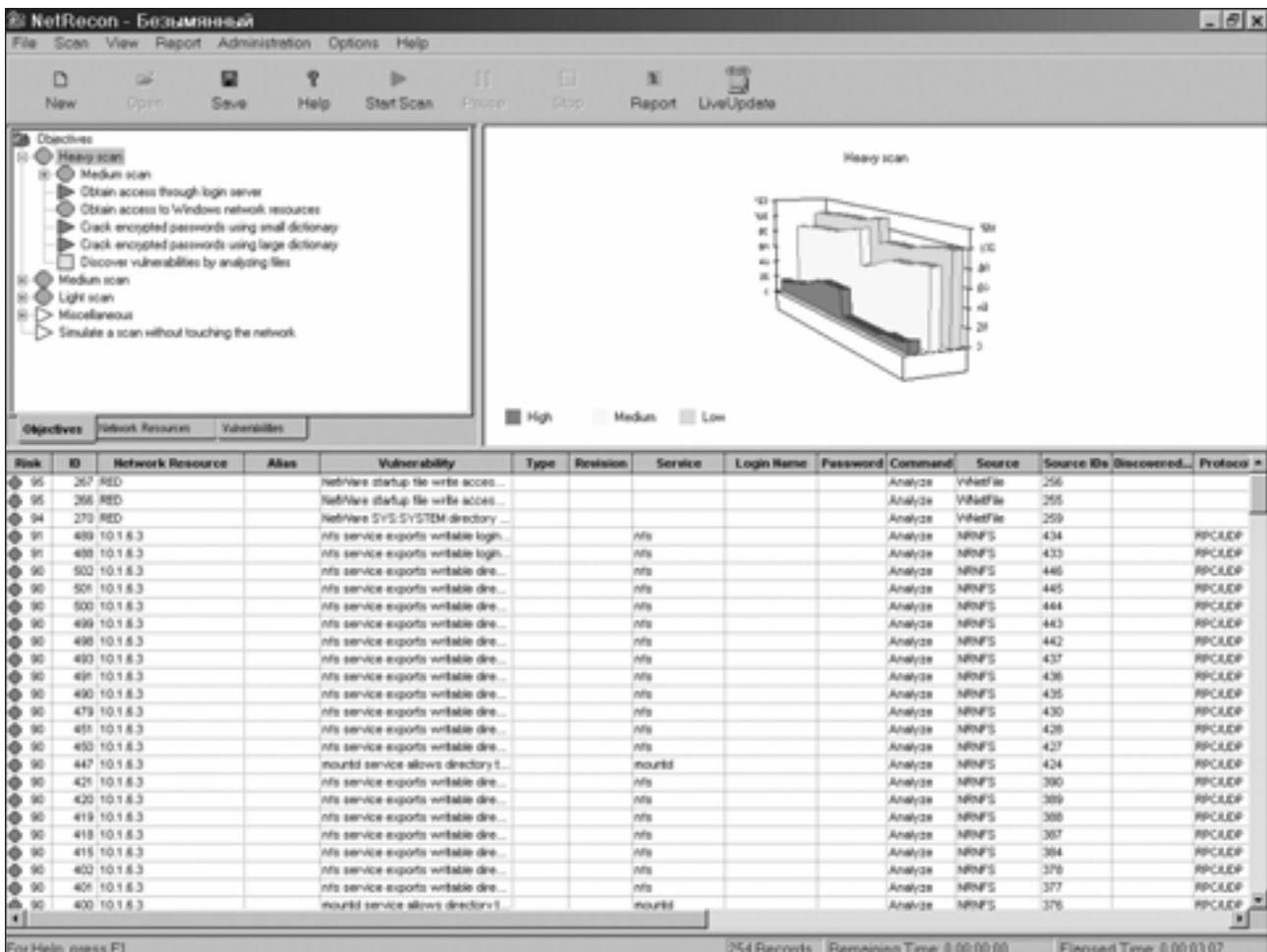


Рис. 3. Сетевой сканер NetRecon

предшественниками считаются сканеры телефонных номеров (war dialers), использовавшиеся с начала 80-х и не потерявшие актуальности по сей день. Первые сетевые сканеры представляли собой простейшие сценарии на языке Shell, сканировавшие различные TCP-порты. Сегодня они превратились в зрелые программные продукты, реализующие множество различных сценариев сканирования.

Современный сетевой сканер выполняет четыре основные задачи:

- Идентификацию доступных сетевых ресурсов;
- Идентификацию доступных сетевых сервисов;
- Идентификацию имеющихся уязвимостей сетевых сервисов;
- Выдачу рекомендаций по устранению уязвимостей.

В функциональность сетевого сканера не входит выдача рекомендаций по использованию найденных уязвимостей для реализации атак на сетевые ресурсы. Возможности сканера по анализу уязвимостей ограничены той информацией, кото-

рую могут предоставить ему доступные сетевые сервисы.

Принцип работы сканера заключается в моделировании действий злоумышленника, производящего анализ сети при помощи стандартных сетевых утилит, таких как host, showmount, traceroute, rusers, finger, ping и т. п. При этом используются известные уязвимости сетевых сервисов, сетевых протоколов и ОС для осуществления удаленных атак на системные ресурсы и осуществляется документирование удачных попыток.

В настоящее время существует большое количество как коммерческих, так и свободно распространяемых сканеров, как универсальных, так и специализированных, предназначенных для выявления только определенного класса уязвимостей. Многие из них можно найти в сети Интернет. Число уязвимостей в базах данных современных сканеров медленно, но уверенно приближается к 1000.

Одним из наиболее продвинутых коммерческих продуктов этого класса является сетевой сканер NetRecon компании Symantec, база дан-

ных которого содержит около 800 уязвимостей UNIX, Windows и NetWare систем и постоянно обновляется через Web. Рассмотрение его свойств позволит составить представление о всех продуктах этого класса.

Сетевой сканер NetRecon

Сетевой сканер NetRecon является инструментом администратора безопасности, предназначенным для исследования структуры сетей и сетевых сервисов и анализа защищенности сетевых сред. NetRecon позволяет осуществлять поиск уязвимостей в сетевых сервисах, ОС, МЭ, маршрутизаторах и других сетевых компонентах. Например, NetRecon позволяет находить уязвимости в таких сетевых сервисах, как ftp, telnet, DNS, электронная почта, Web-сервер и др. При этом проверяются версии и конфигурации сервисов, их защищенность от сетевых угроз и устойчивость к попыткам проникновения. Для поиска уязвимостей используются как стандартные средства тестирования и сбора информации о конфигурации и функционировании сети, так и специальные средства, которые реализуют алгоритмы, эмулирующие действия злоумышленника по осуществлению сетевых атак.

Программа работает в среде ОС Windows NT и имеет удобный графический интерфейс, позволяющий определять параметры сканирования, наблюдать за ходом сканирования, генерировать и просматривать отчеты о результатах сканирования. Результаты отображаются в графической и в табличной форме в реальном масштабе времени.

Создаваемые NetRecon отчеты содержат подробную информацию о найденных уязвимостях, включая слабость паролей пользователей, подверженность определенных сервисов угрозам отказа в обслуживании, уязвимые для сетевых атак конфигурации ОС и многие другие. Наряду с сообщениями о найденных уязвимостях и их описаниями, приводятся рекомендации по их устранению. Отчет о результатах сканирования позволяет наметить план мероприятий по устранению выявленных недостатков.

Для генерации отчетов в NetRecon используется ПО Crystal Report, предоставляющее удобные средства для просмотра отчетов и их экспорта во все популярные форматы представления данных. Найденные уязвимости ранжируются, при этом каждой из них присваивается числовой рейтинг, что позволяет отсортировать их по степени критичности для облегчения последующего анализа результатов сканирования.

Пример описания уязвимости в отчете, сгенерированном сканером NetRecon, приведен на

рис. 5. В NetRecon используется следующий формат описания уязвимости (который, однако, является общим и для всех остальных сетевых сканеров):

- **Vulnerability Name** (Название уязвимости);
- **Risk** (Уровень риска);
- **Description** (Описание уязвимости);
- **Solution** (Способы ликвидации уязвимости);
- **Additional Information** (Дополнительная информация);
- **Links** (Ссылки на источники информации о данной уязвимости);
- **# of Network Resources** (Кол-во сетевых ресурсов, подверженных данной уязвимости);
- **Network Resource** (Список сетевых ресурсов).

NetRecon самостоятельно определяет конфигурацию сети и позволяет выбрать сетевые ресурсы для сканирования. Может осуществляться параллельное сканирование всех сетевых ресурсов, сканирование по диапазону сетевых адресов, сканирование отдельных систем или подсетей. Сеанс сканирования может включать в себя все виды проверок либо отдельные проверки по выбору пользователя. Глубина сканирования определяется продолжительностью сеанса сканирования, которая задается пользователем. Например, проверки, связанные с подбором пользовательских паролей по словарю, сопряжены с существенными временными затратами и не могут быть завершены в течение короткого сеанса сканирования.

Для поиска сетевых уязвимостей в NetRecon используется запатентованная технология UltraScan. Производимые NetRecon проверки тесно взаимосвязаны и результаты одной проверки используются для выполнения другой. Как и в случае реальных атак, в технологии UltraScan информация об обнаруженных уязвимостях используется для выявления других связанных с ними уязвимостей. Например, если NetRecon удалось получить доступ к файлу, содержащему пароли пользователей, и расшифровать несколько паролей, то эти пароли будут использованы для имитации атак на другие системы, входящие в состав сети.

NetRecon дает возможность пользователю отслеживать путь поиска уязвимости, представляющий собой последовательность проверок, производимых NetRecon, которая привела к выявлению данной уязвимости. Путь поиска уязвимости позволяет проследить действия возможного нарушителя, осуществляющего атаку на сетевые ресурсы.

Используемая NetRecon база данных содержит описание известных уязвимостей и сценариев атак. Она регулярно пополняется новыми данными. Обновление этой базы данных производит-

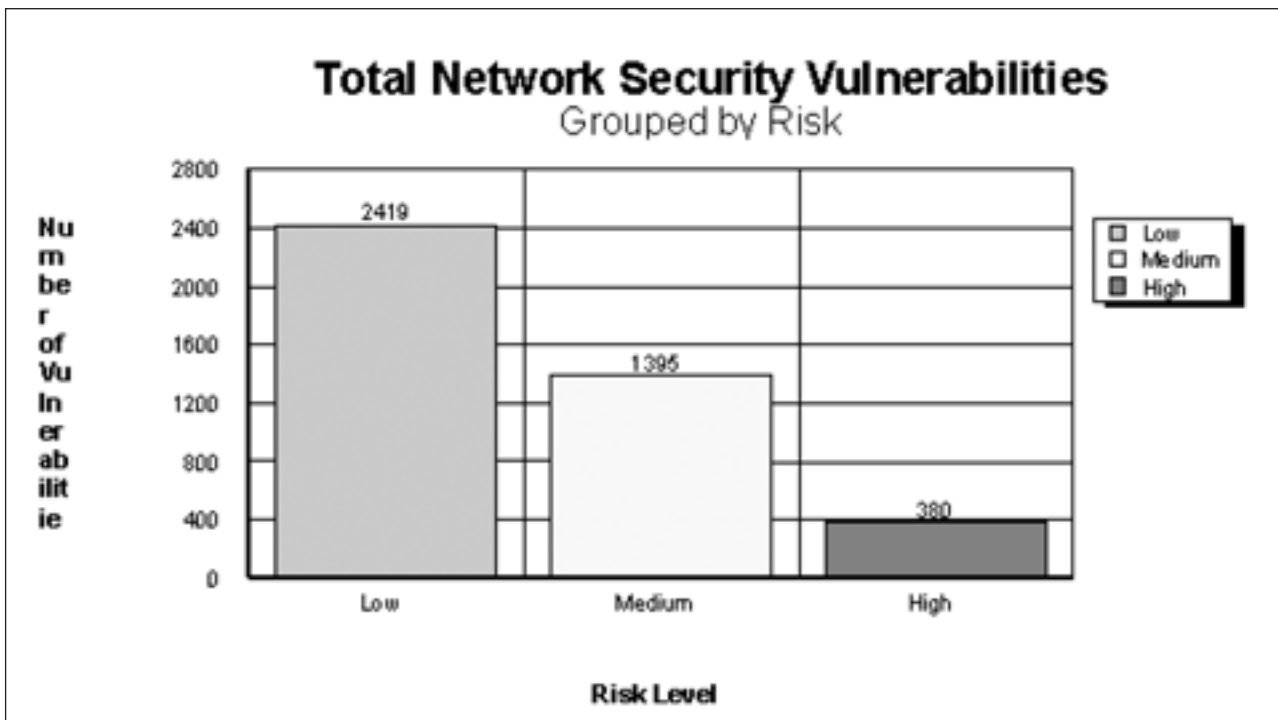


Рис. 4. Суммарное количество уязвимостей, обнаруженных сканером NetRecon

Vulnerability Name: Site Server showcode.asp allows remote file read access
Risk: 93

Description: Microsoft Site Server and Internet Information Server include tools that allow web site visitors to view selected files on the server. These are installed by default with Site Server, but must be explicitly installed with IIS. These tools are provided to allow users to view the source code of sample files as a learning exercise, and are not intended to be deployed on production web servers. The underlying problem in this vulnerability is that the tools do not restrict which files a web site visitor can view.

Solution: Customers should take the following steps to eliminate the vulnerability on their web servers:

Unless the affected file viewers are specifically required on the web site, they should be removed. The following file viewers are affected: ViewCode.asp, ShowCode.asp, CodeRw.asp and Winmtp.exe. Depending on the specific installation, not all of these files may be present on a server. Likewise, there may be multiple copies of some files, so customers should do a full search of their servers to locate all copies.

In accordance with standard security guidelines, file permissions should always be set to enable web visitors to access only the files they need, and no others. Moreover, files that are needed by web visitors should provide the least privilege needed; for example, files that web visitors need to be able to read but not write should be set to read-only.

As a general rule, sample files and roots should always be deleted from a web server prior to putting it into production. If they are needed, file access permissions should be used to regulate access to them as appropriate.

Additional Information: For more information about this vulnerability, see:
<http://phrack.infonexus.com/search.php?view&article=p54-8> (1)
<http://ip.ult.as/vglotsdb/NT/ix38.html> (2)
<http://support.microsoft.com/support/kb/articles/q231368.asp> (3)
<http://www2.merton.co.uk/~security/archive-1999050167.html> (4)

Links: 1. <http://phrack.infonexus.com/search.php?view&article=p54-8>
 2. <http://ip.ult.as/vglotsdb/NT/ix38.html>
 3. <http://support.microsoft.com/support/kb/articles/q231368.asp>
 4. <http://www2.merton.co.uk/~security/archive-1999050167.html>

of Network Resources: 2

Network Resource	Aliases	Network Resource Type	Details
DOC_DOC	10.4.0.132, 00:10:b5:de:88:eb, WDOC_DOC	Windows Networking resource	Service = http, Protocol = TCP, Port = 80, Miscellaneous = aspfile=/msadc/Samples/SELETCOR/showcode.asp
DOC_SQL	10.4.0.131, 00:10:b5:de:91:1e, WDOC_SQL	Windows Networking resource	Service = http, Protocol = TCP, Port = 80, Miscellaneous =

Рис. 5. Описание уязвимости в отчете, сгенерированном сканером NetRecon

ся через Web-узел компании Symantec автоматически, при помощи механизма LiveUpdate.

Сетевой сканер NESSUS

Сетевой сканер Nessus может рассматриваться в качестве достойной альтернативы коммерческим сканерам. Nessus является свободно распространяемым и постоянно обновляемым программным продуктом. Удобный графический интерфейс позволяет определять параметры сеанса сканирования, наблюдать за ходом сканирования, создавать и просматривать отчеты.

По своим функциональным возможностям сканер защищенности Nessus находится в одном ряду, а по некоторым параметрам и превосходит такие широко известные коммерческие сканеры, как NetRecon компании Symantec, Internet Scanner компании ISS и CyberCop Scanner компании NAI.

Версия 0.99 серверной части сканера Nessus была сертифицирована в Гостехкомиссии России (Сертификат N 361 от 18 сентября 2000 г.).

Сценарии атак реализованы в NESSUS в качестве подключаемых модулей (plugins). Количество подключаемых модулей постоянно увеличивается, в настоящее время насчитывается более 700. Новые внешние модули, эмулирующие атаки, можно устанавливать, скопировав файлы, содержащие их исходные тексты, с web-сервера разработчиков www.nessus.org.

Nessus предоставляет очень широкие возможности по поиску уязвимостей корпоративных сетей и исследованию структуры сетевых сервисов. Помимо использования стандартных способов сканирования TCP и UDP портов, Nessus позволяет осуществлять поиск уязвимостей в реализациях протоколов управления сетью ICMP и SNMP. Кроме того, поддерживаются различные стелс-режимы сканирования, реализуемые популярным некоммерческим стелс-сканером nmap, который можно рассматривать в качестве одного из компонентов сканера Nessus. Другой популярный некоммерческий сканер queso используется в составе Nessus для определения типа и номера версии сканируемой ОС.

Высокая скорость сканирования достигается за счет использования при реализации сканера Nessus многопоточной архитектуры программирования, позволяющей осуществлять одновременное параллельное сканирование сетевых хостов. Для сканирования каждого хоста сервером nessusd создается отдельный поток выполнения.

Подробное описание используемых методов сканирования TCP/UDP портов можно найти в онлайн-документации на сканер nmap. Они включают в себя следующее:

- TCP connect scan
- TCP SYN scan
- TCP FIN scan
- TCP Xmas Tree scan
- TCP Null scan
- UDP scan

При реализации Nessus использована нетипичная для сетевых сканеров клиент/серверная архитектура. Взаимодействие между клиентом и сервером осуществляется по защищенному клиент-серверному протоколу, предусматривающему использование надежной схемы аутентификации и шифрование передаваемых данных. Сервер nessusd работает только в среде UNIX и предназначен для выполнения сценариев сканирования. Механизмы собственной безопасности, реализованные в сервере nessusd, позволяют осуществлять аутентификацию пользователей сканера, ограничивать полномочия пользователей по выполнению сканирования и регистрировать все действия пользователей в журнале регистрации событий на сервере.

Клиентская часть Nessus работает и в среде UNIX, и в среде Windows и реализует графический интерфейс пользователя для управления сервером nessusd. Пользователь сканера перед запуском сеанса сканирования определяет параметры сканирования, указывая диапазон сканируемых IP-адресов и TCP/UDP портов, максимальное количество потоков сканирования (число одновременно сканируемых хостов), методы и сценарии сканирования (plugins), которые будут использоваться.

Все сценарии сканирования разделены на группы по типам реализуемых ими сетевых атак (рис. 6), обнаруживаемых уязвимостей, а также по видам тестируемых сетевых сервисов. Так, имеются специальные группы сценариев:

- Backdoors для обнаружения «тройных» программ;
- Gain Shell Remotely — для реализации атак на получение пользовательских полномочий на удаленной UNIX системе;
- Firewalls — для тестирования МЭ;
- FTP — для тестирования FTP-серверов;
- Windows — для поиска уязвимостей Windows-систем и т.п.

Особую группу сценариев сканирования Denial of Service составляют атаки на отказ в обслуживании (DoS). Единственный способ убедиться в том, что сканируемая система подвержена той или иной DoS — это выполнить эту атаку и посмотреть на реакцию системы. Эта группа сценариев, однако, является потенциально опасной, т.к. их

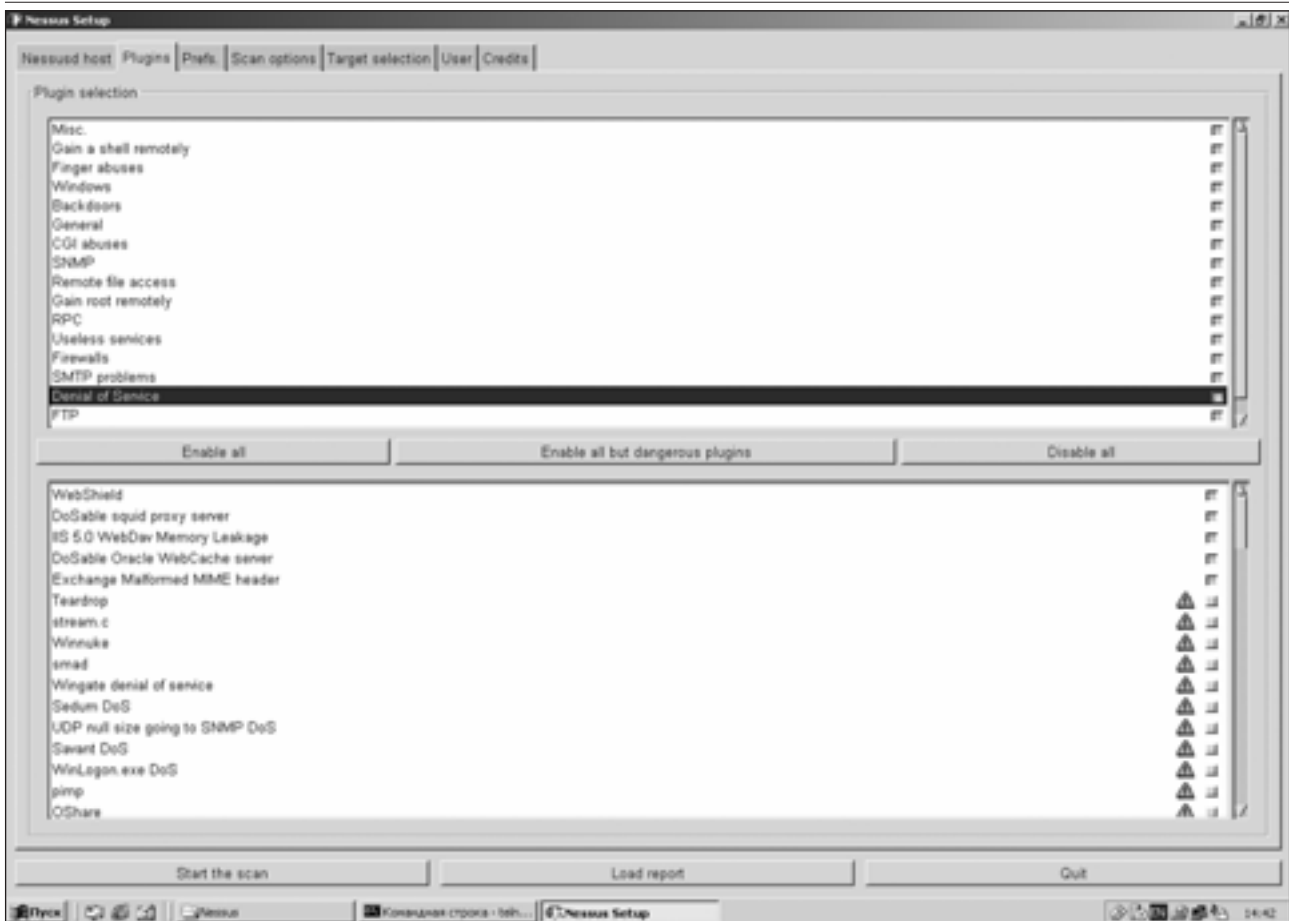


Рис. 6. Выбор сценариев сканирования в сканере Nessus

запуск может привести к непредсказуемым последствиям для сканируемой сети, включая сбои в работе серверов и рабочих станций, потерю данных и «полный паралич» корпоративной сети. Поэтому большинство DoS в данной группе по умолчанию отключено (рис. 6).

Для написания сценариев атак служит специализированный C-подобный язык программирования высокого уровня NASL (Nessus Attack Scripting Language). Существует также интерфейс прикладного программирования (API) для разработки подключаемых модулей со сценариями атак на языке C, однако, предпочтительным является все же использование NASL.

NASL является интерпретируемым языком программирования, что обеспечивает его независимость от платформы. Он предоставляет мощные средства для реализации любых сценариев сетевого взаимодействия, требующих формирования IP-пакетов произвольного вида.

Результаты работы сканера Nessus представлены на рис. 7. Данные об обнаруженных уязвимостях отсортированы по IP-адресам просканированных хостов. Найденные уязвимости проранжированы. Наиболее критичные (security

holes) выделены красным цветом, менее критичные (security warning) — желтым. По каждой уязвимости приводится ее описание, оценка ассоциированного с ней риска (Risk Factor) и рекомендации по ее ликвидации (Solution).

Средства контроля защищенности системного уровня

Обеспечение безопасности компьютерных систем, по существу, заключается в определении множества возможных угроз, оценке величины связанных с ними рисков, выборе адекватных контрмер, реализации этих контрмер процедурными и программно-техническими средствами и контроле их осуществления. Последний вопрос является, пожалуй, одним из наиболее сложных. Реализация программно-технических мер защиты требует произведения настроек большого количества параметров ОС, МЭ, СУБД, сетевых сервисов, прикладных программ и активного сетевого оборудования. Когда речь идет о защите отдельного сервера или рабочей станции, то задача хоть и является сложной, но ее решение вполне по силам опытному системному админис-

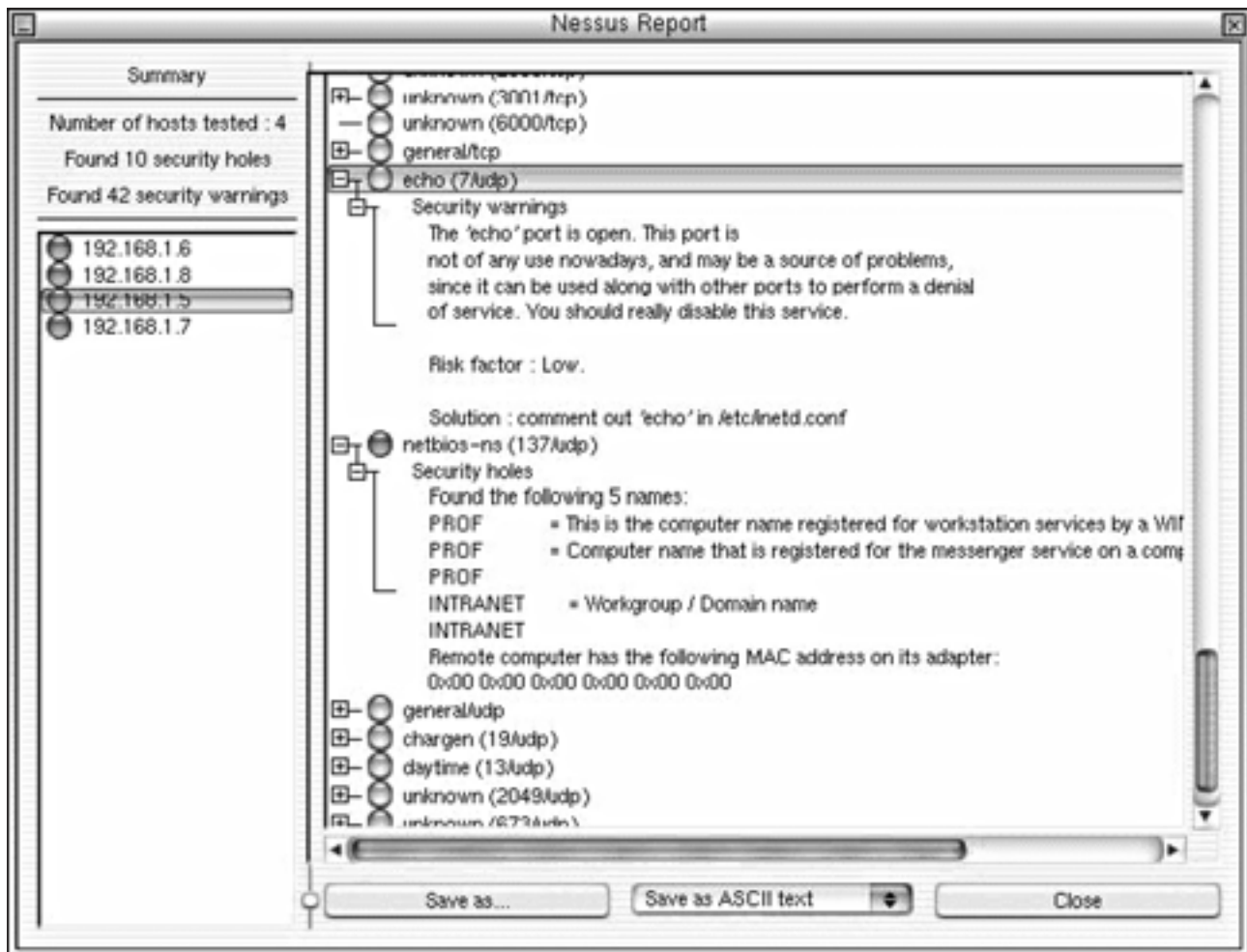


Рис. 7. Представление результатов сканирования в сканере Nessus

тратору. В этом случае для контроля значений параметров программ, связанных с безопасностью, используются специальные списки проверки. Когда же речь заходит о настройке десятков и сотен сетевых устройств, функционирующих на различных программно-аппаратных платформах, в соответствии с единой политикой безопасности, контроле параметров защиты и мониторинге безопасности в реальном масштабе времени, то без специальных средств автоматизации уже не обойтись. Производители ОС предоставляют специальный инструмент для контроля целостности и анализа защищенности ОС (утилита C2 Configuration в Windows NT Resource Kit, утилита ASET в ОС Solaris и т.п.). Имеется немало свободно распространяемых и широко используемых продуктов, предназначенных для решения подобных задач, таких как программа COPS для ОС UNIX. Однако эти средства, функционирующие на системном уровне, позволяют обеспечить только некоторый базовый уровень защищенности самой ОС. Для кон-

троля приложений, сетевых сервисов, активного сетевого оборудования в распределенных системах, функционирующих в динамичной агрессивной среде, необходимо использовать специализированный инструмент, поддерживающий распределенные архитектуры, централизованное управление, различные программно-аппаратные платформы, различные виды приложений, использующий изощренные алгоритмы поиска и устранения уязвимостей, интегрированный с другими средствами защиты и удовлетворяющий многим другим требованиям, предъявляемым к современным продуктам этого класса.

Автоматизированная система управления безопасностью предприятия Enterprise Security Manager

Мощным средством анализа защищенности системного уровня, выполняющим проверки конфигурационных параметров ОС и приложений «изнутри» является автоматизированная система уп-

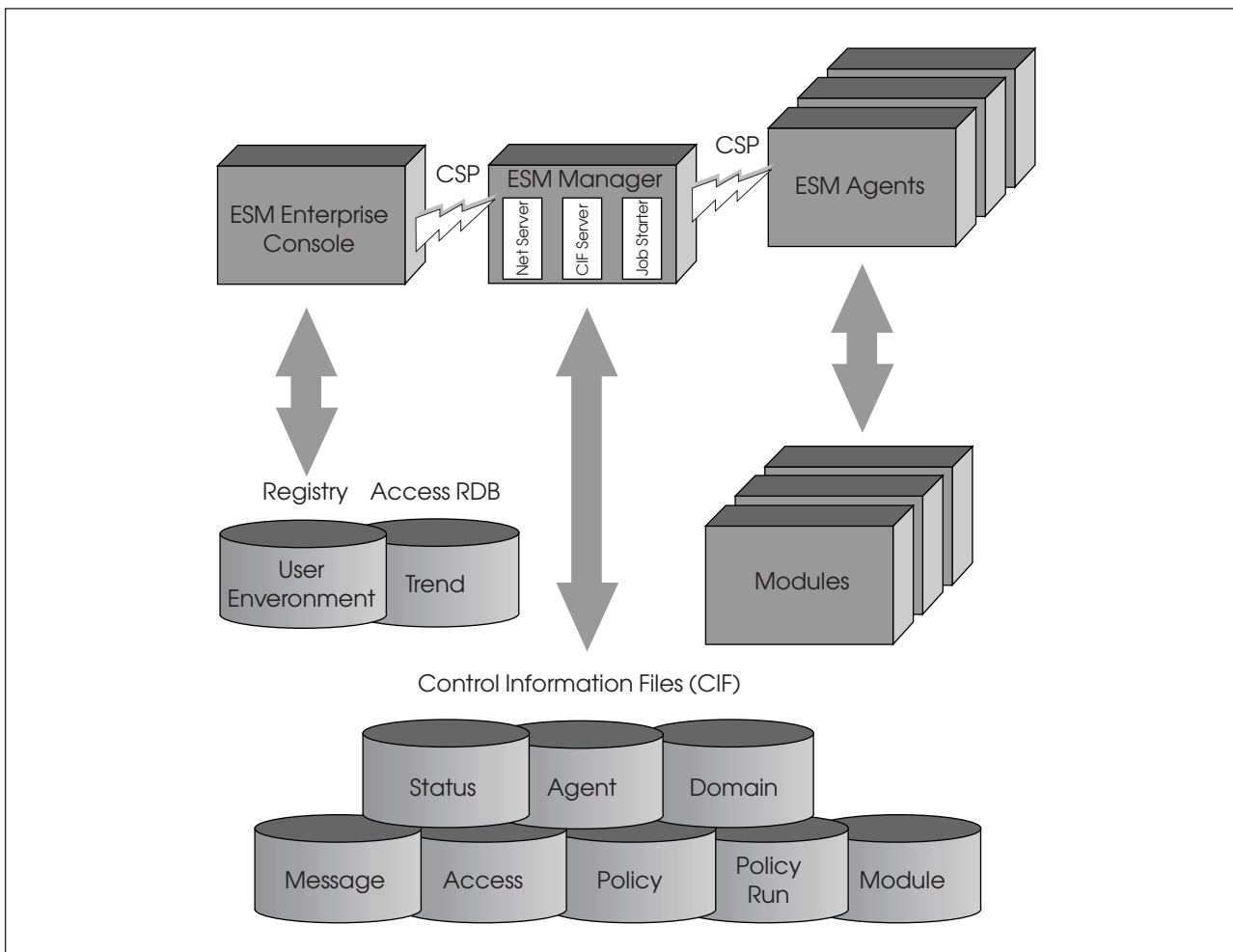


Рис. 8. Архитектура ESM

равления безопасностью предприятия ESM компании Symantec. Программные агенты ESM устанавливаются на каждом контролируемом компьютере сети, выполняя проверки параметров ПО, связанных с безопасностью, и корректируя их по мере необходимости. Программные агенты обычно способны выполнять более сложные проверки и анализировать параметры ПО, недоступные сетевым сканерам, т. к. они действуют изнутри. Анализ защищенности, выполняемый программными агентами, может планироваться по времени и выполняться одновременно на всех контролируемых компьютерах. Кроме того, в отличие от сетевых сканеров, программные агенты не оказывают большого влияния на пропускную способность сети и осуществляют шифрование результатов проверок при передаче данных по сети.

Архитектура ESM

Система ESM построена на архитектуре консоль/менеджер/агент. Она состоит из трех типов компонентов, которые могут быть распределены

по сети произвольным образом: административной консоли (ESM Console), менеджеров (ESM Manager) и агентов (ESM Agent). (См. рис. 8).

Консоль ESM

Административная консоль представляет собой графический пользовательский интерфейс для управления менеджерами и функционирует в среде Windows NT. Для управления менеджерами может также использоваться интерфейс командной строки (CLI).

Административная консоль используется для выполнения следующих задач:

- Управления регистрационными записями пользователей на ESM-менеджере;
- Определения пользовательских полномочий в системе ESM;
- Сбора и анализа информации о состоянии сети от ESM-менеджеров;
- Ранжирования уязвимостей и определения уровней защищенности контролируемых систем;

- Создания и изменения политик безопасности;
- Активизации политик безопасности на контролируемых доменах;
- Установки расписания выполнения проверок;
- Отображения результатов выполнения проверок в табличной и графической формах;
- Генерации и просмотра отчетов по результатам выполняемых проверок;
- Коррекции некоторых параметров ОС.

Менеджер ESM

Центральным компонентом системы является ESM-менеджер. Он выполняет две основные функции:

- хранит данные о политиках безопасности и осуществляет управление этими данными, а также передает эти данные агентам и административной консоли;
- осуществляет управление данными о результатах выполненных проверок, получает эти данные от ESM-агентов и передает их на административную консоль.

Основным компонентом менеджера является сервер управления данными — CIF-сервер. Все данные о пользователях ESM, полномочиях, агентах, доменах, политиках безопасности, результатах проверок и шаблонах, а также сообщения от агентов хранятся в файлах управляющей информации (Control Information Files). CIF-сервер управляет доступом к CIF-файлам. Он предоставляет необходимую информацию по запросам административной консоли и интерфейса командной строки. CIF-сервер также перенаправляет запросы на выполнение другим компонентам менеджера. Например, сообщает менеджеру задач (Job Starter) о необходимости активизировать выполнение политики безопасности на домене. Сетевой сервер (Net Server) является еще одним компонентом менеджера, обеспечивающим связь CIF-сервера и других компонентов с удаленными агентами. Связь между распределенными компонентами ESM осуществляется по защищенному клиент-серверному протоколу ESM's Client Server Protocol (CSP) прикладного уровня, реализованному поверх сетевых протоколов TCP/IP и SPX/IPX. Защита трафика между менеджерами и агентами от прослушивания осуществляется шифрованием по алгоритму DESX, являющемуся усовершенствованной версией американского стандарта шифрования DES.

Агенты ESM

Агенты ESM также как и менеджеры имеют модульную структуру. Они включают в себя серверную часть, модули безопасности и средства коммуникаций. Они собирают информацию о безопасности системы. Сбор и анализ информации начинается с момента получения указания от менеджера на активизацию политики безопасности. Серверный компонент агента собирает данные о результатах проверок от модулей безопасности и посылает их менеджеру. Агенты выполняют также ряд других важных функций:

- Сохраняют мгновенные снимки, содержащие данные о состоянии системы и пользовательских бюджетах;
- Осуществляют обновление мгновенных снимков состояния системы;
- Осуществляют коррекцию некоторых параметров системы по запросам пользователя.

Политики безопасности ESM

Политика безопасности ESM представляет собой совокупность модулей безопасности. ESM содержит набор predetermined политик безопасности, предназначенных для обеспечения различных уровней защищенности. Политика безопасности предприятия реализуется на основе predetermined политик ESM путем настройки модулей безопасности с целью изменения количества и содержания выполняемых ими проверок. Доменная организация агентов позволяет распространить действие политик безопасности на отдельные системы, группы систем и предприятие в целом.

Политика безопасности задает набор правил, которым должны соответствовать контролируемые системы. ESM осуществляет анализ защищенности систем путем сравнения значений их конфигурационных параметров с теми, которые заданы в политике безопасности. ESM выполняет ранжирование результатов проверок по степени критичности и определяет общий уровень защищенности системы, суммируя числовые рейтинги обнаруженных уязвимостей.

Задачу начального конфигурирования ESM существенно облегчает наличие predetermined политик безопасности, перечисленных ниже в порядке увеличения строгости и глубины проверок:

- Phase 1;
- Phase 2;
- Phase 3:a Relaxed;
- Phase 3:b Cautious;
- Phase 3:c Strict.

Политика первого уровня (Phase 1) включает в себя модули безопасности, предназначенные для проверки наиболее существенных и потенциально опасных видов уязвимостей, устранение которых позволяет обеспечить минимально необходимый для большинства систем уровень защищенности.

Политика второго уровня (Phase 2) включает в себя все имеющиеся в ESM модули безопасности, в которых активизированы только ключевые виды проверок, являющиеся наиболее важными.

Политики третьего уровня (Phase 3) включают в себя:

- Базовую версию, идентичную политике второго уровня (Relaxed);
- Усиленную версию, содержащую дополнительные виды проверок (Cautious);
- Строгую версию, включающую все виды проверок во всех модулях безопасности, поддерживаемых для данной ОС (Strict).

Помимо перечисленных в ESM, имеется еще несколько специализированных политик безопасности. Предопределенная политика Queries включает в себя только информационные модули, предоставляющие информацию о пользователях, группах и системах, на которых не установлены ESM и ITA-агенты. Она разработана для платформ NetWare и Windows NT.

Специальная политика NetRecon используется для интеграции со сканером NetRecon на платформе Windows NT, позволяя просматривать и анализировать результаты сканирования сканером NetRecon средствами ESM-консоли. Она осуществляет преобразование записей об уязвимостях, сгенерированных сканером NetRecon, в формат сообщений ESM.

Контроль защищенности корпоративной сети при помощи ESM обычно производится путем постепенного ужесточения требований безопасности, предъявляемых к информационной системе. Начинать следует с активизации политик первого и второго уровней на контролируемых системах. Для большинства коммерческих систем такой уровень защищенности является вполне приемлемым. В случае успешного завершения всех проверок на особо критичных системах можно активизировать политики безопасности третьего уровня, которые позволяют осуществлять наиболее глубокий анализ параметров защиты.

Имеется возможность на основе предопределенных политик создавать свои собственные, которые наилучшим образом соответствуют требованиям организации. Для создания политик безопасности в составе ESM имеется графический

инструментарий, полностью исключающий какое-либо программирование.

Модули ESM

Модули ESM-агентов — это программные модули, осуществляющие проверки, предписываемые политикой безопасности. Имеется две разновидности модулей ESM: модули безопасности и модули запросов. Модули безопасности контролируют различные области безопасности, включая управление пользовательскими бюджетами и параметрами авторизации, настройку сетевых параметров и параметров сервера, атрибуты файловых систем и каталогов. Модули запросов предназначены для сбора информации о состоянии системы. Например, получение списка пользователей, входящих в определенную группу, либо пользователей, наделенных административными полномочиями.

Модули запросов (информационные модули)

Информационные модули служат для сбора информации о различных параметрах системы, существенных при выполнении задач администрирования безопасности. В табл. 1 приводится описание некоторых информационных модулей.

Модули безопасности

Модули безопасности выполняют наборы проверок с целью поиска уязвимостей в ОС и приложениях, попадающих в одну из трех областей:

- Идентификация, аутентификация и авторизация пользователей при входе в систему, управление паролями и пользовательскими бюджетами;
- Конфигурация сетевых протоколов и сервисов;
- Управление доступом к файлам и каталогам.

Пользователь имеет возможность выбора из набора проверок, доступных внутри данного модуля. Каждая проверка осуществляет поиск некоторого типа уязвимостей. Например, проверки, входящие в состав модуля Login Parameters, проверяют систему на наличие неактивных пользователей, зарегистрированных в системе, на наличие паролей с истекшим сроком действия и установку ограничения на количество неудачных попыток входа в систему. (Одни модули безопасности используются только для проверки параметров определенных ОС и приложений, другие — более универсальные и охватывают несколько ОС). В следующей таблице приводится описание основных модулей безопасности.

С целью упрощения задачи управления безопасностью при помощи ESM, все агенты ESM объединяются в домены. Доменом ESM называется группа агентов, объединенных по определен-

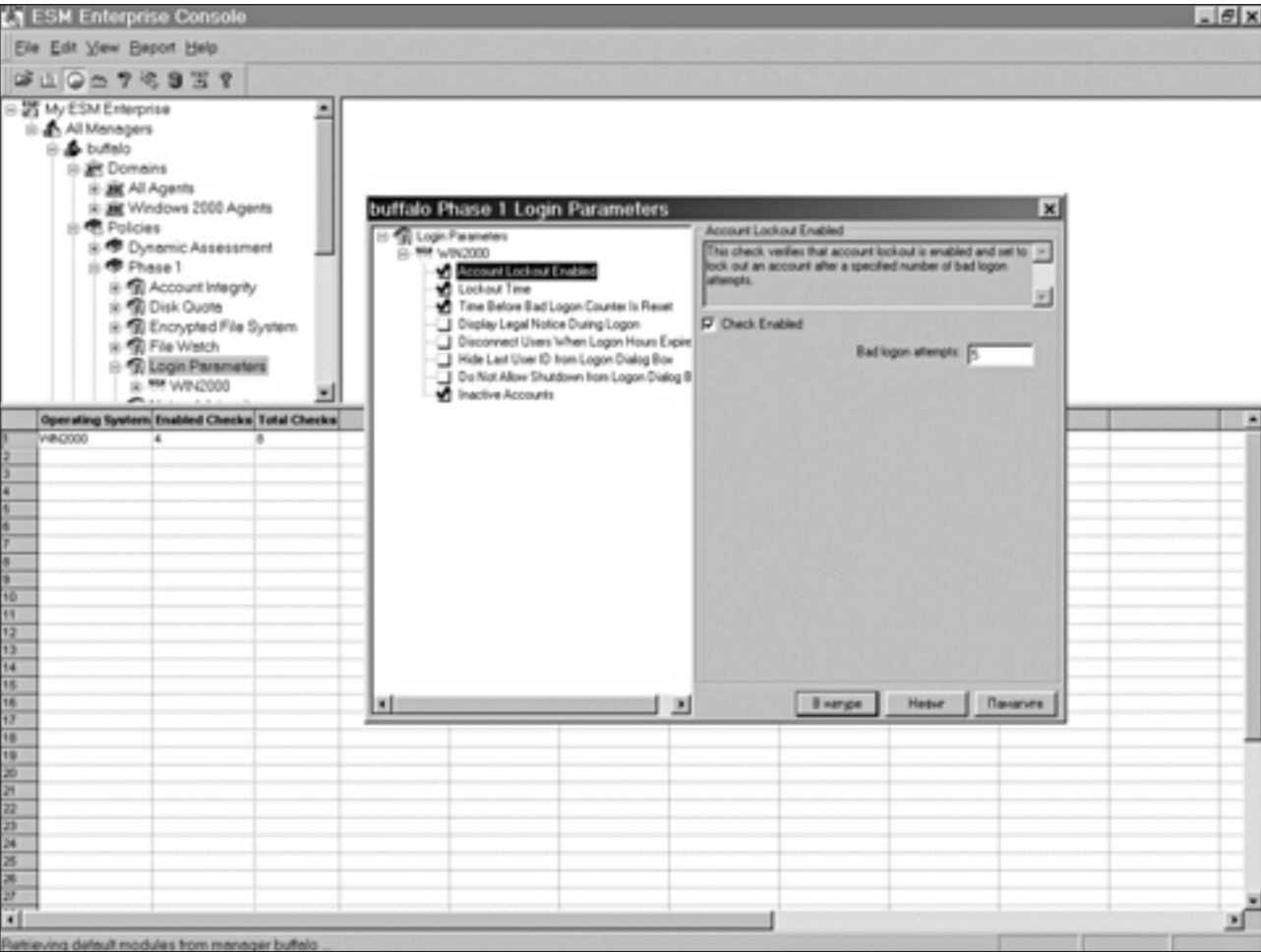


Рис. 9. Управляющая консоль ESM (Проверки, выполняемые модулем Login Parameters)

Account Information	Данный модуль служит для получения информации о регистрационных записях пользователей ОС. В Windows NT он возвращает информацию о полномочиях пользователей, список пользователей с правами администратора, список заблокированных и отключенных регистрационных записей пользователей, список групп и списки пользователей, входящих в каждую группу. В ОС NetWare модуль возвращает список групп и списки пользователей, входящих в каждую группу, эквиваленты безопасности, эффективные права доступа, отношения доверия и т.п.
Discovery	Данный модуль осуществляет сканирование TCP-портов (с целью выявления активных), пытается идентифицировать сетевые ресурсы и составляет список хостов, которые не находятся под контролем программных агентов ESM и ITA.
File Information	Возвращает список параметров доступа к файлам, специфичных для ОС NetWare.

Табл. 1. Информационные модули ESM

ному признаку. Это позволяет активизировать политику безопасности одновременно на всех агентах, входящих в домен. По умолчанию все агенты объединены в домены по типу операционной системы. Таким образом, изначально существует Windows NT-домен, UNIX-домен, NetWare-домен и OpenVMS-домен. Доменная организация

может также отражать организационную или территориальную структуру предприятия.

В ходе осуществления проверок ESM выполняет поиск нарушений политики безопасности. Нарушения политики безопасности могут быть двух типов:

Модуль безопасности	Описание
Account Integrity	Проверяются привилегии пользователей, политика управления паролями и регистрационными записями пользователей.
Backup Integrity	Проверяются параметры подсистемы резервного копирования, выявляются файлы, для которых не были созданы резервные копии.
File Access	Проверяется соответствие прав доступа к файлам установленным правилам политики безопасности.
File Attributes	Осуществляется контроль целостности атрибутов файлов данных.
File Find	Проверяется целостность файлов и контроль файлов на наличие вирусов.
Login Parameters	Проверяются параметры регистрации в системе на соответствие установленным правилам политики безопасности.
Object Integrity	Контролируются изменения прав владения, прав доступа и других атрибутов исполняемых файлов.
Password Strength	Проверяется соответствие паролей пользователей установленным правилам политики управления паролями. Выявляются "слабые" пароли, а также их отсутствие.
Startup Files	Проверяются командные файлы, исполняемые при загрузке системы, на наличие в них уязвимостей.
System Auditing	Проверяются параметры подсистемы аудита и осуществление мониторинга журналов аудита Windows NT.
System Mail	Проверяются конфигурационные параметры системы электронной почты, связанные с безопасностью.
System Queues	Проверяются параметры настройки очередей системных утилит cron, batch и at ОС UNIX, а также параметры подсистемы спулинга ОС OpenVMS.
User Files	Проверяются права владения и права доступа к файлам пользователей.
Registry	Проверяются права доступа и атрибуты ключей реестра ОС Windows NT.
Network Vulnerabilities	Осуществляется анализ уязвимостей настроек сетевых параметров Windows NT, обнаруженных сетевым сканером NetRecon.

Табл. 2. Модули безопасности ESM

- Несоответствие правилам политики безопасности;
- Несоответствие текущего состояния системы последнему мгновенному снимку, сохраненному в ходе проведения предыдущих проверок.

Мгновенные снимки состояния системы

Мгновенные снимки используются ESM для осуществления контроля целостности программной и информационной частей ОС и приложений и для отслеживания изменений в конфигурации системы. Мгновенные снимки содержат значения атрибутов объектов, специфичные для данной системы, такие как времена создания и модификации, контрольные суммы и права доступа к файлам, привилегии пользователей и т. п. Файлы, содержащие мгновенные снимки, создаются при первом запуске политики безопасности на контролируемой системе. В ходе последующих запусков состояние системы сравнивается с мгновенными снимками преды-

дущих состояний и все различия, обнаруженные в параметрах конфигурации и атрибутах системных объектов, рассматриваются в качестве потенциальных уязвимостей. Состояния объектов сравниваются с мгновенными снимками и сообщения обо всех отличиях посылаются Менеджеру, где они записываются в базу данных безопасности.

Каждый агент ESM создает несколько файлов мгновенных снимков под названиями: File, User, Group, Device и т. п. Файлы User, Group и Device содержат информацию о состоянии соответствующих системных объектов. Файл User содержит данные пользовательских бюджетов, включающие пользовательские полномочия и привилегии. Файл Group содержит данные о группах пользователей, включая полномочия и привилегии для группы, а также список членов группы. Файл Device содержит имена владельцев, права доступа и атрибуты устройств.

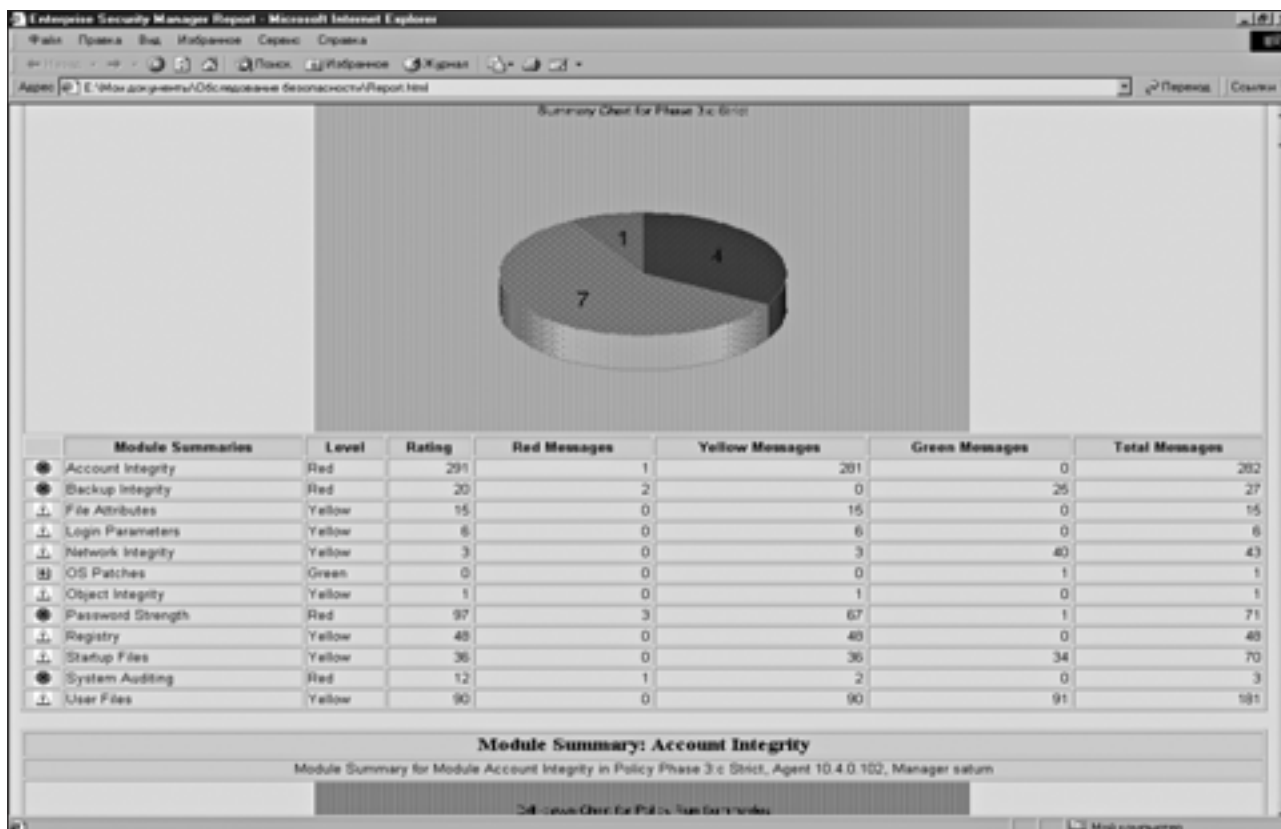


Рис. 10. Результаты проверки системы на соответствие политике безопасности 3:c Strict при помощи ESM

В отличие от других файлов мгновенных снимков File используется для сравнения со специальными шаблонами с целью обнаружения подозрительных изменений файлов, вирусов и троянских коней.

Специализированные модули безопасности, дополнительно устанавливаемые на агентов Oracle modules, Web modules и т. п., могут использовать собственные виды мгновенных снимков.

Шаблоны ESM

Шаблоны используются для выявления несоответствий конфигурации системы правилам политики безопасности. Они представляют собой списки системных объектов и их состояний. Так модуль File Attributes проверяет атрибуты системных файлов ОС Windows 2000 Professional по шаблону (fileatt.w50), а модуль OS Patches проверяет по шаблону (patch.pw5) наличие установленных программных коррекций для ОС.

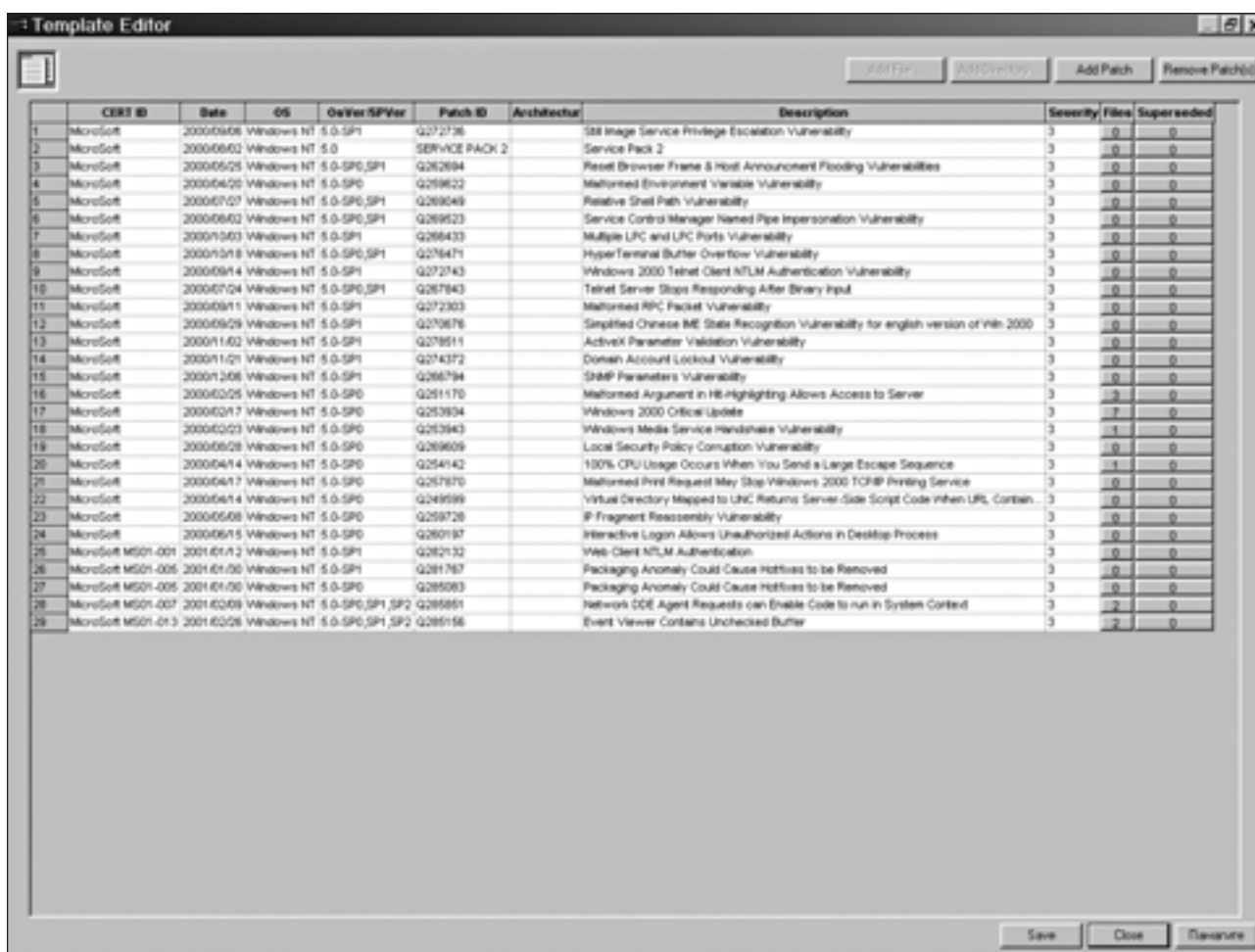
Файлы шаблонов хранятся на Менеджере. При запуске политики модули безопасности определяют по шаблонам объекты и атрибуты объектов, которые будут проверяться.

Основные возможности и характеристики

ESM лучше многих других конкурирующих продуктов подходит для использования в крупных и быстрорастущих сетях, так как обладает хорошими характеристиками масштабируемости. Управляющая консоль ESM 5.0 способна поддерживать до 40 менеджеров и до 10000 агентов. ESM-менеджер на процессоре Pentium 120 MHz или SPARC 276 MHz способен поддерживать до 400 агентов. Управляющая консоль функционирует в различных графических средах, включая X-Window, Windows 3.x, Windows 95/98/NT.

В настоящее время ESM осуществляет более 1000 проверок параметров настройки ОС и приложений. Поддерживается 55 различных продуктов в том числе: ОС, маршрутизаторы, МЭ, Web-серверы, СУБД Oracle и Lotus Notes. Среди поддерживаемых ОС различные версии UNIX, а также Windows NT, NetWare, OpenVMS и т. д.

Возможности ESM могут быть расширены с целью обеспечения поддержки новых приложений. Программный инструмент ESM SDK позволяет создавать новые модули безопасности для поддержки новых приложений, таких как серверы СУБД, Web-серверы, почтовые серверы, МЭ и т. п. Разработка новых модулей осуществляется при помощи библиотечных функций ESM API. В насто-



	CERT ID	Date	OS	OS/Ver/SP/Ver	Patch ID	Architecture	Description	Severity	Files	Superseded
1	Microsoft	2000/09/08	Windows NT	5.0-SP1	Q272736		ISS Image Service Privilege Escalation Vulnerability	3	0	0
2	Microsoft	2000/08/02	Windows NT	5.0	SERVICE PACK 2		Service Pack 2	3	0	0
3	Microsoft	2000/05/25	Windows NT	5.0-SP0,SP1	Q262694		Reset Browser Frame & Host Announcement Flooding Vulnerabilities	3	0	0
4	Microsoft	2000/04/20	Windows NT	5.0-SP0	Q259622		Malformed Environment Variable Vulnerability	3	0	0
5	Microsoft	2000/07/27	Windows NT	5.0-SP0,SP1	Q269049		Relative Shell Path Vulnerability	3	0	0
6	Microsoft	2000/08/02	Windows NT	5.0-SP0,SP1	Q269523		Service Control Manager Named Pipe Impersonation Vulnerability	3	0	0
7	Microsoft	2000/10/03	Windows NT	5.0-SP1	Q266433		Multiple LPC and LPC Ports Vulnerability	3	0	0
8	Microsoft	2000/10/18	Windows NT	5.0-SP0,SP1	Q276471		HyperTerminal Buffer Overflow Vulnerability	3	0	0
9	Microsoft	2000/09/14	Windows NT	5.0-SP1	Q272743		Windows 2000 Telnet Client NTLM Authentication Vulnerability	3	0	0
10	Microsoft	2000/07/24	Windows NT	5.0-SP0,SP1	Q267843		Telnet Server Stops Responding After Binary Input	3	0	0
11	Microsoft	2000/09/11	Windows NT	5.0-SP1	Q272303		Malformed RPC Packet Vulnerability	3	0	0
12	Microsoft	2000/09/29	Windows NT	5.0-SP1	Q270676		Simplified Chinese IME State Recognition Vulnerability for english version of win 2000	3	0	0
13	Microsoft	2000/11/02	Windows NT	5.0-SP1	Q278911		ActiveX Parameter Validation Vulnerability	3	0	0
14	Microsoft	2000/11/21	Windows NT	5.0-SP1	Q274372		Domain Account Lockout Vulnerability	3	0	0
15	Microsoft	2000/11/06	Windows NT	5.0-SP1	Q266794		Shell Parameters Vulnerability	3	0	0
16	Microsoft	2000/02/25	Windows NT	5.0-SP0	Q251170		Malformed Argument in Hb-Highlighting Allows Access to Server	3	0	0
17	Microsoft	2000/02/17	Windows NT	5.0-SP0	Q253904		Windows 2000 Critical Update	3	7	0
18	Microsoft	2000/02/23	Windows NT	5.0-SP0	Q253943		Windows Media Service Handshake Vulnerability	3	1	0
19	Microsoft	2000/06/28	Windows NT	5.0-SP0	Q269609		Local Security Policy Corruption Vulnerability	3	0	0
20	Microsoft	2000/04/14	Windows NT	5.0-SP0	Q254142		100% CPU Usage Occurs When You Send a Large Escape Sequence	3	1	0
21	Microsoft	2000/04/17	Windows NT	5.0-SP0	Q257870		Malformed Print Request May Stop Windows 2000 TCP/IP Printing Service	3	0	0
22	Microsoft	2000/04/14	Windows NT	5.0-SP0	Q249599		Virtual Directory Mapped to UNC Returns Server-Side Script Code when URL Contains	3	0	0
23	Microsoft	2000/05/08	Windows NT	5.0-SP0	Q259728		IP Fragment Reassembly Vulnerability	3	0	0
24	Microsoft	2000/05/15	Windows NT	5.0-SP0	Q260197		Interactive Login Allows Unauthorized Actions in Desktop Process	3	0	0
25	Microsoft MS01-001	2001/01/12	Windows NT	5.0-SP1	Q262132		Web-Client NTLM Authentication	3	0	0
26	Microsoft MS01-005	2001/01/09	Windows NT	5.0-SP1	Q261767		Packaging Anomaly Could Cause Notices to be Removed	3	0	0
27	Microsoft MS01-005	2001/01/09	Windows NT	5.0-SP0	Q265083		Packaging Anomaly Could Cause Notices to be Removed	3	0	0
28	Microsoft MS01-007	2001/02/09	Windows NT	5.0-SP0,SP1,SP2	Q265861		Network CDE Agent Requests can Enable Code to run in System Context	3	2	0
29	Microsoft MS01-013	2001/02/06	Windows NT	5.0-SP0,SP1,SP2	Q265156		Event Viewer Contains Unchecked Buffer	3	2	0

Рис. 11. Редактор шаблонов ESM (загружен шаблон OS Patches)

ящее время разработаны политики безопасности для контроля соответствия настроек ОС требованиям стандарта ISO 17799, а также специализированная антивирусная политика для контроля серверной части NAV Corporate Edition 7.6. Количество политик безопасности, предназначенных для контроля различных аспектов функционирования АС и различных видов приложений, постоянно увеличивается. Список доступных политик и реализующих их модулей безопасности ESM можно найти на Web-сайте Symantec Security Response Team <http://securityresponse.symantec.com/>.

В состав ESM также входят специальные модули для интеграции со средствами сетевого управления HP OpenView и Tivoli.

Несмотря на все свои достоинства, использование программных агентов не может заменить сетевого сканирования, поэтому их лучше применять совместно с сетевыми сканерами.

Выводы

В основе современных методик, используемых для анализа защищенности АС, лежат критерии оценки безопасности ИТ, устанавливающие классы и уровни защищенности. Методики и концепции оценки безопасности, а также набор критериев в достаточном объеме содержатся в международных стандартах ISO 15408 и ISO 17799 (BS 7799), руководящих документах Гостехкомиссии России, других нормативных документах.

К сожалению, отечественная нормативная база в области оценки безопасности ИТ существенно устарела и не соответствует текущему состоянию ИТ. Однако работы по ее совершенствованию в нашей стране идут довольно быстрыми темпами под руководством Гостехкомиссии России. К настоящему времени подготовлен и утвержден Госстандартом ГОСТ Р ИСО/МЭК 15408-1-2002 «Общие критерии оценки безопасности ИТ» (Постановление №133-СТ от 04.04.02), являющийся переводом ISO 15408. Данный ГОСТ

вводится в действие с 1.01.04 г. Это объясняется неготовностью российского ИТ-сообщества немедленно перейти к использованию концепции и методики оценки безопасности ИТ, устанавливаемых этим стандартом. Потребуется приложить немало усилий для того, чтобы схема проведения оценки безопасности ИТ, основанная на подходе, предложенном в «Общих критериях», заработала и позволила бы получить реальные результаты. К настоящему времени на основе «Общих критериев» уже подготовлены проекты Профилей защиты для МЭ и других средств защиты информации. Для обеспечения преемственности результатов работ в области анализа защищенности АС, выполненных по ныне действующим нормативным документам, также необходимо разработать типовые стандартизированные профили защиты, соответствующие классам защищенности, устанавливаемым существующими РД Гостехкомиссии России.

Несмотря на отсутствие каких-либо стандартизированных методик анализа защищенности АС, типовую методику предложить все-таки можно. Она включает в себя изучение исходных данных; анализ рисков и оценку политики безопасности организации; анализ конфигурационных файлов маршрутизаторов, МЭ и прокси-серверов, почтовых и DNS-серверов, а также других критических элементов сетевой инфраструктуры; сканирование АВС снаружи и изнутри; анализ конфигурации серверов и рабочих станций АВС при помощи специализированных программных средств.

Перечисленные методы исследования предполагают использование как активного, так и пассивного тестирования системы защиты, производимого вручную либо с применением специализированных программных средств.

Арсенал программных средств, используемых для анализа защищенности АС, достаточно широк. Причем во многих случаях свободно распространяемые программные продукты ничем не уступают коммерческим. Достаточно сравнить некоммерческий сканер NESSUS с его коммерческими аналогами. Однако на практике, при проведении достаточно глубоких исследований защищен-

ности АС, полностью обойтись без коммерческих программных продуктов такого уровня как, например, Symantec ESM и NetRecon, было бы непросто.

Подводя итог всему вышесказанному, отметим, что в настоящее время вопросы анализа защищенности корпоративных АС являются хорошо проработанными. Имеется богатый арсенал средств и методов для проведения подобных работ. Отработанные методики проведения обследования (аудита) безопасности АС в соответствии с проверенными критериями, утвержденными в качестве международных стандартов, делают возможным получение исчерпывающей информации о свойствах АС, имеющих отношение к безопасности. На практике анализ защищенности АС проводится при помощи мощного программного инструментария, в достаточном объеме представленного на рынке средств защиты информации.

Ссылки на Web-ресурсы

1. Русский перевод стандарта BS7799 (Part II) можно прочесть в JetInfo On-Line
<http://www.jetinfo.ru/annexes/16/annex-16.html>.
2. Официальный Web-сайт Гостехкомиссии России — www.infotecs.ru/gtc.
3. Утилита MS Network Security Hotfix Checker (HFNetCheck) —
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/hfnetchk.asp>
4. Microsoft Security Bulletin Search Web-сайт:
(<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/Default.asp>).
5. Компания St. Bernard Software (www.stbernard.com) — разработчик программы мониторинга установки программных коррекций UpdateExpert.
6. Symantec Security Response Team Web-сайт — <http://securityresponse.symantec.com/>.