Безопасность в Internet

3

В этой главе

- *Internet в структуре информационно-аналитического обеспечения органов государственной власти*
- *Использование электронной почты*
- *Хосты в Internet*
- *Стек протоколов TCP/IP*
- *Слабая аутентификация*
- *Легкость наблюдения за передаваемыми данными*
- *Потенциальные проблемы с электронной почтой*
- *Сложность конфигурирования и мер защиты*
- *Проблемы, возникающие из-за брандмауэров*

<<< Этапы	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				П Э М И Н				Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

Internet страдает от серьезных проблем с безопасностью. Организации, которые игнорируют эти проблемы, подвергают себя риску быть атакованными злоумышленниками. Даже те организации, которые заботятся о безопасности, имеют такие же проблемы из-за появления новых уязвимых мест в сетевом ПО и отсутствия мер защиты.

Информационные системы становятся все более уязвимыми...

Некоторые из проблем безопасности в Internet - результат наличия уязвимых мест из-за ошибок при проектировании, а другие — результат ошибок при конфигурировании хоста или средств управления доступом, которые или плохо установлены, или настолько сложны, что с трудом поддаются администрированию.

Кроме того, важная роль администрирования системы часто не учитывается при описании должностных обязанностей сотрудников, что приводит к тому, что большинство администраторов в лучшем случае нанимаются на неполный рабочий день и плохо подготовлены.

Internet в структуре информационно-аналитического обеспечения органов государственной власти (001)

Кризисное состояние экономики требует радикального изменения существующих информационных связей между различными государственными структурами, а именно перехода от иерархического к корпоративному управлению. При этом большое значение приобретает информация о деятельности государственных и коммерческих структур, в том числе деловая и распорядительная.

В современных, быстро меняющихся условиях ни одна структура органов государственного управления уже не может обходиться без информационного анализа для поддержки управляющих решений. Информационный анализ, или процесс изучения информации, стал неотъемлемой частью процесса управления, а стратегическое планирование, принятое на всех уровнях управления (от государственного до частного), не может довольствоваться только анализом общедоступной информации.

Поэтому неудивительно, что многие органы государственного управления стремятся создать свои информационно-аналитические системы. На практике это приводит к несогласованности и дублированию работ различными организациями, к неквалифицированному анализу представляемых материалов, избыточности в них фактографических сведений, что затрудняет определение главных тенденций в развитии ситуации.

Существенным недостатком является отсутствие обратной связи, которая должна воплощаться в отработанной схеме отслеживания и систематизации возникающих информационных потребностей руководства. Все это является следствием непродуманной схемы информационных потоков между различными уровнями организационной структуры и отсутствия четких требований к составу информации и видам ее представления.

Изложенное подводит к мысли о необходимости создания единой информационной системы для органов государственного управления с применением новейших информационных технологий. При этом все чаще появляются предложения использовать Internet в качестве основы такой системы. Хотя по мнению некоторых специалистов, использование Internet в качестве основы для государственных ИС — все равно, что использование общественного транспорта для перевозки денег инкассаторами — в любой момент могут ограбить.

Движение информационных технологий в сторону открытых распределенных систем, широкое распространение сети Internet как средства межкорпоративного общения придают проблеме информационной защиты особую актуальность. Потери государства в результате разрушения или утечки информации способны многократно превысить затраты на средства защиты, поэтому экономить на мерах по обеспечению безопасности информационных технологий не имеет смысла.

Internet — как объект защиты

Хосты в Internet (220)

На многих системах, подключенных к Internet, работает одна из версий ОС Unix. Впервые TCP/IP был реализован в начале 80-х годов в версии Unix, написанной в университете Беркли (Калифорния), известной

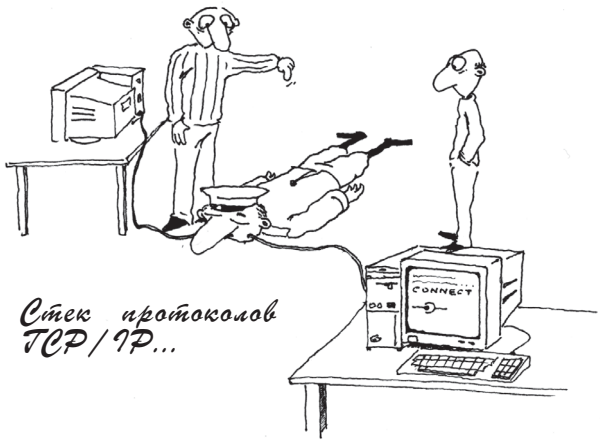
как BSD(Berkeley Software Distribution). Многие современные версии Unix позаимствовали тексты сетевых программ из этой версии, поэтому Unix обеспечивает стандартный набор сервисов TCP/IP, что привело к целесообразности широкого применения стратегий брандмауэров, таких, как фильтрация IP. Следует отметить, что исходные тексты BSD UNIX можно легко получить в Internet, поэтому есть возможность изучить тексты программ, найти в них потенциальные уязвимые места и использовать их для проникновения в ИС.

Возрастающая мощность ПК позволяет обеспечивать предоставление тех же сервисов, которые в настоящее время предоставляются большими компьютерами, но гораздо дешевле. Вследствие этого, полный набор сервисов TCP/IP используется небывалым количеством пользователей.

Хотя это и хорошо в том смысле, что сетевые сервисы стали общедоступными, ***отрицательные последствия заключаются в возникновении огромных возможностей для совершения преступлений в сфере информационных технологий.***

Стек протоколов TCP/IP (220)

Строго говоря, TCP/IP — это стек протоколов, включающий в себя TCP, IP, UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol), и ряд других протоколов.



IP (220)

Уровень IP получает пакеты, доставляемые нижними уровнями, например драйвером интерфейса с ЛВС, и передает их высшим уровням TCP или UDP. И наоборот, IP передает пакеты, полученные от уровней TCP и UDP к низшим уровням.

Пакеты IP являются дейтаграммами с ***негарантированной доставкой***, поскольку IP не гарантирует доставки пакетов IP по порядку и без ошибок. Пакеты IP содержат адрес хоста, с которого был послан пакет, называемый адресом отправителя, и адрес хоста, который должен получить пакет, называемый адресом получателя.

Высокоуровневые сервисы TCP и UDP при приеме пакета предполагают, что адрес отправителя, указанный в пакете, является истинным. Другими словами, адрес IP является основой для аутентификации во многих сервисах; сервисы предполагают, что пакет был послан от существующего хоста, и именно от того хоста, чей адрес указан в пакете.

IP имеет опцию, называемую опцией маршрутизации источника, которая может быть использована для указания точного прямого и обратного путей между отправителем и получателем. Этот путь может задействовать для передачи пакета маршрутизаторы или хосты, обычно не используемые для передачи пакетов к данному хосту-получателю.

Для некоторых сервисов TCP и UDP пакет IP с такой опцией кажется пришедшим от последней системы в указанном пути, а не от своего истинного отправителя. Эта опция появилась в протоколе для его тестирования, но маршрутизация источника может быть использована для обмана систем с целью установления соединения с ними тех хостов, которым это запрещено. ***Поэтому, то, что ряд сервисов доверяют указанному IP-адресу отправителя и полагаются на него при аутентификации, очень опасно и может привести к проникновению в систему.***

TCP (220)

Если IP-пакеты содержат инкапсулированные пакеты TCP, программы IP передадут их верхнему уровню TCP, который последовательно нумерует все пакеты и выполняет исправление ошибок, реализуя таким образом виртуальные соединения между хостами.

Пакеты TCP содержат последовательные номера и подтверждения о приеме пакетов, поэтому ***пакеты, принятые не в порядке передачи, могут быть переупорядочены, а бракованные пакеты повторно посланы.***

TCP передает полученную информацию приложениям верхнего уровня, например клиенту или серверу TELNET. Приложения, в свою очередь, передают информацию обратно уровню TCP, который передает ее ниже уровню IP, после чего она попадает к драйверам устройств, в физическую среду и по ней передается до хоста-получателя.

Сервисы с установлением соединения, такие, как TELNET, FTP, rlogin, X Windows и SMTP требуют на-

дежности и поэтому используют TCP. DNS использует TCP только в отдельных случаях (для передачи и приема баз данных доменных имен), а для передачи информации об отдельных хостах использует UDP.

UDP (220)

UDP взаимодействует с прикладными программами на том же уровне, что и TCP. Тем не менее, он не выполняет функции исправления ошибок или повторной передачи потерянных пакетов. Поэтому UDP не используется в сервисах с установлением соединения, которым требуется создание виртуального канала. Он применяется в таких сервисах типа запрос-ответ, как NFS, где число сообщений в ходе взаимодействия гораздо меньше, чем в TELNET и FTP. В число сервисов, использующих UDP, входят сервисы на базе RPC: NIS и NFS, NTP (протокол сетевого времени) и DNS (также DNS использует TCP).

Пакеты UDP гораздо проще подделать, чем пакеты TCP, так как нет этапа установления соединения (рукопожатия). Поэтому использование сервисов на базе UDP сопряжено с большим риском.

ICMP (220)

ICMP (Протокол межсетевых управляющих сообщений) находится на том же уровне, что и IP; его назначение - передавать информацию, необходимую для управления трафиком IP. В основном он используется для предоставления информации о путях к хостам-получателям. Сообщения ICMP redirect информируют хосты о существовании боле коротких маршрутов к другим системам, а сообщения ICMP unreachable указывает на наличие проблем с нахождением пути к получателю пакета. Кроме того, ICMP может помочь корректно завершить соединение TCP, если путь стал недоступен. PING является широко распространенным сервисом на базе ICMP.

Старые версии Unix могут разорвать все соединения между хостами, даже если только одно из них столкнулось с проблемами. Кроме того, ***сообщения о перенаправлении пути ICMP могут быть использованы для обмана маршрутизаторов и хостов с целью заставить их поверить в то, что хост злоумышленника является маршрутизатором*** и пакеты лучше отправлять через него. Это, в свою очередь, может привести к тому, что атакующий получит доступ к системам, которым не разрешено иметь соединения с машиной атакующего или его сетью.

SMTP (220)

SMTP — это почтовый протокол хост-хост. SMTP-сервер принимает письма от других систем и сохраняет их в почтовых ящиках пользователей. Сохраненные письма могут быть прочитаны несколькими способами. Пользователи с интерактивным доступом на почтовом сервере могут читать почту с помощью локальных почтовых приложений. Пользователи на других системах могут загрузить свои письма с помощью программ почтовых клиентов по протоколам POP3 и IMAP.

UNIX-хосты сделали самым популярным SMTP. Широко используемыми SMTP-серверами являются Sendmail, Smail, MMDF и PP. Самым популярным SMTP-сервером в Unix является Sendmail, написанный Брайаном Эллманом. Он поддерживает создание очередей сообщений, переписывание заголовков писем, алиасы, списки рассылки и т.д. Обычно он конфигурируется так, что должен работать как привилегированный процесс. Это означает, что ***если его защиту можно будет обойти каким-нибудь способом, атакующий сможет нанести вред, значительно превышающий удаление электронных писем.***

POP (220)

POP — это самый популярный протокол приема электронной почты. POP-сервер позволяет POP-клиенту загрузить письма, которые были получены им от другого почтового сервера. Клиенты могут загрузить все сообщения или только те, которые они еще не читали. Он не поддерживает удаление сообщений перед загрузкой на основе таких атрибутов сообщения, как адрес отправителя или получателя.

POP 3 предоставляет метод аутентификации, называемый APOP, который прячет пароль. Некоторые реализации POP могут использовать Kerberos для аутентификации.

IMAP (220)

IMAP — менее популярный протокол чтения электронной почты.

Он поддерживает:

- операции создания, удаления, переименования почтовых ящиков;
- проверку поступления новых писем; оперативное удаление писем;
- установку и сброс флагов операций; разбор заголовков в формате RFC-822 и MIME-IMB;
- поиск среди писем; выборочное чтение писем.

IMAP более удобен для чтения почты в путешествии, чем POP, так как сообщения могут быть оставлены на сервере, что избавляет от необходимости синхронизировать списки прочитанных писем на локальном хосте и на сервере.

MIME (220)

MIME — это сокращение для многоцелевых расширений Internet-почты (Multipurpose Internet Mail Extensions).

Он переопределяет формат сообщений электронной почты, чтобы позволить:

- передачу текстов в кодировке, отличной от US-ASCII,
- передачу в письме нетекстовой информации в различных форматах,
- сообщения из нескольких частей, и
- передачу в заголовке письма информации в кодировке, отличной от US-ASCII.

MIME можно использовать для поддержки таких средств безопасности, как цифровые подписи и шифрованные сообщения. ***Он также позволяет посылать по почте выполняемые файлы, зараженные вирусами.***

Типовые сервисы (220)

Существует ряд сервисов, связанных с TCP/IP и Internet.

Перечислим наиболее распространенные сервисы:

- **TELNET** — для подключения к удаленным системам, присоединенным к сети, применяет базовые возможности по эмуляции терминала;
- **FTP** — протокол передачи файлов для их приема или передачи между системами в сети;
- **DNS** — служба сетевых имен, используется TELNET, FTP и другими сервисами для трансляции имен хостов в IP адреса;
- **gopher** — средство поиска и просмотра информации с помощью системы меню, которое может обеспечить дружественный интерфейс к другим информационным сервисам;
- **WAIS** — глобальный информационный сервис для индексирования и поиска в базах данных файлов;
- **WWW/http** — Всемирная Паутина, объединение FTP, gopher, WAIS и других информационных сервисов, использующее протокол передачи гипертекста(http), и программы Netscape, Microsoft Internet Explorer и Mosaic в качестве клиентских программ;
- **NFS** — сетевая файловая система, позволяющая системам совместно использовать директории и диски, при этом удаленная директория или диск кажутся находящимися на локальной машине;
- **NIS** — Сетевые Информационные Сервисы, позволяют нескольким системам совместно использовать базы данных, например файл паролей, для централизованного управления ими;
- **Система X Windows** — графическая оконная Среда и набор прикладных библиотек, используемых на рабочих станциях;
- **rlogin, rsh и другие r-сервисы** — реализуют концепцию доверяющих друг другу хостов, позволяют выполнять команды на других компьютерах, не вводя пароль.

Хотя сервисы TCP/IP могут в равной степени использоваться как в локальных, так и в глобальных сетях, в локальных сетях, как правило, применяется совместное использование файлов и принтеров, а электронная почта и удаленный терминальный доступ — в обоих случаях.

Структура портов TCP и UDP (220)

Сервисы TCP и UDP используются с помощью схемы клиент-сервер. Например, процесс сервера TELNET вначале находится в состоянии ожидания запроса установления соединения. В какой-нибудь момент пользователь запускает процесс клиента TELNET, который инициирует соединение с сервером TELNET.

Клиент посылает данные серверу, тот читает их, и посылает клиенту ответ. Клиент читает ответ и сообщает о нем пользователю. Поэтому соединение является двунаправленным и может быть использовано как для чтения, так и для записи.

Соединение TCP или UDP уникально идентифицируется с помощью четырех полей, присутствующих в каждом соединении:

- **IP-адрес источника** — адрес системы, пославшей пакет,
- **IP-адрес получателя** — адрес системы, принимающей пакет,
- **порт отправителя** — порт соединения в системе-отправителе,
- **порт получателя** — порт соединения в системе-получателе.

Порт — это программное понятие, которое используется клиентом или сервером для посылки или приема сообщений. Порт идентифицируется 16-битовым числом.

Угрозы для протоколов и служб Internet (220)

Очевидно, что TCP/IP, который обеспечивает коммуникации в Internet и в получающих все большую популярность интрасетях, имеет “врожденные” недостатки защиты. То же самое можно сказать и о таких службах

на базе TCP/IP, как FTP и Domain Naming System (DNS).

Система имен доменов (Domain Name System — DNS) представляет собой распределенную базу данных, которая преобразует имена пользователей и хостов в IP-адреса и наоборот. DNS также хранит информацию о структуре сети компании, например о количестве компьютеров с IP-адресами в каждом домене. ***Одной из проблем DNS является то, что эту базу данных очень трудно "скрыть" от неавторизованных пользователей. В результате, DNS часто используется хакерами как источник информации об именах доверенных хостов.***

FTP (File Transfer Protocol) обеспечивает передачу текстовых и двоичных файлов, поэтому его часто используют в Internet для организации совместного доступа к информации. На FTP-серверах хранятся документы, программы, графика и любые другие виды информации. Некоторые FTP-серверы ограничивают доступ пользователей к своим архивам данных с помощью пароля, другие же предоставляют свободный доступ (так называемый анонимный FTP-сервис). Если вы используете опцию анонимного FTP для своего сервера, то должны быть уверены, что на нем хранятся только файлы, предназначенные для свободного распространения.

World Wide Web (WWW) — система, основанная на сетевых приложениях, которые дают возможность пользователям просматривать содержимое различных серверов в Internet или интрасетях. Самым полезным свойством WWW является использование гипертекстовых документов, со встроенными ссылками на другие документы и Web-узлы, что дает возможность легко переходить от одного узла к другому. Однако это же свойство является и наиболее слабым местом системы WWW, поскольку ***ссылки на Web-узлы, хранящиеся в гипертекстовых документах, включают в себя информацию о том, как осуществляется доступ к соответствующим узлам***. Используя эту информацию, хакеры могут разрушить Web-узел или получить доступ к хранящейся на нем конфиденциальной информации.

Слабая аутентификация (220)

ОС Unix обычно хранит пароли в зашифрованной форме в файле, который может быть прочитан любым пользователем. Этот файл паролей может быть получен простым копированием его или каким-либо другим способом, используемым злоумышленниками. Как только файл получен, ***злоумышленник может запустить легкодоступные программы взлома паролей для этого файла.***

Другая проблема с аутентификацией возникает из-за того, что службы TCP и UDP могут аутентифицировать только отдельный хост, но не пользователя. Например, сервер NFS(UDP) не может дать доступ отдельному пользователю на хосте, он может дать его всему хосту. Администратор сервера может доверять отдельному пользователю на хосте и дать ему доступ, но ***администратор не может запретить доступ других пользователей на этом хосте*** и поэтому автоматически должен предоставить его всем пользователям или не давать его вообще.

Наблюдение за передаваемыми данными (220)

Когда пользователь установил сеанс с удаленным хостом, используя TELNET или FTP, то пароль пользователя передается в Internet незашифрованным.

Поэтому ***другим способом проникновения в системы является наблюдение за соединением с целью перехвата IP-пакетов, содержащих имя и пароль,*** и последующее использование их для нормального входа в систему. Если перехваченный пароль является паролем администратора, то задача получения привилегированного доступа становится гораздо легче.

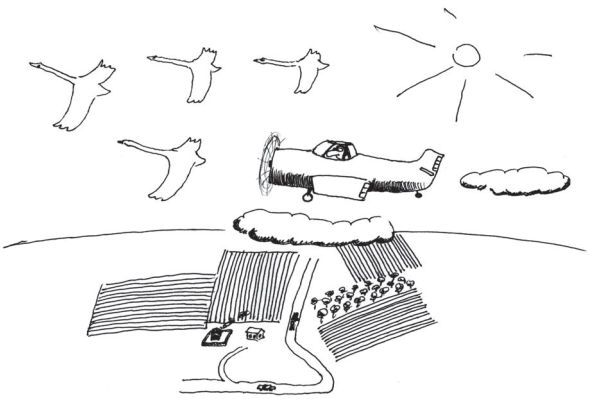
Электронная почта, а также содержимое сеансов TELNET и FTP, может перехватываться и использоваться для получения информации об организации и ее взаимодействии с другими организациями в ходе повседневной деятельности. Большинство пользователей не шифруют почту, так как многие полагают, что электронная почта безопасна и с ее помощью можно передавать конфиденциальную информацию.

Система X Windows, приобретающая популярность, также подвержена перехвату данных. X позволяет открывать несколько окон на рабочей станции для работы с графическими и мультимедийными приложениями (например, WWW-браузером Netscape).

Злоумышленники могут открывать окна на других системах и перехватывать текст, набираемый на клавиатуре, который может содержать пароли и критическую информацию.

Маскировка под других пользователей (220)

Маршрутизация IP-источника — это опция, с помощью которой можно явно указать маршрут к назначению и путь, по которому пакет будет возвращаться к отправителю. Это путь может включать использование других маршрутизаторов или хостов, которые в обычных условиях не используются при передаче пакетов к назначению. ***Используя маршрутизацию IP-источника, хост атакующего может замаскироваться под доверенного хоста или клиента.***



Маскировка под других пользователей...

Хосты Unix принимают пакеты с маршрутизацией источника и будут передавать их по пути, указанному в пакете. Маршрутизаторы также принимают пакеты с маршрутизацией источника, в то время как некоторые маршрутизаторы могут быть сконфигурированы таким образом, что будут блокировать такие пакеты.

Еще более ***простым способом маскировки под клиента является ожидание того момента, когда будет выключена клиентская система, и последующая маскировка под нее.*** Во многих организациях сотрудники используют ПК с сетевой математикой TCP/IP и используют машины с Unix как серверы ЛВС.

Атакующий может сконфигурировать по окончании работы свой ПК таким образом, что он будет иметь то же имя и IP-адрес, что и другая машина, а затем инициировать соединение с Unix-хостом, как если бы он был доверенным клиентом. Это очень просто сделать и именно так поступают атакующие сотрудники организации.

Потенциальные проблемы с электронной почтой (220)

Электронная почта (e-mail) — самый популярный вид использования Internet. С помощью электронной почты в Internete можно направить письмо миллионам людей по всей планете.

Существуют шлюзы частных почтовых систем e-mail в Internet, что занчительно расширяет возможности этого вида связи.

Помимо взаимодействия один-один, e-mail может поддерживать списки электронных адресов для рассылки, поэтому частное лицо или организация может послать e-mail всему этому списку. Иногда списки рассылки e-mail имеют элементы, указывающие на другие списки рассылки, поэтому одно письмо может быть в конце концов доставлено тысячам людей.

Разновидностью списков рассылки являются дискуссионные группы на основе e-mail. Их участники посылают письмо центральному серверу списка рассылки, и сообщения рассылаются всем другим членам группы. Это позволяет участникам, находящимся в разных временных зонах или на разных континентах, вести интересные дискуссии.

При помощи специальных программ пользователи могут подписаться на список или отказаться от него без вмешательства человека. Серверы списков рассылки часто предоставляют такие сервисы, как получение архивов, дайджестов сообщений, или связанных с сообщениями файлов. Группы новостей USENET являются усовершенствованием дискуссионных почтовых групп.

Аналогично политике использования телефона, организациям следует разработать политику правильного использования электронной почты.

Политика должна давать общие рекомендации в таких областях:

- Использование электронной почты для ведения деловой деятельности
- Использование электронной почты для ведения личных дел
- Управление доступом и сохранение конфиденциальности сообщений
- Администрирование и хранение электронных писем

Электронную почту в Internet особенно легко подделать. Ей вообще нельзя доверять без применения таких расширений, как электронная подпись письма.

Взаимодействие между хостами Internet при обмене почтой происходит с помощью простого протокола, использующего текстовые команды. Злоумышленник может легко ввести эти команды вручную, используя TELNET для установления сеанса с портом SMTP (простой протокол передачи почты).

Принимающий хост доверяет тому, что заявляет о себе хост-отправитель, поэтому ***можно легко указать ложный источник письма, введя адрес электронной почты как адрес отправителя,*** который будет отличаться от истинного адреса. В результате, любой пользователь, не имеющий никаких привилегий, может фальсифицировать электронное письмо.

Случайные ошибки (220)

- Можно легко допустить ошибку при работе с электронной почтой.
- Письмо может быть послано случайно.
- Простое нажатие клавиши или щелчок мышкой могут послать письмо по неправильному адресу.

- Почтовые сообщения могут храниться годами, поэтому плохое выражение может аукнуться в дальнейшем.
- Архивы писем могут возрасти до таких масштабов, что система будет аварийно завершаться.
- Неправильно настроенная программа чтения групп новостей может привести к посылке сообщения не в те группы.
- Ошибки в списках рассылки могут привести к долгому блужданию писем между почтовыми серверами, причем число писем может увеличиться до такой степени, что почтовые серверы аварийно завершатся.

Когда почтовая система организации присоединена к Internet, последствия ошибок могут оказаться в тысячу раз хуже.

Вот некоторые из способов предотвращения ошибки:

- учить пользователя принимать решения при совершении ошибки и правильно работать с электронной почтой;
- конфигурировать программы электронной почты так, чтобы стандартные действия пользователя, использующие установки по умолчанию, были бы самыми безопасными;
- использовать программы, которые строго реализуют протоколы и соглашения системы Internet. Каждый раз, когда онлайновый сервис шлюзует письмо из частной почтовой системы в e-mail Internet, слышны вопли протеста при появлении большого числа сообщений с ошибками, возникшими в результате неправильных настроек почтовых серверов этого сервиса.

Персональное использование (220)

Поскольку письмо обычно используется для обеспечения деятельности организации, как телефон и факс, использование его в личных целях должно быть ограничено или запрещено (это зависит от организации).

Хотя проще всего определить, что электронная почта используется только для решения задач организации, все понимают, что эту политику трудно воплотить в жизнь. Если политика не может быть согласованно внедрена, неизбежно ее несоблюдение и невозможность использования в качестве основы для наказания. Гораздо более мудрым будет создать политику, которая устанавливает четкие границы использования e-mail в личных целях, аналогично тому, как устанавливаются рамки использования служебного телефона в личных целях.

Посылка электронного письма с электронным почтовым адресом, содержащим адрес организации, будет похожа на посылку бумажного письма на фирменном бланке компании. Если отправитель использует свой логин в компании для посылки электронной почты в группу новостей, может показаться, что компания одобряет мнение, высказываемое отправителем в письме.

Маркетинг (220)

В прошлом, когда Internet был исследовательской сетью, ее коммерческое использование было запрещено. Кроме того, слишком мало компаний и людей имели доступ к Internet-почте, поэтому было нецелесообразно использовать ее для коммерческих целей.

Сейчас Internet расширился и использовать его в коммерческих целях разрешается, поэтому компании стали поддерживать списки рассылки для обмена информацией со своими клиентами.

Клиенты должны послать запрос для того, чтобы попасть в список рассылки. Когда большие онлайновые сервисы стали шлюзовать письма в Internet, неожиданно обнаружилось, что таким образом можно передать информацию гораздо большей аудитории. Так зародился маркетинг в Internet с помощью посылки отдельных почтовых сообщений.

Взаимное доверие хостов (220)

Хосты затруднительно поддерживать в безопасном состоянии и это занимает много времени. Для упрощения управления хостами некоторые организации используют такие сервисы, как NIS(Network Information Service) и NFS(Network File system). Эти сервисы могут сократить время на конфигурирование хостов, позволяя управлять такими БД, как файлы паролей с помощью удаленного доступа к ним и обеспечивая возможность совместного использования файлов и данных.

Однако ***эти сервисы небезопасны по своей природе*** и могут использоваться для получения доступа грамотными злоумышленниками. Если скомпрометирован центральный сервер, то другие системы, доверяющие центральной системе, также могут быть легко скомпрометированы.

Некоторые сервисы позволяют хостам “доверять” друг другу для удобства работы пользователей и облегчения совместного использования систем и устройств. Если в систему было совершено проникновение или ее обманули с помощью маскарада, то для злоумышленника не составит труда получить доступ к другим системам.

Сложность конфигурирования и мер защиты (220)

Системы управления доступом в хостах часто сложны в настройке и трудны для проверки правильности их работы. В результате ***неправильно сконфигурированные меры защиты могут привести к проникновению злоумышленников.***

Несколько крупных производителей Unix все еще продают свои системы с системой управления доступом, сконфигурированной так, что пользователям предоставлен максимальный, т.е. наименее безопасный доступ, который может привести к неавторизованному доступу, если не будет произведена переконфигурация.

Ряд инцидентов в области безопасности произошел в системе Internet отчасти потому, что злоумышленники обнаружили уязвимые места (позднее их обнаружили пользователи, группы компьютерной безопасности и сами производители).

Поскольку большая часть современных вариантов Unix позаимствовала свой сетевой код из версии BSD, и так как исходный код этой версии широко доступен, злоумышленники смогли изучить его на предмет ошибок и условий, при которых их можно использовать для получения доступа к системам.

Ошибки, приводящие к неавторизованному доступу существуют из-за сложности программ и невозможности проверить их во всех средах, в которых они должны работать. Иногда эти ошибки легко обнаруживаются и исправляются, но бывает и так, что приходится, как минимум, переписать все приложение.

Проблемы, возникающие из-за брандмауэров (220)

Помимо преимуществ использования брандмауэров, существует и ряд проблем, от которых брандмауэры не могут защитить. Брандмауэр не является панацеей от всех проблем безопасности, связанных с системой Internet. Имеется и ряд недостатков при их использовании. Рассмотрим некоторые из них.

Ограничение в доступе к нужным службам (220)

Самым очевидным недостатком брандмауэра является то, что он может блокировать ряд служб, которые широко используют: TELNET, FTP, X Windows, NFS и др. Некоторые сети могут иметь топологию, которая не позволяет применить брандмауэр без серьезных ограничений при работе в сети.

Например, может потребоваться использование NFS и NIS через основные маршрутизаторы. В такой ситуации стоимость установки брандмауэра следует сравнить с ущербом, который понесет организация от атаки на сеть.

Могут оказаться более уместными другие решения, такие как Керберос, но они также не лишены недостатков.

Большое количество уязвимых мест (220)

Брандмауэры не защищают от черных входов (люков) в сети. Например, если можно осуществить неограниченный доступ по модему в сеть, защищенную брандмауэром, атакующие могут эффективно обойти его. Скорости модемов достаточны для того, чтобы сделать возможным использование SLIP (Serial Line IP) и PPP (Point-to-Point Protocol). Эти соединение внутри защищенной сети по сути является уязвимым местом.

Зачем нужен брандмауэр, если разрешен неограниченный доступ по модему?

Плохая защита от атак собственных сотрудников (220)

Брандмауэры обычно не обеспечивают защиты от внутренних угроз. Хотя брандмауэр может защищать от получения посторонними лицами критических данных, он не защищает от копирования своими сотрудниками данных на дискету и выноса ее за пределы сети.

Поэтому, было бы ошибкой думать, что наличие брандмауэра защищает от атак изнутри или атак, для защиты от которых нужен не брандмауэр. Наверное, не стоит вкладывать значительные ресурсы в брандмауэр, если есть другие способы выкрасть данные.

Другие проблемы (220)

С использованием брандмауэра связаны и другие проблемы:

- **WWW**, **gopher** — новые информационные серверы и клиенты, такие как WWW, gopher, WAIS и ряд других не рассчитаны на совместную работу с брандмауэром, и из-за их новизны достаточно рискованны. Имеется потенциальная возможность атак с помощью передачи специальных данных, при которых, обрабатываемые клиентом данные могут содержать команды клиенту, эти команды могут вынудить клиента изменить параметры средств управления доступом или модифицировать важные файлы, связанные с защитой машины клиента.

- **MBONE** — групповые передачи с помощью IP(MBONE), содержащие речь и изображение, инкапсулируются в других пакетах; брандмауэры обычно пропускают эти пакеты, не проверяя их содержимое. Передачи типа MBONE представляют потенциальную угрозу, если пакеты содержат команды, изменяющие параметры работы средств защиты и позволяющие злоумышленникам получить доступ.

- **Вирусы** — брандмауэры не защищают от пользователей, загружающих программы для ПК, зараженные вирусами, из Internet архивов или передачи таких программ в качестве приложений к письму. Поскольку эти программы могут быть закодированы или сжаты многими способами, брандмауэр не может сканировать такие программы с целью обнаружения сигнатур вирусов. Проблема вирусов должна быть решена с помощью других мер защиты.

- **Пропускная способность** — брандмауэры потенциально являются узким местом, так как все соединения должны проходить через брандмауэр и, в некоторых случаях, изучаться брандмауэром. Тем не менее, теперь это не является проблемой, так как брандмауэры могут обрабатывать данные со скоростью 1.5 Мбита/с, а большинство сетей, подключенных к Internet, имеют скорость меньшую или равную этой.

Несмотря на эти недостатки, стандарт NIST рекомендует организациям защищать свои ресурсы с помощью брандмауэров и других средств безопасности.

Резюме

Internet страдает от серьезных проблем с безопасностью. Организации, которые игнорируют эти проблемы, подвергают себя риску того, что они будут атакованы злоумышленниками. Даже те организации, которые заботятся о безопасности, имеют те же самые проблемы из-за появления новых уязвимых мест в сетевом программном обеспечении(ПО) и отсутствия мер защиты.

Некоторые из проблем безопасности в Internete — результат наличия уязвимых мест из-за ошибок при проектировании, а другие — результат ошибок при конфигурировании хоста или средств управления доступом, которые или плохо установлены или настолько сложны, что с трудом поддаются администрированию.

Совершенно очевидно, что TCP/IP, который обеспечивает коммуникации в Internet и в получающих все большую популярность интрасетях, — имеет «врожденные» недостатки защиты. То же самое можно сказать и о службах на базе TCP/IP, таких как FTP и Domain Naming System (DNS).

Электронную почту в Internete особенно легко подделать. Ей вообще нельзя доверять, если не применяются расширения, такие как электронная подпись письма. Взаимодействие между хостами Interneta при обмене почтой происходит с помощью простого протокола, использующего текстовые команды. Злоумышленник может легко ввести эти команды вручную, используя TELNET для установления сеанса с портом SMTP(простой протокол передачи почты).

Брандмауэры обычно не обеспечивают защиты от внутренних угроз. Хотя брандмауэр может защищать от получения посторонними лицами критических данных, он не защищает от копирования своими сотрудниками данных на дискету и выноса ее за пределы сети. Поэтому, было бы ошибкой думать, что наличие брандмауэра защищает от атак изнутри или атак, для защиты от которых нужен не брандмауэр. Не стоит вкладывать значительные ресурсы в брандмауэр, если есть другие способы украсть данные.