Шумилина В.Е., к.э.н., доцент кафедры «Экономическая безопасность, учет и право» ДГТУ, Ростов-на-Дону, Россия; Shumilina.vera@list.ru
Чибизов Р.Р., студент 3-го курса кафедры «Экономическая безопасность, учет и право» ДГТУ, Ростов-на-Дону, Россия;

ПРИМЕНЕНИЕ СПЕЦИАЛИЗИРОВАННЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СЕТЕЙ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Аннотация. Данная статья рассматривает средства защиты сетей, которые используют правоохранительные органы. Рассмотрены элементы, которые требуются злоумышленникам для атаки, их поэтапное применение. Предложены программы для обнаружения злоумышленника, а также методы защиты, которые позволят предотвратить компрометацию всей сети в целом. Рассмотрены недостатки традиционных используемых средств защиты сетей.

Ключевые слова: правоохранительные органы, база данных, информационная безопасность, межсетевой экран следующего поколения, система обнаружения и предотвращения атаки, специализированные средства защиты.

Shumilina V.E., Candidate of Economics, Associate Professor Department of economic security, accounting and law of the DSTU Rostov-on-Don, Russia; Shumilina.vera@list.ru
Chibizov R.R.,3rd year student of the department "Economic security, accounting and law", Don State Technical University, Rostov-on-Don, Russia;

THE USE OF SPECIALISED TOOLS TO PROTECT LAW ENFORCEMENT INFORMATION NETWORKS

Annotation. This article looks at the network defenses used by law enforcement agencies. The elements required by attackers for an attack and their steps are discussed. Programs to detect an attacker are suggested, as well as methods of protection that will prevent the compromise of the entire network. Disadvantages of traditional network defenses in use are discussed.

Keywords: law enforcement agencies, database, information security, next generation firewall, attack detection and prevention system, specialized defense tools.

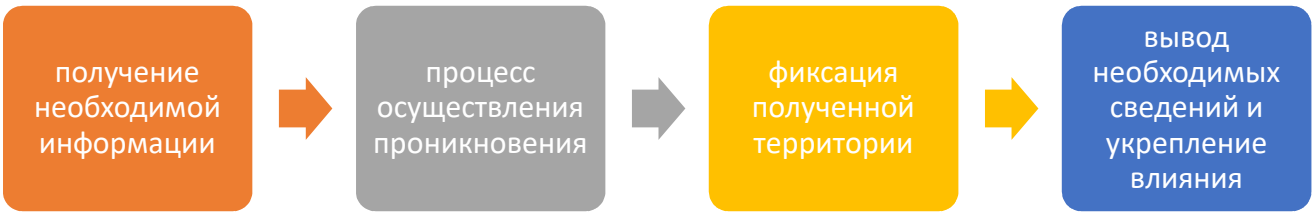
Благодаря ускоренному темпу развития информационных технологий, появились новые угрозы, которые влияют на безопасность государства и его управление. Из-за этого, перед правоохранительными органами, встает важная задача: осуществление безопасности особо важных сегментов информационной структуры нашей страны.

Под новыми угрозами понимаются совершенно новые проблемы, с которыми ранее не сталкивались правоохранительные органы, например, программные роботы и шпионские программы. Они формируют угрозу безопасности информационной структуры, что подтверждается массовыми взломами сетей правоохранительных органов России. Федеральную службу безопасности (ФСБ), в первую очередь, волнуют атаки, которые вызывают потерю конфиденциальной информации, замедляющие или останавливающие полностью доставку услуг. Меньшую степень озабоченности вызывают те проблемы, которые создают постоянные угрозы, вызываемые:

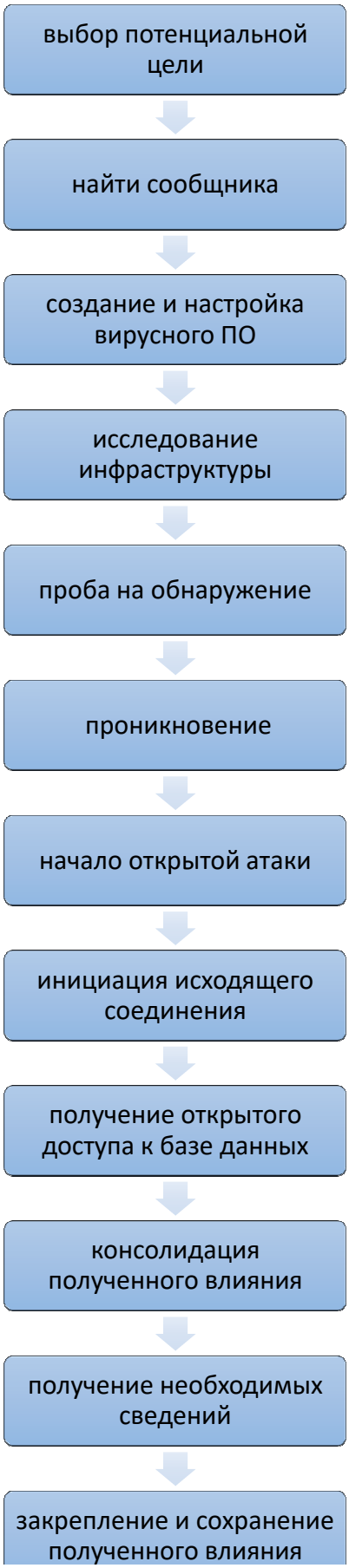
Правоохранительные органы считают лучшим средством защиты всей имеющейся информации в сети – интеграция всех сетевых способов защиты.

В наше время современные информационные технологии представляют собой многоступенчатую систему сбора, обработку и передачи информации по специальным каналам связи с использованием современных технологий. На всех этих этапах должна обеспечиваться безопасность информации. За ее защиту отвечает администратор. Он заботится о распределении ответственности между пользователями и администраторами ЭВМ и субсетей. Администратор вырабатывает и предпринимает специальные меры на случай атаки или повреждения системы, формулирует требования к сетевым паролям, контролирует их выполнение и определяет срок действия таких паролей.

Такие атаки возможны при осуществлении следующих элементов:



Развернутый план такой атаки выглядит следующим образом:



Сценарий такой атаки может выглядеть так:

Чтобы защитить собственную информацию и сведения других пользователей, правоохранительные органы используют межсетевые экраны и системы обнаружения и предотвращения вторжений. Используемые способы защиты, которые для них являются стандартными, традиционными, имеют свои критические недостатки, которыми пользуются злоумышленники. При расположении IPS-устройства за межсетевым экраном, невозможным является отследить или обнаружить сканирования, которые происходят в течение длительного времени, например, в течение нескольких недель. Злоумышленник уже может иметь достаточно большое число зараженных хостов, с которых он может исследовать полученную базу данных атакуемого.

Хост
любое устройство, предоставляющее сервисы формата «клиент-сервер» в режиме сервера по каким-либо интерфейсам и уникально определённое на этих интерфейсах. Простыми словами – пользователь

Это усложняет процесс поиска такого вредителя, усложняет процесс подготовки к его атакам. Кроме этого, ранее отмеченные системы предотвращения вторжений, могли обслуживаться разными людьми. Именно поэтому рекомендуется установление межсетевого экрана следующего поколения (NGFW) для обеспечения дополнительной защиты информации от злоумышленников.

Благодаря аккумулированию всех систем безопасности (межсетевого экрана и системы обнаружения и предотвращения вторжений) мы имеем возможность не только полностью обезопасить всю информацию от атаки злоумышленника, но и получаем шанс обнаружить само вторжение. Благодаря дополнительному анализу сетевого трафика 7-го уровня защиты, мы имеем реальную возможность обнаружить подключение к сети, определить цели такого подключения.

DDoS атаки

DDoS атаки на 7 уровень (на уровень приложения) являются простым способ, чтобы дестабилизировать работу любого сайти и при этом нарушить работу бизнеса. В отличие от атак на другие уровни, когда для отказа сайта необходимо организовать мощный поток сетевого трафика, атаки на 7 уровень могут проходить без превышения обычного уровня сетевого трафика. DDoS-атака — хакерская атака на вычислительную систему, целью которой является доведение её до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не смогут получить доступ к предоставляемым системным ресурсам, либо этот доступ будет затруднён. За счет корреляции информационных потоков и информации о пользователях правоохранительных органов появляется возможность отслеживать внутренних злоумышленников.

После того, как мы смогли вычислить проникновение злоумышленника в систему, наступает следующая фаза, когда правоохранительные органы используют традиционные средства защиты:

Главным недостатком такой защиты, который выявляется при атаке, является невозможность обнаружения вредоносного программного обеспечения. Это происходит из-за уникальности написанной программы, которая создана специально для этого вторжения. Именно поэтому невозможно обнаружить помеху в работе веб-сервисов. В связи с этим, любая конфиденциальная информация становится доступна для злоумышленника.

После того, как злоумышленник проник в базу данных через целую систему информационной безопасности, он начинает исследовать сетевое окружение. Для выявления таких движений злоумышленника, используются SIEM и IPSсистемы. Но в случае APT (программа для установки, обновления и удаления программных пакетов в операционных системах Debian и основанных на них)злоумышленник может использовать ряд специальных методов, которые способны скрыть его пребывание в сети. Например, перебор паролей может осуществляться в течение длительного времени, что позволяет обойти системы, которые сравнивают активность хостов с неким порогом срабатывания. Злоумышленник может использовать различного

рода шифрование, уязвимостей в прикладном программном обеспечении для сокрытия своей активности. Из-за этого невозможно точно предугадать способ вторжения каждого злоумышленника и подготовить под каждого соответствующие сигнатуры – характерные признаки компьютерного вируса, используемые для их обнаружения.

Именно поэтому для обнаружения незаконного вторжения необходимо использовать косвенные признаки присутствия злоумышленника в сети. Косвенным признаком может стать увеличение ICMP-трафика: обычно в сети его мало, а при передаче большого количества данных через туннель будет наблюдаться заметный всплеск. ICMP - это один из протоколов сетевого уровня в модели ISO/OSI. Его задачей является обслуживание функции контроля правильности работы сети. С его помощью передаются всякого рода, низкоуровневые сводки, с раскроенными неправильностями во время сетевых связей. Средства, используемые для защиты, остаются прежними:

Поскольку база данных правоохранительных органов постоянно пополняется, увеличиваются риски роста следующих проблем:

-децентрализация управления. Разные сотрудники из разных подразделений будут управлять системой информационной безопасности;

- мультивендорность решений. Разделение обязанностей между администраторами. Все это может привести к ошибкам администрирования, созданию дополнительных угроз внутри самой сети.

Следовательно, злоумышленнику не нужно добывать сведения обо всей сети, чтобы получить над ней полноценный контроль. Необходимо лишь выявить слабое звено какого-либо подразделения, что позволит скомпрометировать не только его, но и всю сеть целиком. Поэтому внедрение системы централизованного контроля конфигураций является важным условием безопасности системы. Это поспособствует улучшению качества работы администраторов, которые будут делать это «на местах», однако проверка целостности настроек безопасности должна осуществляться централизованно. Помимо всего прочего, существует определенный ряд решений. Они должны помочь в управлении конфигурациями межсетевых экранов различных вендоров из единой системной консоли. Данное действие позволяет минимизировать шансы ошибок во время администрирования, а также увеличивает шанс того, что система безопасности останется не взломанной.

Для того, чтобы реализовать защиту системы от направленных атак, необходимо внедрить:

Таким образом, для эффективного решения проблем отсутствия нормативного и методического обеспечения защиты компьютерной информации, отсутствия единой системы защиты и способов обеспечения безопасности базы данных, значительного отставания в выполнении программы информатизации правоохранительных органов ключевым аспектом в этом вопросе является интеграция всех информационных систем и сетей правоохранительных органов для создания единого информационного пространства, в котором все сведения будут находиться под защитой без риска утратить свою конфиденциальность.

Основополагающим решением является создание общей нормативно-методической базы и инструментального обеспечения защиты компьютерной информации для сотрудников правоохранительных органов. Предложенные подходы к реализации систем защиты сетей правоохранительных органов могут помочь в решении вопросов информационной безопасности.

Список источников

1. Абакарова О.Г. Метод интегральной оценки качества информационных систем правоохранительных органов / О.Г. Абакарова, Г.Х. Ирзаев // Научное обозрение. - 2018. - № 2. -С.180-184.
2. Котенко И.В. Методики визуального анализа в системах управления информационной безопасностью компьютерных сетей / И.В. Котенко, Е.С. Новикова // Вопросы защиты информации. - 2018. - № 3 (102). - С. 33-42.
3. Клейменов С.А. Администрирование в информационных системах / С.А. Клейменов, В.П. Мельников, А.М. Петраков. - М.: Академия, 2017. - 272 с.
4. Губина Е.А. Проектирование информационной системы на основе связывания CASE-инструментария и реляционной базы данных / Е.А. Губина, Г.Х. Ирзаев, М.Г. Адеева // Наука и бизнес: пути развития. - 2019. - № 4 (34). - С. 75-79.
5. Шумилина, В. Е. Информационная безопасность как составляющая экономической безопасности предприятия / В. Е. Шумилина, Е. В. Тетунашвили // Управление безопасностью бизнеса в современных условиях. – Москва : AUSPUBLISHERS, 2021. – С. 119-129. – EDN FESZVK.
6. Шумилина, В. Е. Роль и место правоохранительных органов в обеспечении национальной безопасности / В. Е. Шумилина, А. А. Борзых // Проблемы экономики и права в современной России, Ростов-на-Дону, 15 декабря 2020 года – 28 2021 года. – Мельбурн: AUS PUBLISHERS, 2021. – С. 131-135. – EDN UFIRRS.
7. Шумилина, В. Е. Экономическая преступность в информационной среде / В. Е. Шумилина, Т. А. Щербакова, А. Я. Кочетов // Kant. – 2021. – № 2(39). – С. 121-126. – DOI 10.24923/2222-243X.2021-39.23. – EDN BXFCCP.

8. Шумилина, В. Е. Основные проблемы защиты конфиденциальной информации и пути их решения / В. Е. Шумилина, Ю. И. Коптева, С. А. Тевосян // : Современные проблемы экономической безопасности, учета и права в Российской Федерации. Том 3, 11 января 2018 года – 31 2019 года, 2019. – С. 9. – DOI 10.26526/conferencearticle_5c5060d2f3afe7.25271992. – EDN YWPACT.

References

1. Abakarova O.G. The method of integral assessment of the quality of information systems of law enforcement agencies / O.G. Abakarova, G.Kh. Irzaev // Scientific review. - 2018. - No. 2. - P. 180-184.
2. Kotenko I.V. Methods of visual analysis in information security management systems of computer networks / I.V. Kotenko, E.S. Novikova // Issues of information security. - 2018. - No. 3 (102). - S. 33-42.
3. Kleimenov S.A. Administration in information systems / S.A. Kleymenov, V.P. Melnikov, A.M. Petrakov. - M.: Academy, 2017. - 272 p.
4. Gubina E.A. Designing an information system based on linking CASE tools and a relational database / E.A. Gubina, G.Kh. Irzaev, M.G. Adeeva // Science and business: ways of development. - 2019. - No. 4 (34). - S. 75-79.
5. Shumilina, V. E. Information security as a component of the economic security of an enterprise / V. E. Shumilina, E. V. Tetunashvili // Management of business security in modern conditions. - Moscow: AUSPUBLISHERS, 2021. - P. 119-129. – EDN FESZVK.
6. Shumilina, V. E. The role and place of law enforcement agencies in ensuring national security / V. E. Shumilina, A. A. Borzykh // Problems of Economics and Law in Modern Russia, Rostov-on-Don, December 15, 2020 - 28 2021 of the year. - Melbourne: AUS PUBLISHERS, 2021. - P. 131-135. – EDN UFIRS.

7. Shumilina, V. E. Economic crime in the information environment / V. E. Shumilina, T. A. Shcherbakova, A. Ya. Kochetov // Kant. - 2021. - No. 2 (39). - S. 121-126. – DOI 10.24923/2222-243X.2021-39.23. – EDN BXFCCP.
8. Shumilina, V. E. The main problems of protecting confidential information and ways to solve them / V. E. Shumilina, Yu. I. Kopteva, S. A. Tevosyan // Modern problems of economic security, accounting and law in the Russian Federation. Volume 3, January 11, 2018 - January 31, 2019, 2019. - P. 9. - DOI 10.26526/conferencearticle_5c5060d2f3afe7.25271992. – EDN YWPACT.