DOI 10.36622/1682-7813.2024.27.2.006
УДК 004.056

ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ СЕТЕВОЙ КОНТРРАЗВЕДЫВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ КОРПОРАЦИИ (ЧАСТЬ III)

Д.В. Щербакова, А.Ю. Пекло, Ю.В. Макаров, В.М. Питолин, О.Ю. Макаров, В.Н. Кострова

Предлагается структура и содержание частных инструкций противодействия атакам типа «сетевая разведка». Разработана должностная инструкция администратора по защите информации корпорации в части защиты сети от сетевой разведки. Выделен перечень требований к функциональным знаниям администратора по защите информации, которыми он должен обладать, чтобы успешно защитить сеть организации в рамках, выделенных в частной политике подсистем защиты. Предложены основные рекомендации по выбору и настройке средств защиты для противодействия атаке типа «сетевая разведка». Разработана разграничительной матрицы доступа на основе привилегий пользователей. Сформированы требования к безопасной работе пользователя, чтобы не допустить реализацию сетевой разведки. Предложен план мероприятия по обучению пользователей в части просвещения и защиты персонала корпорации.

Ключевые слова: частная инструкция, сетевая разведка, контрразведка, средство защиты, обучение персонала.

Введение

При условии, что необходимые решения по формированию частной политики и частных регламентов уже приняты, возникает необходимость в разработке инструктивных материалов, обеспечивающих защиту от сетевой разведки на уровне конкретных решений администраторов и пользователей корпорации. Поэтому основные задачи настоящей работы следующие:

- определение основных обязанностей и функций администратора по защите информации в корпорации (далее – администратор) в части защиты от атаки типа «сетевая разведка»;
- выработка основных рекомендаций по выбору и настройке средств защиты информации в рамках противодействия сетевой атаке типа «сетевая разведка»;
- разработка разграничительной матрицы доступа на основе привилегий пользователей.

Рассмотрим возможность их решения.

Функции и обязанности администратора

Перечень требований к функциональным знаниям администратора, которыми он должен обладать, чтобы успешно защитить корпорацию в рамках выделенных в частной политике подсистем защиты от атаки типа «сетевая разведка», сформирован в табл. 1.

Таблица 1

Функциональные знаниям Администратора

Подсистема защиты корпорации от сетевой разведки	Необходимо знать
Подсистема 1 (защита от сканирования IP-адресов)	Структуру доменные имена
	Принцип работы протоколов ICMP, TCP/UDP и ARP
	Способы ротации IP
Подсистема 2 (защита от несанкционированного выявления уязвимостей)	Общие методы активного сбора информации
	Принцип работы сканера уязвимостей
	Общие принципы эксплуатации уязвимости

Продолжение табл.1

Подсистема защиты корпорации от сетевой разведки	Необходимо знать
Подсистема 3 (защита от несанкционированного сканирования портов и служб)	Состояния «открытости» портов
	Алгоритм сканирования портов
	Связь между службами и определенными типами сетевых ресурсов
Подсистема 4 (защита от прослушивания сети)	Принципы строения сети
	Методы сокрытия трафика и способы обхода ограничений для разработки мер защиты от них

Перечень требований к умениям администратора, которыми он должен владеть, чтобы успешно защитить сеть в рамках выделенных в частной политике подсистем защиты корпорации от сетевой разведки, представлен в табл. 2

Таблица 2

Требования к умениям администратора

Подсистема защиты корпорации от сетевой разведки	Необходимо уметь
Подсистема 1	Использовать протоколы защиты данных, такие как SSL и TLS
	Настраивать правила межсетевого экрана для поддержания работы протокола ICMP
	Создавать список доверенных/недоверенных сетей
Подсистема 2	Метод тестирования безопасности, который использует ловушки (Honeypots)
	Анализировать и проводить инвентаризацию компонентов контролируемой системы
	Работать со сканером уязвимостей и анализировать отчеты полученные по результатам сканирования
Подсистема 3	Создавать экземпляры сетевых служб
	Сканировать порты и анализировать отчеты полученные по результатам сканирования
Подсистема 4	Настраивать демилитаризованную зону сети
	Осуществлять эвристический анализ для выявления аномалий сетевого трафика

Выбор средств защиты информации от сетевой атаки типа «сетевая разведка»

При выборе средств защиты информации необходимо учитывать следующие факторы:

1. Уровень защиты. Средство должно обеспечивать высокий уровень защиты информации от угроз сетевой разведки.

2. Функциональные возможности. Средство должно обеспечивать обнаружение и регистрацию инцидента, выделенные в частном регламенте реагирования на инциденты нарушения сетевой безопасности Организации при атаках типа «сетевая разведка».

3. Удобство использования. Средство должно быть простым и удобным в использовании, чтобы снижать вероятность ошибок и повышать эффективность работы с ним.

4. Надежность. Средство должно быть надежным, чтобы избежать простоев и сбоев в работе, что может привести к утечке информации.

5. Расширяемость. Средство должно позволять расширяться по мере необходимости и меняться в соответствии с изменяющимися потребностями и требованиями.

Зачастую [1-4] выбор сводится к средствам защиты информации (СЗИ):

– DLP-системы;

– сканеры безопасности;

– ресурс, представляющий собой «приманку» для злоумышленника.

Более детальный список функций, выбранных СЗИ, и меры по предотвращению атаки типа «сетевая разведка», которые они реализуют, приведен в табл. 3.

Таблица 3

Описание функций выбранных СЗИ

Подсистема	Описание мер	Наименование выбранного СЗИ	Функции СЗИ
Подсистема 1	Обмен сообщениями по протоколу ICMP, по заданному списку IP-адресов	Dallas Lock 8.0	Настройка правил модуля МЭ для поддержания работы протокола ICMP.
	Фильтрование пакетов ICMP;		
	Блокировка сообщений ICMP, которые не требуются для нормального функционирования сети.		
Подсистема 2	Уточнение и учет защищаемых информационных ресурсов, программных и аппаратных средств.	Dallas Lock 8.0	Взятие под контроль объектов файловой системы и устройства через механизмы разграничения доступа и аудита целостности.
	Обнаружение новых ранее не выявленных сетевых ресурсов;	Dallas Lock 8.0	
	Тестирование на проникновение с использованием анализа защищённости.	Honeypot	Для обнаружения и изучения вторжений использование «ловушек».
	При наличии привилегий на сетевом узле осуществление системного сканирования.	Сканер-ВС	Модуль «Поиск уязвимостей», предназначенный для выявления уязвимостей программного обеспечения
	Анализ и инвентаризация компонентов контролируемой системы	Dallas Lock 8.0	Модуль «Системный аудитор», предназначенный для инвентаризации программ и аппаратных средств локальной рабочей станции

Продолжение табл. 3

Подсистема	Описание мер	Наименование выбранного СЗИ	Функции СЗИ
Подсистема 3	Контроль состояния портов устройств	Сканер-ВС	Модуль «Сканирование портов» отображает все открытые порты на хосте, которые видны для других устройств
	Предотвращение несанкционированного сканирования TCP/UDP портов	Dallas Lock 8.0	Система обнаружения вторжений (СОВ), выявляющая аномалии сетевого трафика. Список атак данного модуля содержит тип «Сканирование портов»
	Ограничение доступа к запущенным службам;	Dallas Lock 8.0	«Высокий» уровень защиты СОВ задает ограничения для запускать службы
	Контроль запуска сетевых служб и сервисов	Dallas Lock 8.0	Модуль СОВ позволяет контролировать запуск сетевых служб и сервисов
Подсистема 4	Контроль доступа удаленных пользователей к ресурсам сетевых приложений	Dallas Lock 8.0	Для защищенного компьютера настройка удаленного доступа с незащищенных ресурсов.
	Отслеживание действий субъектов доступа на сетевом уровне	Dallas Lock 8.0	На выбранном объекте защите есть возможность подключить контроль целостности и рассчитать его контрольную сумму
	Фильтрация сетевого трафика	Dallas Lock 8.0	Фильтрация сетевого трафика через список сигнатур трафика и сведения о: действиях, протоколах, источниках, и направлениях.

Рекомендации по настройке средств защиты информации от сетевой разведки

Основные рекомендации по настройке выбранных СЗИ представлены в табл. 4 [5-8].

Таблица 4

План действий Администратора при выборе и настройке СЗИ

Выбор наиболее опасных сочетаний		Требование к защите информации	Настраиваемый СЗИ	Рекомендация по настройке параметров
Вектор атаки	Уязвимость			
VA_1	CWE-20	Наличие фильтрации пакетов ICMP;	Dallas Lock 8.0	Настройка в модуле СОВ обнаружение атаки типа «Ping of death»
VA_1	CWE-200	Существование блокировки сообщений ICMP, которые не требуются для нормального функционирования сети.	Dallas Lock 8.0	Запрет вызова функции для отправки ICMP сообщений в Параметрах МЭ в категория «Фильтр»
VA_1	CWE-862	Наличие контроля работы DNS-сервера	Dallas Lock 8.0	Создание правила для защиты локальных DNS имен
VA_2	CWE-20	Наличие учета защищаемых программных и аппаратных средств системы.	Dallas Lock 8.0	Включение аудита и контроля целостности для информационных ресурсов, программных и аппаратных средств, ресурсов файловой системы во вкладке «Контроль ресурсов» Dallas Lock 8.0
VA_2	CWE-200	Возможность поиска новых (ранее не выявленных) сетевых ресурсов.		
VA_2	CWE-862	Осуществление анализа защищенности в режиме тестирования на проникновение.	Honeypot	1. Открытие портов в качестве наживки для злоумышленника с помощью пакета PenTBox, чтобы побудить его проникнуть в сеть для любого незаконного использования 2. Настройка отображение результата попытки подключения
VA_2	CWE-20	Наличие системного сканирования через привилегии на сетевом узле.	Сканер-ВС	Настройка «полного сканирования» сети Организации по расписанию

Продолжение табл. 4

Выбор наиболее опасных сочетаний		Требование к защите информации	Настраиваемый СЗИ	Рекомендация по настройке параметров
Вектор атаки	Уязвимость			
VA_2	CWE-200	Возможность контроля запуска сетевых служб и сервисов.	Dallas Lock 8.0	Настройка эвристики БС, позволяющая определять несанкционированный запуск службы.
VA_2	CWE-862	Осуществление анализа и инвентаризации компонентов контролируемой системы.	Dallas Lock 8.0	1. С помощью средства контроля подключения носителей информации создание перечня разрешенных сменных накопителей. 2. Периодическая проверка подключения устройств с помощью раздела «Контроль ресурсов».
VA_3	CWE-20	Возможность предотвращения несанкционированного сканирования TCP/UDP портов.	Dallas Lock 8.0	Настройка повышения уровня блокировки для атаки типа «Сканирование портов» во вкладке СОВ.
VA_3	CWE-200	Введение ограничений доступа к запущенным службам	Dallas Lock 8.0	Настройка контроля целостности для служб.
VA_4	CWE-20	Контроль доступа пользователей к ресурсам сетевых приложений	Dallas Lock 8.0	1. Настройка замкнутой программной среды с помощью неактивного режима работы. 2. Отображение списка текущих сетевых соединений компьютера, в котором отображается статистика по каждому соединению с привязкой к процессам.

Окончание табл. 4

Выбор наиболее опасных сочетаний		Требование к защите информации	Настраиваемый СЗИ	Рекомендация по настройке параметров
Вектор атаки	Уязвимость			
VA_4	CWE-200	Отслеживанию действий субъектов доступа на сетевом уровне	Dallas Lock 8.0	Включение аудита доступа\запуска
VA_4	CWE-209	Фильтрация сетевого трафика	Dallas Lock 8.0	Через межсетевое экранирование создание списка перехватываемых исходящих портов.

Разграничительная матрица доступа на основе привилегий пользователей

Разграничительная матрица доступа (РМД) — это инструмент управления доступом, который определяет, какие пользователи и роли могут получить доступ к определенным ресурсам, файлам, сервисам и функциям в системе. Она определяет права доступа и привилегии для каждого пользователя и ограничивает доступ только тем пользователям, которым это необходимо. На основании выделенных объектов защиты, в рамках защиты сети корпорации от атаки разработана РМД (табл.5).

Таблица 5

Разграничительная матрицы доступа

Объекты защиты	Роли пользователей		
	Администратор	Системный администратор	Сотрудник организации
Сервер безопасности DL	Полный доступ	Доступ запрещен	Доступ запрещен
Honeypot	Полный доступ	Полный доступ	Полный доступ
Серверное оборудование (сервера)	Полный доступ	Физический доступ без права вносить изменение в конфигурационные файлы	Доступ запрещен
Сетевое и телекоммуникационное оборудование	Полный доступ	Физический доступ без права вносить изменение в конфигурационные файлы	Доступ запрещен
TCP/UDP порты	Полный доступ	Доступ к просмотру состояний портов	Доступ запрещен
Сетевые службы	Полный доступ	Доступ к просмотру списка служб без возможности вносить изменения	Доступ запрещен
Файлы журналов регистрации событий безопасности	Полный доступ	Доступ к просмотру предупреждения незащищенных сетевых событий	Доступ к просмотру предупреждений о незащищенных сетевых событиях

Частная инструкция пользователя

Основные цели разработки настоящей инструкции таковы:

- формирование требований к безопасной работе пользователя, чтобы не допустить реализацию сетевой разведки;
- планирование мероприятий по обучению пользователей в части просвещения и защиты от сетевой разведки.

Требования к безопасной работе внутреннего пользователя

Чтобы не допустить реализацию сетевой атаки типа «сетевая разведка» пользователю запрещается:

– устанавливать программы-сканеры (например, nmap);

– открывать файлы с нестандартным расширением;

– запускать неизвестное программного обеспечения или подключать расширения браузера (некоторые сканеры могут быть запущены через вредоносные вложения или вредоносные ссылки);

– пропускать обновления операционной системы и программного обеспечения.

Аномалии, связанные с разведывательными действиями на компьютере сотрудника организации, могут включать в себя следующее:

– АРМ довольно новый, но внезапно начал работать гораздо медленнее;

– всплывающие окна, заполняющие экран и мгновенно закрывающиеся автоматически;

– подозрительная активность браузера (в истории браузера находятся страницы, которые сотрудник точно не посещал);

– всплывающие сообщения-предупреждения о сканировании компьютера от уставленного средства защиты.

Обучение и инструктирование пользователя

В целях повышения защищенности системы и противодействию атаке сетевой разведке пользователю необходимо пройти обучение, которое будет включать в себя план мероприятий, представленный в табл. 6.

Таблица 6

План мероприятий по обучению пользователей в части просвещения и защиты от сетевой разведки

№ п/п	Наименование мероприятия	План мероприятия
1	Информирование сотрудников об общих методах и конкретных способах сбора информации, которые может использовать злоумышленник при реализации атаки типа «сетевая разведка»	1) Данные, которые собирает злоумышленник на этапе разведки сети. 2) Активные методы сбора информации. а) Цель и способы сканирования портов. б) Методы и способы сканирования уязвимостей. 3) Пассивные методы сбора информации а) Интернет-мониторинг. б) Анализ открытых источников информации, чем опасен
2	Проведение специальных лекций по системным уязвимостям	1) Примеры реализации уязвимостей. 2)Метод детектирования уязвимостей. 3) Управление уязвимостями
3	Ознакомление сотрудников с уголовными последствиями кибершпионажа	Разбор основных мер пресечения кибершпионажа

Следуя вышеперечисленным инструкциям, можно существенно снизить риски успешности атак типа «сетевая разведка» на защищенную корпоративную сеть.

Заключение

Предложенные в настоящей работе решения ориентированы на инструкции по выбору СЗИ, их настройке, организации разграничения доступа, безопасной работе и обучению пользователей. В условиях массированной сетевой разведки, предваряющей практически все компьютерные атаки на корпоративные сети, предлагаемые инструкции имеют существенное практическое значение и могут быть рекомендованы для использования корпорациями различного масштаба и назначения. При соответствующей их адаптации к корпоративной специфике может

быть существенно повышена защищённость от атак типа «сетевая разведка».

Список литературы

1. Методический документ от 05.02.2021 ФСТЭК России. Методика оценки угроз безопасности информации. URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения: 12.01.24).

2. Сканер-ВС - URL: https://scaner-vs.ru/ (дата обращения: 12.01.24).

3. Подробное руководство по Honeypot - URL: https://habr.com/ru/companies/alexhost/articles/528796/ (дата обращения: 12.01.24).

4. Технология Honeypot, Часть 1: Назначение Honeypot - URL: https://www.securitylab.ru/analytics/275420.php (дата обращения: 12.01.24).

5. Подробное руководство по Honeypot - URL: https://habr.com/ru/companies/alexhost/articles/528796/ (дата обращения: 12.01.24).

6. Технология Honeypot, Часть 1: Назначение Honeypot. URL: https://www.securitylab.ru/analytics/275420.php (дата обращения: 12.01.24).

7. Система Защиты Информации Dallas Lock 8.0 (версия 8.0.710.0). Руководство администратора. URL: https://dallaslock.ru/include/sert/DL8.0-K_Руководство-по-эксплуатации_2022.pdf (дата обращения: 12.01.24).

8. Средство анализа защищенности Сканер-ВС. Руководство пользователя. URL: https://scaner-vs.ru/wp-content/uploads/2017/09/Руководство-пользователя.pdf -(дата обращения: 12.01.24).

Московский государственный университет имени М.В. Ломоносова
Moscow State University named after M.V. Lomonosov

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 07.02.2024

Информация об авторах

Щербакова Дарья Владимировна – аспирант, Московский государственный университет имени М.В. Ломоносова, e-mail: alexanderostapenkoias@gmail.com

Пекло Арина Юрьевна – студентка, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Макаров Юрий Вадимович – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Питолин Владимир Михайлович – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Макаров Олег Юрьевич – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Кострова Вера Николаевна – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

ORGANIZATIONAL AND LEGAL SUPPORT OF NETWORK COUNTERINTELLIGENCE ACTIVITIES OF THE CORPORATION (PART III)

D.V. Shcherbakova, A.Yu. Peklo, Yu.V. Makarov, V.M. Pitolin, O.Yu. Makarov, V.N. Kostrova

The structure and content of private instructions counteracting attacks of the type “network intelligence” is proposed. The job description of the corporation’s information in terms of network protection from network intelligence has been developed. A list of requirements for the functional knowledge of the administrator for the protection of information that he must have in order to successfully protect the organization’s network within the framework of protection subsystems in private policy has been allocated. The main recommendations on the selection and setting of protective equipment to counteract an attack type “network intelligence” are proposed. Developed by a delimiting access matrix based on user privileges. The requirements for the safe work of the user have been formed to prevent the implementation of network intelligence. A plan for user training in terms of education and protection of the corporation personnel has been proposed.

Keywords: private instruction, network intelligence, counterintelligence, means of protection, staff training.

Submitted 07.02.2024

Information about the authors

Daria V. Shcherbakova – graduate student, Moscow State University named after M.V. Lomonosov, e-mail: Alexanderostapenkoias@gmail.com

Arina Yu. Peklo – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Yuri V. Makarov – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Vladimir M. Pitolin – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Oleg Yu. Makarov – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Vera N. Kostrova – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com