DOI 10.36622/1682-7813.2024.27.1.007
УДК 004.056.57

СЕТЕВЫЕ АТАКИ С ПОМОЩЬЮ «СНИФФЕР-ПАКЕТОВ»: ПОСТРОЕНИЕ РИСК-ЛАНДШАФТА

А.А Золотарев, Д.А. Нархов, М.И. Бочаров, А.И. Мордовин, Н.М. Радько, О.В. Поздышева, А.Г. Краснобородкин

В статье рассматривается проблема осуществления сетевых атак на корпоративные сети с помощью «сниффер-пакетов» и обосновывается актуальность данной проблемы. Приводятся наиболее актуальные сочетания вектор-уязвимость для данного типа атак. Описывается и реализуется методика риск-оценки на основе данных по атакам с помощью «сниффер-пакетов» и уязвимостям к ним. Рассчитаны ущербы от реализации атак. Сформирована матрица смежности векторов атак с помощью «сниффер-пакетов» и уязвимостей корпоративных сетей предприятия к данному виду атак. По полученным расчетным данным риск-оценок построен риск-ландшафт. На основе риск-ландшафта проводится оценка степени опасности уязвимостей и векторов атак, а также выделены наиболее опасные их сочетания. Таким образом, были получены все необходимые для формирования частной политики и выработки мер противодействия атакам, проводимых с помощью «сниффер-пакетов», данные.

Ключевые слова: корпоративная сеть, векторы атаки, уязвимости, риск-ландшафт.

Введение

Перевод бизнес-процессов организаций в виртуальное пространство создает необходимость совершенствования внутриорганизационного правового регулирования по защите информации на основе исследования наиболее опасных сочетаний уязвимостей и векторов атак. Риск-анализ сочетаний векторов атак и уязвимостей необходим для получения адекватной картины безопасности, а также позволяет эффективно совершенствовать внутриорганизационные нормативные документы и успешно бороться с нарастающим числом сетевых атак во всем поле реализуемых злоумышленниками сценариев нападений.

Целью данного исследования является выработка мер обеспечения информационной безопасности предприятия для противодействия атакам с помощью «сниффер-пакетов» на основе риск-анализа сценариев атак и используемых ими уязвимостей.

Для достижения поставленной цели решаются следующие задачи:

1) сформировать и описать множества сценариев атак с помощью «сниффер-пакетов» и уязвимостей корпоративных сетей предприятия к данному виду атак,необходимых и достаточных для последующего риск-анализа, путем анализа интернет-пространства и других информационных источников,

2) на основе анализа статистических данных выявить наиболее распространенные сценарии атаки и построить риск-ландшафт для выявления наиболее опасных сочетаний сценарий-уязвимость.

Риск-ландшафт уязвимостей и векторов атак с помощью «сниффер-пакетов»

Векторы атак имеют множество классификаций и видов [1], но в данной работе рассмотрены популярные сценарии атак с помощью «сниффер-пакетов» из матрицы тактик и техник ресурса attack.mitre.org [1,2]. Сценарии заданного типа атак представлены в табл. 1.

Данные, собранные с помощью сценариев (табл. 1), могут включать учетные данные пользователя, особенно те, которые отправляются по небезопасному незашифрованному протоколу. Методы отравления разрешения служб имен, такие как отравление LLMNR / NBT-NS и SMB Relay, также могут использоваться для получения учетных данных для веб-сайтов, прокси-серверов и внутренних систем путем перенаправления трафика злоумышленнику.

Таблица 1

Векторы атак с помощью «сниффер-пакетов»

Вектор атаки	Описание
VA_1 Перечисление сетевых подключений (Network Connection Enumeration)	Этап 1. Злоумышленник получает доступ к узлу сети жертвы. Этап 2. Злоумышленники могут выполнять перечисление сетевых подключений, чтобы обнаружить информацию о схемах связи устройств. Если злоумышленник может проверить состояние сетевого подключения с помощью таких инструментов, как Netstat. Этап 3. Злоумышленник также может использовать прослушивание сети для просмотра сетевого трафика на предмет получения подробной информации об источнике, пункте назначения, протоколе и контенте.
VA_2 Прослушивание сети (Network Sniffing)	Этап 1. Злоумышленник подключается к каналу передачи информации. Этап 2. Злоумышленник может попытаться прослушивать трафик, чтобы получить информацию о цели. Уровень важности этой информации может различаться. Относительно важной информацией могут быть данные для входа в систему. Этап 3. Учетные данные пользователя могут быть отправлены по незашифрованному протоколу, такому как Telnet, который может быть перехвачен и получен с помощью анализа сетевых пакетов.
VA_3 Удаленное обнаружение системы (Remote System Discovery)	Этап 1. Злоумышленник подключается к сетевой инфраструктуре жертвы. Этап 2. Нарушитель проводит действия по получению иных систем по IP-адресу, имени хоста или другому логическому идентификатору в сети. Этап 3. Зачастую, информация, полученная таким образом, используется атакующим для последующего перемещения внутри системы и (или) сокрытия своих действий. В таком случае инструментами злоумышленников могут выступать утилиты, доступные в операционной системе или программном обеспечении поставщика.
VA_4 Удаленное обнаружение системной информации (Remote System Information Discovery)	Этап 1. Злоумышленник подключается к основным концентрирующим сетевым устройствам.

Продолжение табл. 1

Вектор атаки	Описание
	Этап 2. Злоумышленник может попытаться получить подробную информацию об удаленных системах и их периферийных устройствах, таких как марка / модель, роль и конфигурация. Этап 3. Злоумышленники могут использовать информацию, полученную при удаленном обнаружении системной информации, для помощи в нацеливании и формировании последующего поведения. Кроме того, конфигурация системы может быть использована для определения области последующего использования технологии.
VA_5 Беспроводное прослушивание (Wireless Sniffing)	Этап 1. Злоумышленник находится в зоне действия беспроводной сети или получил доступ к маршрутизатору. Этап 2. Злоумышленники могут пытаться перехватить радиочастотную (RF) связь, используемую для дистанционного управления и отчетности в распределенных средах. Вот несколько примеров беспроводных протоколов, которые можно найти в киберфизических средах: WirelessHART, Zigbee, WIA-FA и спектр общественной безопасности 700 МГц.

Для расчетов будем использовать данные, распределенные по стандартной классификации атак UNSW-NB15 [3]. Поскольку в нашем исследовании интересуют атаки с помощью «сниффер-пакетов», то из имеющегося набора данных, сортируя по параметрам, выделенным в табл. 1, получим распределение, показанное на рис.1.

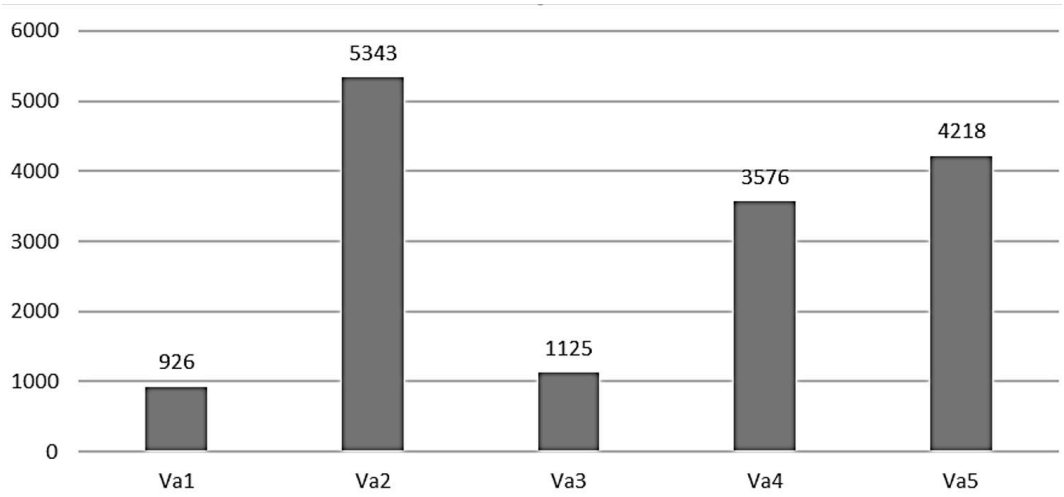

Рис. 1. Количество атак атак с помощью «сниффер-пакетов» по векторам из табл. 1 по данным DataSet «UNSW-NB15»

На основе статистики, приведенной в базе данных угроз ФСТЭК [4] и ресурса CWE [5] с учетом выделенных в табл. 1 векторов атак запишем возможные уязвимости в табл. 2.

Таблица 2

Уязвимости к «сниффер-пакетам»

Наименование уязвимости	Описание	Идентификатор CWE
1	2	3
VB_1 Использование обратного разрешения DNS для критически важных с точки зрения безопасности действий	Поскольку DNS-имена могут быть легко подделаны или сообщены неверно, и продукту может быть затруднительно определить, был ли скомпрометирован доверенный DNS-сервер, DNS-имена не являются допустимым механизмом аутентификации. В момент выполнения продуктом обратного разрешения DNS для IP-адреса, контролирующий DNS-сервер для этого IP-адреса злоумышленник может передать серверу команду возвращать произвольное имя хоста. В результате, такие действия позволяют нарушителю обойти процесс аутентификации, записать некорректное имя хоста в файлы журнала, чтобы скрыть действия или выполнить другие атаки. Злоумышленники могут подделывать имена, либо компрометируя DNS-сервер и изменяя его записи, либо получая законный контроль над DNS-сервером, связанным с их IP-адресом.	CWE-350
VB_2 Передача конфиденциальной информации в открытом виде	Многие каналы связи могут быть "прослушаны" злоумышленниками во время передачи данных. При прохождении пакетов через множество промежуточных узлов от источника к получателю некоторые участники могут иметь привилегированный доступ к сетевому интерфейсу или любому каналу связи. В результате злоумышленники могут перехватить сетевой трафик. Когда полные сообщения записываются или протоколируются, например, с помощью дампа пакета, злоумышленник может попытаться получить дамп спустя долгое время после того, как передача произошла, и попытаться получить открытый текст из записанных сообщений в самом дампе.	CWE-319

Продолжение табл. 2

1	2	3
VB_3 Отсутствует шифрование конфиденциальных данных	Отсутствие надлежащего шифрования данных не дает гарантий конфиденциальности, целостности и подотчетности, которые обеспечивает должным образом внедренное шифрование.	CWE-311
VB_4 Доверие IP-адресу для аутентификации	Злоумышленники могут подделать исходный IP-адрес отправляемых ими пакетов. Для раскрытия ответных пакетов, злоумышленник должен проводить анализ трафика, циркулирующего между машиной-жертвой и поддельным IP-адресом. Для этого нарушители обычно пытаются оказаться в той же подсети, что и компьютер жертвы.	CWE-291
VB_5 Канал, доступный не через конечную точку	Для установления безопасной связи между двумя точками важно проводить сверку идентичности объектов на каждом конце канала связи. Непоследовательная или посредственная проверка зачастую приводит к недостаточной или некорректной идентификации. Это может иметь такие негативные последствия как неуместное доверие к объекту на другом конце канала. Злоумышленник может использовать это, вставляя между взаимодействующими объектами и маскируясь под исходный объект .	CWE-300
VB_6 Вставка конфиденциальной информации в отправляемые данные	Конфиденциальная информация может включать данные, которые являются конфиденциальными сами по себе (например, учетные данные или личные сообщения) или иным образом полезны при дальнейшей эксплуатации системы (например, внутренняя структура файловой системы).	CWE-201

На основе данных банка данных угроз ФСТЭК России за 2022 год, выписав число упоминаний уязвимостей к атакам с помощью «сниффер-пакетов», из табл. 2 получаем данные, приведенные в табл. 3. На рис. 2 представлена иллюстрация по табл. 3 (общее количество упоминаний – 5345).

Таблица 3

Число упоминаний уязвимостей к атакам с помощью «сниффер-пакетов за 2022 год

Уязвимость	Количество упоминаний
CWE-350	54
CWE-319	326
CWE-311	431
CWE-291	266
CWE-300	63
CWE-201	59
Число упоминаний уязвимостей (общее):	5345

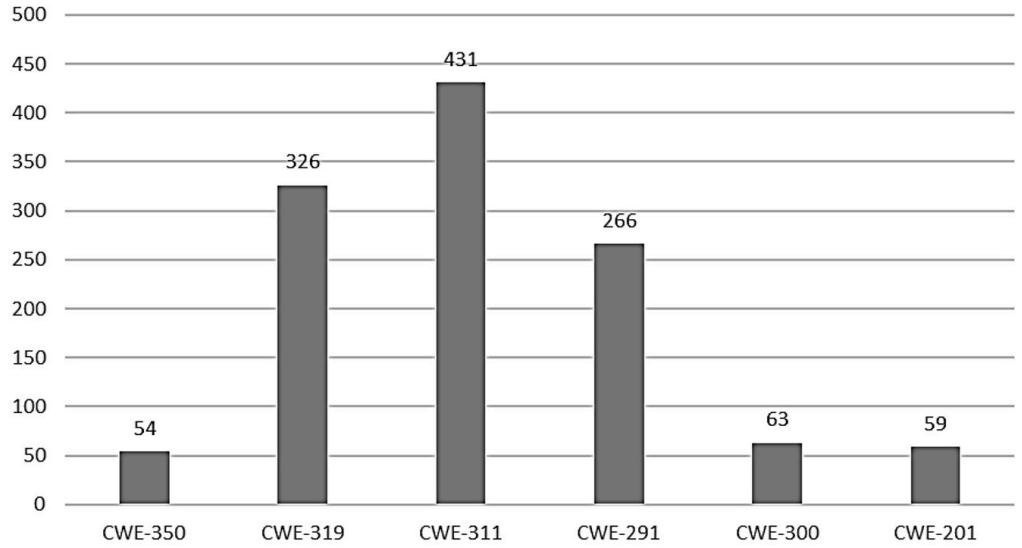

Рис. 2. Число упоминаний уязвимостей к атакам с помощью «сниффер-пакетов» в 2022 году

Наиболее популярными уязвимостями при реализации атак с помощью «сниффер-пакетов» стали отсутствие или плохое шифрование данных. Риск рассчитывается по формуле, предложенной в [6] для расчета сетевых атак на уровне приложений, поскольку в нашем случае она применима.

$$\overline{Risk_{sij}} = F_{sij} \times \overline{U_{sij}}, \quad (1)$$

где F_{sij} – частота успешного использования j-ой уязвимости при реализации атаки типа S посредством i-го вектора атаки, т. е. отношение числа упоминаний j-той уязвимости к общему количеству упоминаний всех уязвимостей при реализации атаки типа S за исследуемый период;

$\overline{U_{sij}}$ – ущерб от реализации атаки типа S посредством i-го вектора.

Ущерб от реализации атаки в нормированном виде рассчитывается следующим образом [6]:

$$\overline{U_{sij}} = \frac{(\Delta t_{si})}{max\ [\Delta t]}, \quad (2)$$

где Δt_{si} – среднестатистическое значение простоя атакуемой сети в результате успеха атаки типа S посредством i-го вектора;

$max\ [\Delta t]$ – максимальное значение Δt_{si}.

Исходные данные для расчетов сформируем из «UNSW-NB15» [3], сортируя их по времени простоя. Результат показан в табл. 4. Проведем расчет для F_{sij} и $\overline{U_{sij}}$ по формуле (2), используя исходные данные из табл. 3 и 4., а также формулу (2). Результаты расчетов приведены в табл. 5 и 6.

Таблица 4

Среднестатистическое время простоя для каждого вектора атаки

Векторы атаки	Δt_{si}
Va_1	0,008
Va_2	0,005
Va_3	0,006
Va_4	0,005
Va_5	0,002

Таблица 5

Значения F_{sij} для уязвимостей к атакам с помощью «сниффер-пакетов» ($\times 10^{-3}$)

Уязвимость	F_{sij}
CWE-350	5,23
CWE-319	32,26
CWE-311	43,57
CWE-291	26,45
CWE-300	6,22
CWE-201	5,47

Таблица 6

Значения $\overline{U_{sij}}$ для векторов атак с помощью «сниффер-пакетов»

Векторы атаки	$\overline{U_{sij}}$
Va_1	0,12
Va_2	0,39
Va_3	0,13
Va_4	0,36
Va_5	0,32

Для построения риск-ландшафта необходимо сформировать матрицу смежности векторов атак с помощью «сниффер-пакетов» и уязвимостей корпоративных сетей предприятия к данному виду атак, с учетом последствий от их эксплуатации для ресурсов системы [7,8] (табл. 7).

По результатам, представленным в табл. 5-7, с помощью формулы (1) рассчитываем риски реализации атак с помощью «сниффер-пакетов». Результаты расчетов образуют матрицу рисков, приведенную в табл. 8.

Таблица 7

Матрица смежности векторов атак с помощью «сниффер-пакетов» и уязвимостей к ним

	CWE-350	CWE-319	CWE-311	CWE-291	CWE-300	CWE-201
Перечисление сетевых подключений	0	0	0	1	1	0
Прослушивание трафика	0	1	1	1	1	1
Удаленное обнаружение системы	1	0	1	1	0	0
Удаленное обнаружение системной информации	1	1	1	1	0	0
Беспроводное прослушивание трафика	0	1	1	0	1	1

Таблица 8

Матрица рисков реализации атак с помощью «сниффер-пакетов» через уязвимости

	CWE-350	CWE-319	CWE-311	CWE-291	CWE-300	CWE-201
Перечисление сетевых подключений	0	0	0	0,101	0,068	0
Прослушивание трафика	0	0,542	0,503	0,146	0,134	0,094
Удаленное обнаружение системы	0,072	0	0,078	0,113	0	0
Удаленное обнаружение системной информации	0,084	0,106	0,487	0,435	0	0
Беспроводное прослушивание трафика	0	0,552	0,497	0	0,093	0,068

На основе табл. 8 построим риск-ландшафт реализации атак, проводимых с помощью «сниффер-пакетов» (рис. 3). Используя полученные данные, проиллюстрированные на рис.3 и сведенные в табл. 8, получим наиболее опасные сочетания векторов атак с помощью «сниффер-пакетов» и уязвимостей к ним (табл. 9).

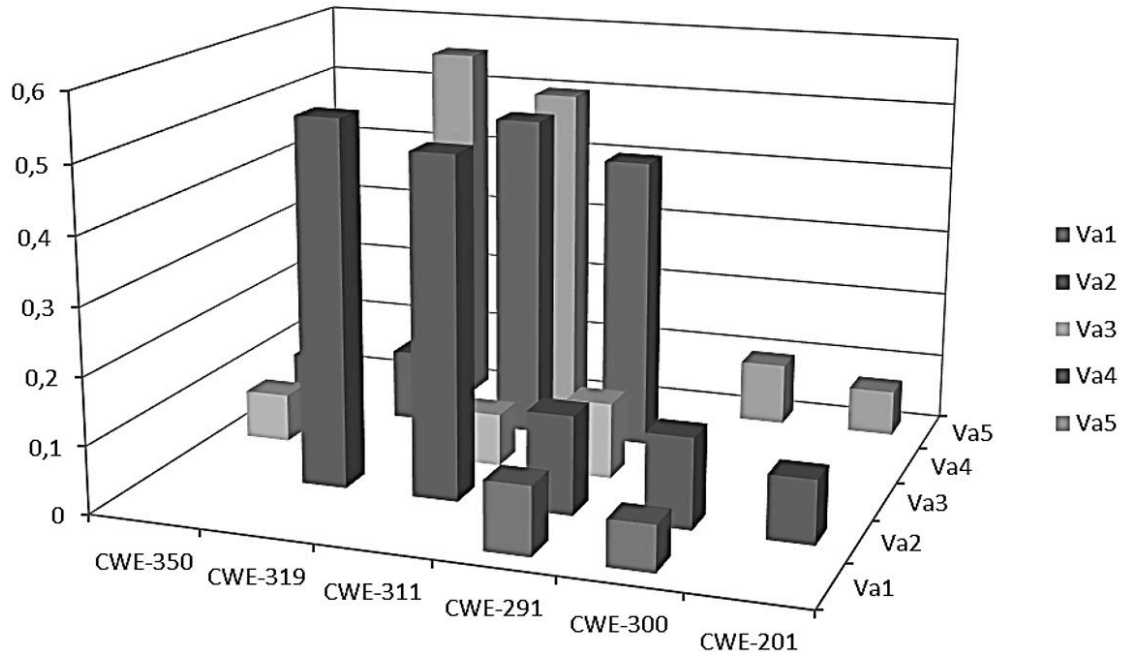

Рис. 3. Риск-ландшафт реализации атак с помощью «сниффер-пакетов» на компоненты корпоративной сети

Таблица 9

Наиболее опасные сочетания уязвимостей и векторов атаки с помощью «сниффер-пакетов»

Вектор атаки	Уязвимость
Перечисление сетевых подключений (Network Connection Enumeration) (Va_1)	CWE-291 Доверие IP-адресу для аутентификации
	CWE-300 Канал, доступный не через конечную точку
Прослушивание сети (Network Sniffing) (Va_2)	CWE-311 Отсутствует шифрование конфиденциальных данных
	CWE-319 Передача конфиденциальной информации в открытом виде

Продолжение табл. 9

Вектор атаки	Уязвимость
Удаленное обнаружение системы (Remote System Discovery) (Va_3)	CWE-311 Отсутствует шифрование конфиденциальных данных
	CWE-291 Доверие IP-адресу для аутентификации
Удаленное обнаружение системной информации (Remote System Information Discovery) (Va_4)	CWE-291 Доверие IP-адресу для аутентификации
	CWE-311 Отсутствует шифрование конфиденциальных данных
Беспроводное прослушивание (Wireless Sniffing) (Va_5)	CWE-311 Отсутствует шифрование конфиденциальных данных

Заключение

В соответствии с данными из табл. 9 можно сделать вывод, что атаки в сочетании с уязвимостями, связанными с недостаточной защитой канала, передачей конфиденциальной информации в открытом виде и полным отсутствием шифрования передаваемых данных, являются наиболее опасными комбинациями [9]. Для разработки частных политики и регламентов наименее опасные сочетания зачастую не учитываются, так как их риски являются пренебрежимо малыми, а меры противодействия – дорогостоящими. Таким образом, были получены все необходимые для формирования частной политики и выработки мер противодействия атакам, проводимых с помощью «сниффер-пакетов», данные.

Список литературы

1. База знаний MITRE. URL: https://attack.mitre.org/ (дата обращения 21.01.2024).

2. Common Attack Pattern Enumeration and Classification.URL: https://capec.mitre.org (дата обращения 21.01.2024).

3. DataSet UNSW-NB15. URL: https://www.kaggle.com/datasets/alextamboli/unsw-nb15 (дата обращения 21.01.2024).

4. Банк данных угроз безопасности информации. URL : https://bdu.fstec.ru/threat

5. Common Wearness Enumeration. URL: https://cwe.mitre.org/index.html (дата обращения 21.01.2024).

6. Хромых С.А. Сетевые атаки на уровне приложений: риск-ландшафт и частная политика информационной безопасности предприятия / С.А. Хромых, Г.А. Остапенко, Д.В. Щербакова, А.А. Остапенко // Информация и безопасность. 2023. Т. 26. Вып. 2. С. 261-276.

7. Национальная база данных уязвимостей. URL : https://nvd.nist.gov/ (дата обращения 21.01.2024).

8. Уязвимости и угрозы сниффер-пакетов в 2020-2021 гг. URL: https://www.ptsecurity.com/ru-ru/research/analytics/web-vulnerabilities-2020-2021/ (дата обращения 21.01.2024).

9. GitHub База данных машинного обучения алгоритмам обнаружения сетевых атак. URL: https://github.com/srtk88/Machine-learning-algorithms-for-detecting-network-attacks-with-UNSW-NB15-data-set (дата обращения 21.01.2024).

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 03.02.2024

Информация об авторах

Золотарев Алексей Александрович – студент, Воронежский государственный технический университет, e-alexanderostapenkoias@gmail.com

Нархов Дмитрий Андреевич – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Бочаров Михаил Иванович – канд. техн. наук, доцент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Мордовин Андрей Иванович – старший преподаватель, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com
Радько Николай Михайлович – канд. техн. наук, доцент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com
Поздышева Оксана Валентиновна – канд. техн. наук, доцент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com
Краснобородкин Александр Геннадьевич – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

NETWORK ATTACKS USING "SNIFFER PACKETS": BUILDING A RISK LANDSCAPE

A.A. Zolotarev, D.A. Narhov, M.I. Bocharov, A.I. Mordovin, N.M. Radko, O.V. Pozdysheva, A.G. Krasnoborodkin

The article discusses the problem of carrying out network attacks on corporate networks using “sniffer packets” and substantiates the relevance of this problem. The most relevant vector-vulnerability combinations for this type of attack are given. A risk assessment methodology is described and implemented based on data on attacks using “sniffer packages” and vulnerabilities to them. The damage caused by the attacks has been calculated. A matrix of contiguity between attack vectors using “sniffer packets” and the vulnerabilities of enterprise corporate networks to this type of attack has been generated. Based on the obtained calculated risk assessment data, a risk landscape was constructed. Based on the risk landscape, the degree of danger of vulnerabilities and attack vectors is assessed, and their most dangerous combinations are identified. Thus, all the data necessary for the formation of private policy and the development of measures to counter attacks carried out using “sniffer packages” were obtained.

Keywords: corporate network, attack vectors, vulnerabilities, risk landscape.

Submitted 03.02.2024

Information about the authors
Alexey A. Zolotarev – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com
Dmitry A. Narhov – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com
Mikhail I. Bocharov – Cand. Sc. (Technical), Associate Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com
Andrey I. Mordovin – Senior Lecturer, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com
Nikolay M. Radko – Cand. Sc. (Technical), Associate Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com
Oksana V. Pozdysheva – Cand. Sc. (Technical), Associate Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com
Alexander G. Krasnoborodkin – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com