DOI 10.36622/VSTU.2023.26.2.003
УДК 004.056.47

СОЗДАНИЕ КИБЕРПОЛИГОНА: БЛОК НАВИГАЦИИ ПО СРЕДСТВАМ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ

А.Л. Сердечный, А.А. Карданов, А.Т. Труфанов

В статье представлены результаты разработки блока навигации по технологиям средств тестирования на проникновение, выполненной в рамках создания киберполигона. Блок базируется на программной реализации интерактивной информационной карты «Средства тестирования на проникновения». Информационная карта объединяет сведения о более чем 6 тыс. средств тестирования на проникновение, содержащихся в 46 различных источниках (специализированных операционных системах, таких как Kali Linux и BlackArch, научных и аналитических статьях о средствах оценки защищённости информационных систем активными методами, telegram-каналах и других информационных ресурсах). В основе информационной карты лежит граф связей между средствами тестирования на проникновение и их типами. Навигационный блок даёт возможность ознакомиться с широким составом средств, используемых для оценки защищённости информационных систем. Систематизация сведений в виде информационной карты позволяет показать сходство и различия между разными классами средств тестирования на проникновение и их отдельными представителями с учётом существования множества различных вариантов наименований, встречающихся в экспертной и научной среде. Блок навигации построен с использованием web-технологий и доступен в тестовом режиме на портале CyberMaps.ru.

Ключевые слова: киберполигон, информационная карта, информационное картографирование, тестирование на проникновение, pentest.

Введение

Одной из важнейших задач киберполигона, создаваемого на кафедре систем информационной безопасности Воронежского государственного технического университета, является отработка навыков обеспечения защиты от угроз безопасности информации. Для её решения в составе киберполигона помимо типовых объектов защиты должны быть включены средства, с помощью которых обеспечивается моделирование действий нарушителей (которым должно оказываться противодействие со стороны администраторов безопасности). Такие средства широко используются в рамках реализации процедур оценки защищённости информационных систем с помощью активных методов, называемых тестированием на проникновение (от англ. penetration test).

Существует множество источников, в которых представлены сведения о таких средствах. К ним относятся специализированные операционные системы (например, Kali Linux и BlackArch и другие), научные и аналитические статьи о средствах оценки защищённости информационных систем активными методами, telegram-каналы, платформы для совместной разработки (такие как GitHub и GitLab) и другие информационные ресурсы.

Средства тестирования на проникновение обладают различными функциональными возможностями, которые соответствуют определённому способу реализации компьютерных атак. Многообразие способов обеспечивает широкое разнообразие типов таких средств. При этом для обозначения одного и того же типа средств в разных источниках могут использоваться различные названия, что осложняет процедуру выбора необходимого инструментария, для включения его в арсенал киберполигона.

Кроме того, непрерывная борьба «меча и щита» (средств защиты и нападения), а также стремительное технологическое развитие, требует постоянной актуализации перечня используемых средств тестирования на проникновение. В этих условиях актуальной является задача разработки

навигационного блока по технологиям тестирования на проникновение. Результаты её решения представлены в настоящей статье.

Для разработки навигационного блока были проанализированы и обобщены сведения о средствах тестирования на проникновение. Для этого использовался метод информационного картографирования [1], который показал свою эффективность в решении задач экспертного анализа, систематизации и представления больших объёмов данных [2, 3, 4]. Суть метода заключается в построении и анализе информационной карты. Он позволяет исследователю одновременно наблюдать как объект исследования, так и контекст, в котором он находится. Таким образом, достигается представление всего многообразия сведений о предметной области. Кроме того, одной из особенностей данного метода является возможность масштабирования, то есть обеспечение детализации структуры объекта исследования.

Для обеспечения единообразного представления результатов исследований используется информационная карта. Она позволяет группе людей работать вместе, а также быстро получать доступ ко всей необходимой информации через интерактивный анализ, что сохраняет концентрацию внимания, поскольку не требуется взаимодействие с другими средствами.

Во время исследования использовалась система картографирования рисков защищаемого киберпространства, разработанная на кафедре систем информационной безопасности.

Также, согласно технологии построения и анализа информационной карты, были выполнены необходимые шаги для достижения поставленной цели исследования, а именно:

– собраны исходные данные о средствах тестирования на проникновение;

– сформирован ландшафт информационной карты на основе полученной базы данных после сбора исходной информации;

– произведена разметка полученного ландшафта;

– сформированы слои, за счет которых обеспечивается сравнение различных видов средств тестирования на проникновение в контексте моделирования действий нарушителя;

– разработана программная реализация блока навигации по средствам тестирования на проникновение.

Исходные данные о средствах тестирования на проникновение

В качестве источников данных о средствах тестирования на проникновение рассматривались:

- специализированные операционные системы (Kali Linux и BlackArch, Сканер-ВС, Tsurugi и др.);
- информационные ресурсы, агрегирующие сведения о средствах тестирования на проникновение;
- научные и аналитические статьи, содержащие результаты сравнения и рейтинги для средств тестирования на проникновение;
- репозитории GitHub с подборкой средств тестирования на проникновение;
- telegram-каналы, посвящённые инструментальным средствам тестирования на проникновение.

Наиболее полными и актуальными источниками являются дистрибутивы операционных систем тестирования на проникновение Kali Linux и BlackArch. Разница между ними заключается в составе инструментов и платформе, на базе которой такие средства функционируют. Kali Linux основан на ядре Debian, а BlackArch – на ядре Arch Linux. Номенклатура инструментов BlackArch более обширна, но многие из них редко используются. При этом в Kali Linux отобраны лишь самые актуальные и поддерживаемые средства. Кроме того, данная операционная система имеет более удобный интерфейс и группировку средств, а BlackArch. Также следует отметить отечественный аналог – операционную систему тестирования на проникновение Сканер-ВС, которая также

как обладает широкой номенклатурой средств и удобным интерфейсом.

Сбор данных осуществлялся в автоматизированном режиме путём извлечения из текста сведений о средствах тестирования на проникновение и внесения их электронную таблицу, форма которой приведена в табл. 1.

Таблица 1

Сведения о средствах тестирования на проникновение, собираемые в ходе анализа источников

Название поля	Описание поля
Уникальное обозначение	Идентификатор средства, формируемый по названию путём приведения букв к нижнему регистру и исключения пробелов, символов нижнего подчёркивания и дефисов
Название	Самое употребляемое в рассматриваемых источниках наименование средства, которое используется в качестве обозначения соответствующего средства на информационной карте
Тип	Название типа, используемое в рассматриваемом источнике для обозначения группы, к которой относится соответствующее средство
Описание	Описание средства, приведённое на языке оригинала источника
Перевод описания	Автоматический перевод (с помощью сервиса Яндекс.Переводчик) описания средства
Ссылка	Ссылка на анализируемый источник данных, в котором содержатся указанные средства

В каждом анализируемом источнике для описания средств тестирования на проникновение используется собственная форма и обозначения типов средств, поэтому в ходе извлечения сведений также осуществлялось сопоставления различных типов между собой. В качестве возможных взаимосвязей между средствами и их типами, а также между различными обозначениями типов средств тестирования на проникновение использовались следующие отношения:

- eq: отношение эквивалентности (два наименования являются обозначением одного и того же объекта),
- part: отношение «часть-целое» (один объект входит в состав другого),
- rel: отношение близости (два объекта имеют существенное сходство, но нельзя однозначно утверждать об их эквивалентности или вхождении одного объекта в состав другого).

Пример страниц с разметкой собираемых данных показан на рис. 1, где в прямоугольниках обозначены сведения о средствах тестирования на проникновение, собираемые в ходе анализа источников; пунктирным линиями показаны отношения между соответствующими узлами графа связей между средствами и их типами.

Всего проанализировано 46 информационных источников. В результате анализа сформирована таблица с 6262 уникальными наименованиями средств. Её фрагмент приведён в табл. 2.

Данные о средствах тестирования на проникновение внесены в графовую систему управления базами данных Neo4j в соответствии с моделью данных, показанной на рис. 2.

Таблица 2

Фрагмент таблицы, заполняемой в ходе анализа источников, содержащих сведения о средствах тестирования на проникновение

Уникальное обозначение	Название	Тип	Описание	Перевод описания	Ссылка
…	…	…	…	…	…
nmap	Nmap	blackarch-scanner	Utility for network discovery and security auditing.	Утилита для обнаружения сети и аудита безопасности	https://nmap.org/
…	…	…	…	…	…

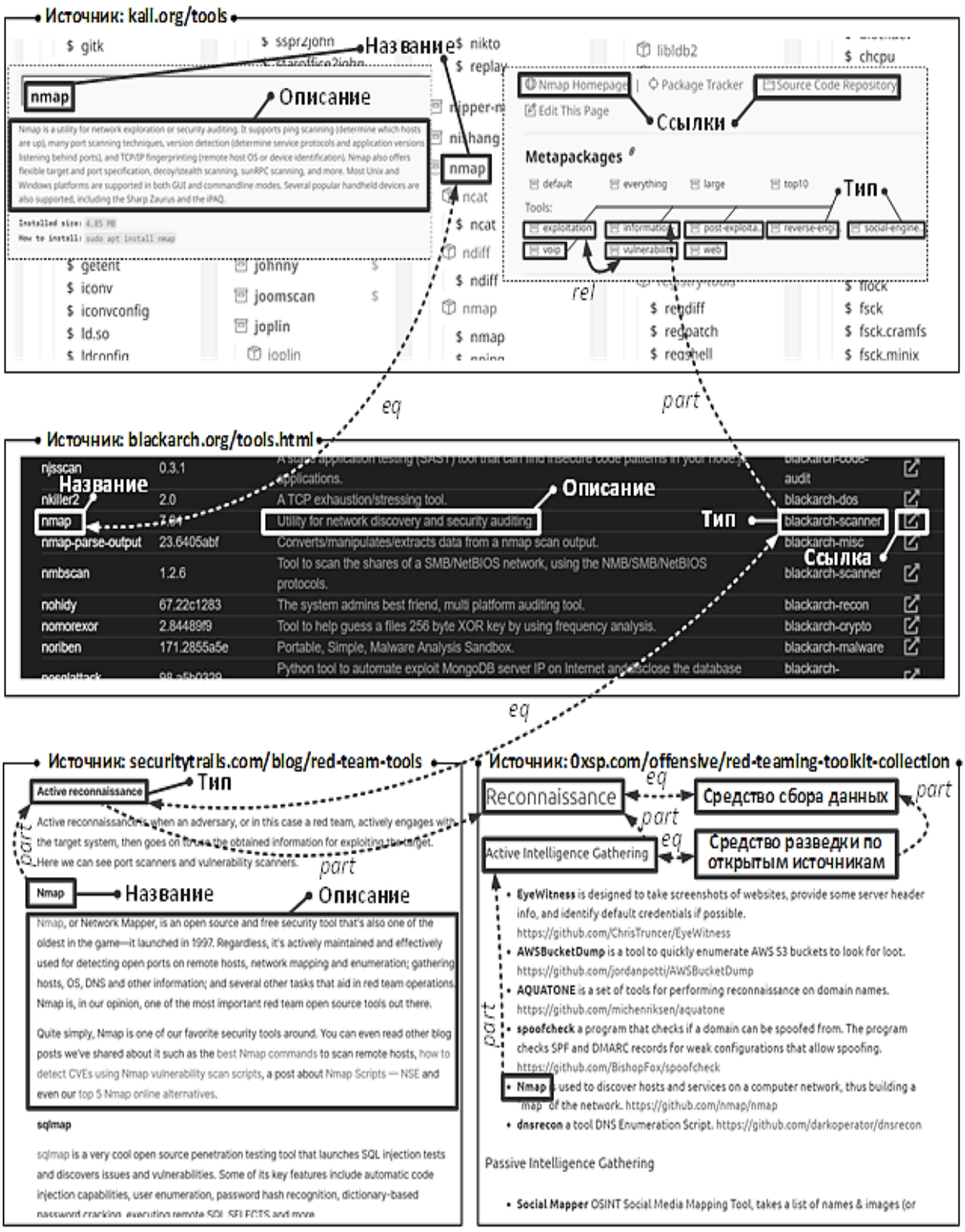

Рис. 1. Демонстрация различия форм описаний средств тестирования на проникновение для различных источников на примере информации о сетевом сканере Nmap

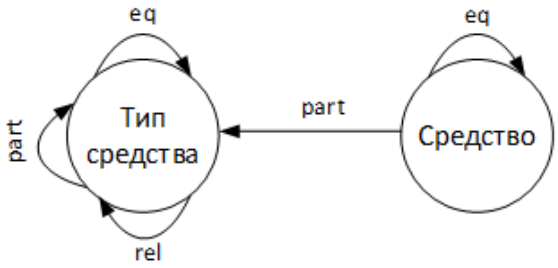

Рис. 2. Модель связей средств тестирования на проникновение и их типов

Узел графа «*Средство*» связывалось с узлом «*Тип средства*» с помощью отношения *part*. Связывание осуществлялось в ручном режиме с помощью модуля Graplytic, входящего в состав системы картографирования рисков. Если два типа средства имели разные названия, то они связывались отношением *eq*. Если один тип являлся подтипом другого, то использовалось отношение *part*. Похожие (но не эквивалентные) типы средств, которые не являлись частью друг друга, связывались отношением *rel*.

Также если в ходе анализа устанавливалось, что два разных называния обозначают одно и то же средство, то соответствующие узлы связывались отношением *eq*

Информационная карта «Средства тестирования на проникновение»

С помощью силового метода ForceAtlas2 был создан граф, описывающий ландшафт информационной карты «Средства тестирования на проникновение». Данная карта представлена в двухмерном пространстве [7].

С целью уменьшения площади пересекающихся областей, в которых представлены различные типы средств тестирования на проникновение, проведён предварительный анализ и изменение графа, в ходе которого выполнялись операции удаления и добавления узлов. Исключались узлы с высоким значением центральности PageRank, которые имели связи с узлами из всех областей ландшафта (рис. 3, а). Операция добавления узлов (рис. 3, б) выполнялась с целью повышения чёткости структуры кластеров, соответствующих наиболее устоявшимся группам средств тестирования на проникновение. Для таких групп вводились узлы-классы, связывающие соответствующие узлы-средства и узлы-типы. Изменённый ландшафт после выполнения операций удаления и добавления узлов графа показан на рис. 3, в.

В результате сформирован ландшафт, на котором прослеживаются три основных класса средств:

- средства тестирования на проникновение,
- программно-аппаратные средства,
- средства сбора и анализа цифровых доказательств.

Четвёртый кластер был вынесен за пределы отображаемой области, так как в него вошли вредоносные программные средства, используемые злоумышленниками при проведении реальных атак. Создание и использование таких средств незаконно и может привести к уголовной ответственности, поэтому возможность включения их в состав киберполигона не рассматривались.

Необходимо отметить, что средства сбора и анализа цифровых доказательств (forensic tools) включены в состав информационной карты «Средства тестирования на проникновение», несмотря на то, что они не отражают заявленную тематику, так как некоторые функциональные возможности данного класса средств могут использоваться при моделировании компьютерных атак. Например, нарушитель, при получении доступа к системе может воспользоваться средствами восстановления удалённой информации или же средствами восстановления пароля из памяти устройства

Разметка ландшафта проводилась в программе QGIS, входящей в систему картографирования рисков защищаемого киберпространства [5] на основание экспертного анализа наиболее влиятельных типов средств тестирования на проникновение (имеющих наибольшее значение PageRank), которые попали в соответствующую область. При этом необходимо отметить, что наносимые на карту границы кластеров используются лишь для обозначения зон наибольшего влияния, где вероятность нахождения объекта

соответствующего типа больше чем в других областях (в области, очерченной границами, могут присутствовать объекты других классов, но вероятность их нахождения существенно ниже по сравнению с вероятностью появления в своей области).

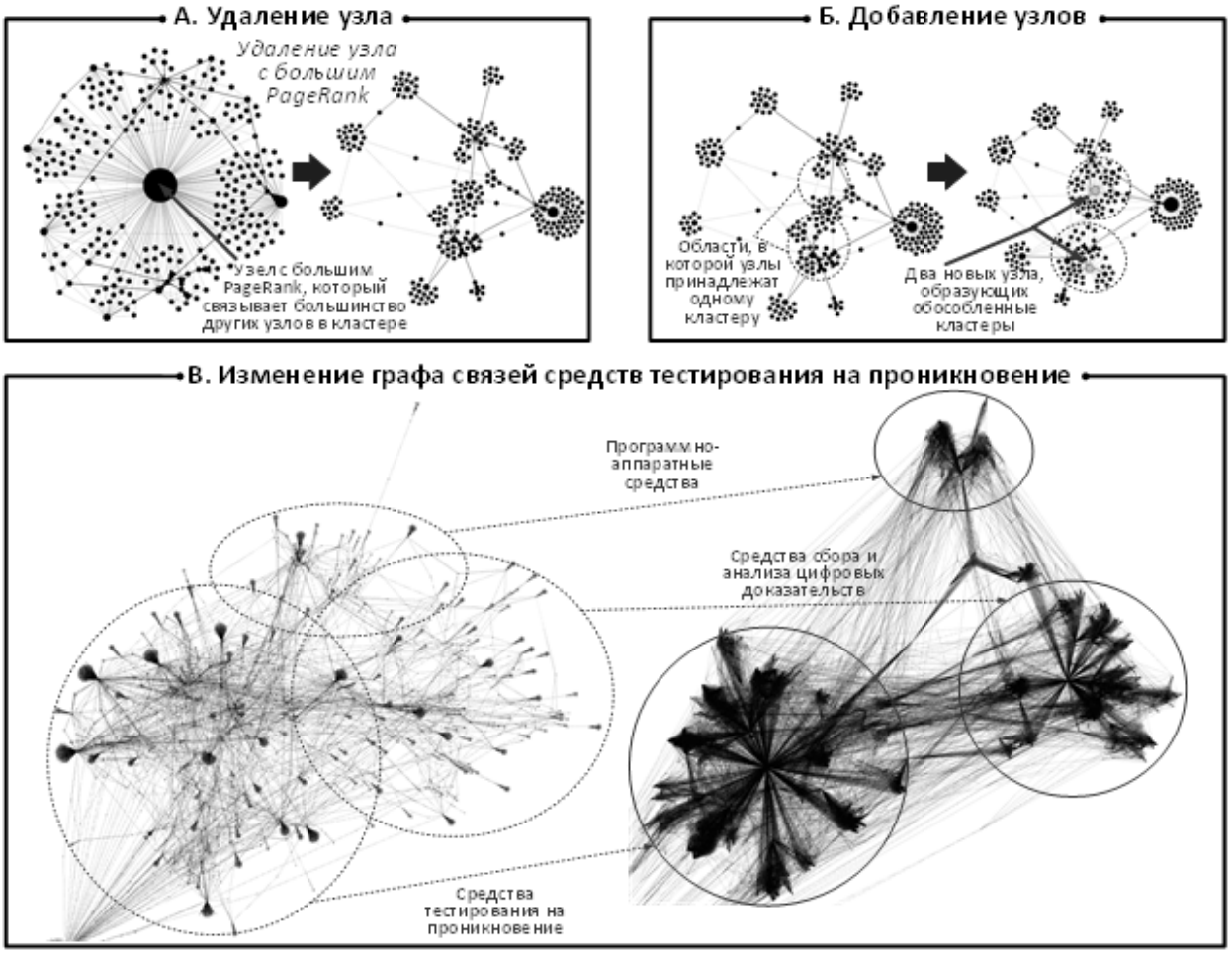

Рис. 3. Изменения ландшафта информационной карты в результате выполнения операций удаления (А) и добавления (Б) узлов графа, лежащего в его основе с целью повышения чёткости кластерной структуры

В результате была сформирована многослойная масштабируемая информационная карта, показанная на рис. 4.

На определённом уровне отображаются только те объекты, которые требуются для решения соответствующей задачи. Так, например, на слое самого мелкого масштаба (1 к 16) отображались лишь наиболее крупные тематические области («Средства тестирования на проникновение», «Средства сбора и анализа цифровых доказательств»). Такой уровень детализации необходим для самого общего представления предметной области, а также для обеспечения узнаваемости контуров ландшафта. Он подходит для задач быстрой навигации по карте с помощью указания на «миникарте» точки, куда должно быть осуществлено перемещение.

Для более углубленного изучения взаимосвязей средствами тестирования на проникновение используются масштабы 1 к 8. На слое масштаба 1 к 4 обозначены конкретные средства.

За счёт генерализации данных и масштабирования преодолевается проблема отображения избыточного числа объектов, приводящего к перегрузке внимания исследователя, а возможность быстрого перемещения между уровнями и участками карты снижает его когнитивную нагрузку.

В табл. 3 приведено формализованное описание построенной информационной карты.

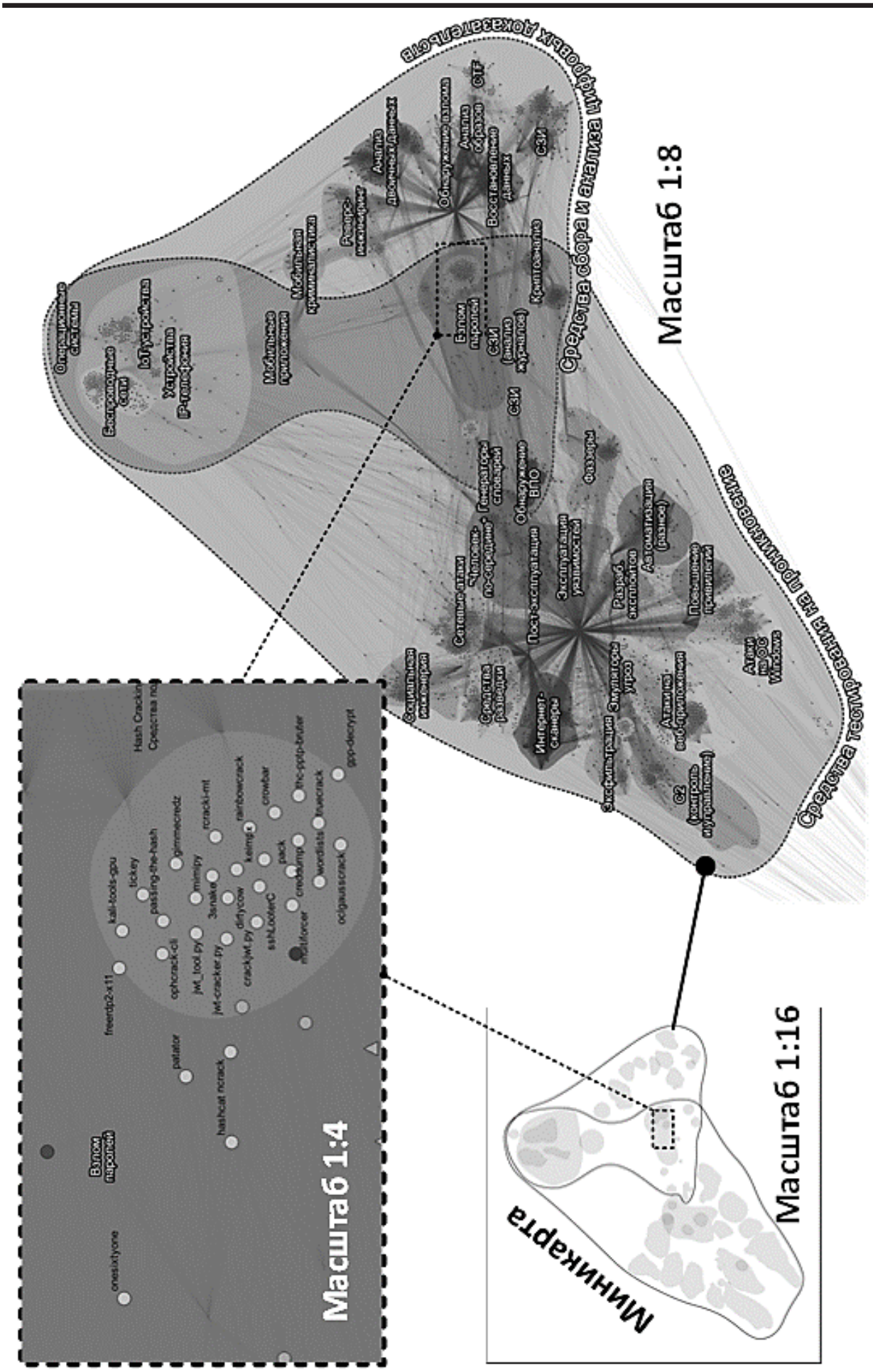

Рис. 4. Информационная карта «Средства тестирования на проникновение»

Таблица 3

Сведения об информационной карте «Средства тестирования на проникновение»

Тип сведений	Характеристика информационной карты
Задачи, решаемые с помощью карты	Систематизация сведений о средствах тестирования на проникновение, сравнительный анализ средств тестирования на проникновение, поиск средства тестирования на проникновение
Исходные данные	Объединение сведений о средствах тестирования на проникновение: - включённых в специализированные операционные системы; - представленных в обзорных статьях; - включённые в персонализированные подборки
Модель данных	*Узлы*: (p) – «Название средства тестирования на проникновение»; (t) – «Тип средства тестирования на проникновение» *Связи*: [part1]: (t)←(p) – «Принадлежность средства к определённому типу»; [part2]: (t)←(t) – «Принадлежность одного типа средств к другом»; [eq1]: (p) ⇄ (p) – «Эквивалентность двух средств»; [eq2]: (t) ⇄ (t) – «Эквивалентность двух типов средств»; [rel]: (t) ⇄ (t) – «Сходство двух типов средств»; *Свойства*: «Уникальный идентификатор»: для объектов (t), (p), [part1], [part2], [eq1], [eq2], [rel]; «Название»: для объектов (t) и (p); «Описание»: для объектов (t) и (p); «Автоматический перевод описания»: для объектов (t) и (p); «Ссылка на источник»: для объекта (p)
Процедура построения карты	В ходе построения карты осуществлены следующие операции: - автоматизированный сбор сведений из 46 источников и внесении их в СУБД Neo4j; - экспертное сопоставление наименований типов средства тестирования на проникновение; - построение графа связей [part1], [part2], [eq1], [eq2], [rel]; - укладка графа в двухмерном пространстве с помощью силового алгоритма ForceAtlas2 (LinLog = true, «Влияние весов рёбер» = 1, «Запрет перекрытия» = true, «Устойчивость» = 1, Theta = 1.2, «Разрежённость» = 10, «Гравитация» = 1); - построение тепловой карты на основании графа связей («Радиус»=0.015, «Распределение пикселей»=0,001); - автоматизированная разметка ландшафта информационной карты; - формирование слоёв в соответствии с задачами исследования
Ландшафт	*Разметка в масштабе 1:4*: отображаются узлы (p) и (t) с надписями и связями [part1], [part2], [eq1], [eq2], [rel]. Разметка позволяет исследовать область с конкретными средствами тестирования на проникновения. *Разметка в масштабе 1:8*: отображается тепловая карта групп средств тестирования на проникновение и узлы (t) с названиями для основных типов средств тестирования на проникновение. Разметка позволяет исследовать взаимосвязи между типами средств тестирования на проникновение *Разметка в масштабе 1:16*: отображается тепловая карта классов средств тестирования на проникновение («Средства тестирования на проникновение» и «Средства сбора и анализа цифровых доказательств») и контуры основных групп таких средств. Разметка может быть использована в качестве миникарты или в качестве фона для отображения отдельных объектов
Слои	Слои объектов исследования включают: - слой с основными средствами тестирования на проникновение; - слои для сравнения различных источников, предоставляющих сведения о средствах тестирования на проникновение («Kali Linux», «BlackArch» и др.).
Форматы карты	.html (карта для выгрузки на сайт), .qgz (карта для программы QGIS), .gephi (графы для программы Gephi), .zip (дамп базы данных Neo4j)

Наиболее крупными тематическими областями являются:

- «Средства тестирования на проникновение»,
- «Средства сбора и анализа цифровых доказательств».

Данные области пересекаются по кластерам «Программно-аппаратные средства (устройства)», «Средства взлома паролей», а также «Средства криптоанализа».

Область средств тестирования на проникновение включает следующие группы:

- средства разведки открытых источников (в том числе Интернет-сканеры, сканеры веб-уязвимостей),
- средства автоматизации социальной инженерии,
- платформы разработки эксплойтов, а также средства эксплуатации уязвимостей и внедрения закладок,
- средства для повышения привилегий и пост-эксплуатации,
- средства для проведения атак (сетевых атак, атак типа «человек посередине», атак на веб-приложения, атак на операционные системы семейства Windows и Linux),
- средства контроля и управления (Command and Control: C2), а также средства эксфильтрации данных (вывода из системы),
- эмуляторы угроз,
- инструменты для обнаружения и сокрытия вредоносного программного обеспечения (ВПО),
- средства выявления уязвимостей (фаззеры, статические анализаторы, средства тестирования интерфейсов веб-приложений и др.),
- прочие средства автоматизации.

Примеры практического использования информационной карты

С целью совместного использования информационной карты «Средства тестирования на проникновение» для решения практических задач отработки навыков защиты информации от угроз безопасности информации в рамках работ по созданию киберполигона был разработан блок навигации по соответствующим средствам. Структура данного блока показана на рис. 5.

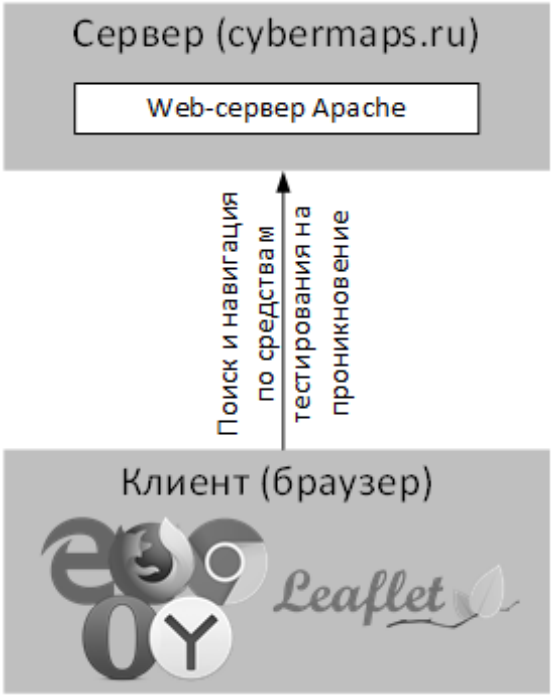

Рис. 5. Структура блока навигации по средствам тестирования на проникновение

Блок построен на базе web-технологий и реализует клиент-серверную архитектуру. Серверная часть размещена на хостинге в сети Интернет с целью предоставления повсеместного доступа к слоям информационной карты из любой точки мира. Слои информационной карты хранятся на сервере в формате *.geojson*. Клиент может загрузить интерактивную карту с помощью обычного браузера. За её отображение отвечает JavaScript-библиотека Leaflet. В ходе интерактивного взаимодействия с картой решается одна из основных задач – получение сведений об актуальном составе арсенала киберполигона.

Другим важным направлением практического применения разработанного модуля является задача поиска средств с заданными характеристиками. Для этой задачи сформированы отдельные слои, на которых отображены различные подборки и результаты сравнения инструментов, проводимые различными исследователями (рис. 6, 7).

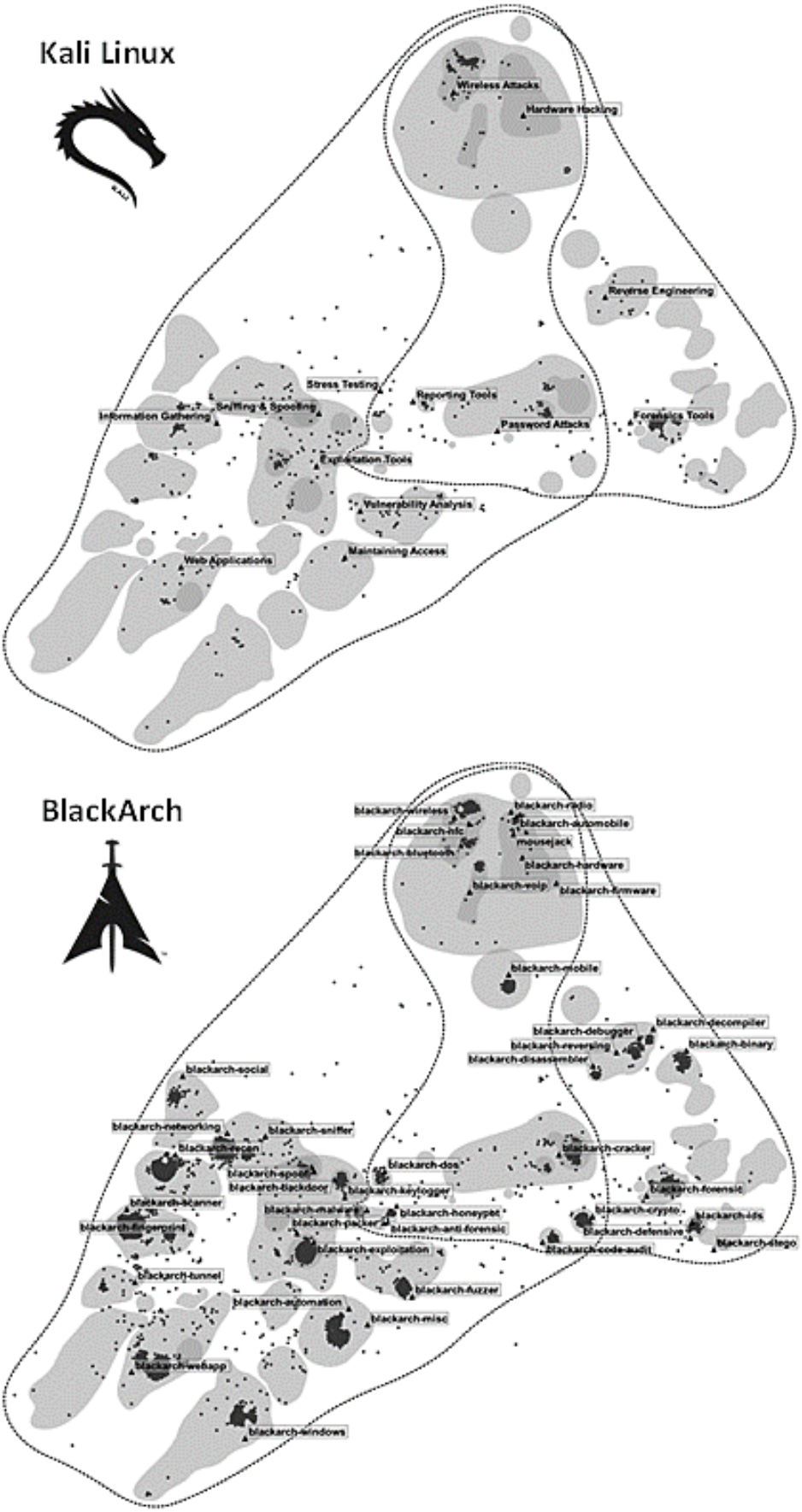

Рис. 6. Слои средств тестирования на проникновение для источников Kali Linux и BlackArch

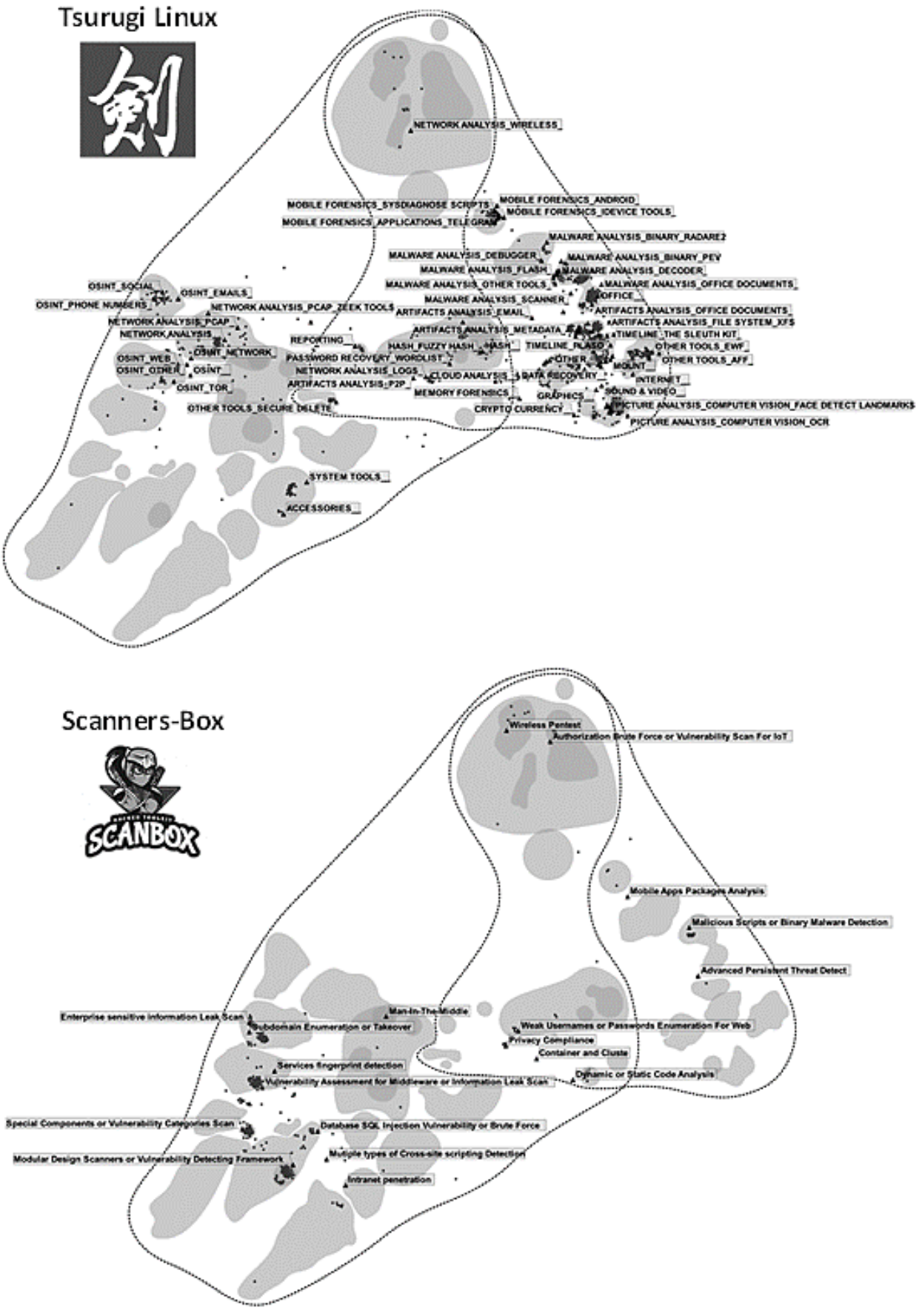

Рис. 7. Слои средств тестирования на проникновение для источников Tsurugi Linux и Scanners-Box

Кроме того, информационная карта упрощает процесс актуализации сформированного набора данных о средствах тестирования на проникновение благодаря принципу близости схожих информационных объектов. Так как близкие по функционалу средства расположены в одной области карты вместе с различными наименованиями соответствующих типов, то в результате поиска по ключевым словам можно достаточно быстро локализовать нужную область, куда следует отнести добавляемое в набор средство. Если же ключевое слово не известно, но указаны инструменты-аналоги, то благодаря графу связей можно автоматизировать задачу определения их типа.

Заключение

В данной статье были представлены результаты построения информационной карты «Средства тестирования на проникновение», на базе которой реализован соответствующий блок навигации, разрабатываемый в рамках работ по созданию киберполигона, выполняемых кафедрой систем информационной безопасности Воронежского государственного технического университета (демонстрация работы данного блока доступна по адресу https://cybermaps.ru/projects/pentest_tools/index.html [8]).

Навигационный блок даёт возможность ознакомиться с широким составом средств, используемых для оценки защищённости информационных систем. Систематизация сведений в виде информационной карты позволяет показать сходство и различия между разными классами средств тестирования на проникновение и их отдельными представителями с учётом существования множества различных вариантов наименований, встречающихся в экспертной и научной среде.

Слои информационной карты используются для повышения удобства, наглядности и скорости выбора средств для проведения соответствующих исследований. Кроме того, благодаря слоям можно визуально оценить полноту и специализацию рассмотренных источников данных. Слой «Арсенал» демонстрирует текущий актуальный состав инструментов, используемых в киберполигоне.

Интерактивная веб-версия информационной карты будет полезна как студентам, обучающимся по специальностям, связанным с защитой информации, так и специалистам, которые проводят оценку защищённости информационных систем с помощью активных методов или участвуют в киберучениях на стороне «красной команды» (атакующей стороне). Наличие на информационной карте средств криминалистического анализа также позволяет использовать её для специалистов, занимающихся расследованием компьютерных преступлений.

Граф связей между средствами, типами и их классами, лежащий в основе информационной карты может рассматриваться в качестве набора данных и быть использован в соответствующих научных исследованиях, посвящённых оценке защищённости информационных систем с применением активных методов.

Дальнейшее развитие блока навигации должно осуществляться за счёт включения новых средств и их типов в рамках актуализации информационной карты средств тестирования на проникновение. Также должно проводиться периодическое уточнение сведений о самих средствах и связях между их типами. В случае существенных изменений (например, в результате появления новых классов средств) ландшафт карты может быть пересмотрен.

Список литературы

1. Картография защищаемого киберпространства : монография / А.Г. Остапенко, А.Л. Сердечный, А.О. Калашников ; под ред. чл.-корр. РАН Д.А. Новикова ; серия «Теория сетевых войн» ; вып. 7. М.: Горячая линия-Телеком, 2022. 372 с.

2. Калашников А.О, Сердечный А.Л., Остапенко А.Г. Картографический подход в библиометрическом исследовании отечественных научных школ, сложившихся

в области защиты информации и обеспечения информационной безопасности. // Информация и безопасность. 2019. Т. 22. Вып. 4. С. 455-484.

3. Сердечный А.Л. Картографическое исследование Blockchain-транзакций и смарт-контрактов киберпреступников, атакующих автоматизированные информационные системы, и оценка ущербов от реализации их атак / А.Л. Сердечный, Д.А. Скогорева, Е.П. Длинный, и др. // Информация и безопасность. 2021. Т. 24. Вып. 4. С. 471-500.

4. Гончаров А.А. Систематизация сведений об ошибках программного обеспечения с использованием информационной карты и оценка их значимости / А.А. Гончаров, М.А. Тарелкин, А.Л. Сердечный // Информация и безопасность. 2021. Т. 25. Вып. 2. С. 295-310.

5. Сердечный А.Л. Информационно-картографические системы как инструментальная основа картографии защищаемого киберпространства / Системы управления и информационные технологии. 2021. № 4 (86). С. 41-46.

6. Сердечный А.Л. К вопросу о создании платформы картографирования рисков защищаемого киберпространства / А.Л. Сердечный, А.А. Гончаров, М.А., Булычев, А.В. Коноплин, О.С. Газизянов, Р.О. Дыкин, Д.С. Нестеров, Д.А. Нархов // Информация и безопасность. 2021. Т. 24. Вып. 4. С. 593-600.

7. Jacomy M. ForceAtlas2, a continuous graph layout algorithm for handy network visualization designed for the Gephi software / M. Jacomy, T. Venturini, S Heymann b и др. // PloS one. 2014. Т. 9. №. 6. С. e98679.

8. Интерактивная информационная карта «Средства тестирования на проникновение» // Информационный ресурс портала CyberMaps, URL: https://cybermaps.ru/projects/pentest_tools/index.html (дата обращения: 12.05.2023).

Государственный научно-исследовательский испытательный институт
проблем технической защиты информации ФСТЭК России
State science research experimental institute of technical information protection
problem of Federal service of technical an export control

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 15.05.2023

Информация об авторах

Сердечный Алексей Леонидович – канд. техн. наук, начальник лаборатории, Государственный научно-исследовательский испытательный институт проблем технической защиты информации ФСТЭК России, e-mail: alex-voronezh@mail.ru

Карданов Ахмед Ануарович – студент, Воронежский государственный технический университет, e-mail: toshka0117@mail.ru

Труфанов Артем Тимурович – студент, Воронежский государственный технический университет, e-mail: trartem2000@mail.ru

CREATING A CYBERPOLYGON: PENETRATION TESTING TOOLS NAVIGATION BLOCK

A.L. Serdechnyi, A.T. Trufanov, A.A. Kardanov

The article presents the results of developing a navigation block for penetration testing technologies as part of creating a cyber polygon. The block is based on software that implements an interactive information card called "Penetration Testing Tools". This information card combines information from over 6,000 penetration testing tools contained in 46 different sources, including specialized operating systems like Kali Linux and BlackArch, scientific and analytical articles on information system security assessment tools, and various other informational resources such as Telegram channels. The information map is designed based on the graph with relationships between the different types of penetration testing tools. The navigation block provides an opportunity to familiarize oneself with a wide range of tools used to assess the security of information systems. The systematization of information in the form of an information map allows readers to understand the similarities and differences between different classes of penetration testing tools and their individual representatives, considering the existence of many different names that are used in expert and scientific environments.

Keywords: cyber polygon, information map, information mapping, penetration testing, pentest.

Submitted 15.05.2023

Information about authors

Alexey L. Serdechnyy – Cand. Sc. (Technical), Chief of Laboratory, State science research experimental institute of technical information protection problem of Federal service of technical an export control, e-mail: alex-voronezh@mail.ru

Kardanov Ahmed Anuarovich – student, Voronezh State Technical University, e-mail: toshka0117@mail.ru

Trufanov Artem Timurovich – student, Voronezh State Technical University, e-mail: trartem2000@mail.ru