1

Карты сетей

Имея на руках карту, генерал может составить план защиты или атаки замка.

Выбирая время и день перемещения лагеря, необходимо соблюдать ряд принципов. Синоби обязан точно знать географию местности и расстояние до врага.

«Ёсимори хяку-сю», № 9

Раздобыв план замка или лагеря, необходимо как можно скорее вернуться, и именно так должен поступить хороший синоби.

«Ёсимори хяку-сю», № 24

Первый совет, который дается в «Руководстве для командиров» («Бансэнсюкай»), призывает создавать очень точные карты, которые военачальники могли бы использовать для планирования атак против врага [5]. «Ёсимори хяку-сю» в стихах № 6–10 и 24 также подчеркивает важность достаточной детализации карт, чтобы они были полезны и солдатам, и синоби.

Создавать карты командиры обычно поручали синоби. Из трактатов явно следует, что умение точно рисовать видимые объекты — горы, реки, поля — это не то же самое, что рисовать специальные подробные карты разведки объекта атаки, пригодные для целей военной стратегии или проникновения синоби. В трактатах говорится, какие детали важны для ведения войны и ремесла синоби и, следовательно, должны фигурировать на карте [5].

- **Все входы и ворота дома, замка или форта.** Какие используются замки́, защелки и механизмы открывания? Насколько сложно открыть ворота или двери, издают ли они шум при открытии или закрытии?

- **Подъездные дороги.** Прямые они или изогнутые? Широкие или узкие? Вымощены ли камнем? Ровные или под уклоном?
- **Внешний вид, схема и планировка здания.** Каковы размер и назначение каждой комнаты? Что хранится в каждой комнате? Скрипят ли в них половицы?
- **Обитатели строения.** Как зовут жителей? Практикуют ли они какие-нибудь примечательные виды искусства, имеют ли какие-либо навыки? Насколько осторожен или подозрителен каждый из жителей?
- **Топология замка и окрестностей.** Будет ли видно сигнал изнутри и снаружи помещения? Где хранятся еда, вода и дрова? Насколько широки и глубоки рвы? Насколько высоки стены?

Понятие о картах сети

Картами сети в кибербезопасности называют графы топологии сети, которые описывают физические и/или логические связи и конфигурацию *связей* (коммуникационные соединения) и *узлов* (устройств) сети. Чтобы лучше понять концепцию, посмотрите на дорожные карты или карты в атласе. Они описывают физическое местоположение, географические особенности, политические границы и природный ландшафт. Информация о дорогах (связях) — их название, ориентация, длина и пересечения с другими дорогами — может использоваться для прокладки маршрута между местами (узлами). Теперь рассмотрим следующий гипотетический сценарий.

Представьте, что вы живете в мире, где дороги и здания внезапно появляются или исчезают в мгновение ока. У вас есть GPS и координаты места, где вы находитесь и куда хотите пойти, но добраться туда можно лишь по запутанной сети постоянно меняющихся дорог.

К счастью, на каждом перекрестке есть специалисты по навигации (*маршрутизаторы*), помогающие путешественникам вроде вас найти путь. Эти маршрутизаторы постоянно обращаются к соседним маршрутизаторам и спрашивают у них, какие маршруты и местоположения открыты, чтобы обновить свою таблицу маршрутизации, хранящуюся в буфере обмена. Вам нужно останавливаться на каждом перекрестке и спрашивать у маршрутизатора, как проехать к следующему узлу, показывая проездной, на котором ваш предполагаемый пункт назначения закодирован в координатах GPS. Маршрутизатор проверяет свой буфер обмена на наличие открытых в данный момент маршрутов, делает определенные вычисления и указывает вам направление, записывая на вашем проездном адрес маршрутизатора, а также пробивает в нем отверстие, чтобы отследить количество маршрутизаторов, на которых вы отметились во время поездки, и отправляет вас

к следующему маршрутизатору. Этот процесс повторяется, пока вы не достигнете точки назначения. А теперь представьте себе лица картографов, которые, вероятно, бросили бы заниматься созданием карт, будучи не в состоянии уследить за постоянно меняющейся сетью. Составителям карт пришлось бы довольствоваться обозначением ключевых ориентиров и достопримечательностей, общими названиями и нечеткими линиями между этими точками, говорящими о том, что между ними существуют какие-то пути.

Эта гипотетическая для нашего мира ситуация на самом деле существует в киберпространстве, и именно поэтому сетевые карты не так точны, а их обслуживание не так приоритетно, каким должно было бы быть. Отсутствие качественной карты сети — это распространенная проблема организаций, занимающихся кибербезопасностью. Если у организации есть карта, она обычно предоставляется операционному центру безопасности (security operations center, SOC), чтобы его специалисты знали, где в потоке данных находятся датчики или устройства безопасности, и могли лучше понять маршрут пакетов, правила брандмауэра, сигналы тревоги и системные журналы. Кроме того, такая карта, скорее всего, довольно абстрактна и описывает только основные функции, такие как границы интернета, периметр сети и интрасети, общее расположение граничных маршрутизаторов или межсетевых экранов, но на ней не указываются сети, концептуальные схемы имеют вид простых кружочков и стрелочек. Пример плохо проработанного, но распространенного вида карты сети, которой пользуются специалисты в области кибербезопасности и ИТ, представлен на рис. 1.1.

Чтобы понять, почему на рис. 1.1 показана «плохая» карта, давайте еще раз рассмотрим приведенный в «Бансэнсюкай» совет по составлению карт, но применим кибераналогию.

- **Все точки доступа узла в сети.** Какие виды интерфейсов доступа присутствуют на устройстве (Ethernet [e], Fast-Ethernet [fe], Gigabit-Ethernet [ge], Universal Serial Bus [USB], Console [con], Loop-back [lo], Wi-Fi [w] и т. д.)? Есть ли фильтрация адресов управления доступом к сети (NAC) или управления доступом к среде (MAC)? Включен или заблокирован доступ к удаленной или локальной консоли? Какой вид физической безопасности реализован? Закрыто ли помещение с серверной стойкой на замóк или есть ли хотя бы USB-замки́? Ведется ли журнал доступа к интерфейсу? Где находится интерфейс управления сетью и сама сеть? Каков IP-адрес и MAC-адрес каждой точки доступа?
- **Граничные шлюзы, переходы и точки выхода.** Сколько интернет-провайдеров (internet service provider, ISP) у сервера — один или больше? Используется надежное подключение к интернету (Trusted Internet Connection, TIC) или управляемая служба интернета (Managed Internet Service, MIS)? Какова пропускная способность интернет-соединения? Применяется оптоволокно,

Ethernet, коаксиальный кабель или другой канал? Какие переходы ведут к сети? Существуют ли способы входа в сеть или выхода из нее через спутник, микроволновую печь, лазер или вайфай?

- **Структура и схема сети.** Каковы имя, назначение и размер каждой подсети, например используется ли бесклассовая междоменная маршрутизация (Classless Inter-Domain routing, CIDR)? Задействуются ли виртуальные локальные сети (virtual local area networks, VLAN)? Заданы ли лимиты пула подключений? Является ли сеть плоской, иерархической или разделена на структуры, защитные слои и/или функции?

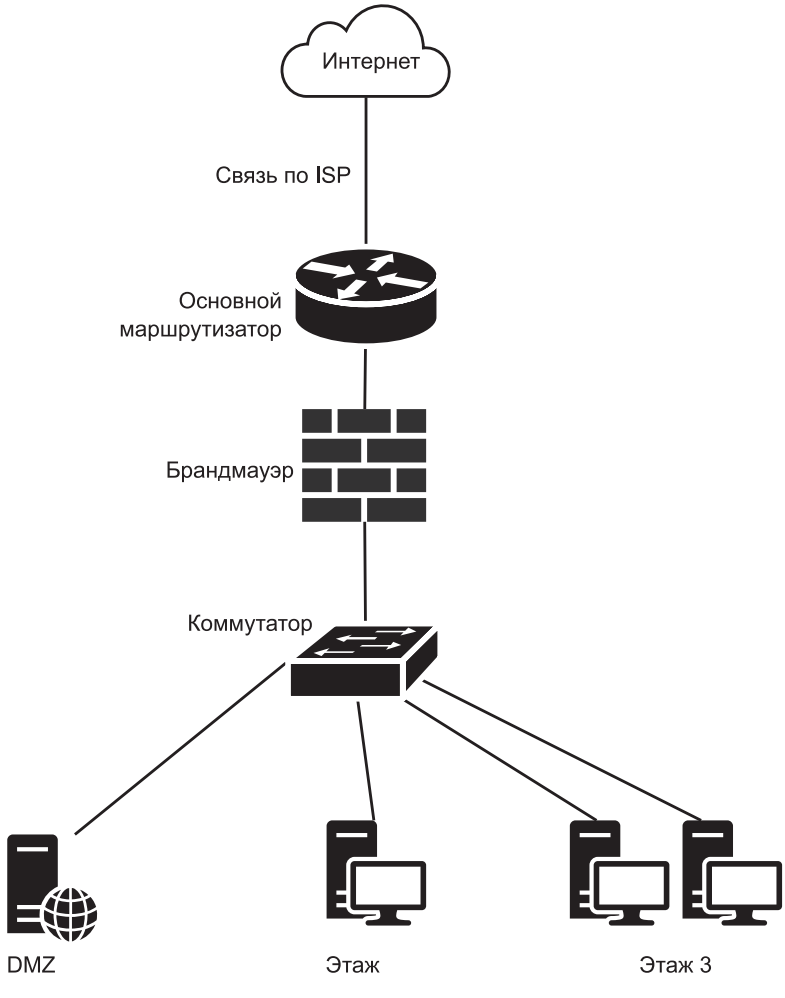

Рис. 1.1. Упрощенная карта сети

- **Хосты и узлы сети.** Как они называются? Какая у них версия операционной системы (ОС)? Какие службы/порты используются, какие из них открыты? Какие на них запущены средства безопасности, которые позволят обнаружить атаку? Есть ли у них общеизвестные уязвимости (common vulnerability exploit, CVE)?
- **Физическая и логическая архитектура сети и здания. Где находится датацентр?** Есть ли в холле разъемы Ethernet? Можно ли поймать вайфай за пределами здания? Видны ли экраны компьютеров и терминалы снаружи здания? Используется ли в офисе безопасное стекло? Правильно ли сегментированы сети гостевых или конференц-залов? Каковы основные списки управления доступом (access control list, ACL) и правила брандмауэра в этой сети? Где разрешается DNS? Что доступно в периметре сети или DMZ (demilitarized zone)? Существуют ли внешние поставщики электронной почты или другие облачные сервисы? Как устроена архитектура удаленного доступа или виртуальной частной сети (VPN)?

Организации, не имеющие действующей карты сети, иногда используют электрические схемы или схемы, составленные их ИТ-отделом. На таких упрощенных рисунках отражено относительное расположение систем, сетевого оборудования и подключения устройств, и они могут служить справочными материалами для устранения технических или эксплуатационных проблем в сети. Но у множества организаций нет даже таких приблизительных схем, зато есть электронные таблицы, в которых перечислены имена хостов, их модели и серийные номера, IP-адреса, а также расположение всего оборудования на стойке в центре обработки данных. При этом если заинтересованные стороны могут использовать такую таблицу для поиска нужных ответов и серьезных сетевых проблем или сбоев не возникает, то даже само наличие такой документации может препятствовать созданию карты сети. Это ужасно, но у некоторых компаний есть архитектор или специалист, который держит карту сети в голове, и ни в каком другом виде ее не существует.

Справедливости ради стоит сказать, что бывают и разумные причины отсутствия полезных сетевых карт. Создание, совместное использование и обслуживание карт отнимает драгоценное время и другие ресурсы. Карты могут часто меняться. Добавление систем в сеть или их удаление, изменение IP-адресов, переделка кабелей или задание новых правил маршрутизатора или брандмауэра — все это может значительно повлиять на точность карты, даже если изменение произошло всего несколько минут назад. Кроме того, современные компьютеры и сетевые устройства используют протоколы динамической маршрутизации и конфигурации хоста, которые автоматически отправляют информацию в другие системы

и сети, не нуждаясь в картах вообще, что означает: сети могут автоматически настраиваться сами.

Разумеется, существует множество программных инструментов для создания карт, например программа Nmap [24], которая сканирует сеть, определяя в ней хосты, визуализирует сеть по количеству переходов от сканера, использует простой протокол управления сетью (Simple Network Management Protocol, SNMP) для обнаружения и отображения топологии сети или задействует файлы конфигурации маршрутизатора и коммутатора для быстрого создания сетевых диаграмм. Сетевые диаграммы, генерируемые программами, удобны, но они редко отражают все подробности и в целом контекст, необходимый для создания по-настоящему качественной карты, которую хотел бы иметь под рукой защитник. Идеальным решением было бы одновременное использование программ для картографии, сетевого сканирования и человеческого опыта, но даже этот подход требует значительных затрат времени сотрудника со специальными навыками, иначе полученные карты не будут достаточно точными или полезными.

Несмотря на эти ограничивающие факторы, чрезвычайно важно, чтобы защитник сети при составлении карты был очень внимателен. Примерная карта, показанная на рис. 1.2, иллюстрирует детали, которые должны быть указаны на составляемой защитником карте сети.

Для представления устройств в сети используют геометрические фигуры, а не пиктограммы. Для схожих типов устройств применяют схожие фигуры. Например, круги на рис. 1.2 обозначают рабочие станции, квадраты — маршрутизаторы, а прямоугольники — серверы. В продолжение этой мысли, треугольники, если бы они были, представляли бы ретрансляторы электронной почты или контроллеры домена. Кроме того, на фигурах отсутствует текстура или фон, потому что информация, размещенная внутри, должна быть хорошо читаемой.

Каждый интерфейс, как виртуальный, так и физический, имеет свой тип и номер. Например, может быть указан тип интерфейса Ethernet, а номер интерфейса будет таким же, как и физически указанный на устройстве, eth 0/0. Также помечаются неиспользуемые интерфейсы. Каждому интерфейсу приписывается назначенный ему IP-адрес и подсеть, если они известны.

Открытая информация об устройстве: имя хоста, марка, модель устройства и версия ОС — указывается в верхней части устройства. Уязвимости, учетные данные по умолчанию, известные учетные данные и другие важные слабости обозначаются в центре устройства. Аналогичным образом документируются запущенные службы, программное обеспечение и открытые порты. На карте также указываются сети VLAN, сетевые границы, макет и структура сети. Рядом с ними записывается любая заслуживающая внимания информация.

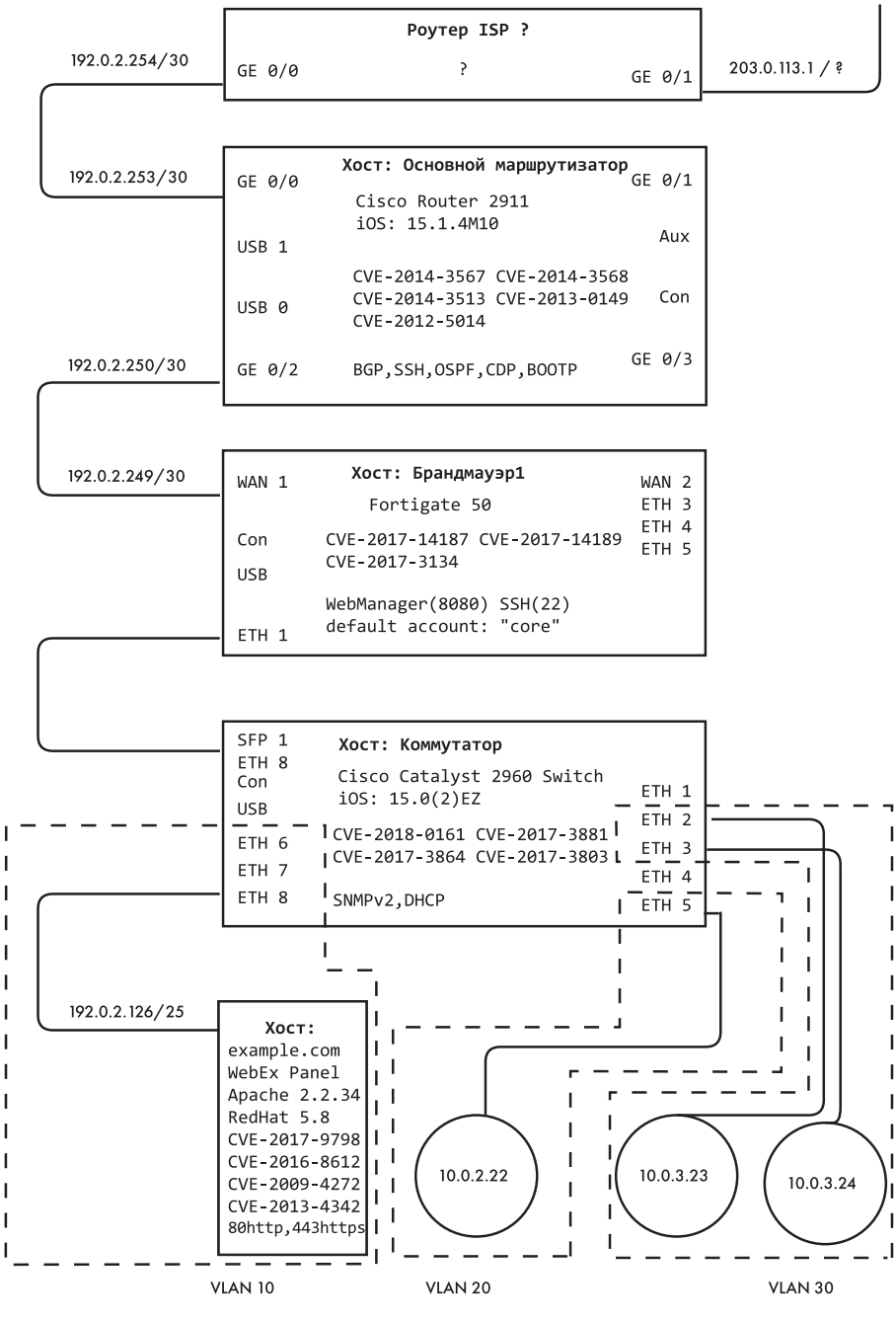

Рис. 1.2. Подробная карта сети

Тайный сбор информации

Высшим пилотажем у синоби считалось умение собрать разведданные, не обнаружив себя. Если он будет прогуливаться возле за́мка и замерять длинной линейкой его размеры, то жители наверняка заподозрят, что тут работает вражеский шпион. Следовательно, старательные синоби составляли карты в мирное время, когда обитатели замка были менее бдительны и можно было более свободно ходить там, где нужно, вызывая во время сбора данных меньше подозрений [5].

Часто синоби приходилось придумывать способы выполнять измерения, отмечать топографические особенности и собирать другую информацию втайне от посторонних глаз. Что характерно, в разделе о методах открытой маскировки трактата «Бансэнсюкай» приведено описание того, как точно создавать карты, и там говорится, что синоби умели создавать карты прямо на глазах у врага. В трактате описывается техника под названием *урамитцу но дзюцу* [5], предназначенная для определения расстояния до знакомого объекта, если известны размеры объекта для масштабирования. *Урамитцу но дзюцу* также рассматривает хитрые приемы из тригонометрии. Например, синоби может лечь ступнями к цели и использовать их известные размеры для измерения расстояния, при этом со стороны кажется, что человек просто дремлет под деревом.

Сбор информации о сетевых узлах — одно из первых действий, которое выполняет злоумышленник перед совершением атаки на сеть или хост. Карты, созданные противником, предназначены для того же, что и карты ниндзя, — идентификации и документирования информации, необходимой для проникновения на объект. К этой информации могут относиться все точки входа в сеть и выхода из нее: подключения к интернет-провайдеру, точки беспроводного доступа, УВЧ, микроволновые, радио- или спутниковые точки, облачные, взаимосвязанные и внешние сети.

Злоумышленники также находят шлюзы протокола пограничного шлюза (BGP) и маршруты или переходы к сети. Определяют репрезентативную структуру, расположение и дизайн сети, оборудование в ней, включая имена хостов, модели устройств, операционные системы, открытые порты, запущенные службы и уязвимости, а также топологию сети, включая подсети, VLAN, ACL и правила брандмауэра.

Многие из инструментов, предназначенные для отображения сети и используемые злоумышленниками, являются «шумными», поскольку они обмениваются данными с большим количеством хостов, применяют специально собранные пакеты и могут быть обнаружены внутренними устройствами безопасности. Но злоумышленники могут обойти этот недостаток за счет замедления или настройки картографа, использования нестандартных (неподозрительных) пакетов и даже ручной разведки с помощью стандартных инструментов, работающих на хосте жертвы, таких как

команды `ping` или `net`. В атаках также могут задействоваться безобидные методы разведки, когда злоумышленник не трогает и не сканирует цель, а лишь собирает информацию с помощью сервиса Shodan или других ранее проиндексированных данных, хранящихся в поисковых системах в интернете.

Более хитроумные злоумышленники пользуются тактикой *пассивного отображения сети*, когда злоумышленник собирает информацию о цели, не взаимодействуя с ней напрямую (без активного сканирования с помощью инструментов вроде Nmap). Еще одна тактика пассивного отображения сети — это интерпретация пакетов, перехваченных с сетевого интерфейса в *беспорядочном режиме*, то есть настройка сетевого интерфейса на запись и проверку всех сетевых коммуникаций. Этот режим противоположен *упорядоченному режиму*, при котором записывается и проверяется только связь внутри сети. Беспорядочный режим позволяет получить представление об используемых сетью соседних хостах, потоках трафика, службах и протоколах, не взаимодействуя с ними активно.

Методами отображения сети без прямого взаимодействия с ней являются также перехват электронных писем администратора сети на выходе из нее, поиск сетевых карт цели во внешнем хранилище файлов или поиск на форумах, где администратор просит помощи в устранении неполадок, для чего может публиковать журналы или ошибки, конфигурации маршрутизатора, информацию о сетевой отладке или другие технические подробности, позволяющие понять структуру и конфигурацию сети. Как и в *урамитцу но дзюцу*, использование наблюдаемой информации из сети цели позволяет составить карту, не обращаясь к сети. Пассивное отображение может включать в себя измерение задержки трассировщиков для определения спутниковых переходов (например, наличие спутника обычно сопровождается внезапным увеличением задержки связи на 500 мс) или обнаружения глубокой обработки пакетов системой брандмауэра (например, препроцессор распознает потенциальную злонамеренную атаку и добавляет ощутимые задержки связи). Пассивное отображение может включать также раскрытие информации внутренней сети из внешних зон DNS и записей ответов. Это могут быть заказы на государственные закупки и запросы на закупку определенного программного либо аппаратного обеспечения, объявления о вакансиях сетевых или системных администраторов с опытом работы в конкретной технологии, сетевом оборудовании или аппаратном/программном обеспечении.

Если злоумышленник тратит так много времени на разработку карт, они в конечном итоге могут оказаться более полными, чем собственные карты цели, и тогда противник будет знать о сети цели больше, чем сама цель. Чтобы не отставать в этой битве, защитники сети должны разрабатывать и поддерживать лучшие карты и обеспечивать высокую степень защиты.