МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ   
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ   
**«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»   
(МОСКОВСКИЙ ПОЛИТЕХ)**

Отчет по практике № 1

Выполнил:

студент учебной группы 241-351, Чуфаров С.Б.

Москва, 2025

**Основные аспекты матрицы Mitre Att&ck**

**1. Reconnaissance (Разведка):**

Разведка — это начальная фаза кибератаки, в которой злоумышленники собирают информацию о цели для планирования своих действий. Эта информация может включать данные о системах, пользователях и сетевой инфраструктуре.

**Методы:**

1. Active Scanning (Активное сканирование):

- Использование инструментов для активного поиска уязвимостей в системах жертвы. Это может включать сканирование портов, обнаружение открытых сервисов и выявление уязвимых приложений.

2. Gather Victim Host Information (Сбор информации о хостах жертвы):

- Сбор данных о конкретных устройствах и серверах, используемых жертвой, включая операционные системы, версии программного обеспечения и конфигурации.

3. Gather Victim Identity Information (Сбор информации об идентификации жертвы):

- Получение данных о пользователях, таких как имена, адреса электронной почты и другие идентифицирующие сведения.

4. Gather Victim Network Information (Сбор сетевой информации о жертве):

- Изучение сетевой инфраструктуры жертвы, включая IP-адреса, маршрутизаторы и другие сетевые устройства.

5. Gather Victim Org Information (Сбор организационной информации о жертве):

- Сбор данных об организации жертвы, таких как структура компании, ключевые сотрудники и бизнес-процессы.

6. Phishing for Information (Фишинг для получения информации):

- Использование фишинговых атак для получения конфиденциальной информации от сотрудников или других лиц, связанных с целью.

7. Search Closed Sources (Поиск закрытых источников):

- Поиск информации в закрытых или защищенных источниках, таких как платные базы данных или внутренние документы.

8. Search Open Technical Databases (Поиск открытых технических баз данных):

- Использование открытых технических баз данных для поиска уязвимостей или другой информации о целевых системах.

9. Search Open Websites/Domains (Поиск открытых веб-сайтов/доменов):

- Исследование публично доступных веб-сайтов и доменов для сбора информации о компании или организации.

10. Search Victim-Owned Websites (Поиск на веб-сайтах, принадлежащих жертве):

- Анализ веб-сайтов самой жертвы для извлечения полезной информации, такой как контактные данные, описания услуг и другие публичные данные.

**2. Resource Development (Разработка ресурсов):**

Разработка ресурсов — это этап, на котором злоумышленники создают или получают необходимые инструменты, инфраструктуру и доступ для осуществления своих атак. Это может включать в себя как технические, так и человеческие ресурсы.

**Методы:**

1. Acquire Access (Получение доступа):

- Процесс получения доступа к системам или учетным записям, которые могут быть использованы для дальнейших действий. Это может включать в себя использование украденных учетных данных или уязвимостей.

2. Acquire Infrastructure (Приобретение инфраструктуры):

- Создание или получение необходимой инфраструктуры для проведения атак, такой как серверы, домены или другие ресурсы.

3. Compromise Accounts (Компрометация учетных записей):

- Получение несанкционированного доступа к учетным записям пользователей или администраторов с целью использования их прав для выполнения атак.

4. Compromise Infrastructure (Компрометация инфраструктуры):

- Взлом сетевой инфраструктуры жертвы, включая маршрутизаторы, серверы и другие устройства, чтобы получить контроль над ними.

5. Develop Capabilities (Разработка возможностей):

- Создание или модификация инструментов и методов для выполнения атак. Это может включать разработку вредоносного ПО или других средств для достижения целей.

6. Establish Accounts (Создание учетных записей):

- Создание новых учетных записей в системах жертвы с целью получения доступа к ресурсам и информации.

7. Obtain Capabilities (Получение возможностей):

- Приобретение необходимых инструментов и технологий для выполнения атак, таких как программное обеспечение для взлома или средства для обхода защиты.

8. Stage Capabilities (Подготовка возможностей):

- Подготовка всех необходимых ресурсов и инструментов перед проведением атаки. Это может включать настройку серверов, загрузку вредоносного ПО и другие действия по подготовке.

**3. Initial Access (Первоначальный доступ):**

Первоначальный доступ — это этап, на котором злоумышленники получают первый доступ к системе или сети жертвы. Это может быть достигнуто различными способами, включая эксплуатацию уязвимостей или использование социальной инженерии.

**Методы:**

1. Content Injection (Инъекция контента):

- Внедрение вредоносного кода или контента в веб-приложения или сайты, что может привести к компрометации пользователей, посещающих эти ресурсы.

2. Drive-by Compromise (Компрометация при посещении сайта):

- Автоматическая установка вредоносного ПО на устройство пользователя при посещении скомпрометированного веб-сайта без ведома пользователя.

3. Exploit Public-Facing Application (Эксплуатация публично доступных приложений):

- Использование уязвимостей в приложениях, которые доступны через интернет, для получения доступа к системам жертвы.

4. External Remote Services (Внешние удаленные сервисы):

- Использование внешних сервисов для доступа к системам жертвы, таких как VPN или удаленные рабочие столы, которые могут быть неправильно настроены или уязвимы.

5. Hardware Additions (Добавление аппаратных средств):

- Физическое добавление вредоносных устройств в инфраструктуру жертвы, таких как USB-накопители с вредоносным ПО.

6. Phishing (Фишинг)\*\*:

- Использование фишинговых атак для обмана пользователей с целью получения их учетных данных или установки вредоносного ПО на их устройства. Это может включать отправку поддельных электронных писем или создание фальшивых веб-сайтов.

7. Replication Through Removable Media (Репликация через съемные носители):

- Распространение вредоносного ПО через съемные носители, такие как USB-накопители, которые могут быть подключены к компьютерам жертвы.

8. Supply Chain Compromise (Компрометация цепочки поставок):

- Внедрение вредоносного ПО в программное обеспечение или оборудование на этапе поставки, что позволяет злоумышленникам получить доступ к системам жертвы через доверенные источники.

9. Trusted Relationship (Доверительные отношения):

- Использование существующих доверительных отношений между организациями для получения доступа к системам жертвы.

10. Valid Accounts (Действительные учетные записи):

- Использование украденных или скомпрометированных учетных записей для получения доступа к системам и ресурсам жертвы.

**4. Execution (Исполнение):**

Этап исполнения включает в себя выполнение вредоносного кода на целевой системе. Злоумышленники используют различные методы для запуска своих скриптов, программ или команд, чтобы достичь своих целей.

**Методы:**

1. Cloud Administration Command (Команда администрирования облака):

- Выполнение команд для управления облачными ресурсами, что может включать в себя запуск вредоносного кода в облачной среде.

2. Command and Scripting Interpreter (Интерпретатор команд и сценариев):

- Использование интерпретаторов командной строки или сценариев (например, PowerShell, Bash) для выполнения команд и скриптов на целевой системе.

3. Container Administration Command (Команда администрирования контейнеров):

- Выполнение команд для управления контейнерами, что может быть использовано для запуска вредоносных приложений внутри контейнеров.

4. Deploy Container (Развертывание контейнера):

- Развертывание контейнеров с вредоносным ПО в средах, поддерживающих контейнеризацию, таких как Docker или Kubernetes.

5. Exploitation for Client Execution (Эксплуатация для выполнения на клиенте):

- Использование уязвимостей в клиентских приложениях для выполнения вредоносного кода на устройствах пользователей.

6. Inter-Process Communication (Межпроцессное взаимодействие):

- Использование механизмов межпроцессного взаимодействия для передачи данных между процессами и выполнения кода.

7. Native API (Нативный API):

- Вызов нативных API операционной системы для выполнения операций и запуска кода.

8. Scheduled Task/Job (Запланированная задача/работа):

- Создание или использование запланированных задач для автоматического выполнения вредоносного кода в определенное время или при определенных условиях.

9. Serverless Execution (Безсерверное исполнение):

- Запуск кода в безсерверных вычислительных средах, таких как AWS Lambda или Azure Functions, что позволяет выполнять код без необходимости управлять серверами.

10. Shared Modules (Общие модули):

- Использование общих библиотек или модулей для выполнения кода, что может помочь скрыть его от обнаружения.

11. Software Deployment Tools (Инструменты развертывания программного обеспечения):

- Использование инструментов развертывания ПО для установки и запуска вредоносных приложений на целевых системах.

12. System Services (Системные службы):

- Запуск вредоносного кода через системные службы операционной системы, что может обеспечить постоянный доступ и скрытность.

13. User Execution (Исполнение пользователем):

- Заставление пользователя выполнять вредоносный код самостоятельно, например, через фишинговые ссылки или вложения в электронных письмах.

14. Windows Management Instrumentation (WMI):

- Использование WMI для выполнения команд и скриптов на удаленных системах Windows, что позволяет злоумышленникам управлять системами издалека.

**5. Persistence (Устойчивость):**

Этап устойчивости включает в себя методы, которые злоумышленники используют для обеспечения постоянного доступа к системе даже после перезагрузки или попыток удаления вредоносного ПО. Это позволяет им оставаться незамеченными и продолжать свои действия.

**Методы:**

1. Account Manipulation (Манипуляция учетными записями):

- Изменение существующих учетных записей или создание новых для обеспечения доступа к системе. Это может включать в себя изменение прав доступа или создание учетных записей с повышенными привилегиями.

2. BITS Jobs (Работы BITS):

- Использование Background Intelligent Transfer Service (BITS) для загрузки и выполнения вредоносного кода на целевой системе.

3. Boot or Logon Autostart Execution (Автозапуск при загрузке или входе в систему):

- Настройка системы на автоматический запуск вредоносного кода при загрузке или входе пользователя в систему.

4. Boot or Logon Initialization Scripts (Скрипты инициализации загрузки или входа):

- Использование скриптов, которые выполняются при загрузке системы или входе пользователя, для запуска вредоносного ПО.

5. Browser Extensions (Расширения браузера):

- Установка вредоносных расширений в браузеры, что позволяет злоумышленникам выполнять код и собирать данные пользователей.

6. Compromise Host Software Binary (Компрометация бинарных файлов программного обеспечения хоста):

- Модификация существующих исполняемых файлов на целевой системе для внедрения вредоносного кода.

7. Create Account (Создание учетной записи):

- Создание новых учетных записей с целью получения постоянного доступа к системе.

8. Create or Modify System Process (Создание или модификация системного процесса):

- Создание новых процессов или изменение существующих для запуска вредоносного кода.

9. Event Triggered Execution (Исполнение по событию):

- Настройка системы на выполнение вредоносного кода при возникновении определенных событий, таких как изменения в системе или действия пользователей.

10. External Remote Services (Внешние удаленные сервисы):

- Использование внешних сервисов для поддержания доступа к системе, например, через VPN или удаленные рабочие столы.

11. Hijack Execution Flow (Перехват потока исполнения):

- Изменение нормального потока выполнения программ для запуска вредоносного кода вместо ожидаемого поведения.

12. Implant Internal Image (Имплантация внутреннего образа):

- Внедрение вредоносных образов в систему для обеспечения их выполнения при старте системы.

13. Modify Authentication Process (Модификация процесса аутентификации):

- Изменение процесса аутентификации для обхода стандартных методов проверки подлинности пользователей.

14. Office Application Startup (Запуск приложений Office):

- Использование приложений Microsoft Office для автоматического выполнения вредоносного кода при их запуске.

15. Power Settings (Настройки питания):

- Изменение настроек питания системы для обеспечения ее постоянной доступности и выполнения вредоносного ПО.

16. Pre-OS Boot (Предварительная загрузка ОС):

- Внедрение вредоносного ПО на уровне загрузчика операционной системы, что позволяет ему исполняться до загрузки самой ОС.

17. Scheduled Task/Job (Запланированная задача/работа):

- Создание запланированных задач для автоматического выполнения вредоносного кода в определенное время или при определенных условиях.

18. Server Software Component (Компонент серверного программного обеспечения):

- Использование серверных компонентов для внедрения и выполнения вредоносного ПО на сервере.

19. Traffic Signaling (Сигнализация трафика):

- Использование сетевого трафика как сигнала для активации определенных действий или запуска вредоносного кода.

20. Valid Accounts (Действительные учетные записи):

- Использование действительных учетных записей для получения постоянного доступа к системам и ресурсам жертвы.

**6. Privilege Escalation (Эскалация привилегий):**

Эскалация привилегий — это процесс, при котором злоумышленник получает более высокий уровень доступа к системе, чем тот, который был изначально предоставлен. Это может позволить им выполнять действия, которые обычно недоступны для обычных пользователей, такие как установка программного обеспечения, изменение системных настроек или доступ к конфиденциальной информации.

**Методы:**

1. Abuse Elevation Control Mechanism (Злоупотребление механизмом контроля повышения привилегий):

- Использование уязвимостей в механизмах контроля доступа для получения повышенных привилегий.

2. Access Token Manipulation (Манипуляция токенами доступа):

- Изменение или подделка токенов доступа для получения прав, которые не были изначально предоставлены пользователю.

3. Account Manipulation (Манипуляция учетными записями):

- Изменение прав существующих учетных записей или создание новых с повышенными привилегиями.

4. Boot or Logon Autostart Execution (Автозапуск при загрузке или входе в систему):

- Настройка системы на автоматический запуск вредоносного кода с повышенными привилегиями при загрузке или входе пользователя.

5. Boot or Logon Initialization Scripts (Скрипты инициализации загрузки или входа):

- Использование скриптов, которые выполняются при загрузке системы или входе пользователя, для повышения привилегий.

6. Create or Modify System Process (Создание или модификация системного процесса):

- Создание новых процессов или изменение существующих для выполнения кода с повышенными привилегиями.

7. Domain or Tenant Policy Modification (Модификация политик домена или арендатора):

- Изменение политик безопасности в домене или арендаторе для получения дополнительных прав доступа.

8. Escape to Host:

- Выход за пределы контейнеров или виртуальных машин для получения доступа к хост-системе с более высокими привилегиями.

9. Event Triggered Execution (Исполнение по событию):

- Настройка системы на выполнение вредоносного кода с повышенными привилегиями при возникновении определенных событий.

10. Exploitation for Privilege Escalation (Эксплуатация уязвимостей для эскалации привилегий):

- Использование известных уязвимостей в программном обеспечении для получения более высоких прав доступа.

11. Hijack Execution Flow (Перехват потока исполнения):

- Изменение нормального потока выполнения программ для запуска вредоносного кода с повышенными привилегиями.

12. Process Injection (Инъекция процессов):

- Внедрение вредоносного кода в адресное пространство другого процесса для выполнения его с правами этого процесса.

13. Scheduled Task/Job (Запланированная задача/работа):

- Создание запланированных задач с повышенными правами для автоматического выполнения вредоносного кода.

14. Valid Accounts (Действительные учетные записи):

- Использование действительных учетных записей с высокими правами доступа для выполнения действий, требующих этих прав.

**7. Defense Evasion (Избежание защиты):**

Этап избегания защиты включает в себя методы, которые злоумышленники используют для обхода систем безопасности и обнаружения. Эти методы позволяют им скрывать свое присутствие и действия в системе, что делает их атаки более успешными и трудными для выявления.

**Методы:**

1. Abuse Elevation Control Mechanism (Злоупотребление механизмом контроля повышения привилегий):

- Использование уязвимостей в механизмах контроля доступа для обхода защитных мер.

2. Access Token Manipulation (Манипуляция токенами доступа):

- Изменение или подделка токенов доступа для обхода механизмов аутентификации.

3. BITS Jobs:

- Использование Background Intelligent Transfer Service (BITS) для загрузки и выполнения вредоносного кода, что может быть менее заметно для систем безопасности.

4. Build Image on Host:

- Создание образов на хосте для внедрения вредоносного ПО без использования стандартных методов развертывания.

5. Debugger Evasion:

- Использование техник, чтобы избежать обнаружения отладчиками или системами анализа.

6. Deobfuscate/Decode Files or Information (Деобфускация/декодирование файлов или информации):

- Применение методов декодирования или деобфускации для скрытия истинного содержания вредоносного кода.

7. Deploy Container:

- Развертывание контейнеров для изоляции вредоносной активности от основной системы.

8. Direct Volume Access:

- Прямой доступ к томам данных для обхода стандартных механизмов защиты.

9. Domain or Tenant Policy Modification (Модификация политик домена или арендатора):

- Изменение политик безопасности для ослабления защиты системы.

10. Execution Guardrails (Ограничения выполнения):

- Обход ограничений, установленных для предотвращения выполнения нежелательных действий.

11. Exploitation for Defense Evasion (Эксплуатация уязвимостей для избегания защиты):

- Использование уязвимостей в программном обеспечении для обхода защитных механизмов.

12. File and Directory Permissions Modification (Модификация прав доступа к файлам и директориям):

- Изменение прав доступа к файлам и директориям, чтобы скрыть вредоносные действия.

13. Hide Artifacts (Скрытие артефактов):

- Скрытие следов своей деятельности, таких как журналы или временные файлы.

14. Hijack Execution Flow (Перехват потока исполнения):

- Изменение нормального потока выполнения программ для запуска вредоносного кода без обнаружения.

15. Impair Defenses (Ослабление защит):

- Устранение или ослабление механизмов защиты системы.

16. Impersonation (Имитация):

- Выдача себя за другого пользователя или процесс с целью получения доступа к защищенным ресурсам.

17. Indicator Removal (Удаление индикаторов):

- Удаление следов своей активности из системных журналов и других мест хранения информации о событиях.

18. Indirect Command Execution:

- Выполнение команд через промежуточные шаги, чтобы избежать обнаружения.

19. Masquerading (Маскировка):

- Выдача вредоносного ПО за легитимные процессы или файлы, чтобы избежать внимания систем безопасности.

20. Modify Authentication Process (Модификация процесса аутентификации):

- Изменение процесса аутентификации для обхода стандартных методов проверки подлинности пользователей.

21. Modify Cloud Compute Infrastructure (Модификация облачной вычислительной инфраструктуры):

- Изменение настроек облачной инфраструктуры с целью получения несанкционированного доступа или обхода защитных мер.

22. Modify Cloud Resource Hierarchy:

- Изменение иерархии ресурсов в облаке для получения дополнительных прав доступа.

23. Modify Registry:

- Внесение изменений в реестр Windows с целью изменения поведения системы или скрытия следов активности.

24. Modify System Image (Модификация образа системы):

- Внесение изменений в образ операционной системы с целью внедрения вредоносного ПО на уровне загрузки.

25. Network Boundary Bridging (Преодоление сетевых границ):

- Обход сетевых барьеров и фильтров безопасности для получения доступа к защищенным ресурсам сети.

26. Obfuscated Files or Information (Обфусцированные файлы или информация):

- Использование обфускации кода или данных для затруднения анализа и обнаружения вредоносной активности.

27. Plist File Modification:

- Модификация файлов plist на macOS для изменения поведения приложений или системных процессов.

28. Pre-OS Boot (Предварительная загрузка ОС):

- Внедрение вредоносного ПО на уровне загрузчика операционной системы до загрузки самой ОС.

29. Process Injection (Инъекция процессов):

- Внедрение вредоносного кода в адресное пространство другого процесса с целью его выполнения с правами этого процесса.

30. Reflective Code Loading:

- Загрузка и выполнение кода непосредственно из памяти без записи на диск, что затрудняет его обнаружение антивирусами и другими средствами защиты.

31. Rogue Domain Controller:

- Создание поддельного контроллера домена с целью перехвата аутентификационных запросов и управления доступом к ресурсам сети.

32. Rootkit:

- Установка руткита — программного обеспечения, которое позволяет злоумышленнику получить полный контроль над системой, оставаясь незамеченным.

33. Subvert Trust Controls (Подрыв доверительных контролей):

- Обход механизмов доверия в системе, таких как цифровые подписи и сертификаты.

34. System Binary Proxy Execution:

- Использование легитимных бинарных файлов системы как прокси для выполнения вредоносного кода.

35. System Script Proxy Execution:

- Использование легитимных скриптов системы как прокси для запуска вредоносной активности.

36. Template Injection:

- Внедрение вредоносного кода через шаблоны документов или приложений.

37. Traffic Signaling (Сигнализация трафика):

- Использование сетевого трафика как сигнала для активации определенных действий.

38. Trusted Developer Utilities Proxy Execution:

- Использование утилит разработчиков с высоким уровнем доверия как прокси для выполнения нежелательных действий.

39. Unused/Unsupported Cloud Regions:

– Использование неиспользуемых или неподдерживаемых регионов облака для развертывания атакующих инфраструктур.

40. Use Alternate Authentication Material (Использование альтернативных материалов аутентификации):

– Применение альтернативных методов аутентификации, таких как токены доступа, чтобы обойти стандартные механизмы проверки подлинности.

41.  Valid Accounts (Действительные учетные записи):

– Использование действительных учетных записей с высокими правами доступа для выполнения действий, требующих этих прав.

42 .  Virtualization/Sandbox Evasion:

– Применение техник уклонения от виртуализации и песочниц, чтобы избежать анализа.

43 .  Weaken Encryption (Ослабление шифрования):

– Уменьшение уровня шифрования данных с целью облегчения их перехвата и анализа.

44 .  XSL Script Processing:

– Использование XSL-скриптов для обработки данных таким образом, чтобы скрыть истинную природу выполняемых операций.

**8. Credential Access (Доступ к учетным данным):**

Этап доступа к учетным данным включает в себя методы, которые злоумышленники используют для получения учетных данных пользователей, таких как пароли, токены доступа и другие формы аутентификации. Эти методы могут быть использованы для получения несанкционированного доступа к системам и данным.

**Методы:**

1. Adversary-in-the-Middle (Противник посередине):

- Злоумышленник перехватывает и потенциально изменяет коммуникации между двумя сторонами, чтобы получить доступ к учетным данным.

2. Brute Force (Грубая сила):

- Попытка перебора всех возможных комбинаций паролей для доступа к учетной записи.

3. Credentials from Password Stores (Учетные данные из хранилищ паролей):

- Извлечение учетных данных из хранилищ паролей, таких как менеджеры паролей или системные хранилища.

4. Exploitation for Credential Access (Эксплуатация для доступа к учетным данным):

- Использование уязвимостей в системах или приложениях для получения учетных данных.

5. Forced Authentication (Принудительная аутентификация):

- Принуждение пользователя к повторной аутентификации с целью перехвата его учетных данных.

6. Forge Web Credentials (Подделка веб-учетных данных):

- Создание поддельных учетных данных для доступа к веб-приложениям.

7. Input Capture (Перехват ввода):

- Использование программного обеспечения или оборудования для захвата вводимых пользователем данных, таких как пароли.

8. Modify Authentication Process (Модификация процесса аутентификации):

- Изменение процесса аутентификации с целью получения доступа к защищенным ресурсам.

9. Multi-Factor Authentication Interception (Перехват многофакторной аутентификации):

- Перехват кодов или токенов, используемых в многофакторной аутентификации.

10. Multi-Factor Authentication Request Generation:

- Генерация запросов на многофакторную аутентификацию с целью перехвата ответов.

11. Network Sniffing (Прослушивание сети):

- Перехват сетевого трафика для извлечения учетных данных и другой конфиденциальной информации.

12. OS Credential Dumping (Извлечение учетных данных ОС):

- Извлечение учетных данных из операционной системы, включая пароли и токены доступа.

13. Steal Application Access Token (Кража токена доступа приложения):

- Получение токенов доступа, используемых приложениями для взаимодействия с API и другими сервисами.

14. Steal or Forge Authentication Certificates (Кража или подделка сертификатов аутентификации):

- Получение или создание поддельных сертификатов для обхода механизмов безопасности.

15. Steal or Forge Kerberos Tickets (Кража или подделка билетов Kerberos):

- Получение или создание поддельных билетов Kerberos для несанкционированного доступа к ресурсам сети.

16. Steal Web Session Cookie (Кража веб-сессионного куки):

- Перехват куки-файлов сессии пользователя для получения несанкционированного доступа к веб-приложениям.

17. Unsecured Credentials (Несанкционированные учетные данные):

- Использование незащищенных или плохо защищенных учетных данных, которые могут быть легко извлечены злоумышленниками.

**9. Discovery (Обнаружение):**

Этап обнаружения включает в себя методы, которые злоумышленники используют для сбора информации о целевой системе, сети или организации. Эти методы помогают им понять структуру системы, доступные ресурсы и потенциальные уязвимости, что может быть использовано для дальнейших атак.

**Методы:**

1. Account Discovery (Обнаружение учетных записей):

- Сбор информации о существующих учетных записях пользователей и их правах доступа.

2. Application Window Discovery:

- Определение открытых окон приложений на целевой системе.

3. Browser Information Discovery:

- Сбор информации о браузерах, установленных на целевой системе, включая версии и расширения.

4. Cloud Infrastructure Discovery:

- Обнаружение компонентов облачной инфраструктуры, используемой организацией.

5. Cloud Service Dashboard:

- Доступ к панелям управления облачными сервисами для получения информации о ресурсах и конфигурациях.

6. Cloud Service Discovery:

- Обнаружение доступных облачных сервисов и их конфигураций.

7. Cloud Storage Object Discovery:

- Изучение объектов хранения в облачных сервисах для выявления конфиденциальных данных.

8. Container and Resource Discovery:

- Обнаружение контейнеров и ресурсов в средах виртуализации или контейнеризации.

9. Debugger Evasion:

- Использование методов уклонения от отладчиков для скрытия действий от систем безопасности.

10. Device Driver Discovery:

- Сбор информации о драйверах устройств, установленных на целевой системе.

11. Domain Trust Discovery:

- Определение доверительных отношений между доменами в сети.

12. File and Directory Discovery:

- Изучение файловой системы для выявления важных файлов и директорий.

13. Group Policy Discovery:

- Сбор информации о групповых политиках, применяемых в сети.

14. Log Enumeration:

- Изучение журналов событий для получения информации о действиях пользователей и системных событиях.

15. Network Service Discovery:

- Обнаружение сетевых служб, работающих на целевой системе или в сети.

16. Network Share Discovery:

- Определение общих ресурсов в сети, доступных для пользователей.

17. Network Sniffing (Прослушивание сети):

- Перехват сетевого трафика для извлечения конфиденциальной информации.

18. Password Policy Discovery:

- Изучение политик паролей, применяемых в организации, чтобы понять требования к паролям пользователей.

19. Peripheral Device Discovery:

- Определение периферийных устройств, подключенных к целевой системе.

20. Permission Groups Discovery (Обнаружение групп разрешений) (3):

- Сбор информации о группах разрешений и их членах в системе.

21. Process Discovery (Обнаружение процессов):

- Определение запущенных процессов на целевой системе для выявления активных приложений и служб.

22. Query Registry (Запрос реестра):

- Изучение реестра Windows для получения конфигурационной информации о системе и установленных приложениях.

23. Remote System Discovery (Обнаружение удаленных систем):

- Сбор информации о системах, доступных через сеть или интернет.

24. Software Discovery (Обнаружение программного обеспечения) (1):

- Определение установленного программного обеспечения на целевой системе для выявления потенциально уязвимых приложений.

25. System Information Discovery (Обнаружение системной информации):

- Сбор общей информации о системе, включая аппаратные характеристики и установленное ПО.

26. System Location Discovery (Обнаружение местоположения системы) (1):

- Определение физического или логического местоположения системы в сети или инфраструктуре организации.

27. System Network Configuration Discovery (Обнаружение конфигурации сети системы) (2):

- Изучение сетевых настроек системы для понимания ее подключения к другим устройствам.

28. System Network Connections Discovery (Обнаружение сетевых подключений системы):

- Определение активных сетевых подключений и их состояния.

29. System Owner/User Discovery (Обнаружение владельца/пользователя системы):

- Сбор информации о владельцах или пользователях системы.

30. System Service Discovery (Обнаружение служб системы):

- Определение запущенных служб на целевой системе.

31. System Time Discovery (Обнаружение времени системы):

- Получение текущего времени и даты на целевой системе.

32. Virtualization/Sandbox Evasion (Уклонение от виртуализации/песочницы) (3):

- Использование методов уклонения от обнаружения в средах виртуализации или песочницах.

**10. Lateral Movement (Боковое перемещение):**

Этап бокового перемещения включает в себя методы, которые злоумышленники используют для перемещения внутри сети после первоначального доступа. Эти методы позволяют им получать доступ к другим системам и ресурсам, что может привести к дальнейшему компрометированию сети.

**Методы:**

1. Exploitation of Remote Services (Эксплуатация удаленных служб):

- Использование уязвимостей в удаленных службах для получения доступа к другим системам в сети.

2. Internal Spearphishing (Внутренний целевой фишинг):

- Отправка фишинговых сообщений внутри организации с целью получения учетных данных или установки вредоносного ПО на другие системы.

3. Lateral Tool Transfer (Передача инструментов бокового перемещения):

- Перемещение инструментов и программного обеспечения между системами для выполнения атак или сбора информации.

4. Remote Service Session Hijacking (Перехват сеансов удаленной службы) (2):

- Перехват активных сеансов удаленных служб для получения доступа к ресурсам и данным.

5. Remote Services (Удаленные службы) (8):

- Использование различных удаленных служб для доступа к другим системам, включая

6. Replication Through Removable Media:

- Использование съемных носителей для распространения вредоносного ПО или получения доступа к другим системам.

7. Software Deployment Tools:

- Использование инструментов развертывания программного обеспечения для установки вредоносных приложений на другие системы.

8. Taint Shared Content:

- Внедрение вредоносного кода в общие ресурсы, такие как файлы или папки, доступные нескольким пользователям.

9. Use Alternate Authentication Material (Использование альтернативных материалов аутентификации) (4):

- Использование других методов аутентификации, таких как токены или сертификаты, для доступа к системам без использования стандартных учетных данных.

**11. Collection (Сбор данных):**

Этап сбора данных включает в себя методы, которые злоумышленники используют для извлечения информации из скомпрометированных систем или сетей. Эти методы могут варьироваться от простого захвата данных до более сложных техник, направленных на получение конфиденциальной информации.

**Методы:**

1. Adversary-in-the-Middle (Противник посередине) (4):

- Техника, при которой злоумышленник перехватывает и потенциально изменяет коммуникации между двумя сторонами без их ведома.

2. Archive Collected Data (Архивирование собранных данных) (3):

- Сохранение собранной информации для дальнейшего анализа или использования.

3. Audio Capture (Запись аудио):

- Захват звуковых данных с помощью микрофонов или других устройств.

4. Automated Collection (Автоматизированный сбор):

- Использование скриптов или программного обеспечения для автоматического извлечения данных из систем.

5. Browser Session Hijacking (Перехват сеансов браузера):

- Перехват активных сеансов браузера для получения доступа к учетным записям и данным пользователей.

6. Clipboard Data (Данные из буфера обмена):

- Сбор информации, скопированной в буфер обмена пользователя.

7. Data from Cloud Storage (Данные из облачного хранилища):

- Извлечение данных из облачных сервисов и хранилищ.

8. Data from Configuration Repository (Данные из репозитория конфигурации) (2):

- Доступ к данным, хранящимся в репозиториях конфигурации систем и приложений.

9. Data from Information Repositories (Данные из информационных репозиториев) (5):

- Извлечение информации из различных репозиториев, таких как базы данных и файловые системы.

10. Data from Local System (Данные с локальной системы:

- Сбор информации непосредственно с локального устройства.

11. Data from Network Shared Drive (Данные с сетевого общего диска):

- Доступ к данным, хранящимся на общих сетевых ресурсах.

12. Data from Removable Media (Данные со съемных носителей):

- Извлечение информации со съемных устройств, таких как USB-накопители.

13. Data Staged (Подготовленные данные) (2):

- Сбор и подготовка данных для дальнейшего использования или передачи.

14. Email Collection (Сбор электронной почты) (3):

- Извлечение данных из электронных писем и почтовых ящиков пользователей.

15. Input Capture (Захват ввода) (4):

- Техника захвата вводимых пользователем данных, таких как пароли или текстовые сообщения.

16. Screen Capture (Снимок экрана):

- Захват изображений экрана для получения визуальной информации о действиях пользователя.

17. Video Capture (Запись видео):

- Запись видео с экрана или веб-камеры для получения дополнительной информации о действиях пользователя.

**12. Command and Control (Командование и управление):**

Этап командования и управления включает в себя методы, которые злоумышленники используют для связи с скомпрометированными системами и управления ими. Эти методы могут варьироваться от использования стандартных протоколов до более сложных техник, направленных на скрытие их активности.

**Методы:**

1. Application Layer Protocol (Протокол прикладного уровня) (5):

- Использование стандартных протоколов для связи с скомпрометированными системами.

2. Communication Through Removable Media (Связь через съемные носители):

- Передача команд и данных через USB-накопители или другие съемные устройства.

3. Content Injection (Инъекция контента):

- Внедрение вредоносного кода или команд в легитимный контент.

4. Data Encoding (Кодирование данных) (2):

- Применение различных методов кодирования для сокрытия данных.

5. Data Obfuscation (Обфускация данных) (3):

- Применение техник для затруднения анализа и понимания данных.

6. Dynamic Resolution (Динамическое разрешение) (3):

- Изменение адресов или доменов для управления скомпрометированными системами.

7. Encrypted Channel (Зашифрованный канал) (2):

- Использование шифрования для защиты передаваемых данных и скрытия их содержания.

8. Fallback Channels (Резервные каналы):

- Альтернативные каналы связи, используемые в случае недоступности основных.

9. Hide Infrastructure (Скрытие инфраструктуры):

- Применение методов для сокрытия серверов и других компонентов инфраструктуры злоумышленника.

10. Ingress Tool Transfer (Передача инструментов через входные каналы):

- Перемещение вредоносных инструментов в скомпрометированные системы.

11. Multi-Stage Channels (Многоуровневые каналы):

- Использование нескольких этапов или уровней для передачи команд и данных.

12. Non-Application Layer Protocol (Протокол не прикладного уровня):

- Использование протоколов, не относящихся к прикладному уровню, для управления системами.

13. Non-Standard Port (Нестандартный порт):

- Использование нестандартных портов для обхода фильтров и обнаружения.

14. Protocol Tunneling (Туннелирование протоколов):

- Инкапсуляция одного протокола в другом для обхода ограничений сети.

15. Proxy (Прокси-сервер) (4):

- Использование прокси-серверов для маршрутизации трафика и скрытия источника команд.

16. Remote Access Software (Программное обеспечение удаленного доступа):

- Использование программ для удаленного управления скомпрометированными системами.

17 Traffic Signaling (Сигнализация трафика) (2):

* Методы управления трафиком для передачи команд или информации.

18. Web Service (Веб-сервис) (3):

- Использование веб-сервисов для взаимодействия с скомпрометированными системами и передачи команд.

**13. Exfiltration (Экстракция данных):**

Этап экстракции данных включает в себя методы, которые злоумышленники используют для извлечения данных из скомпрометированных систем и их передачи на свои серверы или другие места хранения. Эти методы могут варьироваться от автоматизированных процессов до использования альтернативных протоколов и средств.

**Методы:**

1. Automated Exfiltration (Автоматизированная экстракция) (1):

- Использование автоматизированных инструментов и скриптов для извлечения данных без вмешательства человека.

2. Data Transfer Size Limits (Ограничения на размер передачи данных):

- Учет ограничений на размер передаваемых данных, чтобы избежать обнаружения.

3. Exfiltration Over Alternative Protocol (Экстракция через альтернативные протоколы) (3):

- Использование нестандартных или альтернативных протоколов для передачи данных.

4. Exfiltration Over C2 Channel (Экстракция через канал командования и управления):

- Передача данных через каналы, используемые для управления скомпрометированными системами.

5. Exfiltration Over Other Network Medium (Экстракция через другие сетевые среды) (1):

- Использование различных сетевых сред для передачи данных.

6. Exfiltration Over Physical Medium (Экстракция через физические носители) (1):

- Передача данных через физические устройства, такие как USB-накопители или другие съемные носители.

7. Exfiltration Over Web Service (Экстракция через веб-сервис) (4):

- Использование веб-сервисов для передачи данных.

8. Scheduled Transfer (Запланированная передача):

- Настройка автоматической передачи данных в определенное время.

9. Transfer Data to Cloud Account (Передача данных в облачный аккаунт):

- Перемещение собранной информации в облачные хранилища для дальнейшего использования.

**14. Impact (Воздействие):**

Этап воздействия включает в себя последствия, которые могут возникнуть в результате успешной атаки на систему или организацию. Эти последствия могут варьироваться от потери данных до финансовых убытков и нарушения работы систем.

**Методы:**

1. Account Access Removal (Удаление доступа к учетным записям):

- Устранение доступа пользователей к учетным записям, что может привести к потере контроля над системами.

2. Data Destruction (Уничтожение данных) (1):

- Уничтожение данных с целью причинения вреда или затруднения восстановления.

3. Data Encrypted for Impact (Данные зашифрованы для воздействия):

- Шифрование данных с целью вымогательства или создания помех в доступе к информации.

4. Data Manipulation (Манипуляция данными) (3):

- Изменение данных с целью их искажения или подмены.

5. Defacement (Дефейсинг) (2):

- Изменение внешнего вида веб-сайта или приложения для нанесения ущерба репутации.

6. Disk Wipe (Стирание диска) (2):

- Полное удаление данных с диска, что делает их восстановление невозможным.

7. Endpoint Denial of Service (Отказ в обслуживании конечной точки) (4):

- Атаки, направленные на недоступность конечных устройств или сервисов.

8. Financial Theft (Финансовая кража):

- Кража денежных средств или финансовой информации.

9. Firmware Corruption (Порча прошивки):

- Изменение или повреждение прошивки устройств, что может привести к их неработоспособности.

10. Inhibit System Recovery (Препятствование восстановлению системы):

- Создание условий, при которых восстановление системы становится невозможным.

11. Network Denial of Service (Отказ в обслуживании сети) (2):

- Атаки, направленные на недоступность сетевых ресурсов и сервисов.

12. Resource Hijacking (Перехват ресурсов) (4):

- Использование ресурсов системы без разрешения владельца.

13. Service Stop (Остановка сервиса):

- Принудительная остановка работы сервисов и приложений.

14. System Shutdown/Reboot (Выключение/перезагрузка системы):

- Принудительное завершение работы системы или ее перезагрузка.

**OWASP**

**Top Ten:**

OWASP (Open Web Application Security Project) представляет собой международную организацию, занимающуюся повышением безопасности программного обеспечения.

Одним из ключевых документов этой организации является список OWASP Top Ten, который выделяет самые критические риски безопасности для веб-приложений. Этот документ служит важным инструментом для повышения осведомленности разработчиков и организаций о проблемах безопасности.

Основные риски в OWASP Top Ten 2021:

1. A01: Broken Access Control (Нарушение контроля доступа)

- Переместился на первую позицию; 94% приложений были протестированы на наличие нарушений контроля доступа.

2. A02: Cryptographic Failures (Ошибки криптографии)

- Переместился на вторую позицию; акцент на сбоях в криптографии, которые могут привести к утечке данных.

3. A03: Injection (Инъекции)

- Сдвинулся на третью позицию; инъекции остаются одной из самых распространенных уязвимостей.

4. A04: Insecure Design (Небезопасный дизайн)

- Новая категория, подчеркивающая важность безопасного проектирования приложений.

5. A05: Security Misconfiguration (Ошибки конфигурации безопасности)

- Поднялся с шестой позиции; ошибки конфигурации остаются распространенной проблемой.

6. A06: Vulnerable and Outdated Components (Уязвимые и устаревшие компоненты)

- Увеличение числа уязвимостей в устаревших компонентах программного обеспечения.

7. A07: Identification and Authentication Failures (Ошибки идентификации и аутентификации)

- Опустился с второй позиции; включает ошибки идентификации.

8. A08: Software and Data Integrity Failures (Ошибки целостности программного обеспечения и данных)

- Новая категория, сосредоточенная на целостности обновлений и данных.

9. A09: Security Logging and Monitoring Failures (Ошибки ведения журналов безопасности и мониторинга)

- Поднялся с десятой позиции; важность ведения журналов для обнаружения инцидентов.

10. A10: Server-Side Request Forgery (Подделка запросов со стороны сервера)

- Новая категория, выявленная как критическая угроза.

**ASVS:**

OWASP Application Security Verification Standard (ASVS) — это проект, который предоставляет основу для тестирования технических средств безопасности веб-приложений и список требований для безопасной разработки.

**Dependency-Track:**

OWASP Dependency-Track — это интеллектуальная платформа для анализа компонентов, которая помогает организациям выявлять и снижать риски в цепочке поставок программного обеспечения.

**Juice Shop:**

OWASP Juice Shop — это современное и сложное небезопасное веб-приложение, предназначенное для использования в обучении по безопасности, демонстрациях, соревнованиях Capture The Flag (CTF) и тестировании инструментов безопасности. Оно охватывает уязвимости из всего списка OWASP Top Ten, а также множество других недостатков, встречающихся в реальных приложениях.

**Mobile Application Security:**

OWASP Mobile Application Security (MAS) — это флагманский проект, который предоставляет стандарт безопасности для мобильных приложений (OWASP MASVS) и исчерпывающее руководство по тестированию безопасности (OWASP MASTG). Эти ресурсы охватывают процессы, техники и инструменты, используемые во время тестирования безопасности мобильных приложений, а также содержат обширный набор тестовых случаев для обеспечения последовательности и полноты результатов.

**Core Rule Set (CRS):**

OWASP Core Rule Set (CRS) — это набор универсальных правил обнаружения атак, предназначенных для использования с ModSecurity или совместимыми веб-аппликационными фаерволами. CRS направлен на защиту веб-приложений от широкого спектра атак, включая уязвимости из списка OWASP Top Ten, при минимальном количестве ложных срабатываний.

**Software Assurance Maturity Model (SAMM):**

OWASP Software Assurance Maturity Model (SAMM) — это открытая модель, предназначенная для помощи организациям в формулировании и реализации стратегии безопасности программного обеспечения, адаптированной к конкретным рискам, с которыми сталкивается организация. SAMM поддерживает полный жизненный цикл разработки программного обеспечения и не зависит от технологий или процессов.

**Web Security Testing Guide (WSTG):**

OWASP Web Security Testing Guide (WSTG) — это ведущий ресурс по тестированию кибербезопасности для разработчиков веб-приложений и специалистов по безопасности. WSTG представляет собой исчерпывающее руководство по тестированию безопасности веб-приложений и веб-сервисов, созданное в результате совместных усилий профессионалов в области кибербезопасности и преданных волонтеров.

**Кибератака на инфраструктуру Platformix (2023 г.)**

Инцидент с кибератакой на компанию Platformix демонстрирует, как злоумышленники могут использовать различные тактики и процедуры для достижения своих целей, даже если цель кажется неочевидной. Давайте разберем ключевые аспекты этой атаки.

**Тактики и процедуры злоумышленников:**

1. Социальная инженерия:

- Злоумышленники использовали фишинговое письмо, чтобы обмануть сотрудников компании. Письмо было тщательно подготовлено, чтобы выглядеть достоверным и не вызывать подозрений. Это указывает на то, что злоумышленники провели предварительное исследование и выделили потенциальные жертвы среди сотрудников.

2. Компрометация учетных данных:

- После того как жертва открыла фишинговое письмо, был установлен вредоносный драйвер, который отключал антивирусное ПО и повышал привилегии злоумышленника в системе. Это позволило ему получить доступ к учетной записи управления доменом.

3. Горизонтальное перемещение:

- После получения доступа к учетной записи управления доменом злоумышленник смог перемещаться по сети компании, компрометируя другие серверы и рабочие станции. Это свидетельствует о том, что атака была спланирована с учетом возможности дальнейшего распространения вредоносного ПО.

4. Использование доверенных сторонних организаций:

- Атака была осуществлена через стороннюю организацию, которой Platformix ранее доверял. Это подчеркивает важность оценки рисков при работе с внешними партнерами и поставщиками.

5. Скрытность действий:

- Злоумышленники использовали набор вредоносных программ, которые не были обнаружены популярными антивирусами на момент атаки. Это говорит о том, что они применяли современные методы обхода защиты.

**Реакция компании:**

1. Обнаружение инцидента:

- Атака была выявлена только после потери доступа к управлению доменом и отсутствия ответов от антивирусной защиты. Это подчеркивает важность постоянного мониторинга и анализа логов для раннего обнаружения аномалий.

2. Восстановление данных:

- ИТ-специалисты начали восстановление данных из резервных копий и ввели ограничения на удаленный доступ для посторонних пользователей.

3. Привлечение специалистов:

- Для более глубокого анализа инцидента были приглашены эксперты из Kaspersky, что позволило выявить дополнительные зараженные машины и источники атаки.

4. Уроки из инцидента:

- Компания провела мероприятия по повышению осведомленности сотрудников о безопасности информации, переустановила программы и сервисы, сбросила учетные записи пользователей с повышенными правами и пересмотрела политики безопасности.

**Выводы:**

Инцидент с Platformix показывает, что даже компании с высокими стандартами безопасности могут стать жертвами кибератак из-за завышенной самоуверенности или недостаточной бдительности в отношении угроз социальной инженерии. Важно постоянно обновлять меры безопасности, обучать сотрудников и проводить регулярные проверки системы на наличие уязвимостей.