Отчет к заданию для инженера-аналитика

Выполнил: Фролов Олег

Оглавление

Задача 1

Задания:

1. Провести частичный анализ OVAL-файла от компании Red Hat для ОС RHEL8 на первых 3-х уязвимостях (патчах) и определить набор объектов, из которых он состоит. Разобрать основную логику работы с данным форматом.
2. Описать кратко текстом объекты, которые были найдены, и для чего они используются.
3. Установить, какие критерии каждой “уязвимости” являются лишними, а какие обязательными.
4. Упростить текущий формат и описать свой вариант описания уязвимости вместе с проверками.
5. Разработать приложение-скрипт парсинга OVAL-файла для преобразования в предложенный упрощенный формат.

Частичный анализ OVAL-файла

OVAL-файл, это XML файл. Он начинается с XML-заголовка (пролога) и состоит из корня, представленного в виде тега <oval_definitions>. Далее идет блок <generator> с информацией о продукте, версии, версии используемой XML схемы, по которой можно найти всю необходимую информацию о всех используемых параметрах и их значениях.

После <generator> следует блок <definitions>, в котором содержатся объекты <definition> с информацией о патчах, уязвимостях. Далее находится блок <tests>, содержащий всю информацию о тестах. После блока с описанием тестов идет блок <objects>, содержащий информацию об объектах. И замыкает данный файл блок <states>, описывающий условия, при которых выполняются тесты.

Описание объектов

- <xml version> - XML-пролог, включающий версию и используемую кодировку;
- <oval_definitions> - корневой объект, хранит в себе блоки generator, definitions, tests, objects, states;
    - <generator> - блок генератора, указывающий продукт, версию, версию используемой XML схемы;
    - <definitions> - блок/список объектов типа definition с информацией об уязвимостях;
        - <definition> - объект уязвимости, патча (есть ещё compliance, inventory, miscellaneous) содержащий информацию о том, уязвимость это или патч, идентификационную информацию;
            - <metadata> - объект со всеми метаданными данного патча;
                - <title> - название (человекочитаемое);
                - <affected family> - связанное семейство ОС;
                    - <platform> - связанная платформа;
                - <reference> - референсы (ссылки на информацию об уязвимости, закрываемую обновлением, на источник);
                - <description> - описание уязвимого продукта, пакета;
                - <advisory from> - от кого прилетела рекомендация по установке обновления;
                    - <severity> - критичность уязвимости;
                    - <rights> - авторские права;
                    - <issued date> - дата выхода;
                    - <updated date> - дата последнего обновления;
                    - <cve> - информация о CVE (оценка по CVSS 3.0, CWE, референс);
                    - <bugzilla> - информация с bugzill'a с референсом;
                    - <affected_cpe_list> - список cpe объектов;
                        - <cpe> - объект с идентификационной информацией ПО, ОС, к которому применима данная уязвимость;
            - <criteria> - объект для работы с логическими выражениями;

        - <criterion> - объект, включающий условия для проверки в зависимости от указанного параметра в criteria (по умолчанию - AND), там же id соответствующего теста;
- <tests> - список объектов, описывающих тесты;
    - <red-def:rpminfo_test> - объект, содержащий информацию о тесте
        - <red-def:object> - информация об объекте, к которому относится тест (содержит id объекта из этого файла);
        - <red-def:state> - информация о состоянии, к которому относится тест (содержит id состояния из этого файла);
    - <red-def:rpmverifyfile_test> - объект, содержащий информацию о проверке установленной ОС и соответствующие id состояния и объекта из данного файла;
- <objects> - список объектов;
    - <red-def:rpminfo_object> - объект, описывающий *объект*;
        - <red-def:name> - имя проверяемого объекта;
    - <red-def:rpmverifyfile_object> - объект, описывающий файлы для проверки;
        - <red-def:behaviors> - объект, описывающий, как должна проходить проверка файлов;
        - <red-def:epoch> - номер эпохи RPM;
        - <red-def:version> - номер версии сборки;
        - <red-def:release> - номер выпуска сборки;
        - <red-def:arch> - архитектура;
        - <red-def:filepath> - объект, описывающий абсолютный путь к каталогу;
    - <ind-def:textfilecontent54_object> -
- <states> - список состояний;
    - <red-def:rpminfo_state> - объект, содержащий информацию для оценки RPM;
        - <red-def:evr> - эпоха, версия, release в качестве одной строки;
        - <red-def:signatre_keyid> - 64-разрядный идентификатор PGP ключа, используемый издателем RPM;
    - <red-def:rpmverify_state> - объект, содержащий информацию для оценки RPM;
        - <red-def:name> - имя пакета для проверки;

- <red-def:version> - версия;

Оценка критериев уязвимостей

На мой взгляд лишними критериями являются критерии проверки того, являются ли указанные пакеты подписанными с ключом Red Hat redhatrelease2. Т.к. они присутствуют в большом количестве, что увеличивает в целом размер файла, так и усложняет его ручное прочтение, если такое необходимо. Проверки установленной ОС и версий пакетов являются важными, т.к. позволяют проверить систему на наличие указанных уязвимостей и на необходимость установки указанных патчей.

Упростить текущий формат

Для упрощения формата можно убрать упоминание про наличие подписанных пакетов в критериях к патчам, уязвимостям и в тестах. Или, как вариант, вынести этот параметр отдельно, чтобы разгрузить файл. Далее в своей реализации я решил вовсе отказаться от этой информации.

В названии каждого патча присутствует в скобках указание критичности, хотя она упомянута, как отдельный параметр. В своей реализации я решил убрать из названий упоминание о критичности, оставив её в качестве отдельного поля.

В своем новом формате я не включал ссылки на референсы, оставив лишь сами CVE, RHBA, по которым при необходимости можно найти всю информацию в Интернете. Аналогично поступил с CVSS, сократив данные поля (содержат только оценку по CVSS 3 и CVE, для которой приведена оценка).

Отказался от поля advisor, т.к. не совсем понятно, как оно может пригодиться. Из-за аналогичной ненадобности отказался от поля rights.

Поля issued_date и updated_date тоже были удалены. Хотя, с другой стороны, поле issued_date следует оставить, т.к. это может быть полезно в некоторых ситуациях.

Разработать скрипт для парсинга OVAL-файла в новый формат

Скрипт работает следующим образом:

- В main’е указывается путь до OVAL-файла (в oval_file);
- При запуске скрипт парсит указанный OVAL-файл, после чего предлагает пользователю ввести id патча, уязвимости, по которым необходимо получить информацию или ввести “save” для сохранения полученной информации в новом формате с названием result.xml;
- Если пользователь ввел id патча, уязвимости, то получит информацию о данном патче, уязвимости, которую спарсил скрипт из OVAL-файла.

Задача 2

Задания:

1. Провести анализ CIS Microsoft Windows 11 Enterprise;
2. Приоритизировать проверки и выбрать 10 самых критичных;
3. Описать выбранные критерии, почему они важны;
4. Для каждой из 10 выбранных проверок подобрать или составить команду(-ы) для выполнения в командной строке, которая(-ые) поможет(-гут) в проверке на соответствие стандарту.

Анализ CIS Microsoft Windows 11 Enterprise

Список критичных проверок составлен ниже в соответствии с приоритетом проверки, от наивысшего приоритета к наименьшему. В каждом пункте приведено описание проверки: за что отвечает и почему важна. Дополнительно приведена команда для Powershell, позволяющая произвести проверку. Возвращаемое значение должно быть “True”, иначе проверка не пройдена (если выдается ошибка или “False”).

1. **Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' (9.1.1, 9.2.1)**

Отвечает за включение локального фаервола. Крайне необходим для фильтрации входящего/исходящего трафика путем создания правил, это может позволить препятствовать, например, установлению соединения с внешним хостом какой-нибудь малварью, случайно занесенной на устройство, и которую не обнаружил антивирус.

Powershell: (Get-ItemProperty -Path "HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile" -Name "EnableFirewall").EnableFirewall -eq 1

2. **Ensure 'Configures LSASS to run as a protected process' is set to 'Enabled: Enabled with UEFI Lock' (18.9.26.2)**

Отвечает за включение опции доступа к lsass только защищенным процессам. Позволяет защититься от примитивных попыток извлечь креды из дампа lsass процесса (тем же mimikatz). Т.к. у злоумышленника не будет возможности снять дамп lsass.exe даже при наличии прав на такое действие (в случае с mimikatz ему будет отказано в доступе, ошибка - 0x00000005). Есть варианты обхода, но это уже не из разряда простейших действий, а также необходимо принять и иные меры.

Powershell: (Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "RunAsPPL").RunAsPPL -eq 1

3. **Ensure 'WDigest Authentication' is set to 'Disabled' (18.4.8)**

Отвечает за отключение WDigest аутентификации (лучше смотреть в сторону NTLMv2, Kerberos). Необходимо для случаев, когда злоумышленнику все-таки удастся снять дамп lsass.exe и разобрать его. Т.к. WDigest хранит в lsass.exe пароли в открытом виде.

Powershell: (Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest" -Name "UseLogonCredential").UseLogonCredential -eq 0

4. **Ensure 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' is set to '4 or fewer logon(s)' (2.3.7.7)**

Отвечает за количество кэшируемых логонов (количество учеток, с которых было N последних процессов аутентификации, чьи хэши паролей кэшируются). Используется, когда контроллер домена недоступен. Желательно установить значение в 0, чтобы их не кэшировать, т.к. потенциальный злоумышленник может достать данные хэши и поработать с ними.

Powershell: (Get-ItemProperty -Path "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" -Name "CachedLogonsCount").CachedLogonCount -eq 0

5. **Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled' (18.7.1)**

Отключает прием клиентских соединений сервисом Print Spooler. Позволяет защититься от удаленных атак PrintNightmare (CVE-2021-34527).

Powershell: (Get-ItemProperty -Path "HKLM:\Software\Policies\Microsoft\Windows NT\Printers" -Name "RegisterSpoolerRemoteRpcEndPoint").RegisterSpoolerRemoteRpcEndPoint -eq 2

6. **Ensure 'Configure DNS over HTTPS (DoH) name resolution' is set to 'Enabled: Allow DoH' or higher (18.6.4.1)**

Настраивает DNS на работу через HTTPS. Основная суть - добавить шифрование в передаваемые данные и наладить защиту от DNS спуфинга.

Powershell: (Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient" -Name "DoHPolicy" -ErrorAction SilentlyContinue).DoHPolicy -in 2,3

7. **Ensure 'Take ownership of files or other objects' is set to 'Administrators' (2.2.39)**

Устанавливает возможность смены владельца объекта Windows (привилегия SeTakeOwnership) только для группы Administrators. В теории, злоумышленник после получения доступа до системы через не администскую учетку, может попробовать воспользоваться при возможности данной функцией для получения доступа к недоступным объектам или для их изменения (в том числе и прав доступа к ним).

Powershell (если пользователь не в группе Administators): whoami /priv | Select-String "SeTakeOwnershipPrivilege"

8. **Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes' (9.1.6)**

Включает логирование пакетов, которые не пропустил локальный фаервол в соответствии с заданными правилами. Необходимо для мониторинга подозрительного входящего/исходящего трафика. Может помочь выявить несанкционированные попытки установления исходящих соединений, например, для отправки каких-либо данных, или выявить попытки сбора информации о системе (для корпоративной среды это может указать на попытки злоумышленника сканировать доступные хосты в сети и на попытки выявить у них уязвимые места).

Powershell: (Get-ItemProperty -Path "HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging" -Name "LogDroppedPackets").LogDroppedPackets -eq 1

9. **Ensure 'Audit Account Lockout' is set to include 'Failure' (17.5.1)**

Включает логирование неуспешного прохождения аутентификации пользователями (событие 4625). Полезно для мониторинга подозрительной активности. Может позволить выявить прямой или обратный брутфорс.

Powershell: auditpol /get /subcategory:"Account Lockout"

10. **Ensure 'Audit Special Logon' is set to include 'Success' (17.5.6)**

Включает логирование успешного прохождения аутентификации привилегированными пользователями (событие 4964). Полезно для мониторинга подозрительной активности с администских учеток. Позволит выявить факт компрометации такой учетки в идеальном случае и при должном мониторинге.

Powershell: auditpol /get /subcategory:"Special Logon"