Задание 1

Провести частичный анализ OVAL файла от компании Red Hat для ОС RHEL8 (https://www.redhat.com/security/data/oval/v2/RHEL8/rhel8.oval.xml.bz2) на первых 3 уязвимостях (патчах) и

определить набор объектов, из которых он состоит.

Набор объектов указан в приложении.

Разобрать основную логику работы с данным форматом.

Формат oval состоит из 5 частей: generator, definitions, tests, objects, states

generator: содержит общую информацию о файле OVAL

definitions: состоит из 2 частей. Metadata и criteria.

- Metadata: содержит общую информацию об уязвимости.
  Дату создания и обновления, описание уязвимости, CVSS, ссылки на информацию от вендора, уровень критичности, связанные CVE и CPE, и т.д.
- Criteria -содержит информацию для проверки уязвимости, и состоят о тестовх(tests), которые проверят наличие уязвимости. В случае положительного теста, будет подтверждено наличие уязвимости.
  В разделе перечислены id тестов, которые относятся к этой уязвимости (definition)

tests: содержит тесты для определения уязвимости. Тест состоит из объекта, и состояния для этого объекта, в случае если состояние объекта будет подтверждено, тест будет положительным, и наличие уязвимости будет подтверждено. Если объект не находится в ожидаемом состоянии, то тест будет отрицательным, и уязвимость не будет подтверждена.

objects: содержит список объектов для проверки уязвимости. Объект как правило является пакетом или файлом.

states: содержит состояния для объектов, как правило это номер версии или строчка конфига.

При проверке уязвимости, проверяется критерий, который в свою очередь состоят теста, который проверяет состояние объекта, и в случае, если объект находится в том, состоянии, который указан в тесте, то тест считается положительным, и критерий срабатывает, и указывает, что хост подвержен уязвимости.

Описать кратко текстом объекты, которые были найдены и для чего они используются.

Описание объектов указано в приложении.

В рамках каждой «уязвимости», есть условия по её выявлению: какие на ваш взгляд из критериев лишние, а какие обязательны?

RHBA-2019:1992: cloud-init bug fix and enhancement update (Moderate)
Обязательные проверки:

cloud-init is earlier than 0:18.5-1.el8.4

Необязательные проверки

Red Hat Enterprise Linux must be installed

cloud-init is signed with Red Hat redhatrelease2 key

Red Hat Enterprise Linux 8 is installed

Red Hat CoreOS 4 is installed

RHBA-2019:2715: virt:rhel bug fix update (Important)
Обязательные проверки:

Module virt:rhel is enabled

libvirt is earlier than 0:4.5.0-24.3.module+el8.0.0+4084+cceb9f44

qemu-kvm is earlier than 15:2.12.0-65.module+el8.0.0+4084+cceb9f44.5

Module virt-devel:rhel is enabled

Необязательные проверки

Все остальные.

RHBA-2019:3384: ruby:2.5 bug fix and enhancement update (Moderate)
Обязательные проверки:

Module ruby:2.5 is enable

ruby is earlier than 0:2.5.5-105.module+el8.1.0+3656+f80bfa1d

rubygems is earlier than 0:2.7.6.2-105.module+el8.1.0+3656+f80bfa1d

Необязательные проверки

Все остальные.

Есть ли возможность упростить текущий формат, если да, то кратко описать свой вариант для описания уязвимости вместе с проверками.

Для упрощения анализа и восприятия файла видится следующий формат

1. Переформатирование xml в HTML для более удобной работы с файлом.
2. Оставить только необходимую информацию по уязвимости. Это описание, связанные CVE и CPE и критерии.
3. У критериев добавить ссылку на тест, случае необходимости дополнительной проверки теста.

После выполненного в предыдущей пунктах анализа, необходимо разработать приложение (скрипт) на языке Python, которое произведет разбор (парсинг) OVAL-файла (достаточно сделать только первые 3 и связанными с ними объекты) и преобразует его в ваш упрощенный формат.

Запуск скрипта:

py.exe .\oval-simpe.py

Скрипт парсит только первые три уязвимости.

Задание 2

Провести анализ документа CIS Microsoft Windows 11 Enterprise. Приоритизировать проверки и выбрать на ваш взгляд 10 самых критичных.

1. 1.1.4 (L1) Ensure 'Minimum password length' is set to '14 or more character(s)'
2. 1.2.2 (L1) Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0'
3. 2.3.1.1 (L1) Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts
4. 2.3.1.2 (L1) Ensure 'Accounts: Guest account status' is set to 'Disabled'
5. 18.10.42.6.1.1 (L1) Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled'
6. 18.10.42.6.1.2 (L1) Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is configured
7. 18.10.42.6.3.1 (L1) Ensure 'Prevent users and apps from accessing dangerous websites' is set to 'Enabled: Block'
8. 18.10.42.13.2 (L1) Ensure 'Scan removable drives' is set to 'Enabled'
9. 18.10.42.13.3 (L1) Ensure 'Turn on e-mail scanning' is set to 'Enabled'
10. 18.10.56.3.9.1 (L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled'

Приоритизация проверок была сделана с целью защитить устройство от несанкционированного доступа с учетом проверок, включённых по умолчанию, т.е. проверка считается более критичной, если не применяется по умолчанию.

Описать эти критерии своими словами: за что они отвечают и почему важны.

1. Задает минимальную длинно пароля.
   Исключать возможность брутфорс атаки с учетом п.2

2. Блокировка УЗ, если пароль был введен неверно больше 5 раз.
   Исключать возможность брутфорс.

3. Запрет на использование Microsoft аккаунтов.
   Исключать возможность получения доступа злоумышленником, который использует Microsoft аккаунт.

4. Запрет на использование гостевой УЗ.
   Исключает возможность неавторизованного доступа. Гостевая УЗ предполагает аутентификацию без пароля. Если гостевой доступ разрешен, злоумышленник сможет пользоваться доступами, которые разрешены хосту.

5. Включает конфигурацию снижения поверхности атаки.
   Снижает риск использования эксплойтов, и другого ВПО.

6. Включает дополнительные правила для конфигурации снижения поверхности атаки.
   Снижает риск атаки в части запуска подпроцессов другим приложением, запуска обфусцированного кода, получения доступа к LSASS и т.д.

7. Запрещает доступ к опасным сайтам.
   Снижает риск фишинговых атак.

8. Сканирование MS Defender подключаемых USB устройств.
   Снижает риск передачи ВПО на хост с использованием USB устройств.

9. Проверка электронной почты.
   Снижает риск фишинговых атак.

10. Запрос пароля при подключении удаленном подключении.
    Снижает риск несанкционированного удаленного подключения. Если данная проверка отключена, и если хост-клиент был скомпрометирован, то злоумышленник можется воспользоваться «ярлыком» для подключения, при этом не зная пароля для подключения хосту-серверу.

Для каждой из 10-ти выбранных проверок подобрать или составить команду(-ы) для выполнения в командной строке (cmd и/ или PowerShell), которая(-ые) будут помогать в проверки на соответствие стандарту.

1.1.4 (L1) Ensure 'Minimum password length' is set to '14 or more character(s)'

Get-Item -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "MinPasswordLength"

Get-ADFineGrainedPasswordPolicy -Filter “MinPasswordLength”

1.2.2 (L1) Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0'

Get-Item -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "LockoutBadCount"

Get-ADFineGrainedPasswordPolicy -Filter “LockoutBadCount”

2.3.1.1 (L1) Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts

Get-Item -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\System" -Name "NoConnectedUser"

2.3.1.2 (L1) Ensure 'Accounts: Guest account status' is set to 'Disabled'

Get-LocalUser -Name "Guest"

18.10.42.6.1.1 (L1) Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled'

Get-MpPreference | Select-Object AttackSurface*

18.10.42.6.1.2 (L1) Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is configured

Get-MpPreference | Select-Object AttackSurfaceReductionRules_Ids

18.10.42.6.3.1 (L1) Ensure 'Prevent users and apps from accessing dangerous websites' is set to 'Enabled: Block'

Get-MpPreference | Select-Object EnableNetworkProtection

18.10.42.13.2 (L1) Ensure 'Scan removable drives' is set to 'Enabled'

Get-MpPreference | Select-Object DisableRemovableDriveScanning

18.10.42.13.3 (L1) Ensure 'Turn on e-mail scanning' is set to 'Enabled'

Get-Item -Path “HKLM:\SOFTWARE\Policies\Microsoft\Windows Defender\Scan\DisableEmailScanning”

18.10.56.3.9.1 (L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled'

Get-Item -Path “HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:fPromptForPassword”

Приложение

Список объектов с описанием

RHBA-2019:1992: cloud-init bug fix and enhancement update (Moderate)
/etc/redhat-release: файл, который содержит версии ОС
cloud-init:пакет для настройки ВМ

RHBA-2019:2715: virt:rhel bug fix update (Important)
/etc/dnf/modules.d/virt.module: файл, содержит информацию, о том включен ли модуль virt. (1 или 0)
SLOF - используется для загрузки прошивки.
hivex - пакет для работы с файлами реестра Windows
hivex-devel –пакет для разработчиков, который содержит заголовочные файлы для hivex.
libguestfs : пакет для работы с образами дисков виртуальных машин.
libguestfs-bash-completion: пакет для расширения возможности Bash, добавляя поддержку автодополнения для команд libguestfs
libguestfs-benchmarking: пакет помогает понять производительность и эффективность библиотеки libguestfs
libguestfs-devel–пакет для разрабочиков, который содержит заголовочные файлы для libguestfs.
libguestfs-gfs2: пакет для работы с GFS2 внутри виртуальных машин
libguestfs-gobject - обертка для libguestfs, написанная с использованием GObject.
libguestfs-gobject-devel пакет для разрабочиков, который содержит заголовочные файлы libguestfs
libguestfs-inspect-icons - пакет, который специально добавляет поддержку проверки гостевых значков в образах
libguestfs-java: Java интерфейс к libguestfs.
libguestfs-java-devel: Заголовки для разработки Java.
libguestfs-javadoc: Документация Java API.
libguestfs-man-pages-ja/uk: Руководства на японском/украинском.
libguestfs-rescue: Инструменты аварийного восстановления.
libguestfs-rsync: Rsync для образов дисков.
libguestfs-tools: Основные инструменты libguestfs.
libguestfs-tools-c: C версии инструментов libguestfs.
libguestfs-winsupport: Поддержка Windows образов.
libguestfs-xfs: Поддержка XFS файловой системы.
libiscsi: Библиотека для iSCSI протокола.
libiscsi-devel: Заголовки для разработки iSCSI.
libiscsi-utils: Утилиты для управления iSCSI.
libssh2: Библиотека SSH протокола.
libvirt: Основная библиотека управления виртуализацией.
libvirt-admin: Утилиты администрирования libvirt.
libvirt-bash-completion: Автодополнение команд libvirt в bash.
libvirt-client: Клиентские инструменты (virsh).
libvirt-daemon: Демон libvirt, управляющий виртуальными машинами.
libvirt-daemon-config-network: Конфигурация сети по умолчанию.
libvirt-daemon-config-nwfilter: Конфигурация фильтров сети.
libvirt-daemon-driver-interface: Драйвер интерфейса для libvirt (управление сетевыми интерфейсами хоста).
libvirt-daemon-driver-network: Драйвер сети для libvirt (управление виртуальными сетями).
libvirt-daemon-driver-nodedev: Драйвер устройств узла (host) для libvirt (управление физическими устройствами).
libvirt-daemon-driver-nwfilter: Драйвер фильтров сети (nwfilter) для libvirt (управление правилами сетевой фильтрации).
libvirt-daemon-driver-qemu: Драйвер QEMU для libvirt (интеграция с QEMU для управления виртуальными машинами).

libvirt-daemon-driver-secret: Драйвер управления секретами (паролями, ключами) для libvirt.
libvirt-daemon-driver-storage: Драйвер хранения для libvirt (общая функциональность).
libvirt-daemon-driver-storage-core: Ядро драйвера хранения для libvirt (базовые функции).
libvirt-daemon-driver-storage-disk: Драйвер хранения для образов дисков (форматы qcow2, raw, и т.д.).
libvirt-daemon-driver-storage-gluster: Драйвер хранения GlusterFS для libvirt (использование GlusterFS для хранения образов).
libvirt-daemon-driver-storage-iscsi: Драйвер хранения iSCSI для libvirt (подключение к iSCSI таргетам).
libvirt-daemon-driver-storage-logical: Драйвер хранения LVM (Logical Volume Management) для libvirt.
libvirt-daemon-driver-storage-mpath: Драйвер хранения Multipath для libvirt (использование Multipath для отказоустойчивости и производительности).
libvirt-daemon-driver-storage-rbd: Драйвер хранения Ceph RBD для libvirt (использование Ceph для хранения образов).
libvirt-daemon-driver-storage-scsi: Драйвер хранения SCSI для libvirt (прямой доступ к SCSI устройствам).
libvirt-daemon-driver-storage-iscsi-direct: Прямой доступ к iSCSI для хранения данныхlibvirt-daemon-kvm: Конфигурация демона для KVM.
libvirt-dbus: Интеграция с D-Bus.
libvirt-devel: Заголовки для разработки под libvirt.
libvirt-docs: Документация libvirt.
libvirt-libs: Общие библиотеки libvirt.
libvirt-lock-sanlock: Поддержка блокировок sanlock.
libvirt-nss: Интеграция с Name Service Switch (NSS).
lua-guestfs: Lua биндинги для libguestfs.
nbdkit: NBD-сервер для дисковых образов.
nbdkit-bash-completion: Bash-автодополнение для nbdkit.
nbdkit-basic-plugins: Базовые плагины для nbdkit.
nbdkit-devel: Заголовки для разработки плагинов.
nbdkit-example-plugins: Примеры плагинов для nbdkit.
nbdkit-plugin-gzip: Плагин для работы с gzip-образами.
nbdkit-plugin-python-common: Общие файлы для Python плагинов.
nbdkit-plugin-python3: Плагин для написания на Python 3.
nbdkit-plugin-vddk: Плагин для доступа к VMDK образам.
nbdkit-plugin-xz: Плагин для работы с xz-образами.
netcf: Библиотека для конфигурации сети.
netcf-devel: Заголовки для разработки netcf.
netcf-libs: Общие библиотеки netcf.
perl-Sys-Guestfs: Perl интерфейс к libguestfs.
perl-Sys-Virt: Perl интерфейс к libvirt.
perl-hivex: Perl интерфейс к hivex.
python3-hivex: Python 3 интерфейс к hivex.
python3-libguestfs: Python 3 интерфейс к libguestfs.
python3-libvirt: Python 3 интерфейс к libvirt.
qemu-guest-agent: Агент для гостевой ОС.
qemu-img: Утилита для работы с образами QEMU.
qemu-kvm: Основной пакет QEMU с KVM.
qemu-kvm-block-*: Поддержка различных протоколов для хранения дисков.
qemu-kvm-block-curl: Поддержка доступа к дисковым образам QEMU по протоколам HTTP(S) (через libcurl).
qemu-kvm-block-gluster: Поддержка доступа к дисковым образам QEMU, хранящимся в распределенной файловой системе GlusterFS.

qemu-kvm-block-iscsi: Поддержка доступа к дисковым образам QEMU, расположенным на iSCSI таргетах.
qemu-kvm-block-rbd: Поддержка доступа к дисковым образам QEMU, хранящимся в Ceph RBD (Reliable Block Device).
qemu-kvm-block-ssh: Поддержка доступа к дисковым образам QEMU через SSH.
qemu-kvm-common: Общие файлы QEMU.
qemu-kvm-core: Ядро QEMU.
ruby-hivex: Ruby биндинги для hivex.
ruby-libguestfs: Ruby биндинги для libguestfs.
seabios: Открытый BIOS для виртуальных машин.
seabios-bin: Скомпилированный SeaBIOS.
seavgabios-bin: VGA BIOS для виртуальных машин.
sgabios: Альтернативный BIOS для виртуальной видеокарты.
sgabios-bin: Скомпилированный SGABIOS.
supermin: Создание минимальных гостевых образов.
supermin-devel: Заголовки для разработки supermin.
virt-dib: Инструмент создания образов дисков.
virt-p2v-maker: Создание образов физических машин.
virt-v2v: Конвертация виртуальных машин.
/etc/dnf/modules.d/virt-devel.module: файл, содержит информацию, о том включен ли модуль virt-devel (1 или 0)
libssh2-devel: Заголовочные файлы для разработки с libssh2.
libssh2-docs: Документация для libssh2.
ocaml-hivex: OCaml биндинги для hivex.
ocaml-hivex-devel: Заголовки для разработки OCaml с hivex.
ocaml-libguestfs: OCaml биндинги для libguestfs.
ocaml-libguestfs-devel: Заголовки для разработки OCaml с libguestfs.
qemu-kvm-tests: Тесты для QEMU/KVM.

RHBA-2019:3384: ruby:2.5 bug fix and enhancement update (Moderate)
/etc/dnf/modules.d/ruby.module: файл, содержит информацию, о том включен ли модуль ruby (1 или 0)
ruby: Интерпретатор языка Ruby.
ruby-devel: Заголовочные файлы для разработки на Ruby.
ruby-doc: Документация по Ruby.
ruby-irb: Интерактивная оболочка Ruby.
ruby-libs: Общие библиотеки Ruby.
rubygem-abrt: Интеграция с ABRT (Automatic Bug Reporting Tool) для отладки.
rubygem-abrt-doc: Документация к gem-пакету abrt.
rubygem-bigdecimal: Работа с числами произвольной точности (Decimal).
rubygem-bson: Работа с BSON (Binary JSON) форматом (обычно для MongoDB).
rubygem-bson-doc: Документация к gem-пакету bson.
rubygem-bundler: Управление зависимостями Ruby проектов (Gemfile).
rubygem-bundler-doc: Документация к gem-пакету bundler.
rubygem-did_you_mean: Помощь в исправлении опечаток в коде.
rubygem-io-console: Расширенные возможности для работы с консолью.
rubygem-json: Работа с JSON форматом (кодирование и декодирование).
rubygem-minitest: Фреймворк для юнит-тестирования.
rubygem-mongo: Драйвер для работы с базой данных MongoDB.
rubygem-mongo-doc: Документация к gem-пакету mongo.
rubygem-mysql2: Драйвер для работы с базой данных MySQL.
rubygem-mysql2-doc: Документация к gem-пакету mysql2.
rubygem-net-telnet: Работа с протоколом Telnet (для удаленного доступа).

rubygem-openssl: Работа с OpenSSL (шифрование, сертификаты).
rubygem-pg: Драйвер для работы с базой данных PostgreSQL.
rubygem-pg-doc: Документация к gem-пакету pg.
rubygem-power_assert: Расширенный инструмент для утверждений (assertions) в тестах.
rubygem-psych: Работа с YAML форматом (кодирование и декодирование).
rubygem-rake: Система сборки проектов (make-подобная).
rubygem-rdoc: Генерация документации из кода.
rubygem-test-unit: Еще один фреймворк для юнит-тестирования.
rubygem-xmlrpc: Работа с XML-RPC (Remote Procedure Call) протоколом.
rubygems: Менеджер пакетов для Ruby (установка, обновление gem-пакетов).
rubygems-devel: Инструменты для разработки собственных Ruby gem-пакетов.