Vulnerability Assessment

Teach Me Skills

Вопросы по предыдущим темам или ДЗ

Mini-quize по новой теме:

1. **Что такое vulnerability management?**
2. **Как вы думаете, достаточно использовать только сканер безопасности в компании? Если нет, то что ещё можно использовать?**
3. **Что такое Patch Management?**
4. **Что такое инвентаризация?**

Teach Me Skills

План занятия

1. Рассмотрим основные процессы в vulnerability management
2. Изучим сервисы для просмотра информации об уязвимостях
3. Изучим виды скоринга
4. Установим Сканер уязвимости

Vulnerability Management

Управление уязвимостями (Vulnerability Management, VM) – непрерывный, циклический процесс выявления и устранения уязвимостей в инфраструктуре организации и состоит из следующих этапов (Рисунок 1):

- Инвентаризация активов.
- Выявление уязвимостей.
- Выработка рекомендаций.
- Устранение уязвимостей.
- Контроль устранения уязвимостей.

Vulnerability Management

Риски

Риски при отсутствующем или неполном процессе инвентаризации активов:

- недостаток знаний о местоположении ИТ-активов;
- недостаток конфигурационных контролей для ИТ-активов;
- неэффективный патч-менеджмент;
- неэффективное управление уязвимостями;
- неполная операционная картина корпоративных активов;
- отсутствие конвергентного репозитория ИТ-активов.

Информация

бизнес-владелец (business owner) актива;

· риск-владелец (risk owner) актива;

· ответственный за актив со стороны ИТ (IT custodian);

· ответственный за актив со стороны ИБ (IT Security custodian);

· пользователь актива;

· выполняемая активом бизнес-роль/функция;

· выполняемая активом техническая роль/функция;

· зависимый от актива бизнес-процесс;

· критичность, стоимость, ценность актива;

· требования и уровень обеспечения информационной безопасности (целостность, конфиденциальность, доступность) информации, обрабатываемой активом;

· местоположение (адрес, помещение, номер стойки и т.д.);

· конфигурация (FQDN-имя, версия ОС, установленное ПО, VLAN, IP-адрес, MAC-адрес, объем ОЗУ и т.д.).

Vulnerability Management

Инвентаризация – это мероприятия, которые выполняются с определенной цикличностью, и направленные на получение актуальной информации об устройствах в сети организации.

Под актуальной информацией в данном определении понимается информация:
- об ip-адресе устройства в сети;
- о доменном имени устройства;
- об операционной системе устройства;
- о списке установленного программного обеспечения;
- о списке установленных обновлений безопасности (для windows компьютеров);
- о пользователях системы;
- об открытых TCP и UDP портах;
- о критичности данного устройства;
- о параметрах безопасности, используемых на данном устройстве.

Vulnerability Management

Также, в рамках инвентаризации IT-активов необходимо обратить внимание на то, какие устройства (коммутаторы, маршрутизаторы, межсетевые экраны, персональные компьютеры пользователей) используются в организации.
И уже на основе этих исходных данных выстраивать порядок сканирования оборудования.

Проводить инвентаризацию устройств можно с использованием открытого ПО (OpenVas, , Zabbix, Microsoft Windows Defender), коммерческих решений (R-Vision IRP, Security Vision IRP, MaxPatrol, PatrOwl).
Также возможно инвентаризировать устройства с помощью собственных, самописных скриптов.

Vulnerability Management

Цель процесса VM – повышение защищенности организации, путем закрытия актуальных уязвимостей.

Задачи процесса VM:
- актуализация информации об устройствах в сети организации;
- превентивное устранение уязвимостей;
- накопление собственной базы знаний с уязвимостями и рекомендациями;
- организация работы между отделами компании.

Vulnerability Management

Выявление уязвимостей

Уязвимость – это недостаток (слабость) программного (программно-технического) средства или системы в целом, который(ая) может быть использована злоумышленниками для реализации компьютерной атаки.
Ресерч – процесс исследования уязвимости.

CVE.
cve(Common Vulnerabilities and Exposures) общепринятые идентификаторы уязвимостей.

Идентификаторы имеют следующий вид:
CVE-2021-40444, CVE-2022-0847, CVE-2021-3156

Vulnerability Management

CVSS.

cvss (Common Vulnerability Scoring System) – открытый стандарт для оценки серьезности уязвимостей. Существует две версии CVSSv2 и CVSSv3. В настоящий момент вторая версия почти не используется.

CVSS делится на CVSS Vector и CVSS Score.

CVSS Vector – спецификация с основными метриками уязвимости, которая имеет вид:

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N,

где первые символы до двоеточия – метрика, вторые – значение данных символов:

− AV (Attack Vector), который может иметь значения
– N (Network), A (Adjacent Network), L (Local), P
(Physical).
− AC (Attack Complexity) – L (Low), H (High).
− RP (Privileges Required) – H (High), L (Low), N (None).
− UI (User Interaction) – N (None), R (Required).
− S (Scope) – U (Unchanged), C (Changed).
−C (Confidentiality Impact) – N (None), M (Medium), H
(High).
−I (Integrity Impact) – N (None), M (Medium), H (High).
−A (Availability Impact) – N (None), M (Medium), H (High).

Vulnerability Management

CVSS Score – численная величина, которая рассчитывается на основании метрик уязвимости, приведенных в векторе, и показывает критичность конкретной уязвимости.

CVSS Score градируется на 4 общепринятых типа:
- critical (критическая) от 9.0 до 10.0;
- high (высокая) от 7.0 до 8.9;
- medium (средняя) от 4.0 до 6.9;
- low (низкая) от 0.1 до 3.9.

Vulnerability Management

CPE.
cpe (Common Platform Enumeration) – структурированный формат представления информации о продуктах и версиях, для которых актуальна уязвимость.
CPE имеет следующую структуру:

cpe:<cpe_version>:<part>:<vendor>:<product>:<version>:<update>:<edition>:<language>, где:

−cpe_version – это версия cpe. На сегодняшний день последний версия 2.3.
−part может иметь 3 значения:
• a – application, то есть приложения;
• h – hardware, то есть железо;
• OS, то есть операционные системы.
−vendor – это производитель.
−product – это название системы, пакета или компонента.
−version – это версия системы, пакета или компонента.
−update – информация об обновлении продукта. Например, beta, update4, SP1.
−edition – более детальное уточнение о версии продукта.
− language – язык самой cpe, по умолчанию используется английский

Пример cpe для уязвимости CVE-2018-6179:
cpe:2.3:o:redhat:enterprise_linux_workstation:6.0
:*:*:*:*:*:*:*

Vulnerability Management

CWE.
cwe (Common Weakness Enumeration) – общий перечень дефектов (недостатков) безопасности.
Каждую уязвимость можно подвести под данный перечень.

У MITRE есть база знаний где каждому значению CWE присваиваются значения CAPEC.
CWE имеет вид:

CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor;
CWE-123 - Write-what-where Condition.

Vulnerability Management

CAPEC.
capec (Common Attack Pattern Enumeration and Classification) – перечень типовых видов атак с рекомендациями по их закрытию.

CAPEC имеет вид:
CAPEC-200 - Removal of filters: Input filters, output filters, data masking;
CAPEC-100 - Overflow Buffers.

EPSS.
epss (Exploit Prediction Scoring System) – система оценки вероятности использования уязвимости в реальных атаках.
epss score – значение в процентах.

Vulnerability Management

Обзор источников.
В интернете есть много сайтов, которые предоставляют информацию об уязвимостях, как в рамках платной подписки, так и бесплатно. Различия есть, но они не критичны.

Источники:
nvd.nist.gov (NVD)

opencve.io
Данный сайт парсит информацию с NVD и преподносит её в более гармоничном интерфейсе

otx.alienvault.com
На данном ресурсе множество исследователей делятся своими ресерчами по каждой уязвимости. На сайте данные ресерчи называют пульсами.

vulners.com
Данный ресурс, помимо основной информации, ещё ищет все упоминания об уязвимости в интернете

Vulnerability Management

Выработка рекомендаций.

Выработка рекомендаций – это мероприятия, направленные на разработку решающих правил для закрытия конкретной или группы уязвимостей.

На данном этапе выделяют две сущности mitigations (набор смягчающих мер) и официальное решение от производителя.
У обеих сущностей есть свои плюсы и минусы.

Mitigations (далее по тексту – митиги) не всегда позволяют полностью закрыть уязвимость, однако ограничивают злоумышленника в попытках проэксплуатировать уязвимость.

Официальное решение от производителя, в свою очередь, почти всегда подразумевает под собой обновление ПО, операционной системы, прошивки и т.д.

Vulnerability Management

Устранение уязвимостей.

Устранение уязвимостей – мероприятия, направленные на закрытие актуальных для организации уязвимостей.
Тут стоит понимать, что специалист, который вырабатывает рекомендации и специалист, который их применяет – это не один и тот же человек.
Выработкой рекомендаций занимается отдел оценки защищенности инфраструктуры, а применением – отдел администрирования сетевой инфраструктуры.

На данном этапе происходит интеграция процесса Patch Management в процесс Vulnerability Management.

Vulnerability Management

Контроль устранения уязвимостей.

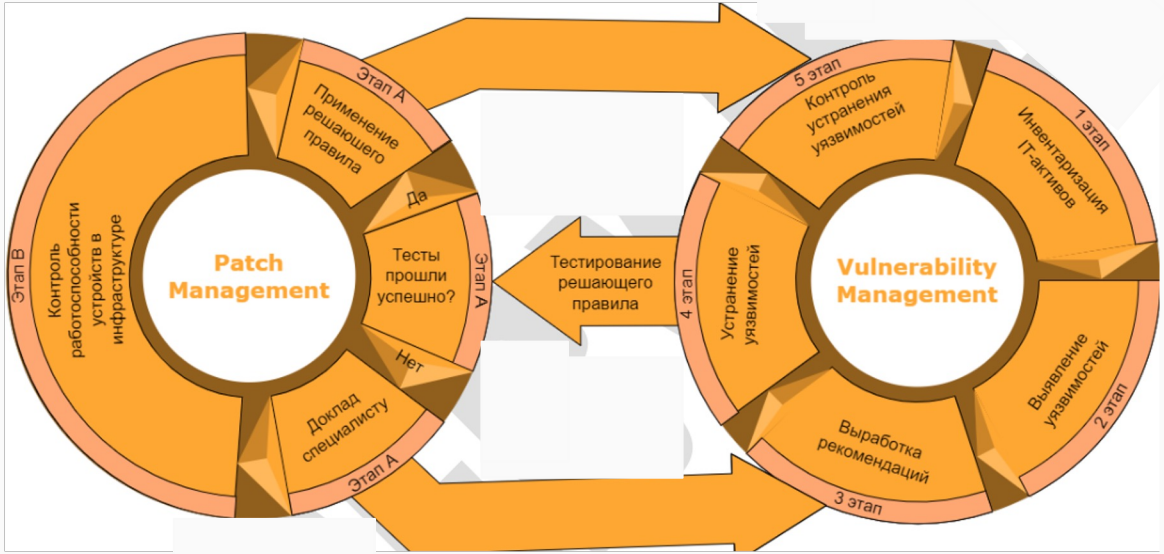
Контроль устранения уязвимостей – мероприятия, направленные на проверку применения решающих правил на устройства организации.

На этом этапе специалисту отдела оценки защищенности стоит следить за тем, как специалисты отдела администрирования сетевой инфраструктуры закрывают уязвимости в соответствии с выработанными рекомендациями.

Данный этап является логическим завершением одной итерации процесса Vulnerability Management, после которого опять начинается инвентаризация IT-активов организации.

Vulnerability Management

Процесс Patch Management – это процесс управления обновлениями программного обеспечения, операционных систем, прошивок и т.д.



Установка Greenbone и работа со сканером

Teach
Me
Skills

Спасибо за внимание!