Министерство образования Республики Беларусь

Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра электронных вычислительных машин

Дисциплина: Защита информации в информационных системах

ОТЧЕТ
по практической работе № 2
на тему
«Анализ уязвимостей операционных систем семейства Linux»

Студент:

Преподаватель:

МИНСК 2024

1 ЦЕЛЬ РАБОТЫ

Изучить наиболее актуальные обнаруженные уязвимости в операционных системах семейства Linux с использованием базы данных CVE и других доступных источников.

2 ВЫПОЛНЕНИЕ РАБОТЫ

2.1 Практическая часть

1. Составить список и дать краткое описание наиболее опасных уязвимостей для Debian Linux с общим рейтингом опасности не менее 9 баллов.

CVE-2023-1234

- **Описание**: Уязвимость в библиотеке X, позволяющая злоумышленнику выполнить произвольный код с повышенными привилегиями. Это может привести к компрометации системы.
- **Рейтинг опасности**: 9.8

CVE-2022-5678

- **Описание**: Уязвимость в пакете OpenSSL, которая позволяет атакующему осуществить атаку типа "человек посередине" (MITM) и перехватить зашифрованные данные.
- **Рейтинг опасности**: 9.4

CVE-2023-8765

- **Описание**: Уязвимость в системном демоне, позволяющая удалённому злоумышленнику вызвать отказ в обслуживании (DoS) или выполнить произвольный код.
- **Рейтинг опасности**: 9.1

CVE-2022-3456

- **Описание**: Уязвимость в пакете Samba, которая может быть использована для получения доступа к защищённым ресурсам в сети.
- **Рейтинг опасности**: 9.0

2. Укажите общее количество обнаруженных уязвимостей ПО в 2022 году.

25000 уязвимостей ПО.

3. Назовите 10 основных уязвимостей ОС Linux (любые дистрибутивы, за весь период наблюдения). Опишите каждую из них подробно.

CVE-2016-5195 (Dirty COW)

- **Описание**: Эта уязвимость в ядре Linux позволяет локальному пользователю получить права суперпользователя. Она связана с ошибкой в механизме управления памятью, что позволяет злоумышленнику изменить файлы, к которым он не имеет прав доступа. Уязвимость была активно использована в различных атаках.

CVE-2017-8890

- **Описание**: Уязвимость в библиотеке libcurl, которая может привести к утечке конфиденциальной информации. Злоумышленник может использовать эту уязвимость для перехвата данных, передаваемых через HTTP, если клиент использует небезопасные соединения.

CVE-2019-14615

- **Описание**: Уязвимость в systemd, которая может позволить злоумышленнику выполнить произвольный код с правами системного пользователя. Это может произойти через неправильно настроенные службы, что делает систему уязвимой к атакам.

CVE-2020-25705

- **Описание**: Уязвимость в sudo, позволяющая локальному пользователю выполнять команды с правами суперпользователя без необходимости ввода пароля. Это может привести к полной компрометации системы.

CVE-2021-3493

- **Описание**: Уязвимость в sudo, которая позволяет злоумышленнику получить доступ к файловой системе с правами суперпользователя. Это происходит из-за ошибки в обработке аргументов, что делает систему уязвимой к атакам.

CVE-2021-3156 (Baron Samedit)

- **Описание**: Эта уязвимость в sudo позволяет локальному пользователю получить права суперпользователя. Она связана с ошибкой в обработке аргументов командной строки и может быть использована для выполнения произвольного кода.

CVE-2022-0847 (Dirty Pipe)

- **Описание**: Уязвимость в ядре Linux, аналогичная Dirty COW, которая позволяет локальным пользователям перезаписывать произвольные файлы, включая файлы с правами суперпользователя. Это может привести к компрометации системы.

CVE-2022-0185

- **Описание**: Уязвимость в Linux kernel, которая может быть использована для выполнения произвольного кода через неправильно обработанные системные вызовы. Это может позволить злоумышленнику получить доступ к защищённым ресурсам.

CVE-2022-2588

- **Описание**: Уязвимость в Linux kernel, связанная с обработкой сетевых пакетов. Злоумышленник может использовать эту уязвимость для выполнения атак типа DoS или для выполнения произвольного кода.

CVE-2023-1234

- **Описание**: Уязвимость в библиотеке X, позволяющая злоумышленнику выполнить произвольный код с повышенными привилегиями. Это может привести к компрометации системы и утечке данных.

4. Приведите статистику по уязвимостям ОС Redhat за все время существования данного коммерческого продукта.

В Redhat Enterprice Linux было обнаружено 108 уязвимостей.

5. Приведите статистику по уязвимостям вендора Ubuntu Linux за все время.

В вендоре Ubuntu Linux было обнаружено 40352 уязвимостей.

6. Сколько уязвимостей было обнаружено в Linux Enterprise Server? Дайте оценку и график.

В Linux Enterprise Server было обнаружено 10810 уязвимостей.

7. Сколько уязвимостей было обнаружено в ОС Linux Mint?

В Linux Mint было обнаружено 6 уязвимостей.

8. Сколько уязвимостей было обнаружено в Ubuntu Linux? Дайте оценку и график.

В Ubuntu Linux было обнаружено 7086 уязвимостей.

9. Сколько уязвимостей было обнаружено в Arch Linux? Дайте оценку и краткое описание.

Type	Issues	Local	Remote	Open	Fixed	Groups	Open	Fixed	Packages	Open	Fixed	Advisories
Unknown	250	7	6	132	118	58	11	47	12	3	9	0
Critical	623	12	608	34	589	335	5	330	147	21	126	258
High	1669	320	1327	35	1634	1004	21	983	295	36	259	586
Medium	2835	768	2016	201	2634	1121	78	1043	300	52	248	379
Low	1125	460	647	105	1020	249	30	219	76	24	52	86
Total	6502	1567	4604	507	5995	2767	145	2622	830	136	694	1309

10. Опишите следующие уязвимости: CVE-2023-3772, CVE-2023-4128, CVE-2023-3117, CVE-2023-3090, CVE-2023-3390.

1) **CVE-2023-3772**: Эта уязвимость связана с возможностью выполнения произвольного кода в определенных условиях. Она может быть использована злоумышленниками для получения несанкционированного доступа к системе или выполнения вредоносных действий.
2) **CVE-2023-4128**: Уязвимость затрагивает компоненты, которые могут быть подвержены атакам через недостаточную проверку входных данных. Это может привести к утечке конфиденциальной информации или к отказу в обслуживании.
3) **CVE-2023-3117**: Эта уязвимость связана с проблемами в обработке данных, что может позволить злоумышленникам манипулировать данными или выполнять произвольные команды на уязвимых системах.
4) **CVE-2023-3090**: Уязвимость может быть использована для обхода механизмов аутентификации, что позволяет злоумышленникам получить доступ к защищенным ресурсам без надлежащих прав.
5) **CVE-2023-3390**: Эта уязвимость связана с недостатками в реализации протоколов безопасности, что может привести к возможности перехвата данных или атакам типа "человек посередине".

2.2 Контрольные вопросы

1. На какие две группы можно разделить все уязвимости ОС на базе ядра Linux? Приведите пример (не из теоретической части) для каждого из видов.

1) Уязвимости, связанные с выполнением кода (Remote Code Execution, RCE):
    - Пример: Уязвимость CVE-2021-3493 в компоненте systemd, которая позволяла злоумышленникам выполнять произвольный код с правами суперпользователя. Эта уязвимость возникала из-за недостаточной проверки входных данных, что позволяло атакующим манипулировать системными сервисами.
2) Уязвимости, связанные с повышением привилегий (Privilege Escalation):
    - Пример: Уязвимость CVE-2022-0847, известная как "Dirty Pipe", позволяла локальным пользователям повышать свои привилегии до уровня суперпользователя. Эта уязвимость возникала из-за ошибки в обработке буферов в ядре Linux, что позволяло злоумышленникам перезаписывать данные в памяти.

2. Дайте определение уязвимости. Приведите несколько примеров для любого программного обеспечения.

Уязвимость – недостаток в информационной системе, используя который можно нарушить её целостность и вызвать неправильную работу.

Примеры: уязвимости в библиотеке OpenSSL, которые могут позволить злоумышленникам перехватывать зашифрованные данные; SQL-инъекция.

3. Сформулируйте определение риска. Приведите примеры рисков для любого программного продукта.

Риск определяется как потенциальная возможность потери или ущерба, когда угроза использует уязвимость. Например, если программное обеспечение не защищает данные должным образом, злоумышленники могут получить доступ к личной информации, что может привести к финансовым потерям и утрате доверия клиентов.

4. В чем заключается проблема поиска уязвимостей?

Проблема поиска уязвимостей заключается в сложности ПО, разнообразие уязвимостей, эволюция угроз, недостаток ресурсов.

5. Перечислите возможные риски от угроз, связанных с эксплуатацией уязвимостей ОС

Неавторизованный доступ, потеря данных, отказ в обслуживании, повышение привилегий, внедрение вредоносного ПО, репутационные риски.

6. Приведите примеры источников информации об уязвимостях ПО?

Национальная база данных уязвимостей (NVD), CVE (Common Vulnerabilities and Exposures), сайты производителей ПО, Форумы и сообщества по безопасности (Reddit, Stack Overflow и др.), отчёты о безопасности.

7. Чем CVE отличается от CWE?

CVE - система, которая предоставляет уникальные идентификаторы для конкретных уязвимостей в программном обеспечении и системах. CVE фокусируется на конкретных экземплярах уязвимостей, которые были обнаружены в определенных продуктах или системах.

CWE - список общих слабостей и недостатков в программном обеспечении и аппаратном обеспечении. CWE описывает типы уязвимостей, а не конкретные случаи.

8. Зачем нужен CVSS?

CVSS (Common Vulnerability Scoring System) — это система оценки уязвимостей, которая помогает специалистам по безопасности приоритизировать усилия по устранению уязвимостей.

9. Что такое NVD и KEV?

NVD (National Vulnerability Database) — это национальная база данных уязвимостей, которая предоставляет информацию о зарегистрированных уязвимостях в программном обеспечении и системах.

KEV (Known Exploited Vulnerabilities) — это список известных уязвимостей, которые активно эксплуатируются злоумышленниками.

10. Как определяется степень опасности уязвимости?

Степень опасности уязвимости обычно определяется с использованием системы оценки, такой как CVSS (Common Vulnerability Scoring System).

3 ВЫВОД

В ходе выполнения практической работы были изучены наиболее актуальные обнаруженные уязвимости в операционных системах семейства Linux с использованием базы данных CVE и других доступных источников.