Презентации по лабораторной работе 1-D

Кибербезопасность предприятия. 1-D

Лушин А.А, Лобанова П.И

18 февраля 2005, 12 декабря 2004

Российский университет дружбы народов, Москва, Россия

Факультет Физико-математических и естественных наук

Информация

Докладчик

- Лушин Артём Андреевич и Лобанова Полина Иннокентьевна
- Бакалавр направления компьютерные и информационные науки
- Кафедра теории вероятности и кибербезопасности
- Российский университет дружбы народов

Вводная часть

Цели и задачи

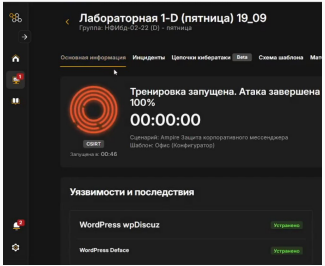
Основная цель работы - подготовить рабочее пространство и инструментарии для работы с языком программирования Julia, на простейших примерах познакомиться с основным синтаксисом Julia.

Ход работы

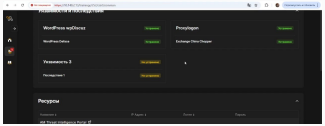
Легенда

Конкуренты решили скомпрометировать деятельность Компании и нашли для этого исполнителя. Злоумышленник находит в Интернете сайт соответствующего предприятия и решает провести атаку на него с целью получения доступа к внутренним ресурсам. Проэксплуатировав обнаруженную на сайте уязвимость, нарушитель стремится захватить управление другими ресурсами защищаемой сети, в том числе, пытается закрепиться на почтовом сервере и продолжить атаку. Главная задача злоумышленника - получение доступа к переписке сотрудников компании, раскрытие учётных данных пользователей, зарегистрированных в приложении корпоративного мессенджера, с целью использования их для нанесения ущерба репутации конкурирующей Компании. Квалификация нарушителя высокая. Он умеет использовать инструментарий для проведения атак, а также знает техники постэксплуатации.

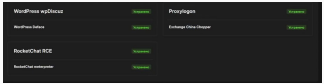
В журнале событий увидели подозрительные события. Используя CVE проверили событие и поняли, что это атака WordPress. Создали инцидент, указали название события и описание, указали время атаки, источник и поражённое устройство, а также прописали рекомендации. Для устранения уязвимости на атакуемом устройстве необходимо было отключить плагин WpDiscuz, а также сформировали резервную копию от 15 сентября 2023 года, чтобы удалить полезную нагрузку. Для устранения уязвимости с атакуемого устройства необходимо было разорвать соединение с Kali. После этого уязвимость и последствие устранены.



В журнале событий увидели следующее подозрительное событие. Создали инцидент, указали время начала атаки, источник и адрес атаки. Написали рекомендации как устранить уязвимость и последствия. Для устранения уязвимости необходимо было с атакуемого устройства ограничить доступ к директориями. Для устранения последствия необходимо было закрыть meterpretter-сессию. Затем удалить файл, который Kali смог подгрузить. После этого последствия и уязвимость будет устранены.



Обнаружили последнюю уязвимость. Создали инцидент, указал все данные. Для устранения инцидента необходимо было зайти на сайт под пользователем администратора. Для этого нужно было сменить пароль от “администратор”, использовав одноразовый код или код восстановления. После смены пароля на сайте включили двухэтапную аутентификацию и обязательное подтверждение почты. Также новых пользователей должен был подключать именно администратор. Для устранения последствия отключили Kali от атакуемого устройства. После этого последствия и уязвимость устранились.



Результаты

Вывод

Мы устранили все последствия и уязвимости после атаки на мессенджер, тем самым обеспечили защиту корпоративного мессенджера.