Анализ защищенности

Что это и зачем нужны анализы

LM SECURITY

ООО “ЛианМедиа” (LMSecurity)

Основная деятельность:

- Тестирвоание на проникновение
- Аудит ИБ
- Разработка ОРД
- Интерграция СЗИ

- Наш телеграм канал - t.me/lmsecurity

LM SECURITY

Что будет в докладе

- Что такое анализ защищенности
- Как составляется реестр недопустимых событий
- Этапы проведения анализа защищенности:
- - Составление реестра недопустимых событий
- - Разведка периметра
- - Сбор и тестирование эксплойтов
- - Отчет
- Как мы анализируем крупную инфраструктуру (ЦОД)

LM SECURITY

Анализ защищенности

Из чего состоит:

- Составление реестра недопустимых событий
- Инструментальный анализ уязвимостей
- Ручной анализ уязвимостей
- Анализ СЗИ
- Построение векторов атак
- Поиск следов компрометации
- Реализация недопустимых событий
- Проводится как на внешнем так и на внутреннем периметре

LM SECURITY

Отличие анализа от пентеста

- Комплексный подход
- Большой объем работ
- Более дорогостоящее мероприятие (раз раз и
- Обработка большого объема данных (логи со сканеров, куча узлов, поиск критичных узлов, анализ трафика, анализ сетевой инфраструктуры и т.п.)

LM SECURITY

Зачем нужен анализ защищенности

- Замер текущего состояния
- Определение вектора развития ИБ
- Планирование развития ИБ
- Поиск и исправление недочетов в ИТ инфраструктуре (человеческий фактор никто не отменял)
- Снятие розовых очков

LM SECURITY

Как это бывает на практике

LM SECURITY

Мы написали Модель угроз - все норм

LM SECURITY

Мы купили СЗИ - теперь все безопасно

LM SECURITY

Мы поставили СЗИ - теперь то норм?

LM SECURITY

Так тоже бывает

LM SECURITY

Уровни зрелости ИБ процессов

LM SECURITY

Реестр недопустимых событий

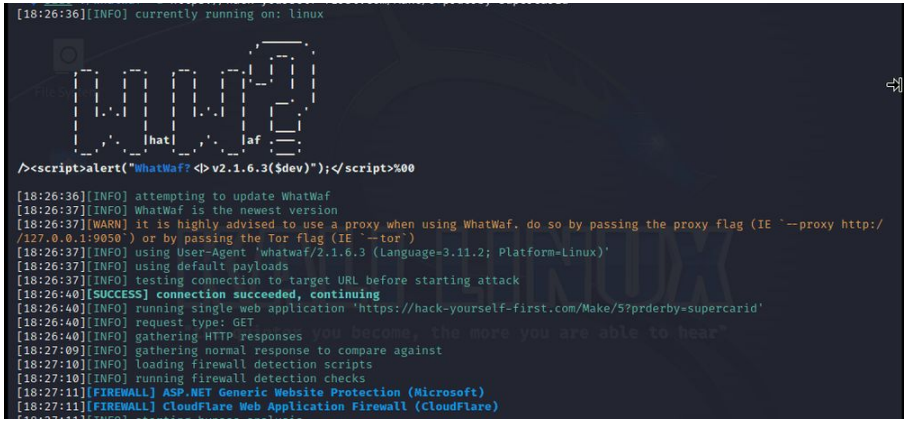
Недопустимое событие — событие, возникшее во время кибератаки, которое может привести к финансовым, репутационным, стратегическим потерям

https://rezbez.ru/article/opredelenie-nedopustimyh-sobytij

LM SECURITY

Разведка

- Поиск периметра
- Пассивнй Анализ Периметра
- Анализ СЗИ
- Подготовка Ресурсов
- Активный Анализ периметра



LM SECURITY

Результат разведки

ID	IP	PORT	PROTOCOL	SERVICE_NAME	DOMAIN	VENDOR	TYPE	PRODUCT	VERSION
1	x.x.x.x	22	tcp	ssh			Software	OpenSSH	7.5
2	x.x.x.x	23	tcp	telnet			Software	OpenSSH	7.5
3	x.x.x.x	80	tcp	http			Software	CherryPy wsgiserver	
4	x.x.x.x	4369	tcp	epmd			Software	Erlang Port Mapper Daemon	
5	x.x.x.x	9002	tcp	dynamid			Software	OpenSSH	7.5
6	x.x.x.x	22	tcp	ssh			Software	OpenSSH	7.3p1.RL Allied Telesis
7	x.x.x.x	22	tcp	ssh			Software	OpenSSH	8.0
8	x.x.x.x	80	tcp	http			Software	Apache httpd	
9	x.x.x.x	443	tcp	http			Software	Apache httpd	
10	x.x.x.x	22	tcp	ssh			Software	OpenSSH	8.0

LM SECURITY

Тестирование уязвимостей

Базы данных уязвимостей

- БДУ ФСТЭК
- CVE
- NVD NIST
- CWE - Common Weakness Enumeration
- ....

LM SECURITY

Белые списки СЗИ

Зачем добавлять в белые списки:

- Ограничение по времени
- Ограничение в ресурсах
- Абузы (НЦКИ)
- Байпасс СЗИ

Мы не будем выключать СЗИ - вы же Хакиры вот и ломайте

LM SECURITY

Отчеты

Виды отчетов:

- Аналитический отчет по Минцифрам
- Технический отчет
- Отчет для руководителей
- Отчет о проделанной работе

По результатам проводимых работ в период с <Скрыто> по <Скрыто> специалисты «ЛианМедиа» (далее - Исполнитель) провели работы по верификации недопустимых событий (далее – НС) в отношении <Скрыто> (далее - Заказчик).

1. **Экспертная оценка уровня защищенности периметра: крайне низкий, низкий, средний, высокий** (где крайне низкий – наличие общеизвестной уязвимости с возможностью удаленного выполнения кода (RCE))

Средний - Внешний периметр: были обнаружены некорректные конфигурации и уязвимости, которые раскрывают информацию о об исследуемом узле сети или пользователях ресурсов, реализованы атаки типа «Межсайтовый скриптинг» и открытое перенаправление. **Внутренний периметр:** было проведено сканирование узлов сети, идентифицированы открытые порты и используемое ПО, осуществлены сетевые атаки, в результате которых были получены учетные данные, обнаружены общеизвестные уязвимости, в результате эксплуатации которых удалось скомпрометировать домены <Скрыто>» и <Скрыто>, был получен доступ к конфиденциальной информации и скомпрометированы службы и сервера MSSQL и 1С. **Социотехническое тестирование:** было реализовано 5 разных векторов атак, направленных на 4 целевые группы, по результатам проведенных проверок были зафиксированы единичные случаи открытия писем, переходов по ссылкам.

2. **Общее количество исследуемых НС, количество реализованных НС**

НС – 27; Реализованных НС - 14.

3. **Реестр реализованных НС (подтверждение, длительность, квалификация)**

1. Получение неправомерного доступа к ИС 1С – получен неправомерный доступ до части ИС 1С, 1 день, средняя квалификация.
2. Компрометация ИС 1С – скомпрометирована часть серверов 1С, 1 день, средняя квалификация.
3. Получение неправомерного доступа к внутреннему порталу – получен доступ к внутреннем порталу, 1 день, средняя квалификация.
4. Обход антивирусной защиты – реализован запуск вредоносного файла в обход антивирусной защиты, 1 день, средняя квалификация.
5. Реализация сетевых атака – реализованы сетевые атаки с перехватом пакетов, 1 день, средняя квалификация.
6. Реализация атаки типа «Подбор паролей» – реализована атака «подбор паролей», получен доступ к сервисам, 1 день, низкая квалификация.
7. Утечка конфиденциальной информации – получен доступ к базам данных, содержащих конфиденциальные данные, 1 день, средняя квалификация.
8. Компрометация службы централизованного управления учетными записями – получен доступ с правами администратора к доменам AD, 1 день, средняя квалификация.
9. Выход за границы начального сегмента сети – был получен доступ к узлам сети, находящимся за пределами начального сегмента, 1 день, низкая квалификация.
10. Получение неправомерного доступа к сервисам для взаимодействия между пользователями – получены пароли пользователей от службы электронной почты, 1 день, средняя квалификация.
11. Компрометация сервисов для взаимодействия между пользователями – скомпрометирована сервер электронной почты с использованием прав доменного администратора, 1 день, средняя квалификация.
12. Прослушивание разговоров по IP-телефонии – был перехвачен разговор посредством IP-телефонии, сделана запись звонков, 1 день, средняя квалификация.

4. **Перечень ограничений, наложенных в рамках реализации работ**

LM SECURITY

Самый большой отчет

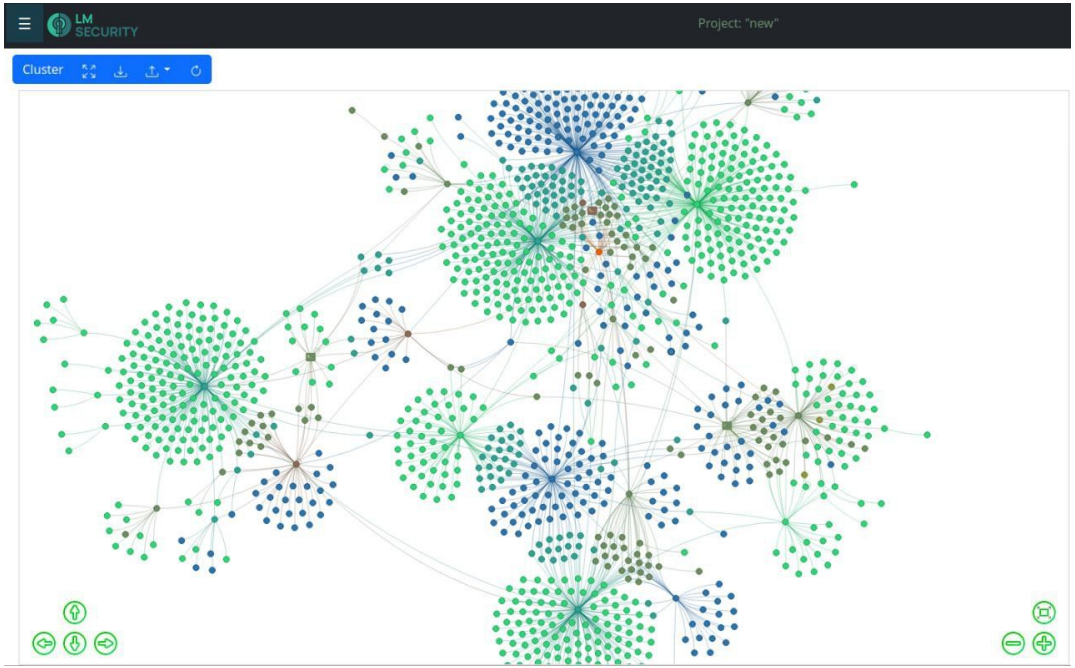
LM SECURITY

Самый большой отчет

Вывод: Важен результат - а не процесс

LM SECURITY

Как тестировать ЦОД



https://github.com/lmsecure/setezor

LM SECURITY

Спасибо за внимание

- Наш телеграм канал - https://t.me/lmsecurity
- Связь со мной - https://t.me/ng_coba

LM SECURITY