METASCAN

ЧТО НЕ ТАК С КОНТРОЛЕМ ЗАЩИЩЕННОСТИ ВНЕШНЕГО ПЕРИМЕТРА

Решаем проблемы защиты периметра для Enterprise сегмента

СБЕР

Альфа Банк

Ростелеком

Селигдар
ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО

МКБ

ПОЧТА РОССИИ

ЦИФРОВОЙ ЭКОНОМИКИ

СПББИРЖА

NOVABEV GROUP

FESCO

Rarible

Идеальное Состояние ИБ

Таблица 1. Уровень зрелости процессов ИБ по методологии ISF

Уровень	Обозначение уровня зрелости	Описание
0	Несуществующий	Процесс ИБ не выполняется
1	Примитивный	Процесс ИБ выполняется на нерегулярной основе
2	Начальный	Процесс ИБ выполняется на регулярной основе и поддерживается на уровне планирования (включая привлечение заинтересованных сторон и использование соответствующих стандартов и руководств)
3	Формализованный	Процесс ИБ выполняется, планируется, и имеется достаточный объем организационных ресурсов для поддержки и управления
4	Управляемый	Процесс ИБ выполняется, планируется, управляется и контролируется
5	Оптимизированный	Процесс ИБ выполняется, планируется, управляется, измеряется при помощи количественных показателей (метрик) и постоянно совершенствуется

Таблица 2. Методология уровня зрелости

№ домена	Наименование процесса ИБ	Направление деятельности
1	Стратегия ИБ	Построение системы менеджмента информационной безопасности
2	Осознание руководством важности ИБ	
3	Управление рисками ИБ	
4	Управление комплаенсом	
5	Аудит ИБ	
6	Политика ИБ	
7	Управление доступом	Построение технической архитектуры информационной безопасности
8	Управление уязвимостями	
9	Управление ЖЦ АС	
10	Управление информационными активами	
11	Управление изменениями	
12	Архитектура ИБ	
13	Управление каналами связи	Управление каналами связи и внешними каналами взаимодействия
14	Управление внешним взаимодействием	
15	Разведка угроз ИБ	Функционирование процессов информационной безопасности при воздействии дестабилизирующих факторов
16	Управление событиями ИБ	
17	Управление инцидентами ИБ	
18	Антикризисное управление	
19	Обеспечение непрерывности бизнеса	
20	Повышение осведомленности персонала	Обеспечение информационной безопасности при работе с персоналом
21	Безопасность персонала	

Идеальное Состояние периметра

Переодичность проверки каждого хоста на внешнем периметре < 24 часов

На периметре отсутсвуют уязвимости критичностью выше X

Назначение каждого порта на внешнем периметре известно ИБ

Что не так?

Чем больше ваш периметр, тем сложнее его защищать

РЕДКИЕ СКАНИРОВАНИЯ

Сканирующее облако

СКАНЕР УЗЯВИМОСТЕЙ ≠ ПРОЦЕСС

Еженедельные встречи с отделом ИБ

ЛОЖНЫЕ СРАБАТЫВАНИЯ

PoC-based подход

Набор инструментов

Amass	Nmap
Cameradar	Patator
Dirsearch	Wafw00f
Nuclei	ZAP

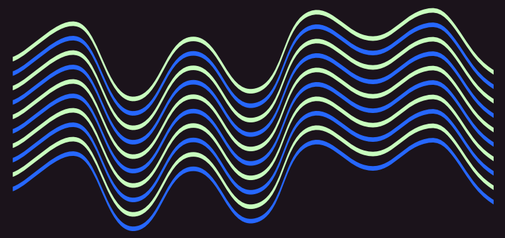
github.com/vulnspace

hub.docker.com/u/metascan

Что плохо работает в сканерах

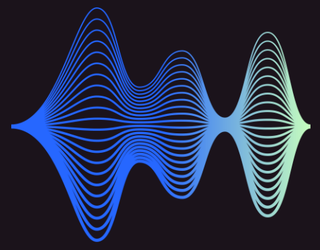
- unknown протоколы и самописные протоколы
- Работа с DOM
- Логические баги
- Анализ client-side библиотек
- Out-of-bounds иньекции

Enterprise и его ДЗО



Влияние метрик ИБ на KPI бизнеса

ИБ выполняет часть ИТ-функций (DNS, FW)



2,5 млн целей в день максимальная нагрузка

Сервисный подход к ИБ

METASCAN
by vulnspace

- Главная
- Мои сайты
- Профили сканера
- Инфраструктура
- Галерея
- Разведка
- Граф
- Расписание
- История проверок
- Мой аккаунт

	1/10	44.228.248.206		
	1/10	44.228.248.196		
	1/10	44.228.248.208		

Domains

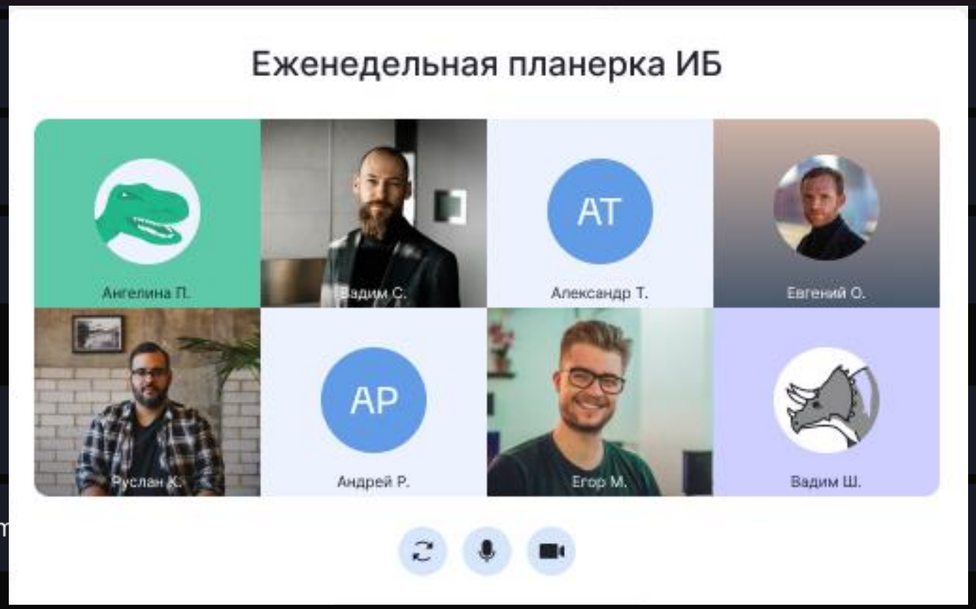
	9.8/10	nmap.org		
	10/10	pgeu01vuln01.public.m		
		.org	45.33.49.119	9 августа 2023 г.
		p.org	45.33.32.156	28 сентября 2023 г.
	9.8/10	svn.nmap.org	45.33.49.119	28 сентября 2023 г.
	9.8/10	echo.nmap.org	45.33.32.156	28 сентября 2023 г.

Поддержка Metascan

Здравствуйте, Вадим, направляем рекомендации по устранению уязвимостей и краткое резюме созвона.

Краткий отчет Рекомендации

10:41



Спасибо!

david.ordyan@metascan.ru

+7 495 152 1337

career.habr.com/companies/metascan