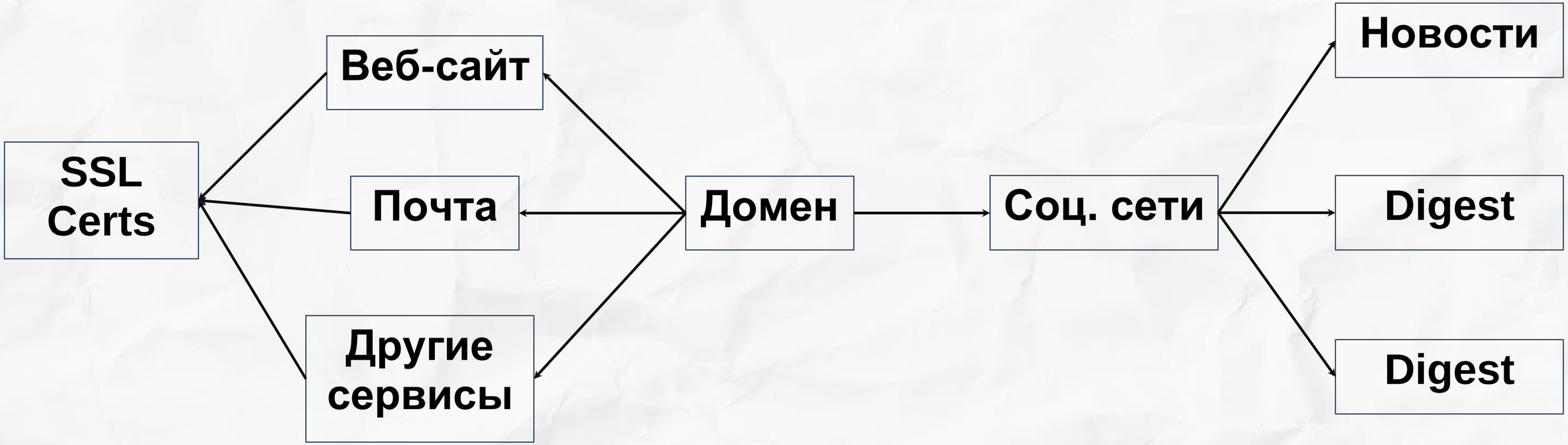
Конкурентная разведка: опыт использования в пентесте

ОБО МНЕ

- Работаю в LMSecurity
- Программирую на Python
- Изучаю OSINT 1 год

Типичная схема роста бизнеса в глобальной сети

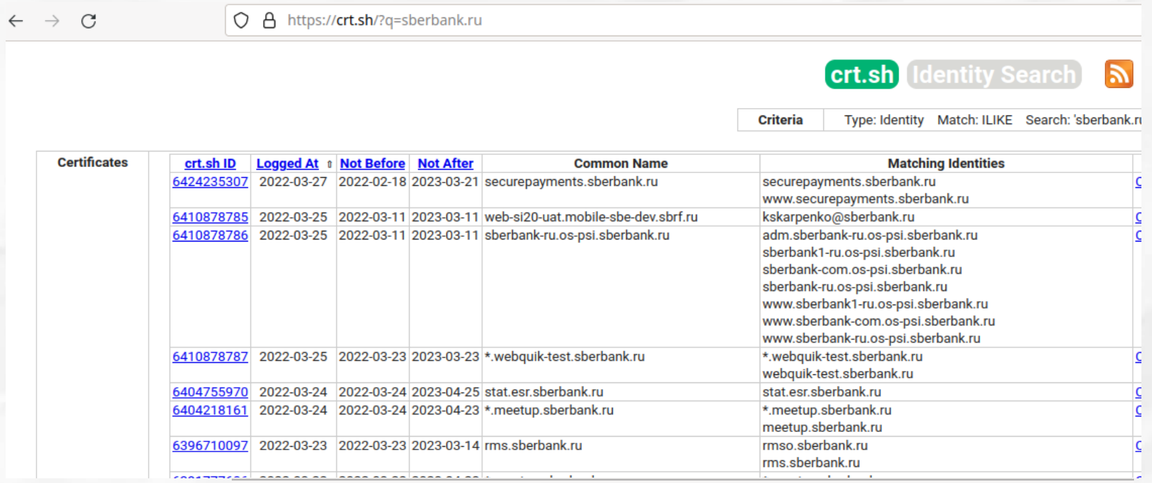


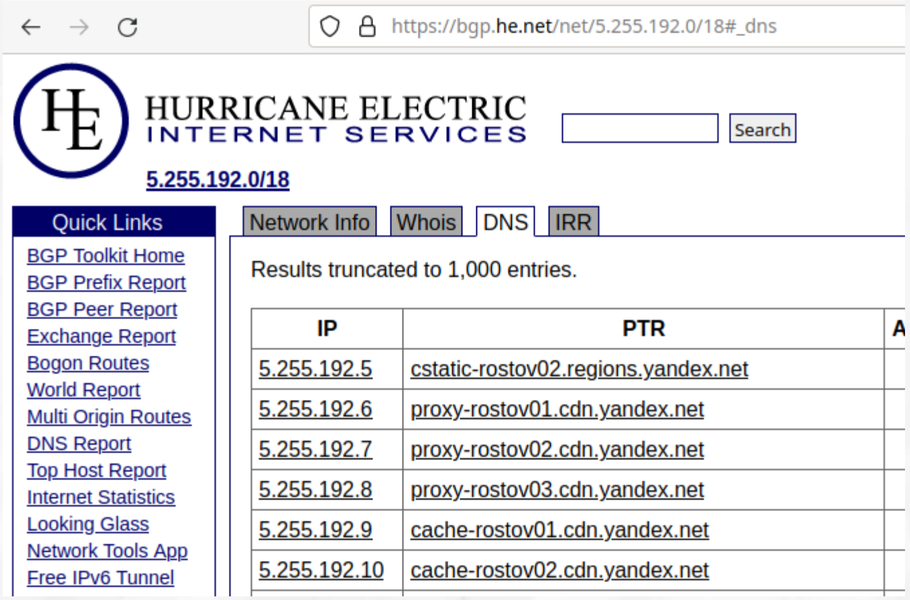
Домены, субдомены, IP адреса и SSL сертификаты

who.is

WHOIS Search, Domain Name, Website, and IP Tools

- Информация о регистрации домена
- Связь домена и IP адреса
- Просмотр DNS записей
- Использование поисковых систем
- Агрегаторы информации о SSL сертификатах





- Сканирование IP адресов
- Определение ПО и его версий
- Сканирование Веб-приложений
- Определение ПО, его версии и используемых плагинов
- Поиск открытых директорий

WPScan

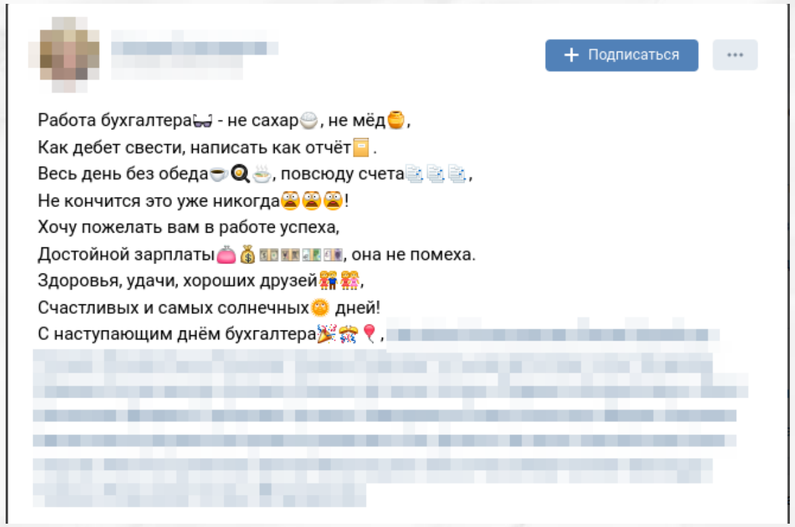
Социальные сети

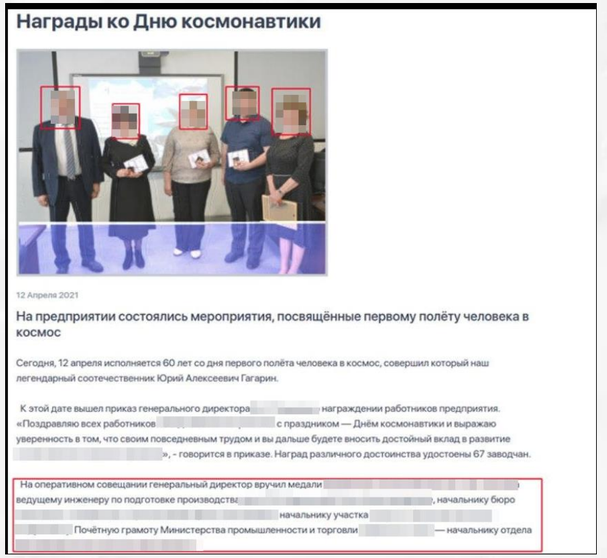
Профиль компании

- Фото / Видео
- Участники
- Посты
- Новости
- Газета
- Digest

Личные профили сотрудников

- Посты
- Фото (с рабочего места)





Публикуемые документы

Инструменты:

- Foca
- Metagoofill

Информация:

- Имена пользователей
- Даты создания и изменения
- Используемое ПО

Метод грубой силы

Дано:

- куча личной информации о сотрудниках

Нужно:

- составить список паролей для брута

Источники:

- Сервисы утечек
- Словари паролей (ТОП-10-е6)
- Генераторы паролей на основе личной информации

Выводы:

- Проведите организационные мероприятия по ИБ
- СисАдмин ≠ сотрудник ИБ
- Планово проводите пентесты и аудиты ИБ
- Регулярно производите резервное копирование данных
- Не позволяйте сотрудникам смешивать работу и личную жизнь

Готов ответить на ваши вопросы!

TG: t.me/eolgert