Конкурентная разведка при тестировании на проникновение

LM SECURITY

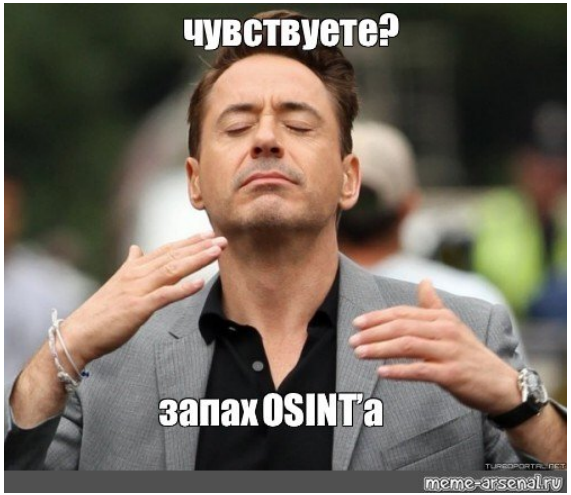
О себе

- Директор ООО “ЛианМедиа” (LMSecurity)
- Программист
- Специалист по OSINT
- Хакер

- Наш телеграм канал - t.me/lmsecurity
- Связаться со мной - t.me/ng_coba

LM SECURITY

О чем расскажу?



- Немного про пентесты
- Чуть больше про разведку
- Реальные кейсы

LM SECURITY

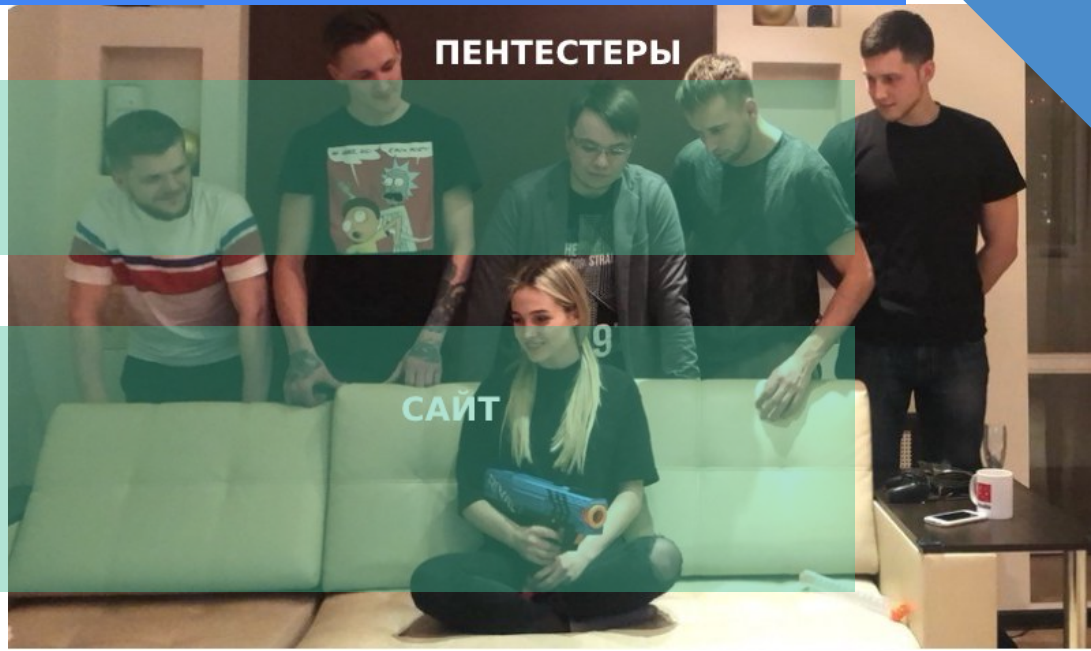
Пентест - тестирование на проникновение

По методу проведения

- ❑ BlackBox
- ❑ GreyBox
- ❑ WhiteBox

По контуру проведения

- ❑ Внешний периметр
- ❑ Web
- ❑ Внутренний периметр
- ❑ Wi-Fi
- ❑ Социотехническое тестирование



LM SECURITY

Этапы Пентеста

- ❑ Разведка
- ❑ Анализ результата разведки
- ❑ Сбор информации об уязвимостях
- ❑ Тестирование уязвимостей
- ❑ Отчет

LM SECURITY

Типы проводимых разведок

OSINT - Информация о юридическом лице (Структура предприятия, Сотрудники), Социальные сети, Тендерные закупки

TechINT - Корпоративная почта, Сайты, Домены, IP адреса, ПО, Утечки (ПДн сотрудников)

HumINT - Пароли, Информация о юридическом лице

LM SECURITY

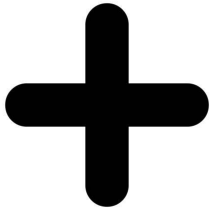
Кейсы.

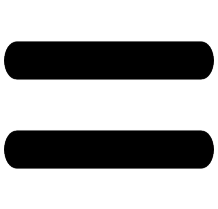
Главная проблема безопасности находится между стулом и монитором © Профессиональный юмор

1. Утечки данных от сотрудников
2. Утечки данных из локальной сети
3. Мисконфиги
4. Деанон

LM SECURITY

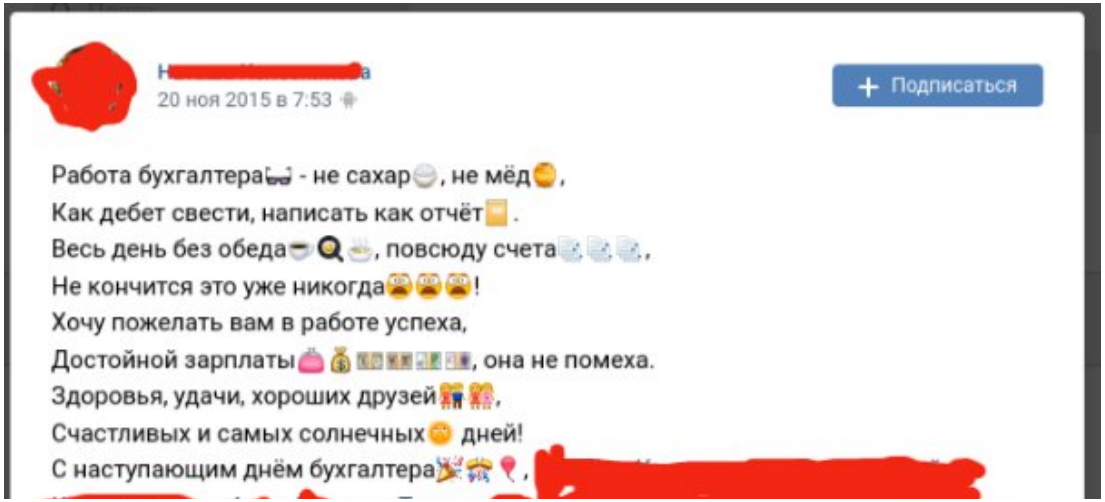
Утечка данных от сотрудников. GitLab





LM SECURITY

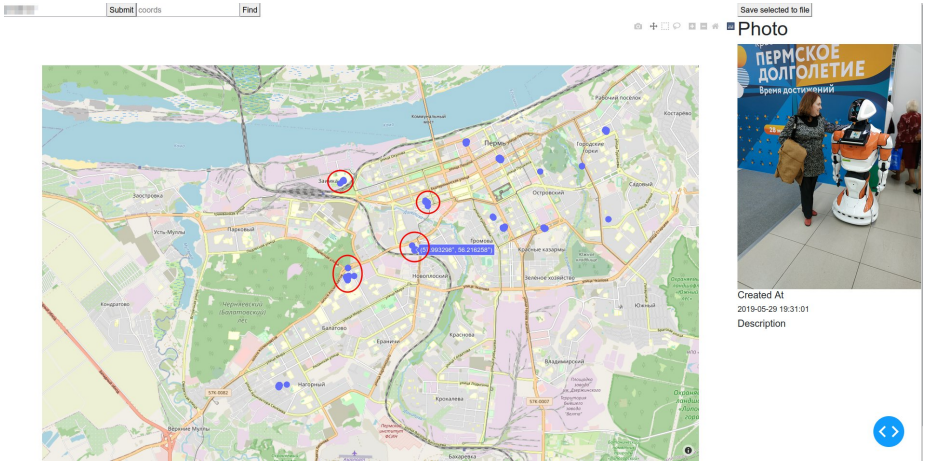
Утечка данных от сотрудников. Бухие бухи



В органах тоже бывают утечки

LM SECURITY

Утечка данных от сотрудников. Фото с рабочего места



Визуализация данных из метаданных фотографий vk с помощью vk_visualizer.

LM SECURITY

Утечка данных из локальной сети. Утечка домена

[redacted] - - [redacted]/2021:07:55:21 +0000] "GET /wpad.dat HTTP/1.1" 404 197 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36"

[redacted] - - [redacted]/2021:07:55:21 +0000] "GET /wpad.dat HTTP/1.1" 404 197 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36"

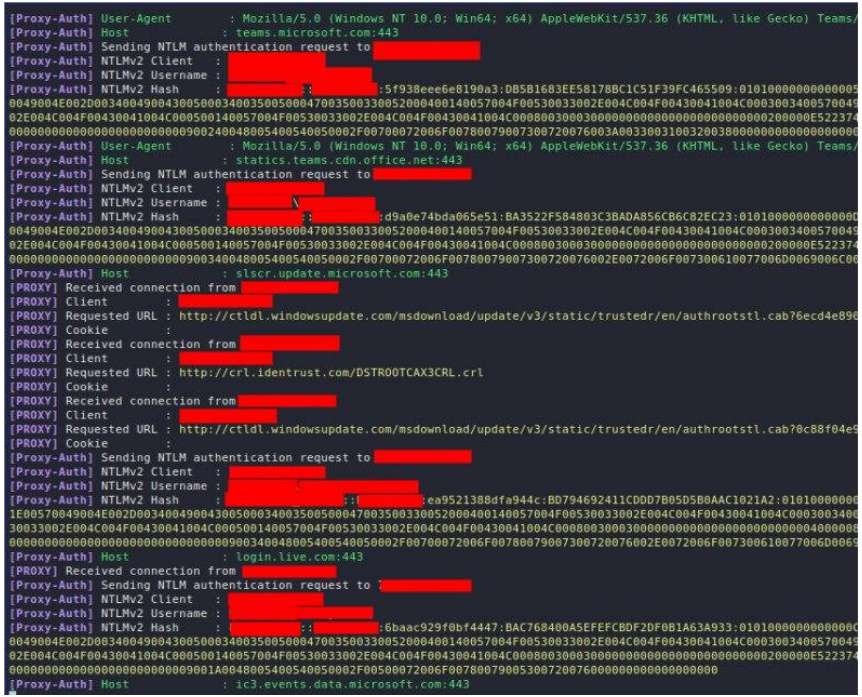
[redacted] - - [redacted]/2021:07:55:21 +0000] "GET /wpad.dat HTTP/1.1" 404 197 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Teams/1.4.00.19572 Chrome/85.0.4183.121 Electron/10.4.3 Safari/537.36"

[redacted] - - [redacted]/2021:07:56:08 +0000] "GET /wpad.dat HTTP/1.1" 404 197 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36"

1:37 PM

LM SECURITY

Утечка данных из локальной сети. Утечка домена



LM SECURITY

Утечка данных из локальной сети. Болтун m@il

ТОП-3 самые прибыльные профессии 2023-24 гг. по версии hh.ru

НП Новая профессия info@anogorodok.ru 21 октября в 5:49
Я ›

Открыть веб-версию

ТОП-3
Востребованных профессий по версии hh.ru в 2023-24 гг.

Приветствуем! Мы подготовили самую горячую подборку **бесплатных** вводных курсов для тех, кто планирует сменить профессию или научиться чему то новому

Новинка Акция

Дизайнер интерьера

Востребованность этой профессии на первом месте среди других. Столько домов еще не строилось никогда за всю историю!

Закрепить
Перевести
Распечатать
Создать правило
Свойства письма

Письма от Новая профе...

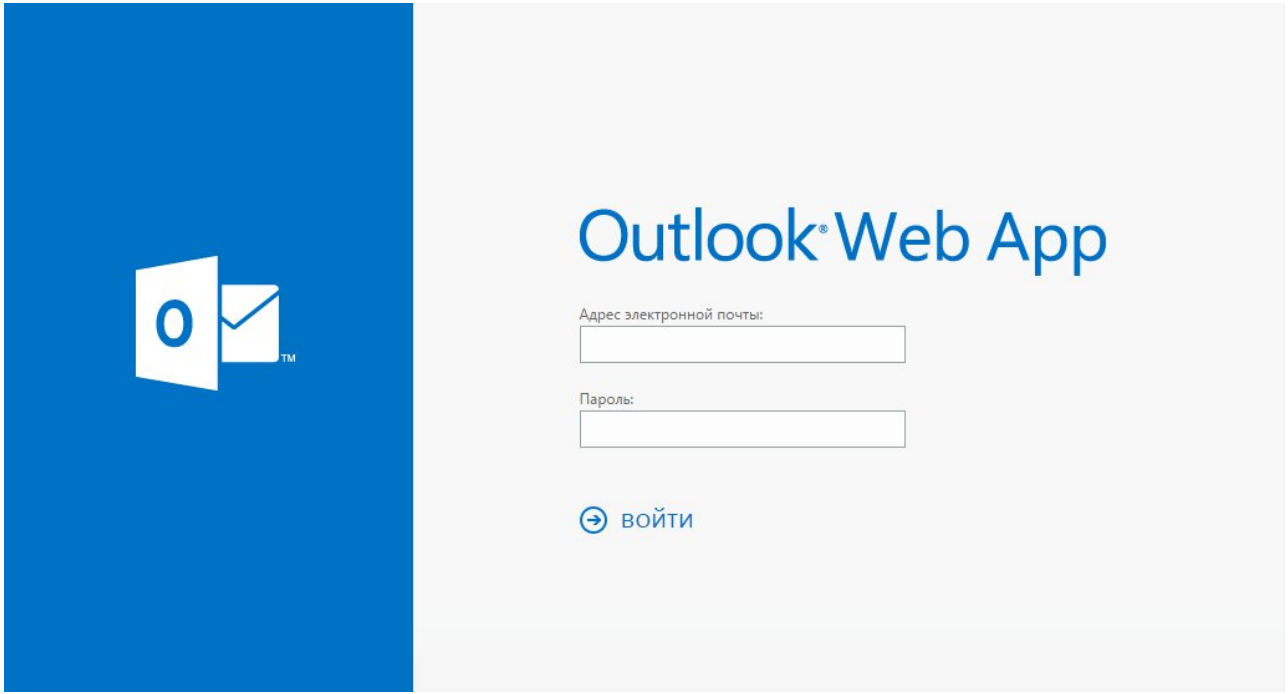
LM SECURITY

Утечка данных из локальной сети. Болтун m@il

```
Received: from postback28a.mail.yandex.net (postback28a.mail.yandex.net [2a02:6b8:c0e:500:1:45:d181:da28])
        by 6tnn3iljxohqlkhm.vla.yp-c.yandex.net with LMTP id QzPAzVQJuz-2wbBaMAs
        for <bat44anbat@ya.ru>; Mon, 24 Apr 2023 08:35:32 +0300
Received: from mail-nwsmtp-mxfront-production-main-95.vla.yp-c.yandex.net (mail-nwsmtp-mxfront-production-main-95.vla.yp-c.yanc
        by postback28a.mail.yandex.net (Yandex) with ESMTP id 576C45E4F2
        for <bat44anbat@ya.ru>; Mon, 24 Apr 2023 08:35:32 +0300 (MSK)
Received: from mrelay-rt5.hh.ru (mrelay-rt5.hh.ru [94.124.201.130])
        by mail-nwsmtp-mxfront-production-main-95.vla.yp-c.yandex.net (mxfront/Yandex) with ESMTPS id WZ73Jm0YIa60-njCFx3TI;
        Mon, 24 Apr 2023 08:35:32 +0300
X-Yandex-Fwd: 1
Authentication-Results: mail-nwsmtp-mxfront-production-main-95.vla.yp-c.yandex.net; spf=pass (mail-nwsmtp-mxfront-production-ma
rule=[ip4:94.124.200.0/21]) smtp.mail=no-reply@verp.hh.ru; dkim=pass header.i=@hh.ru
X-Yandex-Spam: 1
X-Yandex-Uid-Status: 1 1565755085
Received: from docker58.prod (balancer4.prod [172.16.20.27])
        by mrelay-rt5.hh.ru (Postfix) with SMTP id 4Q4YkW75Zkz95K5
        for <bat44anbat@ya.ru>; Mon, 24 Apr 2023 08:35:31 +0300 (MSK)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=hh.ru; s=mail;
        t=1682314532; bh=Huer6p/vTRV1GoHY1ndBXw/Nr1i1G2wMVLD8KEOjmVU=;
        h=Subject:From:To:Date:From;
        b=wTiDbjZyVqV/t25AguxyPiAXoZIlsRMD831IFklbcY9n7EWXdZvafOVdnhAG/xTR4
         Nu6d4oRZtYR7RP4Q9qT1xsjwTeRutsk7ui4st5W6NMfY94MV7qTvXO1klxmXXx8i2d
         RuUnF+NMAlN1gyQ6dC7f/Zt9HpTGkL1rGVjLSQI0=
X-HH-TEMPLATE-CODE: ResumeModerationApprovedWarning
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: quoted-printable
Subject: =?UTF-8?B?0JLRiyDQs9C+0YLQvtCy0Ysg0Log?=
 =?UTF-8?B?0L/QvtC40YHQutGDINGA0LDQsdC+0YLRiw==?=
From: "hh.ru" <noreply@hh.ru>
MIME-Version: 1.0
To: =?UTF-8?B?0J/QtdC90LrQuNC9INCY0LLQsNC9?= <bat44anbat@ya.ru>
X-HH-TAGS: [sender=hh-xmlback]
X-Postmaster-Msgtype:
Message-Id: <4Q4YkW75Zkz95K5@mrelay-rt5.hh.ru>
Date: Mon, 24 Apr 2023 08:35:31 +0300 (MSK)
Return-Path: no-reply@verp.hh.ru
X-Yandex-Forward: 31b8c675b76d15eeae4899cd11516e1a
```

LM SECURITY

Мискофиги. Google -> OWA -> 1C



LM SECURITY

Деанонимизация. 20 идей - 1 дырка

Дмитрий Давыдов
=
Ренат Фатхуллин

LM SECURITY

Как защититься

- ❑ Обучение сотрудников (Лекции, Рассылки)
- ❑ Проводите разведку по себе (лучше аутсорс, т.к. имеет место быть эффект замыленного глаза)
- ❑ Анализ защищенности
- ❑ Социотехнические тестирования

LM SECURITY

Спасибо за внимание.

Готов ответить
на Ваши вопросы!

Связаться со мной - t.me/ng_coba
Наш телеграм канал - t.me/lmsecurity