OSINT Primer：人员（第2部分）

请吃栗子吧 / 2019-04-01 09:40:00 / 浏览数 4633 渗透测试 渗透测试 顶(0) 踩(0)

翻译文章，原文链接：https://0xpatrik.com/osint-people/

原文作者：Patrik Hudak

在这篇文章中，继续讨论与OSINT相关的主题，我们将着眼于研究人员。与域名类似，在我们的"人员分析"中有一些特定的目标：

- 这个人是我们新认识的人。我们想找到一些关于他/她的信息。
- 你想雇用一名新员工。除了HR的标准背景检查之外，你可能想要执行你的OSINT以查看他/她是否是一个优秀的候选人。
- 你希望向某个特定公司的知名人士推销新的商业产品。你需要先获取他/她的电子邮件或手机号码。请注意，此步骤通常包括一些组织研究，将在本系列的下一部分中介绍
- 你是渗透测试人员，目前正在进行鱼叉式网络钓鱼评估。你需要查找信息以增加网络钓鱼评估的潜在成功。

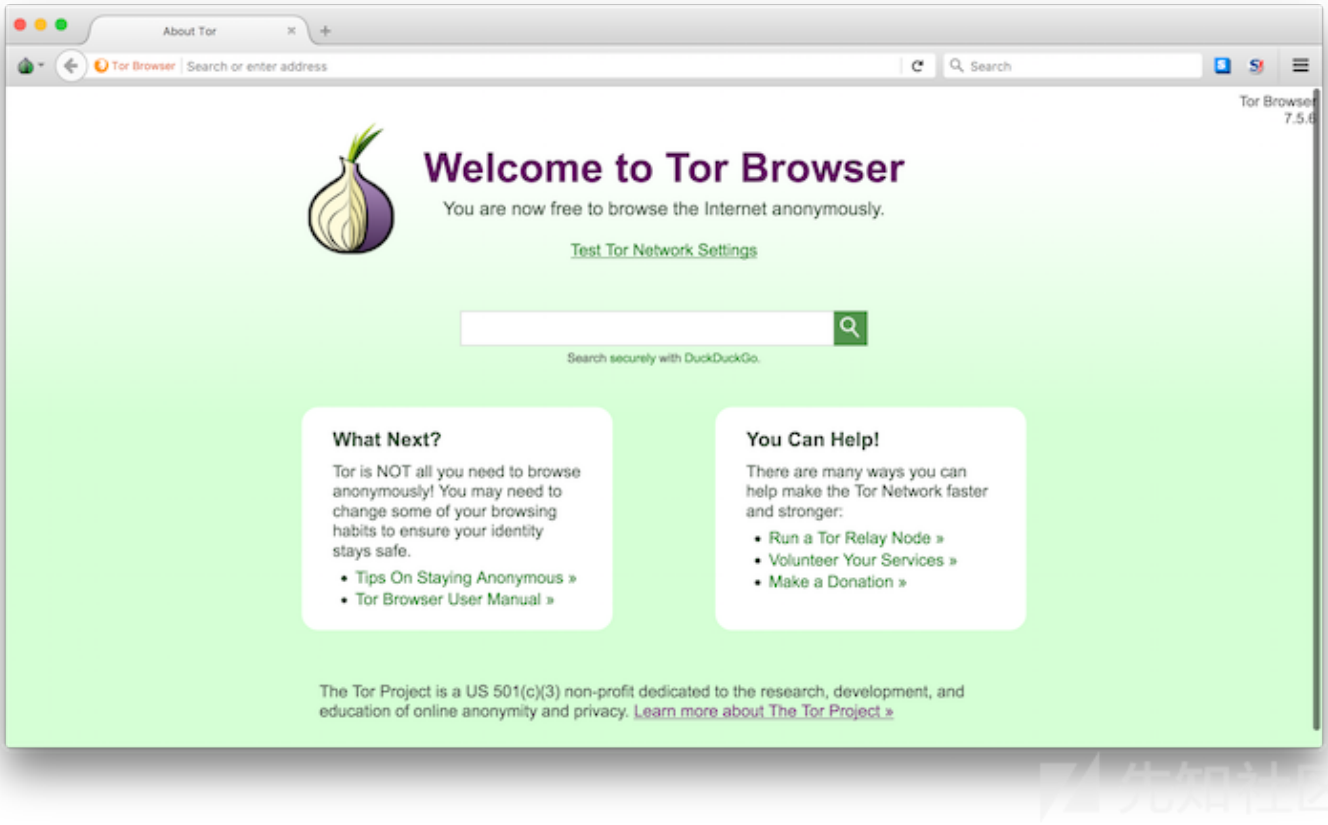
如你所见，有很多情况下关于人的OSINT可能会派上用场。我们来看一些具体的技巧。

注意：本指南中的技术不应用于恶意目的。虽然没有可用于恶意场景的方法很难编写指南，但我不对此类操作负责。

OPSEC

在开始之前，我想提一些重要的事情。你可能听说过运营安全或OPSEC。在搜索过程中，你可能会以多种不同的方式暴露自己。例如，如果你登录LinkedIn并访问其他一些

我建议使用Tor Browser Bundle进行所有与OSINT相关的活动。首先，由于多个加密连接（即onion），你的IP身份被隐藏。其次，Firefox的定制版本确保在重新启动之间删除cookie，因此不能对



如果你因Tor的速度而困扰，你可以选择使用VPN服务并结合一些安全的浏览环境。同样，你不希望以任何方式公开cookie。最简单的选择是在浏览器中使用私有模式，尽管

社交媒体

我喜欢做的第一件事是找到社交媒体配置文件。为什么？我相信他们掌握了大部分有用的OSINT信息。在处理诸如John Smith等流行名称时，你应该预料到多重误报。

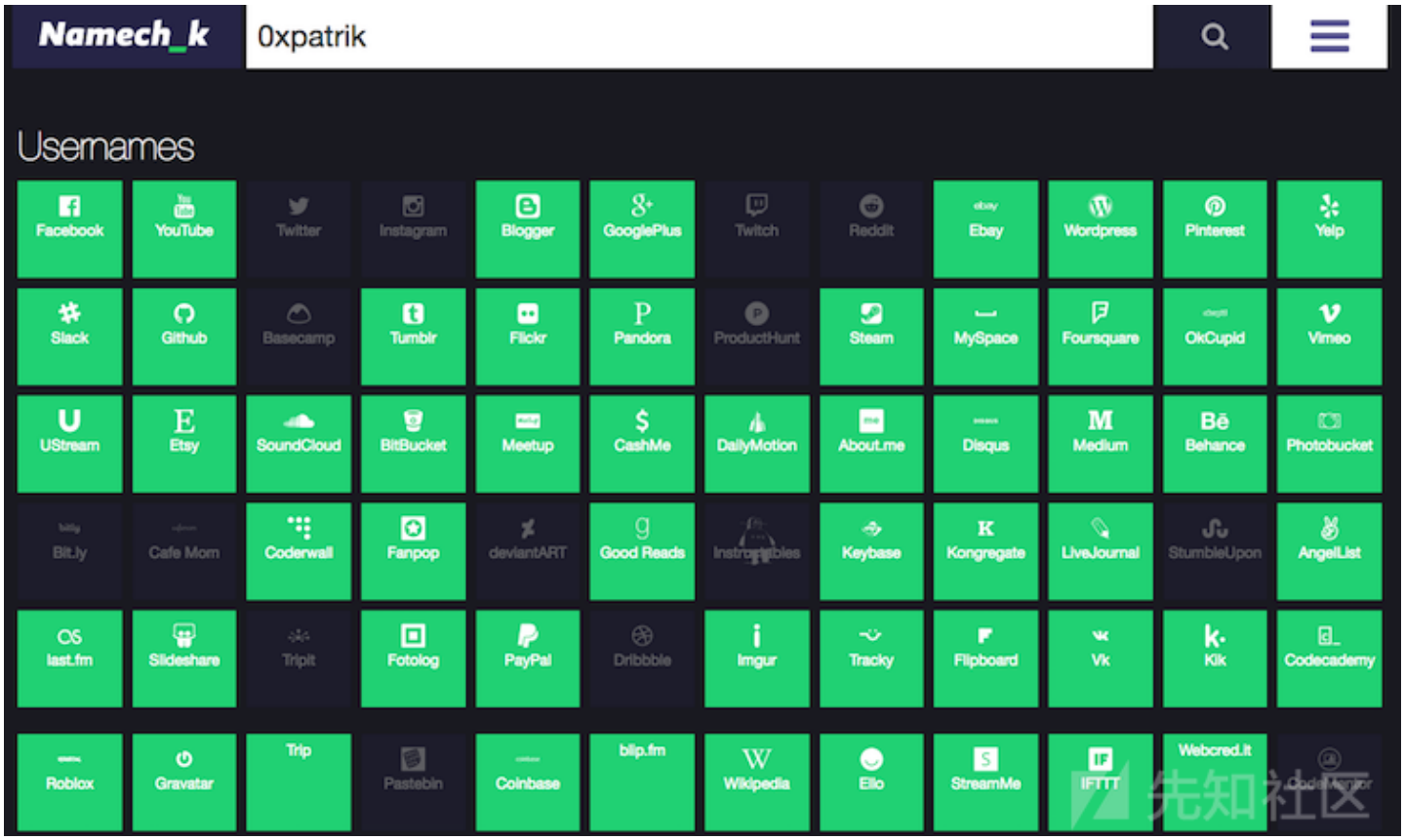
根据目标的隐私和一致性，查找社交媒体配置文件可能很困难，也可能很容易。简单的谷歌搜索有时会奏效：

```
John Doe site:facebook.com
John Doe site:instagram.com
```

```
John Doe site:linkedin.com
...
```

请注意，有许多社交媒体网站需要创建一个帐户才能查看完整的个人资料。我建议为此创建一个假帐户。

人们倾向于在不同的服务中重用他们的用户名。用户名在互联网上充当人的唯一标识符。我喜欢从这个人的Instagram中提取用户名。然后，我使用名为namechk的服务在



我不得不说我没有在所有指定的平台上注册帐户。你应该像往常一样期待一些误报。

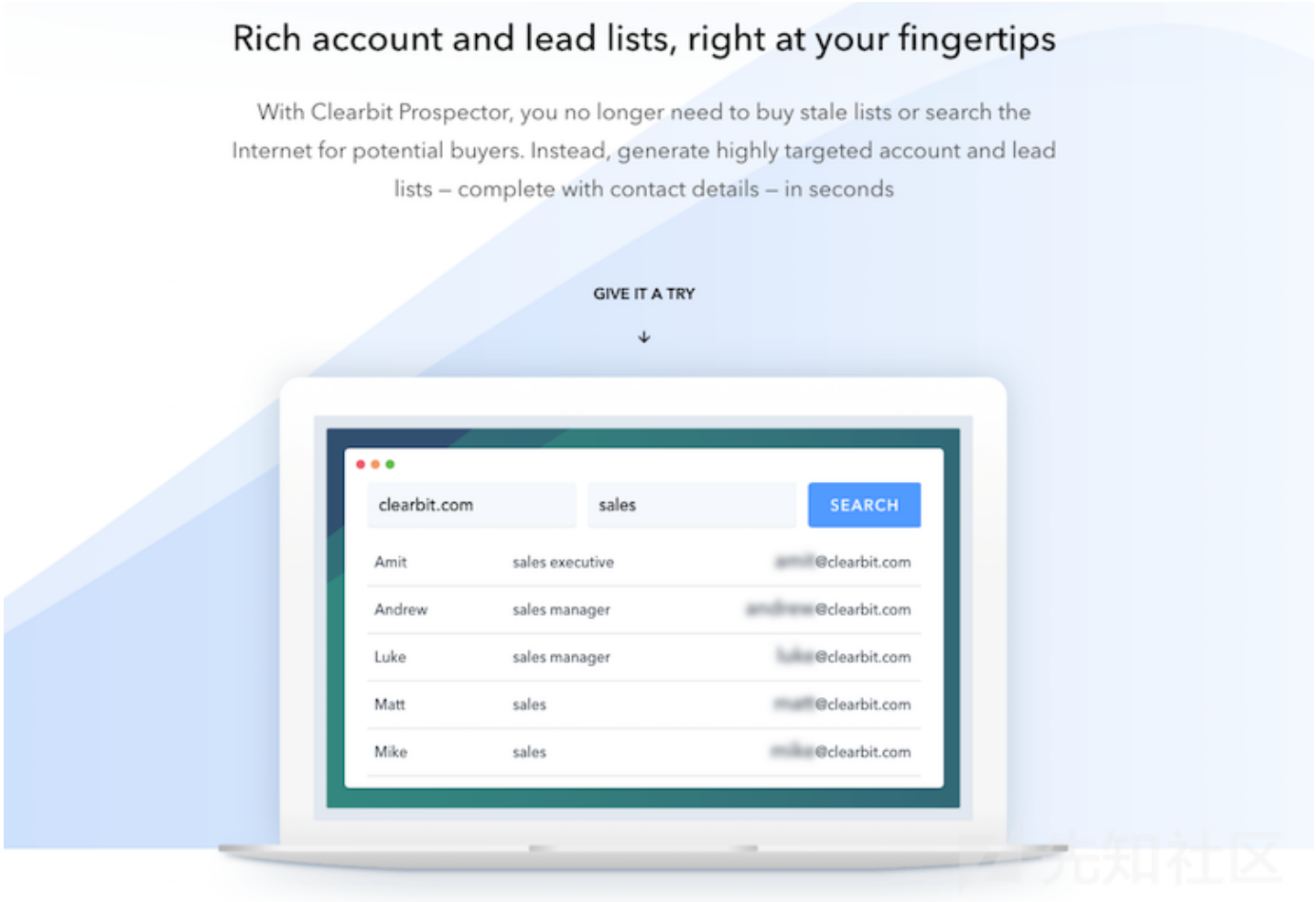
还有聚合器，如pipl.com或 social-searcher。虽然我并不总是使用它们，但它们往往能提供更高层次的人物视角。

电子邮件

这个主题既适用于此处，也适用于组织OSINT。我决定把它放在这里，因为我认为它主要与人而不是组织本身有关。

在处理销售时，通常需要在组织中建立良好的联系以便投资。你应该聪明一点，并决定哪个人是正确的选择。当然，向财富500强公司的首席执行官推销信息安全相关产品并

我不想在这里描述完整的获取电子邮件方法; 我想解释一下找到目标组织中关键人物的联系信息的最佳方法。我强烈建议你检查Clearbit Prospector以完成此任务。它是一款出色的具有准确数据的产品。虽然它是付费产品，但老实说，如果你做了很多这样的搜索，这是值得的。是的，它不是真正意义上的OS



我喜欢的另一种产品是Hunter.io。它也是付费产品，但你每月可免费获得100次搜索。类似的服务被称为voilanorbert和headreach。它们还采用免费增值模式。我认为这是

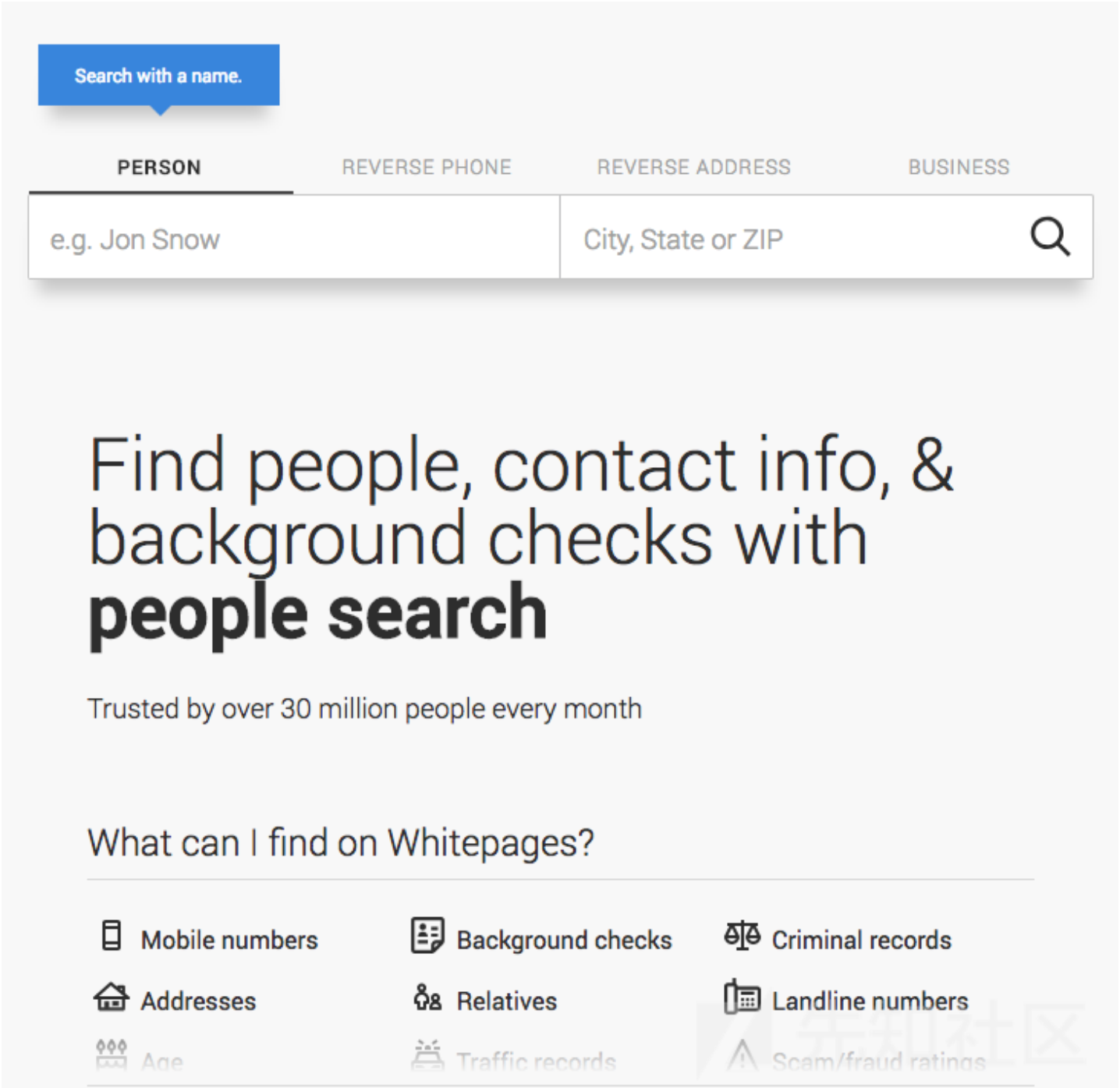
或者，你可以使用LinkedIn获取最初的冷消息。你只需将搜索栏与查询一起使用即可`<COMPANY_NAME>` `<POSITION>`获得最准确的结果。人们倾向于保持他们的LinkedIn个人资料更新。然后，你可以轻松地与他们联系（虽然不是通过电子邮件）。类似的，你也可以通过Twitt

专业提示：对于较小的公司，电子邮件通常直接列在他们的网站上。

对于一些关于冷呼叫的有用的Google Dorks，我推荐这篇文章。

电话号码

查找电话号码比电子邮件更难。我的首选工具是Google，我尝试使用此人的姓名和某些`telephone number`关键字组合进行dork，或在特定国家/地区使用白/黄页，例如whitepages.com。请务必检查awesome-osint以获取电话号码搜索服务列表。



有时，我需要执行反向电话搜索：给定电话号码，我想检索其所有者的名称。当你想要与所有者关联的未接来电时，此功能非常有用。你可以使用上述服务，但更通用的方法

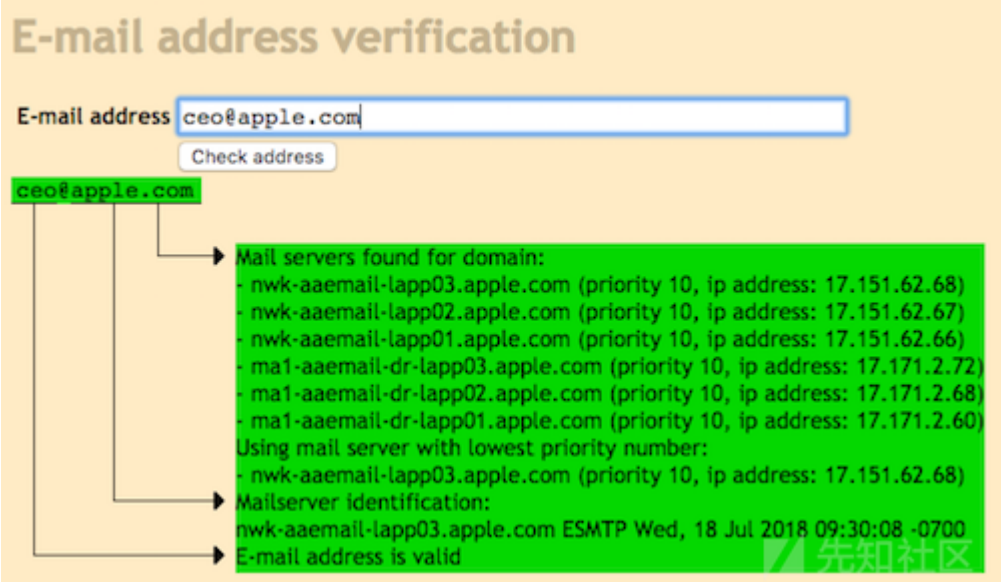
1. 尝试使用号码进行Facebook搜索。如果他/她具有与个人资料相关联的号码，则所有者应该在结果中出现。
2. 将号码保存在手机中，然后查看Viber或WhatsApp联系人列表。这些服务允许指定照片和所有者的姓名，只需知道电话号码即可提取此信息。

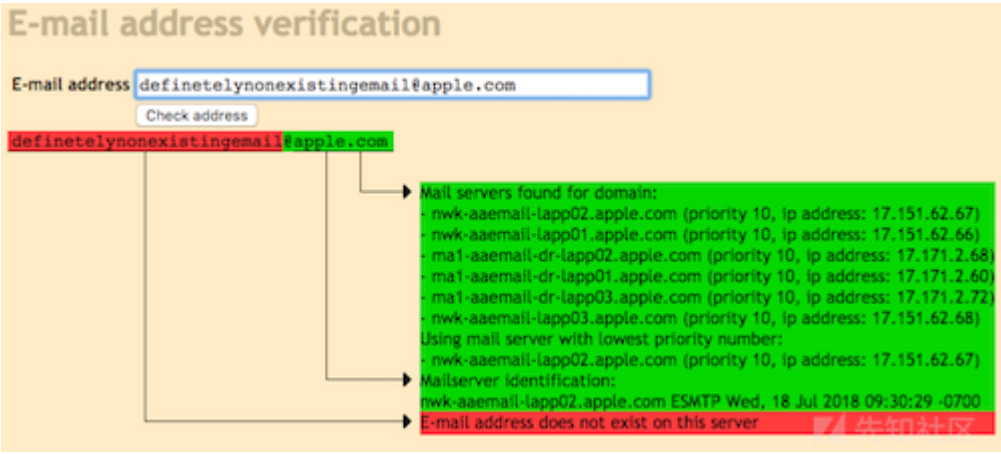
电子邮件

我描述了在上面的部分找到电子邮件。现在，我想扩展它并讨论有关电子邮件OSINT的更多技术问题。SMTP支持两种，不是很有名的命令VRFY和EXPN。前者用于直接在邮

```
lastname@company.tld
firstname.lastname@company.tld
firstletterfirstname.lastname@company.tld
```

最简单的测试方法是使用MailTester.com等在线工具。不要被这个网站的历史设计分心。与其他类似服务相比，它做得非常出色。请注意，并非每个SMTP服务器都允许此命





该EXPN命令用于列出一些通讯组列表的成员。SMTP服务器提供此类成员的个人电子邮件地址。

我还想测试一些泄露凭证转储中是否存在某些电子邮件地址。最简单的方法就是用 Troy Hunt的[Have I Been Pwned
。这与安全评估结合使用非常有用。为什么？通常人们重复使用密码，并且用户在某些服务中使用的密码也有可能在企业环境中使用。

本指南的目的不是为你提供尽可能多的工具。相反，我尝试解释不同的技术。如果你想使用不同的工具，可以在这里找到合适的工具。请注意，某些工具仅适用于特定国家/

上一篇：RemTeam攻击技巧和安全防御 下一篇：Real World Finals...
1. 0 条回复
   - 动动手指，沙发就是你的了！