Asset Discovery: Doing Reconnaissance the Hard Way

落花四月 / 2019-01-24 08:35:00 / 浏览数 3284 安全技术 WEB安全 顶(0) 踩(0)

Asset Discovery: Doing Reconnaissance the Hard Way

第一次翻译文章，如有错误的地方，希望各位能够指正(Ths)

原文链接：https://0xpatrik.com/asset-discovery/

在这篇文章中，我想概括和讨论一个发现某个特定实体（企业，大学.....）资产的框架。什么时候有用？

渗透测试 - 您拥有一个非常广泛的评估范围。您的第一个目标是找到机器和服务出现的漏洞。

Bug赏金狩猎 - 与上面的一样。一些bug赏金程序没有明确列出所有目标(只是简单的给出域名)。你经常需要自己做。

定期“检查” - 有时，公司将服务和应用程序暴露在互联网上。这些服务通常不会更新，可能包含公共漏洞，或者应用程序不应被公开

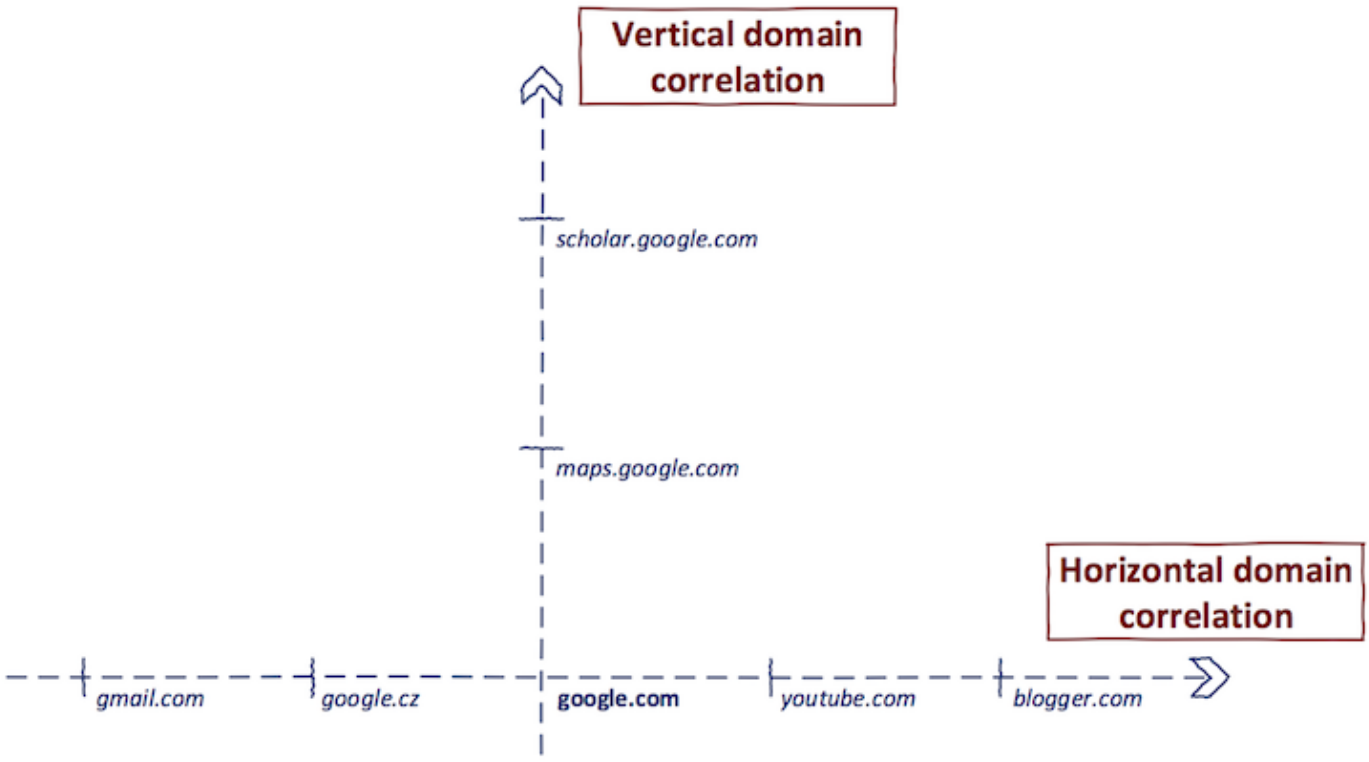
域名

简单地说;
域名代表Internet上IP地址的一些标签。因为公司将他们的基础设施迁移到云端，我们需要“像大海捞针般寻找公司的服务器”。然而，域名提供某种到IP地址的链接。

我们的目标是查找/关联我们感兴趣的单个实体所拥有的所有域名。我们将逐步实现垂直和水平域名相关。在下文中，单词目标表示相关过程中感兴趣的实体。

垂直域名相关 - 给定域名，垂直域名相关是查找域名共享相同基础域名的过程。此过程也称为子域名枚举 1。

水平域名关联 - 给定域名，水平域名关联是查找其他域名的过程，这些域名具有不同的二级域名但是连接相同的实体1。



为了演示，我选择了eff.org作为目标。

步骤1： 在eff.org上执行垂直域名关联

这可以使用Sublist3r，amass或aquatone等工具实现。请注意，有许多用于子域名枚举的开源工具，它们提供的结果很差。

根据我的经验，最好使用“meta-subdomain枚举”，它结合了多个枚举服务（如上面提到的工具）的结果。

Sublist3r的样本（剥离）输出

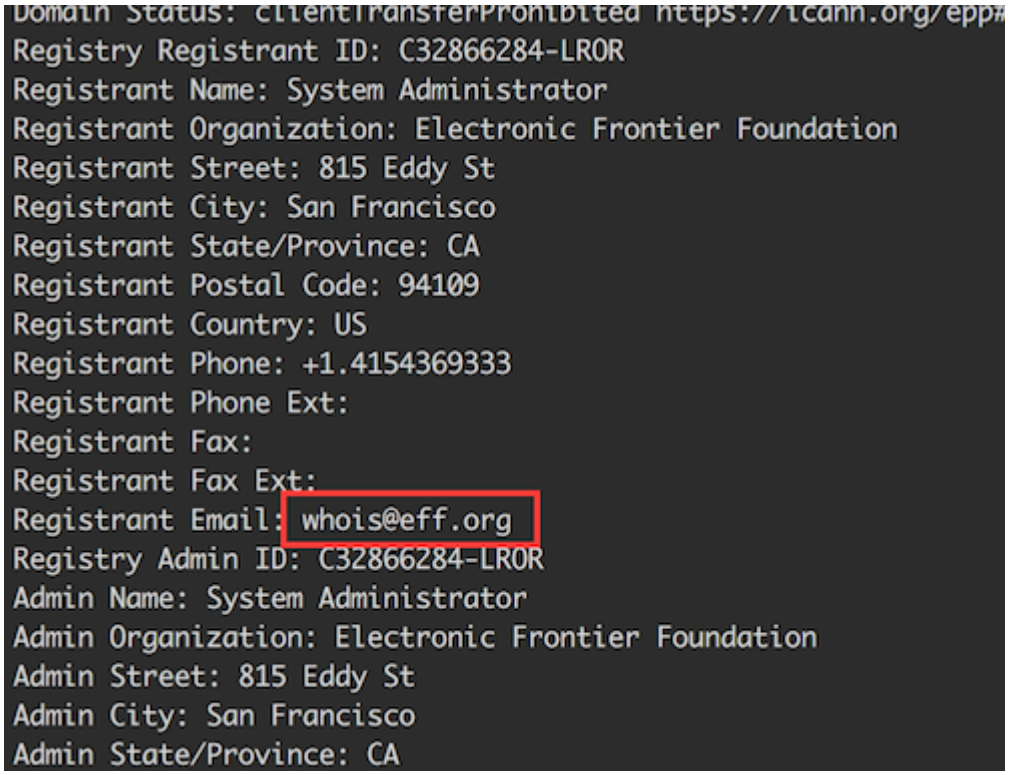
```
...
observatory.eff.org
```

```
observatory6.eff.org
observatory7.eff.org
office.eff.org
outage.eff.org
owncloud.eff.org
panopticlick.eff.org
projects.eff.org
push.eff.org
redmine.eff.org
robin.eff.org
s.eff.org
...
```

第2步： 在eff.org上执行水平域名关联

这一步有点棘手。首先，让我们考虑一下。我们不能像上一步那样依赖语法匹配。潜在地，`abcabcabc.com`和`cbacbacba.com`可以由同一实体拥有。

但是，它们在语法上不匹配。为此，我们可以使用WHOIS数据。有一些反向WHOIS服务允许您根据WHOIS数据库的共同价值进行搜索。让我们查询eff.org的WHOIS:



如您所见，一封电子邮件发给了注册人。现在，我们可以进行反向WHOIS搜索，使用相同的注册人电子邮件显示其他域名：

Reverse Whois results for whois@eff.org

There are 118 domains that matched this search query.
These are listed below:

Domain Name	Creation Date	Registrar
addtls.com	2016-03-08	GANDI SAS
addtls.net	2016-03-08	GANDI SAS
addtls.org	2016-03-09	GANDI SAS
canvastrackersimulator.org	2016-01-20	GANDI SAS
certbot.com	2013-12-29	GANDI SAS
certbot.info	2016-03-16	GANDI SAS
certbot.net	2016-03-16	GANDI SAS
certbot.org	2016-03-16	GANDI SAS
checkyourreps.org	2018-02-05	GANDI SAS
comebackwithawarrant.org	2007-08-30	GANDI SAS
copycrime.com	2007-04-02	GANDI SAS
copycrime.org	2007-04-02	GANDI SAS
copyright-watch.org	2008-05-30	GANDI SAS
copyrighttrap.net	2015-04-07	GANDI SAS
copyrighttrap.org	2015-04-07	GANDI SAS
cryptobot.org	2013-11-15	GANDI SAS
crystalprison.org	2012-06-20	GANDI SAS
dearfcc.com	2014-05-07	GANDI SAS

对于反向WHOIS，我使用了viewdns.info服务。诸如domlink或amass之类的工具也可用于水平域名的查询。

步骤3： 迭代

在此阶段，您应该拥有与目标相关联的相当广泛的域名列表。

IP地址如果幸运的话，您的目标将拥有专用的IP地址范围。最简单的检查方法是在从域名中找到的三个IP地址上运行IP到ASN的转换：

eff.org：

```
$ dig a eff.org +short
69.50.232.54
$ whois -h whois.cymru.com 69.50.232.54
AS  | IP   | AS Name
13332   | 69.50.232.54 | HYPEENT-SJ - Hype Enterprises, US
```

certbot.eff.org：

```
$ dig a certbot.eff.org +short
lb5.eff.org.
173.239.79.196
$ whois -h whois.cymru.com 173.239.79.196
AS  | IP   | AS Name
32354   | 173.239.79.196   | UNWIRED - Unwired, US
```

falcon.eff.org：

```
$ dig a falcon.eff.org +short
mail2.eff.org.
173.239.79.204
$ whois -h whois.cymru.com 173.239.79.204
AS  | IP   | AS Name
32354   | 173.239.79.204   | UNWIRED - Unwired, US
```

在这种情况下，似乎EFF.org没有专门的IP空间（我们可能会认为它是UNWIRED，但它很可能也会覆盖其他实体）。举个例子，我们来看看谷歌：

```
$ dig a google.com +short
mail2.eff.org.
173.239.79.204
$ whois -h whois.cymru.com 216.58.210.14
AS  | IP   | AS Name
15169   | 216.58.210.14| GOOGLE - Google LLC, US
```

正如你看到的这样，Google在AS15169上运行（这是他们的AS之一）。

拥有专用IP范围可以使事情变得更轻松：我们知道公司拥有AS中列出的IP范围。使用此信息，我们可以从CIDR表示法编译IP地址列表。

如果目标没有专用空间，我们将需要依赖上一步中编译的域名。从这些，我们将解析IP地址。即使目标具有专用IP范围，我也建议您按照以下流程进行操作。部分基础架构很

请注意，使用此方法很可能出现误报。您的目标可能使用共享托管，例如，用于登录页面。该主机的IP地址将包含在您的列表中。但是，此地址并非专用于您的目标。

对于此上下文中的DNS解析，我建议使用massdns，它会将已编译到列表中的域名解析为其相应A记录中的IP地址：

```
./massdns -r lists/resolvers.txt -t A -q -o S domains.txt
| awk '{split($0,a," "); print a[3]}'
| sort
| uniq
```

这将生成与目标的FQDN对应的IP地址列表。然后，您可以将此结果集附加到CIDR块（如果有）的IP地址。

在此阶段，您应该有一个链接到目标的IP地址列表。

服务

收集域名和IP地址的原因是为了寻找哪些服务（应用程序）把漏洞暴露给Internet上的攻击者。因此，我们需要扫描主机进行查询。

我们有两种选择：

主动扫描 -
传统的nmap方法。对于大量主机，我也建议使用masscan。主动扫描更耗时，并且可能触发公开面临的IDS。但是，您可以获得打开服务的最准确表示。

被动扫描 - 依赖从其他来源收集的数据。这些来源包括例如Shodan或Censys。缺点是结果可能会持续数天，某些服务可能已经关闭。

另一方面，您没有直接连接到目标网络。在进行APT模拟时，这种“秘密”模式通常是首选。你需要在新鲜感和积极性之间找到平衡点。

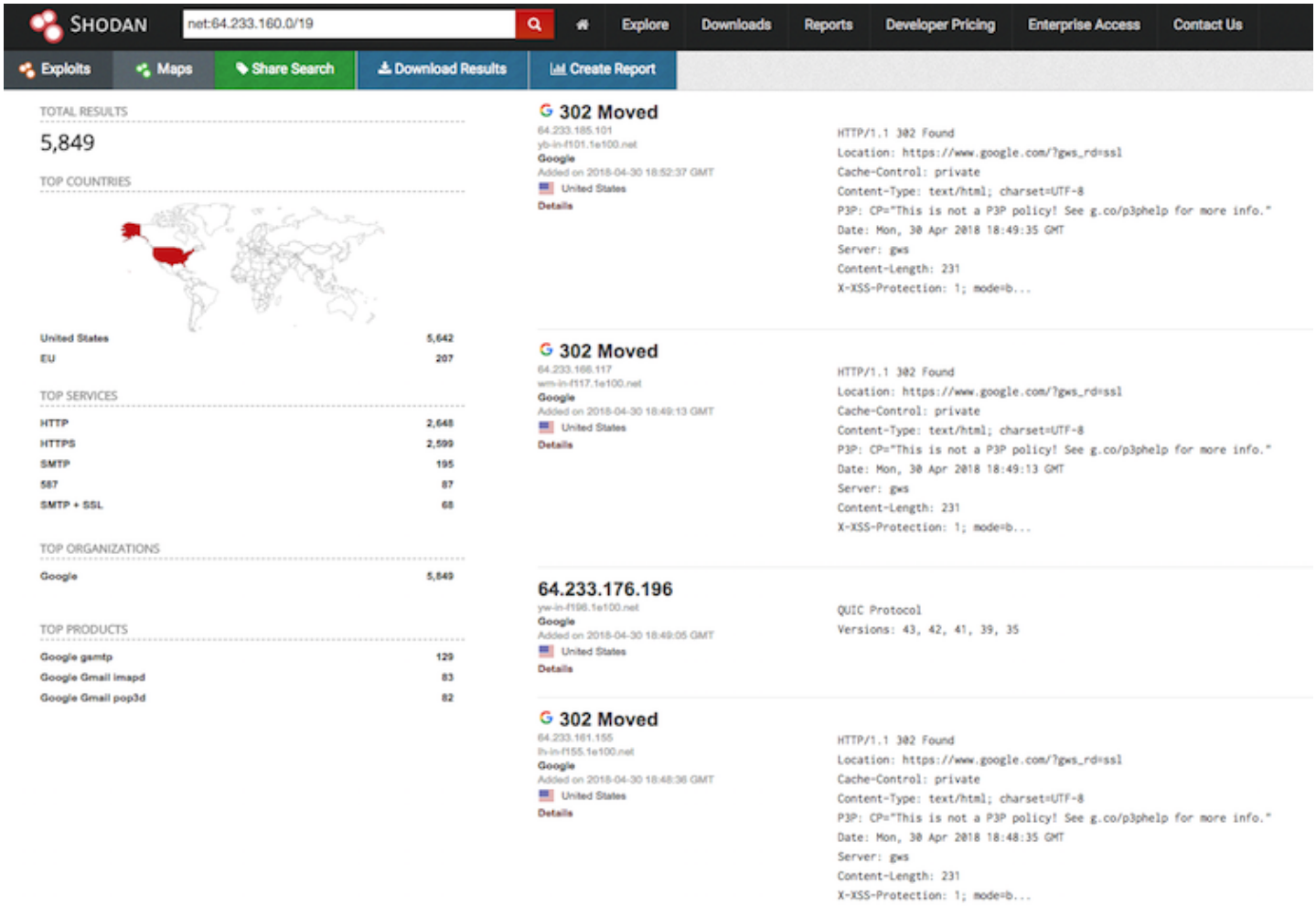
Shodan为此提供了非常好的 dorks。我们可以像这样搜索指定的IP范围：

```
net:64.233.160.0/19
```

更好的是，我们可以根据WHOIS数据库中的组织进行过滤：

```
org:"Google"
```

请注意，此搜索还包括“Google Cloud”■“Google Fiber”等，它们不属于AS15169。我还没有成功过滤“Google”。



Censys提供了几乎相同的功能：

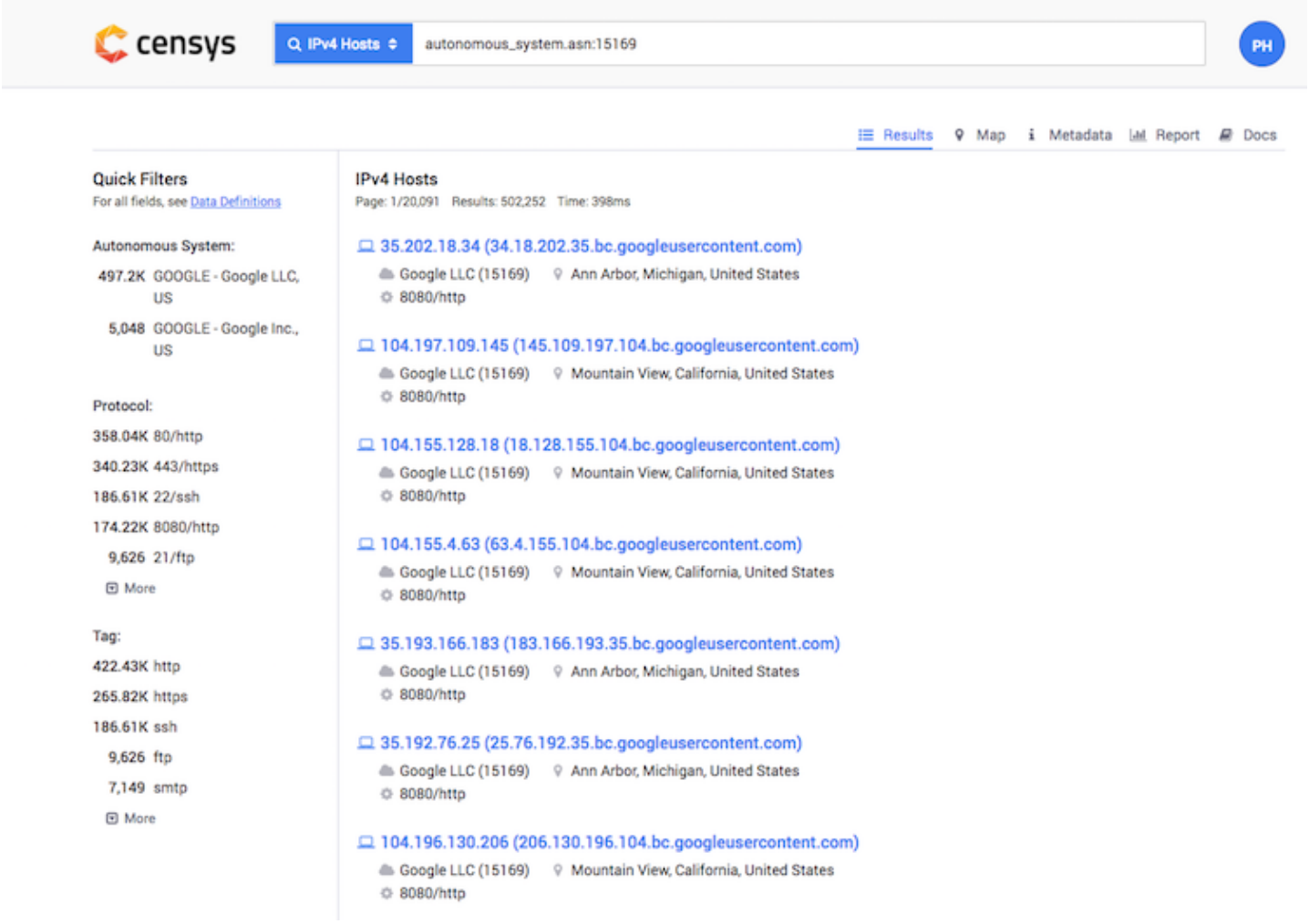
```
ip:64.233.160.0/19
```

对于组织/ ASN过滤器：

```
autonomous_system.asn:15169
```

要么

```
autonomous_system.organization:"Google Inc."
```

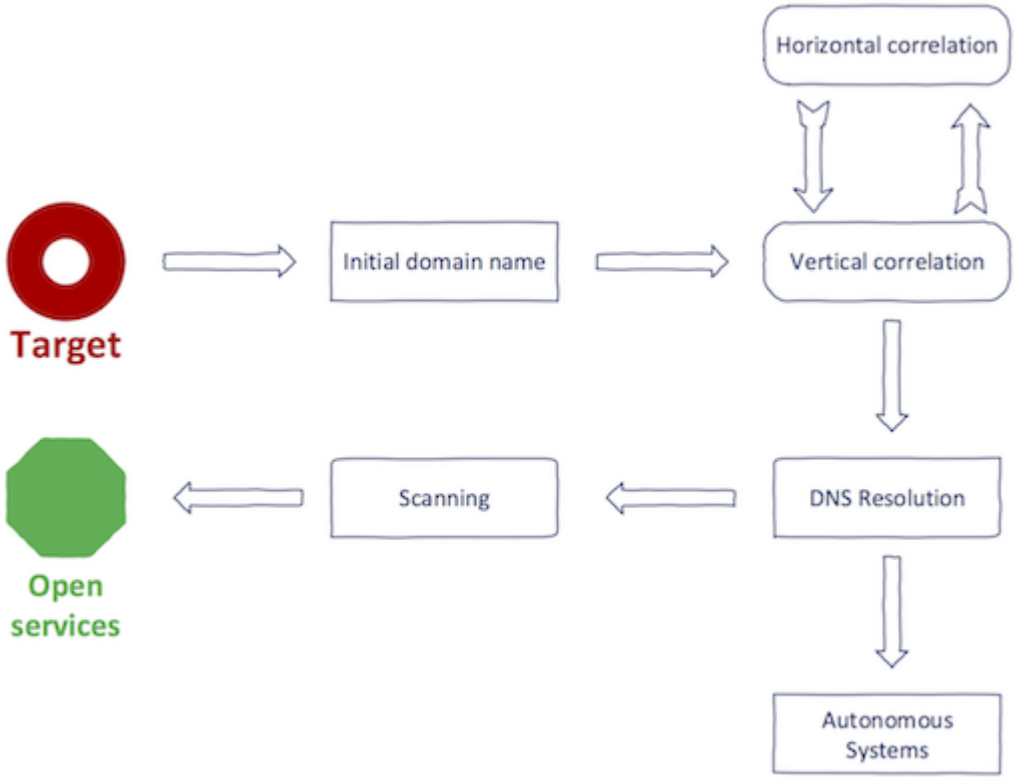


有关Censys的完整教程，请查看我的其他帖子。

对于完全隐藏模式，您可以使用Project Sonar检索从域名到开放端口的所有内容。

整理信息

此时，您应该在整理一下思路。您实现它的过程看起来像这样：



最终收集的信息应包含目标的IP地址以及端口。

您仍然可以执行后处理任务以快速显示最有趣的服务。例如，您可以运行大量网站截图工具，例如Snapper，它将提供在一个地方运行网站的绝佳概述。对于VNC或RDP可以

其他资源：

spyonweb.com

domain_analyzer

VHostScan

fierce

domain-profiler

zonemaster

Visual Recon

上一篇：使用AMP技术分析RAT威胁 下一篇：PDO场景下的SQL注入探究

1. 0 条回复

- 动动手指，沙发就是你的了！

目录