fierce.pl (C) Copywrite 2006,2007 - By RSnake at http://ha.ckers.org/fierce/

默认字典位置 locate hosts.txt

格式: perl fierce.pl [-dns example.com] [参数]

查找目标IP 子域名 可以设置 不需要的地址 并且可以爆破 和枚举

简介:

Fierce is a semi-lightweight scanner that helps locate non-contiguous

IP space and hostnames against specified domains. It's really meant

as a pre-cursor to nmap, unicornscan, nessus, nikto, etc, since all

of those require that you already know what IP space you are looking

for. This does not perform exploitation and does not scan the whole

internet indiscriminately. It is meant specifically to locate likely

targets both inside and outside a corporate network. Because it uses

DNS primarily you will often find mis-configured networks that leak

internal address space. That's especially useful in targeted malware.

简单的说说 这个是一个轻量级的扫描器 有助于定位不连续的IP 地址

Dns是你经常会发现配置错误的地方 特别是一些恶意软件

**参数**:

-connect 试图通过HTTP连接到任何非RFC1918（公网）地址 他将输出返回头 但是会被警告，这可能需要很长一段时间对一家公司的许多目标进行扫描，取决于网络/机器延迟。

我不推荐这样做，除非它是一个小公司或你有一个大量的空闲时间在你的手上（可能需要几天）。在文件中指定的文本“主机：N”将被替换 由主机指定

格式:

perl fierce.pl -dns example.com -connect headers.txt

-delay 查找等之间的响应秒数。

-dns 您要扫描的域。

-dnsfile 使用DNS服务器提供的文件（每行一个）为反向查找（暴力）。

-dnsserver 反向查找使用特定的DNS服务器（应该是目标DNS服务器）。激烈的使用你的DNS服务器的初始SOA查询和再利用目标DNS服务器的所有其他查询默认

-file 您希望输出的文件将被保存在哪里

-fulloutput 当结合-连接，这将输出一切服务器返回的HTTP头，不只是。

-help 显示帮助文件

-nopattern 在寻找附近时不要使用搜索模式 而是转储一切。这是很吵，但发现其他的领域，你可能会使用是有用的。 它也会给你大量的错误, 特别是在大的DNS区域.

-range 扫描内部IP范围 (must be combined with

-dnsserver). 请注意，这不支持一个模式，并简单地输出它发现的任何东西。

格式:

perl fierce.pl -range 111.222.333.0-255 -dnsserver ns1.example.co

-search 搜索列表. 当试图穿越所有ips可能遇到其他服务器内，可能属于同一公司的其他领域。 如果你提供一个逗号分隔的列表，它会报告任何发现。 这是特别有用的，如果企业服务器被命名为不同于公共面对的网站。

Usage:

perl fierce.pl -dns examplecompany.com -search corpcompany,blahcompany

**默认的搜索列表**

请注意，使用搜索也可以大大扩展找到的主机数量，因为它将继续遍历一旦它位于您在您的搜索列表中指定的服务器。 这将会更好

-suppress 抑制所有TTY输出(when combined with -file).

-tcptimeout 指定一个不同的超时时间 (default 10 seconds). 你可能要增加这个如果你查询的DNS服务器是缓慢的或有很多网络滞后。

-threads 指扫定在描时使用多少个线程 (默认是单线程).

-traverse 指定一个数字的IPS上面和下面你会发现寻找附近的IPS无论IP。默认为5以上和以下。 移动不会移动到其他模块。

-version 输出版本号

-wide 扫描整个C类C类后，找到任何匹配的主机名。这会产生更多的流量，但可以发现更多的信息。

-wordlist 使用一个单独的表去扫描 (每行一个条).

Usage:

perl fierce.pl -dns examplecompany.com -wordlist dictionary.txt