InTrace

InTrace是类似与路由追踪的应用程序，他能使得使用者或安全人员使用现有的TCP连接来枚举IP跳数

从本地网络或远程主机发起，可能对网络进行侦察和防火墙绕过.

——*Robert Swiecki*

一，帮助手册

intrace -h 主机 -p 端口 -d 调试级别 -s 有效负载大小 -4 IPV4 -6 IPV6

二，相关原理与实例

首先要与目标建立一个TCP连接，之后InTrace进行嗅探及抓取目。

1.建立一个TCP链接

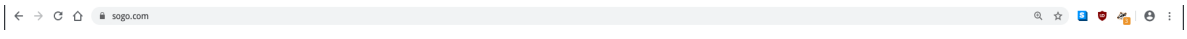
> nc www.sogo.com 443

2.在终端中输入 intrace -h baidu.com -p 443 -d 10 -s 10 -4

通过443端口对目标主机进行探测，调试级别和有效负载大小为10设置为Ipv4地址

3.在iintrace中如果当前状态为 “Press ENTER"则可按”回车键“来查看intrace追踪到的结果

三，80和443端口的区别



根据钟山计算机端口安全响应平台所收入的80和443端口看，”80端口通常只提供Web服务“，而”443端口通常提供HTTPS服务“。

> **”80“**
>
> 80端口通常提供web服务。目前黑客对80端口的攻击典型是采用SQL注入的攻击方法，脚本渗透技术也是一项综合性极高的web渗透技术，同时脚本渗透技术对80端口也构成严重的威胁。
>
> 端口危害：
> windows2000的IIS5.0版本，黑客使用远程溢出直接对远程主机进行溢出攻击/ windows2000中IIS5.0版本，黑客也尝试利用‘Microsoft IISCGI’文件名错误解码漏洞攻击/ IIS写权限漏洞是由于IIS配置不当造成的安全问题，攻击者可向存在此类漏洞的服务器上传恶意代码/ 普通的http封包是没有经过加密就在网络中传输的，这样就可通过嗅探类工具截取到敏感的数据/ 进行CC或者DDOS攻击.
>
> 相关漏洞：windows2000的IIS5.0版本，黑客使用远程溢出直接对远程主机进行溢出攻击/ windows2000中IIS5.0版本，黑客也尝试利用‘Microsoft IISCGI’文件名错误解码漏洞攻击/ IIS写权限漏洞是由于IIS配置不当造成的安全问题，攻击者可向存在此类漏洞的服务器上传恶意代码/ 普通的http封包是没有经过加密就在网络中传输的，这样就可通过嗅探类工具截取到敏感的数据/ 进行CC或者DDOS攻击.
>
> 相关文章：暂无
>
> 威胁系统：Windows / Linux
>
> 贡献者：燃/ Khan安全团队
> 提交时间：2019年12月29日

> **443端口**
>
> 端口信息：443端口即网页浏览端口，主要是用于HTTPS服务，是提供加密和通过安全端口传输的另一种HTTP。
>
> 端口危害：心血漏洞/CVE-2014-0160，可导致提取部分心跳包获取内存中的敏感数据.心血漏洞/CVE-2014-0160，可导致提取部分心跳包获取内存中的敏感数据攻击者可以利用这点，构造异常的数据包，来获取心跳数据所在的内存区域的后续数据。这些数据中可能包含了证书私钥、用户名、用户密码、用户邮箱等敏感信息。该漏洞允许攻击者，从内存中读取多达64KB的从内存中读取多达64KB的数据。
>
> 相关漏洞：心血漏洞/CVE-2014-0160
>
> 相关文章：https://www.jianshu.com/p/08600e2f4530
>
> 威胁版本：OpenSSL1.0.1、1.0.1a 、1.0.1b 、1.0.1c 、1.0.1d 、1.0.1e、1.0.1f、Beta 1 of OpenSSL 1.0.2等版本
>
> 威胁系统：Windows / Linux
> 端口评分：暂无
> 收入编号：ZSDK-3-443
> 端口贡献者：ying，燃 / Khan安全团队