此文章已于 1:09:01 2015/12/25 发布到 Net | Linux | 安全

★Kali信息收集~★7.FPing ：ip段扫描

* 1. **参数：**

计算机生成了可选文字:
/ home/ dnt# fping -h 
fping (options) (targets. . .1 
i fied) 
-g spec 
a IP netmask) 
Usage: 
-g 
H 
-p 
-q 
-S 
T 
file 
n 
if 
addr 
n 
show targets that are alive 
show targets by address 
of ping data to send, 
in bytes (default 
56) 
amount 
set exponential backoff factor to 
of pings to send to each target (default 
1) 
ount 
report results in verbose format 
same as -c, 
print timestamp before each output line 
show elapsed 
time on return packets 
read list 
f targets from a fil 
means stdin) (only if no 
generate target list ( o Y 
nl_ if no 
speci fied) 
( spec Y 
if the start and end IP in the target list, 
fping -g 192. 168. 1.0 192. 168. 1. 255 or fping 
Set the IP TTL 
value ( 
Time To Live hops) 
interval between sending ping packets (in millisec) 
bind to a particular interface 
loop sending pings forever 
ping multiple interfaces on target host 
show targets by name ( -d IS equivalent) 
or supply 
-g 192. 168. 1. 0/24) 
( default 
25) 
et the type of service (tos) 
flag on the ICMP packets 
interval between ping packets to one target (in 
in looping and counting modes, default 
1000) 
quiet (don' t show per- target/ per-ping results) 
same as - q, but show summary every n seconds 
number of ret ries (default 
3) 
print final stats 
set source address 
individual target initial timeout in millisec) 
ignored ( for compatibility with fping 2. 4) 
show targets that are unreachable 
show version 
list 
of targets to check (if no 
i fied) 
spec 
millisec) 
( default 
500) 
targets 

使用方法: fping [选项] [目标...]

-a显示是活着的目标

-A 显示目标地址

-b n 大量 ping 数据要发送，以字节为单位 (默认 56)

-B f 将指数退避算法因子设置为 f

-c n 的计数的 ping 命令发送到每个目标 (默认为 1)

-C n-c，相同报告结果在冗长的格式

-D 打印前每个输出行的时间戳

-e 显示经过的时间上返回数据包

-f 文件读取列表中的目标是从一个文件 (-意味着 stdin) (仅当没有-g 指定)

-g 生成目标列表 (仅当没有-f 指定)

(指定的开始和结束 IP 在目标列表中，或提供一个 IP 子网掩码)

(如: fping-g 192.168.1.0 192.168.1.255 或 fping-g 192.168.1.0/24)

-H n 设置 IP TTL (生存时间跃点)

-i n (在毫秒的时间内) 发送 ping 数据包之间的间隔 (默认为 25)

-我如果将绑定到特定的接口

-l 循环永远发送 ping 信号

-m ping 目标主机上的多个接口

-n 显示目标的名称 (-d 是等效)

-O n 设置的服务 (tos) 标志类型的 ICMP 数据包

-p n 间隔 ping 数据包到一个目标 (在毫秒的时间内)

(在循环和计数模式，默认值 1000年)

-q 安静 (不显示每个目标/每-平结果)

-Q n-q，相同但显示摘要每隔 n 秒钟

-r n 试次数 (默认 3)

-s 打印最终统计

-S 地址设置源地址

-t n 个人目标初始超时 (以毫秒的时间内) (默认 500)

-T n 忽略 (为了兼容 fping 2.4)

-u 显示是遥不可及的目标

-v 显示版本

要检查 (如果没有-f 指定) 的目标的目标列表

* 1. **实例：**

1.扫描局域网里面的ip地址：**fping -a -g** 起始ip 结束ip

计算机生成了可选文字:
无 线 局 域 网 适 配 器 
I Pu 6 
子 网 掩 
默 认 网 关 ． 
WLR N ： 
f e 8 ø ： ： d4e ： b2 f 2 ： 8 71 ： 9 7 c 3 
19 2 ． 16 8 ． 16 9 ． 1 ø5 
2 5 " " ø 

==>扫描这个局域网里面的ip（192.168.169.1~192.168.169.255）

重要 **方式一：**

**fping -a -g 192.168.169.1 192.168.169.254**

计算机生成了可选文字:
/ home/ dnt# fping 
-g 192. 168. 169. 1 
192. 168. 169. 1 
192. 168. 169. 105 
192. 168. 169. 105 
192. 168. 169. 105 
192. 168. 169. 105 
192. 168. 169. 105 
192. 168. 169. 105 
192. 168. 169. 105 
192. 168. 169. 105 
192. 168. 169. 254 
192. 168. 169. 9 
192. 168. 169. 8 
192. 168. 169. 7 
192. 168. 169. 6 
192. 168. 169. 5 
192. 168. 169. 4 
192. 168. 169.3 
192. 168. 169. 2 
1 CMP 
1 CMP 
1 CMP 
1 CMP 
1 CMP 
1 CMP 
1 CMP 
1 CMP 
Host 
Host 
Host 
Host 
Host 
Host 
Host 
Host 
Un reachable 
Un reachable 
Un reachable 
Un reachable 
Un reachable 
Un reachable 
Un reachable 
Un reachable 
f rom 
f rom 
f rom 
f rom 
f rom 
f rom 
f rom 
f rom 
for 
for 
for 
for 
for 
for 
for 
for 
1 CMP 
1 CMP 
1 CMP 
1 CMP 
1 CMP 
1 CMP 
1 CMP 
1 CMP 
Echo 
Echo 
Echo 
Echo 
Echo 
Echo 
Echo 
Echo 
sent 
sent 
sent 
sent 
sent 
sent 
sent 
sent 
0 
0 
0 
0 
0 
0 
0 
0 
192. 168. 169. 104 
192. 168. 169. 105 
192. 168. 169. 108 

解释：-a 存活地址 -g 指定的开始和结束 IP 或 指定 IP 子网掩码（192.168.169.0/24）

重要 **方式二：**

**fping -a -g 192.168.169.0/24**

计算机生成了可选文字:
/ home/ dnt# fping 
-g 192. 168. 169. 0/24 
192. 168. 169. 1 
192. 168. 169. 105 
192. 168. 169. 103 
192. 168. 169. 105 
192. 168. 169. 12 
192. 168. 169. 105 
192. 168. 169. 11 
192. 168. 169. 105 
192. 168. 169. 10 
192. 168. 169. 105 
192. 168. 169. 105 
192. 168. 169. 105 
192. 168. 169. 105 
192. 168. 169. 105 
192. 168. 169. 105 
192. 168. 169. 105 
192. 168. 169. 105 
Echo 
Echo 
Echo 
Echo 
Echo 
Echo 
Echo 
Echo 
Echo 
Echo 
Echo 
sent 
sent 
sent 
sent 
sent 
sent 
sent 
sent 
sent 
sent 
sent 
0 
0 
0 
0 
0 
0 
0 
0 
0 
0 
0 
192. 168. 169. 9 
192. 168. 169. 8 
192. 168. 169. 7 
192. 168. 169. 6 
192. 168. 169. 5 
192. 168. 169. 4 
192. 168. 169.3 
192. 168. 169. 2 
1 CMP 
1 CMP 
1 CMP 
1 CMP 
1 CMP 
1 CMP 
1 CMP 
1 CMP 
1 CMP 
1 CMP 
1 CMP 
Host 
Host 
Host 
Host 
Host 
Host 
Host 
Host 
Host 
Host 
Host 
Un reachable 
Un reachable 
Un reachable 
Un reachable 
Un reachable 
Un reachable 
Un reachable 
Un reachable 
Un reachable 
Un reachable 
Un reachable 
f rom 
f rom 
f rom 
f rom 
f rom 
f rom 
f rom 
f rom 
f rom 
f rom 
f rom 
for 
for 
for 
for 
for 
for 
for 
for 
for 
for 
for 
1 CMP 
1 CMP 
1 CMP 
1 CMP 
1 CMP 
1 CMP 
1 CMP 
1 CMP 
1 CMP 
1 CMP 
1 CMP 
192. 168. 169. 108 

得到ip后你可以先尝试一下：(99%失败，偶尔也会成功哦~后面会深入讲的)

* + Windows**：telnet ip地址**
  + Linux系列**：ssh root@ip地址**