lasthop说明文档

1.介绍

Lasthop能够对目标进行末跳发现。一共有三种方法获取末跳：

方法1：UDP大端口获取，仅对20%左右目标有效

方法2：二分法获取，对所有目标有效，平均发包5.1

方法3：步进法获取，对所有目标有效，平均发包4~6

* 工具位置：

10.10.11.130:/home/ly/nmap\_script/last\_hop/script/

Github: <https://github.com/yiqiaoxihui/last_hop/tree/master/script>

* 文件结构

**├── combine\_divide.lua //结合方法1，3**

**├── combine.lua //结合方法1，2**

**├── guess\_one\_step.lua //方法3，推荐使用**

**├── udp\_big\_port.lua //方法1**

**├── only\_binrary.lua //方法2**

**├── ping\_test.lua //无用**

**└── send.lua /无用**

* 使用方法

**nmap -sn -n -e eno2 --script 脚本名 目标 |tee result**

**示例1：nmap -sn -n -e eno2 --script guess\_one\_step.lua 76.103.255.142 |tee result**

**示例2：nmap -sn -n -e eno2 --script guess\_one\_step.lua -iL ip\_file |tee result**

注:每种方法原理在论文里详细描述

2.末跳发现输出结果result处理脚本

* 位置10.10.11.130/home/ly/fastrace\_nmap/python\_script/ extract\_lasthop\_result.py

Github:<https://github.com/yiqiaoxihui/fastrace_nmap/tree/master/python_script>

* 说明：末跳输出结果处理脚本，统计末跳获取量，写入文件
* 使用方法

例如：python extract\_combine.py result 1

参数 1：输入文件，realtest/ip.10w.combine为末跳初始原始数据

参数2：1表示统计末跳写入文件，0表示仅输出控制台，默认文件名在输入文件名后加”.lh”

