

一、实验简介

本实验主要针对于 nmap 工具的发现主机功能的使用。

二、实验环境

实验环境

主机系统: kali2023

IP 地址: x.x.x.x

用户名/密码:无

三、实验步骤

在 kali2023 里打开命令行界面, 输入 `nmap -h` 命令确定 nmap 可用。

```
(kali㉿kali)-[~]  
$ nmap -h 127  
Nmap 7.94SVN ( https://nmap.org )  
Usage: nmap [Scan Type(s)] [Options] {target specification}  
TARGET SPECIFICATION:  
  Can pass hostnames, IP addresses, networks, etc.  
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254  
  -iL <inputfilename>: Input from list of hosts/networks  
  -iR <num hosts>: Choose random targets  
  --exclude <host1[,host2][,host3], ...>: Exclude hosts/networks  
  --excludefile <exclude_file>: Exclude list from file  
HOST DISCOVERY:  
  -sL: List Scan - simply list targets to scan  
  -sn: Ping Scan - disable port scan  
  -Pn: Treat all hosts as online -- skip host discovery  
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports  
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes  
  -PO[protocol list]: IP Protocol Ping  
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]  
  --dns-servers <serv1[,serv2], ...>: Specify custom DNS servers  
  --system-dns: Use OS's DNS resolver  
  --traceroute: Trace hop path to each host
```

输入 `nmap -sP xxx.xxx.xxx.1/24`(任意网段地址, 如本机所在网段), 使用 ping 批量扫描对应网段存活主机。

(kali@kali)-[~]

\$ nmap -sP 172.16.15.1/24

Starting Nmap 7.94SVN (<https://nmap.org>) at 2023-12-15 10:01 CST

Nmap scan report for 172.16.15.1

Host is up (0.025s latency).

Nmap scan report for 172.16.15.2

Host is up (0.0012s latency).

Nmap scan report for 172.16.15.4

Host is up (0.0025s latency).

Nmap scan report for 172.16.15.5

Host is up (0.0024s latency).

Nmap scan report for 172.16.15.6

Host is up (0.0023s latency).

Nmap scan report for 172.16.15.7

Host is up (0.0022s latency).

Nmap scan report for 172.16.15.8

Host is up (0.0021s latency).

Nmap scan report for 172.16.15.14

Host is up (0.0016s latency).

Nmap scan report for 172.16.15.15