

一、实验简介

本实验主要针对于 nmap 工具的探测版本和系统的使用。

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 -sV xxx.xxx.xxx.xxx`(任意 ip 地址, 如本机), 扫描打开的端口以确定服务/版本信息

```
ES
(kali@kali)-[~]
└─$ nmap -sV 172.16.15.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-15 09:54 CST
Nmap scan report for 172.16.15.2
Host is up (0.0016s latency).
Not shown: 992 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.4 (protocol 2.0)
81/tcp    open  http         nginx
111/tcp   open  rpcbind      2-4 (RPC #100000)
2049/tcp  open  nfs_acl      3 (RPC #100227)
8080/tcp  open  http         Apache httpd
8089/tcp  open  unknown
8888/tcp  open  http         nginx
9090/tcp  open  tcpwrapped
```