KALI - 信息收集 - 二层扫描

原创

诔若 于 2019-09-24 10:14:21 发布 88 收藏

0x0 目的

发现本网段内的存活主机

0x1 协议

ARP

0x2 工具

arping、nmap、netdiscover、scapy

0x3 py脚本

```
#! /usr/bin/python
import logging
import subprocess
logging.getLogger("scapy.runtime").setLevel(logging.ERROR)
from scapy.all import *

if len(sys.argv) != 2:
    print "####################"
    print "usage ./arp.py eth0 "
    print "####################"
    sys.exit()

interface = str(sys.argv[1]) #get arguments
subnet = subprocess.check_output("ifconfig "+interface+" | grep 'netmask'|awk '{print $2}'|cut -d \".\" -f 4 --complement",shell=True).strip()+"." #excute system command
for host in range(1,254):
    re_packet=sr1(ARP(pdst=subnet+str(host)),timeout=0.1,verbose=0)
    if re_packet != None:
        print subnet+str(host)
```

0x4 shell脚本

```
#! /bin/bash

if test $# -ne 1
then
echo "###############";
echo "#./arping eth0#"
echo "###############";
exit
fi
```

```
interface=$1
eth=`ifconfig $interface`
subnet=$(echo $eth | awk '{print $6}'|cut -d "." -f 4 --complement)"."
echo "subnet ==> $subnet0";
echo "Let's start scan!"
echo "================="
for host in `seq 1 254`
do
arping $subnet$host -c 1 | grep 'bytes from'|awk '{print $5}' | awk -F ')' '{print $1}'| cut -d '(' -f 2 >> /root/Desktop/shell/ip.txt
done
cat /root/Desktop/shell/ip.txt
echo "=====end====="
```