Zitian Yue

1. Passive information gathering

I picked the domain mihoyo.com to investigate. Its IP address is 139.224.19.81. The domain's registration expires on 2024-02-09 T11:59:59Z. I found that the eName Technology Co., Ltd is the registrar of this domain created on 2011-02-20 T14:04:29Z. The registrant country is China, and the registrant state is Shanghai. The Domain Status suggests that this domain can be neither deleted nor transferred to another registrar.
It should be noted that this IP address range is not registered in the ARIN database but in the APNIC (Asia Pacific Network Information Centre) Whois Database. The IP address belongs to Aliyun Computing Co., LTD, located in China. It is under the supervision of the China Internet Network Information Center. I also found three names, Li Jia, Guoxin Gao, and Guowei Pan, related to this domain. Information like addresses and phone numbers are provided. Guowei Pan might be the founder since the last-modified date is the earliest for him.

2. Host detection

The IP addresses for active hosts I found on the local network are:

- 192.168.124.2: Two packets of TCP protocols were firstly sent to this IP address from the address of my network interface. It then sent two packets of TCP protocols with [RST, ACK] to end the TCP transmission. Finally, my network interface sent a packet of DNS protocol to this IP address and received another packet of DNS protocol containing information about this host.
- 192.168.124.128: Since this host has the same IP address as my network interface, only packets of DNS protocols were transmitted. My network firstly sent a DNS protocol to this address and received a DNS protocol containing information about this host in response.

- 192.168.124.129: Six packets of TCP protocols were transmitted before the exchange of DNS protocols between my network interface and this host. My network interface first sent two TCP protocols to this IP address and received two TCP protocols. It then sent back two packets of TCP protocols to confirm the acknowledgment and reset. After that, DNS protocols were transmitted between my network interface and this host to acquire information about the host.

These IP addresses represent the possibilities of my computer's connection to other systems through the internet. 192.168.124.129 represents the Metasploitable2 which is running in the background.

The IP address for active hosts I found on the Math/CS network are:

- 137.22.4.5: Eight packets of TCP protocols were transmitted between my computer interface and this host. My computer interface sent two TCP protocols to this IP address and then received one TCP protocol. This process is then repeated again until my computer interface sent the last two packets of TCP protocols to confirm the acknowledgment and reset. After that, DNS protocols were transmitted between IP addresses 192.168.124.128 and 192.168.124.2 to acquire information about the host at this IP address.
- 137.22.4.17: My computer interface firstly sent two packets of TCP protocols to this host and received one TCP protocol in return. It then sent another two TCP protocols to request the acknowledgment. Then DNS protocols were transmitted between IP addresses 192.168.124.128 and 192.168.124.2 to acquire information about the host at this IP address. After that, this host sent a packet of TCP protocol to my computer interface to confirm the acknowledgement and reset.
- 137.22.4.131: My computer interface firstly sent two packets of TCP protocols to this host and received one TCP protocol in return. It then sent another two TCP

protocols to request the acknowledgment. Then my computer interface sent one packet of DNS protocol to the IP address 192.168.124.2. After that, this host sent one packet of TCP protocol to conform to the acknowledgment. Next, my computer interface sent the last TCP protocol to this host to confirm the reset. Finally, my computer interface received a packet of DNS packet from the IP address 192.168.124.2 to acquire information about the host at this IP address.

These IP addresses represent the possibilities of the Math/CS network's connection to other systems through the internet.

3. Port scanning

The open ports for the Metasploitable are port 21/FTP; port 22/SSH; port 23/TELNET; port 25/SMTP; port 53/DOMAIN; port 80/HTTP; port 111/RPCBIND; port 139/ NETBIOS-SSN; port 445/MICROSOFT-DS; port 512/EXEC; port 513/LOGIN; port 514/SHELL; port 1099/RMIREGISTRY; port 1524/INGRESLOCK; port 2049/NFS; port 2121/ CCPROXY-FTP; port 3306/MYSQL; port 5432/POSTGRESQL; port 5900/VNC; port 6000/X11; port 6667/IRC; port 8009/AJP13; port 8180/unknown.

The database servers that are available on Metasploitable are the FTP server and the IRC server. The value of the RSA SSH host key is 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3. The host key is regarded as the public key for this host. Therefore, recipients can utilize this key to retrieve information from messages sent from the server encrypted by its secret key. Its purpose is to authenticate the identity of the systems you are trying to connect.

Port 6667 provides the service of Internet Relay Chat (IRC). It is implemented as an application layer protocol for instant messaging. It facilitates group communications in the form of text.