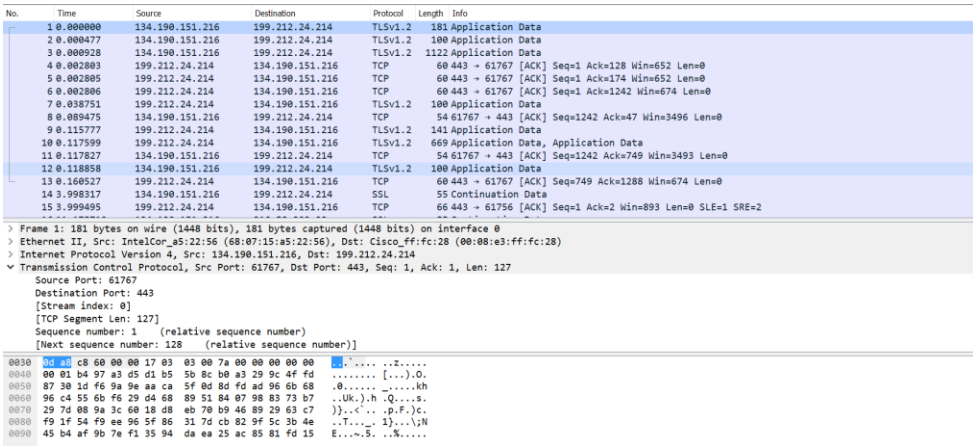
Assignment 1

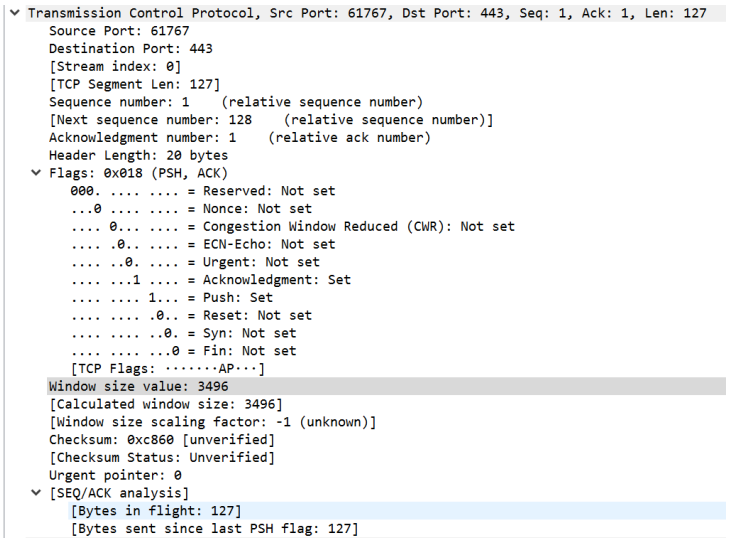
Zehao Ba(B00732676)

1. Experimental study of Wireshark

   Wireshark capture of www.google.ca



TCP Segment:



0 15 16 31

Source port number:61767								Destination port number:443
Sequence number:1								
Acknowledgement Number:1								
Header length : 20	Reserved: Not set	Urg: Not set	Ack: set	Psh: set	Rst: Not set	Syn: Not Set	Fin: Not Set	Window size: 3496
TCP checksum = 0xc860								Urgent pointer: 0
TCP Segment data = 127 bytes								

Urg=urgent, Ack=acknowledgment, Psh=push, rst=Reset

IP header:

```
Internet Protocol Version 4, Src: 134.190.151.216, Dst: 199.212.24.214
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 167
    Identification: 0x261c (9756)
  Flags: 0x02 (Don't Fragment)
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0x14f4 [validation disabled]
    [Header checksum status: Unverified]
    Source: 134.190.151.216
    Destination: 199.212.24.214
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

0 16 31

<table>
<tr><td>IP version:4</td><td>Header Length: 20 bytes</td><td>Type of service: 0x00</td><td colspan="4">Total length: 167</td></tr>
<tr><td colspan="3">Identification: 0x261c</td><td>R: not set</td><td>DF: set</td><td>MF: not set</td><td>Fragment Offset: 0</td></tr>
<tr><td>Time-to-live:64</td><td colspan="2">Protocol: TCP(6)</td><td colspan="4">Header Checksum: 0x14f4</td></tr>
<tr><td colspan="7">Source IP Address: 134.190.151.216</td></tr>
<tr><td colspan="7">Destination IP Address: 199.212.24.214</td></tr>
</table>

R: Reserved bit, DF: Don’t fragment, MF: more fragment

Ethernet Header:

```
Ethernet II, Src: IntelCor_a5:22:56 (68:07:15:a5:22:56), Dst: Cisco_ff:fc:28 (00:08:e3:ff:fc:28)
  Destination: Cisco_ff:fc:28 (00:08:e3:ff:fc:28)
      Address: Cisco_ff:fc:28 (00:08:e3:ff:fc:28)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: IntelCor_a5:22:56 (68:07:15:a5:22:56)
      Address: IntelCor_a5:22:56 (68:07:15:a5:22:56)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
```

Destination Address: 00:08:e3:ff:fc:28	Source Address: 68:07:15:a5:22:56	Type: IPv4 (0x0800)	DATA

Ethernet trailer:

```
0000  00 08 e3 ff fc 28 68 07  15 a5 22 56 08 00 45 00   .....(h. ..."V..E.
0010  00 a7 26 1c 40 00 40 06  14 f4 86 be 97 d8 c7 d4   ..&.@.@. ........
0020  18 d6 f1 47 01 bb 74 65  bf 60 ee 5c 5e b4 50 18   ...G..te .`.\^.P.
0030  0d a8 c8 60 00 00 17 03  03 00 7a 00 00 00 00 00   ...`.... ..z.....
0040  00 01 b4 97 a3 d5 d1 b5  5b 8c b0 a3 29 9c 4f fd   ........ [...).O.
0050  87 30 1d f6 9a 9e aa ca  5f 0d 8d fd ad 96 6b 68   .0...... _.....kh
0060  96 c4 55 6b f6 29 d4 68  89 51 84 07 98 83 73 b7   ..Uk.).h .Q....s.
0070  29 7d 08 9a 3c 60 18 d8  eb 70 b9 46 89 29 63 c7   )}..<`.. .p.F.)c.
0080  f9 1f 54 f9 ee 96 5f 86  31 7d cb 82 9f 5c 3b 4e   ..T..._. 1}...\;N
0090  45 b4 af 9b 7e f1 35 94  da ea 25 ac 85 81 fd 15   E...~.5. ..%.....
00a0  d3 6b ab ab 4f ec d7 45  3b 44 a1 0b ec da 8c 99   .k..O..E ;D......
00b0  2e 47 c2 13 bb                                    .G...
```

Application layer:

```
▾ Secure Sockets Layer
  ▾ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 26
      Encrypted Application Data: 0000000000000004a525a8f9b4176b8d2cc89b032b3ee33b...
```

Application layer protocol: TLS/SSL

2. Exploratory of Metasploit
   - Tool features

     The metasploit frame is written by Perl, a scripting language, including vary parts that are written in C, assembler and Python. The most important part of metasploit framework is the dual-licenses, which is allowed the framework to be used in open-source and other commercial area. The elementary attacks of metasploit are based on the following basis. The first one is choose an exploit and construct it. The second one is check the awareness. Third, choose a payload and construct it. Forth, choose an encoding scheme. The last one is implement the exploit. It can work in two methods, the first one is using command-line, or you can also use multiple sessions by a web server [3].

     The major part of metasploit is the exploits. There is another important module named auxiliary. The auxiliary exists in the Metasploit without a payload, it is more like a accessory which can help the framework to be extended [1].

     For payloads, it remains in each exploit. The payload is selected to execute the order after the exploit is initiated, no matter the target is remote or not. The payload is decided by Operating System [1]. There are three payload types in Metasploit, singles, stagers and stages [2]. Singles means the payloads are independent of any users, and they can do any modification. For example, add a new user into the target system. Stagers just make a small but reliable part of delivery connection because there is a trade-off between connection limitation and connection reliable. Stages is the final part of the stagers which can be used as a deploy of the stager. In summary, payloads can be used on posting the exploitations and making sure the attacker and victims' connection are encrypted, such as hash or salt [1].

- What it provides
  At the beginning, Metasploit is provided as a framework which allows penetration testers to do the exploits, payloads, and for surveillance purposes. According to the internet development, it becomes the security tools of designing and developing the surveillance, and doing exploitation. Now, the metasploit framework becomes a tool to collect exploits to a central location, generally speaking, a security researcher's location. The metasploit framework makes the security researchers work better and easier. Originally, the users of metasploit are network security experts, product vendors, security analysts and other security scientists. The primary users can use the metasploit framework to do the penetration testing, installation authentication or exploits developments [4].

- How it works
  The first step of penetration test is gathering and scanning the information. The user can use any method to collect the information. The target can be a website, an organization or an investment company. You can use the tradition way or use social media to find target information. Foot printing is also an efficient way. Get known of your target makes the tester to find a proper and accuracy attack approach, which can reduce the penetrate time. This step costs 40% to 60% time, it decides whether the penetrate is success or not. Besides, it should be clear of the security measures of deploy and how to destroy the measures. The network stress testing tool can help us to evaluate our internet [4].
  The second step is operating system-based vulnerability assessment. This step makes sure we can do the penetrate testing successfully. In this step, the primary task is stimulating the threat and analyzing how the threat will work, the influences of the threats and classify them. We can find the best way to attack in this step.
  The third step is analyzing the exploit. It indicates the process of finding the exploit of the application. The exploits are varied from server configuration to web application server. This process including three different systems, testing, verifying and researching. Testing is divided into positive testing and negative testing; verifying including discard the mistake and verify the exploits manually; researching means find the exploits and verify it [4].
  The third step is penetration attack and further penetration attack. It is the real attack process. During this process, the penetration tester can get the controlling by using chunk to attack the target system exploit.
  The last step is report. Creating penetration test report is the last step of the penetration test. The report should be including four parts. The primary thing is find the most important threat; and then generate the table and charts based on the data from the penetration test; next, give the suggestion of the target system; finally, find the solution of these suggestion [4].

- Why is useful to network security specialist

The metasploit framework is useful because it can keep the security of network. The exist of metasploit framework makes the network security experts, analyzer and researchers work easier. The network security manager use metasploit framework to do the penetration test so that the network defense module is working well; the product vendors use metasploit framework to do the regression test so that they can evaluate the recovery function of the network; the security administrator use it to do the patch installation verification; and the network security researchers can also use it to do some research of exploits [2].

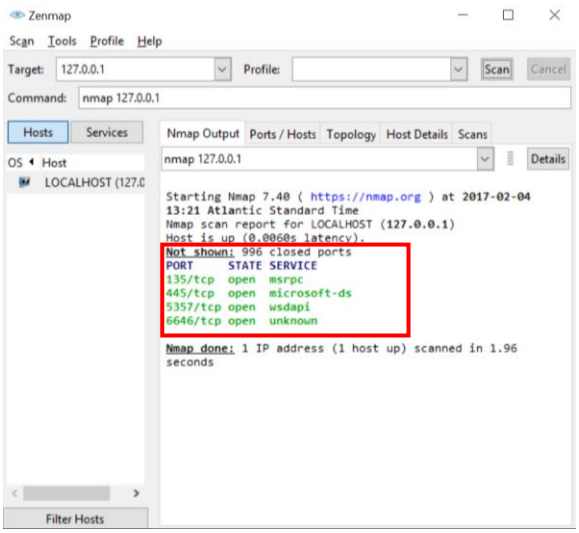
- How it may be used for harmful purposes by a hacker
  The hackers can use metasploit framework payload generate the relevant backdoor application, then hackers can go to the category and modify the property. More specific, to make the system allow to execute some file. The hacker will open metasploit framework console and load the handler module to make setting for local host. After that, they can do eavesdropping. Also, they can copy the files to the target local host and execute the files. Based on the above attack, the hacker can back connect the metasploit framework by the backdoor application, and use metasploit framework to attack the local host again. Here is a new terminology, meterpreter. The meterpreter is an extension of metasploit framework, if the meterpreter overload, the hacker can attack the payload.

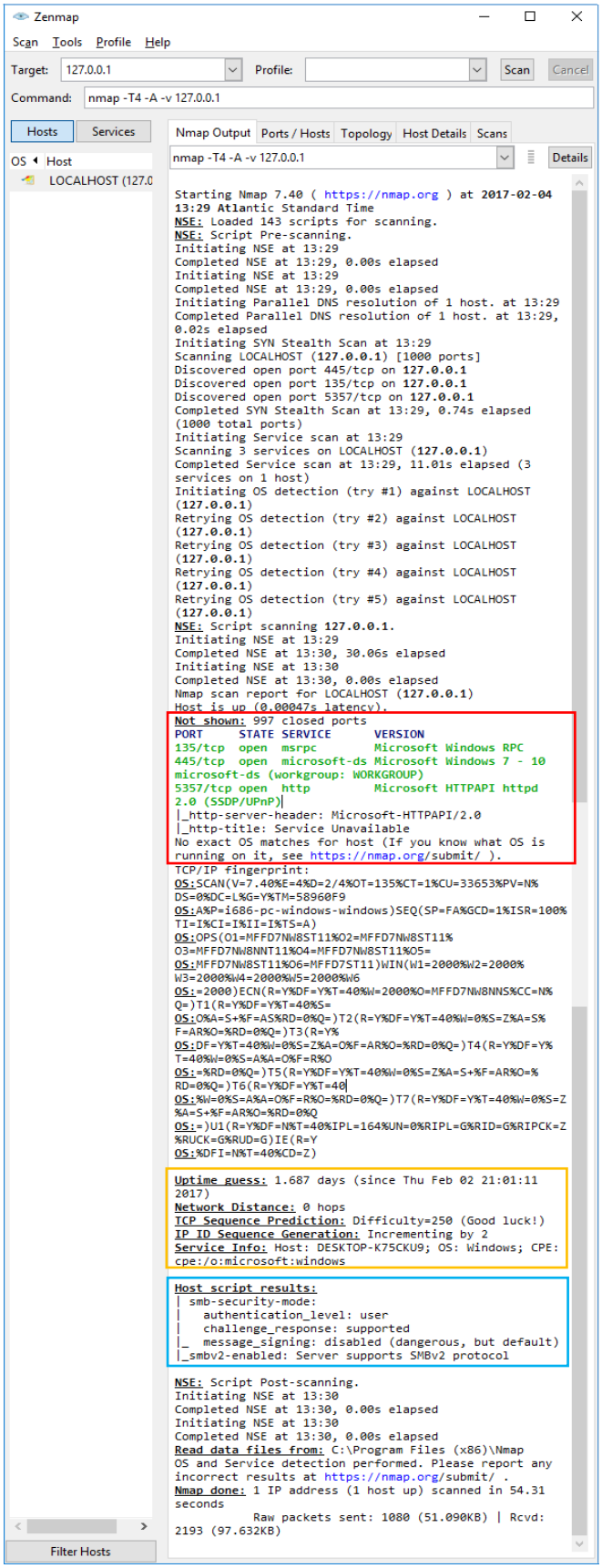
3. Experimentation of zenmap/nmap

Nmap is one of network discovery and security auditing tool. Nmap is network mapper, to monitor whether the target host is turn on or not, the situation of the host, probe the service type, operating system, and other services' information [5].

- Target host situation

From this snapshot, we can find the whole port of the loopback address and the ports' state, services.



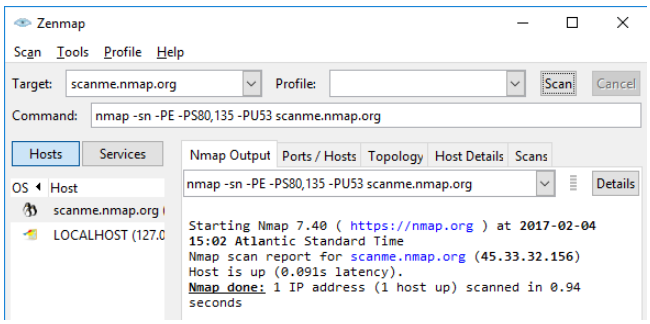


I did the thorough scan for the loopback address and found the information as followed (see the left snapshot): scan the host and port, version detection, and operating system detection. '-T4' is setting the timing template, the higher value, the faster scanning it is; '-A' uses to do the OS detection, version detection, script scanning, and traceroute; '-v' increases the verbosity level, which can show the details during the scanning. From the red circle, we can found there are 997 closed ports and three open ports because the Nmap default to scan 1000 ports which are the most probable open; While the orange square shows the version detection, and the application and version of the running ports; The blue square is the information intelligence based on using the NSE script on Nmap [6].

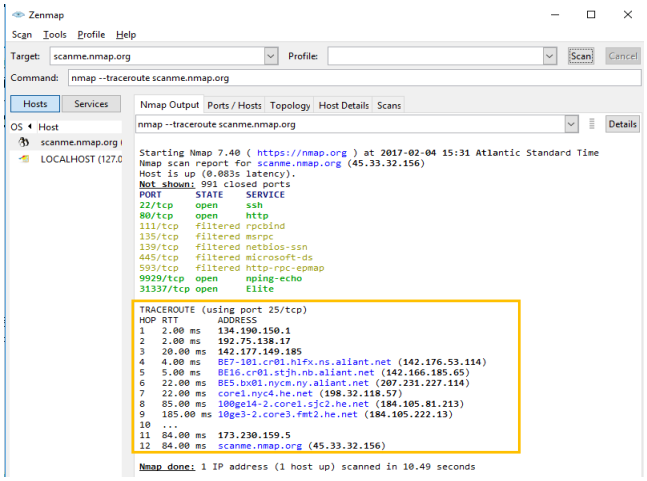
Basically, there are four functions of Nmap, host discovery, port scanning, version detection and operating system detection [5].

- Host discovery

  The host discovery aims to find whether the host is alive. It is similar to the Ping command. It sends the detection packet to the target host, if the host responses, which means the host is alive. There are multiple ways to do the detection, such as send ICMP ECHO request, TCPSYN/ACK packet, SCTP INIT/COOKIE-ECHO packet, etc.

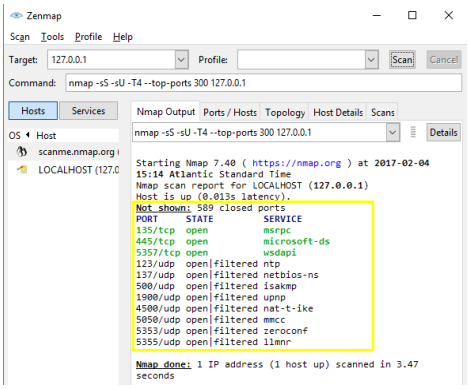


This figure is the host discovery experiment to www.nmap.org. I used the command 'nmap -sn -PE -PS80,135 -PU53 scanme.nmap.org' and found the host is alive. '-sn' means Ping Scan, which indicates only do the host detection but not scan the port; '-PE' means use the OCMP echo, timestamp, and netmask request packet to detect the host; '-PS80' is use TCPSYN to detect [6].



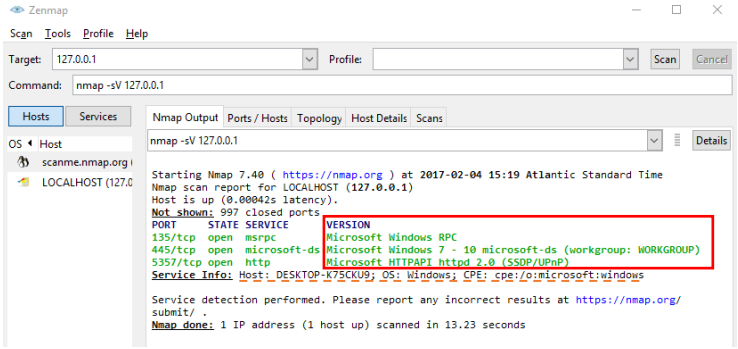
I used '--traceroute' command to trace every router, and get the information of traceroute, including hop, RTT and the addresses.

- Port scanning



Then I did the port scanning on my host. There are six situations of the port, open, closed, filtered (shielded by the firewall and can not see the status), unfiltered (the port is unshielded but needs to be decided), open|filtered (open and shielded) and closed|filtered (closed and unshielded) [6]. According to the above figure, it can be found the closed and open ports and their services. In the command, '-sS' menas we use TCP/SYN method to scan the TCP ports; '-Su' indicates we scan UDP port; '-top-ports 300' means we scan 300 the most probable open ports.

- Version detection



We can found there are 997 ports are closed, and Nmap detect the three-open port's version. The information in the red square it the version information of the ports. Besides, the Nmap detect the Microsoft service from the application, therefore, it refers we use Windows operating system. '-sV' in the command line means do the version detection.

4. Exploratory of DDoS attack

Dyn is an international performance management company. The main business of Dyn is dealing with the online infrastructure, including control, monitor, and optimize it. Besides, they also handle the domain registration service, like a web addresses book of the internet [7]. On October 21th, 2016, there was a DDoS attack aimed at Managed DNS infrastructure at Dyn. The Dyn's network operations center met the attacks too much time, however, they found this time is different. The attack was lasted for two hours, a second attack was launched. The customer can not use the Dyn's server on the East Coast of the US to some sites. The servers are stopped because of a flood of malicious requests which came from millions IP addresses. It was an attack that Dyn have never experienced. Dyn said that this attack is a sophisticated and complex one. In fact, the attack began on September 20th, 2016. The volume of network traffic reached to 655Gbps suddenly, it is called the largest attack [8]. The fastest attack which is recorded earlier is 600 Gig, it attacked against Donald Trump's website.

Mostly, the DDoS attack use botnet to send big volumetric requests to server by running certain vulnerable programs, for example, DNS, to generate millions addresses that match the target. The request messages are legitimate and the responses are considerably larger than the original one. Once the amplified response is sent to the target, the server will down because of the overwhelmed traffic [8]. Dyn DNS has a wide range of websites and services. The attack at Dyn company caused millions of IP addresses down in 10 seconds. They observed that Mirai botnet is one of the main part of this attack [7].

In this attack, the main players are not the traditional PCs but the internet-connected devices. They are called Internet of Things(IoT), such as routers, intelligence devices, etc. However, little of them have security protection and they become the target of the hackers. Also, the IoT devices is one of the most important part in Dyn's attack. In Dyn's case, the Mirai botnet is the main weapon, which is difference as before [9]. The attack continue strength is 1.2TBps, which is twice as any previous DDoS attack.

Mirai is a malware which constantly scan the vulnerable IoT services of the internet. Once the Mirai infects the services, it will report the command to the control server so that the service can be one part of the botnet [9]. If the IoT services want to get rid of the malware, only turn it off and restart again as usual will not work unless the user change the password, or the devices will be infected again. Basically, the botnets are only had weak password. The botnet scan and find the vulnerable devices, try to exploit the device. Now, the Mirai botnet is one of the most frequently attack because the source code for Mirai has already been posted. The hacker said they are capability to build botnets to 380,000 devices within a security community, by exploiting telnet connection. However, it is considerably difficult to find a solution to defense our devices. Right now, the internet service provider has already shut down almost 300,000 bots, but there is still a long way to go [8].

There are approximately 100,000 devices participated in the Dyn's attack, however, the reality is Mirai botnet forged source IP addresses and camouflaged million devices to attack the Dyn server. It is hard to say who should response for this attack, some network security experts believe that the most probability is 'script kiddies' from hacktivism groups [10].

The motivation of the DDoS attacker is public nature, it is the most frequent type of attack. When the network is down, people become panic, the report and tweet about it. A classic scenario is the attackers intrude the website before the important event, and then ask for

money. Extortion appeals the attackers to do the gambling. In 2014, there is a group named DD4BC (which means the DDoS for Bitcoin), they targeted several companies of online game currency exchanges. The DD4BC proved their ability by did a small attack, and then ask money to the company or they will operate a bigger attack. A lot of companies gave the ransom because they would not allow their network server to stop, or they would loss much. However, it is proved that the DD4BC can not operate so much volume, which means they are not able to achieve a bigger attack. But this news reflects the attitude of this companies at that time [8].

In the Dyn case, they shaped the incoming network traffic, employed the anycast policies, internal filter application, deployed the scrub services to rebalanced the traffic. After took these measures, the attack subsided [7]. If we want to prevent this kind of attacks, the first step is to aware where the attack it is. The company awareness of protecting their server has already raised, which is a good phenomenon. However, when people are attacked by Mirai botnet, they will not consider about the influence of the traffic, which increases the difficulty of mitigate the attack. The Arbor Network reports indicate that there are several categories of DDoS attack, including “SYN-flooding, Valve Source Engine query flooding, GRE-flooding, ACK-flooding, pseudo-random DNS label-prepending attacks” [8]. Although there is no updated DDoS attack, but it is flexible system and can launch tremendous DDoS attack. It is hard to prevent because of its high-volume endpoints to generate the traffic.

The position of put the DDoS mitigation is an essential problem. Generally, we put the mitigation at the edge of the network. However, it is not so efficient because of the perimeter dissolves and the increase of cloud services. Moving the protection to the cloud or pushing it to the further upstream are good solutions. A firewall, DDoS protection and other protections to deal with different attack types so that build the network defences. The weakest part in the network is the bandwidth, which decides the datacentre of the pipe. We put the hardware appliance to the cloud, which mitigates most attacks the network itself. Nevertheless, if the attack is unusual, the cloud-based solution will cost a lot. Therefore, the cloud-based solutions usually update depends on the demand. The demands can be evaluated by the time of updating the cloud and the quality you use. A mix solution is the common method, which can not only finish the basic protection, but also pay attention on the non-volumetric intrusion. But the based-cloud is not the solution for all problems because you still connect the internet. There is a tool named Cloud Piercer, which helps attackers to identify the real server IP address that hided behind the cloud server. The attackers can find the address and fudge the cloud protection by identifying the hard-code IP addresses [8].

In summary, the DDoS protection is like the insurance of the network, which the risk and cost are exist at the same time. It is considerably essential to evaluate the network and financial situation. Ideally, the DDoS protection is the prior thing which should be considered before anything, so that the attack will occur with less probability. The company usually treat the DDoS protection as a technical problem to solve. A DDoS mitigation solution can free up some of network security engineers during the attack so that they can concentrate on other issues because the mitigation solution can cover at least one aspect. Connecting the DDoS solutions with threat intelligence to accelerate the defences’ efficiency.

Reference

[1] C. McNab, Network security assessment: know your network, Sebastopol: O'Reilly Media, Inc., 2007.

[2] C. J. Marquez, “An analysis of the ids penetration tool: Metasploit.,” *The InfoSec Writers Text Library,* 2010.

[3] M. Unleashed, “Main_Page,” [Online]. Available: http://www. offensive-security. com/metasploitunleashed. [Access: 26 January 2014].

[4] D. Maynor, Metasploit toolkit for penetration testing, exploit development, and vulnerability research, Burlington: Elsevier, 2011.

[5] P. Girdhar, "Design of tool to monitor and capture packets," *Journal of Network Communications and Emerging Technologies (JNCET),* vol. 6, no. 9, pp. 14-15, 2016.

[6] G. Lyon, “Nmap network scanning,” Insecure.Com LLC, [Online]. Available: https://nmap.org/book/man-briefoptions.html.

[7] “Dyn Statement on 10/21/2016 DDoS Attack | Dyn Blog,” Dyn, 2017. [Online]. Available: http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/.

[8] S. Mansfield-Devine, “DDoS goes mainstream: how headline-grabbing attacks could make this threat an organisation's biggest nightmare,” *Network Security ,* volume 2016, issue 11, pp. 7-13, 2016.

[9] M. Castelluccio, “THE MOST NOTORIOUS HACKS OF 2016,” *Strategic Finance ,* volume 98, issue 7, pp. 55-56, 2017.

[10] M. Mimoso, “ThreatPost,” 25 October 2016. [Online]. Available: https://threatpost.com/dyn-ddos-work-of-script-kiddies-not-politically-motivated-hackers/121537/. [Access: 25 October 2016].