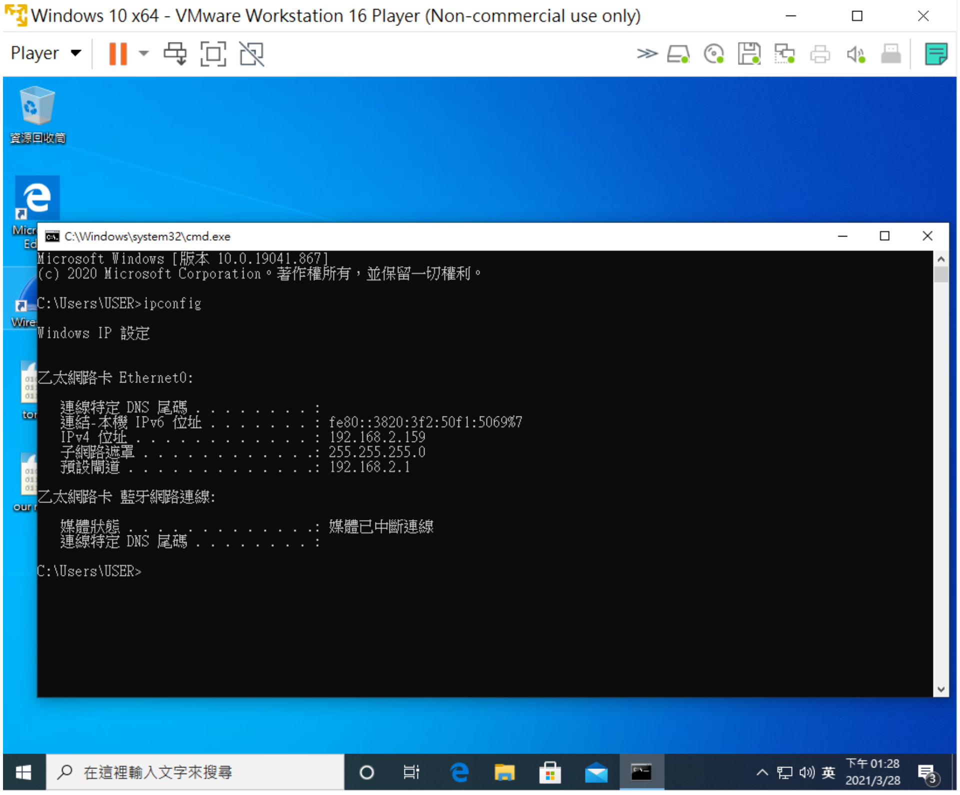
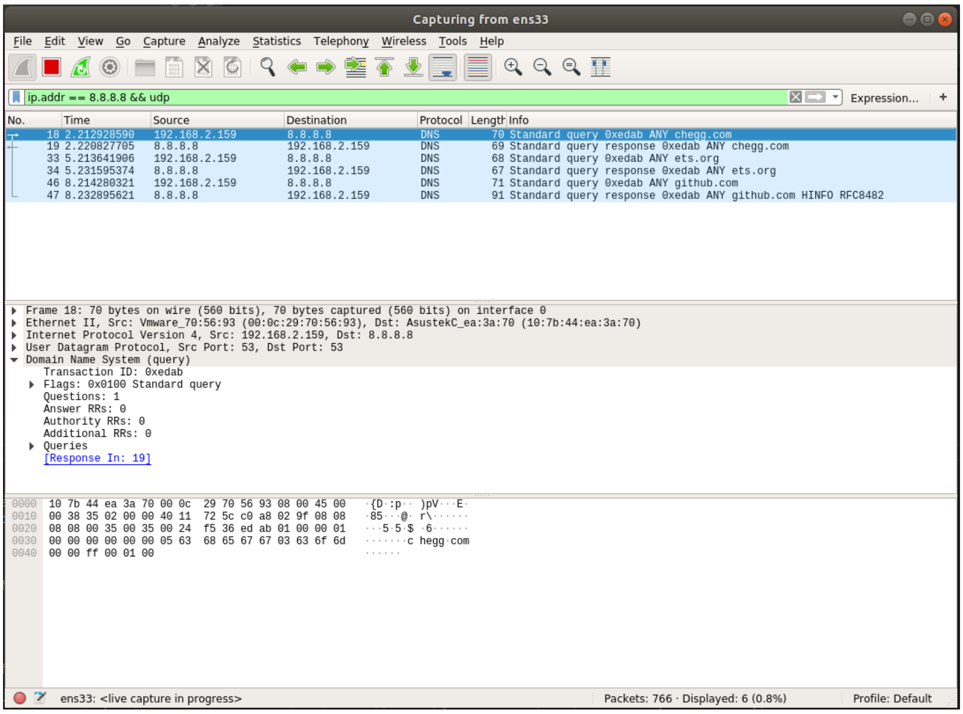
Computer Security Capstone Homework 1 Report

- Part 1 : Snapshot of creating ip spoofing packets and DNS query message


Windows 10 x64 - VMware Workstation 16 Player (Non-commercial use only)
Player
資源回收筒
C:\Windows\system32\cmd.exe
在這裡輸入文字來搜尋
英
下午 01:28
2021/3/28

```
Microsoft Windows [版本 10.0.19041.867]
(c) 2020 Microsoft Corporation。著作權所有，並保留一切權利。

C:\Users\USER>ipconfig

Windows IP 設定


乙太網路卡 Ethernet0:

   連線特定 DNS 尾碼 . . . . . . . . :
   連結-本機 IPv6 位址 . . . . . . . : fe80::3820:3f2:50f1:5069%7
   IPv4 位址 . . . . . . . . . . . . : 192.168.2.159
   子網路遮罩 . . . . . . . . . . . .: 255.255.255.0
   預設閘道 . . . . . . . . . . . . .: 192.168.2.1

乙太網路卡 藍牙網路連線:

   媒體狀態 . . . . . . . . . . . . .: 媒體已中斷連線
   連線特定 DNS 尾碼 . . . . . . . . :

C:\Users\USER>
```


Capturing from ens33
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

ip.addr == 8.8.8.8 && udp

```
No.   Time          Source          Destination     Protocol Length Info
   18 2.212928590   192.168.2.159   8.8.8.8         DNS      70 Standard query 0xedab ANY chegg.com
   19 2.220827705   8.8.8.8         192.168.2.159   DNS      69 Standard query response 0xedab ANY chegg.com
   33 5.213641906   192.168.2.159   8.8.8.8         DNS      68 Standard query 0xedab ANY ets.org
   34 5.231595374   8.8.8.8         192.168.2.159   DNS      67 Standard query response 0xedab ANY ets.org
   46 8.214280321   192.168.2.159   8.8.8.8         DNS      71 Standard query 0xedab ANY github.com
   47 8.232895621   8.8.8.8         192.168.2.159   DNS      91 Standard query response 0xedab ANY github.com HINFO RFC8482
```

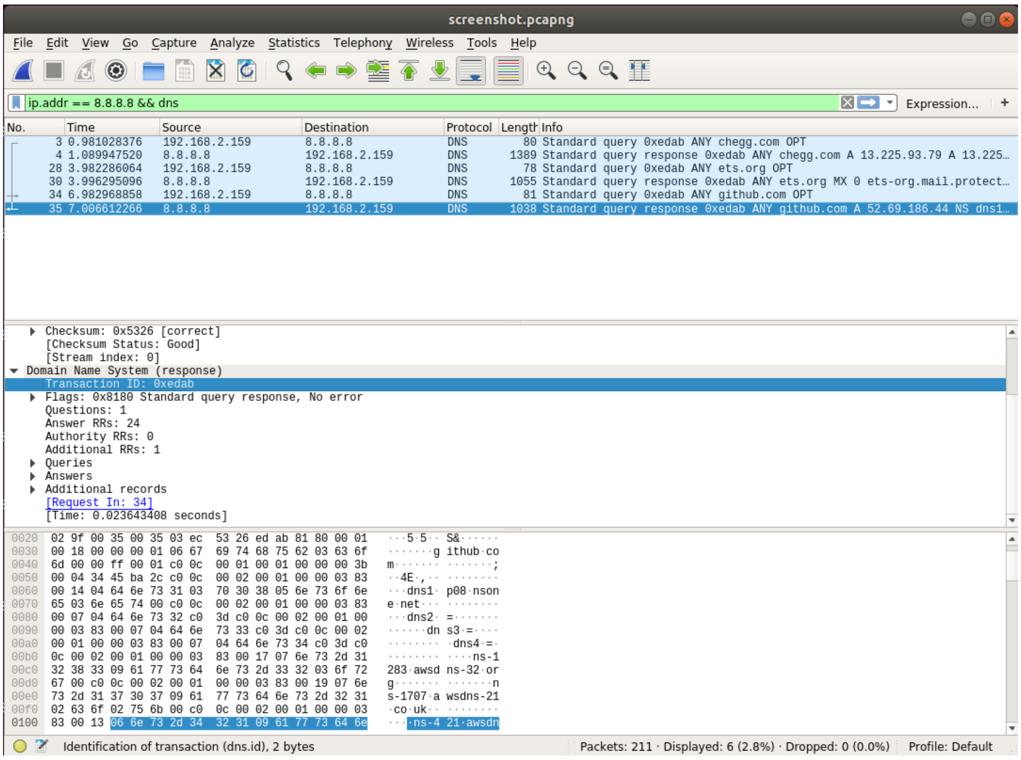
```
▸ Frame 18: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
▸ Ethernet II, Src: Vmware_70:56:93 (00:0c:29:70:56:93), Dst: AsustekC_ea:3a:70 (10:7b:44:ea:3a:70)
▸ Internet Protocol Version 4, Src: 192.168.2.159, Dst: 8.8.8.8
▸ User Datagram Protocol, Src Port: 53, Dst Port: 53
▾ Domain Name System (query)
     Transaction ID: 0xedab
   ▸ Flags: 0x0100 Standard query
     Questions: 1
     Answer RRs: 0
     Authority RRs: 0
     Additional RRs: 0
   ▸ Queries
     [Response In: 19]
```

```
0000  10 7b 44 ea 3a 70 00 0c  29 70 56 93 08 00 45 00   ·{D·:p·· )pV···E·
0010  00 38 35 02 00 00 40 11  72 5c c0 a8 02 9f 08 08   ·85···@· r\······
0020  08 08 00 35 00 35 00 24  f5 36 ed ab 01 00 00 01   ···5·5·$ ·6······
0030  00 00 00 00 00 00 05 63  68 65 67 67 03 63 6f 6d   ·······c hegg·com
0040  00 00 ff 00 01 00                                  ······
```

ens33: <live capture in progress>   Packets: 766 · Displayed: 6 (0.8%)   Profile: Default

- ○ Victim’s ip is 192.168.2.159
- ○ We spoofed the victim’s ip as the sender and send a DNS query to google.com
- ○ Google server replies to the victim
- ○ The responding packet size isn’t large enough
- ○ Snapshot of task 2 is in part 2

- Part 2 : How we amplify the DNS response


screenshot.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression… +

```
ip.addr == 8.8.8.8 && dns
```

```
No.   Time         Source          Destination     Protocol Length Info
    3 0.981028376  192.168.2.159   8.8.8.8         DNS        80 Standard query 0xedab ANY chegg.com OPT
    4 1.089947520  8.8.8.8         192.168.2.159   DNS      1389 Standard query response 0xedab ANY chegg.com A 13.225.93.79 A 13.225…
   28 3.982286064  192.168.2.159   8.8.8.8         DNS        78 Standard query 0xedab ANY ets.org OPT
   30 3.996295096  8.8.8.8         192.168.2.159   DNS      1055 Standard query response 0xedab ANY ets.org MX 0 ets-org.mail.protect…
   34 6.982968858  192.168.2.159   8.8.8.8         DNS        81 Standard query 0xedab ANY github.com OPT
   35 7.006612266  8.8.8.8         192.168.2.159   DNS      1038 Standard query response 0xedab ANY github.com A 52.69.186.44 NS dns1…
```

```
    ▶ Checksum: 0x5326 [correct]
      [Checksum Status: Good]
      [Stream index: 0]
  ▼ Domain Name System (response)
      Transaction ID: 0xedab
    ▶ Flags: 0x8180 Standard query response, No error
      Questions: 1
      Answer RRs: 24
      Authority RRs: 0
      Additional RRs: 1
    ▶ Queries
    ▶ Answers
    ▶ Additional records
      [Request In: 34]
      [Time: 0.023643408 seconds]
```

```
0020  02 9f 00 35 00 35 03 ec  53 26 ed ab 81 80 00 01   ···5·5·· S&······
0030  00 18 00 00 00 01 06 67  69 74 68 75 62 03 63 6f   ·······g ithub·co
0040  6d 00 00 ff 00 01 c0 0c  00 01 00 01 00 00 00 3b   m······· ·······;
0050  00 04 34 45 ba 2c c0 0c  00 02 00 01 00 00 03 83   ··4E·,·· ········
0060  00 14 04 64 6e 73 31 03  70 30 38 05 6e 73 6f 6e   ···dns1· p08·nson
0070  65 03 6e 65 74 00 c0 0c  00 02 00 01 00 00 03 83   e·net··· ········
0080  00 07 04 64 6e 73 32 c0  3d c0 0c 00 02 00 01 00   ···dns2· =·······
0090  00 03 83 00 07 04 64 6e  73 33 c0 3d c0 0c 00 02   ······dn s3·=····
00a0  00 01 00 00 03 83 00 07  04 64 6e 73 34 c0 3d c0   ········ ·dns4·=·
00b0  0c 00 02 00 01 00 00 03  83 00 17 07 6e 73 2d 31   ········ ····ns-1
00c0  32 38 33 09 61 77 73 64  6e 73 2d 33 32 03 6f 72   283·awsd ns-32·or
00d0  67 00 c0 0c 00 02 00 01  00 00 03 83 00 19 07 6e   g······· ·······n
00e0  73 2d 31 37 30 37 09 61  77 73 64 6e 73 2d 32 31   s-1707·a wsdns-21
00f0  02 63 6f 02 75 6b 00 c0  0c 00 02 00 01 00 00 03   ·co·uk·· ········
0100  83 00 13 06 6e 73 2d 34  32 31 09 61 77 73 64 6e   ····ns-4 21·awsdn
```

```
Identification of transaction (dns.id), 2 bytes    Packets: 211 · Displayed: 6 (2.8%) · Dropped: 0 (0.0%)    Profile: Default
```

In order to make the DNS response larger, we use type ANY to get larger packets and add additional section in the DNS structure to increase the upper limit of UDP payload size.

We've tried out many websites to acquire the DNS responses with the largest length. At first, we thought that websites such as youtube.com or netflix.com will respond to us with huge response length. However, it's far from what we expected. After trying it out several times, we figured out that the three websites that will stably respond to us with long-length packets are "chegg.com", "ets.org" and "github.com".

The above screenshot shows that the amplification ratio is 1389/80 = 17.3 in the query name "chegg.com", 1055/78 = 13.5 in the query name "ets.org" and 1038/81 = 12.8 in the query name "github.com".

- Part 3 : Solution that can defend against the DoS attack based on the DNS reflection

We considered source IP verification a feasible way to defend DoS attack. Since the attacker will spoof the source IP address to the victim's IP, letting Internet service providers (ISPs) reject traffic with spoofed IP will surely reduce the efficiency of amplification attack. If a packet is being sent from inside the network with a source address that makes it appear like it originated outside the network, it's likely a spoofed packet and can be dropped. Furthermore, implementing ingress filtering helps reaching out to ISPs who are unknowingly taking part in DDoS attacks and let them realize their vulnerability at times.