Lab0

卞雨喆 18307110428

一、我的IP地址

图1 “status”为“active”

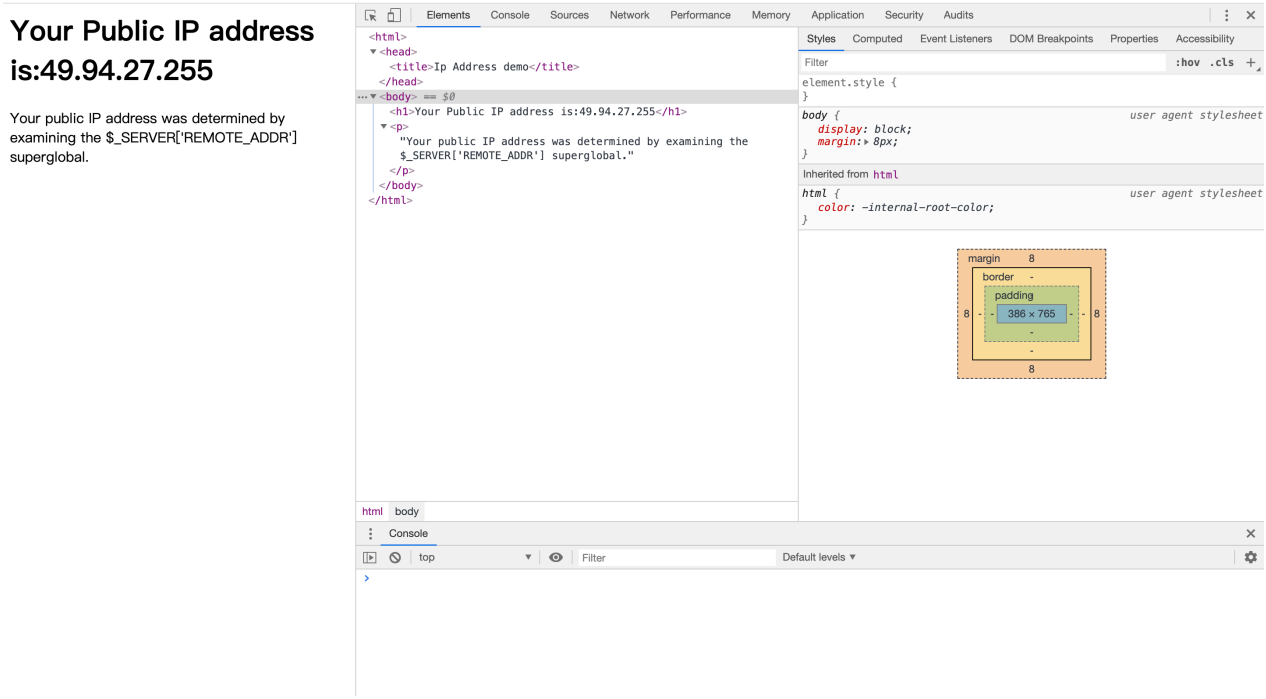
```
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether f0:18:98:1c:7e:17
        inet6 fe80::c5e:15e8:eb5d:97bb%en0 prefixlen 64 secured scopeid 0xa
        inet 192.168.3.30 netmask 0xffffff00 broadcast 192.168.3.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active

awdl0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1484
        ether 12:ea:98:b6:74:62
        inet6 fe80::10ea:98ff:feb6:7462%awdl0 prefixlen 64 scopeid 0xc
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active

en5: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether ac:de:48:00:11:22
        inet6 fe80::aede:48ff:fe00:1122%en5 prefixlen 64 scopeid 0x8
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect (100baseTX <full-duplex>)
        status: active
```

二、分析一个网页的组成部分

图2 展开左边所有的 HTML 标签，将整个网页内容连同开发者工具页面一同截图



三、域名服务器

图3 查询 baidu.com 的 A 地址记录截图

```
bianyuzhedeMacBook-Pro:~ fortunebian$ nslookup -type=A baidu.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   baidu.com
Address: 39.156.69.79
Name:   baidu.com
Address: 220.181.38.148
```

图4 查询 baidu.com 的 域名服务器截图

```
bianyuzhedeMacBook-Pro:~ fortunebian$ nslookup -type=ns baidu.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
baidu.com       nameserver = ns2.baidu.com.
baidu.com       nameserver = ns4.baidu.com.
baidu.com       nameserver = dns.baidu.com.
baidu.com       nameserver = ns7.baidu.com.
baidu.com       nameserver = ns3.baidu.com.

Authoritative answers can be found from:
```

图5 使用授权服务器查询 baidu.com 的 IP 地址的截图

```
bianyuzhedeMacBook-Pro:~ fortunebian$ nslookup baidu.com ns2.baidu.com
Server:         ns2.baidu.com
Address:        220.181.33.31#53

Name:   baidu.com
Address: 220.181.38.148
Name:   baidu.com
Address: 39.156.69.79
```

图6 查询 114.114.114.114 匹配的主机名的截图

```
bianyuzhedeMacBook-Pro:~ fortunebian$ nslookup 114.114.114.114
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
114.114.114.114.in-addr.arpa    name = public1.114dns.com.

Authoritative answers can be found from:
```

四、观察HTTP标头

图7 观察完Headers之后截下User-Agent的完整信息

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36

五、追踪数据包

图8 跟踪一个从你的计算机发往 microsoft.com 的数据包，并截图

```
 1  172.20.10.1 (172.20.10.1)  4.426 ms  4.378 ms  9.130 ms
 2  * * *
 3  * * *
 4  172.19.2.18 (172.19.2.18)  25.601 ms
    172.19.2.10 (172.19.2.10)  38.291 ms
    172.19.2.18 (172.19.2.18)  34.022 ms
 5  * * *
 6  192.168.0.254 (192.168.0.254)  25.735 ms *  44.950 ms
 7  * * *
 8  118.84.194.45 (118.84.194.45)  35.705 ms
    221.228.49.5 (221.228.49.5)  26.277 ms
    118.84.194.41 (118.84.194.41)  39.285 ms
 9  202.97.92.25 (202.97.92.25)  57.161 ms
    202.97.92.5 (202.97.92.5)  41.033 ms  45.711 ms
10  202.97.48.14 (202.97.48.14)  87.745 ms  95.448 ms  83.687 ms
11  202.97.33.154 (202.97.33.154)  45.205 ms  31.209 ms
    202.97.12.210 (202.97.12.210)  36.937 ms
12  * 202.97.25.230 (202.97.25.230)  62.225 ms
    202.97.63.118 (202.97.63.118)  76.402 ms
13  203.215.232.174 (203.215.232.174)  132.417 ms  105.391 ms  111.785 ms
14  ae24-0.icr02.hkg31.ntwk.msn.net (104.44.237.198)  80.082 ms  64.894 ms *
15  be-102-0.ibr01.hkg31.ntwk.msn.net (104.44.11.121)  233.150 ms
    be-122-0.ibr02.hkg31.ntwk.msn.net (104.44.11.137)  254.987 ms
    be-102-0.ibr01.hkg31.ntwk.msn.net (104.44.11.121)  233.692 ms
16  be-11-0.ibr01.tyo79.ntwk.msn.net (104.44.17.134)  233.967 ms *  253.519 ms
17  be-7-0.ibr01.pdx30.ntwk.msn.net (104.44.18.167)  259.384 ms
    be-5-0.ibr02.pdx30.ntwk.msn.net (104.44.19.85)  262.443 ms  273.216 ms
18  be-4-0.ibr03.mwh01.ntwk.msn.net (104.44.16.66)  241.205 ms  221.671 ms
    be-4-0.ibr04.mwh01.ntwk.msn.net (104.44.16.68)  283.902 ms
19  be-2-0.ibr01.mwh01.ntwk.msn.net (104.44.16.84)  248.259 ms
    be-2-0.ibr02.mwh01.ntwk.msn.net (104.44.16.81)  249.402 ms  248.648 ms
20  be-7-0.ibr02.cys04.ntwk.msn.net (104.44.18.224)  229.940 ms
    be-8-0.ibr01.cys04.ntwk.msn.net (104.44.18.222)  257.777 ms *
21  * * *
22  ae142-0.icr02.dsm05.ntwk.msn.net (104.44.22.180)  216.095 ms  229.979 ms
    ae163-0.icr04.dsm05.ntwk.msn.net (104.44.22.192)  275.823 ms
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
31  * * *
32  * * *
33  * * *
34  * * *
35  * * *
36  * * *
37  * * *
38  * * *
39  * * *
40  * * *
41  * * *
42  * * *
43  * * *
```

```
44  * * *
45  * * *
46  * * *
47  * * *
48  * * *
49  * * *
50  * * *
51  * * *
52  * * *
53  * * *
54  * * *
55  * * *
56  * * *
57  * * *
58  * * *
59  * * *
60  * * *
61  * * *
62  * * *
63  * * *
64  * * *
```

图9 利用 whois 查询 tencent.com 的相关信息，并截图

```
refer:        whois.verisign-grs.com

domain:       COM

organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston Virginia 20190
address:      United States

contact:      administrative
name:         Registry Customer Service
organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston Virginia 20190
address:      United States
phone:        +1 703 925-6999
fax-no:       +1 703 948 3978
e-mail:       info@verisign-grs.com

contact:      technical
name:         Registry Customer Service
organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston Virginia 20190
address:      United States
phone:        +1 703 925-6999
fax-no:       +1 703 948 3978
e-mail:       info@verisign-grs.com

nserver:      A.GTLD-SERVERS.NET 192.5.6.30 2001:503:a83e:0:0:0:2:30
nserver:      B.GTLD-SERVERS.NET 192.33.14.30 2001:503:231d:0:0:0:2:30
nserver:      C.GTLD-SERVERS.NET 192.26.92.30 2001:503:83eb:0:0:0:0:30
nserver:      D.GTLD-SERVERS.NET 192.31.80.30 2001:500:856e:0:0:0:0:30
nserver:      E.GTLD-SERVERS.NET 192.12.94.30 2001:502:1ca1:0:0:0:0:30
nserver:      F.GTLD-SERVERS.NET 192.35.51.30 2001:503:d414:0:0:0:0:30
nserver:      G.GTLD-SERVERS.NET 192.42.93.30 2001:503:eea3:0:0:0:0:30
nserver:      H.GTLD-SERVERS.NET 192.54.112.30 2001:502:8cc:0:0:0:0:30
nserver:      I.GTLD-SERVERS.NET 192.43.172.30 2001:503:39c1:0:0:0:0:30
nserver:      J.GTLD-SERVERS.NET 192.48.79.30 2001:502:7094:0:0:0:0:30
nserver:      K.GTLD-SERVERS.NET 192.52.178.30 2001:503:d2d:0:0:0:0:30
nserver:      L.GTLD-SERVERS.NET 192.41.162.30 2001:500:d937:0:0:0:0:30
nserver:      M.GTLD-SERVERS.NET 192.55.83.30 2001:501:b1f9:0:0:0:0:30
ds-rdata:     30909 8 2 E2D3C916F6DEEAC73294E8268FB5885044A833FC5459588F4A9184CFC41A5766

whois:        whois.verisign-grs.com

status:       ACTIVE
remarks:      Registration information: http://www.verisigninc.com

created:      1985-01-01
changed:      2017-10-05
source:       IANA
```

```
   Domain Name: TENCENT.COM
   Registry Domain ID: 3216596_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
```

```
   Updated Date: 2019-08-12T09:11:43Z
   Creation Date: 1998-09-14T04:00:00Z
   Registry Expiry Date: 2021-09-13T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2083895740
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS1.QQ.COM
   Name Server: NS2.QQ.COM
   Name Server: NS3.QQ.COM
   Name Server: NS4.QQ.COM
   DNSSEC: unsigned
```