



دانشگاه صنعتی شریف
دانشکده مهندسی کامپیوتر

گزارشکار آزمایشگاه شبکه

آزمایش شماره ۳

استاد محترم:

جناب آقای دکتر صفایی

اعضای تیم:

امیرمهدی نامجو ۹۷۱۰۷۲۱۲

محمدسپهر پورقناد ۹۷۱۰۱۳۵۹

سپهر صفری ۹۷۱۰۸۲۶۳

نیم سال دوم تحصیلی ۱۴۰۰-۱۴۰۱

Wireshark

بدست آوردن captcha

پس از انجام مراحل گفته شده عکس زیر بدست آمد. همان طور که معلوم است مقدار کیچا برابر با p94kuq است.



شکل ۱.۱: کیچا

سوالها

(۱) می توان به کمک تب Statistics به این اطلاعات آماری دسترسی پیدا کرد.

به کمک این اطلاعات می توان درباره طول بسته ها، ترافیک بین آدرس های مختلف و لایه های مختلف شبکه اطلاعات کسب کرد. همچنین می توان درباره پروتکل های مختلف مانند DHCP، HTTP و DNS آمار بدست آورد. درباره IP ها هم می توانیم اطلاعاتی کسب کنیم.

(۲) RTP یا همان Realtime Transfer Protocol یک پروتکل بی درنگ برای انتقال فیلم و صوت است که معمولاً بر بستر پروتکل UDP قرار می گیرد. از کاربردهای آن می توان به پخش زنده فیلم اشاره کرد.

در Wireshark می توان با رفتن به قسمت RTP Streams > RTP > Telephony اطلاعاتی از قبیل تعداد بسته های RTP، Max jitter، Mean jitter، تعداد بسته های از دست رفته، مدت زمان و ... را برای این پروتکل به دست آورد.

راه اندازی DNS

سناریوی آزمایش

این آزمایش در سیستم عامل Ubuntu 18.04 انجام شده است.

دامنه سرور را به صورت netlab.edu در نظر گرفتیم. name server در آدرس ns.netlab.edu قرار دارد و آی پی آن برابر با 192.168.88.1 است. زیر دامنه های group1.netlab.edu و group2.netlab.edu به ترتیب در آی پی های 192.168.88.11 و 192.168.88.22 قرار دارند و نام های مستعار آنها هم به ترتیب برابر با group1name.netlab.edu و group2name.netlab.edu هست.

ابتدا فایل /etc/bind/named.conf.local را مطابق زیر پر می کنیم:

```
File Edit View Search Terminal Help
GNU nano 2.9.3 named.conf.local

//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "netlab.edu" {
    type master;
    file "/etc/bind/db.netlab.edu";
};

zone "88.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.192.168.88";
};

^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line
```

شکل ۲.۲: /etc/bind/named.conf.local

سپس فایل /etc/bind/db.netlab.edu را که برای رکوردها است، مانند زیر پر می‌کنیم:

```
File Edit View Search Terminal Tabs Help
sepehr@sepehr-nb: /etc/... x sepehr@sepehr-nb: ~/uni... x sepehr@sepehr-nb: ~ x
GNU nano 2.9.3 db.netlab.edu

;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      ns.netlab.edu. root.netlab.edu. (
                        13      ; Serial
                        604800   ; Refresh
                        86400    ; Retry
                        2419200  ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       ns.netlab.edu.
@         IN      A        192.168.88.1
@         IN      AAAA     ::1
ns        IN      A        192.168.88.1

group1    IN      A        192.168.88.11
group2    IN      A        192.168.88.22
group1name IN      CNAME    group1
group2name IN      CNAME    group2

^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text ^T To Spell ^_ Go To Line
```

شکل ۳.۲: /etc/bind/db.netlab.edu

در ادامه فایل /etc/bind/db.192.168.88 را که برای رکوردهای معکوس است، طبق شکل زیر پر می‌کنیم:

```
File Edit View Search Terminal Help
GNU nano 2.9.3 db.192.168.88

; BIND reverse data file for local loopback interface
$TTL      604800
@         IN      SOA      ns.netlab.edu. root.netlab.edu. (
                        13      ; Serial
                        604800   ; Refresh
                        86400    ; Retry
                        2419200  ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       ns.
1         IN      PTR      ns.netlab.edu.
11        IN      PTR      group1.netlab.edu.
22        IN      PTR      group2.netlab.edu.

[ Read 16 lines ]
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text ^T To Spell  ^ _ Go To Line
```

شکل ۴.۲: /etc/bind/db.192.168.88

حال فایل /etc/resolvconf/resolv.conf.d/head را مانند زیر پر می‌کنیم:

```
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/resolvconf/resolv.conf.d/head

# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
# 127.0.0.53 is the systemd-resolved stub resolver.
# run "systemd-resolve --status" to see details about the actual nameservers.

search netlab.edu # your private domain
nameserver 127.0.0.1 # ns private IP address

[ Read 7 lines ]
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text ^T To Spell  ^ Go To Line
```

شکل ۵.۲: /etc/resolvconf/resolv.conf.d/head

در ادامه دو دستور زیر را اجرا می‌کنیم. اولی راه‌اندازی مجدد bind9 و دومی برای اضافه شدن آدرس سرور ما قبل از سرورهای مورد اعتماد سیستم است:

```
sudo /etc/init.d/bind9 restart
```

```
sudo resolvconf -u
```

همان گونه که در عکس‌های زیر مشاهده می‌شود خروجی‌های nslookup مطابق انتظار است. عکس اول برای رکوردهای معمولی و عکس دوم برای رکوردهای معکوس است:

```
File Edit View Search Terminal Help
sepehr@sepehr-nb:/etc/bind$ nslookup netlab.edu
Server:          127.0.0.1
Address:         127.0.0.1#53

Name:   netlab.edu
Address: 192.168.88.1
Name:   netlab.edu
Address: ::1

sepehr@sepehr-nb:/etc/bind$ nslookup ns.netlab.edu
Server:          127.0.0.1
Address:         127.0.0.1#53

Name:   ns.netlab.edu
Address: 192.168.88.1

sepehr@sepehr-nb:/etc/bind$ nslookup group1.netlab.edu
Server:          127.0.0.1
Address:         127.0.0.1#53

Name:   group1.netlab.edu
Address: 192.168.88.11

sepehr@sepehr-nb:/etc/bind$ nslookup group2.netlab.edu
Server:          127.0.0.1
Address:         127.0.0.1#53

Name:   group2.netlab.edu
Address: 192.168.88.22

sepehr@sepehr-nb:/etc/bind$ nslookup group1name.netlab.edu
Server:          127.0.0.1
Address:         127.0.0.1#53

group1name.netlab.edu canonical name = group1.netlab.edu.
Name:   group1.netlab.edu
Address: 192.168.88.11

sepehr@sepehr-nb:/etc/bind$ nslookup group2name.netlab.edu
Server:          127.0.0.1
Address:         127.0.0.1#53

group2name.netlab.edu canonical name = group2.netlab.edu.
Name:   group2.netlab.edu
Address: 192.168.88.22

sepehr@sepehr-nb:/etc/bind$
```

شکل ۶.۲: nslookup domain-name


```
File Edit View Search Terminal Help
sepehr@sepehr-nb:/etc/bind$ nslookup 192.168.88.1
1.88.168.192.in-addr.arpa      name = ns.netlab.edu.

sepehr@sepehr-nb:/etc/bind$ nslookup 192.168.88.11
11.88.168.192.in-addr.arpa    name = group1.netlab.edu.

sepehr@sepehr-nb:/etc/bind$ nslookup 192.168.88.22
22.88.168.192.in-addr.arpa    name = group2.netlab.edu.

sepehr@sepehr-nb:/etc/bind$
```

شکل ۷.۲: nslookup ips

سوالات

- (۱) بسته‌های مربوط به دو آدرس group1.netlab.edu و 192.168.88.22 بررسی می‌کنیم. عکس زیر مربوط به دستور nslookup group1.netlab.edu هست.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	127.0.0.1	127.0.0.1	UDP	43	54178 → 54178 Len=1
2	0.000062476	:::1	:::1	UDP	63	33323 → 33323 Len=1
3	0.000123974	127.0.0.1	127.0.0.1	DNS	77	Standard query 0xe114 A group1.netlab.edu
4	0.000376670	127.0.0.1	127.0.0.1	DNS	126	Standard query response 0xe114 A group1.netlab.edu
5	0.000935042	127.0.0.1	127.0.0.1	DNS	77	Standard query 0x126a AAAA group1.netlab.edu
6	0.001263825	127.0.0.1	127.0.0.1	DNS	121	Standard query response 0x126a AAAA group1.netlab.edu

Authority RRs: 1
Additional RRs: 1

▼ Queries

- group1.netlab.edu: type A, class IN
 - Name: group1.netlab.edu
 - [Name Length: 17]
 - [Label Count: 3]
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)

▼ Answers

- group1.netlab.edu: type A, class IN, addr 192.168.88.11
 - Name: group1.netlab.edu
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)
 - Time to live: 604800
 - Data length: 4
 - Address: 192.168.88.11

► Authoritative nameservers

▼ Additional records

- ns.netlab.edu: type A, class IN, addr 192.168.88.1
 - Name: ns.netlab.edu
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)
 - Time to live: 604800
 - Data length: 4
 - Address: 192.168.88.1

[Request In: 3]
[Time: 0.000252696 seconds]

0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00 ... E

شکل ۲.۸: nslookup group1.netlab.edu

همان طور که در تصویر می بینیم، کویری آی پی آدرس group1.netlab.edu را درخواست کرده است که در پاسخ آی پی 192.168.88.11 برگردانده شده است که همان چیزی است که انتظار داریم. همچنین آی پی مربوط به رکورد ns.netlab.edu هم برگردانده شده است تا اگر سیستم به آن احتیاج داشت نیاز نباشد دوباره برای آن درخواست بزنیم. این عمل توسط DNS server ها برای بهبود عملکرد صورت می گیرد.

عکس بعدی مربوط به دستور nslookup 192.168.88.22 هست.

nslookup-192.168.88.22.pcapng						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Apply a display filter ... <Ctrl-/> Expression... +						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	127.0.0.1	127.0.0.1	UDP	43	55585 → 55585 Len=1
2	0.000083923	:::1	:::1	UDP	63	37469 → 37469 Len=1
3	0.000174479	127.0.0.1	127.0.0.1	DNS	86	Standard query 0x04b7 PTR 22.88.168.
4	0.000490482	127.0.0.1	127.0.0.1	DNS	133	Standard query response 0x04b7 PTR 22.88.168.

▶ Frame 4: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits) on interface 0
 ▶ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
 ▶ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
 ▶ User Datagram Protocol, Src Port: 53, Dst Port: 33061
 ▶ Domain Name System (response)
 Transaction ID: 0x04b7
 Flags: 0x8580 Standard query response, No error
 Questions: 1
 Answer RRs: 1
 Authority RRs: 1
 Additional RRs: 0
 ▼ Queries
 22.88.168.192.in-addr.arpa: type PTR, class IN
 Name: 22.88.168.192.in-addr.arpa
 [Name Length: 26]
 [Label Count: 6]
 Type: PTR (domain name PoinTeR) (12)
 Class: IN (0x0001)
 ▼ Answers
 22.88.168.192.in-addr.arpa: type PTR, class IN, group2.netlab.edu
 Name: 22.88.168.192.in-addr.arpa
 Type: PTR (domain name PoinTeR) (12)
 Class: IN (0x0001)
 Time to live: 604800
 Data length: 19
 Domain Name: group2.netlab.edu
 ▶ Authoritative nameservers
 [Request In: 3]
 [Time: 0.000316003 seconds]

0060	00 13 06 67 72 6f 75 70 32 06 6e 65 74 6c 61 62	...group 2.netlab
------	---	-------------------

شکل ۹.۲: nslookup 192.168.88.22

همان طور که در تصویر هم می بینیم، کویری آدرس مربوط به آی پی 192.168.88.22 را درخواست کرده است که در پاسخ آدرس group2.netlab.edu برگردانده شده است که همان چیزی است که انتظار داریم.

۲) همان طور که در عکس های قبلی از Wireshark می توان دید، رکورد اول از نوع A یا همان host address است. در واقع با می خواهیم با دادن نام دامنه آدرس میزبان را که یک آی پی است، دریافت کنیم.

رکورد دوم هم از نوع PTR یا همان domain name PoinTeR است. در واقع می خواهیم با دادن آی پی که اشاره گری به نام دامنه است، نام دامنه میزبان را دریافت کنیم.