



دانشگاه صنعتی امیرکبیر

(پلی تکنیک تهران)

دانشکده مهندسی کامپیوتر

درس شبکه

کار با کاربردهای Web، DNS، سوکت و پوشش سرویس‌ها

نگارش

هلیاسادات هاشمی پور

۹۸۳۱۱۰۶

اردیبهشت ۱۴۰۱

سوال اول: نام و اطلاعات فردی که در دامنه به اسم ثبت شده است چیست؟

```
WHOIS Information for soft98.ir
=====
% This is the IRNIC Whois server v1.6.2.
% Available on web at http://whois.nic.ir/
% Find the terms and conditions of use on http://www.nic.ir/
%
% This server uses UTF-8 as the encoding for requests and responses.
% NOTE: This output has been filtered.
% Information related to 'soft98.ir'

domain: soft98.ir
ascii: soft98.ir
remarks: (Domain Holder) alireza bagheri
remarks: (Domain Holder Address) Shariati-Khiaban Mirzapour-Mehr 3 Gharbi-Pelak 20, Tehran, Tehran, IR
holder-c: ab590-irnic
admin-c: ab590-irnic
tech-c: ab590-irnic
bill-c: fa482-irnic
nserver: ir1.hostdl.com
nserver: ir2.hostdl.com
last-updated: 2018-03-25
expire-date: 2023-04-27
source: IRNIC # Filtered

nic-hdl: ab590-irnic
person: alireza bagheri
e-mail: soft98.ir@gmail.com
address: Shariati-Khiaban Mirzapour-Mehr 3 Gharbi-Pelak 20, Tehran, Tehran, IR
phone: 0912 3549940
source: IRNIC # Filtered

nic-hdl: fa482-irnic
org: Faraso Samaneh Pasargad Co.
e-mail: irnic@faraso.org
source: IRNIC # Filtered
```

nic-hdl: ab590-irnic

person: alireza bagheri

e-mail: soft98.ir@gmail.com

address: Shariati-Khiaban Mirzapour-Mehr 3 Gharbi-Pelak 20, Tehran, Tehran, IR

phone: 0912 3549940

source: IRNIC # Filtered






سوال دوم: آدرس name server آن چیست؟

nserver: ir1.hostdl.com

nserver: ir2.hostdl.com




سوال سوم: رکوردهای NS، A، TXT و MX را مشخص کنید.
هر یک از این رکوردها چه چیزی را مشخص می‌کند؟

رکورد NS

Parent Nameserver Tests		
Status	Test Case	Information
	NS records listed at parent servers	<div>Nameserver records returned by the parent servers are:</div> <div>ir2.hostdl.com. [NO GLUE] [TTL=1440] ir1.hostdl.com. [NO GLUE] [TTL=1440]</div> <div>This information was kindly provided by ns5.univie.ac.at.</div>
	Domain listed at parent servers	Good! The parent servers have information on your domain. Some other domains (like .co.us) do not have a DNS zone at the parent servers.
	NS records listed at parent servers	Good! The parent servers have your NS records listed. If they didn't, people wouldn't be able to find your domain!
	Parent servers return glue	OK. The TLD of your domain (ir) differs from that of your nameservers (com). As such, the parent servers are not required to send glue.
	A record for each NS at parent	OK. The parent servers don't need to have A records for your nameservers since the TLD of your domain (ir) differs from that of your nameservers (com).

مخفف کلمه‌ی Name Server هست. این رکورد در اصل می‌گوید که به کدام سرویس DNS برای آن دامنه باید رجوع کرد. به بیانی دیگر رکوردهای NS کمک می‌کنند تا DNS server مناسبی را که می‌تواند به درخواست‌ها درباره‌ی یک وب‌سرویس خاص پاسخ دهد، پیدا شود.

رکورد A

WWW Record tests		
Status	Test Case	Information
	WWW record	www.soft98.ir A records are: www.soft98.ir. CNAME soft98.ir. [TTL=14400] soft98.ir. A 79.127.127.35 [TTL=14400]
	WWW A record has public IP	Good! The IP address(es) of the A records returned for your WWW record have public IP addresses.
	WWW CNAME lookup	Good! You have a CNAME entry for your WWW record which also returns the associated A record! This saves an extra lookup which would delay loading times for your site.











این رکورد IP و دامنه مورد نظر خود را نگه می‌دارد. این رکورد در اصل نگاشت یک Domain name به یک آدرس IPv4 می‌کند. حال توسط رکورد AAAAA انجام می‌شود نگاشت به آدرس IPv6 صورت می‌گیرد.

رکورد TXT:

این رکورد به عنوان مکانی برای یادداشت‌های قابل خواندن در نظر گرفته شده است. ب این رکورد می‌توان یک متن دلخواه را به یک دامنه نسبت داد. این رکورد طور مستقل روی DNS تاثیر ندارد. موارد استفاده‌ی این رکورد برای دادن اطلاعات درباره‌ی عملکرد دامنه‌ی خود به سرویس‌هاست. این رکورد داخل سایت گزارش نبود.

رکورد MX


Mail eXchanger (MX) Tests

Status	Test Case	Information
	MX Records	Your Mail eXchanger (MX) records are: 0 soft98.ir. [TTL=14400]
	All nameservers have same MX records	Good! All of your nameservers have the same MX records.
	All MX records contain valid hostnames	Good! All of your MX entries have valid hostnames (e.g. are not IP's or invalid domain names).
	All MX records use public IP addresses	Good! All of your MX entries have public IP addresses.
	MX record is not a CNAME/alias	Good! When querying for your MX records we did not receive a CNAME record as a result.
	MX A records are not CNAME's	Good! No CNAME records are present for your MX A records.
	Number of MX records	Oops! You only have one MX record! In the event that this mail server is down, you could potentially lose mail! It is recommended to have two or more MX records (and hence mail servers) if you want uninterrupted mail functionality.
	Duplicate MX A records	Good! No two MX records resolve to the same IP address.
	Differing MX A records	Good! You have no different IP's for your MX A records than the DNS server that is authoritative for that hostname.
	MX records have reverse DNS entries	Good! All your MX IP addresses have reverse DNS entries. The reverse entries returned were: 35.127.127.79.in-addr.arpa <--> hosted-by.hostdl.com.asiatech.ir.


این رکورد مخفف Mail Exchange است. این رکورد ایمیل را به یک سرویس ایمیل هدایت می کند و وظیفه‌ی مبادله کردن ایمیل را دارد. این رکورد سرور ایمیل این رکورد را می‌سازد که به کمک آن بتواند مقصد ایمیل را مشخص کند.

سوال چهارم: در قسمت DNS Report با وارد کردن دامنه‌ی دانشگاه (aut.ac.ir)، mail server دانشگاه را مشخص کنید.

Mail eXchanger (MX) Tests

Status	Test Case	Information
	MX Records	Your Mail eXchanger (MX) records are: 5 asg.aut.ac.ir. [TTL=3600]

آیا آدرس IP آن را می‌توانید مشخص کنید؟

	WWW record	www.aut.ac.ir A records are: www.aut.ac.ir. A 185.211.88.131 [TTL=3600]
---	------------	--


این آدرس IP ۱۸۵.۲۱۱.۸۸.۲۰ است.

سوال پنجم: چه وبسایت‌های دیگری بر روی همین سرور قرار دارند؟ چند مورد از آن‌ها را نام ببرید (آدرس IP آن‌ها را با آدرس IP سایت **cert.ir** مقایسه کنید).


IP وبسایت خواسته شده با IP این دامنه یکسان می باشد.

Domain	Last Resolved Date
7peykar.ir	2022-05-09
92762.ir	2022-05-09
abrmarketing.net	2022-05-09
aghlovahy.com	2022-05-09
agoracomplex.com	2022-04-30
alotasvirgar.ir	2022-05-09
bemanbespar.ir	2022-05-04
bimehnama.com	2022-04-30
binazirshop.com	2022-04-30
bizilyapp.com	2022-04-30
bodyspinners.com	2022-04-30
bornosmode.com	2022-04-30
brifenews.ir	2022-05-04
carbilla.ir	2022-05-04
cert.ir	2022-05-10
chang.ir	2022-03-18
chargoona.com	2022-04-30
diatech.ir	2022-05-04
electro-tech.ir	2022-05-04
esfimo.ir	2021-12-29
eshghabad.com	2022-04-30
geotechnical.ir	2022-05-04
green.ir	2022-05-04
gym24.ir	2022-05-04


WWW Record Tests

Status	Test Case	Information
	WWW record	<p>www.141.ir A records are:</p> <p>www.141.ir. A 185.143.233.5 [TTL=180]</p> <p>www.141.ir. A 185.143.234.5 [TTL=180]</p>

WW Record Tests

Status	Test Case	Information
	WWW record	www.1zodpaz.ir A records are: www.1zodpaz.ir. A 185.143.234.5 [TTL=180] www.1zodpaz.ir. A 185.143.233.5 [TTL=180]

www Record Tests

Status	Test Case	Information
	WWW record	www.cert.ir A records are: www.cert.ir. A 185.143.234.5 [TTL=180] www.cert.ir. A 185.143.233.5 [TTL=180]

سوال ششم: به نظر شما سرور چگونه وب سرور درخواست شده را تشخیص می‌دهد؟ آیا این روش نیز نوعی **Multiplexing** است؟

از مقدار header ای که در درخواست HTTP فرستادیم تشخیص می‌دهد. بله، چون با استفاده از یک آدرس IP، چندین وبسایت ایجاد شده است. در اصل نوعی multiplexing می‌باشد زیرا امکان استفاده از یک سرور به ازای هر کلاینت را فراهم می‌کند. نتیجه از کاربران بیشتری در همان زمان می‌تواند پشتیبانی کند.

سوال هفتم: برای لیست کردن برنامه‌هایی که در حال حاضر پورت‌های لایه انتقال را بر روی سیستم باز کرده‌اند، از چه دستور خط فرمانی استفاده می‌شود؟

با استفاده از `netstat -b` (البته می‌توان از آپشن `-ab` هم استفاده کرد که تمامی پورت‌ها را نشان دهد).

Active Connections			
Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	LAPTOP-R0MMVD6I:0	LISTENING
RpcSs			
[svchost.exe]			
TCP	0.0.0.0:445	LAPTOP-R0MMVD6I:0	LISTENING
Can not obtain ownership information			
TCP	0.0.0.0:5040	LAPTOP-R0MMVD6I:0	LISTENING
CDPSvc			
[svchost.exe]			
TCP	0.0.0.0:7680	LAPTOP-R0MMVD6I:0	LISTENING
Can not obtain ownership information			
TCP	0.0.0.0:9330	LAPTOP-R0MMVD6I:0	LISTENING
[Speedify.exe]			
TCP	0.0.0.0:17500	LAPTOP-R0MMVD6I:0	LISTENING
[Dropbox.exe]			
TCP	0.0.0.0:49664	LAPTOP-R0MMVD6I:0	LISTENING
[lsass.exe]			
TCP	0.0.0.0:49665	LAPTOP-R0MMVD6I:0	LISTENING
Can not obtain ownership information			
TCP	0.0.0.0:49666	LAPTOP-R0MMVD6I:0	LISTENING
EventLog			
[svchost.exe]			
TCP	0.0.0.0:49667	LAPTOP-R0MMVD6I:0	LISTENING

سوال هشتم: دستوری را پیدا کنید که به وسیلهی آن تمام پورت‌های سیستم در هر وضعیت اتصالی همراه با مبدا و مقصد اتصال به صورت عددی لیست شوند.

با استفاده از دستور netstat -an

Active Connections			
Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING
TCP	0.0.0.0:7680	0.0.0.0:0	LISTENING
TCP	0.0.0.0:9330	0.0.0.0:0	LISTENING
TCP	0.0.0.0:17500	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49669	0.0.0.0:0	LISTENING
TCP	10.202.0.2:14790	149.154.167.92:443	ESTABLISHED
TCP	10.202.0.2:14796	91.108.4.220:443	ESTABLISHED
TCP	127.0.0.1:843	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1269	127.0.0.1:1270	ESTABLISHED
TCP	127.0.0.1:1270	127.0.0.1:1269	ESTABLISHED
TCP	127.0.0.1:1271	127.0.0.1:1272	ESTABLISHED
TCP	127.0.0.1:1272	127.0.0.1:1271	ESTABLISHED
TCP	127.0.0.1:1331	127.0.0.1:1332	ESTABLISHED
TCP	127.0.0.1:1332	127.0.0.1:1331	ESTABLISHED
TCP	127.0.0.1:1333	127.0.0.1:1334	ESTABLISHED

سوال نهم: دلیل وارد کردن دو **enter** پشت سر هم چیست؟

در ابتدا باید بدانیم که جدا کنندهی request Header و request Body یک خط خالی است. پس برای نشان دادن اینکه header ها تمام شده باید یک بار دیگر enter بزنیم.

سوال دهم: پیامی که در پاسخ تقاضای شما داده می‌شود چیست؟ صفحه‌ی اصلی در کجا قرار دارد؟

پیام 301 Moved permanently در پاسخ به تقاضای ما داده شده است.
صفحه‌ی اصلی در آدرس https://aut.ac.ir:443 قرار دارد (در بخش Location)

```
GET / HTTP/1.1
Host: aut.ac.ir

HTTP/1.1 301 Moved Permanently
Date: Wed, 09 Dec 2020 15:39:50 GMT
Server: Apache
Location: https://aut.ac.ir:443/
Content-Length: 230
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://aut.ac.ir:443/">here</a>.</p>
</body></html>
```

No.	Time	Source	Destination	Protocol	Length	Info
→	1076 20.717964	192.168.1.105	185.211.88.131	HTTP	60	GET / HTTP/1.1
←	1082 20.802593	185.211.88.131	192.168.1.105	HTTP	528	HTTP/1.1 301 Moved Permanently (text/html)

```
> Frame 1082: 528 bytes on wire (4224 bits), 528 bytes captured (4224 bits) on interface \Device\NPF_{FAE24E43-63D0-49A6-98B9-5
> Ethernet II, Src: Tp-LinkT_b3:7a:c9 (50:d4:f7:b3:7a:c9), Dst: IntelCor_17:3f:68 (74:e5:f9:17:3f:68)
> Internet Protocol Version 4, Src: 185.211.88.131, Dst: 192.168.1.105
> Transmission Control Protocol, Src Port: 80, Dst Port: 1872, Seq: 1, Ack: 1467, Len: 474
> Hypertext Transfer Protocol
  Line-based text data: text/html (7 lines)
    <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
    <html><head>\n
    <title>301 Moved Permanently</title>\n
    </head><body>\n
    <h1>Moved Permanently</h1>\n
    <p>The document has moved <a href="https://aut.ac.ir:443/">here</a>.</p>\n
    </body></html>\n
```

با استفاده از وایرشارک و فیلتر کردن http توانستیم اثبات کنیم.

سوال یازدهم: آیا این ارتباط **persistent** است؟

بله، زیرا Response version ما HTTP/1.1 است.

```
> Internet Protocol Version 4, Src: 185.211.88.131, Dst: 172.20.10.2
> Transmission Control Protocol, Src Port: 80, Dst Port: 14577, Seq: 1, Ack: 36, Len: 417
  Hypertext Transfer Protocol
    HTTP/1.1 301 Moved Permanently\r\n
      [Expert Info (Chat/Sequence): HTTP/1.1 301 Moved Permanently\r\n]
      Response Version: HTTP/1.1
```

سوال دوازدهم: پورت ۱۶۰۰۰ بر روی کدام آدرس IP، bind شده است؟

IP: 0.0.0.0


```

[svchost.exe]
TCP    0.0.0.0:443      0.0.0.0:0        LISTENING
[vmware-hostd.exe]
TCP    0.0.0.0:445      0.0.0.0:0        LISTENING
Can not obtain ownership information
TCP    0.0.0.0:902      0.0.0.0:0        LISTENING
[vmware-authd.exe]
TCP    0.0.0.0:912      0.0.0.0:0        LISTENING
[vmware-authd.exe]
TCP    0.0.0.0:1947     0.0.0.0:0        LISTENING
[hasplms.exe]
TCP    0.0.0.0:5040     0.0.0.0:0        LISTENING
CDPSvc
[svchost.exe]
TCP    0.0.0.0:5357     0.0.0.0:0        LISTENING
Can not obtain ownership information
TCP    0.0.0.0:7070     0.0.0.0:0        LISTENING
[AnyDesk.exe]
TCP    0.0.0.0:16000    0.0.0.0:0        LISTENING
[ncat.exe]
TCP    0.0.0.0:49664    0.0.0.0:0        LISTENING
[lsass.exe]

```

سوال سیزدهم: به نظر شما وجود خط اول در این فایل چیست؟ یک فایل دیگر بدون خط اول این فایل بسازید و نتیجه را امتحان کنید.

همانطور که در سوالات قبلی نیز اشاره شد، در پروتکل HTTP جدا کننده‌ی request Header و request Body یک خط خالی است. و در صورتیکه این خط را رعایت نکنیم با ارور مواجه خواهیم شد زیرا قوانین پروتکل HTTP را رعایت نکرده‌ایم و از فرمت آن خارج شده ایم.

سوال چهاردهم: سیستم عامل این وبسایت چیست؟

Linux 3.10 - 4.11

سوال پانزدهم: چه پورت‌هایی روی این سرور باز است؟

شماره پورت‌ها برابر است با ۸۰ و ۴۴۳

سوال شانزدهم: سرویس‌هایی که از طریق پورت‌ها ارائه می‌شود چیست؟

از طریق HTTP webserver