



دانشکده مهندسی
کامپیوتر و فناوری اطلاعات

دانشگاه صنعتی امیرکبیر

(پلی تکنیک تهران)

دانشکده مهندسی کامپیوتر



دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

آزمایشگاه شبکه های کامپیوتری

(پاییز ۱۴۰۰)

جلسه چهارم

کار با کاربرد های Web,Dns ، سوکت و پویش سرویس
ها

محمد چوپان ۹۸۳۱۱۲۵

۱. در قسمت Domain / IP Whois رفته و آدرس soft98.ir را وارد نمایید.

سوال ۱: نام و اطلاعات فردی که دامنه به اسم ثبت شده است چیست؟

سوال ۲: آدرس name server آن چیست؟

سوال ۱:

```
nic-hdl: ab590-irnic
person: alireza bagheri
e-mail: soft98.ir@gmail.com
source: IRNIC # Filtered
```

سوال ۲:

```
-----
nserver: ir1.hostdl.com
nserver: ir2.hostdl.com
-----
```






۲. در وبسایت به قسمت DNS Report رفته و آدرس soft98.ir را وارد نمایید.

سوال ۳: رکوردهای NS، A، TXT و MX را مشخص کنید. هر یک از این رکوردها چه چیزی را مشخص می‌کنند؟

سوال ۴: در قسمت DNS Report با وارد کردن دامنه‌ی دانشگاه (aut.ac.ir)، mail server دانشگاه را مشخص کنید. آیا آدرس IP آن را می‌توانید مشخص کنید؟

سوال ۳:

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.

i	NS records listed at parent servers	Nameserver records returned by the parent servers are: ir1.hostdl.com. [NO GLUE] [TTL=1440] ir2.hostdl.com. [NO GLUE] [TTL=1440] This information was kindly provided by a.nic.ir.
✓	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!
i	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.
i	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).

رکورد NS : رکوردی برای نمایش name server ها و اطمینان از درست کار کردن domain name های درخواستی

رکورد A : برای مپ کردن یک دامنه یا زیردامنه به آدرس IP

رکورد TXT : از این رکورد برای اضافه کردن یک متن دلخواه به یک host استفاده می‌شود بطوریکه این متن برای انسان قابل فهم است.

رکورد MX : از این رکورد برای تعیین mail server که مسئول دریافت ایمیل های سمت domain name است.

سوال ۴ :

Record Type	Information
MX Records	Your Mail eXchanger (MX) records are: 5 asg.aut.ac.ir. [TTL=3600]
All nameservers have	
WWW record	www.aut.ac.ir. A records are: www.aut.ac.ir. A 185.211.88.131 [TTL=3600]

آدرس ای پی و میل سرور از بالا به پایین به ترتیب اند.

۳. در قسمت Reverse IP Lookup آدرس cert.ir را وارد کنید.

سوال ۵: 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)

سوال ۶: به نظر شما سرور چگونه وب سرور درخواست شده را تشخیص می‌دهد؟ آیا این روش نیز نوعی Multiplexing است؟

سوال ۵:

Reverse IP results for cert.ir (185.143.233.41, 185.143.234.41)
=====

Domain	Last Resolved Date
7peykar.ir	2022-06-22
92762.ir	2022-06-22
abrmarketing.net	2022-06-22
aghlovahy.com	2022-06-22
agoracomplex.com	2022-05-31
alotasvirgar.ir	2022-06-22
behnamasrollahi.ir	2022-06-22
bemanbespar.ir	2022-06-22
bimehnama.com	2022-05-31
binazirshop.com	2022-05-31
bizilyapp.com	2022-06-22
bodyspinners.com	2022-05-31
bornosmode.com	2022-06-22
brifenews.ir	2022-06-22
carbill.ir	2022-06-22
cert.ir	2022-06-23
chang.ir	2022-03-18
chargoan.com	2022-06-04
diatech.ir	2022-06-22
drpayamhayati.com	2022-05-31
electro-tech.ir	2022-06-22

تعداد زیادی سایت روی این سرور قرار دارند که نام های آن ها در تصویر موجود است.

```
Reverse IP results for 7peykar.ir (185.143.233.41, 185.143.234.41)
=====
```

```
Reverse IP results for abrmarketing.net (185.143.233.41, 185.143.234.41)
=====
```

همانطور که میبینم ادرس آی پی آن ها نیز با cert.ir برابر است.

سوال ۶ :

در فرمت پیام درخواستی کلاینت از سرور پروتکل HTTP 1.1 یک هدر بنام host وجود دارد که در آن مشخص می شود کدام وبسایت با وجود آدرس IP های یکسان انتخاب شود.

منبع :

<https://serverfault.com/questions/106882/how-do-you-have-one-ip-address-and-many-websites>

سوال ۷: برای لیست کردن برنامه هایی که در حال حاضر پورت های لایه انتقال را بر روی سیستم باز کرده اند، از چه دستور خط فرمانی استفاده می شود؟

سوال ۷ :

با دستور netstat -an این لیست مشاهده می شود.

```
C:\Users\ASUS>netstat -an

Active Connections

Proto Local Address           Foreign Address         State
TCP    0.0.0.0:135               0.0.0.0:0               LISTENING
TCP    0.0.0.0:443              0.0.0.0:0               LISTENING
TCP    0.0.0.0:445              0.0.0.0:0               LISTENING
TCP    0.0.0.0:902              0.0.0.0:0               LISTENING
TCP    0.0.0.0:912              0.0.0.0:0               LISTENING
TCP    0.0.0.0:1042             0.0.0.0:0               LISTENING
TCP    0.0.0.0:1043             0.0.0.0:0               LISTENING
TCP    0.0.0.0:5040             0.0.0.0:0               LISTENING
TCP    0.0.0.0:5357             0.0.0.0:0               LISTENING
TCP    0.0.0.0:7680             0.0.0.0:0               LISTENING
TCP    0.0.0.0:9012             0.0.0.0:0               LISTENING
TCP    0.0.0.0:9013             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    0.0.0.0:49670            0.0.0.0:0               LISTENING
TCP    0.0.0.0:49680            0.0.0.0:0               LISTENING
TCP    0.0.0.0:49681            0.0.0.0:0               LISTENING
TCP    10.0.85.2:139            0.0.0.0:0               LISTENING
TCP    10.0.85.2:49154          131.253.33.254:443      TIME_WAIT
TCP    10.0.85.2:49157          204.79.197.200:443      TIME_WAIT
TCP    10.0.85.2:49160          204.79.197.200:443      ESTABLISHED
TCP    10.0.85.2:49163          204.79.197.200:443      ESTABLISHED
TCP    10.0.85.2:49570          167.235.234.219:443    ESTABLISHED
TCP    10.0.85.2:49571          167.235.234.219:443    ESTABLISHED
TCP    10.0.85.2:50093          74.125.200.93:443      ESTABLISHED
TCP    10.0.85.2:50542          1.1.1.1:53              TIME_WAIT
TCP    10.0.85.2:50545          204.79.197.200:443      ESTABLISHED
TCP    10.0.85.2:51205          1.1.1.1:53              TIME_WAIT
TCP    10.0.85.2:51616          20.198.162.78:443      ESTABLISHED
TCP    10.0.85.2:51910          13.107.42.12:443        CLOSE_WAIT
TCP    10.0.85.2:52441          1.1.1.1:53              TIME_WAIT
TCP    10.0.85.2:52444          74.125.200.94:443      ESTABLISHED
TCP    10.0.85.2:52710          1.1.1.1:53              TIME_WAIT
TCP    10.0.85.2:53237          52.98.71.210:443        CLOSE_WAIT
TCP    10.0.85.2:53525          142.250.4.149:443      ESTABLISHED
TCP    10.0.85.2:54502          74.125.130.106:443     ESTABLISHED
TCP    10.0.85.2:54591          1.1.1.1:53              TIME_WAIT
TCP    10.0.85.2:54701          140.82.112.26:443      ESTABLISHED
```

سوال ۸: دستوری را پیدا کنید که به وسیله آن تمام پورت های سیستم در هر وضعیت اتصالی همراه با مبدا و مقصد اتصال به صورت عددی لیست شوند.

سوال ۸:

با دستور : `netstat -aon | findstr` این لیست مشاهده می شود.

برای مثال :

`netstat -na | find "80"`

```
C:\Users\ASUS>netstat -na | find "80"
TCP    0.0.0.0:7680          0.0.0.0:0            LISTENING
TCP    0.0.0.0:49680         0.0.0.0:0            LISTENING
TCP    10.0.85.2:52080      1.1.1.1:53           TIME_WAIT
TCP    10.0.85.2:56979      117.18.237.29:80     TIME_WAIT
TCP    10.0.85.2:58085      1.1.1.1:53           TIME_WAIT
TCP    10.0.85.2:58088      142.250.4.132:443    ESTABLISHED
TCP    10.0.85.2:58090      142.250.4.132:443    TIME_WAIT
TCP    10.0.85.2:58094      142.251.10.101:443   ESTABLISHED
TCP    10.0.85.2:58095      142.251.10.101:443   TIME_WAIT
TCP    127.0.0.1:1081       127.0.0.1:51880      TIME_WAIT
TCP    127.0.0.1:1081       127.0.0.1:56780      TIME_WAIT
TCP    127.0.0.1:1081       127.0.0.1:58089      ESTABLISHED
TCP    127.0.0.1:1081       127.0.0.1:58096      ESTABLISHED
TCP    127.0.0.1:56980      127.0.0.1:1081      TIME_WAIT
TCP    127.0.0.1:58086      127.0.0.1:1081      TIME_WAIT
TCP    127.0.0.1:58089      127.0.0.1:1081      ESTABLISHED
TCP    127.0.0.1:58091      127.0.0.1:1081      TIME_WAIT
TCP    127.0.0.1:58096      127.0.0.1:1081      ESTABLISHED
TCP    127.0.0.1:58097      127.0.0.1:1081      TIME_WAIT
TCP    172.20.10.3:58087    194.124.35.42:812    TIME_WAIT
TCP    172.20.10.3:58092    194.124.35.42:812    ESTABLISHED
TCP    172.20.10.3:58093    194.124.35.42:812    TIME_WAIT
TCP    172.20.10.3:58098    194.124.35.42:812    ESTABLISHED
TCP    172.20.10.3:61380    194.124.35.42:812    ESTABLISHED
TCP    [::]:7680            [::]:0               LISTENING
UDP    [fe80::3d38:5eae:6b3d:18ab%24]:1900 *:*
UDP    [fe80::3d38:5eae:6b3d:18ab%24]:59657 *:*
UDP    [fe80::7123:2894:ccbf:36e3%21]:1900 *:*
UDP    [fe80::7123:2894:ccbf:36e3%21]:59656 *:*
UDP    [fe80::8918:aa72:36bf:45a4%25]:1900 *:*
UDP    [fe80::8918:aa72:36bf:45a4%25]:59654 *:*
UDP    [fe80::a919:8333:a301:930%7]:1900 *:*
UDP    [fe80::a919:8333:a301:930%7]:59655 *:*
```

C:\Users\ASUS>

۱. در این بخش می‌خواهیم با استفاده از ابزار ncat و پروتکل HTTP یک ارتباط با وب سرور دانشگاه ایجاد کنیم. CMD را باز کرده و با استفاده از دستور زیر ابتدا یک ارتباط TCP با aut.ac.ir روی پورت ۸۰ ایجاد کنید.

```
ncat -v aut.ac.ir 80
```

۲. در ادامه پیام HTTP مربوط به دریافت آدرس / را مطابق دستورات زیر وارد کنید. پس از فشردن دکمه enter در خط دوم یکبار دیگر enter را وارد کنید.

```
GET / HTTP/1.1
```

```
Host: aut.ac.ir
```

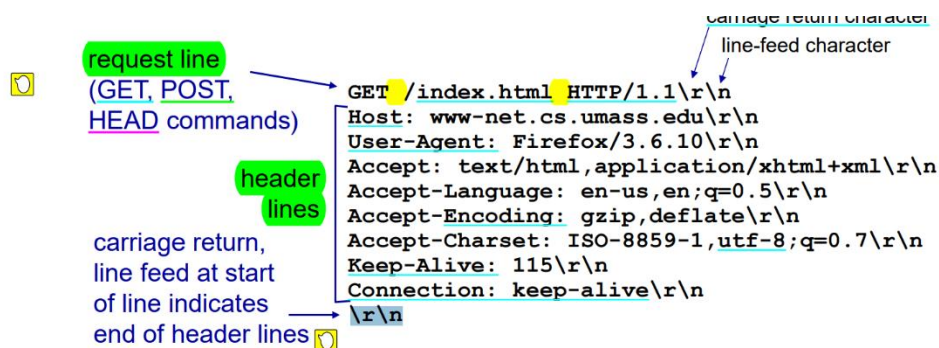
سوال ۹: دلیل وارد کردن دو enter پشت سر هم چیست؟

سوال ۱۰: پیامی که در پاسخ تقاضای شما داده می‌شود چیست؟ صفحه‌ی اصلی در کجا قرار دارد؟ ادعای خود را با استفاده از تقاضا به همین صفحه در مرورگر و ضبط پیام‌ها با استفاده از wireshark اثبات کنید.

سوال ۱۱: آیا این ارتباط persistent است؟

سوال ۹:

هر درخواست HTTP دارای صفر یا بیشتر هدر است و در انتهای هدر یک خط خالی وجود دارد (و بعد از آن body اگر نیاز باشد). بنابراین اینتر اول برای خط خالی پس از هدر و اینتر دوم برای ارسال درخواست است. در شکل زیر این خط خالی (\r\n) با آبی کمرنگ انتخاب شده است و در انتهای header lines می‌باشد



* Check out the online interactive exercises for more examples: http://gaia.cs.umass.edu/kurose_ross/interactive/

Application Layer 2-27

سوال ۱۰ :

```
C:\Users\ASUS>ncat -C aut.ac.ir 80
GET / HTTP/1.1
Host: aut.ac.ir

HTTP/1.1 301 Moved Permanently
Date: Fri, 24 Jun 2022 07:35:00 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>
```

به این معنا که این صفحه انتقال پیدا کرده است.

حال از طریق وایر شارک:

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

HTTP/1.1 301 Moved Permanently
```

دقیقا همان پاسخ بالا است یعنی انتقال یافته صفحه به اصطلاح رب دایرکت.

سوال ۱۱:

باتوجه به اینکه فیلد Connection در پیام درخواست مقدار ندارد و از HTTP 1.1 استفاده شده، مقدار پیشفرض این فیلد Keep-Alive است و درنتیجه ارتباط persistent خواهد بود. اگر از HTTP 1.0 استفاده می‌شد پیشفرض این فیلد Close و درنتیجه non-persistent می‌بود.

سوال ۱۲: این پورت بر روی کدام آدرس IP bind شده است؟ بعد از برقراری ارتباط با این سوکت، برنامه CMD نیز اجرا می‌شود. در ادامه دستوراتی که فرستنده ارسال کند به این برنامه داده می‌شوند و خروجی دستورات از طریق ارتباط برقرار شده منتقل خواهد شد.

سوال ۱۲ :

روی آدرس ۰/۰/۰/۰ که همان خروجی سیستم است که در اینجا برابر :


```
Pv4 Address. . . . . : 192.168.136.1(Preferred)
0.0.0.0:0.0.0.0 LISTENING
ArmourySocketServer.exe]
TCP 0.0.0.0:16000 0.0.0.0:0 LISTENING
ncat.exe]
```

آدرس بالا است.

سوال ۱۳: دقت کنید یک خط خالی بین HTTP و <html> باید وجود داشته باشد. به نظر شما دلیل وجود خط اول در این فایل چیست؟ یک فایل دیگر بدون خط اول این فایل بسازید و نتیجه را امتحان کنید.

سوال ۱۳:

اگر خط اول را پاک کنیم محتوای نمایش داده شده همان قسمت html... خواهد بود و نه کلمه !salam .

این خط هدر این پیام است اگر بخواهد یک درخواست HTTP باشد. در صورت عدم وجود این خط، این پیام بعنوان درخواست (request) HTTP توسط مرورگر دیده نمی‌شود و فقط قسمت html بعنوان یک پیام ساده در مرورگر چاپ می‌شود و نه آبجکت html.



Salam!

بدون اینتر :

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,fa;q=0.8
Cookie: _ga=GA1.1.446602934.1618377866; _ga_Y43NRD378Z=GS1.1.1618377865.1.0.1618377868.0; _hantanaUser=a7ytocfsb; _ga_K32PRE3205=GS1.1.1631963485.20.1.1631966836.0; csrftoken=16x0DncGzHMQ6L25U10RyVegq72Z2aF6c6j0xva27tsNcpezhTRRQ1qiVfy; username=127-0-0-1-8888-2[1:0]10:1654344708[23:username=127-0-0-1-8888[44:ZjVlPDBmY2E5ODY0MGYzNzhINDkxZTJlNDZlZlQ4YmU-835486a5a692eb1cd92f17f5ff178967281198b383581a26cd631b90d58f5e7d"; _xsrf=2[b858219]92cd77b1d5082b505425480492fbcc06[1654344708

S:\uni6\GN LAB\AUT-Computer-Network-Course-Lab\LAB4\ncat -l -p 4444 < index.html
GET / HTTP/1.1
Host: 127.0.0.1:4444
Connection: keep-alive
Cache-Control: max-age=0
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="102", "Google Chrome";v="102"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,fa;q=0.8
Cookie: _ga=GA1.1.446602934.1618377866; _ga_Y43NRD378Z=GS1.1.1618377865.1.0.1618377868.0; _hantanaUser=a7ytocfsb; _ga_K32PRE3205=GS1.1.1631963485.20.1.1631966836.0; csrftoken=16x0DncGzHMQ6L25U10RyVegq72Z2aF6c6j0xva27tsNcpezhTRRQ1qiVfy; username=127-0-0-1-8888-2[1:0]10:1654344708[23:username=127-0-0-1-8888[44:ZjVlPDBmY2E5ODY0MGYzNzhINDkxZTJlNDZlZlQ4YmU-835486a5a692eb1cd92f17f5ff178967281198b383581a26cd631b90d58f5e7d"; _xsrf=2[b858219]92cd77b1d5082b505425480492fbcc06[1654344708
```

که در امتحان من یک صفحه خالی را بالا آورد که اطلاعاتی ندارد احتمالا به خاطر مرورگر

سوال ۱۴: سیستم عامل این وب سایت چیست؟

سوال ۱۵: چه پورت هایی روی این سرور باز است؟

سوال ۱۶: سرویس هایی که از طریق این پورت ها ارائه می شود چیست؟

سوال ۱۴:

در پاسخ من یافت نکرد اما برای دوستان لینوکس ورژن ۴/۴

```
OS CPE: cpe:/o:nodemcu:nodemcu cpe:/a:lwip_project:lwip cpe:/
h:hp:laserjet_2200dtn cpe:/h:hp:jetdirect_2591a cpe:/
h:philips:hue_bridge cpe:/a:lwip_project:lwip:1.4
Aggressive OS guesses: NodeMCU firmware (lwIP stack) (95%), Espressif
esp8266 firmware (lwIP stack) (94%), ESPEasy OS (lwIP stack) (90%), HP
LaserJet 2200dtn printer (88%), HP JetDirect 2591A print server (87%),
HP LaserJet 4050 printer (87%), HP LaserJet 4MV or 4000TN printer (87%
), Philips Hue Bridge (lwIP stack v1.4.0) (87%), Cognex DataMan 200 ID
reader (lwIP TCP/IP stack) (87%), Enlogic PDU (FreeRTOS/lwIP) (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

سوال ۱۵:

و سوال ۱۶:

Port	Protocol	State	Service	Version
1	tcp	open	tcpmux	
3	tcp	open	tcpwrapped	
4	tcp	open	tcpwrapped	
6	tcp	open	unknown	
7	tcp	open	echo	
9	tcp	open	discard	
13	tcp	open	tcpwrapped	
17	tcp	open	qotd	
19	tcp	open	chargen	
20	tcp	open	ftp-data	
21	tcp	open	ftp	
22	tcp	open	ssh	
23	tcp	open	tcpwrapped	
24	tcp	open	tcpwrapped	
25	tcp	open	tcpwrapped	
26	tcp	open	tcpwrapped	
30	tcp	open	unknown	
32	tcp	open	unknown	
33	tcp	open	dsp	
37	tcp	open	time	
42	tcp	open	nameserver	
43	tcp	open	whois	
49	tcp	open	tacacs	
53	tcp	open	domain	
70	tcp	open	tcpwrapped	
79	tcp	open	finger	

انواع پرت ها باز است که سرویس های آن ها قابل مشاهده است.