

به نام خدا

نام و نام خانوادگی : روزینا کاشفی

شماره دانشجویی: ۹۸۳۱۱۱۸

کار با کاربردهای Web، DNS، سوکت و پویس سرویس ها

• کارکرد DNS

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

دامنه به نام علیرضا باقری ثبت شده است. بخشی از اطلاعات این دامنه مانند آدرس و تلفن مالک آن را در زیر می بینیم .

```
domain: soft98.ir
ascii: soft98.ir
remarks: (Domain Holder) alireza bagheri
remarks: (Domain Holder Address) Shariat: .rzapour-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
```






سوال (۲) آدرس name server آن چیست؟

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


سوال ۳) رکوردهای NS، A، TXT، MX را مشخص کنید. هر یک از این رکوردها چه چیزی را مشخص می کنند؟

رکورد NS: این رکوردها مشخص می کنند که در ادامه ی فلایند ترجمه نام دامنه به آدرس IP باید به کدام name server معتبر درخواست بفرستیم .

Parent Nameserver Tests




Status	Test Case	Information
	NS records listed at parent servers	Nameserver records returned by the parent servers are: <div> ir1.hostdl.com. [NO GLUE] [TTL=1440] ir2.hostdl.com. [NO GLUE] [TTL=1440] </div> 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!
	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).

Local Nameserver Tests

Status	Test Case	Information
	NS records at your local servers	NS records retrieved from your local nameservers were: <div> ir1.hostdl.com. [NO GLUE] [TTL=86400] ir2.hostdl.com. [NO GLUE] [TTL=86400] </div>

رکورد A: این رکورد که نام آن مخفف Address است، شامل آدرس IP درخواستی است .











WWW Record Tests

Status	Test Case	Information
	WWW record	www.soft98.ir A records are: <div> www.soft98.ir. CNAME soft98.ir. [TTL=14400] soft98.ir. A 79.127.127.35 [TTL=14400] </div>
	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.

رکورد TXT: مخفف text است. رکوردی است که در آن اطلاعات اضافی می شود که توسط domain در رکوردهای DNS مربوط به آن گذاشته می شود و می تواند شامل یک سری دستورالعمل ها برای انسان ها یا ماشین ها باشد یا برای شناسایی قابل اطمینان بودن منبع ایمیل مورد استفاده قرار گیرد. که البته در این پویش چنین رکوردی یافت نشد .



رکورد MX: استفاده از این رکورد برای مشخص کردن mail server ایست که مسئول دریافت ایمیل‌های این دامنه می‌باشد.

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.

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

برای این کار باید رکوردهای MX را بررسی کنیم که در تصویر زیر می‌بینیم. ادرس mail server دانشگاه عبارت است از asg.aut.ac.ir و ادرس IP آن هم ۱۸۵.۲۱۱.۸۸.۲۰ می‌باشد که از A رکورد بدست می‌آید.

Status	Test Case	Information
	MX Records	Your Mail eXchanger (MX) records are: 5 asg.aut.ac.ir. [TTL=3600]
	MX records have reverse DNS entries	Good! All your MX IP addresses have reverse DNS entries. The reverse entries returned were: 20.88.211.185.in-addr.arpa <--> asg525.aut.ac.ir.

سوال ۵) چه وبسایت‌های دیگری بر روی همین سرور قرار دارند؟ چند مورد از آن‌ها را نام ببرید.

```
Reverse IP results for cert.ir (185.143.233.5, 185.143.234.5)
=====
```

141.ir
1zodpaz.ir
24talk.ir
3pco.ir

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

زمانی که مرورگر یک درخواست HTTP ارسال می‌کند، در هدر آن مقدار Host را برابر نام دامنه مورد نظر قرار می‌دهد. این روش که به نوعی Multiplexing است، میتواند نام دامنه‌های زیادی را روی یک سرور میزبانی کرد.

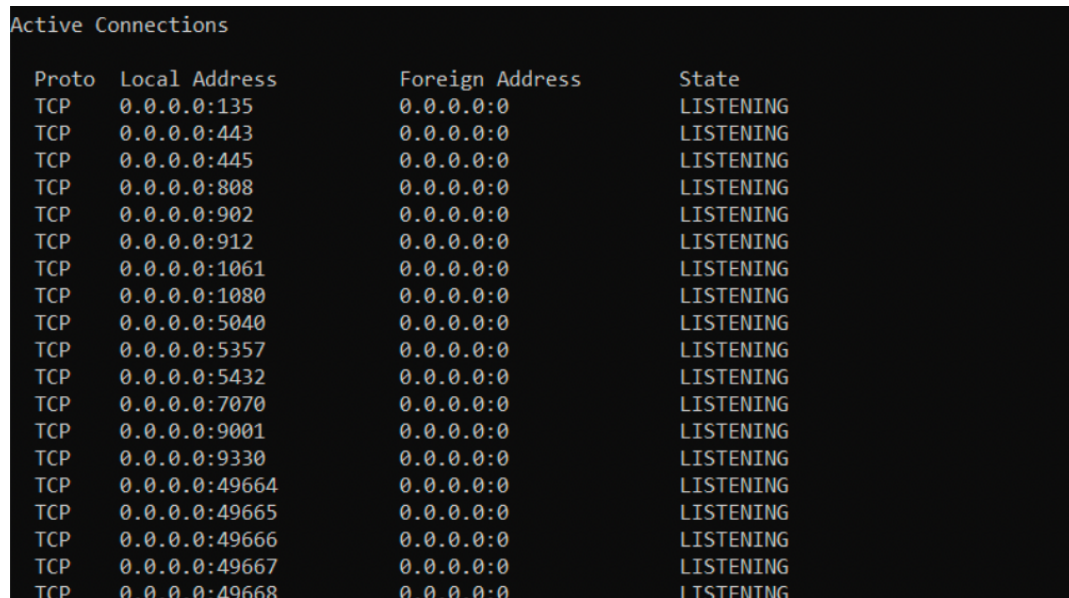
سوال ۷) برای لیست کردن برنامه‌هایی که در حال حاضر پورت‌های لایه انتقال را بر روی سیستم باز کرده‌اند، از چه دستور خط فرمانی استفاده می‌شود؟

با دستور `netstat -b` می‌توان برنامه‌هایی که پورتهای را استفاده می‌کنند مشاهده کرد. سوئیچ `-b` شماره پراسس برنامه‌ها نشان می‌دهند.

Active Connections			
Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:1028	www:9330	ESTABLISHED
[msedgewebview2.exe]			
TCP	127.0.0.1:1030	www:1036	ESTABLISHED
[firefox.exe]			
TCP	127.0.0.1:1035	www:1037	ESTABLISHED
[firefox.exe]			
TCP	127.0.0.1:1036	www:1030	ESTABLISHED
[firefox.exe]			
TCP	127.0.0.1:1037	www:1035	ESTABLISHED
[firefox.exe]			
TCP	127.0.0.1:1039	www:1040	ESTABLISHED
[firefox.exe]			
TCP	127.0.0.1:1040	www:1039	ESTABLISHED
[firefox.exe]			
TCP	127.0.0.1:1043	www:1045	ESTABLISHED
[firefox.exe]			
TCP	127.0.0.1:1045	www:1043	ESTABLISHED
[firefox.exe]			
TCP	127.0.0.1:1045	www:1046	ESTABLISHED
[firefox.exe]			
TCP	127.0.0.1:1046	www:1045	ESTABLISHED
[firefox.exe]			

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

برای این کار از همان netstat با سوییچ‌های -a برای نشان دادن تمام پورت‌ها و -n برای نشان دادن به صورت عددی استفاده کرد. (netstat -an)



The screenshot shows the output of the netstat -an command. It lists active connections with columns for Protocol, Local Address, Foreign Address, and State. All connections are in the LISTENING state.

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	0.0.0.0:808	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	0.0.0.0:1061	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1080	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	0.0.0.0:5432	0.0.0.0:0	LISTENING
TCP	0.0.0.0:7070	0.0.0.0:0	LISTENING
TCP	0.0.0.0:9001	0.0.0.0:0	LISTENING
TCP	0.0.0.0:9330	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

• کارکرد Web

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

جدا کننده request Header و request Body یک خط خالی است. پس برای نشان دادن اینکه header تمام شده باید یک بار دیگر enter بزنیم.

سوال ۱۰) پیامی که در پاسخ تقاضای شما داده می‌شود چیست؟ صفحه 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.

پاسخ درخواست به صورت زیر است و با ارور ۳۰۱ مواجه می‌شویم که به معنی moved permanently است و با بررسی این پاسخ مشخص است که آدرس جدیدی که دامنه به آن منتقل شده است <https://aut.ac.ir:۴۳۳> می‌باشد.


```

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

HTTP/1.1 301 Moved Permanently
Date: Wed, 23 Jun 2021 17:36:36 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
373	11.346117	192.168.1.103	185.211.88.131	TCP	66	14913 → 80 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM=1
374	11.346428	192.168.1.103	185.211.88.131	TCP	66	1027 → 80 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM=1
375	11.377200	185.211.88.131	192.168.1.103	TCP	62	80 → 14913 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1390 SACK_PERM=1
376	11.377262	192.168.1.103	185.211.88.131	TCP	54	14913 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
377	11.377624	192.168.1.103	185.211.88.131	HTTP	668	GET / HTTP/1.1
378	11.378506	185.211.88.131	192.168.1.103	TCP	62	80 → 1027 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1390 SACK_PERM=1
379	11.378568	192.168.1.103	185.211.88.131	TCP	54	1027 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
380	11.420135	185.211.88.131	192.168.1.103	TCP	60	80 → 14913 [ACK] Seq=1 Ack=615 Win=30086 Len=0
381	11.421719	185.211.88.131	192.168.1.103	HTTP	528	HTTP/1.1 301 Moved Permanently (text/html)
382	11.423898	192.168.1.103	185.211.88.131	TCP	66	32164 → 443 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM=1
383	11.454012	185.211.88.131	192.168.1.103	TCP	62	443 → 32164 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1390 SACK_PERM=1
384	11.454172	192.168.1.103	185.211.88.131	TCP	54	32164 → 443 [ACK] Seq=1 Ack=1 Win=17520 Len=0
385	11.454770	192.168.1.103	185.211.88.131	TLShv1.2	571	Client Hello
386	11.462327	192.168.1.103	185.211.88.131	TCP	54	14913 → 80 [ACK] Seq=615 Ack=475 Win=17046 Len=0
387	11.495781	185.211.88.131	192.168.1.103	TCP	60	443 → 32164 [ACK] Seq=1 Ack=518 Win=30016 Len=0
391	11.509858	185.211.88.131	192.168.1.103	TLShv1.2	1444	Server Hello
392	11.511241	185.211.88.131	192.168.1.103	TCP	622	[TCP Previous segment not captured] 443 → 32164 [PSH, ACK] Seq=2781 Ack=518
393	11.511331	192.168.1.103	185.211.88.131	TCP	66	32164 → 443 [ACK] Seq=518 Ack=1391 Win=17520 Len=0 SLE=2781 SRE=3349
394	11.514258	185.211.88.131	192.168.1.103	TCP	1444	[TCP Out-Of-Order] 443 → 32164 [ACK] Seq=1391 Ack=518 Win=30016 Len=1390
395	11.514370	192.168.1.103	185.211.88.131	TCP	54	32164 → 443 [ACK] Seq=518 Ack=3349 Win=17520 Len=0
396	11.530274	192.168.1.103	185.211.88.131	TLShv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
397	11.530776	192.168.1.103	185.211.88.131	TLShv1.2	886	Application Data
399	11.565680	185.211.88.131	192.168.1.103	TLShv1.2	105	Change Cipher Spec, Encrypted Handshake Message
400	11.606770	192.168.1.103	185.211.88.131	TCP	54	32164 → 443 [ACK] Seq=1476 Ack=3400 Win=17469 Len=0
401	11.617279	185.211.88.131	192.168.1.103	TCP	60	443 → 32164 [ACK] Seq=3400 Ack=1476 Win=31616 Len=0
402	11.827471	185.211.88.131	192.168.1.103	TLShv1.2	364	[TCP Previous segment not captured] , Ignored Unknown Record
403	11.827562	192.168.1.103	185.211.88.131	TCP	66	[TCP Dup ACK 400#1] 32164 → 443 [ACK] Seq=1476 Ack=3400 Win=17469 Len=0 SLE
404	11.830165	185.211.88.131	192.168.1.103	TCP	1444	[TCP Out-Of-Order] 443 → 32164 [ACK] Seq=3400 Ack=1476 Win=31616 Len=1390
405	11.830289	192.168.1.103	185.211.88.131	TCP	54	32164 → 443 [ACK] Seq=1476 Ack=5100 Win=17520 Len=0
406	11.834968	185.211.88.131	192.168.1.103	TLShv1.2	1444	[TCP Previous segment not captured] , Ignored Unknown Record
> Frame 381: 528 bytes on wire (4224 bits), 528 bytes captured (4224 bits) on interface \Device\NPF_{06D8CCB2-7CC6-46ED-9FEA-E154E3CD055D}, id 0						
> Ethernet II, Src: Tp-LinkTf2:55:60 (18:a6:f7:f2:55:60), Dst: AzureWav_1e:36:59 (08:c5:f2:1e:36:59)						
> Internet Protocol Version 4, Src: 185.211.88.131, Dst: 192.168.1.103						
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 14913, Seq: 1, Ack: 615, Len: 474						
Source Port: 80						
Destination Port: 14913						
[Stream index: 41]						
[TCP Segment Len: 474]						
Sequence Number: 1 (relative sequence number)						

همانطوری که مشاهده می‌کنید، ابتدا درخواست HTTP برای پورت ۸۰ سرور فرستاده می‌شود و با پیام moved permanently رو به رو می‌شود و پس از استفاده از پروتکل TLS و به دست‌آوردن key، ادامه‌ی ارتباط روی پورت ۴۴۳ خواهد بود.

سوال (۱۱) آیا این ارتباط **persistent** است؟

از آنجایی که در هدر درخواست HTTP مشخص نکردیم که مقدار Keep-Alive چه باشد و نوع Connection را نیز تعیین نکردیم، این مقادیر به در ورژن HTTP ۱.۱ به صورت دیفالت برای یک اتصال persistent تنظیم می‌شوند.

سوال (۱۲) این پورت بر 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.

با ورود این دستور، هرگاه به پورت ۱۶۰۰۰ درخواستی فرستاده شود، cmd اجرا خواهد شد. آدرس bind IP شده ۰.۰.۰.۰ است.

```
Ncat: Listening on :::16000
Ncat: Listening on 0.0.0.0:16000
```

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.

دلیل وجود خط اول آن است که بعد از اینکه درخواست http برای این سرور ارسال شد، این سرور در پاسخی که برای کلاینت ارسال می‌کند ابتدا در یک خط status code به درخواست http پاسخ می‌دهد که وجود این خط در پاسخ‌های http الزامی است در حالی که هدرهای بعد از آن اختیاری هستند و در انتهای خطوط مربوط به هدر یک enter اضافی می‌گذاریم که اتمام هدر http را نشان می‌دهد و در سوال ۹ نیز به آن اشاره کردیم که این enter نهایی هم اجباری است و در نهایت data مورد درخواست کاربر که یک فایل html است را قرار می‌دهیم.

• پوشش سرویس‌ها

سوال (۱۴) سیستم‌عامل این وبسایت چیست؟

```
Device type: WAP|phone
Running: Linux 2.4.X|2.6.X, Sony Ericsson embedded
OS CPE: cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6.22 cpe:/
h:sonyericsson:u8i_vivaz
OS details: Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony
Ericsson U8i Vivaz mobile phone
```

سوال (۱۵) چه پورت‌هایی روی این سرور باز است؟

۸۰ http / ۴۴۳ https

Hosts	Services	Nmap Output	Ports / Hosts	Topology	Host Details	Scans
Service	Hostname	Port	Protocol	State	Version	
tcpwrapped	aut.ac.ir (185.211.88.131)	443	tcp	open		
	aut.ac.ir (185.211.88.131)	80	tcp	open		

سوال (۱۶) سرویس‌هایی که از طریق این پورت‌ها ارائه می‌شود چیست؟

سرویس tcpwrapped در این پورت‌ها ارائه می‌شود. روی پورت ۸۰ http و ۴۴۳ https ارائه می‌شود.