

به نام خدا



---

# کار با کارکرد های WEB, DNS

---

فصل دو، آزمایش دو



محمد جواد زندیه ۹۸۳۱۰۳۲

۲۱ اردیبهشت ۱۴۰۰

دانشکده مهندسی کامپیوتر، دانشگاه صنعتی امیرکبیر

سوال ۱:

remarks: (Domain Holder) alireza Bagheri

person: alireza bagheri

e-mail: [soft98.ir@gmail.com](mailto:soft98.ir@gmail.com)

سوال ۲:

nserver: ir1.hostdl.com

nserver: ir2.hostdl.com

سوال ۳:










NS: name server : حاوی نام سرور معتبر، به همراه یک دامنه یا منطقه برای DNS می باشد. وقتی که یک کاربر برای یک آدرس ip درخواست می کند، میتواند آدرس ip خود را از یک رکورد NS از طریق جست و جوی DNS پیدا کند.

A: address : آدرس ip دامنه درخواست شده را تعیین می کند.






TXT: تعیین مالکیت دامنه و اطمینان از منیت ایمیل از جمله کاربرد های آن است.

MX: mail exchange : ایمیل را به mail server هدایت می کند. رکورد MX نشان می دهد که چگونه پیام های ایمیل باید مطابق با پروتکل انتقال نامه ساده (SMTP، پروتکل استاندارد برای همه ایمیل ها) مسیریابی شوند. مانند رکوردهای CNAME، یک رکورد MX همیشه باید به دامنه دیگری اشاره کند.



#### 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.

#### Parent Nameserver Tests




Status	Test Case	Information
	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!
	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: ir1.hostdl.com. [NO GLUE] [TTL=86400] ir2.hostdl.com. [NO GLUE] [TTL=86400]
	Glue at local nameservers	Oops! Your local nameservers don't return IP addresses (glue) along with your NS records! This isn't a fatal error but means an extra lookup needs to be performed increasing the load time to your site. You can fix this by adding A records for each of the nameservers listed above.

سوال ۴:

#### WWW Record Tests


Status	Test Case	Information
	WWW record	www.aut.ac.ir A records are: www.aut.ac.ir. A 185.211.88.131 [TTL=3600]
	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	OK! You don't have a CNAME entry for your WWW record! This is ok though because you have an A record for your WWW record. When people visit www.aut.ac.ir they will go to the IP address in the A record above.

سوال ۵:

[behnamasrollahi.ir](http://behnamasrollahi.ir) , [jeanswest.club](http://jeanswest.club) , [repex.ir](http://repex.ir)

## Reverse IP Domain Check

Remote Address

 Found 2 domains hosted on the same web server as 185.143.233.41.

[repex.ir](http://repex.ir)

[www.cert.ir](http://www.cert.ir)

# Reverse IP Domain Check

Remote Address

Check

Found 2 domains hosted on the same web server as 185.143.234.41.

behnamnasrollahi.ir

jeanswest.club

behnamnasrollahi.ir (185.143.233.41, 185.143.234.41)

jeanswest.club (185.143.233.41, 185.143.234.41)

repex.ir (185.143.234.41, 185.143.233.41)

cert.ir (185.143.233.41, 185.143.234.41)

آدرس ip همگی یکسان است.

سوال ۶: بله همانند مالتی پلکسینگ آدرس آپی وب سرور مربوطه جست و جو میشود. مرورگر مورد استفاده از طریق جستجو در حافظه کش خود یا با استفاده از DNS ها آدرس IP را به دست می آورد. سپس تشخیص می دهد اطلاعات سایت شما در چه مسیری قرار دارد.

سوال ۷: دستور netstat -a ارتباط های فعال را به ما می دهد.

```
C:\Users\Javad\Desktop\cmd.exe
λ netstat -a

Active Connections

Proto Local Address           Foreign Address         State
TCP    0.0.0.0:135             DESKTOP-95J4G2F:0      LISTENING
TCP    0.0.0.0:443             DESKTOP-95J4G2F:0      LISTENING
TCP    0.0.0.0:445             DESKTOP-95J4G2F:0      LISTENING
TCP    0.0.0.0:980             DESKTOP-95J4G2F:0      LISTENING
TCP    0.0.0.0:912             DESKTOP-95J4G2F:0      LISTENING
TCP    0.0.0.0:5040            DESKTOP-95J4G2F:0      LISTENING
TCP    0.0.0.0:5357            DESKTOP-95J4G2F:0      LISTENING
TCP    0.0.0.0:47546           DESKTOP-95J4G2F:0      LISTENING
TCP    0.0.0.0:49664           DESKTOP-95J4G2F:0      LISTENING
TCP    0.0.0.0:49665           DESKTOP-95J4G2F:0      LISTENING
TCP    0.0.0.0:49666           DESKTOP-95J4G2F:0      LISTENING
TCP    0.0.0.0:49667           DESKTOP-95J4G2F:0      LISTENING
TCP    0.0.0.0:49668           DESKTOP-95J4G2F:0      LISTENING
TCP    0.0.0.0:49696           DESKTOP-95J4G2F:0      LISTENING
TCP    127.0.0.1:8307          DESKTOP-95J4G2F:0      LISTENING
TCP    127.0.0.1:50041         DESKTOP-95J4G2F:0      LISTENING
TCP    127.0.0.1:50041         care-eyes:62693        ESTABLISHED
TCP    127.0.0.1:62658         DESKTOP-95J4G2F:0      LISTENING
TCP    127.0.0.1:62658         care-eyes:62679        ESTABLISHED
TCP    127.0.0.1:62677         DESKTOP-95J4G2F:0      LISTENING
TCP    127.0.0.1:62677         care-eyes:62716        ESTABLISHED
TCP    127.0.0.1:62677         care-eyes:62717        ESTABLISHED
TCP    127.0.0.1:62679         care-eyes:62658        ESTABLISHED
TCP    127.0.0.1:62693         care-eyes:50041        ESTABLISHED
TCP    127.0.0.1:62712         care-eyes:62677        TIME_WAIT
TCP    127.0.0.1:62713         care-eyes:62677        TIME_WAIT
TCP    127.0.0.1:62716         care-eyes:62677        ESTABLISHED
TCP    127.0.0.1:62717         care-eyes:62677        ESTABLISHED
TCP    192.168.56.1:139        DESKTOP-95J4G2F:0      LISTENING
TCP    192.168.88.1:139        DESKTOP-95J4G2F:0      LISTENING
TCP    192.168.110.1:139       DESKTOP-95J4G2F:0      LISTENING
TCP    192.168.253.76:139      DESKTOP-95J4G2F:0      LISTENING
TCP    192.168.253.76:62620    ec2-54-76-29-49:http   ESTABLISHED
TCP    192.168.253.76:62628    ec2-54-76-166-0:http   ESTABLISHED
TCP    192.168.253.76:62632    20.198.162.78:https    ESTABLISHED
```

سوال ۸:

با دستور netstat -q میتوان این کار را انجام داد

```

C:\Users\Javad\Desktop\cmd.exe
λ netstat -q

Active Connections

Proto Local Address           Foreign Address         State
TCP    0.0.0.0:135             DESKTOP-95J4G2F:0      LISTENING
TCP    0.0.0.0:443             DESKTOP-95J4G2F:0      LISTENING
TCP    0.0.0.0:445             DESKTOP-95J4G2F:0      LISTENING
TCP    0.0.0.0:980             DESKTOP-95J4G2F:0      LISTENING
TCP    0.0.0.0:912             DESKTOP-95J4G2F:0      LISTENING
TCP    0.0.0.0:5848            DESKTOP-95J4G2F:0      LISTENING
TCP    0.0.0.0:5357            DESKTOP-95J4G2F:0      LISTENING
TCP    0.0.0.0:47546           DESKTOP-95J4G2F:0      LISTENING
TCP    0.0.0.0:49664           DESKTOP-95J4G2F:0      LISTENING
TCP    0.0.0.0:49665           DESKTOP-95J4G2F:0      LISTENING
TCP    0.0.0.0:49666           DESKTOP-95J4G2F:0      LISTENING
TCP    0.0.0.0:49667           DESKTOP-95J4G2F:0      LISTENING
TCP    0.0.0.0:49668           DESKTOP-95J4G2F:0      LISTENING
TCP    0.0.0.0:49696           DESKTOP-95J4G2F:0      LISTENING
TCP    127.0.0.1:8307          DESKTOP-95J4G2F:0      LISTENING
TCP    127.0.0.1:58041         DESKTOP-95J4G2F:0      LISTENING
TCP    127.0.0.1:58041         care-eyes:62693        ESTABLISHED
TCP    127.0.0.1:62658         DESKTOP-95J4G2F:0      LISTENING
TCP    127.0.0.1:62658         care-eyes:62679        ESTABLISHED
TCP    127.0.0.1:62677         DESKTOP-95J4G2F:0      LISTENING
TCP    127.0.0.1:62679         care-eyes:62658        ESTABLISHED
TCP    127.0.0.1:62693         care-eyes:58041        ESTABLISHED
TCP    192.168.47.76:53787     20.197.71.89:https     TIME_WAIT
TCP    192.168.56.1:139        DESKTOP-95J4G2F:0      LISTENING
TCP    192.168.88.1:139        DESKTOP-95J4G2F:0      LISTENING
TCP    192.168.110.1:139       DESKTOP-95J4G2F:0      LISTENING
TCP    0.0.0.0:62679           DESKTOP-95J4G2F:0      BOUND
TCP    0.0.0.0:62693           DESKTOP-95J4G2F:0      BOUND
TCP    [::]:135               DESKTOP-95J4G2F:0      LISTENING
TCP    [::]:443               DESKTOP-95J4G2F:0      LISTENING
TCP    [::]:445               DESKTOP-95J4G2F:0      LISTENING
TCP    [::]:5357              DESKTOP-95J4G2F:0      LISTENING
TCP    [::]:47546             DESKTOP-95J4G2F:0      LISTENING
TCP    [::]:49664             DESKTOP-95J4G2F:0      LISTENING

```

سوال ۹: به این معنا است که در پیام HTTP خود فیلد دیگری نمیخواهیم قرار دهیم و با همین اطلاعات که وارد شده است، میخواهیم فرایند صورت گیرد.

سوال ۱۰: پیام Moved Permanently در پاسخ داده میشود که به معنای redirect است. صفحه اصلی در <https://aut.ac.ir:443> Location: قرار دارد طبق پیام داده شده.

```

λ ncat -C aut.ac.ir 80
GET / HTTP/1.1
Host: aut.ac.ir

HTTP/1.1 301 Moved Permanently
Date: Fri, 17 Jun 2022 10:10:00 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>

```

1	0.000000	192.168.30.76	192.168.202.174	DNS	73	Standard query 0xb0b4 A p13n.adobe.io
2	0.407207	192.168.30.76	239.255.255.250	SSDP	143	M-SEARCH * HTTP/1.1
3	1.445392	192.168.30.76	185.211.88.131	TCP	66	2463 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4	1.473580	185.211.88.131	192.168.30.76	TCP	62	80 → 2463 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1
5	1.473695	192.168.30.76	185.211.88.131	TCP	54	2463 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
6	1.473865	192.168.30.76	185.211.88.131	HTTP	127	GET / HTTP/1.1
7	1.510880	185.211.88.131	192.168.30.76	TCP	54	80 → 2463 [ACK] Seq=1 Ack=74 Win=29200 Len=0
8	1.510950	185.211.88.131	192.168.30.76	HTTP	471	HTTP/1.1 301 Moved Permanently (text/html)
9	1.518799	192.168.30.76	185.211.88.131	TCP	54	2463 → 80 [FIN, ACK] Seq=74 Ack=418 Win=63823 Len=0
10	1.546964	185.211.88.131	192.168.30.76	TCP	54	80 → 2463 [FIN, ACK] Seq=418 Ack=75 Win=29200 Len=0
11	1.547058	192.168.30.76	185.211.88.131	TCP	54	2463 → 80 [ACK] Seq=75 Ack=419 Win=63823 Len=0
12	3.416609	192.168.30.76	239.255.255.250	SSDP	143	M-SEARCH * HTTP/1.1

سوال ۱۱: persistent است زیرا از ورژن 1.1 برای HTTP استفاده شده است که میدانیم به صورت persistent عمل میکند.

```

λ ncat -C aut.ac.ir 80
GET / HTTP/1.1
Host: aut.ac.ir

HTTP/1.1 301 Moved Permanently
Date: Fri, 17 Jun 2022 10:10:00 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>

```

سوال ۱۲: آدرسی که bind شده است (netstat -abn حاصل اجرای) 0.0.0.0 <-

TCP	0.0.0.0:16000	0.0.0.0:0	LISTENING
[ncat.exe]			

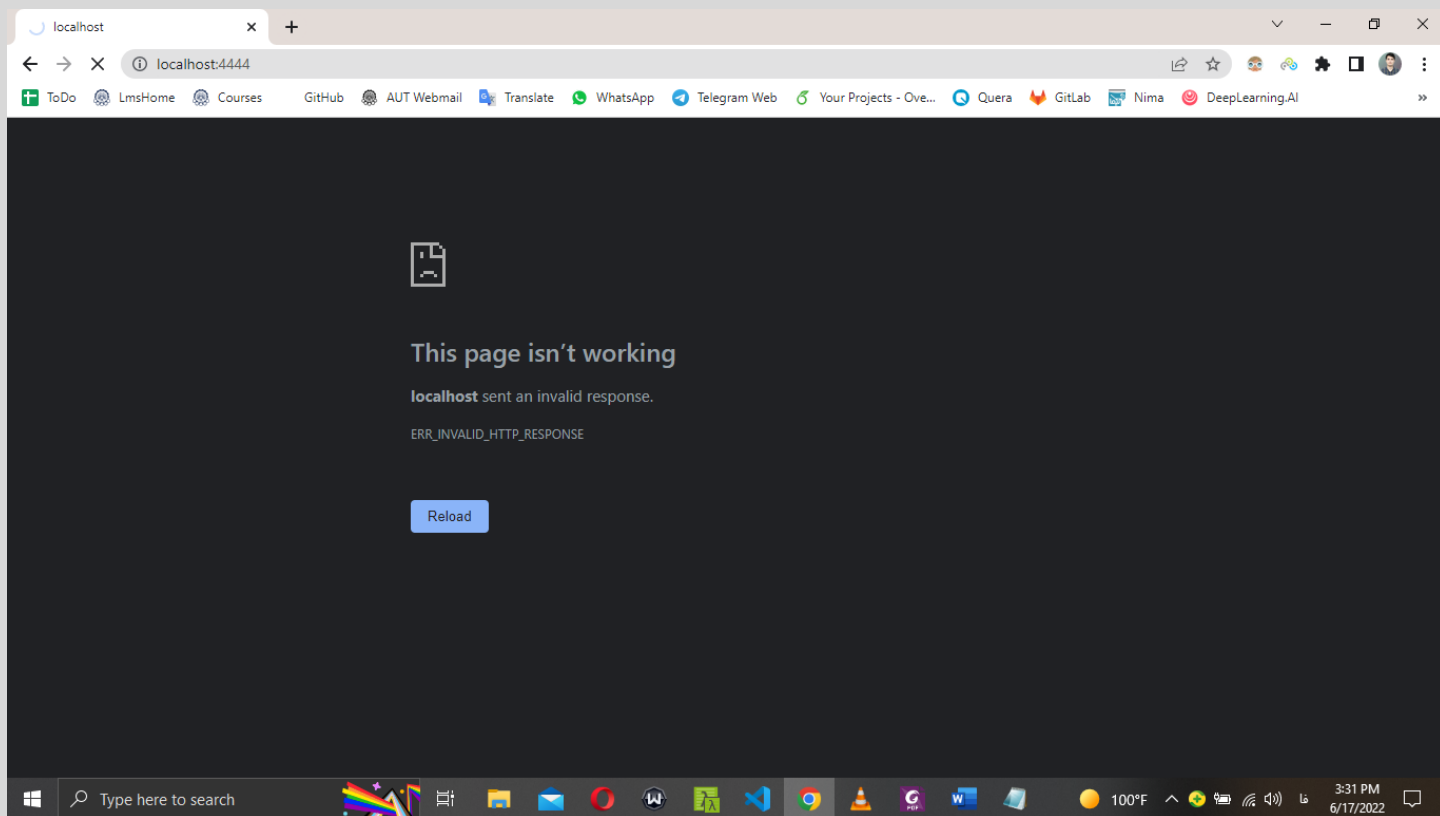
سوال ۱۳:

این خط جدا کننده header و body است و اگر نباشد، در پاسخ، پیامی که در body وجود دارد نمایش داده نمیشود و انگار body ای نداریم.

اگر خط اول وجود نداشته باشد، پیغام زیر به عنوان خطا داده خواهد شد:

Localhost sent invalid response یعنی پیامی غیر معتبر (به دلیل نبود هدر ارسال شده است) و به پیام ارسال شده HTTP ایراد میگيرد.

در واقع این هدر، پروتکل و ورژن مربوطه را بیان میکند و پیامی که ندانیم از طریق چه پروتکلی ارسال کنیم دچار خطا خواهد شد.



سوال ۱۴: لینوکس cpe:/o:linux:linux\_kernel:4 cpe:/o:linux:linux\_kernel:3.13

سوال ۱۵: از ۱۰۰۰ پورتهای که scan کرده است، پورتهای زیر باز بوده اند:

Scanning aut.ac.ir (185.211.88.131) [1000 ports]

Discovered open port 25/tcp on 185.211.88.131

Discovered open port 443/tcp on 185.211.88.131

Discovered open port 1723/tcp on 185.211.88.131

سوال ۱۶: سرویس tcp بوده است.