

کاربردهای Web ، DNS ، سوکت و پویش سرویس‌ها

سوال اول) مشخصات دقیق در عکس زیر آمده اسم. نام این فرد علیرضا باقری است.






```
domain: soft98.ir
ascii: soft98.ir
remarks: (Domain Holder) alireza bagheri
holder-c: ab590-irnic
admin-c: ab590-irnic
tech-c: ab590-irnic
bill-c: fa482-irnic
nserver: ir1.hostdl.com
nserver: ir2.hostdl.com
source: IRNIC # Filtered

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











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

سوال دوم) این آدرس‌ها ir1.hostdl.com و ir2.hostdl.com هستند که متعلق به name server ها هستند.

سوال سوم) همانطور که در عکس پایین پیداست، NS مخفف Namespace و نامی است برای شبیه سازی پروتکل‌های مختلف. برای این سایت TXT نداریم اما MX مخفف Mail eXchanger بوده و آن را مشخص می‌کند.











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 b.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).

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 چهارم) بله، آدرس آن برابر **asg.aut.ac.ir** است که آدرس IP برابر ۲۰.۸۸.۲۱۱.۱۸۵ را دارد.

Mail eXchanger (MX) Tests

Status	Test Case	Information
	MX Records	Your Mail eXchanger (MX) records are: 5 asg.aut.ac.ir. [TTL=3600]
	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: 20.88.211.185.in-addr.arpa <--> asg525.aut.ac.ir.

سوال پنجم) به ۶ سایت دیگر میرسیم از ای طریق، مطابق شکل زیر:

Reverse IP results for farsnews.ir (178.22.78.1, 178.22.78.2, 178.22.78.3, 178.22.78.4)
 =====

Domain	Last Resolved Date
farsnashr.ir	2021-05-05
farsnews.com	2020-01-24
farsnews.ir	2022-06-12
farsnews.net	2020-01-24
farsnews.org	2020-01-24
fna.ir	2022-06-08

سوال ششم) به طریقی بله، به طوری که IP Address را برعکس طی میکنیم و مشابه ترین های آنها را باز میگردانیم همانطور که در شکل سوال قبل مشخص است IP ها فقط در رقم آخر متفاوت هستند.

مشاهده شد؟):

سوال هفتم) دستور netstat -at نیاز به Run as Admin است.

Administrator: Command Prompt - netstat -at

Proto	Local Address	Foreign Address	State	Offload St
TCP	0.0.0.0:80	Keivan:0	LISTENING	InHost
TCP	0.0.0.0:135	Keivan:0	LISTENING	InHost
TCP	0.0.0.0:443	Keivan:0	LISTENING	InHost
TCP	0.0.0.0:445	Keivan:0	LISTENING	InHost
TCP	0.0.0.0:902	Keivan:0	LISTENING	InHost
TCP	0.0.0.0:912	Keivan:0	LISTENING	InHost
TCP	0.0.0.0:5040	Keivan:0	LISTENING	InHost
TCP	0.0.0.0:5357	Keivan:0	LISTENING	InHost
TCP	0.0.0.0:5432	Keivan:0	LISTENING	InHost
TCP	0.0.0.0:7680	Keivan:0	LISTENING	InHost
TCP	0.0.0.0:49664	Keivan:0	LISTENING	InHost
TCP	0.0.0.0:49665	Keivan:0	LISTENING	InHost
TCP	0.0.0.0:49666	Keivan:0	LISTENING	InHost
TCP	0.0.0.0:49667	Keivan:0	LISTENING	InHost
TCP	0.0.0.0:49668	Keivan:0	LISTENING	InHost
TCP	0.0.0.0:49675	Keivan:0	LISTENING	InHost
TCP	127.0.0.1:1001	Keivan:0	LISTENING	InHost
TCP	127.0.0.1:8307	Keivan:0	LISTENING	InHost
TCP	127.0.0.1:10042	Keivan:0	LISTENING	InHost
TCP	127.0.0.1:50911	Keivan:0	LISTENING	InHost
TCP	127.0.0.1:50912	Keivan:0	LISTENING	InHost
TCP	127.0.0.1:54863	lmlicenses:61190	ESTABLISHED	InHost
TCP	127.0.0.1:55240	Keivan:0	LISTENING	InHost
TCP	127.0.0.1:61190	Keivan:0	LISTENING	InHost
TCP	127.0.0.1:61190	lmlicenses:54863	ESTABLISHED	InHost
TCP	127.0.0.1:62522	Keivan:0	LISTENING	InHost
TCP	192.168.1.4:139	Keivan:0	LISTENING	InHost

سوال هشتم) دستور netstat -n مطابق شکل زیر:

```
C:\WINDOWS\system32>netstat -n

Active Connections

Proto Local Address          Foreign Address         State
TCP    127.0.0.1:54863         127.0.0.1:61190        ESTABLISHED
TCP    127.0.0.1:61190        127.0.0.1:54863        ESTABLISHED
TCP    192.168.1.4:56374      20.198.162.76:443      ESTABLISHED
TCP    192.168.1.4:56384      84.17.47.96:9002       ESTABLISHED
TCP    192.168.1.4:56386      84.17.47.96:9002       ESTABLISHED
TCP    192.168.1.4:56392      84.17.47.96:9002       ESTABLISHED
TCP    192.168.1.4:56397      84.17.47.96:9002       ESTABLISHED
TCP    192.168.1.4:56398      84.17.47.96:9002       ESTABLISHED
TCP    192.168.1.4:56404      84.17.47.96:9002       ESTABLISHED
TCP    192.168.1.4:56405      84.17.47.96:9002       ESTABLISHED
TCP    192.168.1.4:56406      84.17.47.96:9002       ESTABLISHED
TCP    192.168.1.4:56408      84.17.47.96:9002       ESTABLISHED
TCP    192.168.1.4:56433      84.17.47.96:9002       ESTABLISHED
TCP    192.168.1.4:56446      8.8.4.4:443            FIN_WAIT_1
TCP    192.168.1.4:56453      142.250.181.42:443     ESTABLISHED
TCP    192.168.1.4:56454      84.17.47.96:9002       ESTABLISHED
TCP    192.168.1.4:56455      142.250.181.42:443     ESTABLISHED
TCP    192.168.1.4:56456      84.17.47.96:9002       ESTABLISHED
TCP    192.168.1.4:56479      84.17.47.96:9002       ESTABLISHED
TCP    192.168.1.4:56480      84.17.47.96:9002       ESTABLISHED
TCP    192.168.1.4:56481      84.17.47.96:9002       ESTABLISHED
TCP    192.168.1.4:56485      20.205.146.149:443     TIME_WAIT
TCP    192.168.1.4:56491      84.17.47.96:9002       ESTABLISHED
TCP    192.168.1.4:56497      142.250.181.68:443     TIME_WAIT
```

سوال نهم) می توان وارد کردن Header ها ادامه دار باشند و با این کار به برنامه میفهمانیم که دستور ما تمام شده است.

سوال دهم) پیغام ۳۰۱ دریافت می کنیم که بیانگر Moved permanently است. در واقع این به دلیلی درست نبودن پورت ها است. این رفتار با نرم افزار Wireshark و مرورگر تست شد.

سوال یازدهم) خیر از این نوع نیست.

سوال دوازدهم) بر روی local و به صورت 0.0.0.0:16000 به 0.0.0.0 ساخته شده است.

سوال سیزدهم) این خط اضافه در واقع همان enter دومی است که در سوالات پیشین جواب دادیم. اگر آن را نگذاریم صفحه load نمیشود.

سوال چهاردهم) اسم سیستم عامل خواهر من Windows است.

سوال پانزدهم) پورت ۴۴۳ باز بود.

سوال شانزدهم) از پورت ۴۴۳ سرویس HTTPS ارائه می شود.

سوال هفدهم) سیستم عامل این سایت Linux 3.16 - 4.6 (94%), Linux 3.2 - 4.9 (94%), Linux 3.16 (93%), Linux 4.2 (93%), Linux 3.10 - 4.11 (۹۳٪) است.

سوال هجدهم) نتایج:

rDNS record for 185.211.88.20: asg525.aut.ac.ir

Scan report for "asg.aut.ac.ir"

Nmap scan (nmap asg.aut.ac.ir)

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-12 15:38 EDT
Nmap scan report for asg.aut.ac.ir (185.211.88.20)
Host is up (0.19s latency).
All 1000 scanned ports on asg.aut.ac.ir (185.211.88.20) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 15.28 seconds
```