

سوال ۱-

```

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 ۲-

```

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

```

سوال ۳-

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.
Mail eXchanger (MX) Tests		
Status	Test Case	Information
	MX Records	Your Mail eXchanger (MX) records are: 0 soft98.ir. [TTL=14400]
	return glue	nameserver records listed at 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		

TXT: در این بخش وجود نداشت.

A: آدرس های ip مربوط به دامنه ما و زیر دامنه های آنرا مشخص میکند

TXT: برای ذخیره اطلاعاتی مربوط به دامنه ما استفاده می شود.

MX: بیانگر آن است که ایمیل های دامنه ما کجا تحویل داده شده است.

NS: به طور معمول در زمان رجیستر تنظیم می شود و برای اختصاص دامنه یا زیر دامنه به مجموعه ای از name server ها به کار گرفته می شود.

سوال ۴-

185.211.88.20.in-addr.arpa <--> asg525.aut.ac.ir.

سوال ۵-

DELICIOUS.IR	2021-06-07
carbilla.ir	2021-06-16
cert.ir	2021-06-21
chang.ir	2021-06-20
chargoona.com	2021-06-20
charmkar.com	2021-06-07
cscs.ir	2021-06-20
diatech.ir	2021-06-20
drland.ir	2021-06-16
ehsanchameh.com	2021-06-07
electro-tech.ir	2021-06-16
esfimo.ir	2021-06-16
geicgroup.com	2021-06-20
geotechnical.ir	2021-06-16
gholamnia.com	2021-06-07
green.ir	2021-06-20
gym24.ir	2021-06-16
ham-yaar.com	2021-06-07
hamsepar.com	2021-06-07
hamedannews.com	2021-06-17

Ip آنها با cert.ir برابر و 185.215.235.5 – 192.215.234.5 مشترک است

بله – به این دلیل که ip بین چند دامنه تقسیم می‌شود به این دلیل که در هر درخواست HTTP شامل host است و می‌توان آن‌ها را از این طریق حتی با وجود ip یکسان آن‌ها را از هم تشخیص داد

سوال ۷-

netstat -ab

سوال ۸-

Netsat -aonb

سوال ۹-

در مرحله اول برای request header line و مرحله بعد برای ایجاد یک خط جدید که از هدر جدا شود و اگر بدنه پیام خالی نباشد باید برای آن هم enter استفاده شود

سوال ۱۰-

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

HTTP/1.1 301 Moved Permanently
Date: Mon, 21 Jun 2021 10:17:53 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>
```

1977	98.216116	185.211.88.131	192.168.1.12	HTTP	471	HTTP/1.1 301 Moved Permanently (text/html)
------	-----------	----------------	--------------	------	-----	--

```
> Frame 1977: 471 bytes on wire (3768 bits), 471 bytes captured (3768 bits) on interface \Device\NPF_{D8C16DA8-58DF-4309-8098-AD64EC597957}, id 0
> Ethernet II, Src: ARGTelec_e8:dd:ae (30:a2:20:e8:dd:ae), Dst: Microsof_19:da:64 (bc:83:85:19:da:64)
> Internet Protocol Version 4, Src: 185.211.88.131, Dst: 192.168.1.12
> Transmission Control Protocol, Src Port: 80, Dst Port: 1070, Seq: 1, Ack: 36, Len: 417
> Hypertext Transfer Protocol
  > HTTP/1.1 301 Moved Permanently\r\n
    Date: Mon, 21 Jun 2021 11:25:06 GMT\r\n
    Server: Apache\r\n
    Location: https://aut.ac.ir:443/\r\n
  > Content-Length: 230\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.027184000 seconds]
    [Request in frame: 1975]
    [Request URI: http://aut.ac.ir/]
    File Data: 230 bytes
  > Line-based text data: text/html (7 lines)
```

301 به دست می آید و ما را به صورت خودکار به location موجود در header منتقل می‌کند.

سوال ۱۱-

خیر موقتی است

سوال ۱۳-

در فرم پاسخ درخواست HTTP بین هدرها وضعیت پاسخ با خود body یک خط خالی وجود دارد. اکنون هنگامی که یک درخواست ارسال میکنیم برنامه ncat همه فایل های browser را ارسال میکند. Browser فایل را به عنوان یک پاسخ HTTP نگاه میکند که باید بین body و header یک خط خالی باشد. در صورت عدم وجود browser بدنه را به عنوان body می شناسد و به همین دلیل چیزی به ما نشان نخواهد داد

سوال ۱۴-

Linux 3.10 – 4.11

سوال ۱۵-

Hosts	Services	Nmap Output	Ports / Hosts	Topology	Host Details	Scans
OS ▾ Host		Port	Protocol	State	Service	Version
aut.ac.ir (185.211.88)		80	tcp	open	http	Apache
		443	tcp	open	ssl	Apache httpd (SSL-only mode)

80 و 443

سوال ۱۶-

ssl - http