گزارش آزمایش

کار با کاربرد های Web، DNS، سوکت و پویش سرویس ها

آرتا اسدی
9731006

سوال 1

نام او علیرضا باقری است و شماره تلفن او 09123549940 و ایمیل او soft98.ir@gmail.com می باشد. همین طور آدرس ثبت شده تهران، خیابان شریعتی، میرزاپورمهر 3، پلاک 20 می باشد.

سوال 2

```
ir1.hostdl.com
ir2.hostdl.com
```

```
WHOIS Information for soft98.ir
==============

% This is the IRNIC Whois server v1.6.2.
% Available on web at http://whois.nic.ir/
% Find the terms and conditions of use on http://www.nic.ir/
%
% This server uses UTF-8 as the encoding for requests and responses.

% NOTE: This output has been filtered.

% Information related to 'soft98.ir'


domain: soft98.ir
ascii: soft98.ir
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

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 3

رکورد های NS :

```
ir1.hostdl.com. [NO GLUE] [TTL=1440]
ir2.hostdl.com. [NO GLUE] [TTL=1440]
ir1.hostdl.com. [NO GLUE] [TTL=86400]
ir2.hostdl.com. [NO GLUE] [TTL=86400]
```

نام سرور ها را مشخص می کند و به زیردامنه های مختلف اشاره می کند. TTL هم همان time to live است که مدت زمانی که NS در cache باقی می ماند را نشان می دهد. فایده رکورد های NS اطمینان حاصل کردن از domain name ها است.

Status	Test Case	Information
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.

ℹ	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]

رکورد های A :

این رکورد ها به منظور اشاره کردن یک دامنه یا زیر دامنه به IP مشخص است و درواقع کارش map کردن است.

رکورد های TXT :

این رکورد ها برای اضافه کردن متن قابل درک برای انسان به host هستند.

رکورد های MX :

```
0 soft98.ir. [TTL=14400]
```

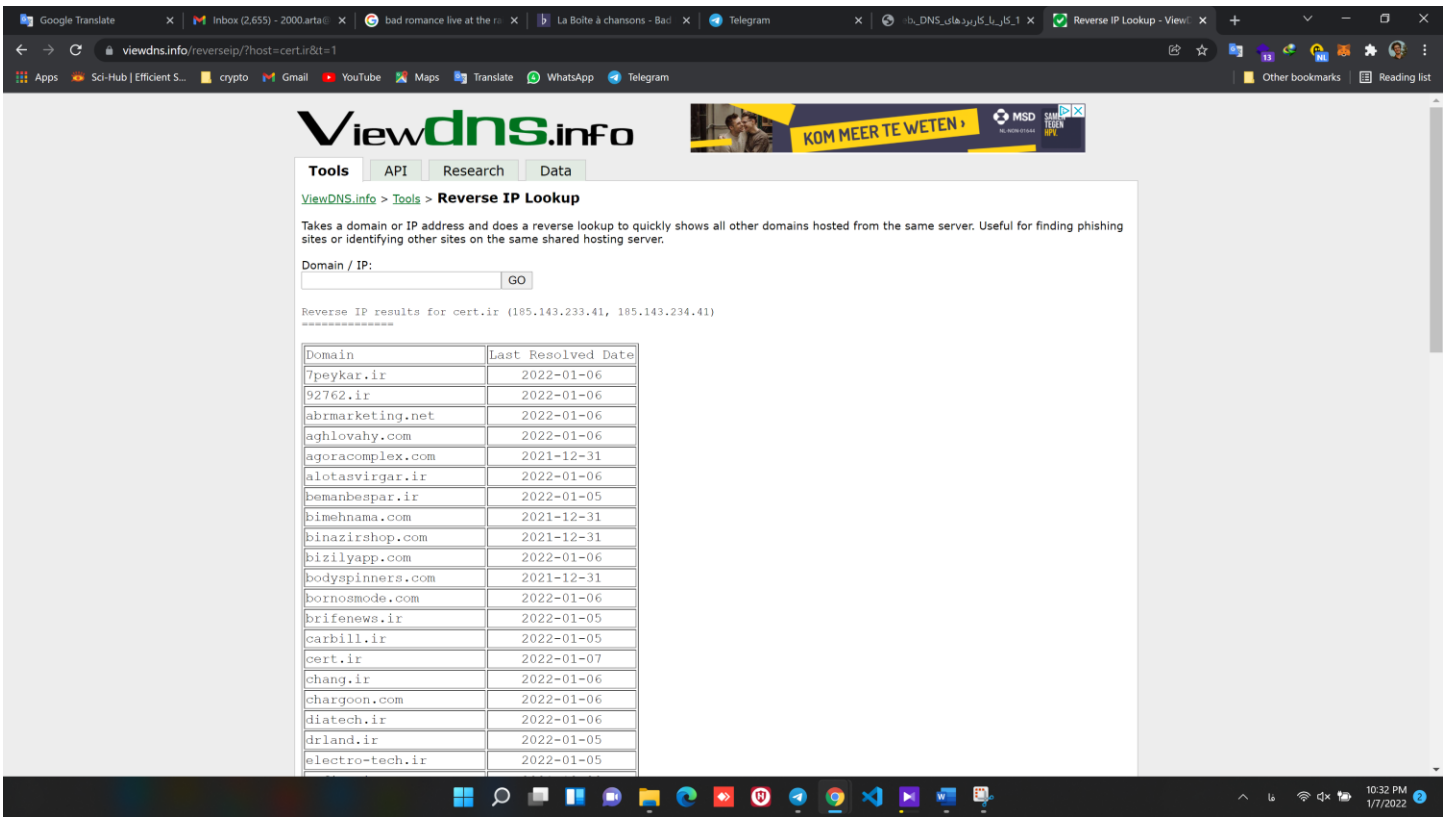
این رکورد mail server را تایین می کند که مسئولیت دریافت ایمیل ها را دارد.

سوال 4

```
asg.aut.ac.ir
20.88.211.185
```

سوال 5

آدرس ip همه آنها یکی است



Domain	Last Resolved Date
7peykar.ir	2022-01-06
92762.ir	2022-01-06
abrmarketing.net	2022-01-06
aghlovahy.com	2022-01-06
agoracomplex.com	2021-12-31
alotasvirgar.ir	2022-01-06
bemanbespar.ir	2022-01-05
bimehnama.com	2021-12-31
binazirshop.com	2021-12-31
bizilyapp.com	2022-01-06
bodyspinners.com	2021-12-31
bornosmode.com	2022-01-06
brifenews.ir	2022-01-05
carbill.ir	2022-01-05
cert.ir	2022-01-07
chang.ir	2022-01-06
chargoon.com	2022-01-06
diatech.ir	2022-01-06
drland.ir	2022-01-05
electro-tech.ir	2022-01-05

سوال 6

در header درخواست یک پارامتر به نام host وجود دارد که اگر IP ها یکسان باشند سایت مقصد را تشخیص می دهد.

سوال 7

netstat -an

سوال 8

netstat -ano

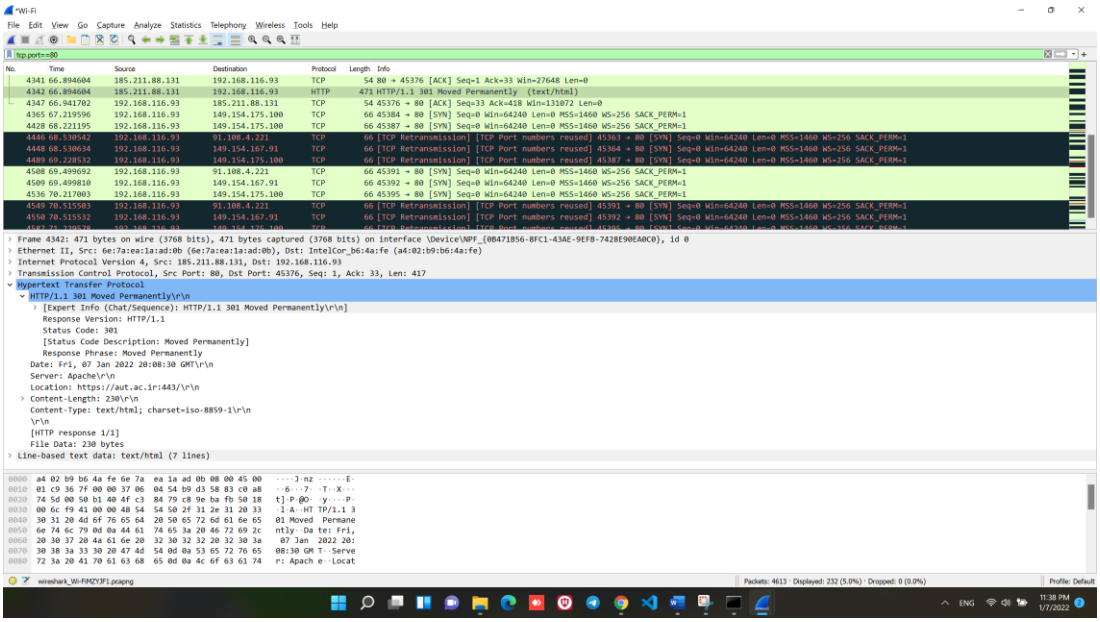
سوال 9

درخواست http دارای هدر می باشد و بعد از آن یک خط خالی وجود دارد و سپس body می آید (شاید هم نیاید) در نتیجه ابتدا یک اینتر برای خط خالی و یک اینتر بعدی برای ارسال درخواست است.

```
C:\Users\asadi>ncat -v aut.ac.ir 80
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Connected to 185.211.88.131:80.
GET / HTTP/1.1
Host: aut.ac.ir

HTTP/1.1 301 Moved Permanently
Date: Fri, 07 Jan 2022 19:37:34 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 10

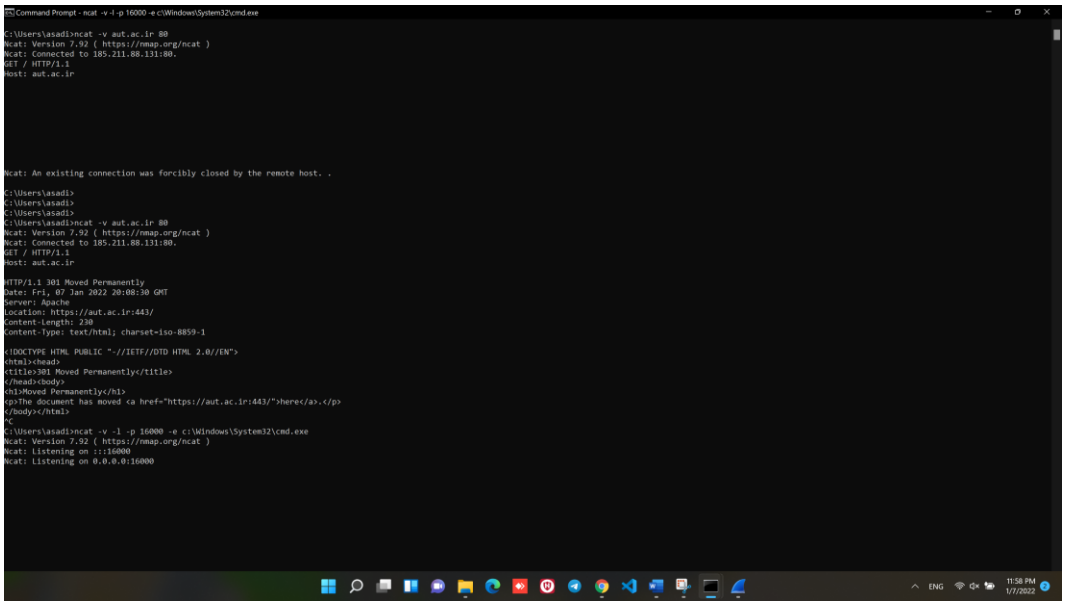
میگوید آدرس به aut.ac.ir:443 تغییر داده شده

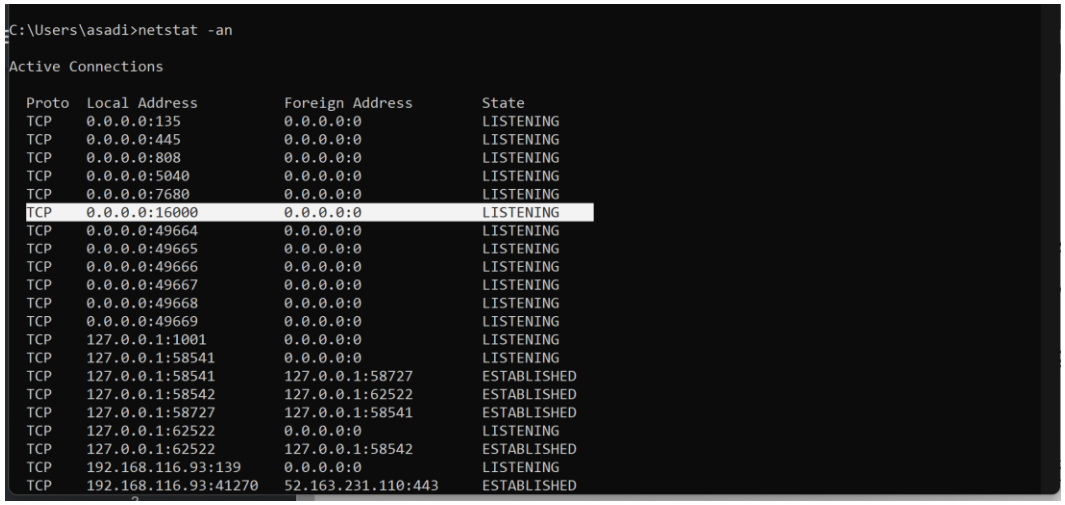


سوال 11

پروتکل HTTP 1.1 به صورت پیشفرض مقدار connection را برابر Keep-Alive قرار می دهد که به این معنا است که ارتباط persistent می باشد و با توجه به اینکه این مقدار در درخواست مشخص نشده پس ارتباط ما persistent است.

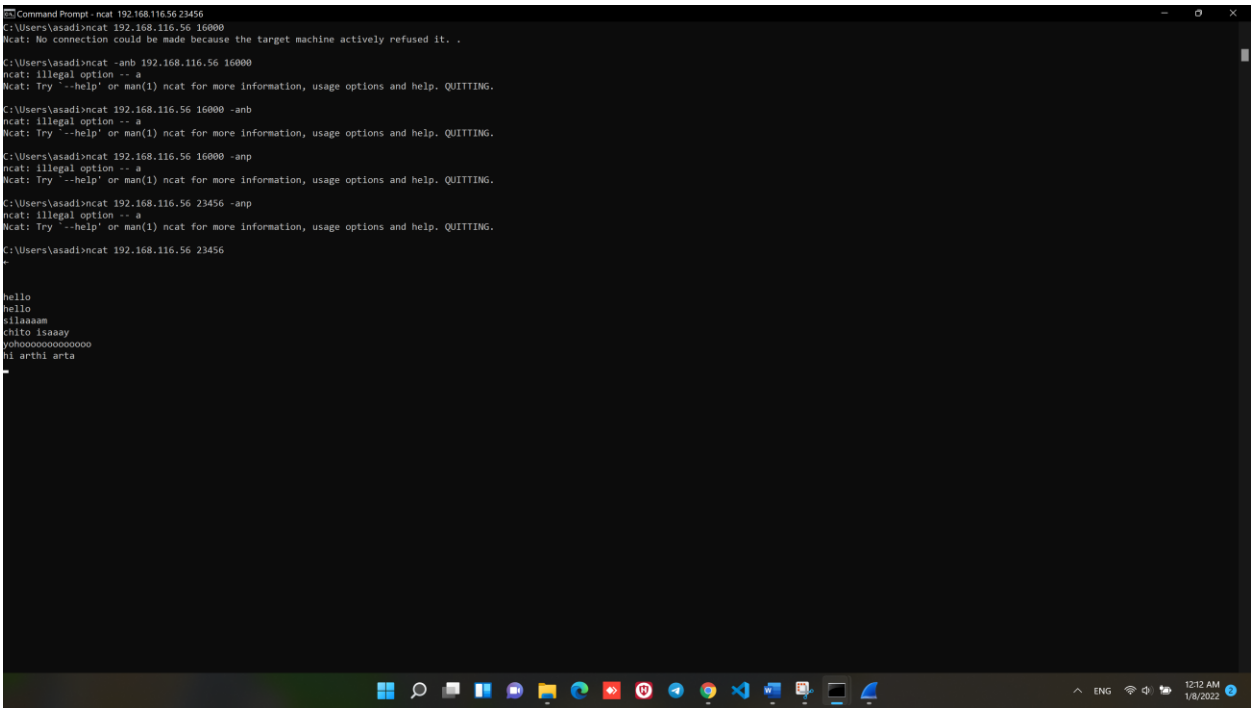
سوال 12



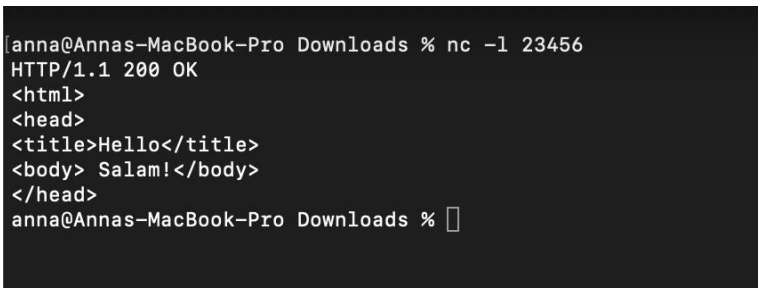


```
C:\Users\asadi>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:808            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:16000          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    0.0.0.0:49669          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1001         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:58541        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:58541        127.0.0.1:58727        ESTABLISHED
  TCP    127.0.0.1:58542        127.0.0.1:62522        ESTABLISHED
  TCP    127.0.0.1:58727        127.0.0.1:58541        ESTABLISHED
  TCP    127.0.0.1:62522        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:62522        127.0.0.1:58542        ESTABLISHED
  TCP    192.168.116.93:139     0.0.0.0:0              LISTENING
  TCP    192.168.116.93:41270   52.163.231.110:443     ESTABLISHED
```

سوال 13



درخواست به صورت یک متن ساده خوانده می شود نه درخواست HTTP و به صورت یک فایل html خوانده نمی شود و فقط متن ساده است.



سوال 14

Linux 4.4

سوال 15

25 و 443

سوال 16

پورت 25 برای stmp و 443 برای ssl