

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
	NS records listed at parent servers	<pre>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.</pre>

i	NS records at your local servers	NS records retrieved from your local nameservers were: irl.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

The screenshot shows a web browser window with several tabs open. The active tab is 'Reverse IP Lookup - ViewDNS.info'. The address bar shows 'viewdns.info/reverseip/?host=cert.ir&t=1'. The page content includes the ViewDNS.info logo and navigation tabs: Tools, API, Research, and Data. Under the 'Tools' tab, there is a section for 'Reverse IP Lookup' which explains that it takes a domain or IP address and shows other domains hosted on the same server. Below this, there is a search bar with 'Domain / IP:' and a 'GO' button. The results for 'cert.ir' (IP: 185.143.233.41, 185.143.234.41) are displayed in a table:

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
chargoan.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\sasadi>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

The image shows a Wireshark packet capture of an HTTP 301 Moved Permanently response. The packet list on the left shows a sequence of packets, with the selected packet being the HTTP response. The packet details pane on the right shows the structure of the HTTP response, including the status code 301, the location header pointing to https://aut.ac.ir:443/, and the content type text/html. The packet bytes pane at the bottom shows the raw data of the response, including the status line and the location header.

Frame 4342: 471 bytes on wire (3768 bits), 471 bytes captured (3768 bits) on interface \Device\NPF{08A71856-8FC1-43AE-9EFB-7428E90A8C0}, id 0

Ethernet II, Src: 6e:7a:ea:1a:ad:0b (6e:7a:ea:1a:ad:0b), Dst: IntelCor_b6:4a:fe (a4:82:b9:b6:4a:fe)

Internet Protocol Version 4, Src: 185.211.88.131, Dst: 192.168.136.93

Transmission Control Protocol, Src Port: 80, Dst Port: 45376, Seq: 1, Ack: 33, Len: 417

Hypertext Transfer Protocol

HTTP/1.1 301 Moved Permanently\r\n

[Expert Info (Chat/Sequence): HTTP/1.1 301 Moved Permanently\r\n]

Response Version: HTTP/1.1

Status Code: 301

[Status Code Description: Moved Permanently]

Response Phrase: Moved Permanently

Date: Fri, 07 Jan 2022 20:08:30 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]

File Data: 230 bytes

Line-based text data: text/html (7 lines)

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

```
Command Prompt: ncat -v -l -p 16000 -e c:\Windows\System32\cmd.exe
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

Ncat: An existing connection was forcibly closed by the remote host.

C:\Users\asadi>
C:\Users\asadi>
C:\Users\asadi>
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 20:08:30 GMT
Server: Apache
Location: https://aut.ac.ir:443/
Content-Length: 200
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>
<p>The document has moved <a href="https://aut.ac.ir:443/">here</a>.</p>
</body></html>
</>
C:\Users\asadi>ncat -v -l -p 16000 -e c:\Windows\System32\cmd.exe
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::16000
Ncat: Listening on 0.0.0.0:16000
```

```
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
```

```

C:\Users\asad>ncat 192.168.116.56 23456
C:\Users\asad>ncat 192.168.116.56 16000
Ncat: No connection could be made because the target machine actively refused it. .

C:\Users\asad>ncat -anb 192.168.116.56 16000
ncat: illegal option -- a
Ncat: Try '--help' or man(1) ncat for more information, usage options and help. QUITTING.

C:\Users\asad>ncat 192.168.116.56 16000 -anb
ncat: illegal option -- a
Ncat: Try '--help' or man(1) ncat for more information, usage options and help. QUITTING.

C:\Users\asad>ncat 192.168.116.56 16000 -anp
ncat: illegal option -- a
Ncat: Try '--help' or man(1) ncat for more information, usage options and help. QUITTING.

C:\Users\asad>ncat 192.168.116.56 23456 -anp
ncat: illegal option -- a
Ncat: Try '--help' or man(1) ncat for more information, usage options and help. QUITTING.

C:\Users\asad>ncat 192.168.116.56 23456
-
hello
hello
silaaaaa
chito isaaaay
yokoooooo
hi arthi arta

```

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.

```

anna@Annas-MacBook-Pro Downloads % nc -l 23456
HTTP/1.1 200 OK
<html>
<head>
<title>Hello</title>
<body> Salam!</body>
</head>
anna@Annas-MacBook-Pro Downloads % 

```