

به نام خدا

۹۷۲۳۱۰۰	محمد مهدی هجرتی
کار با کاربردهای وب Web، DNS، سوکت و پویش سرویس ها	آزمایشگاه شبکه آزمایش پنجم
۸ اردیبهشت ۱۴۰۰	استاد نقی زاده

سوال ۱

همان طور که مشاهده می شود دامنه به نام فردی با اسم علیرضا باقری و شماره موبایل مشخص شده و آدرس خیابان شریعتی ثبت شده است.

سوال ۲

آدرس name server های آن ir1.hostdl.com و ir2.hostdl.com می باشد.

```
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
```

تصاویر نتایج حاصل از بخش DNS Report را در زیر مشاهده می کنیم.









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 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).











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.
	Same glue at local and parent servers	OK. Since the GTLD for your domain (ir) differs from that of your nameservers (com), the result of this test are irrelevant since the parent servers aren't even required to hold the A records for your nameservers.
	Same NS records at each local nameserver	Good! All your local nameservers have identical NS records for your domain.
	Check that all nameservers respond	Good! All of your nameservers listed at the parent servers responded.
	Check all nameservers are valid	Good! All of your nameservers appear to be valid (e.g. are not IP addresses or partial domain names)
	Number of nameservers	Good! You have at least 2 nameservers. Whilst RFC218 section 2.5 specifies a minimum of 3, as long as you have 2 or more, you should be ok!
	Local nameservers answer authoritatively	Good! All your nameservers answer authoritatively for your domain.
	Missing NS records at parent servers	Good! The parent servers have all the nameservers listed for your domain as your local nameservers!
	Missing NS records at local servers	Good! Your local servers have all the nameservers listed for your domain that are listed at the parent servers!
	No CNAME records for domain	Good! No CNAME records are present for 'soft98.ir'. RFC1912 section 2.4 and RFC2181 section 10.3 state that there should be no CNAME records if any other records are present for a given domain.
	No CNAME records for nameservers	Good! No CNAME records are present for your nameservers. RFC1912 section 2.4 and RFC2181 section 10.3 state that there should be no CNAME records if any other records (e.g. an A record) are present for a nameserver.
	Nameservers are on different IP subnets	Good! All your nameservers are in separate class C (/24) subnets.
	Nameservers have public IP's	Good! All your NS records have public IP addresses.
	Nameservers allow TCP connections	Good! We can establish a TCP connection with each of your nameservers on port 53. Whilst UDP is most commonly used for the DNS protocol, TCP connections are occasionally used.




Start of Authority (SOA) Tests

Status	Test Case	Information
	SOA Record	Your Start of Authority (SOA) record is: Primary nameserver: ir1.hostdl.com. Hostmaster E-mail address: hostdl@gmail.com. Serial number: 2021032600 Refresh: 600 Retry: 7200 Expire: 6000 Minimum TTL: 86400
	All nameservers have same SOA serial number	Good! All your nameservers agree that your SOA serial number is 2021032600
	SOA primary nameserver listed at parent	Good! The primary nameserver listed in your SOA record (ir1.hostdl.com.) is listed at the parent servers!
	SOA serial number format	Good! Your SOA serial number (2021032600) appears to be in the recommended format (YYYYMMDDnn - where nn is the revision number).
	SOA Refresh value	Oops! Your SOA Refresh value (600) is outside of the recommended range of 1 hour (3600) to 1 day (86400). This value basically means 'how long can the secondary nameserver have out of date information after updating the primary nameserver?' and should be within the recommended range.
	SOA Retry value	Good! Your SOA Retry value (7200) is within the recommended range of 5 minutes (300) to 4 hours (14400).
	SOA Expire value	Oops! Your SOA Expire value (6000) is less than either your Refresh value (600) or your Minimum TTL value (86400). This is bad because it means that the data will IMMEDIATELY expire if one of your nameservers can't reach the primary nameserver! Set your Expire value to be greater than your Refresh and Minimum TTL values. The recommended range is 2 weeks (1209600) to 4 weeks (2419200).
	SOA Minimum TTL value	Good! Your SOA Minimum TTL value (86400) is within the recommended range of less than 3 days (259200).

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.

WWW Record Tests

Status	Test Case	Information
	WWW record	www.soft98.ir A records are: www.soft98.ir. CNAME soft98.ir. [TTL=14400] soft98.ir. A 79.127.127.35 [TTL=14400]
	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	Good! You have a CNAME entry for your WWW record which also returns the associated A record! This saves an extra lookup which would delay loading times for your site.

رکورد های NS و MX و A در تصاویر بالا نشان داده شده است.











۱. رکورد A، نام دامنه و آدرس IP متناظرش را نگهداری میکند.
۲. رکورد MX ایمیل را به یک سرور ایمیل هدایت می کند.
۳. رکورد nameserver (NS) میگوید به کدام سرور DNS برای آن دامنه باید رجوع کنیم.
۴. رکورد TXT به عنوان مکانی برای یادداشت های قابل خواندن توسط انسان یا حتی سیستم ها در نظر گرفته شده است.

سوال ۴

آدرس mail server دانشگاه `asg525.aut.ac.ir` می باشد.

آدرس IP آن `185.211.88.20` می باشد.

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 ۵

لیست برخی از سایت هایی که بر روی همین سرور قرار دارند، در تصویر زیر آمده است.
آدرس IP آن ها با IP همان cert.ir یکی است یعنی 185.143.233.5 و یا 185.143.234.5 می باشد.

Reverse IP results for cert.ir (185.143.233.5, 185.143.234.5)
=====

Domain	Last Resolved Date
141.ir	2021-04-28
1773.ir	2020-06-09
1zodpaz.ir	2021-01-27
24talk.ir	2021-04-28
3pco.ir	2021-04-28
3sheen.ir	2021-04-28
4kprojectors.ir	2019-12-11
54113.ir	2021-04-28
7030.ir	2021-04-28
7030x.ir	2021-04-28
75424.ir	2021-04-28
8513030.ir	2020-01-29
851cc.ir	2020-01-22
a-portal.ir	2021-04-28
a97.ir	2021-04-04
abfacs.ir	2021-04-28
abp-co.ir	2021-04-28
abplus.ir	2021-04-28
abzarat.ir	2021-04-28
accounts.pod.land	2019-11-25
accra.mfa.ir	2021-04-27
adnix.ir	2021-04-28
adpay.ir	2021-04-28
ads-it.ir	2021-04-28
adser.ir	2021-04-28
afarid.com	2021-04-27
afastore.ir	2021-02-23
afrangdigital.com	2021-04-27

سوال ۶

بله. به نوعی می توان گفت که multiplexing است. چون یک IP بین چندین دامنه تقسیم می شود.
چون هر درخواست HTTP شامل آدرس هاست، می توان آن ها را از این طریق حتی با وجود IP مشترک از همدیگر تشخیص داد.

سوال ۷

دستور Netstat -ab برای نمایش نام برنامه هایی که در پروتکل های tcp و udp در حال حاضر در حال استفاده می باشند، به کار برده می شود.

سوال ۸

Netstat -an تمام پورت ها را به صورت عددی لیست نشان می دهد.

سوال ۹

می دانیم در پیام های HTTP هر کدام از بخش های هدر پیام با یک اینتر از هم جدا شده اند. از طرفی قرار دادن ۲ اینتر پشت سر هم نشان دهنده ی تمام شدن پیام می باشد.

سوال ۱۰

به ما اعلام میکند که این صفحه ی سایت در محل دیگری به آدرس <https://aut.ac.ir:443> قرار دارد.

```
Command Prompt - ncat -v aut.ac.ir 80
'Host:' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\MASHADSERVICE>Host: aut.ac.ir

C:\Users\MASHADSERVICE>

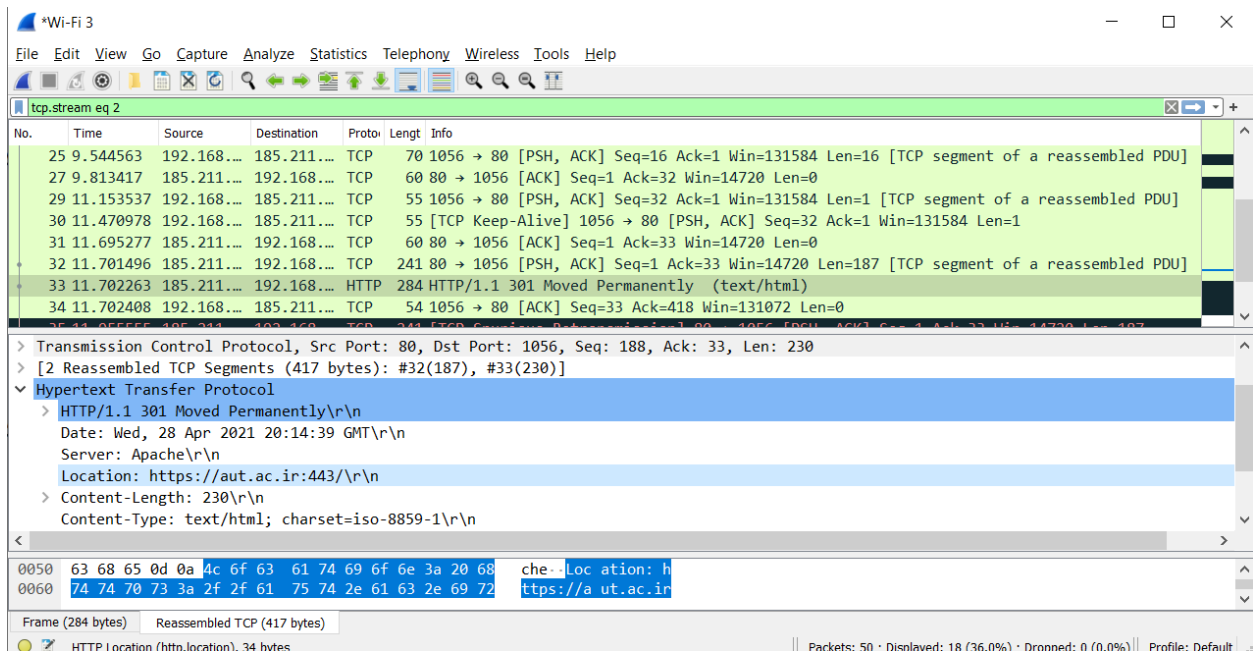
C:\Users\MASHADSERVICE>

C:\Users\MASHADSERVICE>ncat -v aut.ac.ir 80
Ncat: Version 7.91 ( 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: Wed, 28 Apr 2021 20:14:39 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>
```

همان طور که مشاهده میکنید در بخش مشخص شده ی پیام زیر، این پیغام آورده شده است.

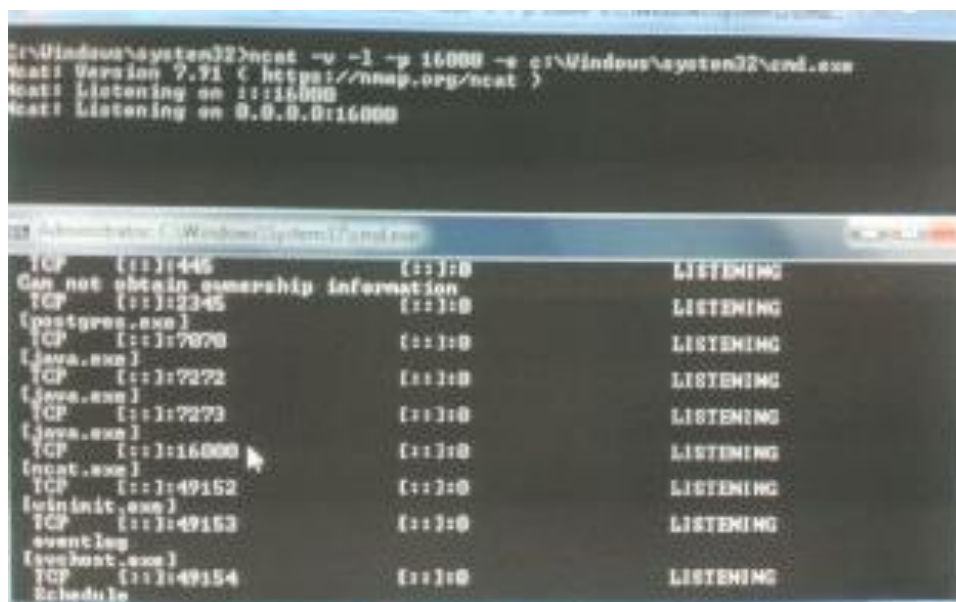


سوال ۱۱

در http ورژن ۱/۱ تمام کانکشن ها به طور پیش فرض persistent هستند. مگر اینکه هدر مربوط به Connection به صورت close باشد. پس در اینجا نیز persistent می باشد.

سوال ۱۲

روی پورت ۱۶۰۰۰ گوش می کند.



```

C:\WINDOWS\system32>ncat 192.168.1.100 16000
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd ..
cd ..

C:\Windows>cd ..
cd ..

C:\>cd ..
cd ..

C:\>ls
ls

C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is F8AC-E383

Directory of C:\

08/15/2018 12:41 PM <DIR> 94f7fdb9cf348db703328819d2
06/22/2017 12:08 PM <DIR> AMD
06/10/2017 11:18 AM <DIR> Brother
01/23/2018 05:27 PM 109,617 DOC001.exe
11/07/2007 08:00 AM 17,734 eula.1028.txt
11/07/2007 08:00 AM 17,734 eula.1031.txt
11/07/2007 08:00 AM 10,134 eula.1033.txt
11/07/2007 08:00 AM 17,734 eula.1036.txt
11/07/2007 08:00 AM 17,734 eula.1040.txt
11/07/2007 08:00 AM 118 eula.1041.txt
11/07/2007 08:00 AM 17,734 eula.1042.txt
11/07/2007 08:00 AM 17,734 eula.2052.txt
11/07/2007 08:00 AM 17,734 eula.3082.txt
11/07/2007 08:00 AM 1,110 globdata.ini
04/29/2021 01:22 PM 0 hsrv.txt
11/07/2007 08:03 AM 562,688 install.exe

```

می بینیم که بعد از اتصال از سیستم خودمان پیام موفقیت آمیز بودن در سیستم دوستان نمایش داده می شود.


```

Administrator: C:\Windows\System32\cmd.exe - ncat -v -l -p 16000 -e c:\Windows\system32\cmd.exe
ncat: Version 7.91 ( http://nmap.org/ncat )
ncat: Listening on :::16000
ncat: Listening on 0.0.0.0:16000
ncat: Connection from 192.168.1.107.
ncat: Connection from 192.168.1.107:5677.

C:\Windows\system32>ncat -v -l -p 16000 -e c:\Windows\system32\cmd.exe
ncat: Version 7.91 ( http://nmap.org/ncat )
ncat: Listening on :::16000
ncat: Listening on 0.0.0.0:16000
ncat: Connection from 192.168.1.107.
ncat: Connection from 192.168.1.107:21841.
'ls' is not recognized as an internal or external command,
operable program or batch file.

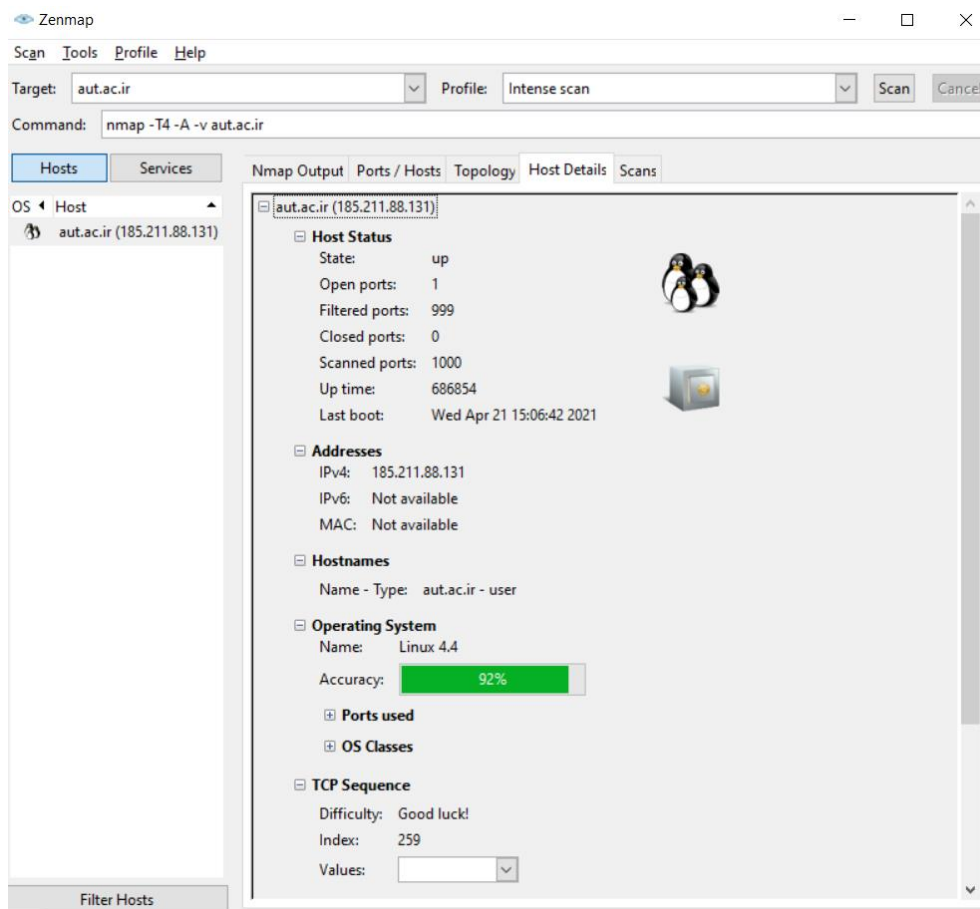
```

سوال ۱۳

در فرم پاسخ درخواست HTTP بین هدرها و Body یک خط خالی وجود دارد. در این حالت هنگامی که یک درخواست میدهیم، برنامه ی ncat کل فایل را به عنوان هدر برای مرورگر ارسال میکند. پس چون بخش body شناسایی نشده است، این قسمت نشان داده نخواهد شد.

سوال ۱۴

این وبسایت با احتمال ۹۲ درصد از سیستم عامل لینوکس ۴/۴ استفاده می کند.



سوال ۱۵

پورت ۴۴۳ باز می باشد.

سوال ۱۶

برای سرویس ssl استفاده می شود.

