فرم گزارش کار آزمایشگاه شبکه

نام و نام خانوادگی	**کیان پورآذر**	**شماره دانشجویی**	**۴۰۱۳۱۴۰۳**	**نام و شماره آزمایش**	**۵-کار با کاربردهایWeb ، DNS، سوکت و پویش سرویسها**
هدف آزمایش	با تعدادي از ابزارهاي شبکه که به وسیله آنها میتوانیم در کاربردهاي Web و DNS به عنوان سرویس گیرنده استفاده شوند، آشنا شویم				
ابزارهای مورد نیاز	کامپیوتر شخصی با سیستم عامل ویندوز ۷ یا بالاتر برنامه Nmap نسخه ۷٫۷ برنامه وایرشارک نسخه ۲٫۴				
شرح آزمایش	سوال۱: از انجایی که سیاست های ثبت دامنه در دنیا عوض شده در بسیاری از سایت ها ما نمیتوانیم به نام و اطلاعات فردی که دامنه به اسم ان ثبت شده است دسترسی داشته باشیم. سوال ۲: طبق عکس زیر name server برابر است با: ir1.hostdl.com ir2.hostdl.com				

ViewDNS.info

Tools | API | Research | Data

ViewDNS.info > Tools > **Domain / IP Whois**

Displays owner/contact information for a domain name or IP address. Can also be used to deterr

Need to lookup a large number of domains? Enquire about our bulk whois service by emailing us

Domain / IP Address:
GO

```
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: The information about this domain is hidden by the domain holder
nserver: ir1.hostdl.com
nserver: ir2.hostdl.com
source: IRNIC
```

سوال۳:

NS: با استفاده از این رکورد میتوانیم بفهمیم برای پیداکردن هر IP باید به کدام یک از nameserverها درخواست بدهیم.
A: این رکورد IP دامنه درخواستی را نشان میدهد.
TXT: این رکورد دارای اطلاعات اضافی است که توسط دامنه در DNS قرار داده میشود.
MX: این رکورد mail server را مشخص میکند.

ViewDNS.info

Tools | API | Research | Data

ViewDNS.info > Tools > **DNS Report**

View a complete report on the DNS settings for your domain. This tool is designed to assist webmasters and system administrators diagnose DNS related issues. A number of tests are run on your DNS settings with results displayed in an easy to understand manner.

Domain (*e.g. domain.com*):

GO

DNS Report for soft98.ir

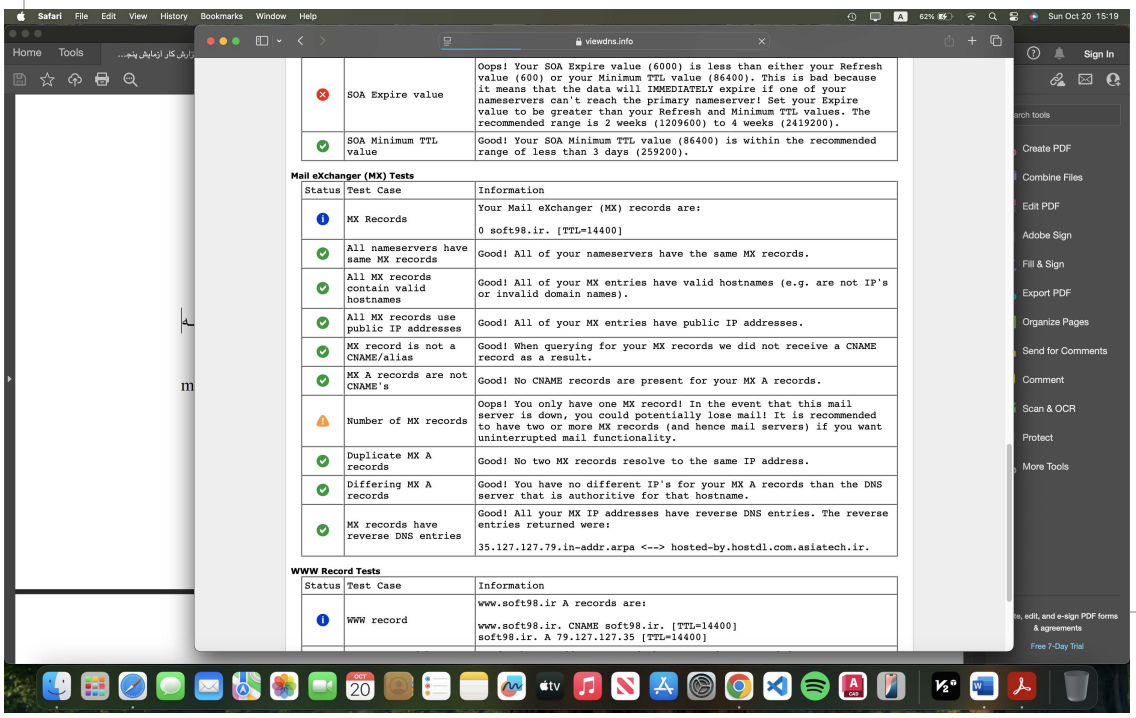
==========

Parent Nameserver Tests

Status	Test Case	Information
ℹ	NS records listed at parent servers	Nameserver records returned by the parent servers are: ir2.hostdl.com. [NO GLUE] [TTL=1402] ir1.hostdl.com. [NO GLUE] [TTL=1402] This information was kindly provided by a.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!
ℹ	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.
ℹ	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
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]
⚠	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.



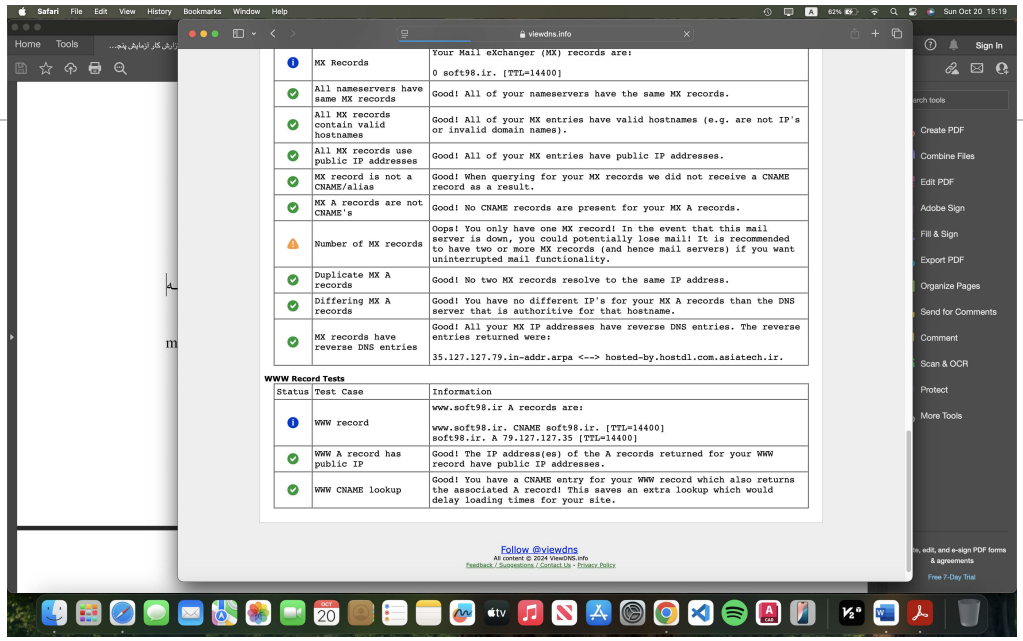
✗	SOA Expire value	Oops! Your SOA Expire value (6000) is less than either your Refresh value (600) or your Minimum TTL value (86400). This is bad because it means that the data will IMMEDIATELY expire if one of your nameservers can't reach the primary nameserver! Set your Expire value to be greater than 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
ℹ	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 authoritive 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
ℹ	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]

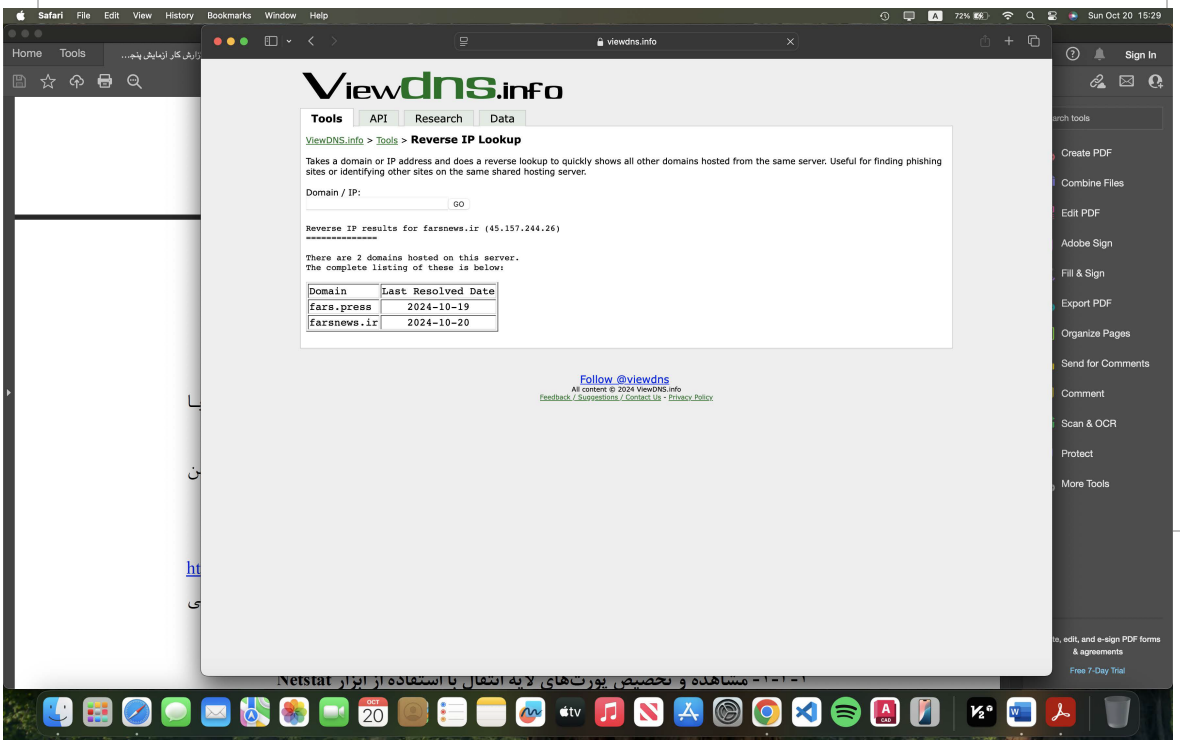


سوال۴:
طبق عکس های زیر

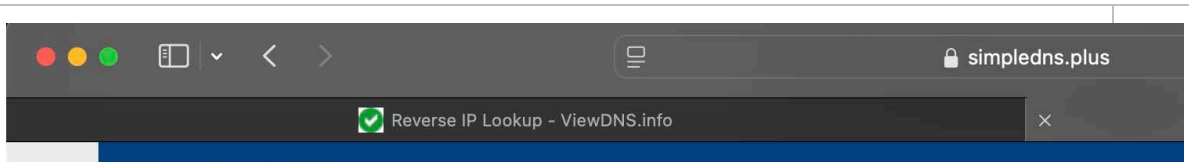
Mail eXchanger (MX) Tests

Status	Test Case	Information
ℹ	MX Records	Your Mail eXchanger (MX) records are: 5 asg.aut.ac.ir. [TTL=3600]
✗	All nameservers have same MX records	Oops! One or more of your nameservers has differing MX records. This may lead to serious issues with receiving emails and should be investigated.
✓	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 authoritive 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:



سوال ۶: نام دامنه سایت مورد نظر در هدر درخواست قرار میگیرد و این روش یک نوع multiplexing است که نام دامنه های مختلفی روی یک سرور میتوان میزبانی کرد.



Simple DNS Plus

Loading root server list (static data):
-> a.root-servers.net (198.41.0.4)
-> b.root-servers.net (192.228.79.201)
-> c.root-servers.net (192.33.4.12)
-> d.root-servers.net (128.8.10.90)
-> e.root-servers.net (192.203.230.10)
-> f.root-servers.net (192.5.5.241)
-> g.root-servers.net (192.112.36.4)
-> h.root-servers.net (128.63.2.53)
-> i.root-servers.net (192.36.148.17)
-> j.root-servers.net (192.58.128.30)
-> k.root-servers.net (193.0.14.129)
-> l.root-servers.net (199.7.83.42)
-> m.root-servers.net (202.12.27.33)

Sending request to "i.root-servers.net" (192.36.148.17)

Received referral response - DNS servers for "ir":
-> b.nic.ir (193.189.122.83)
-> a.nic.ir (193.189.123.2)
-> d.nic.ir (194.225.70.83)
-> c.nic.ir (45.93.171.206)

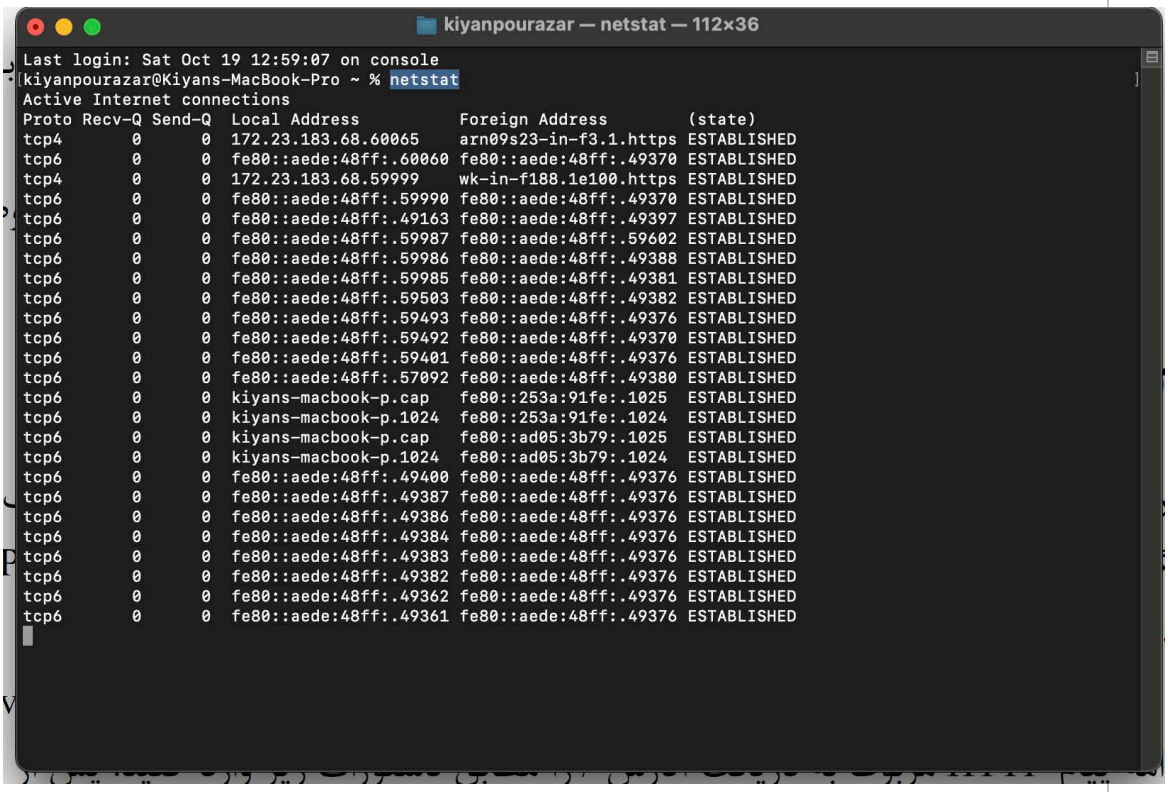
Sending request to "a.nic.ir" (193.189.123.2)

Received referral response - DNS servers for "aut.ac.ir":
-> ns3.aut.ac.ir (185.211.88.6)
-> ns2.aut.ac.ir (185.211.90.9)
-> ns1.aut.ac.ir (185.211.89.14)

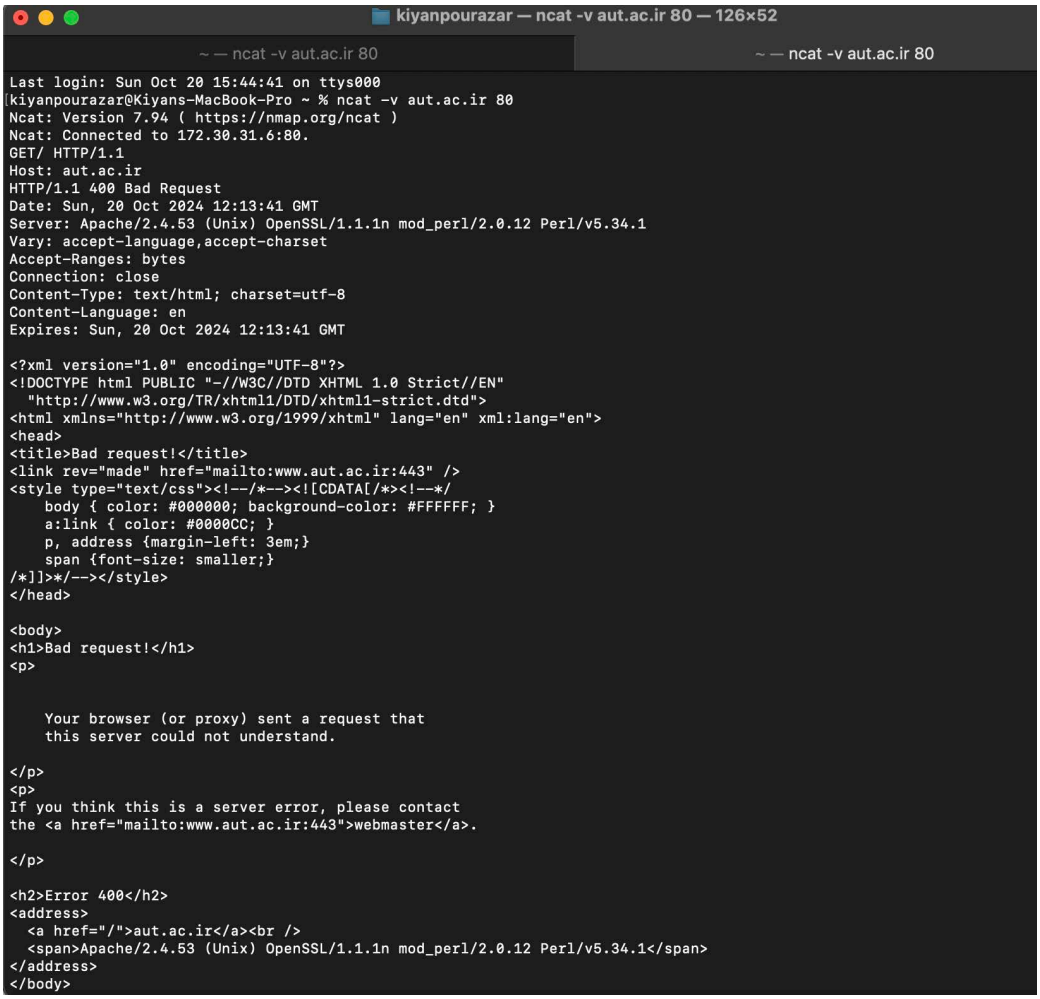
Sending request to "ns3.aut.ac.ir" (185.211.88.6)

Received authoritative (AA) response:
-> Answer: A-record for aut.ac.ir = 185.211.88.131

سوال ۷:
از دستور netstat –p TCP استفاده میکنیم.



سوال ۸:
از دستور netstat –an استفاده میکنیم.



سوال ۹:
با توجه به اینکه میان هدر و بدنه باید به اندازه یک خط خالی فاصله وجود داشته باشد دو اینتر وارد میکنیم.

سوال ۱۰: با توجه به اینکه کد ۲۰۰ امده است پس ارتباط به درستی برقرار شده است.

ادعامون را با استفاده از نرم افزار وایرشارک اثبات میکنیم.

```
Line-based text data: text/html (46 lines)
    <!doctype html>\n
    <html>\n
    <head>\n
        <title>Example Domain</title>\n
    \n
        <meta charset="utf-8" />\n
        <meta http-equiv="Content-type" content="text/html; charset=utf-8" />\n
        <meta name="viewport" content="width=device-width, initial-scale=1" />\n
        <style type="text/css">\n
        body {\n
            background-color: #f0f0f2;\n
            margin: 0;\n
            padding: 0;\n
            font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", "Helvetica Neue", Helvetica, Arial, sans-serif;\n
            \n
        }\n
        div {\n
            width: 600px;\n
            margin: 5em auto;\n
            padding: 2em;\n
            background-color: #fdfdff;\n
            border-radius: 0.5em;\n
            box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);\n
        }\n
        a:link, a:visited {\n
            color: #38488f;\n
            text-decoration: none;\n
```

39	10.271981	172.23.189.114	93.184.216.34	HTTP	55 GET / HTTP/1.1
40	10.451885	93.184.216.34	172.23.189.114	TCP	60 80 → 63405 [ACK] Seq=1 Ack=35 Win=128 Len=0
41	10.451885	93.184.216.34	172.23.189.114	TCP	1514 80 → 63405 [ACK] Seq=1 Ack=35 Win=128 Len=1460 [
42	10.451892	93.184.216.34	172.23.189.114	HTTP	206 HTTP/1.1 200 OK (text/html)

سوال ۱۱:
از انجایی که نوع connection و keep-alive را مشخص نکردیم به صورت پیش فرض ست میشود و ارتباط از نوع persiatant است.

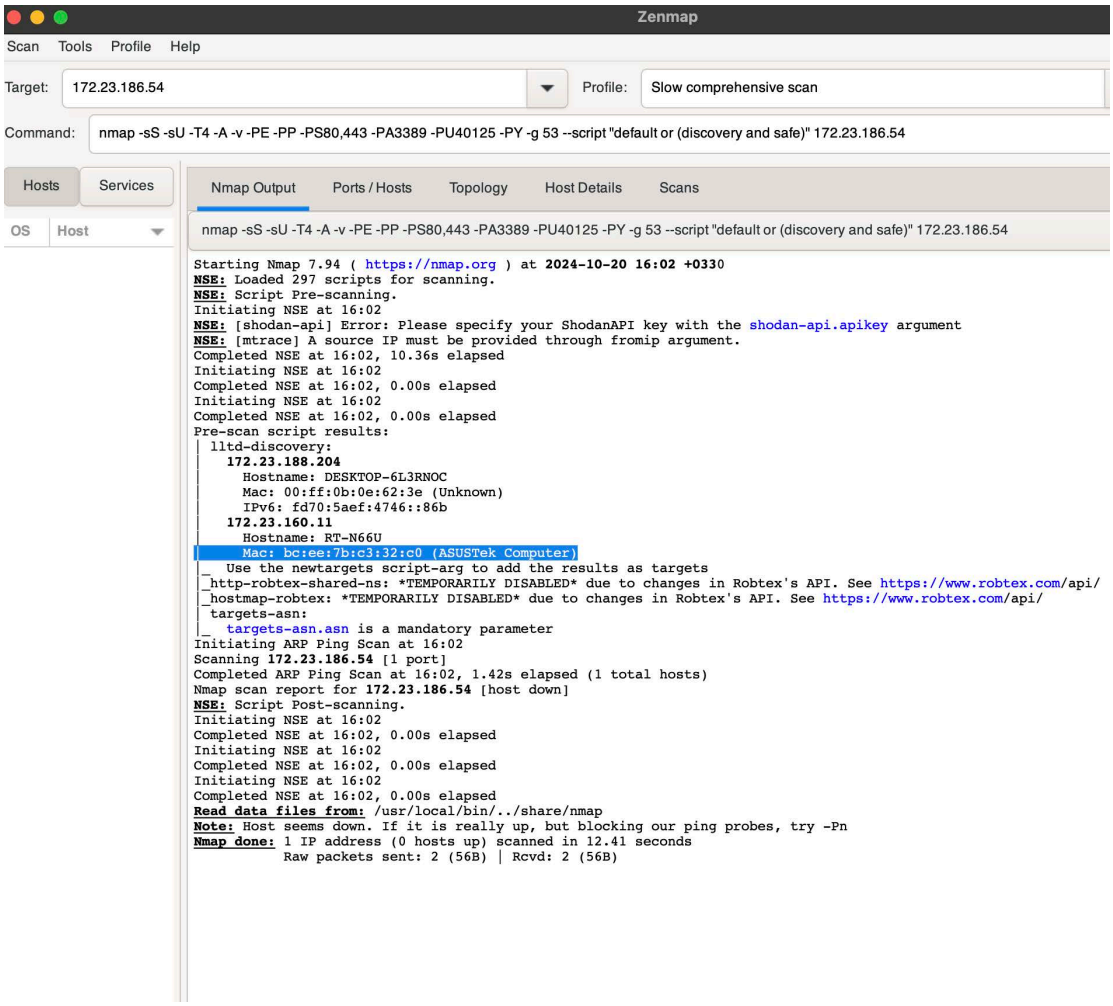
سوال ۱۲:
دستور زیر را وارد میکنیم و با دستور netstat –abn میبینیم که سوکت روی ۱۶۰۰۰ باز شده و به **0.0.0.0** بایند شده است

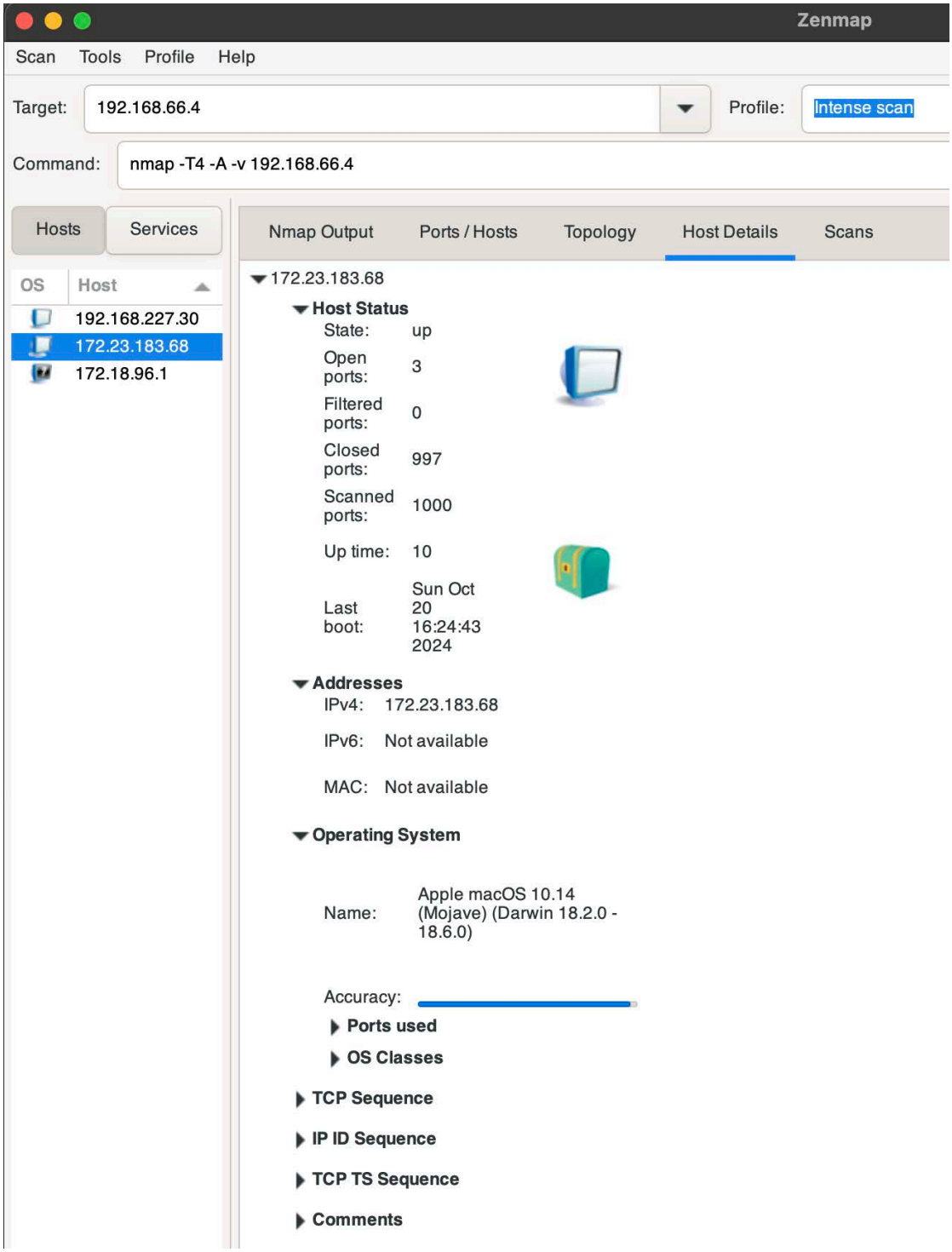
```
C:\Users\Windows >ncat -v -l -p 16000 -e c:\Windows\System32\cmd.exe
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::16000
Ncat: Listening on 0.0.0.0:16000
```

```
an not obtain ownership information
TCP    [::]:5432              [::]:0                 LISTENING
postgres.exe]
TCP    [::]:5672              [::]:0                 LISTENING
erl.exe]
TCP    [::]:16000             [::]:0                 LISTENING
ncat.exe]
TCP    [::]:33060             [::]:0                 LISTENING
mysqld.exe]
```

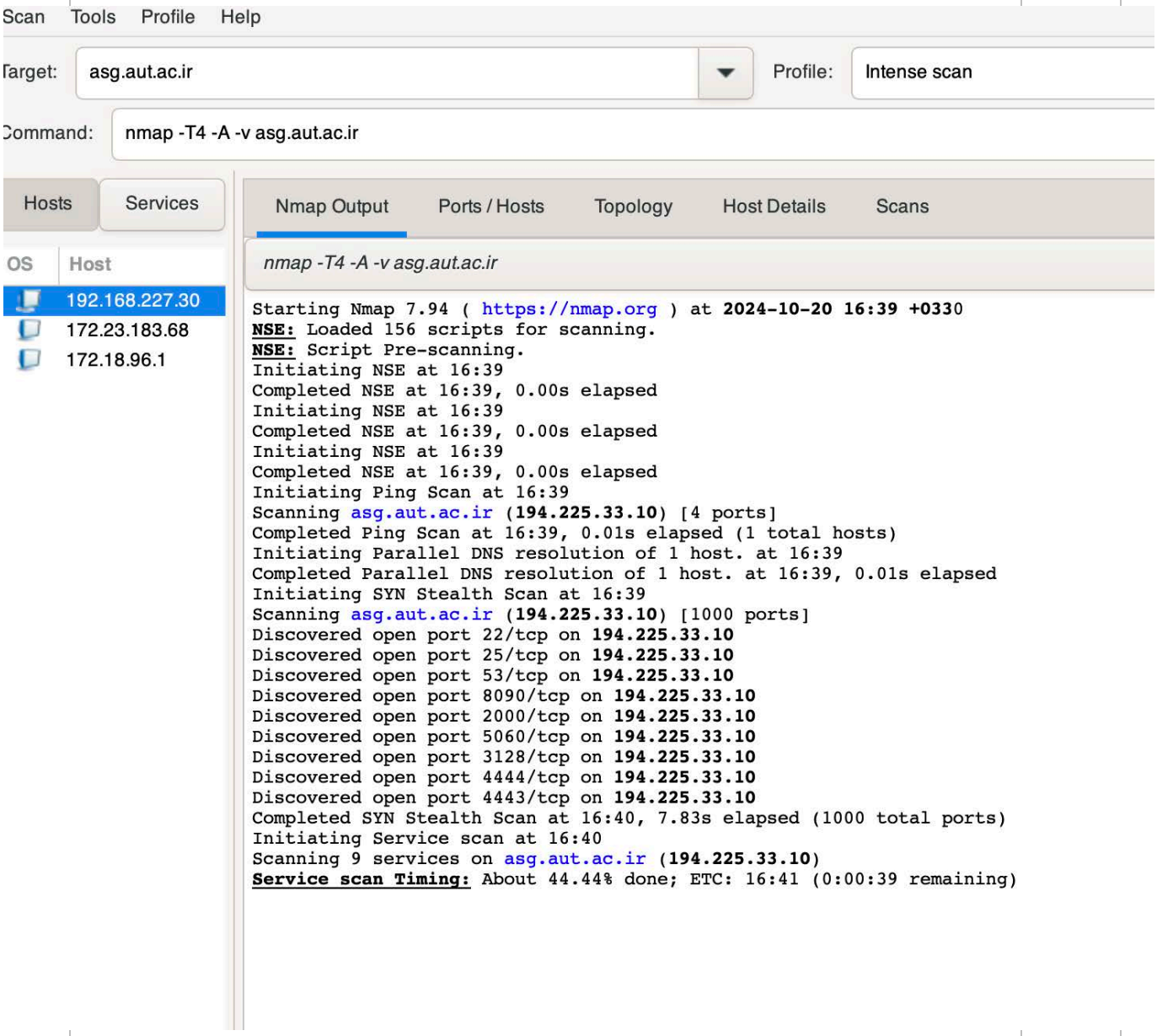
```
PS C:\Users\Windows > ncat 192.168.1.33 16000
Ncat: No connection could be made because the target machine actively refused it. .
PS C:\Users\Hossein asadi> ncat -v -l -p 16000 -e c:\Windows\System32\cmd.exe
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::16000
Ncat: Listening on 0.0.0.0:16000
```

سوال ۱۴و ۱۵ و ۱۶:




Zenmap
Scan
Tools
Profile
Help
Target:
192.168.66.4
Profile:
Intense scan
Command:
nmap -T4 -A -v 192.168.66.4
Hosts
Services
OS
Host
192.168.227.30
172.23.183.68
172.18.96.1
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
172.23.183.68
Host Status
State: up
Open ports: 3
Filtered ports: 0
Closed ports: 997
Scanned ports: 1000
Up time: 10
Last boot: Sun Oct 20 16:24:43 2024
Addresses
IPv4: 172.23.183.68
IPv6: Not available
MAC: Not available
Operating System
Name: Apple macOS 10.14 (Mojave) (Darwin 18.2.0 - 18.6.0)
Accuracy:
Ports used
OS Classes
TCP Sequence
IP ID Sequence
TCP TS Sequence
Comments

سوال ۱۷ و۱۸



نتیجه-گیری	در این آزمایش، نحوه کار با ابزارهای Nmap، netstat و ncat را اموختیم و اینکه هر کدام از این ابزارها برای چه اهدافی استفاده میشوند. برای مثال از ncat برای ساخت وب سرور، از nmap برای بررسی سیستم های انتهایی و از netstat برای بررسی پورتهای باز سیستم ها استفاده میشود.