

## فرم گزارش کار آزمایشگاه شبکه

نام و نام خانوادگی	کیان پورآذر	شماره دانشجویی	۴۰۱۳۱۴۰۳	نام و شماره آزمایش	۵-کار با کاربردهای Web ، DNS ، سوکت و پویش سرویسها
هدف آزمایش	با تعدادی از ابزارهای شبکه که به وسیله آنها میتوانیم در کاربردهای 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	سوال ۱: 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 deter

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
```

:سوال ۳

NS: با استفاده از این رکورد میتوانیم بفهمیم برای پیدا کردن هر IP باید به کدام یک از nameserver ها درخواست بدھیم.

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
!	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!
!	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.

Safari File Edit View History Bookmarks Window Help

viewdns.info Sun Oct 20 15:19

Home Tools ...چک این پایه

Mail eXchanger (MX) Tests

Status	Test Case	Information
!	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).

MX Records

Status	Test Case	Information
!	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]

Sign In

Search tools

Create PDF

Combine Files

Edit PDF

Adobe Sign

Fill & Sign

Export PDF

Organize Pages

Send for Comments

Comment

Scan & OCR

Protect

More Tools

Fill, edit, and e-sign PDF forms & agreements

Free 7-Day Trial

**MX Records**

Status	Test Case	Information
Info	MX Records	Your Mail eXchanger (MX) records are: 0 soft98.ir. [TTL=14400]
Good	All nameservers have same MX records	Good! All of your nameservers have the same MX records.
Good	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).
Good	All MX records use public IP addresses	Good! All of your MX entries have public IP addresses.
Good	MX record is not a CNAME/alias	Good! When querying for your MX records we did not receive a CNAME record as a result.
Good	MX A records are not CNAME's	Good! No CNAME records are present for your MX A records.
Warning	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.
Good	Duplicate MX A records	Good! No two MX records resolve to the same IP address.
Good	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.
Good	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.hostd1.com.asiatech.ir.

**WWW Record Tests**

Status	Test Case	Information
Info	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]
Good	www A record has public IP	Good! The IP address(es) of the A records returned for your WWW record have public IP addresses.
Good	www CNAME lookup	Good! You have a CNAME entry for your www record which also returns the associated A records. This saves an extra lookup which would delay loading times for your site.

سوال: ۴  
طبق عکس های زیر

#### Mail eXchanger (MX) Tests

Status	Test Case	Information
Info	MX Records	Your Mail eXchanger (MX) records are: 5 asg.aut.ac.ir. [TTL=3600]
Bad	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.
Good	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).
Good	All MX records use public IP addresses	Good! All of your MX entries have public IP addresses.
Good	MX record is not a CNAME/alias	Good! When querying for your MX records we did not receive a CNAME record as a result.
Good	MX A records are not CNAME's	Good! No CNAME records are present for your MX A records.
Warning	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.
Good	Duplicate MX A records	Good! No two MX records resolve to the same IP address.
Good	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.
Good	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:

The screenshot shows a Mac desktop with a Safari browser window open to the ViewDNS.info website. The URL in the address bar is `viewdns.info`. The main content of the page is a "Reverse IP Lookup" result for the IP address 45.157.244.26. It states that there are 2 domains hosted on this server and provides a table listing them:

Domain	Last Resolved Date
fars.press	2024-10-19
farsnews.ir	2024-10-20

Below the table, there are links for "Follow @viewdns", "Feedback / Suggestions / Contact Us", and "Privacy Policy". The browser's sidebar on the right lists various tools: Tools, API, Research, Data, Sign In, Create PDF, Combine Files, Edit PDF, Adobe Sign, Fill & Sign, Export PDF, Organize Pages, Send for Comments, Comment, Scan & OCR, Protect, More Tools, and a trial offer for "Fill, edit, and e-sign PDF forms & agreements". The desktop dock at the bottom contains icons for Mail, Calendar, Photos, and other Mac applications.

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.

The screenshot shows a Mac OS X application window titled "Simple DNS Plus". The title bar includes standard OS X controls (red, yellow, green buttons, zoom, minimize, maximize) and the URL "simpledns.plus". Below the title bar is a toolbar with a magnifying glass icon and the text "Reverse IP Lookup - ViewDNS.info". The main content area is a dark blue header with the text "Simple DNS Plus".

The log output is as follows:

```
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)

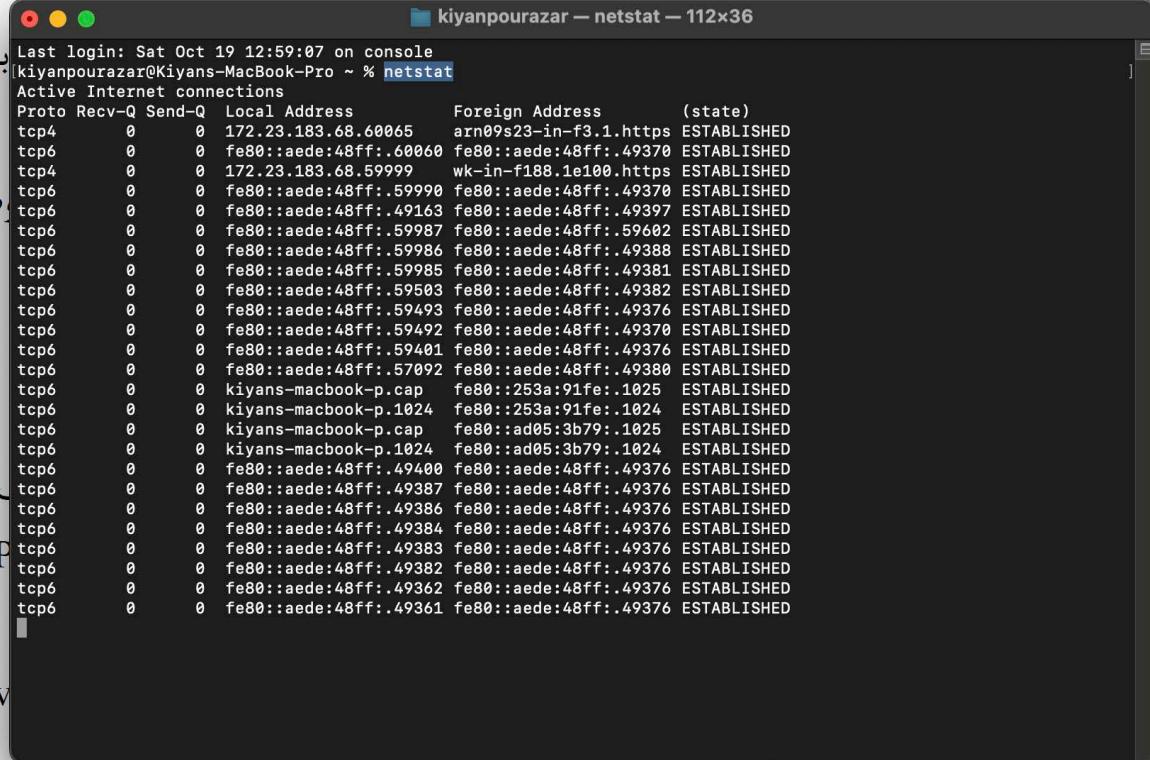
Received referral response - DNS servers for "aut.ac.ir":
-> ns3.aut.ac.ir (185.211.88.6)
-> ns2.aut.ac.ir (185.211.90.9)
-> ns1.aut.ac.ir (185.211.89.14)

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.



A terminal window titled "kiyanpourazar — netstat — 112x36" displays the output of the netstat -p TCP command. The output shows various TCP connections with their local and foreign addresses and states. The window has a dark background with white text and standard OS X window controls.

```
Last login: Sat Oct 19 12:59:07 on console
[kiyanpourazar@Kiyans-MacBook-Pro ~ % netstat
Active Internet connections
Proto Recv-Q Send-Q Local Address          Foreign Address      (state)
tcp4   0      0    172.23.183.68.60065    arn0s23-in-f3.1.https ESTABLISHED
tcp6   0      0    fe80::aede:48ff:.60060  fe80::aede:48ff:.49370 ESTABLISHED
tcp4   0      0    172.23.183.68.59999    wk-in-f188.1e100.https ESTABLISHED
tcp6   0      0    fe80::aede:48ff:.59990  fe80::aede:48ff:.49370 ESTABLISHED
tcp6   0      0    fe80::aede:48ff:.49163  fe80::aede:48ff:.49397 ESTABLISHED
tcp6   0      0    fe80::aede:48ff:.59987  fe80::aede:48ff:.59602 ESTABLISHED
tcp6   0      0    fe80::aede:48ff:.59986  fe80::aede:48ff:.49388 ESTABLISHED
tcp6   0      0    fe80::aede:48ff:.59985  fe80::aede:48ff:.49381 ESTABLISHED
tcp6   0      0    fe80::aede:48ff:.59503  fe80::aede:48ff:.49382 ESTABLISHED
tcp6   0      0    fe80::aede:48ff:.59493  fe80::aede:48ff:.49376 ESTABLISHED
tcp6   0      0    fe80::aede:48ff:.59492  fe80::aede:48ff:.49370 ESTABLISHED
tcp6   0      0    fe80::aede:48ff:.59401  fe80::aede:48ff:.49376 ESTABLISHED
tcp6   0      0    fe80::aede:48ff:.57092  fe80::aede:48ff:.49380 ESTABLISHED
tcp6   0      0    kiyans-macbook-p.cap    fe80::253a:91fe:.1025 ESTABLISHED
tcp6   0      0    kiyans-macbook-p.1024   fe80::253a:91fe:.1024 ESTABLISHED
tcp6   0      0    kiyans-macbook-p.cap    fe80::ad05:3b79:.1025 ESTABLISHED
tcp6   0      0    kiyans-macbook-p.1024   fe80::ad05:3b79:.1024 ESTABLISHED
tcp6   0      0    fe80::aede:48ff:.49400  fe80::aede:48ff:.49376 ESTABLISHED
tcp6   0      0    fe80::aede:48ff:.49387  fe80::aede:48ff:.49376 ESTABLISHED
tcp6   0      0    fe80::aede:48ff:.49386  fe80::aede:48ff:.49376 ESTABLISHED
tcp6   0      0    fe80::aede:48ff:.49384  fe80::aede:48ff:.49376 ESTABLISHED
tcp6   0      0    fe80::aede:48ff:.49383  fe80::aede:48ff:.49376 ESTABLISHED
tcp6   0      0    fe80::aede:48ff:.49382  fe80::aede:48ff:.49376 ESTABLISHED
tcp6   0      0    fe80::aede:48ff:.49362  fe80::aede:48ff:.49376 ESTABLISHED
tcp6   0      0    fe80::aede:48ff:.49361  fe80::aede:48ff:.49376 ESTABLISHED
```

سوال ۸:

از دستور netstat -an استفاده میکنیم.

```

kiyanpourazar — ncat -v aut.ac.ir 80 — 126x52
~ — ncat -v aut.ac.ir 80
Last login: Sun Oct 20 15:44:41 on ttys000
[kiyanpourazar@Kiyans-MacBook-Pro ~ % ncat -v aut.ac.ir 80
Ncat: Version 7.94 ( https://nmap.org/ncat )
Ncat: Connected to 172.30.31.6:80.
GET/ HTTP/1.1
Host: aut.ac.ir
HTTP/1.1 400 Bad Request
Date: Sun, 20 Oct 2024 12:13:41 GMT
Server: Apache/2.4.53 (Unix) OpenSSL/1.1.1n mod_perl/2.0.12 Perl/v5.34.1
Vary: accept-language,accept-charset
Accept-Ranges: bytes
Connection: close
Content-Type: text/html; charset=utf-8
Content-Language: en
Expires: Sun, 20 Oct 2024 12:13:41 GMT

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en">
<head>
<title>Bad request!</title>
<link rev="made" href="mailto:www.aut.ac.ir:443" />
<style type="text/css"><!--/*--><![CDATA[/*<!---->
  body { color: #000000; background-color: #FFFFFF; }
  a:link { color: #0000CC; }
  p, address {margin-left: 3em;}
  span {font-size: smaller;}>
/*]]><!----></style>
</head>

<body>
<h1>Bad request!</h1>
<p>

  Your browser (or proxy) sent a request that
  this server could not understand.

</p>
<p>
If you think this is a server error, please contact
the <a href="mailto:www.aut.ac.ir:443">webmaster</a>.

</p>

<h2>Error 400</h2>
<address>
  <a href="/">aut.ac.ir</a><br />
  <span>Apache/2.4.53 (Unix) OpenSSL/1.1.1n mod_perl/2.0.12 Perl/v5.34.1</span>
</address>
</body>

```

سوال ۹:

باتوجه به اینکه میان هدر و بدن باید به اندازه یک خط خالی فاصله وجود داشته باشد دو اینتر وارد میکنیم.

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

ادعامون را با استفاده از نرم افزار وایرشارک اثبات میکنیم.

```
<!doctype html>
<html>
<head>
    <title>Example Domain</title>
</head>
<body>
    background-color: #f0f0f2;
    margin: 0;
    padding: 0;
    font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", Helvetica, Arial, sans-serif;
</body>
</html>
div {
    width: 600px;
    margin: 5em auto;
    padding: 2em;
    background-color: #fdfdff;
    border-radius: 0.5em;
    box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);
}
a:link, a:visited {
    color: #38488f;
    text-decoration: none;
}
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 keep-alive و connection 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 ۰.۰.۰.۰ 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]
TCP      [::]:40664          [::]:0          LISTENING
```

```

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 ۱۴ و ۱۵ و ۱۶:

Zenmap

Scan Tools Profile Help

Target: 172.23.186.54 Profile: Slow comprehensive scan

Command: nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" 172.23.186.54

Hosts Services OS Host

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" 172.23.186.54

```

Starting Nmap 7.94 ( https://nmap.org ) at 2024-10-20 16:02 +0330
NSE: Loaded 297 scripts for scanning.
NSE: Script Pre-scanning.
NSE: [shodan-api] Error: Please specify your ShodanAPI key with the shodan-api.apikey argument
NSE: [mtrace] A source IP must be provided through fromip argument.
Completed NSE at 16:02, 10.36s elapsed
Initiating NSE at 16:02
Completed NSE at 16:02, 0.00s elapsed
Initiating NSE at 16:02
Completed NSE at 16:02, 0.00s elapsed
Pre-scan script results:
  lnd-discovery:
    172.23.188.204
      Hostname: DESKTOP-6L3RNOC
      Mac: 00:ff:0b:0e:62:3e (Unknown)
      IPv6: fd70:5ae1:4746::86b
    172.23.160.11
      Hostname: RT-N66U
      Mac: bc:ee:17:b:c3:32:c0 (ASUSTek Computer)
    Use the newtargets script-arg to add the results as targets
    http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
    hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
    targets-asn:
      _targets-asn.asn is a mandatory parameter
Initiating ARP Ping Scan at 16:02
Scanning 172.23.186.54 [1 port]
Completed ARP Ping Scan at 16:02, 1.42s elapsed (1 total hosts)
Nmap scan report for 172.23.186.54 [host down]
NSE: Script Post-scanning.
Initiating NSE at 16:02
Completed NSE at 16:02, 0.00s elapsed
Initiating NSE at 16:02
Completed NSE at 16:02, 0.00s elapsed
Initiating NSE at 16:02
Completed NSE at 16:02, 0.00s elapsed
Read data files from: /usr/local/bin/../share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 12.41 seconds
Raw packets sent: 2 (56B) | Rcvd: 2 (56B)

```

Zenmap

Scan Tools Profile Help

Target: 192.168.66.4 Profile: Intense scan

Command: nmap -T4 -A -v 192.168.66.4

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

192.168.227.30  
172.23.183.68  
172.18.96.1

▼ 172.23.183.68

▼ Host Status

State:	up
Open ports:	3
Filtered ports:	0
Closed ports:	997
Scanned ports:	1000

Up time: 10 Sun Oct 20 16:24:43 2024

Last boot: 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

Scan Tools Profile Help

Target: asg.aut.ac.ir

Profile: Intense scan

Command: nmap -T4 -A -v asg.aut.ac.ir

Hosts	Services
OS	Host
192.168.227.30	
172.23.183.68	
172.18.96.1	

Nmap Output      Ports / Hosts      Topology      Host Details      Scans

```
nmap -T4 -A -v asg.aut.ac.ir

Starting Nmap 7.94 ( https://nmap.org ) at 2024-10-20 16:39 +0330
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:39
Completed NSE at 16:39, 0.00s elapsed
Initiating NSE at 16:39
Completed NSE at 16:39, 0.00s elapsed
Initiating NSE at 16:39
Completed NSE at 16:39, 0.00s elapsed
Initiating Ping Scan at 16:39
Scanning asg.aut.ac.ir (194.225.33.10) [4 ports]
Completed Ping Scan at 16:39, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:39
Completed Parallel DNS resolution of 1 host. at 16:39, 0.01s elapsed
Initiating SYN Stealth Scan at 16:39
Scanning asg.aut.ac.ir (194.225.33.10) [1000 ports]
Discovered open port 22/tcp on 194.225.33.10
Discovered open port 25/tcp on 194.225.33.10
Discovered open port 53/tcp on 194.225.33.10
Discovered open port 8090/tcp on 194.225.33.10
Discovered open port 2000/tcp on 194.225.33.10
Discovered open port 5060/tcp on 194.225.33.10
Discovered open port 3128/tcp on 194.225.33.10
Discovered open port 4444/tcp on 194.225.33.10
Discovered open port 4443/tcp on 194.225.33.10
Completed SYN Stealth Scan at 16:40, 7.83s elapsed (1000 total ports)
Initiating Service scan at 16:40
Scanning 9 services on asg.aut.ac.ir (194.225.33.10)
Service scan Timing: About 44.44% done; ETC: 16:41 (0:00:39 remaining)
```

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 سیستم‌های انتهایی و از netstat برای بررسی پورت‌های باز سیستم‌ها استفاده می‌شود.

نتیجه-  
گیری