

«باسم‌هه تعالی»



## گزارش کار آزمایش پنجم

کار با کاربردهای Web ، سوکت و پویش سرویس‌ها



طراحی و تدوین:

9731701 / مهدی رحمانی

## هدف آزمایش

در این آزمایش قصد داریم با تعدادی از ابزارهای شبکه که به وسیله‌ی آن‌ها می‌توانیم در کاربردهای Web و DNS به عنوان سرویس گیرنده استفاده شوند، آشنا شویم.

قطعات و ابزارهای مورد نیاز

ابزارهای موردنیاز برای این آزمایش عبارتند از:

کامپیوتر شخصی با سیستم عامل ویندوز 7 یا بالاتر برای هرگروه

برنامه Nmap نسخه 7.7 به بالا

برنامه Wireshark نسخه 2.4 به بالا

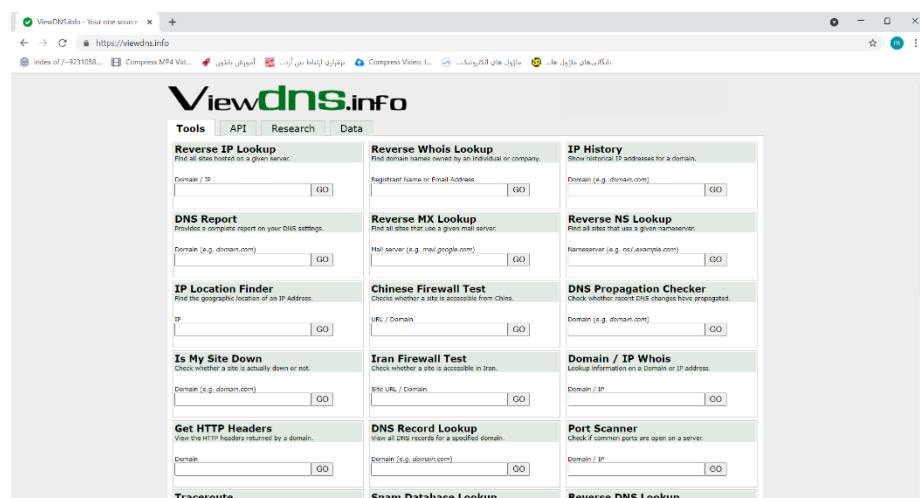
خب از آزمایش‌های قبل برنامه‌ی Wireshark را نصب داریم. حال به سایت مراجعه می‌کنیم و برنامه Nmap را دانلود و نصب می‌کنیم. <https://nmap.org/download.html>

## DNS کارکرد

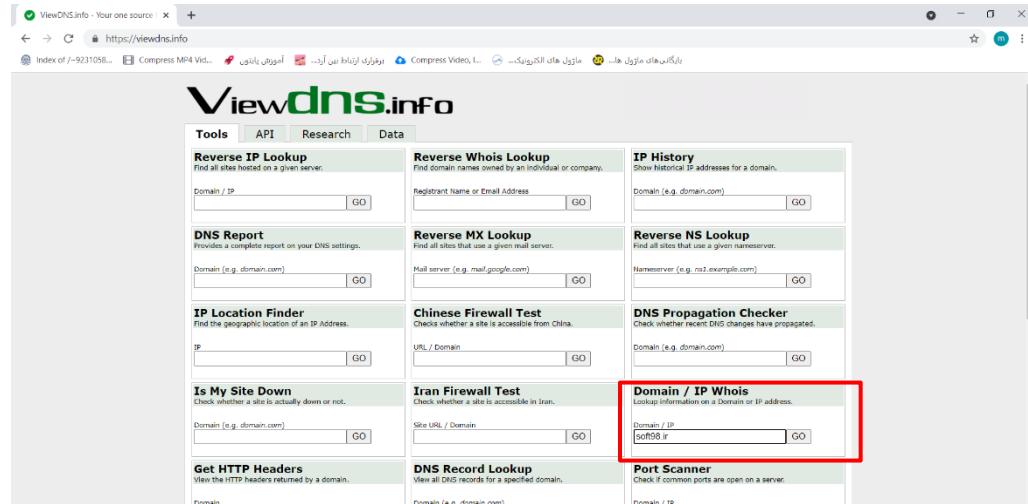
در ابتدا با ابزارهای برشط کارکرد DNS آشنا می‌شویم. یکی از این ابزارها وب سایت ViewDNS است. در گام اول با آدرس زیر وارد این وب سایت شوید:

<http://viewdns.info/>

صفحه‌ی اول سایت به صورت زیر می‌باشد:



## مرحله اول) در قسمت Domain/IP Whois رفته و آدرس soft98.ir را وارد نمایید.



### سوال 1: نام و اطلاعات فردی که دامنه به اسم او ثبت شده است چیست؟

بعد از اینکه دکمه GO را بزنیم آنگاه در این قسمت میتوانیم نام و اطلاعات فردی که دامنه به اسم او ثبت شده است را ببینیم:

```
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: 2019-03-25
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
```

نام: جلوی عبارت person اسم فردی که دامنه به نام او ثبت شده است آمده است، که علیرضا باقری میباشد.

ایمیل: همچنین ایمیلی که دامنه با آن رجیستر شده است soft98.ir@gmail.com میباشد.

آدرس فرد: ایران- استان تهران- شهر تهران- شریعتی- خیابان میرزاپور- کوچه مهر 3 غربی- پلاک 20

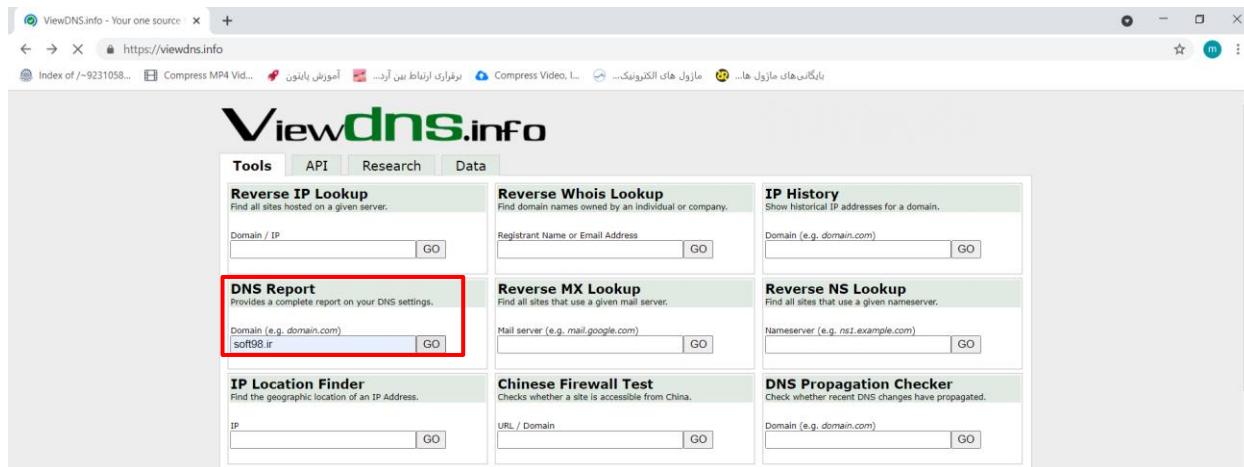
شماره تماس: 0912 3549940

## سؤال 2: آدرس name server آن چیست؟

با توجه به همان قسمت میتوان این را هم پیدا کرد. دو آدرس ir2.hostdl.com و ir1.hostdl.com دو آدرس های آن میباشند.

```
nserver: ir1.hostdl.com  
nserver: ir2.hostdl.com
```

**مرحله دوم) در وب سایت به قسمت DNS Report رفته و آدرس soft98.ir را وارد نمایید.**



### سوال 3: رکوردهای NS، A، MX و TXT را مشخص کنید. هریک از این رکوردها چه چیزی را مشخص می‌کنند؟

بعد از اینکه دکمه‌ی GO را بزنیم به اطلاعات موردنظر میتوانیم دست پیدا کنیم.

رکوردهای NS:

NS مخفف کلمه "Name Server" است و NS record نشان می‌دهد کدام سرور DNS برای آن دامنه معترض است و به عبارتی کدام سرور شامل authoritative actual DNS record می‌باشد. در واقع، NS record به اینترنت می‌گوید که کجا باید بروود تا آدرس IP دامنه را پیدا کند.

برای این سایت رکوردهای NS شامل name server های زیر می‌باشد:

ir1.hostdl.com

ir2.hostdl.com

همچنین این اطلاعات را میتوانید در تصویر زیر ببینید:

	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.

## رکوردهای A :

"A" مخفف "Address" است و این اساسی ترین نوع DNS record میباشد. نشان دهنده آدرس IP یک دامنه میباشد و درواقع A record شما به سرورهای DNS اجازه می دهد تا آدرس IP متناسب با نام دامنه شما را داشته باشند.

( رکوردهای A برای اشاره‌ی مستقیم به آدرس IP میباشد و همچنین AAAA هم برای اشاره به آدرس IP ورژن 6 به کار میرود)

برای این سایت رکوردهای A شامل IP Address زیر میباشد:

79.127.127.35

همچنین اطلاعات مربوط به این رکورد را میتوانید در زیر ببینید:

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.

## رکوردهای TXT :

این رکورد اجازه می دهد تا متن دلخواه خود را به رکورد DNS اضافه کنید. معمولاً این رکورد به سایر سرویس ها درباره عمل کرد دامنه اطلاعاتی را می دهد و اجازه میدهد که یک متن دلخواه را به یک دامنه متناظر کنیم.

بنابراین TXT records برای ارائه‌ی یک متن دلخواه برای اطلاعات بیشتر است که میتواند شامل متن قابل خواندن برای انسان و یا ماشین باشد و میتواند شامل اطلاعات دلخواهی مانند اطلاعات شبکه یا data center و ... باشد.

سایت soft98.ir TXT رکورد ندارد.

## رکوردهای MX :

رکوردهای MX برای شناخت mail server میباشد. (مثلا وقتی ایمیلی به آدرس [info@soft98.ir](mailto:info@soft98.ir) زده شد، به کدام IP باید تحویل داده شود).

برای توضیحات بیشتر: این رکورد اجراه می دهد تا mail server ها نامهای مستعار ساده داشته باشند. به عبارتی میتوان گفت که این رکورد ایمیل ها را به یک mail server مخصوص هدایت میکند. توجه کنید که با این رکورد به شرکتها اجازه میدهد از یک نام مستعار واحد همزمان برای mail server و برای یکی از سرورهای دیگرش mail server canonical name استفاده کنید. اگر یک DNS client بخواهد Web Server یک canonical name را مانند MX استفاده کند. بداند باید برای رکورد MX آن دامنه درخواست دهد؛ برای یافتن hostname را مانند CNAME سرورهای دیگر باید برای رکورد CNAME درخواست دهد. این رکورد ها یک و یک کد اولویت نگه میدارند.

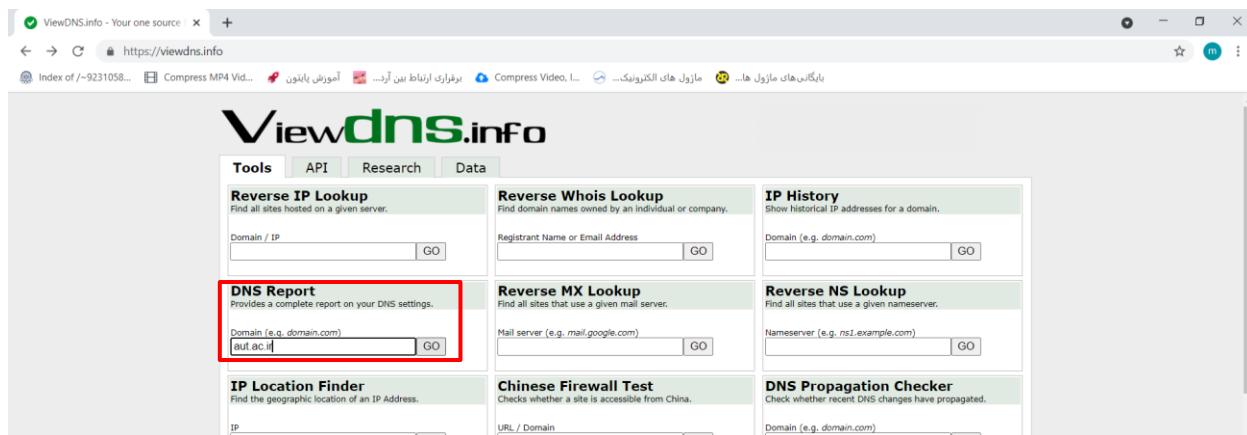
برای این سایت در رکورد MX یک وجود دارد و آن هم soft98.ir میباشد. کد اولویت آن نیز 0 میباشد.

همچنین اطلاعات مربوط به این رکورد را میتوانید در زیر ببینید:

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.hostd1.com.asiatech.ir.

## سوال 4 : در قسمت DNS Report با وارد کردن دامنهی دانشگاه ( aut.ac.ir ) دانشگاه را مشخص کنید. آیا آدرس IP آن را میتوانید مشخص کنید؟

خب حال به قسمت DNS Report میرویم و این نام دامنه را وارد میکنیم:



The screenshot shows the Viewdns.info homepage with various tools like Reverse IP Lookup, Reverse Whois Lookup, and IP History. The 'DNS Report' section is highlighted with a red box. In this section, the domain 'aut.ac.ir' is entered into the 'Domain (e.g. domain.com)' input field.

سپس GO را میزنیم. برای یافتن mail server را چک کنیم. پس به جدول مربوط Mail eXchanger (MX) Tests به میرویم:

Test	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.

طبق تصویر فوق دامنهی mail server دانشگاه asg.aut.ac.ir میباشد.

آدرس IP مربوط به این دامنه برابر با 185.211.88.20 میباشد.

این آدرس IP را میتوانیم هم با ping کردن در CMD به دست بیاوریم. هم اینکه در قسمت ping در این سایت دامنه asg.aut.ac.ir را وارد کنیم و IP Address را بیابیم:

The screenshot shows the ViewDNS.info homepage with various tools like Firewall Test, Whois, and Port Scanner. The 'Ping' tool is highlighted with a red box. In the 'Domain / IP' input field, the value 'asg.aut.ac.ir' is entered. A 'GO' button is located to the right of the input field.

و سپس طبق عکس زیر در ستون IP Address مقدار آن را یافت که برابر 185.211.88.20 میباشد:

[ViewDNS.info > Tools > Ping Tool](#)

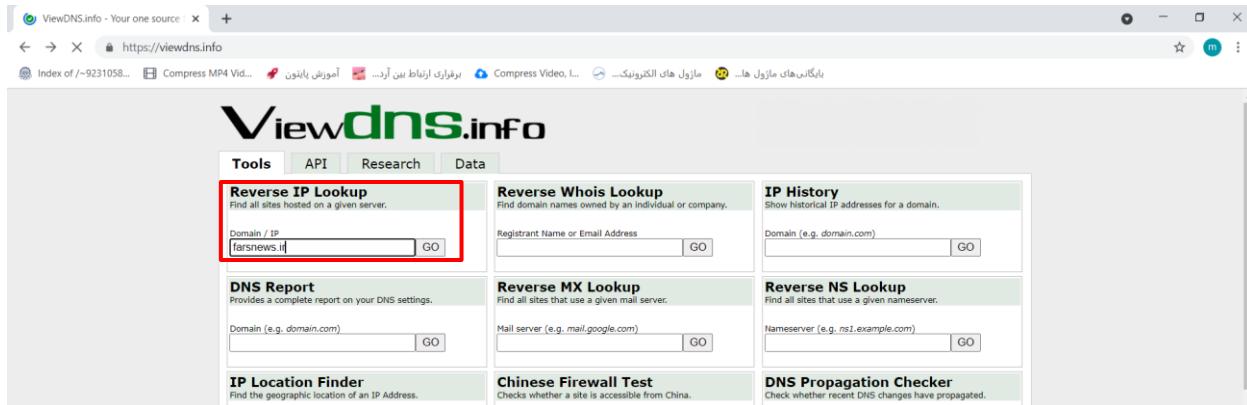
Test the response time to your domain name or IP address from multiple locations around the world. Useful for detecting latency issues on network connections.

Domain / IP Address:  GO

PING Results for asg.aut.ac.ir

Location	IP Address	Minimum RTT	Maximum RTT	Average RTT	Packet Loss
<b>Asia</b>					
Hong Kong, China	185.211.88.20	287.706	287.706	287.706	75%
Seoul, South Korea	185.211.88.20	357.445	357.702	357.616	25%
Singapore, Singapore	185.211.88.20	323.617	323.844	323.728	25%
Tokyo, Japan		-	-	-	100%
<b>Oceania</b>					
Perth, Australia	185.211.88.20	411.814	411.943	411.964	0%
Sydney, Australia	185.211.88.20	364.031	364.242	364.136	0%
<b>Europe</b>					
Falkenstein, Germany	185.211.88.20	99.583	99.802	99.645	0%
Helsinki, Finland	185.211.88.20	112.376	112.742	112.621	0%
Rotterdam, Netherlands	185.211.88.20	94.211	94.428	94.344	0%
Sandefjord, Norway	185.211.88.20	112.276	112.476	112.397	0%
<b>North America</b>					
Beauharnois, Canada	185.211.88.20	174.386	174.464	174.430	0%
Atlanta, USA	185.211.88.20	177.334	177.454	177.398	0%
Los Angeles, USA	185.211.88.20	225.529	225.669	225.599	50%
New York USA	185.211.88.20	162.203	162.600	162.491	0%

مرحله سوم) در قسمت Reverse IP Lookup آدرس farsnews.ir را وارد کنید.

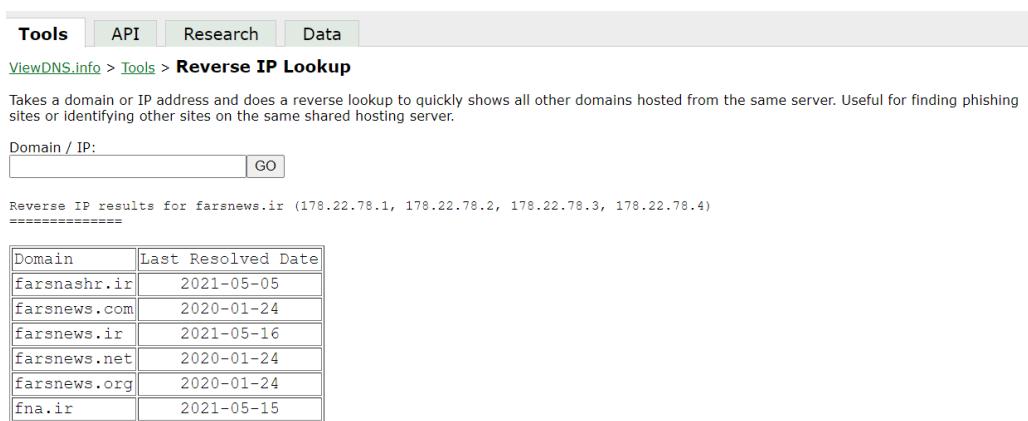


The screenshot shows the ViewDNS.info homepage with the 'Tools' tab selected. In the 'Reverse IP Lookup' section, the domain 'farsnews.ir' is entered into the 'Domain / IP' field, and the 'GO' button is highlighted with a red box. Other sections visible include 'Reverse Whois Lookup', 'IP History', 'DNS Report', 'Reverse MX Lookup', 'Reverse NS Lookup', 'IP Location Finder', 'Chinese Firewall Test', and 'DNS Propagation Checker'.

سوال ۵: چه وب سایت‌های دیگری بر روی همین سرور قرار دارند؟ چندمورد از آنها را نام ببرید.

(آدرس IP آنها را با آدرس IP سایت farsnews.ir مقایسه کنید.)

بعد از اینکه دکمه GO را بزنیم با صفحه‌ی زیر مواجه میشویم:



The screenshot shows the 'Reverse IP Lookup' results for 'farsnews.ir'. The results table is as follows:

Domain	Last Resolved Date
farsnashr.ir	2021-05-05
farsnews.com	2020-01-24
farsnews.ir	2021-05-16
farsnews.net	2020-01-24
farsnews.org	2020-01-24
fna.ir	2021-05-15

بر روی این سرور چندین وب سایت دیگر قرار دارند که عبارتند از :

farsnashr.ir

farsnews.com

farsnews.net

farsnews.org

fna.ir

آدرس IP مربوط به farsnews.ir میتواند هریک از IP های 178.22.78.1, 178.22.78.2, 178.22.78.3, 178.22.78.4 باشند . وقتی چندین IP دارد از آن میتواند برای load balancing استفاده کند. همچنین آدرس shared IP دیگر وب سایت هایی که روی این سرور میباشند نیز میتواند هریک از این موارد باشد و به صورت IP hosting میباشد.

## سوال 6: به نظر شما سرور چگونه وب سرور درخواست شده را تشخیص می‌دهد؟ آیا این روش نیز نوعی Multiplexing است؟

باتوجه به درخواستی که آمده یکی از وب سرورها انتخاب می‌شود. مانند hostهای اشتراکی که اکنون وجود دارند اگر روی یک IP بیشتر از یک وب سایت وجود داشته باشد باید در قسمت سرآیند یا هدر HTTP نام host شود تا Web Server بفهمد که فایل‌های کدام وب سایت مورد نظر است.

بله می‌توان گفت نوعی Multiplexing به صورت SDM می‌باشد. چون درواقع طبق تعریفی که برای مالتی پلکسینگ داشتیم و چند جریان از یک لینک عبور می‌کرد، در اینجا نیز چند درخواست مربوط به وب سایت‌های مختلف به یک وب سرور می‌رود.

( توضیحات بیشتر: در shared IP hosting که بهش name-based virtual hosting هم می‌گویند، host های مجازی چندین host name را روی یک ماشین با یک IP Address واحد ارائه میدهند. این امکان وجود دارد زیرا وقتی یک مرورگر وب با استفاده از HTTP از Web Server منبعی را درخواست می‌کند، را هم به عنوانی بخشی از درخواست درخواست می‌کند. سرور از این اطلاعات برای اینکه چه وبسایتی را به کاربر نشان دهد، استفاده می‌کند).

<https://superuser.com/questions/577070/is-it-possible-for-many-domain-names-to-share-one-ip-address/577072#:~:text=7%20Answers&text=Yes%2C%20this%20is%20an%20extra,with%20a%20single%20IP%20address>.

مرحله چهارم) به وب سایت زیر بروید:

<https://simpledns.com/lookup-dg>

The screenshot shows a web browser window with the URL <https://simpledns.com/lookup-dg>. The page title is "Simple DNS Plus by JH Software". Below the title, there is a section titled "Trace DNS Delegation". A sub-section explains that this function traces DNS delegation from the Internet DNS root servers down to the DNS servers responsible for the domain. It notes that results may vary if tracing is done multiple times or on different servers due to updates. A note also states that entering an IP address will trace its reverse DNS PTR record. Below this, there is a form with a "Domain Name / IP Address" input field containing "aut.ac.ir" and a "Trace >>" button. At the bottom of the page, there is a link to "Other on-line DNS tools at this web-site".

مرحله پنجم) در این وب سایت آدرس aut.ac.ir را وارد کرده و درخواست‌ها و پاسخ‌های دریافت شده را بررسی کنید.

The screenshot shows the "Trace DNS Delegation" results for the domain "aut.ac.ir". The process starts by loading the root server list. It then sends a request to the first root server, "b.root-servers.net" (192.228.79.201). It receives a referral response from "ir.cctld.authdns.ripe.net" (193.0.9.85), which includes the IP addresses of authoritative servers for ".ac" and ".ir". Subsequent requests are made to these servers, with the final result being an A-record for "aut.ac.ir" with the IP address 185.211.88.6.

```
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 (192.203.230.10)
-> e.root-servers.net (192.5.5.241)
-> f.root-servers.net (192.112.36.4)
-> g.root-servers.net (192.63.2.53)
-> h.root-servers.net (192.36.148.17)
-> i.root-servers.net (192.36.148.30)
-> 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 "b.root-servers.net" (192.228.79.201)

Received referral response - DNS servers for ".ir":
-> a.ir.cir (193.189.123.2)
-> b.ir.cir (193.189.122.83)
-> ir.cctld.authdns.ripe.net (193.0.9.85)
-> ns5.univie.ac.at (193.171.256.77)

Sending request to "ir.cctld.authdns.ripe.net" (193.0.9.85)

Received referral response - DNS servers for "aut.ac.ir":
-> ns1.aut.ac.ir (194.225.33.14)
-> ns2.aut.ac.ir (194.225.34.9)
-> ns3.aut.ac.ir (185.211.88.6)

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
```

## مشاهده و تخصیص پورت‌های لایه‌ی انتقال با استفاده از ابزار Netstat

**سوال 7:** برای لیست کردن برنامه‌هایی که در حال حاضر پورت‌های لایه‌ی انتقال را بر روی سیستم باز کرده‌اند، از چه دستور خط فرمانی استفاده می‌شود؟

ابتدا وارد CMD می‌شویم. سپس به کمک netstat –h میتوانیم help مربوط به netstat را بیابیم:

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.18363.1256]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>netstat -h

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [interval]

-a          Displays all connections and listening ports.
-b          Displays the executable involved in creating each connection or
           listening port. In some cases well-known executables host
           multiple independent components, and in these cases the
           sequence of components involved in creating the connection
           or listening port is displayed. In this case the executable
           name is in [] at the bottom, on top is the component it called,
           and so forth until TCP/IP was reached. Note that this option
           can be time-consuming and will fail unless you have sufficient
           permissions.
-e          Display Ethernet statistics. This may be combined with the -s
           option.
-f          Displays Fully Qualified Domain Names (FQDN) for foreign
           addresses.
-n          Displays addresses and port numbers in numerical form.
-o          Displays the owning process ID associated with each connection.
           Shows connection information for a specific process proto; proto
           may be any of: TCP, UDP, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
-p proto    Show connection statistics for a specific protocol proto. If used with the -s
           option to display per-protocol statistics, proto may be any of:
           IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
-q          Displays all connections, listening ports, and bound
           nonlistening TCP ports. Bound nonlistening ports may or may not
           be associated with an active connection.
-r          Displays the routing table.
-s          Displays per-protocol statistics. By default, statistics are
           shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
           the -p option may be used to specify a subset of the default.
-t          Displays the current connection offload state.
-x          Displays NetworkDirect connections, listeners, and shared
           endpoints.
-y          Displays the TCP connection template for all connections.
           Cannot be combined with the other options.
interval   Redisplay statistics, pausing for the specified interval seconds
           between each display. Press CTRL+C to stop redisplaying
           statistics. If omitted, netstat will print the current
           configuration information once.

C:\WINDOWS\system32>
```

همانطور که مشاهده می‌شود به کمک –a میتوان همه‌ی connection‌ها و listening port‌ها را مشاهده کرد. به کمک –b میتوان فایل exe‌ای که در باز کردن این پورت نقش داشته را هم تعیین کرد و به کمک –o هم میتوان یک ستون اضافه کرد که PID مربوط به اون پردازه‌ها را هم نشان دهد. (البته لازم به ذکر است برای –b netstat را به صورت Run as administrator باید CMD را به صورت Run as administrator اجرا کرد).

برای این که به صورت کامل این موارد را با هم داشته باشیم میتوان از دستور زیر استفاده کرد:

netstat –abn

```
C:\Windows\system32>Administrator: Command Prompt
Microsoft Windows [Version 10.0.18363.1256]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>netstat -abn

Active Connections

 Proto Local Address          Foreign Address        State      PID
 Proto Local Address          Foreign Address        State      PID
 TCP    0.0.0.0:135             DESKTOP-2Q4PCST:0    LISTENING  1056
 RpcSs
 [svchost.exe]
 TCP    0.0.0.0:445              DESKTOP-2Q4PCST:0    LISTENING  4
 Can not obtain ownership information
 TCP    0.0.0.0:808              DESKTOP-2Q4PCST:0    LISTENING  4484
 [OneApp.IGCE.WinService.exe]
 TCP    0.0.0.0:5040             DESKTOP-2Q4PCST:0    LISTENING  7084
 CDPSync
 [svchost.exe]
 TCP    0.0.0.0:5357             DESKTOP-2Q4PCST:0    LISTENING  4
 Can not obtain ownership information
 TCP    0.0.0.0:7070             DESKTOP-2Q4PCST:0    LISTENING  4316
 [AnyDesk.exe]
 TCP    0.0.0.0:7688             DESKTOP-2Q4PCST:0    LISTENING  8472
 Can not obtain ownership information
 TCP    0.0.0.0:49664            DESKTOP-2Q4PCST:0    LISTENING  812
 [lsass.exe]
 TCP    0.0.0.0:49665            DESKTOP-2Q4PCST:0    LISTENING  756
```

## سوال 8: دستوری را پیدا کنید که به وسیله آن تمام پورت‌های سیستم در هر وضعیت اتصالی همراه با مبدأ و

مقصد اتصال به صورت عددی لیست شوند.

به کمک a – که میتوانستیم همهی connection‌ها و listening port‌ها را لیست کنیم.

به کمک n – میتوان آدرس‌ها و پورت‌ها را به صورت عددی نمایش داد.

پس به کمک an – میتوان تمام پورت‌های سیستم را به همراه مبدأ و مقصد اتصال لیست کرد.

به کمک q – میتوان تمام پورت‌ها در هر وضعیت اتصالی را نشان داد. طبق توضیحات داخل help آن به کمک این دستور میتوان تمامی connection‌ها و listening port‌ها را نشان داد.

بنابراین برای نمایش کاملتر خواسته سوال میتوان از دستور زیر استفاده کرد:

netstat –anq

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	0.0.0.0:5357	0.0.0.0:0	LISTENING
TCP	0.0.0.0:7670	0.0.0.0:0	LISTENING
TCP	0.0.0.0:7688	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	0.0.0.0:49704	0.0.0.0:0	LISTENING
TCP	0.0.0.0:55555	0.0.0.0:0	LISTENING
TCP	127.0.0.1:63978	0.0.0.0:0	LISTENING
TCP	127.0.0.1:63978	127.0.0.1:63979	ESTABLISHED
TCP	127.0.0.1:63979	127.0.0.1:63978	ESTABLISHED
TCP	192.168.43.175:139	0.0.0.0:0	LISTENING
TCP	192.168.43.175:63667	52.163.231.110:443	ESTABLISHED
TCP	192.168.43.175:63677	51.83.238.220:80	ESTABLISHED
TCP	192.168.43.175:63681	157.240.20.57:443	ESTABLISHED
TCP	192.168.43.175:63727	64.233.167.188:5228	ESTABLISHED
TCP	192.168.43.175:63728	52.139.250.253:443	ESTABLISHED
TCP	192.168.43.175:64255	52.149.21.60:443	ESTABLISHED
TCP	192.168.43.175:64577	198.252.206.25:443	ESTABLISHED
TCP	192.168.43.175:64850	149.82.113.26:443	ESTABLISHED
TCP	192.168.43.175:64908	40.90.189.152:443	ESTABLISHED
TCP	192.168.43.175:64929	142.256.181.66:443	ESTABLISHED
TCP	192.168.43.175:64933	216.58.207.3:443	TIME_WAIT
TCP	192.168.43.175:64934	54.175.29.162:443	ESTABLISHED
TCP	192.168.43.175:64935	216.58.207.2:443	TIME_WAIT
TCP	192.168.43.175:64936	54.175.29.162:443	TIME_WAIT
TCP	192.168.43.175:64937	142.256.181.99:443	TIME_WAIT
TCP	192.168.43.175:64938	52.109.68.14:443	TIME_WAIT
TCP	192.168.43.175:64939	13.107.21.200:443	ESTABLISHED
TCP	192.168.43.175:64940	13.107.18.11:443	ESTABLISHED
TCP	192.168.43.175:64941	13.107.21.200:443	ESTABLISHED
TCP	192.168.43.175:64945	157.240.20.52:443	ESTABLISHED
TCP	192.168.43.175:64946	13.107.246.254:443	ESTABLISHED
TCP	192.168.43.175:64947	131.251.33.254:443	ESTABLISHED
TCP	192.168.43.175:64948	13.107.3.254:443	ESTABLISHED
TCP	192.168.43.175:64949	204.79.197.222:443	ESTABLISHED
TCP	192.168.56.1:139	0.0.0.0:0	LISTENING
TCP	0.0.0.0:53667	0.0.0.0:0	BOUND
TCP	0.0.0.0:53677	0.0.0.0:0	BOUND

Command Prompt			
TCP	0.0.0.0:63667	0.0.0.0:0	BOUND
TCP	0.0.0.0:63677	0.0.0.0:0	BOUND
TCP	0.0.0.0:63681	0.0.0.0:0	BOUND
TCP	0.0.0.0:63727	0.0.0.0:0	BOUND
TCP	0.0.0.0:63728	0.0.0.0:0	BOUND
TCP	0.0.0.0:63979	0.0.0.0:0	BOUND
TCP	0.0.0.0:64255	0.0.0.0:0	BOUND
TCP	0.0.0.0:64577	0.0.0.0:0	BOUND
TCP	0.0.0.0:64667	0.0.0.0:0	BOUND
TCP	0.0.0.0:64850	0.0.0.0:0	BOUND
TCP	0.0.0.0:64856	0.0.0.0:0	BOUND
TCP	0.0.0.0:64908	0.0.0.0:0	BOUND
TCP	0.0.0.0:64929	0.0.0.0:0	BOUND
TCP	0.0.0.0:64934	0.0.0.0:0	BOUND
TCP	0.0.0.0:64939	0.0.0.0:0	BOUND
TCP	0.0.0.0:64940	0.0.0.0:0	BOUND
TCP	0.0.0.0:64941	0.0.0.0:0	BOUND
TCP	0.0.0.0:64945	0.0.0.0:0	BOUND
TCP	0.0.0.0:64946	0.0.0.0:0	BOUND
TCP	0.0.0.0:64947	0.0.0.0:0	BOUND
TCP	0.0.0.0:64948	0.0.0.0:0	BOUND
TCP	0.0.0.0:64949	0.0.0.0:0	BOUND
TCP	[::]:135	[::]:0	LISTENING
TCP	[::]:445	[::]:0	LISTENING
TCP	[::]:808	[::]:0	LISTENING
TCP	[::]:5357	[::]:0	LISTENING
TCP	[::]:7688	[::]:0	LISTENING
TCP	[::]:49664	[::]:0	LISTENING
TCP	[::]:49665	[::]:0	LISTENING
TCP	[::]:49666	[::]:0	LISTENING
TCP	[::]:49667	[::]:0	LISTENING
TCP	[::]:49668	[::]:0	LISTENING
TCP	[::]:49704	[::]:0	LISTENING
TCP	[::]:1:49747	[::]:0	LISTENING
UDP	0.0.0.0:500	*.*	
UDP	0.0.0.0:3702	*.*	
UDP	0.0.0.0:3702	*.*	
UDP	0.0.0.0:3702	*.*	
UDP	0.0.0.0:4500	*.*	
UDP	0.0.0.0:5050	*.*	
UDP	0.0.0.0:5353	*.*	

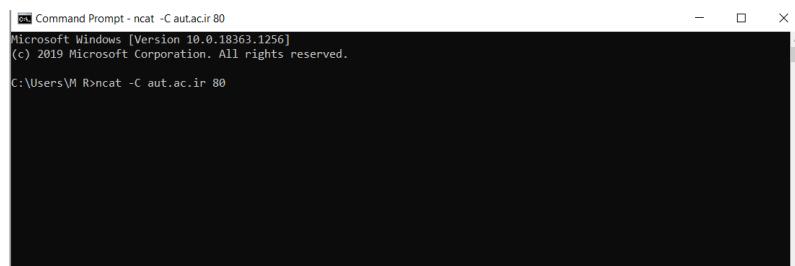
<https://www.computerweekly.com/tip/How-to-use-a-netstat-command-in-Windows-to-watch-open-ports>

## Web کارکرد

مرحله اول) در این بخش می خواهیم با استفاده از ابزار ncat و پروتکل HTTP یک ارتباط با وب سرور دانشگاه ایجاد کنیم. CMD را باز کرده و با استفاده از دستور زیر ابتدا یک ارتباط TCP با aut.ac.ir روی پورت 80 ایجاد کنید.

**ncat -C aut.ac.ir 80**

ابتدا در CMD دستور بالا را وارد میکنیم و enter میزنیم:



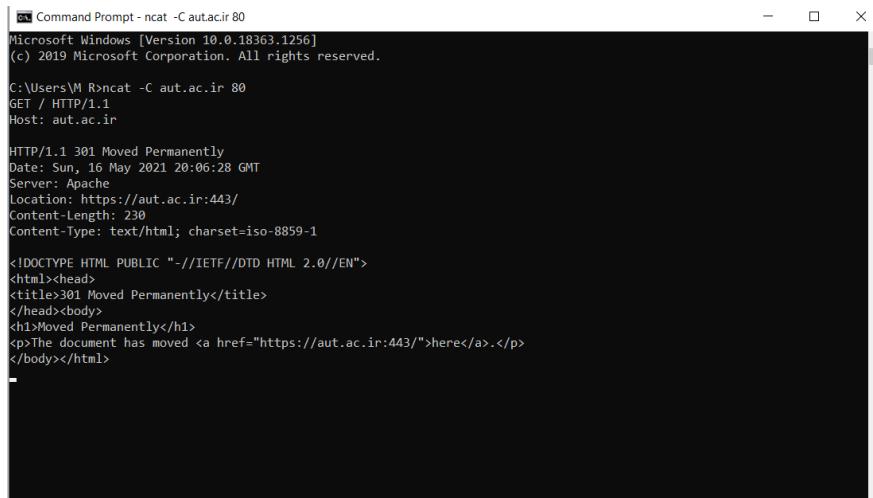
```
Command Prompt - ncat -C aut.ac.ir 80
Microsoft Windows [Version 10.0.18363.1256]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\M R>ncat -C aut.ac.ir 80
```

مرحله دوم) در ادامه پیام HTTP مربوط به دریافت آدرس / را مطابق دستور زیر وارد کنید. پس از فشردن دکمه enter در خط دوم یک بار دیگر enter را وارد کنید.

**GET / HTTP/1.1**

**Host: aut.ac.ir**



```
Command Prompt - ncat -C aut.ac.ir 80
Microsoft Windows [Version 10.0.18363.1256]
(c) 2019 Microsoft Corporation. All rights reserved.

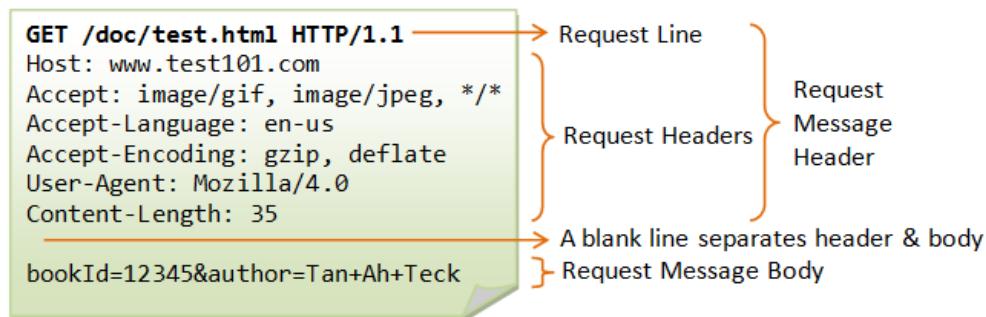
C:\Users\M R>ncat -C aut.ac.ir 80
GET / HTTP/1.1
Host: aut.ac.ir

HTTP/1.1 301 Moved Permanently
Date: Sun, 16 May 2021 20:06:28 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 ۹: دلیل وارد کردن دو enter پشت سرهم چیست؟

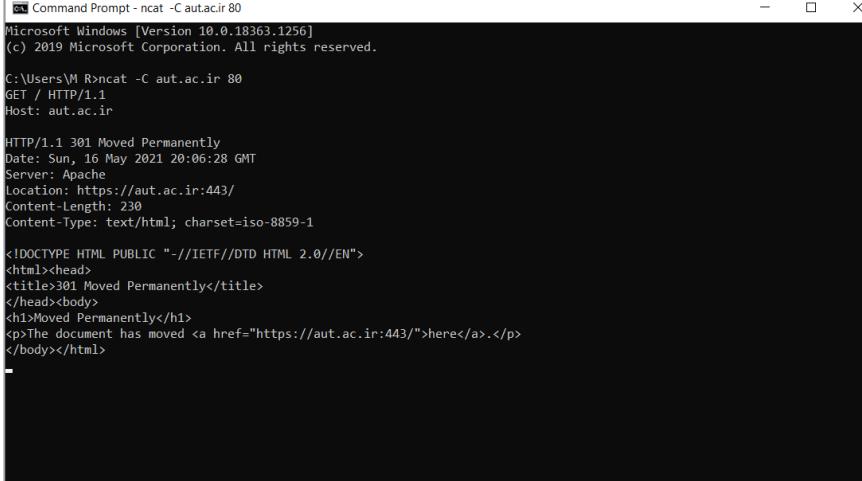
پیامی که ما میفرستیم یک request line دارد. بعد میتواند ۰ یا چندین header line داشته باشد. هر کدام از این line ها با یک enter header line میباشند. حال اگر بخواهیم بگوییم که blank ما تمام شده است باید یک enter بیشتر بزنیم و یک خط خالی ایجاد شود. در واقع پس این line پایان header field را نشان میدهد. برای مثال میتوانید فرمت کلی درخواست HTTP را در زیر ببینید:



(به صورت خلاصه: چون HTTP پروتکل Payload بعد از header یک enter توسط یک enter جدا میشود که خب با دو اینتر ما هدر درخواست را مشخص کردیم.)

**سوال 10:** پیامی که در پاسخ تقاضای شما داده می‌شود چیست؟ صفحه‌ی اصلی در کجا قرار دارد؟ ادعای خود را با استفاده از تقاضا به همین صفحه در مرورگر و ضبط پیام‌ها با استفاده از wireshark اثبات کنید.

پیامی که در پاسخ تقاضای ما داده می‌شود به صورت زیر می‌باشد:



```
Command Prompt - ncat -C aut.ac.ir 80
Microsoft Windows [Version 10.0.18363.1256]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\IR>ncat -C aut.ac.ir 80
GET / HTTP/1.1
Host: aut.ac.ir

HTTP/1.1 301 Moved Permanently
Date: Sun, 16 May 2021 20:06:28 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>
```

پیامی که در پاسخ به تقاضای ما داده می‌شود 3 بخش دارد: یک خط اول در ابتدای پیام است، بعد از آن یک سری header line می‌آید و یک خط خالی یا enter اضافه داریم و بعد از آن است که در حالت کلی شامل همان شیء درخواست شده توسط کاربر است که سرور برمی‌گرداند:

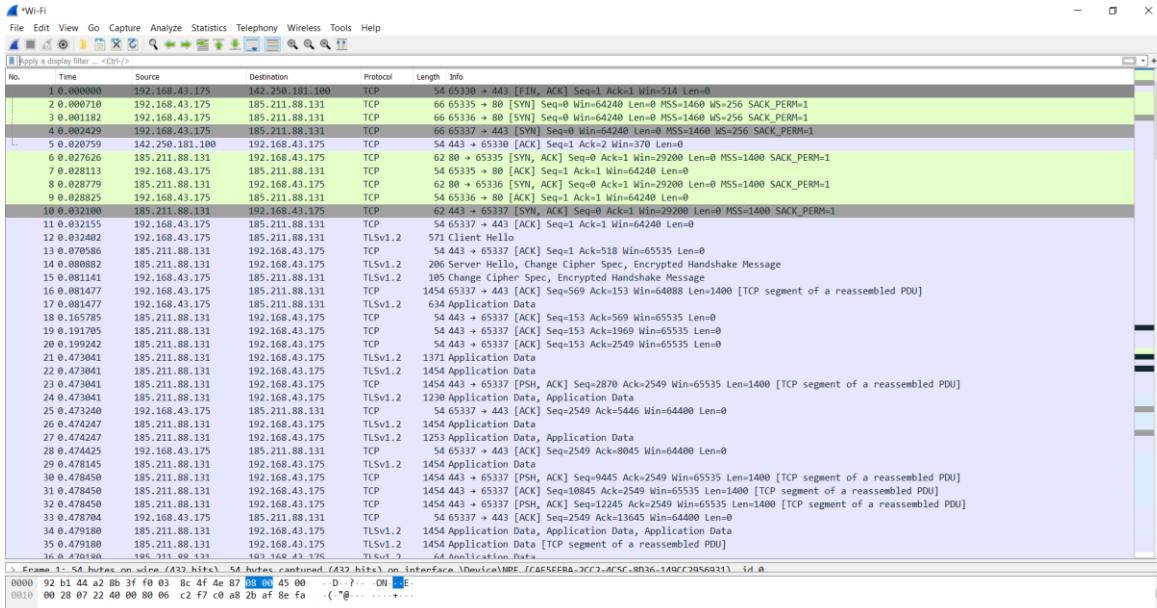
```
HTTP/1.1 301 Moved Permanently
Date: Sun, 16 May 2021 20:06:28 GMT
Server: Apache
Location: https://aut.ac.ir:443/
Content-Length: 230
Content-Type: text/html; charset=iso-8859-1
```

```
<!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>
```

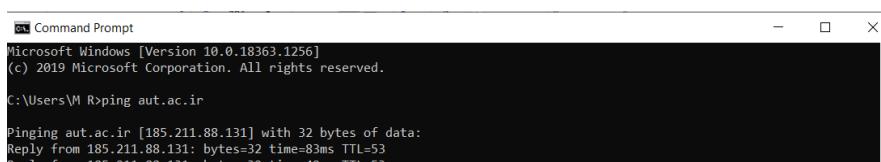
در کد وضعیت قرار گرفته که برابر 301 است که معنی انتقال دائمی این آدرس است. شیء درخواست شده برای همیشه از این سرویس دهنده منتقل شده است.

سرور URL جدید این شیء را در header field Location: به نام پیام پاسخ به کاربر برمیگرداند. بنابراین صفحه‌ی اصلی در https://aut.ac.ir و روی پورت 443 قرار دارد.

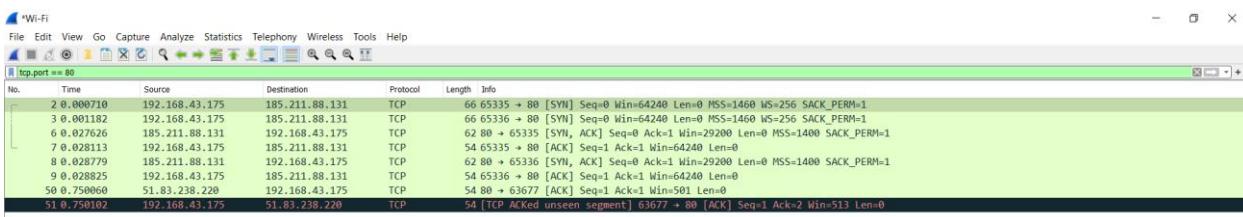
حال برای اثبات ادعای خود در مرورگر <http://aut.c.ir> را وارد میکنیم و با واپرشارک شنود میکنیم:



اولاً که IP مربوط به aut.ac.ir برابر با 185.211.88.131 میباشد. پس بسته‌هایی که آدرس مبدأ یا مقصدشان این میباشد برای این سایت میباشند (که با ping کردن سایت این آدرس را میتوان مشاهده کرد):



طبق عکسی که از واپرشارک مشاهده میشود ابتدا که آدرس سایت را با http در مرورگر وارد میکنیم، درخواست ها روی پورت 80 میباشد:



سپس اندکی که میگذرد اگر دقت شود همهی درخواست ها به پورت 443 انتقال داده شده اند و روی آن ادامه

پیدا کرده اند:

No.	Time	Source	Destination	Protocol	Length	Info
1 0.000000	192.168.43.175	142.250.181.100	TCP	54	65330 → 443 [FIN, ACK] Seq=1 Ack=1 Win=514 Len=0	
4 0.002429	192.168.43.175	185.211.88.131	TCP	66	65337 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1	
5 0.020759	142.250.181.100	192.168.43.175	TCP	54	443 → 65330 [ACK] Seq=1 Ack=2 Win=370 Len=0	
10 0.032100	185.211.88.131	192.168.43.175	TCP	62	443 → 65337 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1	
11 0.032155	192.168.43.175	185.211.88.131	TCP	54	65337 → 443 [ACK] Seq=1 Ack=1 Win=64248 Len=0	
12 0.032402	192.168.43.175	185.211.88.131	TLSv1.2	571	Client Hello	
13 0.070586	185.211.88.131	192.168.43.175	TCP	54	443 → 65337 [ACK] Seq=1 Ack=518 Win=65535 Len=0	
14 0.080882	185.211.88.131	192.168.43.175	TLSv1.2	206	Server Hello, Change Cipher Spec, Encrypted Handshake Message	
15 0.081141	192.168.43.175	185.211.88.131	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message	
16 0.081477	192.168.43.175	185.211.88.131	TCP	1454	65337 → 443 [ACK] Seq=569 Ack=153 Win=64088 Len=1400 [TCP segment of a reassembled PDU]	
17 0.081478	192.168.43.175	185.211.88.131	TLSv1.2	634	Application Data	
18 0.165785	185.211.88.131	192.168.43.175	TCP	54	443 → 65337 [ACK] Seq=153 Ack=569 Win=65535 Len=0	
19 0.191705	185.211.88.131	192.168.43.175	TCP	54	443 → 65337 [ACK] Seq=153 Ack=1969 Win=65535 Len=0	
20 0.199242	185.211.88.131	192.168.43.175	TCP	54	443 → 65337 [ACK] Seq=153 Ack=2549 Win=65535 Len=0	
21 0.473841	185.211.88.131	192.168.43.175	TLSv1.2	1371	Application Data	
22 0.473841	185.211.88.131	192.168.43.175	TLSv1.2	1454	Application Data	
23 0.473841	185.211.88.131	192.168.43.175	TCP	1454	443 → 65337 [PSH, ACK] Seq=2870 Ack=2549 Win=65535 Len=1400 [TCP segment of a reassembled PDU]	
24 0.473841	185.211.88.131	192.168.43.175	TLSv1.2	1230	Application Data, Application Data	
25 0.473240	192.168.43.175	185.211.88.131	TCP	54	65337 → 443 [ACK] Seq=2549 Ack=5446 Win=64400 Len=0	
26 0.474247	185.211.88.131	192.168.43.175	TLSv1.2	1454	Application Data	
27 0.474247	185.211.88.131	192.168.43.175	TLSv1.2	1253	Application Data, Application Data	
28 0.474425	192.168.43.175	185.211.88.131	TCP	54	65337 → 443 [ACK] Seq=2549 Ack=8045 Win=64400 Len=0	
29 0.478145	185.211.88.131	192.168.43.175	TLSv1.2	1454	Application Data	
30 0.478450	185.211.88.131	192.168.43.175	TCP	1454	443 → 65337 [PSH, ACK] Seq=9445 Ack=2549 Win=65535 Len=1400 [TCP segment of a reassembled PDU]	
31 0.478450	185.211.88.131	192.168.43.175	TCP	1454	443 → 65337 [ACK] Seq=10845 Ack=2549 Win=65535 Len=1400 [TCP segment of a reassembled PDU]	
32 0.478450	185.211.88.131	192.168.43.175	TCP	1454	443 → 65337 [PSH, ACK] Seq=12245 Ack=2549 Win=65535 Len=1400 [TCP segment of a reassembled PDU]	
33 0.478704	192.168.43.175	185.211.88.131	TCP	54	65337 → 443 [ACK] Seq=2549 Ack=13645 Win=64400 Len=0	
34 0.479180	185.211.88.131	192.168.43.175	TLSv1.2	1454	Application Data, Application Data, Application Data	
35 0.479180	185.211.88.131	192.168.43.175	TLSv1.2	1454	Application Data [TCP segment of a reassembled PDU]	
36 0.479180	185.211.88.131	192.168.43.175	TLSv1.2	64	Application Data	
37 0.479180	185.211.88.131	192.168.43.175	TLSv1.2	1454	Application Data	
38 0.479180	185.211.88.131	192.168.43.175	TLSv1.2	954	Application Data, Application Data	
39 0.479180	185.211.88.131	192.168.43.175	TLSv1.2	1454	Application Data	
40 0.479560	192.168.43.175	185.211.88.131	TCP	54	65337 → 443 [ACK] Seq=2549 Ack=20155 Win=64400 Len=0	
41 0.479877	185.211.88.131	192.168.43.175	TCP	1454	443 → 65337 [PSH, ACK] Seq=20155 Ack=2549 Win=65535 Len=1400 [TCP segment of a reassembled PDU]	
42 0.479877	185.211.88.131	192.168.43.175	TLSv1.2	1700	Application Data, Application Data, Application Data, Application Data	

Frame 1 - 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF\_{CAF5E7FA-2CC2-4C5C-8D36-1A0C29560311 id 0

0000 92 b1 44 a2 8b 3f f0 03 8c 4f 4e 87 08 00 45 00 D..?...ON...E

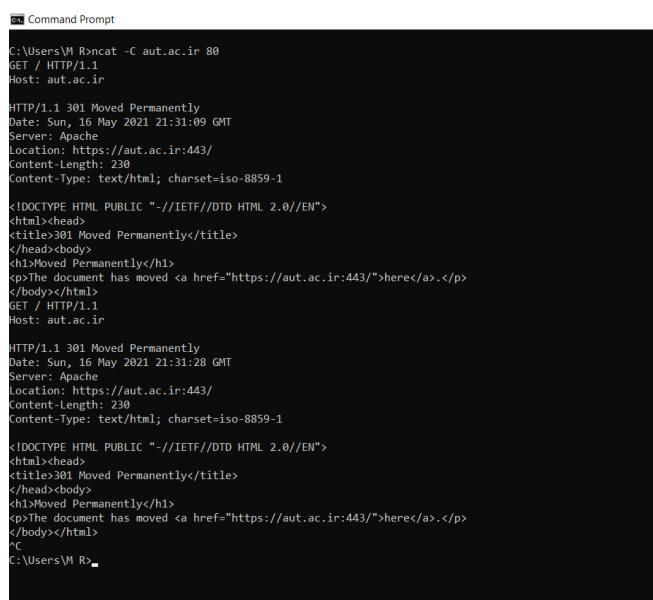
0010 00 28 07 22 40 00 00 06 c2 f7 c0 a8 2b af 8e fa .-."@-----+--

## سوال 11: آیا این ارتباط persistent است؟

بله با توجه به اینکه در پاسخ دریافتی connection را close نکرده است بنابراین میتوان گفت که به صورت persistent میباشد.

اگر به صورت non-persistent بود در پاسخی که سرور برمیگرداند در connection header field مربوط به مینوشت close که یعنی سرور میگوید بعد از ارسال این پیام اتصال TCP را خواهد بست.

برای مثال امدمیم بعد از درخواست اول یک بار دیگر درخواست را بدون باز کردن پورت ارسال کردیم و در نهایت با CRTL+C در CMD به ارتباط خاتمه دادیم پس ارتباط قبلی هنوز بسته نشده است:



```
Windows Command Prompt
C:\Users\IR>ncat -C aut.ac.ir 80
GET / HTTP/1.1
Host: aut.ac.ir

HTTP/1.1 301 Moved Permanently
Date: Sun, 16 May 2021 21:31:09 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>
GET / HTTP/1.1
Host: aut.ac.ir

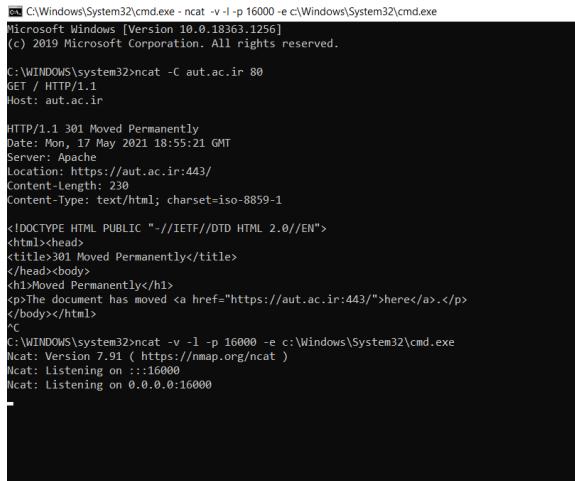
HTTP/1.1 301 Moved Permanently
Date: Sun, 16 May 2021 21:31:28 GMT
Server: Apache
Location: https://aut.ac.ir:443/
Content-Length: 230
Content-Type: text/html; charset=iso-8859-1

<!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>
C:\Users\IR>
```

مرحله سوم) با فشردن **CTRL+C** ارتباط قبلی را خاتمه دهید و دستور زیر را وارد کنید:

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

همانطور که گفته شده ابتدا با **CRTL+C** به ارتباط قبلی خاتمه میدهیم و دستور گفته شده را وارد میکنیم:



```
C:\Windows\System32\cmd.exe - ncat -v -l -p 16000 -e c:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.18363.1256]
(c) 2019 Microsoft Corporation. All rights reserved.

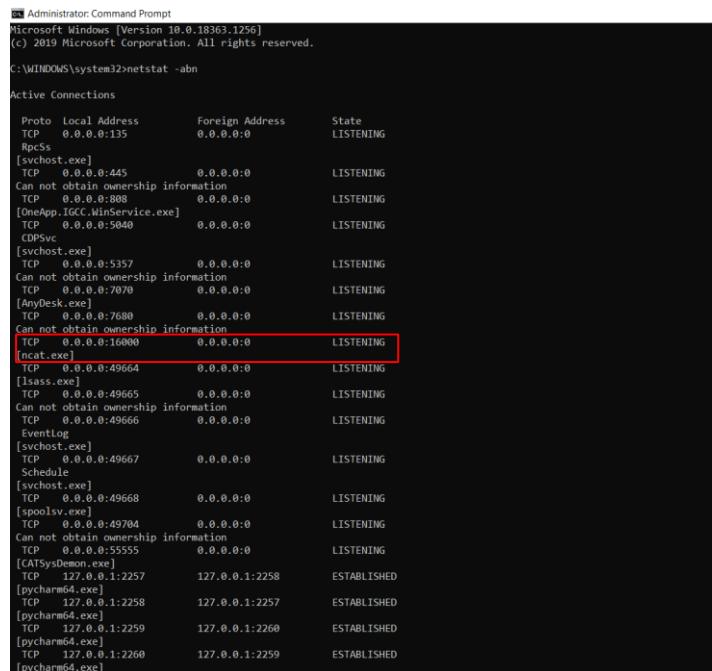
C:\WINDOWS\system32>ncat -C aut.ac.ir 80
GET / HTTP/1.1
Host: aut.ac.ir

HTTP/1.1 301 Moved Permanently
Date: Mon, 17 May 2021 18:55:21 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>
<C
C:\Windows\System32>ncat -v -l -p 16000 -e c:\Windows\System32\cmd.exe
[ncat: Version 7.91 ( https://nmap.org/ncat )
[ncat: Listening on :::16000
[ncat: Listening on 0.0.0.0:16000
```

مرحله چهارم) این دستور یک سوکت TCP ایجاد میکند که بر روی پورت 16000 گوش فرا می دهد، این موضوع را با استفاده از **netstat -anb** مشاهده کنید.

برای این کار بار دیگر CMD را به صورت run باز میکنیم و دستور گفته شده را وارد میکنیم:



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.18363.1256]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netstat -anb

Active Connections

Proto Local Address          Foreign Address        State
TCP   0.0.0.0:135           0.0.0.0:0             LISTENING
[RpcSs
[svchost.exe]
TCP   0.0.0.0:445           0.0.0.0:0             LISTENING
Can not obtain ownership information
TCP   0.0.0.0:888           0.0.0.0:0             LISTENING
[OneApp.IGCC.WinService.exe]
TCP   0.0.0.0:5040          0.0.0.0:0             LISTENING
[CDPSvc
[svchost.exe]
TCP   0.0.0.0:5357          0.0.0.0:0             LISTENING
Can not obtain ownership information
TCP   0.0.0.0:7670          0.0.0.0:0             LISTENING
[AnyDesk.exe]
TCP   0.0.0.0:7680          0.0.0.0:0             LISTENING
Can not obtain ownership information
TCP   0.0.0.0:16000          0.0.0.0:0             LISTENING
[ncat.exe]
TCP   0.0.0.0:49664         0.0.0.0:0             LISTENING
[isass.exe]
TCP   0.0.0.0:49665         0.0.0.0:0             LISTENING
Can not obtain ownership information
TCP   0.0.0.0:49666         0.0.0.0:0             LISTENING
[EventLog
[svchost.exe]
TCP   0.0.0.0:49667         0.0.0.0:0             LISTENING
Schedule
[svchost.exe]
TCP   0.0.0.0:49668         0.0.0.0:0             LISTENING
[spoolsv.exe]
TCP   0.0.0.0:49704         0.0.0.0:0             LISTENING
Can not obtain ownership information
TCP   0.0.0.0:55555         0.0.0.0:0             LISTENING
[CATSysDemon.exe]
TCP   127.0.0.1:2257        127.0.0.1:2258       ESTABLISHED
[pycharm.exe]
TCP   127.0.0.1:2258        127.0.0.1:2257       ESTABLISHED
[pycharm64.exe]
TCP   127.0.0.1:2259        127.0.0.1:2260       ESTABLISHED
[pycharm64.exe]
TCP   127.0.0.1:2260        127.0.0.1:2259       ESTABLISHED
[pycharm64.exe]
```

**سوال 12:** این پورت بر روی کدام آدرس IP ، bind شده است؟ بعد از برقراری ارتباط با این سوکت، برنامه CMD نیز اجرا می‌شود. در ادامه دستوراتی که فرستنده ارسال کند به این برنامه داده می‌شوند و خروجی دستورات از طریق ارتباط برقرار شده منتقل خواهد شد.

طبق اسکرین شات نشان داده شده ، این پورت بر روی آدرس IP ، 0.0.0.0 بایند شده است.

Can NOT obtain ownership information		
TCP	0.0.0.0:16000	0.0.0.0:0
[ncat.exe]		LISTENING

این آدرس به معنی تمامی آدرس IP های سیستم ما روی interface های مختلف شبکه میباشد. در پروتکل اینترنت ورژن 4 ، آدرس 0.0.0.0 یک مta آدرس غیرقابل مسیریابی است که برای تعیین یک هدف نامعتبر ، ناشناخته یا غیر قابل استفاده استفاده می شود. در زمینه مسیریابی ، 0.0.0.0 معمولاً به معنای مسیر پیش فرض است ، یعنی مسیری که به جای جایی در شبکه محلی به "بقیه" اینترنت منتهی می شود. آدرس IP 0.0.0.0 چندین معنی خاص در شبکه های کامپیوتری دارد. با این حال ، نمی توان آن را به عنوان یک آدرس کلی دستگاه مورد استفاده قرار داد. چند دلیل برای نمایش آی پی 0.0.0.0 وجود دارد:

- کامپیوترها بصورت عادی و پیشفرض وقتی به شبکه TCP/IP وصل نباشند؛ آی پی صفر را نمایش می دهند. در صورت داشتن آی پی؛ کامپیوتر قادر به دسترسی و تبادل اطلاعات با سایر تجهیزات متصل به شبکه نخواهد بود.
- نرم افزارهای کاربردی تحت شبکه هم از آی پی صفر بعنوان تکنیکی برای رصد و مشاهده ترافیک شبکه استفاده می کنند. زمانی که کامپیوتر های بهم متصل از این آدرس استفاده نمی کنند؛ پیامی روی آی پی جاری می شود که شامل آی پی صفر در هدر آن است که نشان دهنده ناشناخته بودن منبع ارسال است

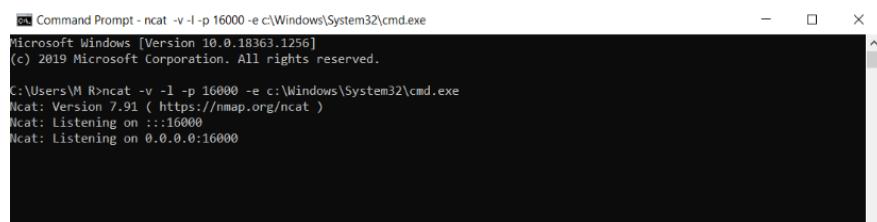
مرحله پنجم) آدرس آیپی سیستم دوست خود را یادداشت کنید، دستور زیر را اجرا کرده تا به پورت 16000

سیستم دوست خود متصل شوید:

ncat friend\_ip 16000

مرحله ششم) برای اینکه مطمئن شوید، با استفاده از دستور ipconfig تایید کنید که در سیستم دوستان هستید. ارتباط را با دستور CRTL+C ارتباط قبلی را خاتمه دهید.

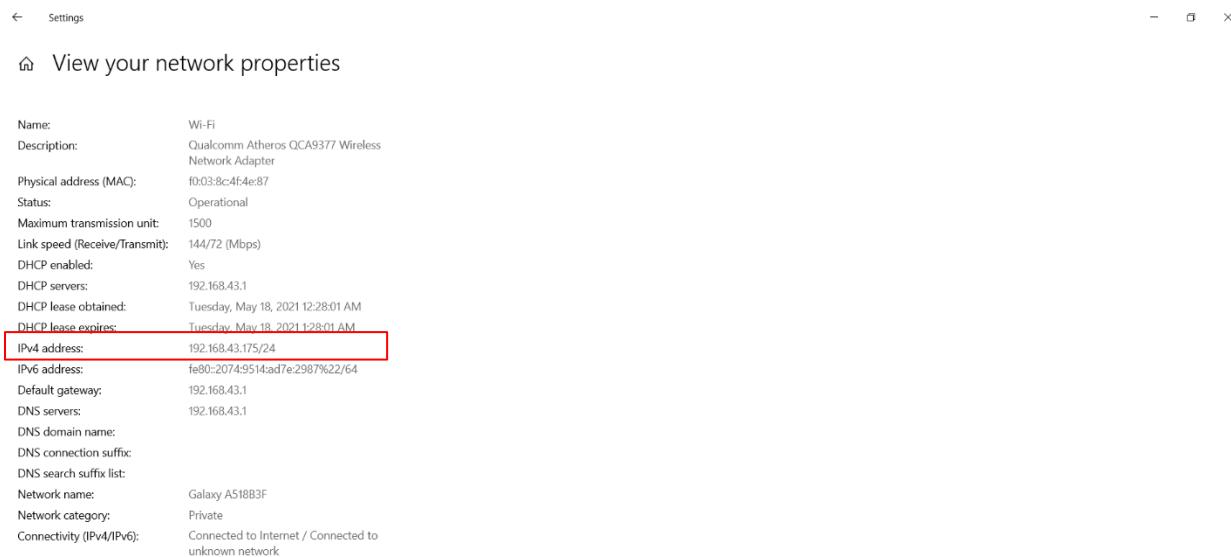
برای این کار من از گوشی همراه خود استفاده میکنم که به کمک آن اینترنت را برای لپ تاپ هات اسپات کرده ام. همچنین روی آن برنامه‌ی termux را نصب میکنم. سپس در کامپیوتر خودم روی پورت 16000 شنود میکنم و یک سوکت باز میکنم:



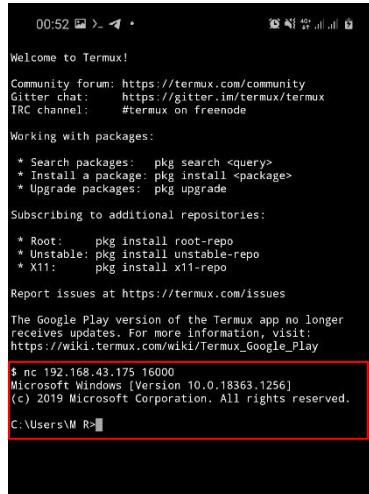
```
Command Prompt - nc -v -l -p 16000 -e c:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.18363.1256]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\W>Rncat -v -l -p 16000 -e c:\Windows\System32\cmd.exe
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::16000
Ncat: Listening on 0.0.0.0:16000
```

همچنین IP Address مربوط به کامپیوتر بنده 192.168.43.175 میباشد:



حال به سراغ گوشی میرویم و در آن دستور nc 192.168.43.175 16000 را وارد میکنیم(در termux به جای ncat باید ncat نوشت) :

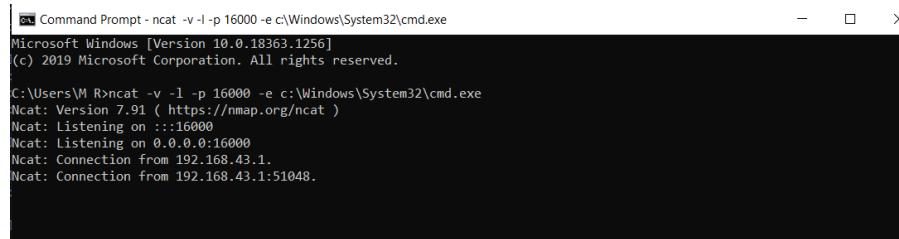


```

00:52 2023-07-11 14:52:00
Welcome to Termux!
Community forum: https://termux.com/community
Gitter chat: https://gitter.im/termux/termux
IRC channel: #termux on freenode
Working with packages:
  * Search packages: pkg search <query>
  * Install a package: pkg install <package>
  * Upgrade packages: pkg upgrade
Subscribing to additional repositories:
  * Root: pkg install root-repo
  * Unstable: pkg install unstable-repo
  * X11: pkg install x11-repo
Report issues at https://termux.com/issues
The Google Play version of the Termux app no longer
receives updates. For more information, visit:
https://wiki.termux.com/wiki/Termux_Google_Play
$ nc 192.168.43.175 16000
Microsoft Windows [Version 10.0.18363.1256]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Users\M R>

```

همانطور که مشاهده میشود به سیستم لپ تاپ وارد شدم. در این سمت هم در لپ تاپ به صورت زیر میشود:



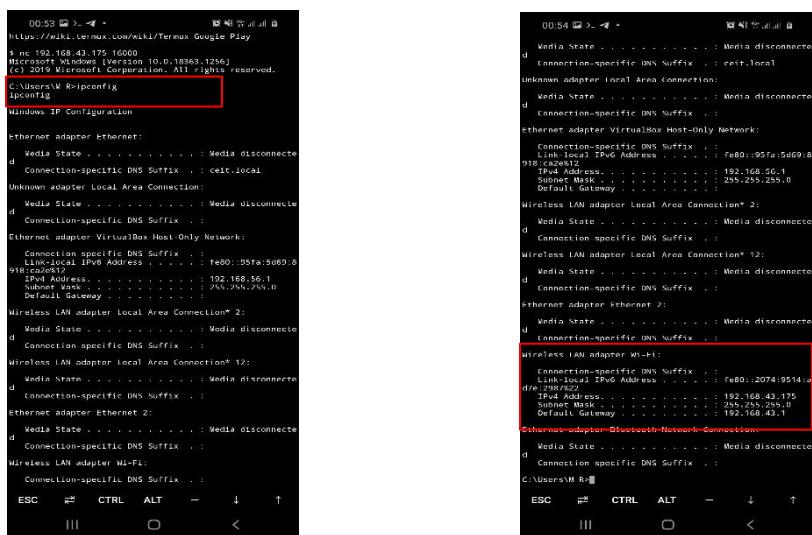
```

C:\ Command Prompt - ncat -v -l -p 16000 -e c:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.18363.1256]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\M R>ncat -v -l -p 16000 -e c:\Windows\System32\cmd.exe
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::16000
Ncat: Listening on 0.0.0.0:16000
Ncat: Connection from 192.168.43.1.
Ncat: Connection from 192.168.43.1:51048.

```

حال اگر در گوشی خود ipconfig را بزنم خواهیم داشت:



```

00:53 2023-07-11 14:53:00
https://wiki.termux.com/wiki/Termux_Google_Play
$ nc 192.168.43.175 16000
Microsoft Windows [Version 10.0.18363.1256]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\M R>ipconfig

Windows IP Configuration

Ethernet adapter ethernet:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . : cest.local
  Unknown adapter Local Area Connection:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
  Ethernet adapter VirtualBox Host-Only Network:
    Connection-specific DNS Suffix . : fe80::95fa:5d99%1
    Link-local IPv6 Address . . . . . : fe80::95fa:5d99%1
    IPv4 Address . . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
  Wireless LAN adapter local Area Connection* 2:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
  Wireless LAN adapter local Area Connection* 3:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
  Ethernet adapter Ethernet 2:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
  Wireless LAN adapter Wi-Fi:
    Connection-specific DNS Suffix . :
 00:54 2023-07-11 14:54:00
https://wiki.termux.com/wiki/Termux_Google_Play
$ ipconfig

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : cest.local
Unknown adapter Local Area Connection:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :
  Ethernet adapter VirtualBox Host-Only Network:
    Connection-specific DNS Suffix . : fe80::95fa:5d99%1
    Link-local IPv6 Address . . . . . : fe80::95fa:5d99%1
    IPv4 Address . . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
  Wireless LAN adapter Local Area Connection* 2:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
  Wireless LAN adapter Local Area Connection* 3:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
  Ethernet adapter Ethernet 2:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
  Wireless LAN adapter Wi-Fi:
    Connection-specific DNS Suffix . :
 00:54 2023-07-11 14:54:00
https://wiki.termux.com/wiki/Termux_Google_Play
$ ipconfig

Media State . . . . . : Media disconnected
Link-local IPv6 Address . . . . . : fe80::2074:9514%1
IPv4 Address . . . . . : 192.168.43.175
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.43.1
Ethernet adapter Ethernet 2:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :
  C:\Users\M R>

```

همانطور که مشاهده میشود اطلاعات سیستم لپتاپ را نمایش میدهد.

حال در گوشی CRTL+C را میزنیم و به سیستم خودمون در گوشی برمیگردیم:

```
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.43.1

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
d
    Connection-specific DNS Suffix . :

C:\Users\VM R>^C
$ █

    ESC      ↵     CTRL     ALT     -     ↓     ↑

    |||     ○     <
```

مرحله هفتم) با استفاده از دستور زیر می توانید یک web server ساده ایجاد کنید. این سرور تنها فایل index.html را که به آن داده اید میزبانی می کند و به کاربر تحويل می دهد.

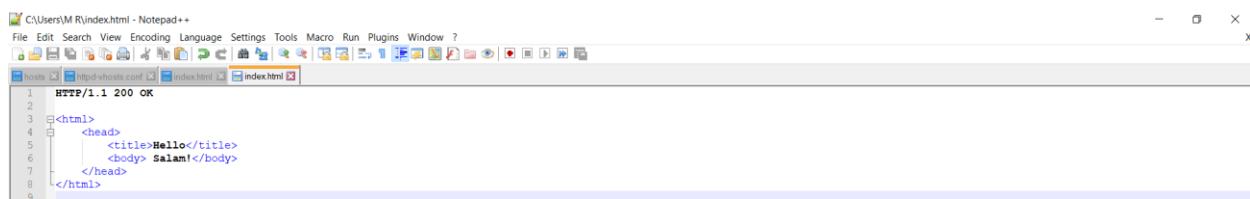
```
ncat -l -p 4444 < index.html
```

مرحله هشتم) برای فایل index.html می توانید از محتوای زیر استفاده کنید:

HTTP/1.1 200 OK

```
<html>  
<head>  
<title>Hello</title>  
<body> Salam!</body>  
</head>  
</html>
```

با توجه که در مسیر C:\Users\M R index ایجاد میکنیم:



سیسی دستور گفته شده را در CMD اجرا میکنیم:



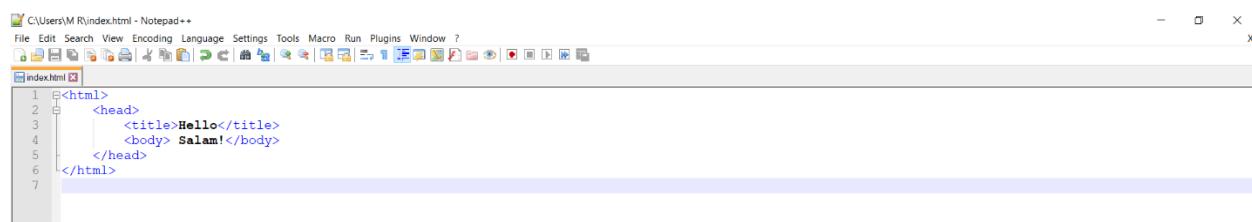
سپس اگر در آدرس بار مرورگر خود 127.0.0.1:4444 را وارد کنیم:



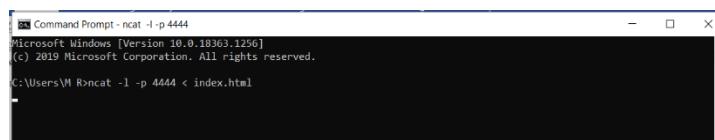
**سوال 13:** دقت کنید یک خط خالی بین HTTP و <html> باید وجود داشته باشد. به نظر شما دلیل وجود خط اول در این فایل چیست؟ یک فایل دیگر بدون خط اول این فایل بسازید و نتیجه را امتحان کنید.

وجود این خط اول تعیین میکند که بسته و درخواست از نوع HTTP میباشد و درخواست با موفقیت پاسخ داده شود.

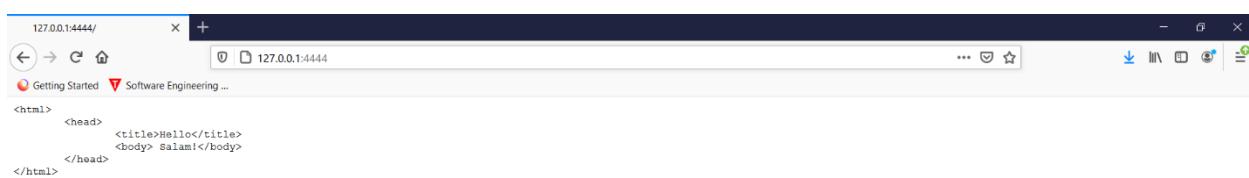
حال اگر این خط را حذف کنیم به صورت زیر:



حال اگر دوباره اجرا کنیم، چون فرمات پاسخ رعایت نشده است و عدد و کد پاسخ در آن نیامده است بنابراین نمیتوانیم به محتوا دسترسی داشته باشیم و به عنوان بسته HTTP شناخته نمیشود.:



سپس اگر بار دیگر در مرورگر 127.0.0.1:4444 را وارد کنیم با این صفحه مواجه میشویم:



هچنین همانطور که در سوال 9 نیز گفته شده بود، این خط خالی برای جدا کردن بخش body از header میباشد:

«پیامی که ما میفرستیم یک request line دارد. بعد میتواند ۰ یا چندین header line داشته باشد. هر کدام از این header line ها با یک enter از هم جدا میشوند. حال اگر بخواهیم بگوییم که Request Message ما تمام شده است باید یک enter بیشتر بزنیم و یک خط خالی ایجاد شود. درواقع پس این blank header field line پایان headerها را نشان میدهد...»

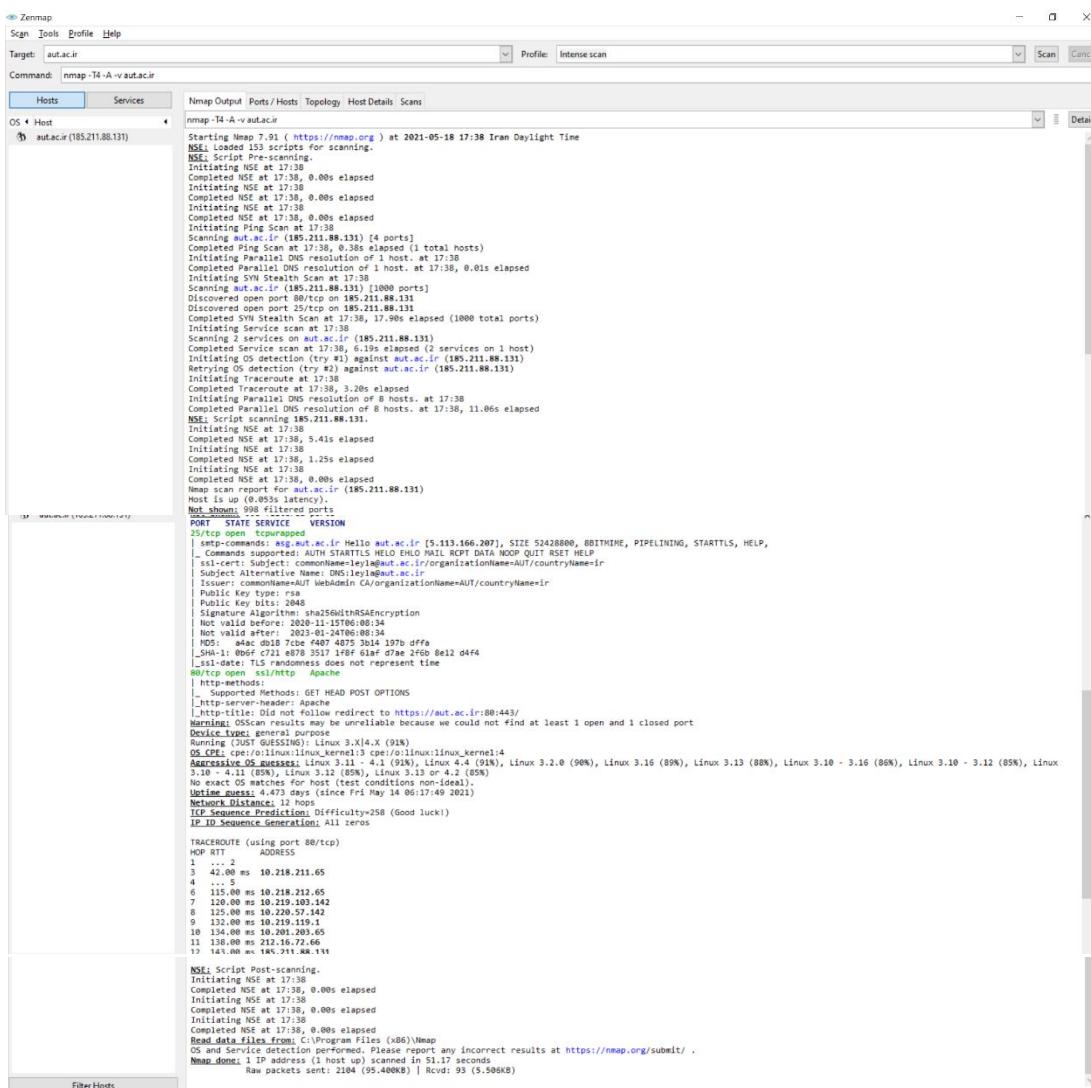
اگر این کار را نکنیم این فرمت و قالب را رعایت نکرده ایم و درنتیجه مرورگر نمیتواند این صفحه را بخواند و نمایش دهد.

پویش سرویس‌ها

برنامه NMAP به منظور پویش شبکه و سرویس‌های سیستم‌های انتهایی مورد استفاده قرار می‌گیرد. با استفاده از این برنامه می‌توانید تشخیص دهید بر روی هر سیستم چه سرویس‌هایی قرار دارد و آیا آن سرویس‌ها در دسترس هستند و یا خیر. رابط کاربری گرافیکی این ابزار Zenmap نام دارد.

مرحله اول) برنامه Zenmap را اجرا کرده و با استفاده از آن آدرس آی پی aut.ac.ir را اسکن کنید.

برنامه موردنظر را اجرا میکنیم و آدرس آی پی aut.ac.ir را اسکن میکنیم:



## سوال 14 : سیستم عامل این وب سایت چیست؟

میتوانیم برای دیدن مشخصات و جزئیات مربوطه به Host Details مراجعه کنیم. همانطور که مشاهده میشود سیستم عامل این وب سایت ، لینوکس میباشد.

The screenshot shows the Zenmap interface with the target set to aut.ac.ir (185.211.88.131) and the command nmap -T4 -A -v aut.ac.ir. The Host Details tab is selected, displaying the following information:

- Host Status:** State: up, Open ports: 2, Filtered ports: 998, Closed ports: 0, Scanned ports: 1000, Up time: 386470, Last boot: Fri May 14 06:17:49 2021.
- Addresses:** IPv4: 185.211.88.131, IPv6: Not available, MAC: Not available.
- Hostnames:** Name - Type: aut.ac.ir - user.
- Operating System:** Name: Linux 3.11 - 4.1, Accuracy: 91% (indicated by a green progress bar).
- Other sections include Ports used, OS Classes, TCP Sequence, IP ID Sequence, TCP TS Sequence, and Comments.

مشخصات کامل مربوط به سیستم عامل در بخش Operating System قرار گرفته است:

A detailed view of the Operating System section from the previous screenshot:

- Operating System:** Name: Linux 3.11 - 4.1, Accuracy: 91% (green bar).
- Ports used:** Port-Protocol-State: 80 - tcp - open, Port-Protocol-State: 44477 - udp - closed.
- OS Classes:** A table showing general purpose, Linux, Linux, 4.X, and 91% accuracy.

**سوال 15:** چه پورت‌هایی روی این سرور باز است؟

2 پورت باز روی این سرور وجود دارد که یکی پورت 80 و دیگری پورت 25 میباشد:

در تصویر زیر نیز اطلاعات بیشتری راجع به این دو پورت باز روی سرور ارائه شده است:

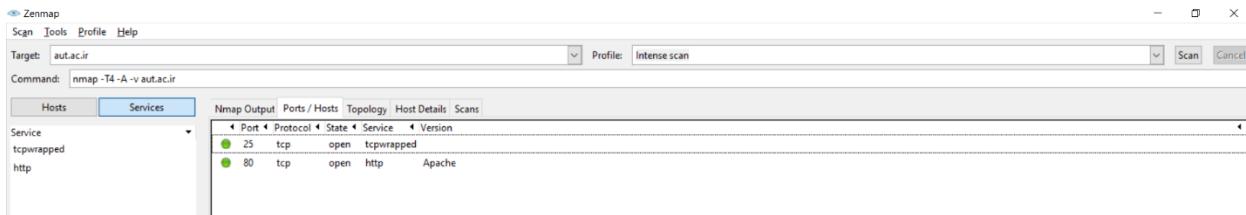
```
PORT      STATE SERVICE          VERSION
25/tcp    open  tcprwaped
|_smtp-commands: asg@aut.ac.ir Hello aut.ac.ir [5.113.166.207], SIZE 52428800, 8BITNIME, PIPELINING, STARTTLS, HELP
|_Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA NOOP QUIT RSET HELP
|_ssl-cert: Subject: commonName=ley@aut.ac.ir/organizationName=AUT/countryName=ir
|_Subject Alternative Name: DNS:ley@aut.ac.ir
Issuing certificate: Webmin CA/organizationName=AUT/countryName=ir
Public Key type: rsa
Public Key bits: 2048
Signature Algorithm: sha256WithRSAEncryption
Not valid before: 2028-11-15T06:08:34
Not valid after: 2023-11-15T06:08:34
NODS: 0x40000000 7c08 4f07 4b75 3d14 197b dffa
|_SHA-1: 0b6f c271 87b8 3517 1f8f 61af d7ae 2f6b 8e12 d4fa
|_ssl-date: TLS randomness does not represent time
80/tcp    open  ssl/tls Apache
| http-methods:
|   _ Supported Methods: GET HEAD POST OPTIONS
|_http-user-agent: Apache/2.4.42 (Ubuntu)
Warning: SSL/TLS can't be tested as it is unavailable because we could not find at least 1 open and 1 closed port
```

البته لازم به ذکر است دفعات متعددی که اسکن میکردیم ، نتایج مختلفی بعضاً نمایش داده میشد و در مجموع این موارد به دست آمد که پورت های 25 و 80 و 443 و 587 و همچنین پورت های 21 و 1723 و 8080 روی آن باز میباشند. مثلاً در عکس زیر یک حالتی که تعدادی از این پورت ها باز هستند را یک جا نمایش میدهد:

	Port	Protocol	State	Service	Version
●	21	tcp	open	ftp	
●	80	tcp	open	http	Apache httpd
●	443	tcp	open	ssl	Apache httpd (SSL-only mode)
●	1723	tcp	open	pptp	
●	8080	tcp	open	http-proxy	

## **سوال 16: سرویس هایی که از طریق پورت ها ارائه میشود چیست؟**

سرویس http از طریق پورت 80 و سرویس tcpwrapped از طریق پورت 25 ارائه میشوند.



در انتهای قبل برخی پورت های دیگر نیز معرفی شد که سرویس هایی که روی آن ها ارائه میشند نیز به صورت زیر است. چون همگی غالبا در یک اسکن نشان داده نمیشند به همین دلیل به صورت موردی در زیر ذکر کردم:

روی پورت 80 سرویس http

روی پورت 25 سرویس ESMTMP بیشتر دیده میشد منتها در مورد بالا که اسکرین قرارداده شده است نوع سرویس را tcpwrapped معرفی کرده است.

روی پورت 587 سرویس ESMTMP

روی پورت 443 سرویس های http/ssl

روی پورت 21 سرویس ftp

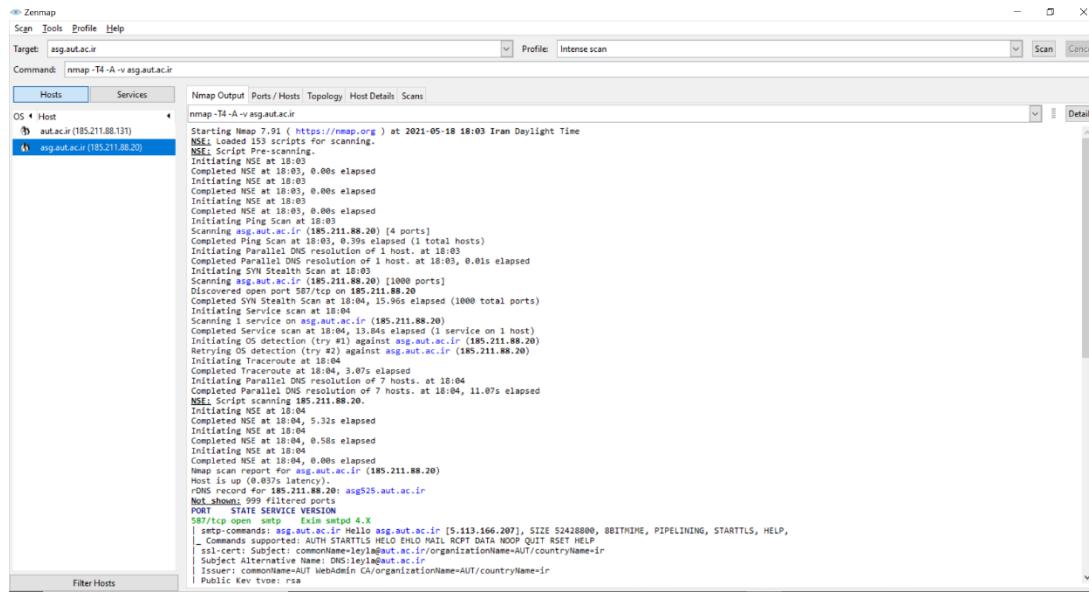
روی پورت 1723 سرویس pptp

روی پورت 8080 سرویس http-proxy

سوال 17: این بار آدرس asg.aut.ac.ir را پیش کنید. با انتخاب پروفایل Intense scan نتیجه چیست؟  
آدرس asg.aut.ac.ir را انتخاب کنید. نتیجه چیست؟ آدرس asg.aut.ac.ir را Ping کنید.

به نظر شما نتیجه اسکن به چه دلیلی تغییر کرده است؟ این ماشین چه نقشی در دانشگاه دارد؟

وقتی آدرس asg.aut.ac.ir را با پروفایل Intense scan پیش میکنیم نتیجه و خروجی Nmap به صورت زیر است:

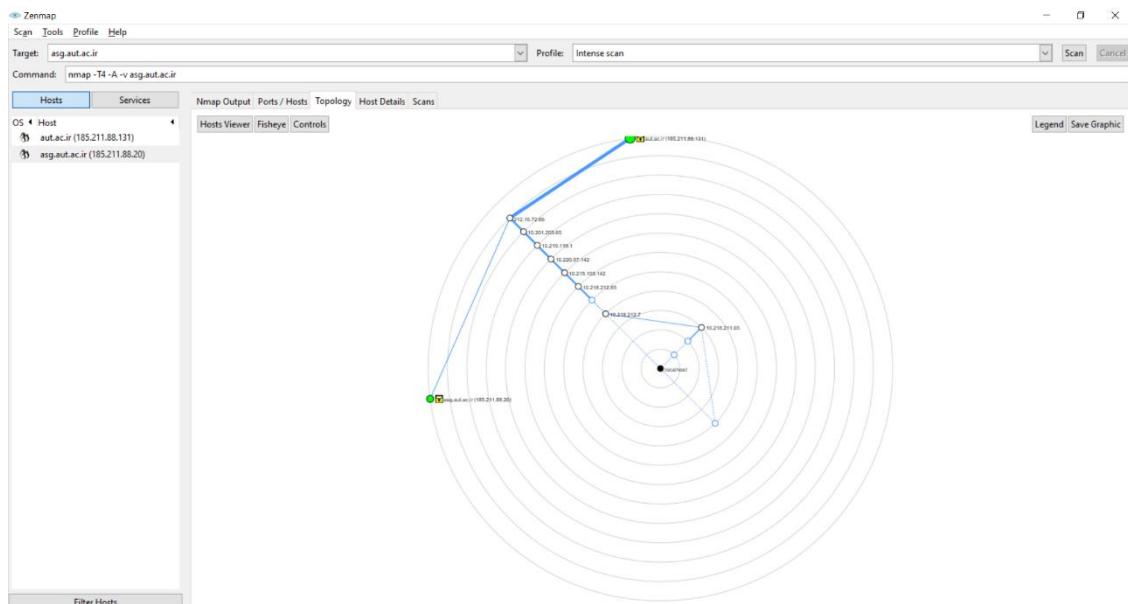


```

Zenmap
Scan Tools Profile Help
Target: asg.aut.ac.ir Profile: Intense scan
Command: nmap -T4 -A -v asg.aut.ac.ir
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v asg.aut.ac.ir
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-18 18:03 Iran Daylight Time
NSE: Loaded 193 scripts for scanning.
NSE Script Pre-scanning.
Initiating NSE at 18:03
Completed NSE at 18:03, 0.00s elapsed
Initiating NSE at 18:03
Completed NSE at 18:03, 0.00s elapsed
Initiating NSE at 18:03
Completed NSE at 18:03, 0.00s elapsed
Initiating NSE at 18:03
Completed NSE at 18:03, 0.00s elapsed
Initiating Ping Scan at 18:03
Scanning asg.aut.ac.ir (185.211.88.20) [4 ports]
Completed Ping Scan at 18:03, 0.39s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host at 18:03
Completed Parallel DNS resolution of 1 host at 18:03, 0.01s elapsed
Initiating OS detection (try #2) against asg.aut.ac.ir (185.211.88.20)
Scanning asg.aut.ac.ir (185.211.88.20) [1090 ports]
Discovered open port 587/tcp on 185.211.88.20
Completed SYN Stealth Scan at 18:04, 15.96s elapsed (1000 total ports)
Initiating Service scan at 18:04
Scanning 1 service on asg.aut.ac.ir (185.211.88.20)
Completed Service scan at 18:04, 13.84s elapsed (1 service on 1 host)
Initiating Parallel DNS resolution of 1 host at 18:04
Completed Parallel DNS resolution of 1 host at 18:04, 0.01s elapsed
Retrying OS detection (try #2) against asg.aut.ac.ir (185.211.88.20)
Initiating traceroute at 18:04
Completed traceroute at 18:04, 3.07s elapsed
Initiating Parallel DNS resolution of 7 hosts at 18:04
Completed Parallel DNS resolution of 7 hosts at 18:04, 11.07s elapsed
NSE Script scanning 185.211.88.20.
NSE Script scanning 185.211.88.20.
Initiating NSE at 18:04
Completed NSE at 18:04, 5.32s elapsed
Initiating NSE at 18:04
Completed NSE at 18:04, 5.58s elapsed
Initiating NSE at 18:04
Completed NSE at 18:04, 0.00s elapsed
NSE Script scanning 185.211.88.20.
NSE Script scanning 185.211.88.20.
Initiating NSE at 18:04
Completed NSE at 18:04, 0.00s elapsed
Nmap scan report for asg.aut.ac.ir (185.211.88.20)
Host is up (0.037s latency).
rDNS record for: 185.211.88.20 asg$25.aut.ac.ir
Not shown: 999 filtered ports
PORT      STATE SERVICE
587/tcp    open  smtp  Exim setup 4.x
| smtp-commands: asg.aut.ac.ir Hello asg.aut.ac.ir [5.113.166.207], SIZE 52428800, 8BITMIME, PIPELINING, STARTTLS, HELP,
| Commands supported: AUTH STANZA XFORWARD MAIL RCPT DATA NOOP QUIT RSET HELP
| Subject Alternative Name: asg.aut.ac.ir/organizationName=AUT/countryName=ir
| Subject Alternative Name: DNS-leyla@aut.ac.ir
| Issuer: commonName=AUT WebAdmin CA/organizationName=AUT/countryName=ir
| Public Key type: rsa

```

توپولوژی مربوط به آن نیز به صورت زیر میباشد:



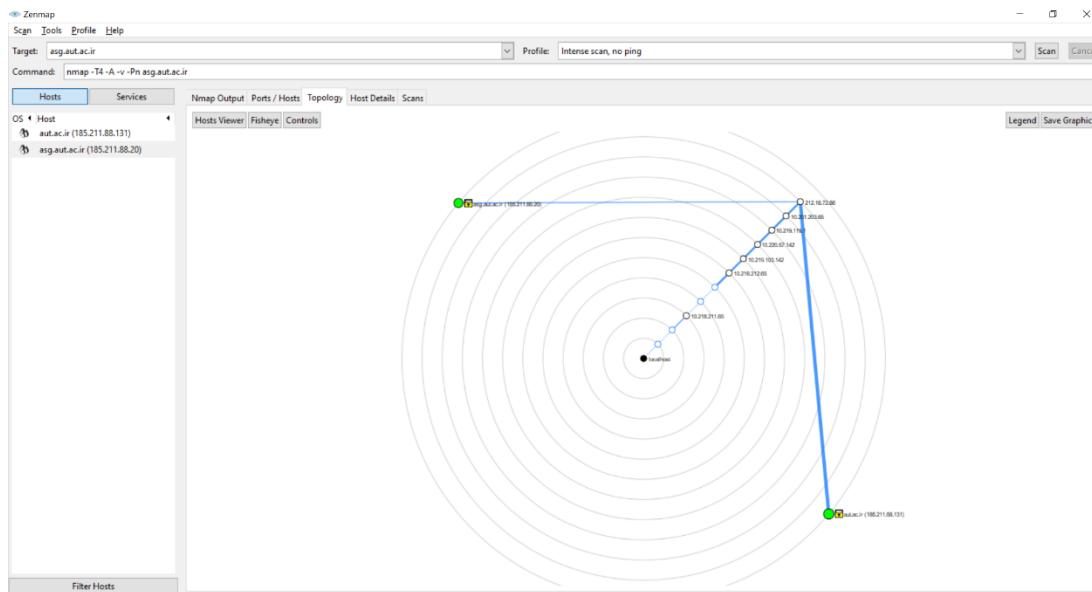
حال اگر پروفایل Intense scan, No ping Nmap را انتخاب کنیم خروجی به صورت زیر است:

The screenshot shows the Zenmap interface with the following details:

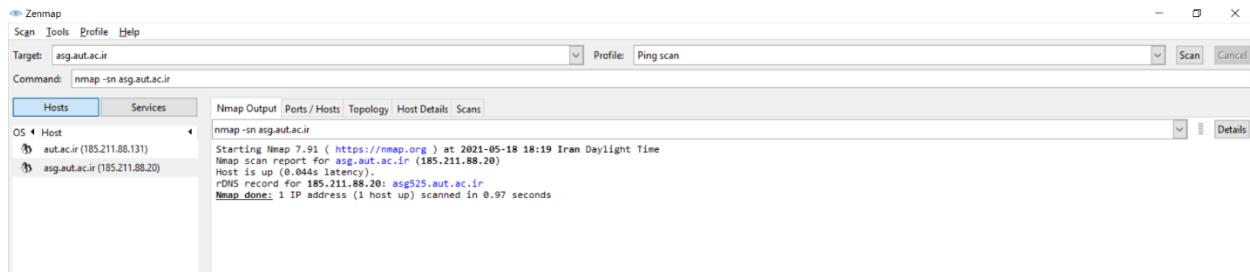
- Target:** asg.aut.ac.ir
- Profile:** Intense scan, no ping
- Command:** nmap -T4 -A -v -Pn asg.aut.ac.ir
- Hosts:** OS Host (aut.ac.ir (185.211.88.131)) and OS asg.aut.ac.ir (185.211.88.20).
- Nmap Output:** Displays the full Nmap log, including:
  - Starting Nmap 7.81 [https://nmap.org ] at 2021-05-18 18:14 Iran Daylight Time
  - NSEi: Loaded 193 scripts for scanning.
  - NSE: Script Pre-scanning.
  - Initiating Parallel DNS resolution of 1 host. at 18:14
  - Completed NSE at 18:14, 0.00s elapsed
  - Initiating NSE at 18:14
  - Completed NSE at 18:14, 0.00s elapsed
  - Initiating Ping Scan at 18:14
  - Scanning aut.ac.ir (185.211.88.20) [4 ports]
  - Completed Ping Scan at 18:14, 0.37s elapsed (1 total hosts)
  - Initiating Parallel DNS resolution of 1 host. at 18:14
  - Completed NSE at 18:14, 0.01s elapsed
  - Initiating SYN Stealth Scan at 18:14
  - Scanning asg.aut.ac.ir (185.211.88.20) [1000 ports]
  - Completed SYN Stealth Scan at 18:14, 30.61s elapsed (1000 total ports)
  - Initiating OS detection (try #1) against asg.aut.ac.ir (185.211.88.20)
  - Retrying OS detection (try #2) against asg.aut.ac.ir (185.211.88.20)
  - Initiating Service scan at 18:15
  - Completed Service scan at 18:15, 3.80s elapsed
  - Initiating Traceroute at 18:15, 3.80s elapsed
  - Completed Traceroute at 18:15, 3.80s elapsed
  - Initiating Parallel DNS resolution of 8 hosts. at 18:15
  - Completed Parallel DNS resolution of 8 hosts. at 18:15, 11.07s elapsed
  - NSE: Script scanning 185.211.88.20
  - Script scanning at 18:15
  - Completed Script scan at 18:15, 0.00s elapsed
  - Initiating NSE at 18:15
  - Completed NSE at 18:15, 0.00s elapsed
  - Initiating NSE at 18:15
  - Completed NSE at 18:15, 0.00s elapsed
  - Initiating NSE at 18:15
  - Completed NSE at 18:15, 0.00s elapsed
  - Nmap scan report for asg.aut.ac.ir (185.211.88.20)
  - Host is up (0.0000s latency or 185.211.88.20: asg925.aut.ac.ir)
  - All 1000 scanned ports on asg.aut.ac.ir (185.211.88.20) are filtered
  - Too many fingerprints match this host to give specific OS details
  - Network Distances: 12 hops
  - TRACE ROUTE (using proto icmp)  
HOP RTT ADDRESS  
1 ... 2  
3 44.00 ms 10.218.211.65  
4 45.00 ms 10.218.212.7  
5 ...  
6 35.00 ms 10.218.212.65  
7 37.00 ms 10.219.185.142

در این حالت تعداد واسطه هایی که طی میکنیم تا به مقصد برسیم نیز کمتر میباشد.

توپولوژی مربوط به آن نیز به صورت زیر میباشد:



حال آگر این سایت را پینگ کنیم خروجی به صورت زیر است:



همانطور که مشاهده میشود فقط مقصد را ping میکند و پورت ها را اسکن نمیکند.

همچنین اگر این آدرس را در CMD ، پینگ کنیم:

```
Microsoft Windows [Version 10.0.18363.1256]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\M R>ping asg.aut.ac.ir

Pinging asg.aut.ac.ir [185.211.88.20] with 32 bytes of data:
Reply from 185.211.88.20: bytes=32 time=49ms TTL=53
Reply from 185.211.88.20: bytes=32 time=41ms TTL=53
Reply from 185.211.88.20: bytes=32 time=55ms TTL=53
Reply from 185.211.88.20: bytes=32 time=31ms TTL=53

Ping statistics for 185.211.88.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 31ms, Maximum = 55ms, Average = 44ms

C:\Users\M R>
```

و خب همانطور هم که مشاهده میشود آدرس IP این domain با آن domain ای که در سوالات قبل در zenmap بررسی کردیم متفاوت میباشد و یک وب سرور دیگر است پس نسبت به آن ها تغییراتی خواهد داشت.

پس همانطور که مشاهده میشود نتیجه تغییر کرده است چراکه این ماشین نقش متفاوتی در مقصد دارد.

نقش این ماشین در دانشگاه:

این ماشین mail server دانشگاه میباشد.