

پاسخ سوال ۱:

این دامنه برای آقای علیرضا باقری است.
















ایمیلی که با آن دامنه رجیستر شده است soft98.ir@gmail.com می باشد.

پاسخ سوال ۲:











دو آدرس `ir1.hostdl.com` و `ir2.hostdl.com` نیم سرورهای این دامنه است.

پاسخ سوال ۳:




رکوردهای NS برای شناخت نیم سرورها است:

Status	Test Case	Information
	NS records at your local servers	NS records retrieved from your local nameservers were: <code>ir1.hostdl.com. [79.127.127.23] [TTL=86400]</code> <code>ir2.hostdl.com. [79.127.127.25] [TTL=86400]</code>
	Glue at local nameservers	Good! Your local nameservers send the IP address (glue) along with your NS records.
	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	Oops! One or more of your nameservers are on the same class C subnet. RFC2182 section 3.1 states that all of your nameservers should be in geographically and topologically dispersed locations for redundancy purposes.
	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 MX برای شناخت میل سرور است: (مثلا وقتی ایمیلی به ادرس info@soft98.ir زده شد به کدام ای پی باید تحویل داده شود؟!)

Status	Test Case	Information
	MX Records	Your Mail eXchanger (MX) records are: 0 soft98.ir. [TTL=14400]
	All nameservers have same MX records	Good! All of your nameservers have the same MX records.
	All MX records contain valid hostnames	Good! All of your MX entries have valid hostnames (e.g. are not IP's or invalid domain names).
	All MX records use public IP addresses	Good! All of your MX entries have public IP addresses.
	MX record is not a CNAME/alias	Good! When querying for your MX records we did not receive a CNAME record as a result.
	MX A records are not CNAME's	Good! No CNAME records are present for your MX A records.
	Number of MX records	Oops! You only have one MX record! In the event that this mail server is down, you could potentially lose mail! It is recommended to have two or more MX records (and hence mail servers) if you want uninterrupted mail functionality.
	Duplicate MX A records	Good! No two MX records resolve to the same IP address.
	Differing MX A records	Good! You have no different IP's for your MX A records than the DNS server that is authoritative for that hostname.
	MX records have reverse DNS entries	Good! All your MX IP addresses have reverse DNS entries. The reverse entries returned were: 35.127.127.79.in-addr.arpa <--> hosted-by.hostdl.com.asiatech.ir.

رکوردهای A برای اشاره مستقیم به آدرس آی پی است(AAAA هم برای اشاره به آدرس آی پی ورژن ۶ به کار می رود):



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 برای ارائه یک متن دلخواه برای اطلاعات بیشتر است که می تواند شامل متن قابل خواندن برای انسان و یا ماشین باشد و می تواند شامل اطلاعات دلخواهی مانند اطلاعات شبکه یا دیتاسنتر و یا ... باشد.

دامنه سافت ۹۸ فاقد این نوع رکورد است.

پاسخ سوال ۴:

Mail eXchanger (MX) Tests

Status	Test Case	Information
	MX Records	Your Mail eXchanger (MX) records are: 5 asg.aut.ac.ir. [TTL=3600]
	All nameservers have same MX records	Good! All of your nameservers have the same MX records.

با توجه به تصویر فوق آدرس میل سرور asg.aut.ac.ir است.

در همین سایت از طریق منوی پینگ و وارد کردن این آدرس دامنه، آدرس آی پی مشخص شد: 185.211.88.20

پاسخ سوال ۵:

Reverse IP results for farsnews.ir (178.22.78.1, 178.22.78.2, 178.22.78.3, 178.22.78.4)
=====

Domain	Last Resolved Date
farsnews.com	2020-01-24
farsnews.ir	2020-09-14
farsnews.net	2020-01-24
farsnews.org	2020-01-24
fna.ir	2020-09-14

باتوجه به جدول مقابل این وبسایت دارای ای‌پی‌های متفاوتی است و همچنین چندین دامنه بر روی این آی‌پی‌ها قرار دارند.

پاسخ سوال ۶:

مانند هاست‌های اشتراکی که اکنون وجود دارند اگر روی یک ای‌پی بیشتر از یک وبسایت وجود داشته باشد باید در قسمت هدر HTTP مقدار host ارسال شود تا وب سرور بفهمد که فایل‌های کدام وب سایت مورد نظر است. می‌شود گفت بله نوعی مالیتی پلکسینگ SDM است.

پاسخ سوال ۷:

```
>netstat -abo
```

پاسخ سوال ۸:

```
>netstat -anq
```

پاسخ سوال ۹:

چون Payload پروتکل HTTP بعد از header توسط یک اینتر جدا می‌شود که خب با دو تا اینتر ما هدر درخواست را مشخص کردیم.

پاسخ سوال ۱۰:

```
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, 14 Sep 2020 21:45:06 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>
```

پاسخ کد ۳۰۱ به معنای انتقال دائمی این ادرس است که در ادامه در location آمده است.

این درخواست های روی پورت ۸۰ است وقتی که سایت را باز می کنیم:

*Ethernet						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
tcp.port == 80						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.104	185.211.88.131	TCP	66	1186 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.001503	192.168.1.104	185.211.88.131	TCP	66	1187 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4	0.045956	185.211.88.131	192.168.1.104	TCP	62	80 → 1186 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1
5	0.046038	192.168.1.104	185.211.88.131	TCP	54	1186 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
6	0.053271	185.211.88.131	192.168.1.104	TCP	62	80 → 1187 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1
7	0.053303	192.168.1.104	185.211.88.131	TCP	54	1187 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0

و این هم درخواست هایی روی پورت ۴۴۳ است بعد از باز کردن سایت:

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
tcp.port == 443						
No.	Time	Source	Destination	Protocol	Length	Info
25	0.466884	192.168.1.104	185.211.88.131	TCP	66	1189 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
26	0.468525	185.211.88.131	192.168.1.104	TLShv1.2	1454	Application Data
27	0.469278	192.168.1.104	185.211.88.131	TCP	66	1190 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
28	0.470698	192.168.1.104	185.211.88.131	TCP	66	1191 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
29	0.470913	185.211.88.131	192.168.1.104	TCP	1454	443 → 1183 [PSH, ACK] Seq=12284 Ack=1071 Win=34464 Len=1400 [TCP segment of a reassembled PDU]
30	0.470913	185.211.88.131	192.168.1.104	TLShv1.2	355	Application Data, Application Data
31	0.470978	192.168.1.104	185.211.88.131	TCP	54	1183 → 443 [ACK] Seq=1071 Ack=13985 Win=64400 Len=0
32	0.472453	192.168.1.104	185.211.88.131	TCP	66	1192 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
33	0.474037	185.211.88.131	192.168.1.104	TLShv1.2	1454	Application Data
34	0.474092	192.168.1.104	185.211.88.131	TCP	54	1183 → 443 [ACK] Seq=1071 Ack=15385 Win=64400 Len=0
35	0.475407	185.211.88.131	192.168.1.104	TLShv1.2	1454	Application Data, Application Data, Application Data
36	0.479136	185.211.88.131	192.168.1.104	TCP	1454	443 → 1183 [ACK] Seq=16785 Ack=1071 Win=34464 Len=1400 [TCP segment of a reassembled PDU]
37	0.479394	192.168.1.104	185.211.88.131	TCP	54	1183 → 443 [ACK] Seq=1071 Ack=18185 Win=64400 Len=0
38	0.480212	185.211.88.131	192.168.1.104	TLShv1.2	1454	Application Data, Application Data, Application Data
39	0.483151	185.211.88.131	192.168.1.104	TCP	1454	443 → 1183 [ACK] Seq=19585 Ack=1071 Win=34464 Len=1400 [TCP segment of a reassembled PDU]
40	0.483187	192.168.1.104	185.211.88.131	TCP	54	1183 → 443 [ACK] Seq=1071 Ack=20985 Win=64400 Len=0
41	0.485256	185.211.88.131	192.168.1.104	TLShv1.2	1438	Application Data, Application Data, Application Data, Application Data
42	0.485595	192.168.1.104	185.211.88.131	TLShv1.2	1055	Application Data
43	0.504165	192.168.1.104	13.35.43.67	TCP	55	1175 → 443 [ACK] Seq=1 Ack=1 Win=514 Len=1 [TCP segment of a reassembled PDU]
44	0.513803	185.211.88.131	192.168.1.104	TCP	62	443 → 1188 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1
45	0.513198	192.168.1.104	185.211.88.131	TCP	54	1188 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
46	0.514183	192.168.1.104	185.211.88.131	TLShv1.2	571	Client Hello
47	0.516823	185.211.88.131	192.168.1.104	TCP	62	443 → 1190 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1
48	0.516823	185.211.88.131	192.168.1.104	TCP	62	443 → 1189 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1
49	0.516869	192.168.1.104	185.211.88.131	TCP	54	1190 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
50	0.516873	192.168.1.104	185.211.88.131	TCP	54	1189 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
51	0.517585	192.168.1.104	185.211.88.131	TLShv1.2	571	Client Hello
52	0.518164	192.168.1.104	185.211.88.131	TLShv1.2	571	Client Hello
53	0.524983	185.211.88.131	192.168.1.104	TCP	62	443 → 1191 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1
54	0.524407	192.168.1.104	185.211.88.131	TCP	54	1191 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
55	0.524757	185.211.88.131	192.168.1.104	TCP	62	443 → 1192 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1
56	0.524804	192.168.1.104	185.211.88.131	TCP	54	1192 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
57	0.525157	192.168.1.104	185.211.88.131	TLShv1.2	571	Client Hello
58	0.525775	192.168.1.104	185.211.88.131	TLShv1.2	571	Client Hello

بنظر میرسد بعد از چند درخواست همه به پورت ۴۴۳ انتقال داده شدند و روی آن ادامه پیدا کرده اند.

پاسخ سوال ۱۱:

با توجه به تصویر header درخواست ارسال شده و پاسخ دریافتی درخواستی مبنی بر persistent بودن مشاهده نمی کنیم.

پاسخ سوال ۱۲:

بر روی آدرس ای پی ۰.۰.۰.۰ بایند شده است.

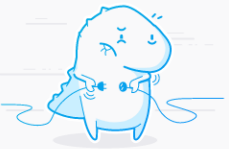
پاسخ سوال ۱۳:

همان طور که پیش تر در سوال ۹ مطرح شد برای جدا کردن body از header است.

اگر این خط جدید از قلم بیافتد باعث می شود که مرورگر نتواند این صفحه را بخواند و نمایش دهد که تصویر رو به رو نتیجه این کار است.

Unable to connect

Firefox can't establish a connection to the server at localhost:4444.

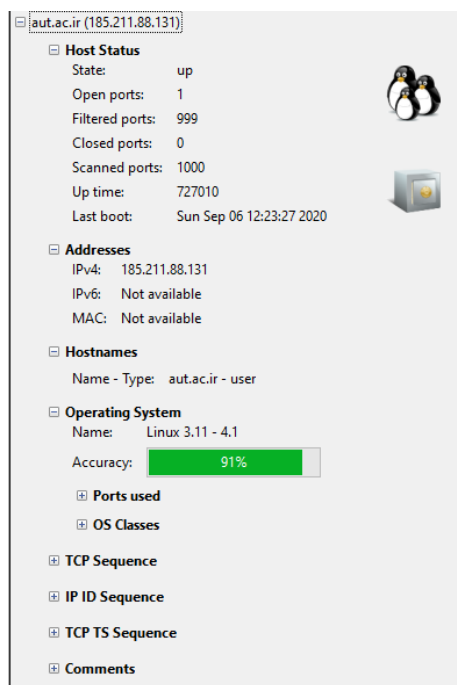


- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Try Again

پاسخ سوال ۱۴:

اطلاعات کامل منجمله سیستم عامل:

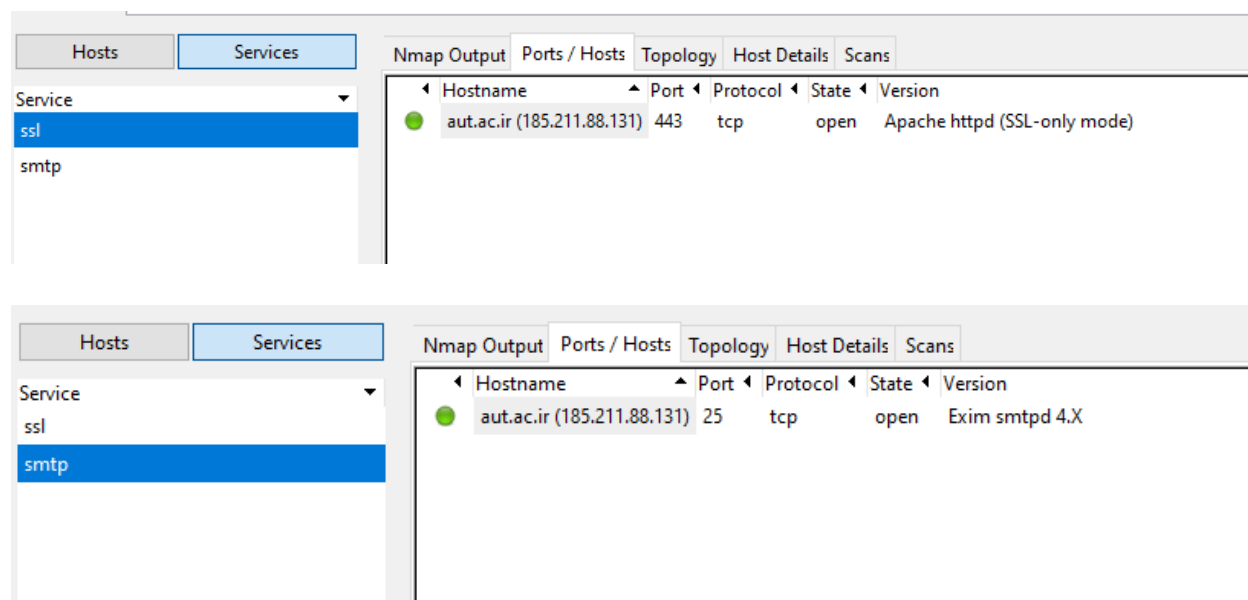


پاسخ سوال ۱۵:

Discovered open port 25/tcp on 185.211.88.131

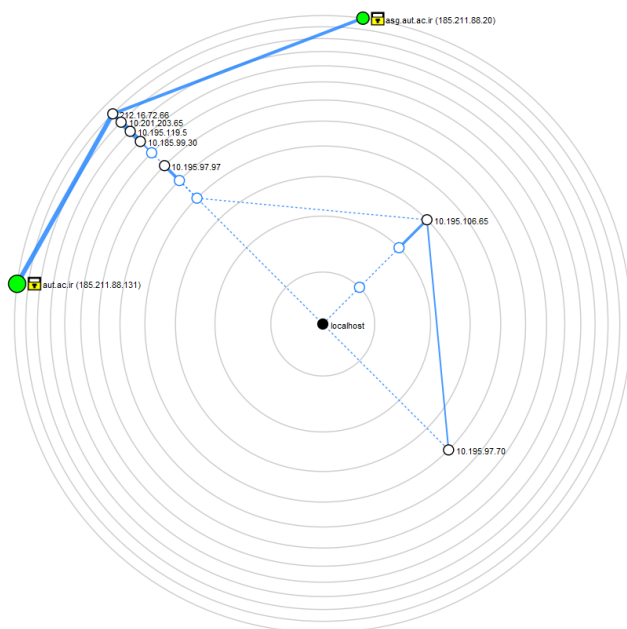
Discovered open port 443/tcp on 185.211.88.131

پاسخ سوال ۱۶:



پاسخ سوال ۱۷:

پس از intense scan شکل زیر اومد که نفهمیدم چیه !!!؟



فقط وقتی no ping گذاشتم خیلی طول کشید.

این ماشین میل سرور دانشگاه است.