



**دانشگاه صنعتی امیر کبیر**  
(پلی تکنیک تهران)

# آزمایشگاه شبکه‌های کامپیوتری

سپهر مقیسه

شماره دانشجویی: ۹۸۳۱۱۰۳

زمستان ۱۴۰۰

سوال ۱-

دامنه به نام علیرضا باقری ثبت شده است. بخشی از اطلاعات این دامنه مانند آدرس و تلفن مالک آن را در زیر می بینیم

. 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

nserver: ir1.hostdl.com

nserver: ir2.hostdl.com

nic-hdl: ab590-irnic

person: alireza bagheri

e-mail: [soft98.ir@gmail.com](mailto:soft98.ir@gmail.com)

address: Shariati-Khiaban Mirzapour-Mehr 3 Gharbi-Pelak 20, Tehran, Tehran, IR

phone: 0912 3549940

source: IRNIC # Filtered

سوال ۲

-همان طور که در بالا دیدیم، آدرس نیم سرورهای آن ir1.hostdl. com و ir2.hostdl. com هستند

سوال ۳

-رکوردهای NS که مشخص کننده نیم سرورهای authoritative هستند برابر

ir1.hostdl.com.

ir2.hostdl.com

است. رکورد MX که به عنوان alias برای آدرس اصلی میل سرور به کار می روند برابر

soft98.ir

است. رکورد TXT این سایت

```
v=spf1 ip4:79.127.127.23 ip4:79.127.127.33 +a +mx +ip4:79.127.127.1/24  
+ip4:185.120.222.1/24 +ip4:79.127.127.1/24 +ip4:185.120.222.1/24  
+ip4:185.49.85.1/24 ~all
```

است. این رکورد به منظور نگهداری متن، برای خواندن ماشین یا حتی انسان، استفاده می شود. رکورد A این سایت نیز ۳۵,۱۲۷,۱۲۷,۷۹ است که آدرس آی پی سرور آن را مشخص می کند.

سوال ۴ -

رکورد MX دانشگاه ir.ac.aut.asg است که آدرس آی پی آن 185.211.88.20 است

سوال ۵ -

سایت cert.ir دو آدرس آی پی دارد. برخی از وب سایت هایی که آدرس آی پی آن ها برابر این مقدار است (روی همان سرورها هوست می شوند) عبارتند از:

141.ir

1773.ir

1zodpaz.ir

24talk.ir

سوال ۶ -

زمانی که مرورگر یک درخواست HTTP ارسال می کند، در هدر آن مقدار Host را برابر نام دامنه مورد نظر قرار می دهد. با این روش که به نوعی Multiplexing است، می توان نام دامنه های زیادی را روی یک سرور میزبانی کرد .

بررسی دامنه دانشگاه در <https://simplifiedns.com/lookup-dg>

برای پیدا کردن آدرس IP دانشگاه، دیتابیس DNS را که به شکل درخت است از ریشه پیمایش می کنیم .ابتدا به یکی از روت سرورها (مثلا j.root-server.net) درخواست می دهیم. با این کار ۴ رکورد NS زیر، که مربوط به دامنه مرتبه بالای ir است، برمی گردد.

-> b.nic.ir (193.189.122.83)

-> ir.cctld.authdns.ripe.net (193.0.9.85)

-> ns5.univie.ac.at (193.171.255.77)

-> a.nic.ir (193.189.123.2)

با درخواست به یکی از آن ها به نیم سرورهای زیر منتقل می شویم.

-> ns3.aut.ac.ir (185.211.88.6)

-> ns2.aut.ac.ir (194.225.34.9)

-> ns1.aut.ac.ir (194.225.33.14)

در نهایت با درخواست دادن به یکی از نیم سرور های بالا به رکورد مورد نظر زیر می رسیم.

-> Answer: A-record for aut.ac.ir = 185.211.88.131

سوال ۷

-با دستور `netstat -bo` میتوان برنامه هایی که پورتی را استفاده می کنند مشاهده کرد. سوییچ `b` - شماره پراسس برنامه ها و `o` - نام آن پراسس را نشان می دهند.

سوال ۸-

برای این کار از همان `netstat` با سوییچ های `a`- برای نشان دادن تمام پورت ها و `n`- برای نشان دادن به صورت عددی استفاده کرد.

سوال ۹-

دلیل نیاز به دو `enter` آن است که با یک `enter` ممکن است بخواهیم اطلاعات هدر دیگری هم در خطوط بعدی بفرستیم. به همین دلیل در پروتکل HTTP هدرها و بدنه پیام ها با یک خط خالی جدا می شوند .

سوال ۱۰-

در پاسخ پیام 301 Moved Permanently داده می شود و آدرس `https://aut.ac.ir:443/` ( نسخه با پروتکل TLS)، آدرس اصلی اعلام می شود.

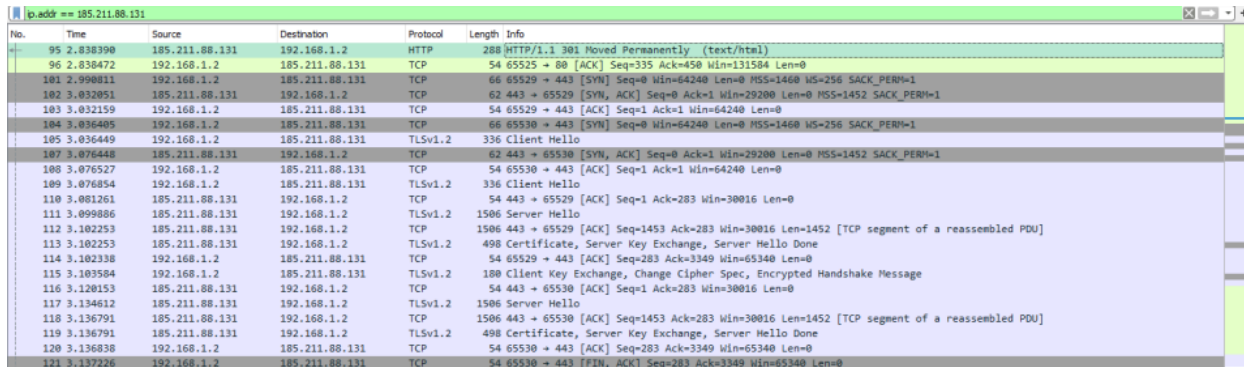
در وایرشارک، مطابق شکل ۱، می بینیم که پس از درخواست به پورت ۸۰، به پورت ۴۴۳ منتقل می شویم

(پیام ها در این حالت قابل فهم نیستند)

سوال ۱۱ -

ارتباطی که با ncat با پورت ۸۰ برقرار کردیم persistent است. این مسئله هم از عبارت-Connection alive: در پاسخ سرور قابل برداشت است و هم از باز ماندن اتصال در برنامه ncat.

سوال ۱۲-



No.	Time	Source	Destination	Protocol	Length	Info
95	2.818390	185.211.88.131	192.168.1.2	HTTP	288	HTTP/1.1 301 Moved Permanently (text/html)
96	2.838472	192.168.1.2	185.211.88.131	TCP	54	65525 → 80 [ACK] Seq=335 Ack=450 Win=131584 Len=0
101	2.990811	192.168.1.2	185.211.88.131	TCP	66	65529 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
102	3.032051	185.211.88.131	192.168.1.2	TCP	62	443 → 65529 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1452 SACK_PERM=1
103	3.032159	192.168.1.2	185.211.88.131	TCP	54	65529 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
104	3.036405	192.168.1.2	185.211.88.131	TCP	66	65530 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
105	3.036449	192.168.1.2	185.211.88.131	TLSv1.2	336	Client Hello
107	3.076448	185.211.88.131	192.168.1.2	TCP	62	443 → 65530 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1452 SACK_PERM=1
108	3.076527	192.168.1.2	185.211.88.131	TCP	54	65530 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
109	3.076854	192.168.1.2	185.211.88.131	TLSv1.2	336	Client Hello
110	3.081261	185.211.88.131	192.168.1.2	TCP	54	443 → 65529 [ACK] Seq=1 Ack=283 Win=30016 Len=0
111	3.099806	185.211.88.131	192.168.1.2	TLSv1.2	1506	Server Hello
112	3.102253	185.211.88.131	192.168.1.2	TCP	1506	443 → 65529 [ACK] Seq=1453 Ack=283 Win=30016 Len=1452 [TCP segment of a reassembled PDU]
113	3.102253	185.211.88.131	192.168.1.2	TLSv1.2	498	Certificate, Server Key Exchange, Server Hello Done
114	3.102338	192.168.1.2	185.211.88.131	TCP	54	65529 → 443 [ACK] Seq=283 Ack=3349 Win=65340 Len=0
115	3.103584	192.168.1.2	185.211.88.131	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
116	3.120153	185.211.88.131	192.168.1.2	TCP	54	443 → 65530 [ACK] Seq=1 Ack=283 Win=30016 Len=0
117	3.134612	185.211.88.131	192.168.1.2	TLSv1.2	1506	Server Hello
118	3.136791	185.211.88.131	192.168.1.2	TCP	1506	443 → 65530 [ACK] Seq=1453 Ack=283 Win=30016 Len=1452 [TCP segment of a reassembled PDU]
119	3.136791	185.211.88.131	192.168.1.2	TLSv1.2	498	Certificate, Server Key Exchange, Server Hello Done
120	3.136838	192.168.1.2	185.211.88.131	TCP	54	65530 → 443 [ACK] Seq=283 Ack=3349 Win=65340 Len=0
121	3.137226	192.168.1.2	185.211.88.131	TCP	54	65530 → 443 [FIN, ACK] Seq=283 Ack=3349 Win=65340 Len=0

شکل ۱: انتقال به پورت ۸۰ و استفاده از HTTPS به جای HTTP

نسخه ۴ این آدرس ۰.۰.۰.۰ و نسخه ۶ آن :: (نشان دهنده ۱۲۸ بیت صفر) است. این آدرس ها به این معنی است که بر روی همه ی آدرس های آی پی رایانه، این پورت bind شده است.

سوال ۱۳-

محتویات فایل index.html تمام پیامی است که ncat ارسال می کند و خود برنامه به آن هدر HTTP اضافه نمی کند. در نتیجه بایستی در این فایل، کل پیام (HTTP از جمله هدر آن) قرار گیرد. در صورتی که این هدر حذف شود، پیام ارسالی توسط مرورگر قابل فهم نخواهد بود و به عنوان مثال در مرورگر فایرفاکس خطای Unable to connect داده می شود

سوال ۱۴-

در قسمت سیستم عامل می بینیم که HP P2000 G3NAS به عنوان دستگاه نوشته شده و نرم افزار روی این دستگاه سرویس دهی می کند.

سوال ۱۵-

در این سرور تنها پورت های ۸۰ و ۴۴۳ باز هستند .

سوال ۱۶ -

روی پورت ۸۰ سرویس HTTP و روی پورت ۴۴۳ سرویس HTTPS ارائه می شود