کار با کاربردهای Web، DNS، سوکت و پویش سرویس‌ها

سوال ۱: نام و اطلاعات فردی که دامنه به اسم ثبت شده‌است چیست؟

remarks: (Domain Holder) alireza bagheri
remarks: (Domain Holder Address) Shariati-Khiaban Mirzapour-Mehr 3 Gharbi-Pelak 20, Tehran, Tehran, IR

سوال ۲: آدرس name server آن چیست؟

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

سوال ۳: رکوردهای NS، A، TXT و MX را مشخص کنید و هر یک از این رکوردها چه چیزی را مشخص می‌کنند؟

NS: مشخص‌کننده آدرس name server ها

```
ir1.hostdl.com. [79.127.127.23] [TTL=86400]
ir2.hostdl.com. [79.127.127.25] [TTL=86400]
```

A: آدرس IP را نگه‌داری می‌کند

TXT: نگه‌داری اطلاعات مانند توضیحات domain

MX: آدرس عامل(های) انتقال پیام

```
0 soft98.ir. [TTL=14400]
```

سوال ۴: در قسمت DNS Report با وارد کردن دامنه‌ی دانشگاه(aut.ac.ir)، mail server دانشگاه را مشخص کنید. آیا آدرس IP آن را می‌توانید مشخص کنید؟

```
5 asg.aut.ac.ir. [TTL=3600]
IP address: 185.211.88.20
```

سوال ۵: چه وب‌سایت‌های دیگری بر روی همین سرور قرار دارند؟ چند مورد از آن‌ها را نام ببرید. (آدرس IP آن‌ها را با آدرس IP سایت farsnews.ir مقایسه کنید)

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

farsnews.com: 178.22.78.1
farsnews.ir: 178.22.78.4
fna.ir: 178.22.78.1
```

سه بخش اول آدرس IP آن‌ها یکسان است.

سوال۶: به نظر شما سرور چگونه وب‌سرور درخواست‌شده را تشخیص می‌دهد؟ آیا این روش نیز نوعی Multiplexing است؟

در پروتکل HTTP 1.1، قسمتی به نام :Host وجود دارد که مشخص می‌کند کدام سایت درخواست‌شده است. می‌توان این روش را Multiplexing در نظر گرفت چرا که با یک IP می‌توان چند وب‌سرور مختلف داشت.

سوال ۷: برای لیست‌کردن برنامه‌هایی که در حال حاضر پورت‌های لایه انتقال را بر روی سیستم بازکرده‌اند، از چه دستور خط فرمانی استفاده می‌شود؟

netstat -b

سوال ۸: دستوری را پیدا کنید که به‌وسیله آن تمام پورت‌های سیستم در هر وضعیت اتصالی همراه با مبدأ و مقصد اتصال به‌صورت عددی لیست شوند.

netstat –n

سوال ۹: دلیل واردکردن دو enter پشت‌سرهم چیست؟

چون دو خط درخواست وجود دارد و هر بار enter زدن یک خط را ارسال می‌کند.

سوال ۱۰: 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.

```
HTTP/1.1 301 Moved Permanently
Date: Thu, 12 Nov 2020 10:08:14 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>
```

صفحه‌ی اصلی در https://aut.ac.ir:443 قرار دارد.

سوال ۱۱: آیا این ارتباط persistent است؟

بله، چون Connection از نوع keep-alive است.

سوال ۱۲: این پورت بر روی کدام آدرس IP، bind شده‌است؟

[ncat.exe]
TCP **0.0.0.0**:49664 **0.0.0.0**:0 LISTENING
IP address: 0.0.0.0

سوال ۱۳: دقت کنید یک خط خالی بین HTTP و <html> باید وجود داشته‌باشد. 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 خط خالی معادل enter است و پاسخ سرور (HTTP/1.1 200 ok) را ارسال می‌کند. در صورت عدم وجود این خط، پاسخ سرور برای کاربر ارسال نشده و چیزی در سمت کاربر نمایش داده نمی‌شود.

سوال ۱۴: سیستم‌عامل این وب‌سایت چیست؟

FreeBSD 6.2

سوال ۱۵: چه پورت‌هایی روی این سرور باز است؟

Discovered open port **21/tcp** on 185.211.88.131
Discovered open port **1723/tcp** on 185.211.88.131
Discovered open port **25/tcp** on 185.211.88.131
Discovered open port **443/tcp** on 185.211.88.131

سوال ۱۶: سرویس‌هایی که از طریق این پورت‌ها ارائه می‌شود چیست؟

21: FTP
1723: TCP
25: SMTP (Simple Mail Transfer Protocol)
443: HTTPS

سوال ۱۷: این بار آدرس asg.aut.ac.ir را پویش کنید. با انتخاب پروفایل Intense scan، نتیجه چیست؟ پروفایل No ping، Intense scan 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؟

اسکن اول (Intense scan) به غیر از آدرس IP (185.211.88.20) و پورت‌های باز، خروجی خاصی ندارد.
اسکن دوم (Intense scan, No ping) به غیر از آدرس IP، خروجی خاصی ندارد.

این ماشین mail server دانشگاه است.