گزارش دستورکار چهارم آزمایشگاه درس شبکه‌های کامپیوتری

نگار موقتیان، ۹۸۳۱۰۶۲

۱. نام و اطلاعات فردی که دامنه به اسم آن ثبت شده‌است چیست؟

مطابق اطلاعات بخش زیر این دامنه به نام علیرضا باقری ثبت شده و ایمیل مربوط به آن soft98.ir@gmail.com می‌باشد.

```
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
holder-c: ab590-irnic
admin-c: ab590-irnic
tech-c: ab590-irnic
bill-c: fa482-irnic
nserver: ir1.hostdl.com
nserver: ir2.hostdl.com
source: IRNIC # Filtered

nic-hdl: ab590-irnic
person: alireza bagheri
e-mail: soft98.ir@gmail.com
source: IRNIC # Filtered

nic-hdl: fa482-irnic
org: Faraso Samaneh Pasargad Co.
e-mail: irnic@faraso.org
source: IRNIC # Filtered
```

۲. آدرس name server آن چیست؟

طبق بخش‌های مشخص شده در بالا آدرس name server این وبسایت ir1.hostdl.com و ir2.hostdl.com می‌باشد.

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

رکورد NS:

رکوردهایی از این نوع برای مشخص کردن نام دامنهٔ name server ای که به یک دامنهٔ خاص سرویس ارائه می‌دهد استفاده می‌شود. این رکورد hostname هر name server را به main domain آن مربوط می‌کند.

ℹ	NS records listed at parent servers	Nameserver records returned by the parent servers are: ir1.hostdl.com. [NO GLUE] [TTL=1440] ir2.hostdl.com. [NO GLUE] [TTL=1440] This information was kindly provided by b.nic.ir.

رکورد A:

در این نوع از رکوردها هر hostname به یک آدرس IP نگاشت می‌شود.

ℹ	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]

رکورد TXT:

رکوردهایی هستند که در قالب سوابق متنی اطلاعاتی را دربارهٔ سرورها نگهداری می‌کنند. با توجه به اینکه رکورد TXT مربوطه در قسمت DNS Report وبسایت معرفی شده نمایش داده نمی‌شد، اطلاعات زیر از بخش DNS Record Lookup سایت بدست آمده‌است که شامل اطلاعات مربوط به رکورد TXT و دیگر رکوردها می‌باشد.

Name	TTL	Class	Type	Priority	Data
soft98.ir.	21600	IN	SOA		ir1.hostdl.com. hostdl.gmail.com. 2021092600 600 7200 6000 86400
soft98.ir.	21600	IN	NS		ir1.hostdl.com.
soft98.ir.	21600	IN	NS		ir2.hostdl.com.
soft98.ir.	14400	IN	A		79.127.127.35
soft98.ir.	14400	IN	TXT		"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"
soft98.ir.	14270	IN	MX	0	soft98.ir.

رکورد MX:

برای یک رکورد از این نوع Value نام کانونی سرور ایمیلی است که یک نام alias با نام Name دارد. این نوع از رکوردها به کمپانی‌ای که از آن‌ها استفاده می‌کند اجازه می‌دهند تا یک نام alias مشترک برای سرورهای ایمیل و دیگر سرورهای خود داشته باشند (برای مثال aut.ac.ir هم نام دامنهٔ ایمیل‌ها را مشخص می‌کند و هم نام دیگر سرورهای دانشگاه).

ℹ	MX Records	Your Mail eXchanger (MX) records are: 0 soft98.ir. [TTL=14400]

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

با توجه به توضیحات قسمت قبل برای بدست آوردن اطلاعات مربوط به mail server ها باید به رکوردهای MX مراجعه کنیم. با توجه به شکل زیر آدرس mail server دانشگاه asg.aut.ac.ir می‌باشد.

ℹ	MX Records	Your Mail eXchanger (MX) records are: 5 asg.aut.ac.ir. [TTL=3600]

به علاوه همانطور که در قسمت زیر مشاهده می‌شود IP مربوط به این mail server برابر است با 185.211.88.20.

✔	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.

۵. چه وبسایت‌های دیگری بر روی همین سرور قرار دارند؟ چند مورد از آن‌ها را نام ببرید.

وبسایت‌های مشخص شده در شکل زیر همگی بر روی یک سرور مشترک با cert.ir قرار دارند. نمونه‌ای از این وبسایت‌ها عبارت است از:

7peykar.ir, abrmarketing.net, agoracomplex.com, alotasvirgar.ir, brifenews.ir, carbill.ir, …

Domain	Last Resolved Date
7peykar.ir	2022-05-17
92762.ir	2022-05-17
abrmarketing.net	2022-05-17
aghlovahy.com	2022-05-17
agoracomplex.com	2022-04-30
alotasvirgar.ir	2022-05-17
behnamnasrollahi.ir	2022-05-17
bemanbespar.ir	2022-05-11
bimehnama.com	2022-04-30
binazirshop.com	2022-04-30
bizilyapp.com	2022-05-17
bodyspinners.com	2022-04-30
bornosmode.com	2022-04-30
brifenews.ir	2022-05-11
carbill.ir	2022-05-11
cert.ir	2022-05-18
chang.ir	2022-03-18
chargoon.com	2022-04-30

۶. به نظر شما سرور چگونه وب سرور درخواست شده را تشخیص می‌دهد؟ آیا این روش نیز نوعی multiplexing است؟

بله؛ یکی از خدمات مهمی که پروتکل‌های لایهٔ انتقال (TCP و UDP) ارائه می‌دهند این است که انتقال داده میان دو سیستم انتهایی که لایهٔ IP ارائه می‌کند را به انتقال داده میان دو اپلیکشن (یا پردازه) که بر روی سیستم‌های انتهایی اجرا می‌شوند گسترش دهد؛ به این کار multiplexing و demultiplexing لایهٔ انتقال گفته می‌شود.

زمانی که می‌خواهیم به یک وب سرور درخواست دهیم باید IP و شماره پورت آن را مشخص کنیم. آدرس IP مشخص می‌کند که می‌خواهیم به چه سیستمی در شبکه پیغام را برسانیم (کدام سرور). شماره پورت در هدر بسته‌ها قرار خواهد گرفت و در حقیقت مشخص می‌کند که درخواستی که به سرور می‌دهیم باید به کدام وب سرور تحویل داده شود.

۷. **برای لیست کردن برنامه‌هایی که در حال حاضر پورت‌های لایهٔ انتقال را بر روی سیستم باز کرده‌اند، از چه دستور خط فرمانی استفاده می‌شود؟**

با استفاده از دستور netstat و آرگومان o– مطابق شکل زیر می‌توان لیستی از پورت‌هایی که در حال حاضر فعال هستند، وضعیت آن‌ها و pid پردازه‌ای که آن‌ها را در اختیار دارد را مشاهده کرد.

```
C:\Users\win10>netstat -o

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    192.168.1.33:10658     20.199.120.182:https   ESTABLISHED     4184
  TCP    192.168.1.33:10837     wq-in-f188:5228        ESTABLISHED     1060
  TCP    192.168.1.33:10840     ej-in-f189:https       ESTABLISHED     1060
  TCP    192.168.1.33:10879     mct01s20-in-f5:https   ESTABLISHED     1060
  TCP    192.168.1.33:10881     odinvzc:https          TIME_WAIT       0
  TCP    192.168.1.33:10883     www:https              TIME_WAIT       0
  TCP    192.168.1.33:10884     www:https              TIME_WAIT       0
  TCP    192.168.1.33:10885     www:https              TIME_WAIT       0
  TCP    192.168.1.33:10886     www:https              TIME_WAIT       0
  TCP    192.168.1.33:10887     a:https                ESTABLISHED     6692
  TCP    192.168.1.33:10888     teams:https            ESTABLISHED     6692
  TCP    192.168.1.33:10889     l:https                ESTABLISHED     6692
  TCP    192.168.1.33:10890     fp:https               ESTABLISHED     6692
  TCP    192.168.1.33:10892     www:https              ESTABLISHED     1060
  TCP    192.168.1.33:10893     www:https              ESTABLISHED     1060
  TCP    192.168.1.33:10894     www:https              ESTABLISHED     6692
  TCP    192.168.1.33:10896     ajax:https             ESTABLISHED     1060
  TCP    192.168.1.33:10897     p:https                CLOSE_WAIT      1060
  TCP    192.168.1.33:10902     s7:https               ESTABLISHED     1060
  TCP    192.168.1.33:10903     z:https                SYN_SENT        1060
  TCP    192.168.1.33:10904     z:https                SYN_SENT        1060
  TCP    192.168.1.33:10905     z:https                SYN_SENT        1060
  TCP    192.168.1.33:10906     z:https                SYN_SENT        1060
  TCP    192.168.1.33:10907     ipapi:https            ESTABLISHED     1060
```

۸. **دستوری را پیدا کنید که به وسیلهٔ آن تمام پورت‌های سیستم در هر وضعیت اتصالی همراه با مبدا و مقصد اتصال به صورت عددی لیست شوند.**

برای این کار از دستور netstat استفاده کرده و به منظور لیست کردن تمام پورت‌ها (و نه فقط پورت‌های فعال) از آرگومان a– و برای لیست کردن مبدا و مقصد اتصال به صورت عددی از آرگومان n– استفاده می‌کنیم. خروجی این دستور مانند زیر می‌باشد.

```
C:\Users\win10>netstat -a -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:912            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    0.0.0.0:49664          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    0.0.0.0:49670          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1001         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:8307         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:57611        0.0.0.0:0              LISTENING
  TCP    192.168.1.36:139       0.0.0.0:0              LISTENING
  TCP    192.168.1.36:27041     20.199.120.182:443     ESTABLISHED
  TCP    192.168.1.36:27199     23.61.80.8:443         ESTABLISHED
  TCP    192.168.1.36:27258     13.107.21.200:443      ESTABLISHED
  TCP    192.168.1.36:27264     13.107.246.254:443     ESTABLISHED
  TCP    192.168.1.36:27265     13.107.42.254:443      ESTABLISHED
```

۹. دلیل وارد کردن دو enter پشت سر هم چیست؟

در فرمت درخواست‌های HTTP پس از آن‌که header ها به پایان رسیدند لازم است که یک خط خالی گذاشته شده و پس از آن بدنهٔ پیام آورده شود. در مورد درخواست گفته شده در این سوال، بدنهٔ درخواست مورد نظر خالی است، لذا enter اول برای جداسازی سرآیند پیام از بدنهٔ آن و enter دوم برای ارسال درخواست بوده‌است.

۱۰. پیامی که در پاسخ تقاضای شما دهده می‌شود چیست؟ صفحهٔ اصلی در کجا قرار دارد؟

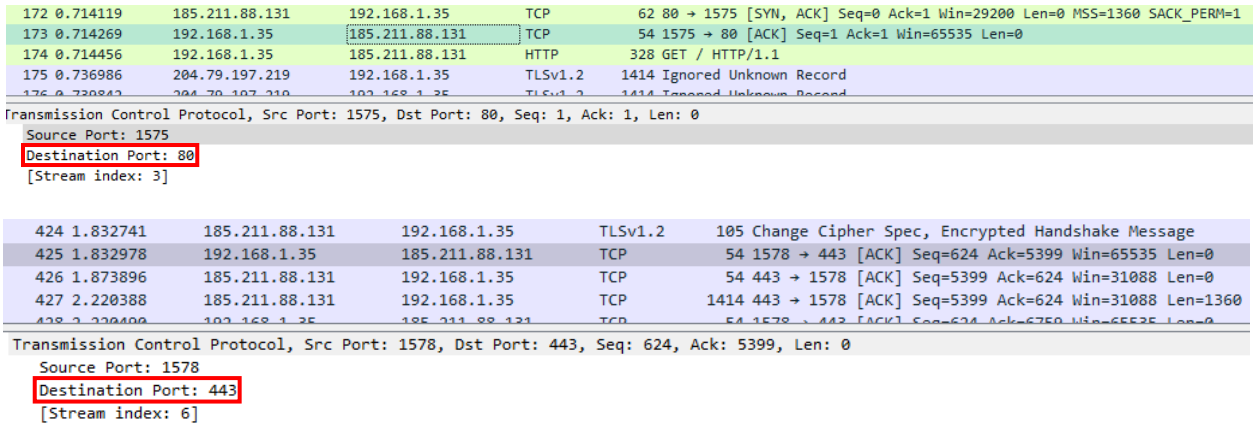
Status code پیغام داده شده 301 بوده و به این معناست که شیءای که درخواست آن داده شده‌است به طور دائمی به آدرس دیگری منتقل شده‌است. با توجه به پاسخ داده شده آدرس جدید صفحهٔ اصلی عبارت است از:
https://aut.ac.ir:443/
به عبارتی وب سرور اصلی بر روی پورت 443 (و نه 80) اجرا می‌شود.

```
C:\Users\win10>ncat -C aut.ac.ir 80
GET / HTTP/1.1
Host: aut.ac.ir

HTTP/1.1 301 Moved Permanently
Date: Thu, 19 May 2022 04:36:46 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>
```

اگر همین درخواست را توسط مرورگر داده و بسته‌های انتقال یافته را توسط Wireshark شنود کنیم متوجه می‌شویم که در ابتدا درخواستی بر روی پورت ۸۰ داده شده و پس از آن باقی بسته‌ها از طریق پورت ۴۴۳ انتقال یافته‌اند.



۱۱. آیا این ارتباط persistant است؟

بله؛ زیرا پس از این که پیغام HTTP بالا را فرستادیم امکان ارسال پیغام‌های بعدی نیز از طریق همان ارتباط ایجاد شده وجود دارد.

۱۲. این پورت بر کدام آدرس IP، bind شده‌است؟

مطابق شکل زیر این پورت (16000) به آدرس 0.0.0.0 بایند شده‌است. به طور کلی این آدرس به host های unknown تخصیص داده می‌شود.

```
C:\Users\win10>ncat -v -l -p 16000 -e c:\Windows\System32\cmd.exe
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::16000
Ncat: Listening on 0.0.0.0:16000
```

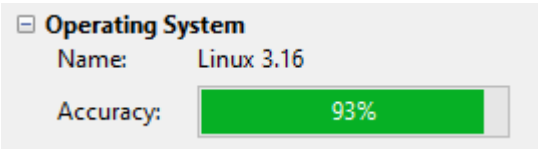
۱۳. دقت کنید یک خط خالی بین HTTP و <html> باید وجود داشته باشد. به نظر شما دلیل وجود خط اول در این فایل چیست؟

در ابتدای این خط پروتکل استفاده شده برای انتقال پیام (HTTP) و ورژن آن (1.1) را مشخص کرده‌ایم.

در ادامه از آن‌جایی که در این قسمت در حال فرستادن یک HTTP Response هستیم، باید به گیرندهٔ پیغام یک status code و status message نیز اعلام کنیم. این کد و message مشخص می‌کند نتیجهٔ درخواست کلاینت چه بوده‌است. برای مثال در این پیغام کد را برابر با 200 و message آن را برابر با OK قرار داده‌ایم، به این معنا که در دریافت و پردازش پیغام مشکلی وجود نداشته‌است.

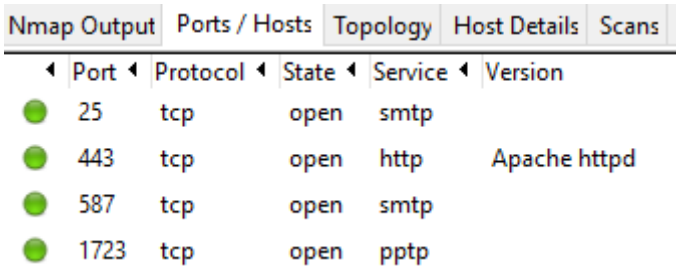
۱۴. سیستم عامل این وب‌سایت چیست؟

با توجه به قسمت زیر از نتایج اسکن وب‌سایت، با دقت 93% سیستم عامل استفاده شده Linux 3.16 می‌باشد.



۱۵. چه پورت‌هایی بر روی این سرور باز است؟

با توجه به قسمت زیر از نتایج اسکن وب‌سایت، پورت‌های ۲۵، ۴۴۳، ۵۸۷ و ۱۷۲۳ بر روی این سرور باز هستند.



۱۶. سرویس‌هایی که از طریق این پورت‌ها ارائه می‌شود چیست؟

با توجه به شکل قسمت قبل سرویس SMTP بر روی پورت ۲۵ و ۵۸۷، سرویس HTTP بر روی پورت ۴۴۳ و سرویس PPTP بر روی پورت ۱۷۲۳ ارائه می‌گردد.