علی نظری – ۹۶۳۱۰۷۵

آزمایشگاه شبکه – سه‌شنبه‌ها ساعت ۱۶:۳۰

آزمایش مربوط به ۱۸ شهریور ۹۹

سوال ۱:

صاحب این دامنه علیرضا باقری است که اطلاعات بیشتر ایشان به شرح زیر است:

person: alireza bagheri

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

phone: 0912 3549940

سوال ۲:

این دامنه دارای دو name server به آدرس‌های ir1.hostdl.com و ir2.hostdl.com است.

سوال ۳:

رکورد **NS**: این رکورد DNS سرورهای متصل به این دامنه را مشخص می‌کند.

ir1.hostdl.com. [NO GLUE] [TTL=1440]

ir2.hostdl.com. [NO GLUE] [TTL=1440]

رکورد **A**: این رکورد نگاشتی بین دامنه و IP است.

soft98.ir. A 79.127.127.35 [TTL=14400]

رکورد **TXT**: این رکورد شامل اطلاعاتی متنی درباره منابع خارجی این دامنه هستند.

v=spf1 +a +mx +ip4:79.127.127.23 +ip4:79.127.127.33 +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

رکورد **MX**: این رکورد میل‌سروری که به دامنه متصل است را مشخص می‌کند.

soft98.ir. [TTL=14400]

سوال ۴:

میل‌سرور دانشگاه دارای آدرس asg.aut.ac.ir است و آیپی متصل به آن نیز برابر 185.211.88.20 است.

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	2020-09-10
farsnews.net	2020-01-24
farsnews.org	2020-01-24
fna.ir	2020-09-10

سوال ۶:

از طریق هدر host در پروتکل http تشخیص داده می‌شود که کدام وب سرور درخواست شده است.

سوال ۷:

با استفاده از دستور netstat -b برنامه‌هایی که پورتی را بازکرده‌اند، لیست می‌شوند.

سوال ۸:

با استفاده از دستور netstat -a همه پورت‌ها با آدرس و وضعیتشان مشخص می‌شوند.

سوال ۹:

در انتهای پیام HTTP یک خط خالی وجود دارد تا بتوان پایان پیام را تشخیص داد.

سوال ۱۰:

با کد ۳۰۱ ما به آدرس https سایت دانشگاه بر روی پورت ۴۴۳ redirect شدیم.

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

HTTP/1.1 301 Moved Permanently
Date: Thu, 10 Sep 2020 16:45:43 GMT
Server: Apache
Location: https://aut.ac.ir:443/
Content-Length: 230
Content-Type: text/html; charset=iso-8859-1
Connection: keep-alive

<!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>
```

همان درخواست را ارسال می کنیم:

```
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
  Host: aut.ac.ir\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9,fa;q=0.8\r\n
```

همان پاسخ را می‌گیریم:

```
Hypertext Transfer Protocol
  HTTP/1.1 301 Moved Permanently\r\n
  Date: Thu, 10 Sep 2020 16:31:40 GMT\r\n
  Server: Apache\r\n
  Location: https://aut.ac.ir:443/\r\n
  Content-Length: 230\r\n
  Content-Type: text/html; charset=iso-8859-1\r\n
  Connection: keep-alive\r\n
  \r\n
```

سوال ۱۱:

بله همان‌طور که در عکس‌های بالا مشاهده می‌کنیم، ارتباط از نوع keep-alive بوده و persist محسوب می‌شود.

سوال ۱۲:

```
  TCP    0.0.0.0:16000          0.0.0.0:0              LISTENING
[ncat.exe]
```

که این آدرس 0.0.0.0 یعنی تمام آدرس ip های لوکال ما.

سوال ۱۳:

لازم است در پایان هدرهای HTTP یک خط خالی وجود داشته باشد تا پایان آن را اعلام کند.

سوال ۱۴:

cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:2.4.20

سوال ۱۵:

پورت‌های ۸۰ و ۴۴۳ باز هستند.

سوال ۱۶:

از طریق پورت ۸۰ سرویس http و از طریق پورت ۴۴۳ نیز سرویس tcpwrapped نوشته شده که ارائه می‌شود ولی خب قراره ssl ارائه بشه.

سوال ۱۷:

این آدرس میل‌سرور دانشگاه است.
