به نام خدا

راه‌اندازی سرویس Web و FTP

نام و نام‌خانوادگی: روژینا کاشفی

شماره دانشجویی : ۹۸۳۱۱۱۸

• تنظیمات سرور web

سوال ۱) ادرس پورت مبدا مقصد چیست؟ روند برقراری ارتباط در پروتکل HTTP چگونه است؟ وب سرور چگونه ادرس سایت درخواستی شما را تشخیص می‌دهد؟

ادرس پورت مبدا و مقصد در شکل مشخص شده است.

567	20.971257	127.0.0.1	127.0.0.1	HTTP	490	GET / HTTP/1.1
568	20.971329	127.0.0.1	127.0.0.1	TCP	44	80 → 4184 [ACK] Seq=1 A
569	20.974360	127.0.0.1	127.0.0.1	HTTP	249	HTTP/1.1 304 Not Modifi
570	20.974447	127.0.0.1	127.0.0.1	TCP	44	4184 → 80 [ACK] Seq=447
639	25.974713	127.0.0.1	127.0.0.1	TCP	44	80 → 4184 [FIN, ACK] Se
640	25.974825	127.0.0.1	127.0.0.1	TCP	44	4184 → 80 [ACK] Seq=447
641	25.974898	127.0.0.1	127.0.0.1	TCP	44	4184 → 80 [FIN, ACK] Se
642	25.974921	127.0.0.1	127.0.0.1	TCP	44	80 → 4184 [ACK] Seq=207

```
Transmission Control Protocol, Src Port: 4184, Dst Port: 80, Seq: 1, Ack: 1, Len: 446
```

برقراری ارتباط از طریق سوکت TCP می‌باشد و روند در خواست به این شکل است که ایتدا یک tcp handshake اتفاق می‌افتد و یک درخواست از سمت hostبه destination (sync) فرستاده می‌شود و سپس dest پاسخ ack می‌دهد که بدان معناست که connectionبرقرار شده است و سپس درخواست http‌زده می‌شود وب سرور ادرس سایت را که داخل etc/hosts دخیره شده که در آن لوکال هاست را به www.aut۲.ac.ir مپ کرده بودیم تشخیص می دهد و همچنین اگر در قایل ذکر شده ادرس مورد نظر پیدا نشود آنگاه سلسه مراتب query زدن DNS طی می‌شود.

با استفاده از دستور HOST ادرس سایت درخواستی مشخص می‌شود.

```
Host: www.aut2.ac.ir
```

سوال ۲) مقدار بخش connection چیست؟ درخواست HTTP از نوع get بوده یا post؟ مقدار useragent چیست؟ به نظر شما این مقدار بیانگر چه چیزی است؟

مقدار connectionبرابر با keep-aliveاست و این بدان معناست که سوکت TCPبعد از ارسال جواب در یافتن آن این ارتباط قطع نمی‌شود و برای درخواست های آینده باز می‌ماند و persistent است.

```
Connection: keep-alive
```

از نوع get

```
GET / HTTP/1.1
```

Useragent نشان‌گر استفاده ما از نوع مرورگر و سیستم‌عامل ما است.

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
```

به نام خدا

سوال ۳) در پنجره باز شده، اولین بسته را انتخاب کنید. سپس مقدار FLAGS در پروتکل TCP را مشاهده کنید. چه مقادیری برای این بسته تنظیم شده است؟

در اولین بسته انتخابی SYN=۱ است.

```
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  ⌄ Flags: 0x002 (SYN)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    > .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
```

سوال ۴) یک سایت دیگر با نام دلخواه ایجاد کنید و بسته‌های مربوط به آن را شنود کنید. چه تفاوتی بین این دو سایت وجود دارد؟

این بار از ادرس aut۳.com استفاده کردیم. همانطوری که مشاهده می‌کنید:

۱. آدرس پورت مبدا متفاوت است تا بتوان بسته‌های مربوط به آن‌ها را از هم جدا کرد.
۲. طول بسته‌های آنها نیز متفاوت است.
۳. پارامترهای acknowledge number وsequence number هم متفاوت است .
۴. مقدار پورت مقصد یکسان است.
۵. زمان ارسال درخواست متفاوت است.
۶. اسم هاست‌ها متفاوت است.

```
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 13884, Dst Port: 80, Seq: 1, Ack: 1, Len: 333
⌄ Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: www.aut3.com\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://www.aut3.com/]
    [HTTP request 1/2]
    [Response in frame: 6354]
```

به نام خدا

سوال ۵) مشخص کنید که گواهی را چه کسی برای چه کسی صادر کرده، مدت اعتبار گواهی چقدر است، کلید عمومی صادرکننده چیست و امضای دیجیتال انجام شده با چه الگوریتم‌هایی انجام شده است.

گواهی توسط localhost برای localhost صادر شده است. مدت اعتبار آن ۱۰ سال است، اما تاریخ اعتبار آن گذشته است.
صادر کننده کلید عمومی RSA است.

Public key	RSA (1024 Bits)
Public key parameters	05 00
Thumbprint	b0238c547a905bfa119c4...

امضای دیجیتال با الگوریتم SHA۱RSA و الگوریتم هش SHA۱ انجام شده است.

Field	Value
Version	V1
Serial number	00b5c752c98781b503
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	localhost
Valid from	Wednesday, November 1...
Valid to	Saturday, November 9, 2...
Subject	localhost

سوال ۶) آیا می‌توانید متن ارتباط را بخوانید؟ چرا؟

خیر. از آنجایی که از پروتکل tls استفاده شده است، متن این ارتباط قابل خواندن نیست. پروتکل tls وظیفه‌ی رمزگذاری (encryption)ارتباط بین سرور و کلاینت را به عهده دارد .

```
TLSv1.3 Record Layer: Application Data Protocol: http-over-tls
    Opaque Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 38
    Encrypted Application Data: c57fd94a52940ca01a7afafd6c305f256adf50ce15257a16d4e61e17245813c15029a5e0…
    [Application Data Protocol: http-over-tls]
```

سوال ۷) گواهی آن سایت با سایت شما چه تفاوت‌هایی دارد؟

1 . تفاوت ان که گواهی سایت گوگل معتبر است و از طرف GTS CA ۱C۳ صادر شده است.
2 . الگوریتم رمزنگاری به‌کار رفته نیز ECC صادر شده است.
3 . همچنین مدت اعتبار گواهی برخلاف سایت ما منقضی نشده است .

Issued to: www.google.com

Issued by: GTS CA 1C3

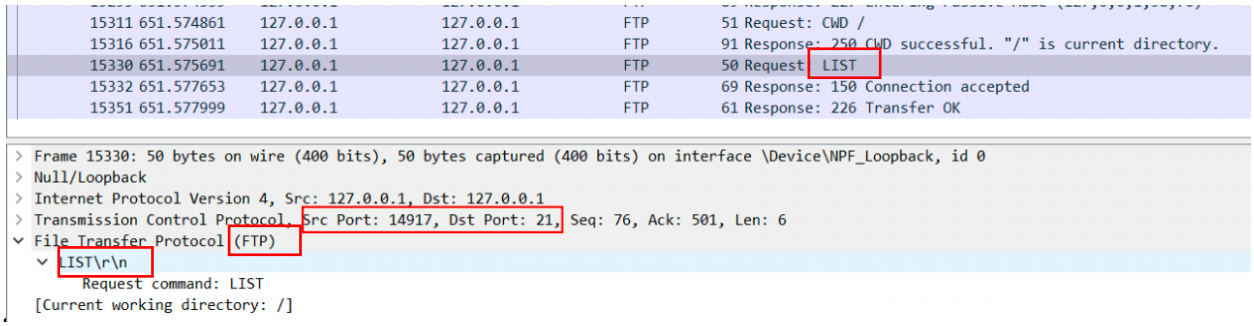
Valid from 4/11/2022 **to** 7/4/2022

به نام خدا

• تنظیمات سرور FTP

سوال ۸) مشخص کنید چه دستوری برای لیست کردن فایل‌های دایرکتوری استفاده شده است. مشخص کنید چه نام کاربری برای دسترسی به سایت استفاده شده است. پروتکل لایه Transport استفاده شده برای این بسته‌ها چیست؟ آدرس پورت مبدا و مقصد را مشخص کنید.

از دستور LIST برای گرفتن لیست فایل‌ها استفاده می‌شود .نام کاربری استفاده شده در اینجا test است (همانطوری که در تنظیمات FileZilla ایجادش کردیم و با ان لاگین کردیم)



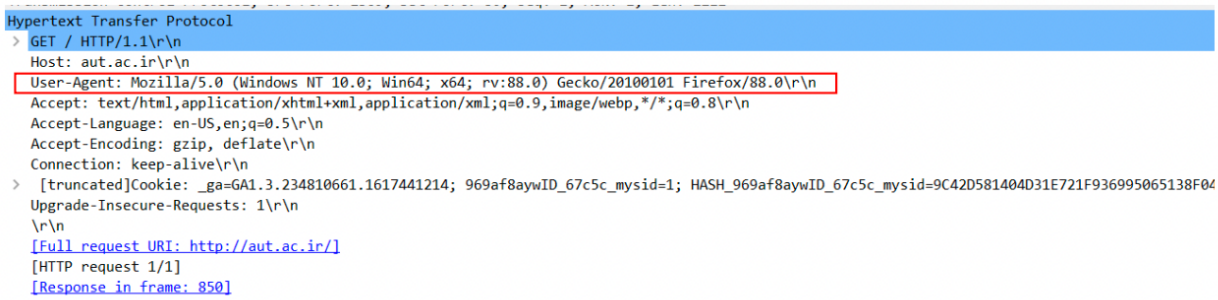
سوال ۹) سعی کنید دوباره مرورگر را باز کنید. آیا می‌توانید به سایت وارد شوید؟

طبق گفته مدرسین حذف شده.

• پروتکل HTTP

۱) شنود انجام و متوقف شد.

۲)



۳)

Connection = keep alive

درخواست از نوع get است.

User agent نیز در شکل مشخص شده است و بیانگر این موضوع است که درخواست از طریق firefox ارسال شده و نشان‌دهنده اطلاعات مبدا است.

به نام خدا

۴)

```
Transmission Control Protocol, Src Port: 1369, Dst Port: 80, Seq: 1, Ack: 1, Len: 1211
    Source Port: 1369
    Destination Port: 80
    [Stream index: 64]
    [TCP Segment Len: 1211]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1380490331
    [Next Sequence Number: 1212    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2664919712
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 1... = Push: Set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·····AP···]
    Window: 17520
    [Calculated window size: 17520]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0xafee [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
```