



دانشگاه صنعتی امیر کبیر
(پلی تکنیک تهران)

آزمایشگاه شبکه‌های کامپیوتری

سپهر مقیسه

شماره دانشجویی: ۹۸۳۱۱۰۳

زمستان ۱۴۰۰

سوال ۱ -

مطابق شکل ۱، پورت مبدا (پورت سوکت مرورگر) ۵۳۸۲۱ و پورت مقصد (پورت وب سرور) ۸۰ است. در پروتکل HTTP، که از پروتکل TCP استفاده می کند، پس از برقراری و اتصال TCP و انجام way-3 handshake، یک درخواست GET برای آدرس مورد نظر توسط مرورگر ارسال می شود. پس از آن پاسخ این درخواست توسط وب سرور داده می شود

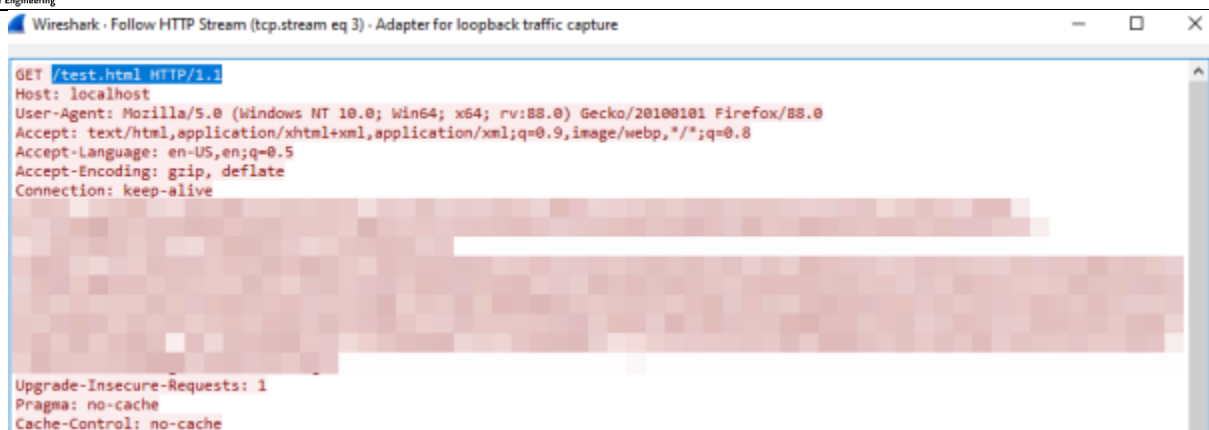
No.	Time	Source	Destination	Protocol	Length	Info
96	1.209071	127.0.0.1	127.0.0.1	TCP	56	53821 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
97	1.209975	127.0.0.1	127.0.0.1	TCP	56	80 → 53821 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
98	1.210037	127.0.0.1	127.0.0.1	TCP	44	53821 → 80 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
103	1.211026	127.0.0.1	127.0.0.1	HTTP	1391	GET /test.html HTTP/1.1
104	1.211276	127.0.0.1	127.0.0.1	TCP	44	80 → 53821 [ACK] Seq=1 Ack=1348 Win=2619648 Len=0
105	1.211642	127.0.0.1	127.0.0.1	HTTP	465	HTTP/1.1 200 OK (text/html)
106	1.211694	127.0.0.1	127.0.0.1	TCP	44	53821 → 80 [ACK] Seq=1348 Ack=422 Win=2619136 Len=0
151	1.265108	127.0.0.1	127.0.0.1	HTTP	1348	GET /favicon.ico HTTP/1.1
152	1.265237	127.0.0.1	127.0.0.1	TCP	44	80 → 53821 [ACK] Seq=422 Ack=2644 Win=2618368 Len=0
153	1.265652	127.0.0.1	127.0.0.1	HTTP	549	HTTP/1.1 404 Not Found (text/html)
154	1.265679	127.0.0.1	127.0.0.1	TCP	44	53821 → 80 [ACK] Seq=2644 Ack=927 Win=2618624 Len=0

>	Frame 103: 1391 bytes on wire (11128 bits), 1391 bytes captured (11128 bits) on interface \Device\NPF_{...} id 0
>	Null/Loopback
>	Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
>	Transmission Control Protocol, Src Port: 53821, Dst Port: 80, Seq: 1, Ack: 1, Len: 1347
>	Hypertext Transfer Protocol
>	GET /test.html HTTP/1.1\r\n
>	Host: localhost\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

شکل ۱: بسته های درخواست و پاسخ HTTP برای آدرس `http://localhost/test.html` در وایرشارک

در شکل ۲، محتوای پیام ارسال شده توسط مرورگر را می بینیم. وب سرور با توجه به خطوط `GET /test.html HTTP/1.1` و `Host:localhost`

که دو خط ابتدایی پیام ارسالی هستند، متوجه هوست و آدرس مورد نظر می شود و با توجه به آن آبجکت مربوطه را برمی گرداند.



شکل ۲ header های HTTP ارسال شده توسط مرورگر

سوال ۲- همان طور که در شکل ۲ می بینیم، مقدار بخش Connection برابر keep-alive است که به معنی استفاده از حالت persistent است. همچنین درخواست از نوع GET است.

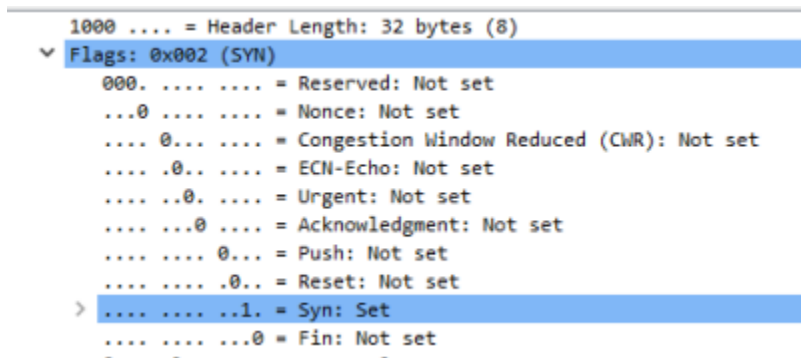
مقدار user-agent برابر

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

است. این مقدار نشان دهنده نوع دستگاه و مرورگر مورد استفاده است و وب سرور می تواند با توجه مقدار آن، آبیکت های متفاوتی را ارسال کند

سوال ۳- در اولین بسته که توسط مرورگر ارسال شده است، تنها فلاگ Syn مقداری برابر یک دارد که اولین مرحله از برقراری اتصال TCP است. در شکل ۳ این فلگ ها را مشاهده می کنیم .

سوال ۴-



شکل ۳ فلگ ها در پکت Syn ارسالی در ابتدای برقراری اتصال T

با توجه به مقدار Host که در هدر HTTP ارسال می شود، یک وب سرور با یک آدرس IP و روی یک پورت (پورت ۸۰ یا ۴۴۳) می تواند وب سایت های متفاوتی را میزبانی کند. در نتیجه وقتی که آدرس سایت دیگری را در مرورگر وارد می کنیم، مقدار Host آن در پیام درخواست که توسط مرورگر ارسال می شود تغییر می کند و از روی آن، وب سرور محتوای متفاوتی را برمی گرداند

سوال ۵

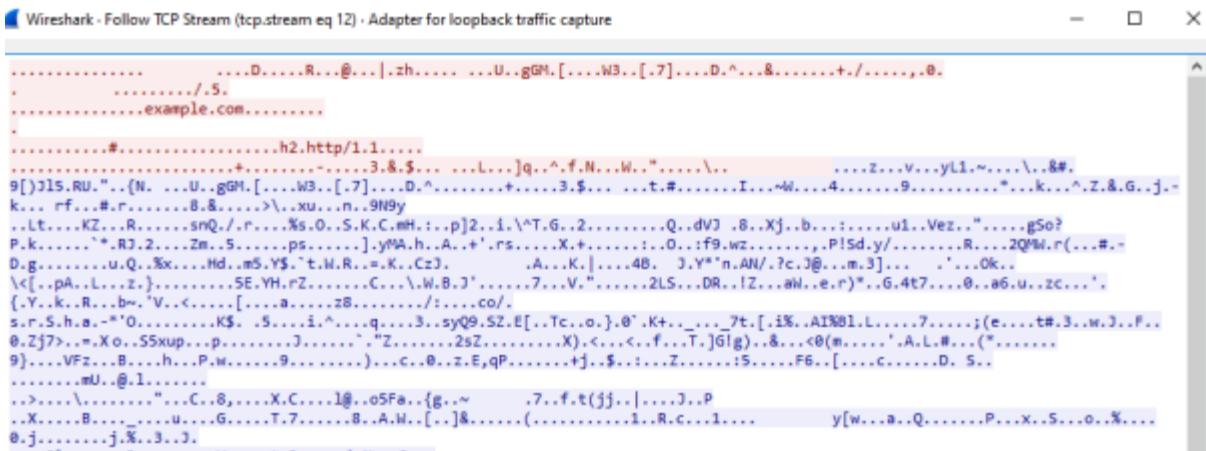
- مطابق شکل ۴، از آنجا که این گواهی self-signed است، صادرکننده آن مشخص و معتبر نیست. در قسمت subject name اطلاعات وارد شده توسط بنده در هنگام ساخت گواهی مشاهده می شود که نشان دهنده شخصی است که گواهی برای آن صادر شده است. این گواهی به برای مدت ۳۶۵۰۰ روز صادر شده و از الگوریتم RSA با اندازه کلید ۲۰۴۸ بیتی استفاده می کند .

سوال ۶

- خیر؛ زمانی که از TLS استفاده می کنیم، پیام ها رمزنگاری می شوند و امکان خوانده و دستکاری شدن توسط دیگر در بین راه وجود ندارد (شکل ۴)

سوال ۷ -

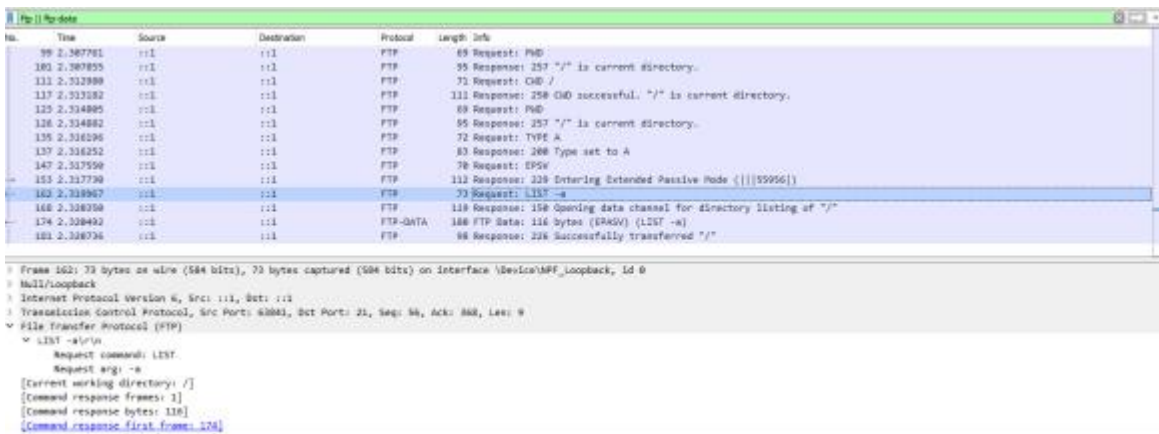
گواهی google.com توسط مراجع معتبر و برای این سایت ایجاد و امضا شده است. این گواهی توسط google trust service امضا و صادر شده که آن هم توسط GlobalSign تایید شده است. در نتیجه در هنگام ورود به این سایت، پیغام هشدار توسط مرورگر داده نمی شود. الگوریتم رمزنگاری آن نیز با سایت داخلی خودمان متفاوت است و از Elliptic Curve استفاده می کند.



شکل ۴: ناخوانا بودن پیام ها زمانی که از پروتکل TLS استفاده می شود

سوال ۸

در این پروتکل، مطابق شکل ۵، از دستور LIST برای گرفتن لیست دایرکتوری فعلی استفاده شده است. پس از آن یک اتصال TCP دیگر برای ارسال اطلاعات تحت پروتکل FTP-DATA برقرار شده است. از آنجا که از رمزنگاری خاصی استفاده نشده است، نام کاربری و رمز عبور به راحتی قابل مشاهده است. همان طور که پیشتر ذکر شد، این پروتکل از TCP در لایه انتقال استفاده می کند. در اینجا آدرس پورت مبدا ۶۳۸۴۱ و آدرس پورت مقصد (سرور FTP) ۲۱ است



No.	Time	Source	Destination	Protocol	Length	Info
99	2.367761	111	111	FTP	69	Request: PWD
100	2.367855	111	111	FTP	95	Response: 257 "/" is current directory.
111	2.372988	111	111	FTP	72	Request: CWD /
112	2.373182	111	111	FTP	111	Response: 250 CWD successful. "/" is current directory.
125	2.374885	111	111	FTP	69	Request: PWD
126	2.374882	111	111	FTP	95	Response: 257 "/" is current directory.
135	2.376296	111	111	FTP	72	Request: TYPE A
137	2.376252	111	111	FTP	83	Response: 200 Type set to A
147	2.377598	111	111	FTP	78	Request: EPSV
155	2.377738	111	111	FTP	112	Response: 220 Entering Extended Passive Mode (55956)
162	2.378967	111	111	FTP	72	Request: LIST -a
168	2.380358	111	111	FTP	118	Response: 150 Opening data channel for directory listing of "/"
174	2.380492	111	111	FTP-DATA	168	FTP Data: 116 bytes (KGV) (LIST -a)
181	2.380736	111	111	FTP	88	Response: 226 Successfully transferred "/"

Frame 162: 72 bytes on wire (584 bits), 72 bytes captured (584 bits) on interface \Device\NPF_{...} Id 0
 Null/loopback
 Internet Protocol Version 6, Src: 111, Dst: 111
 Transmission Control Protocol, Src Port: 63841, Dst Port: 21, Seq: 86, Ack: 888, Len: 9
 File Transfer Protocol (FTP)
 Request command: LIST
 Request arg: -a
 [Current working directory: /]
 [Command response frames: 1]
 [Command response bytes: 116]
 [Command response first frame: 176]

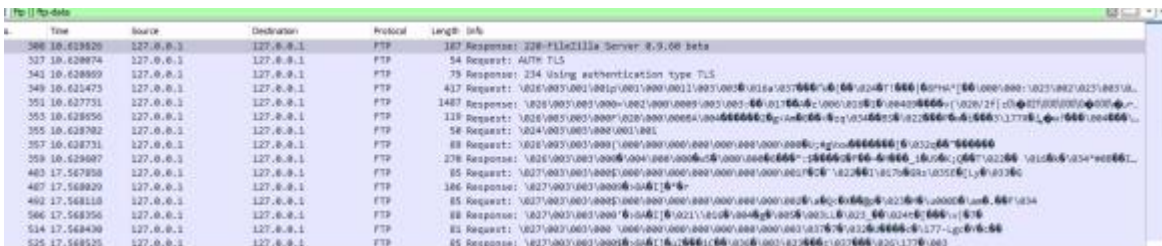
شکل ۵: بسته های پروتکل FTP و دستور LIST برای گرفتن لیست فایل ها در دایرکتوری فعلی

سوال ۹ -

خیر؛ امکان بازکردن آن با مرورگر وجود ندارد. با اتصال از طریق برنامه FileZilla، مطابق شکل ۶، امکان خواندن اطلاعات (از جمله نام کاربری و رمز عبور) وجود ندارد

پروتکل HTTP

سوال ۱ -



No.	Time	Source	Destination	Protocol	Length	Info
54	10.628826	127.0.0.1	127.0.0.1	FTP	162	Response: 228-FileZilla Server: 0.9.60 beta
57	10.628874	127.0.0.1	127.0.0.1	FTP	54	Request: AUTH TLS
58	10.628889	127.0.0.1	127.0.0.1	FTP	79	Response: 234 Using authentication type TLS
59	10.628475	127.0.0.1	127.0.0.1	FTP	417	Request: USER user@127.0.0.1:63841
60	10.627731	127.0.0.1	127.0.0.1	FTP	1487	Response: 331 Password required for user@127.0.0.1:63841
61	10.628656	127.0.0.1	127.0.0.1	FTP	119	Request: PASS *****
62	10.628782	127.0.0.1	127.0.0.1	FTP	58	Request: ACCT user@127.0.0.1:63841
63	10.628731	127.0.0.1	127.0.0.1	FTP	88	Response: 332 Account required for user@127.0.0.1:63841
64	10.628807	127.0.0.1	127.0.0.1	FTP	278	Response: 331 Password required for user@127.0.0.1:63841
65	17.567858	127.0.0.1	127.0.0.1	FTP	85	Request: USER user@127.0.0.1:63841
66	17.568820	127.0.0.1	127.0.0.1	FTP	186	Response: 331 Password required for user@127.0.0.1:63841
67	17.568118	127.0.0.1	127.0.0.1	FTP	85	Request: USER user@127.0.0.1:63841
68	17.568356	127.0.0.1	127.0.0.1	FTP	88	Response: 332 Account required for user@127.0.0.1:63841
69	17.568430	127.0.0.1	127.0.0.1	FTP	81	Request: USER user@127.0.0.1:63841
70	17.568525	127.0.0.1	127.0.0.1	FTP	85	Response: 331 Password required for user@127.0.0.1:63841

شکل ۶: رمزنگاری در پروتکل FTP. در این حالت امکان خواندن اطلاعات رد و بدل شده وجود ندارد.

پاسخ این سوال در بخش اول نیز داده شد. به طور خلاصه مقدار Connection: alive-keep است، نوع درخواست GET و مقدار User-Agent برابر

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

است. کاربرد آن نیز پیشتر توضیح داده شد .

سوال ۲ -

پاسخ این سوال نیز در بخش اول نیز داده شد. تنها فلگی که مقدار آن یک است، فلگ Syn است

پروتکل ftp

سوال ۱ -

پروتکل لایه انتقال مورد استفاده TCP است. پورت مبدا ۶۵۳۹۲ و مقصد آن ۲۱ است

سوال ۲ -

از آنجا که نام کاربری و رمز عبوری برای ورود تعریف و استفاده نشده است، نام کاربری مقدار anonymous ارسال شده. همچنین مطابق پیام سرور، نام کاربر به جای رمز وارد شده است. هر چند برنامه کلاینت مقدار example@anonymous.com را برای این قسمت ارسال کرده است (شکل ۷).

```
AUTH TLS
502 RFC 2228 authentication not implemented.
AUTH SSL
502 RFC 2228 authentication not implemented.
USER anonymous
331 Guest login ok, type your name as password.
PASS anonymous@example.com
230-
```

شکل ۷ لاگین به صورت کاربر مهمان در FTP