

گزارش دستور کار سوم آزمایشگاه درس شبکه‌های کامپیوتری

نگار موقتیان، ۹۸۳۱۰۶۲

۱. اطلاعات مربوط به پروتکل HTTP

با توجه به بخش زیر می‌توان گفت برای بسته انتخاب شده آدرس پورت مبدا برابر با 61745 و آدرس پورت مقصد برابر با 80 (که پورت مربوط به سایت اجرا شده است) می‌باشد.

No.	Time	Source	Destination	Protocol	Length	Info
19	5.312133	127.0.0.1	127.0.0.1	TCP	56	61745 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256
20	5.312217	127.0.0.1	127.0.0.1	TCP	56	80 → 61745 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
21	5.312284	127.0.0.1	127.0.0.1	TCP	44	61745 → 80 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
22	5.313233	127.0.0.1	127.0.0.1	HTTP	493	GET / HTTP/1.1
23	5.313271	127.0.0.1	127.0.0.1	TCP	44	80 → 61745 [ACK] Seq=1 Ack=450 Win=2619648 Len=0
24	5.315515	127.0.0.1	127.0.0.1	HTTP	519	HTTP/1.1 200 OK (text/html)
25	5.315631	127.0.0.1	127.0.0.1	TCP	44	61745 → 80 [ACK] Seq=450 Ack=476 Win=2619136 Len=0
29	5.487115	127.0.0.1	127.0.0.1	HTTP	436	GET /favicon.ico HTTP/1.1
30	5.487153	127.0.0.1	127.0.0.1	TCP	44	80 → 61745 [ACK] Seq=476 Ack=842 Win=2619392 Len=0
31	5.487802	127.0.0.1	127.0.0.1	HTTP	586	HTTP/1.1 404 Not Found (text/html)
32	5.487894	127.0.0.1	127.0.0.1	TCP	44	61745 → 80 [ACK] Seq=842 Ack=1018 Win=2618624 Len=0

> Frame 22: 493 bytes on wire (3944 bits), 493 bytes captured (3944 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: 61745, Dst Port: 80, Seq: 1, Ack: 1, Len: 449
> Hypertext Transfer Protocol

همچنین با توجه به شکل زیر می‌توان به مراحل طی شده در این ارتباط پی برد (هر مرحله با یک مستطیل رنگی مشخص شده‌است). در مرحله اول دست‌تکانی سه مرحله‌ای TCP انجام شده و یک اتصال TCP ایجاد شده‌است. پس از آن در هر مرحله کلاینت یک پیام HTTP به سرور فرستاده و ACK آن را دریافت می‌کند، سپس سرور به کلاینت یک پیام دیگر HTTP حاوی پاسخ درخواست داده شده ارسال می‌کند. این روند به همین شکل ادامه پیدا می‌کند تا یکی از طرفین اتصال را خاتمه دهد (که به دلیل وجود هدر keep-alive در این جا شاهد خاتمه ارتباط نیستیم).

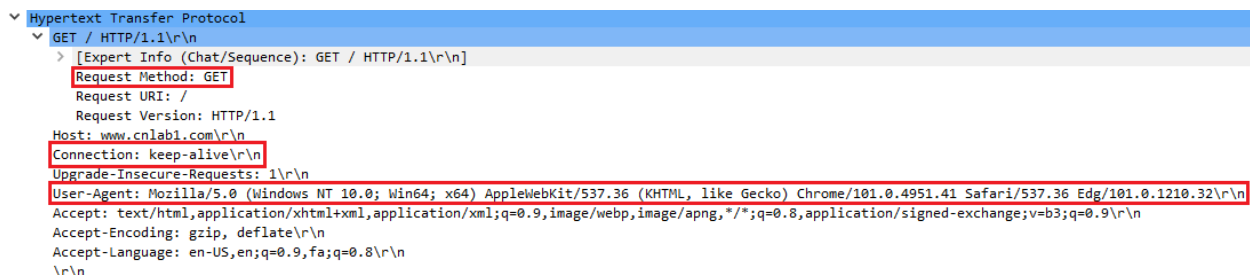
در مثال زیر ابتدا اتصال TCP برقرار شده، سپس کلاینت درخواستی برای گرفتن صفحه مورد نظر فرستاده و سرور با فرستادن اطلاعات صفحه index.html به آن پاسخ داده‌است. سپس کلاینت برای گرفتن آیکون سایت مورد نظر درخواست داده و سرور به او اطلاع داده که چنین فایل‌ای وجود ندارد.

No.	Time	Source	Destination	Protocol	Length	Info
19	5.312133	127.0.0.1	127.0.0.1	TCP	56	61745 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
20	5.312217	127.0.0.1	127.0.0.1	TCP	56	80 → 61745 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
21	5.312284	127.0.0.1	127.0.0.1	TCP	44	61745 → 80 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
22	5.313233	127.0.0.1	127.0.0.1	HTTP	493	GET / HTTP/1.1
23	5.313271	127.0.0.1	127.0.0.1	TCP	44	80 → 61745 [ACK] Seq=1 Ack=450 Win=2619648 Len=0
24	5.315515	127.0.0.1	127.0.0.1	HTTP	519	HTTP/1.1 200 OK (text/html)
25	5.315631	127.0.0.1	127.0.0.1	TCP	44	61745 → 80 [ACK] Seq=450 Ack=476 Win=2619136 Len=0
29	5.487115	127.0.0.1	127.0.0.1	HTTP	436	GET /favicon.ico HTTP/1.1
30	5.487153	127.0.0.1	127.0.0.1	TCP	44	80 → 61745 [ACK] Seq=476 Ack=842 Win=2619392 Len=0
31	5.487802	127.0.0.1	127.0.0.1	HTTP	586	HTTP/1.1 404 Not Found (text/html)
32	5.487894	127.0.0.1	127.0.0.1	TCP	44	61745 → 80 [ACK] Seq=842 Ack=1018 Win=2618624 Len=0

به طور کلی وب سرورها می توانند چندین سایت را به طور همزمان بر روی خود اجرا کنند. با استفاده از IP و پورت سرور مقصد می توانیم به طور خاص مشخص کنیم که می خواهیم با چه سروری ارتباط برقرار کنیم. پس از آن همانطور که در شکل زیر مشخص شده، در هدر host درخواست HTTP ای که به وب سرور می فرستیم آدرس سایت مورد نظر آمده است.

```
GET / HTTP/1.1
Host: www.cnlab1.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.41 Safari/537.36 Edg/101.0.1210.32
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,fa;q=0.8
```

۲. هدرهای استفاده شده در پروتکل HTTP



```
▼ Hypertext Transfer Protocol
  ▼ GET / HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
      Host: www.cnlab1.com\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/101.0.4951.41 Safari/537.36 Edg/101.0.1210.32\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
      \r\n
```

با توجه به شکل بالا اتصال برقرار شده برای ارسال این بسته از نوع keep-alive می باشد، به این معنا که ارتباط برقرار شده پایا می باشد و چند پیغام HTTP می توانند بر روی یک اتصال TCP منتقل شوند.

همچنین درخواست داده شده از نوع GET بوده و برای دریافت فایل index.html سایت مورد نظر فرستاده شده است.

مقدار هدر User-Agent برای فرستادن اطلاعات مربوط به سیستم عامل و مرورگر استفاده شده به کار می رود. مقدار این هدر از آن جایی می تواند اهمیت داشته باشد که بعضی از قابلیت های وبسایت ها ممکن است برای یک مرورگر خاص قابل استفاده نباشد. در این صورت باید به کاربر پیغام خاصی نشان داده شود و یا از برنامه جایگزینی استفاده شود. مقدار این هدر برای بسته فرستاده شده مانند زیر می باشد:

```
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/101.0.4951.41 Safari/537.36 Edg/101.0.1210.32
```

۳. مقدار هدر Flags در پروتکل TCP

برای اولین بسته TCP مقدار Flags برابر با SYN می‌باشد، بنابراین می‌توان گفت از این بسته برای شروع ارتباط از سمت کلاینت به سرور استفاده شده‌است.

```
Acknowledgment number (raw): 0
1000 .... = Header Length: 32 bytes (8)
> Flags: 0x002 (SYN)
Window: 65535
[Calculated window size: 65535]
```

همچنین برای اولین بسته HTTP مقدار Flags برابر با (PSH, ACK) است، به این معنا که این بسته برای اعلام ACK بوده و پیش از پر شدن segment، PUSH شده‌است (زیرا ACK داده کوچکی است که باید پیش از اتمام time out فرستاده شود).

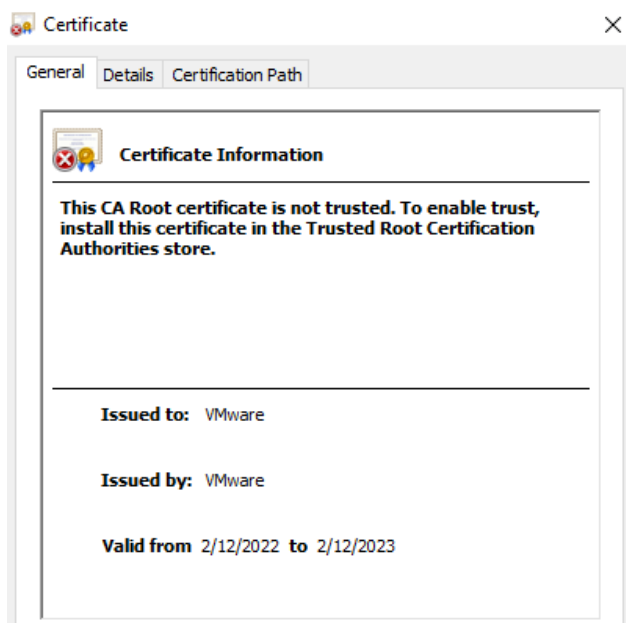
```
Acknowledgment number (raw): 1802169247
0101 .... = Header Length: 20 bytes (5)
> Flags: 0x018 (PSH, ACK)
Window: 10233
[Calculated window size: 2619648]
```

۴. تفاوت میان دو سایت اجرا شده بر روی یک وب‌سرور

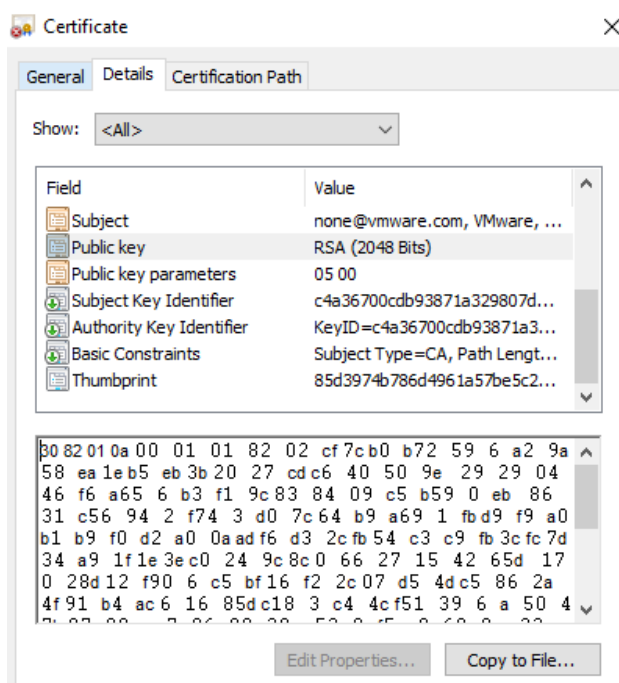
با توجه به هدرهای بسته‌های منتقل شده در این اتصال، می‌توان مشاهده کرد که آدرس IP و شماره پورت این دو سایت یکسان، اما مقدار هدر host آن‌ها متفاوت است. از این طریق با توجه به آدرسی که در مرورگر خود وارد می‌کنیم می‌توانیم مشخص کنیم که می‌خواهیم به کدام یک از سایت‌های روی وب‌سرور دسترسی داشته باشیم.

۵. اطلاعات مربوط به گواهی وبسایت ساخته شده

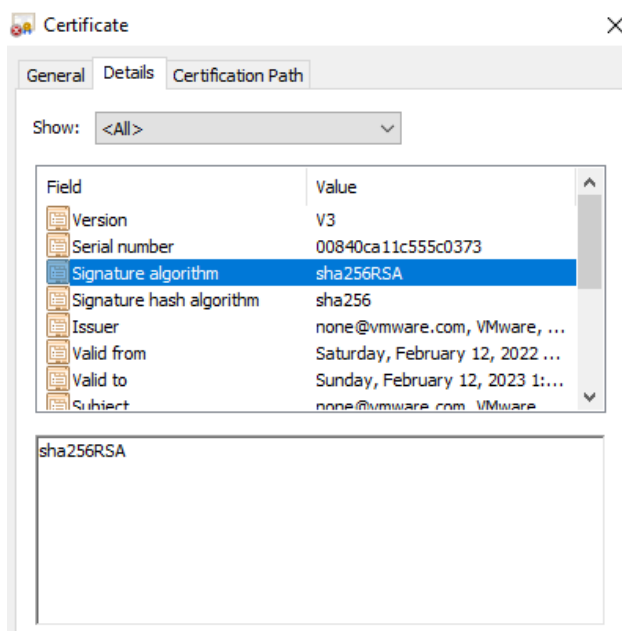
با توجه به قسمت نشان داده در شکل زیر این گواهی توسط VMware و برای VMware صادر شده و مدت اعتبار آن یک سال می باشد



همچنین کلید عمومی صادر کننده در قسمت زیر قابل مشاهده است.



به علاوه با توجه به قسمت زیر امضای دیجیتال انجام شده از الگوریتم sha256RSA استفاده کرده و توسط الگوریتم sha256 هش شده است.



۶. بررسی متن ارتباط در پروتکل TLS

خیر؛ متنی که برای ارتباط در این پروتکل استفاده شده بر خلاف پروتکل HTTP قابل خواندن نیست و داده‌های آن رمزنگاری شده‌اند، بنابراین اگر کسی بسته‌های منتقل شده را شنود کرد نمی‌تواند به محتوای آن‌ها پی ببرد. به همین دلیل این پروتکل به نسبت HTTP می‌تواند امنیت را در ارتباط تامین کند.

۷. تفاوت گواهی وبسایت google با وبسایت ساخته شده

از تفاوت‌های این دو گواهی می‌توان به موارد زیر اشاره کرد:

۱. صادر کننده گواهی (GTS CA 1C3) و کسی که گواهی برای آن صادر شده (تمام وبسایت‌هایی که با google.com خاتمه می‌یابند) متفاوت است.

۲. کلید عمومی گوگل از نوع ECC و کلید عمومی سایت ساخته شده از نوع RSA است که قدر رمزنگاری متفاوتی دارند.

۳. گواهی گوگل بخش‌های اضافه‌ای از جمله Enhanced Key Usage, Authority Information Access, Subject Alternative Name, Certificate Policies, CLR Distribution Point, SCT List و Key Usage دارد.

۴. گواهی سایت گوگل دارای سلسه مراتبی بوده و status آن بر خلاف وبسایت ما “This Certificate is OK” است.

۸. اطلاعات مربوط به پروتکل FTP

همانطور که در قسمت زیر مشاهده می‌شود، سرور با دریافت دستور LIST از سمت کلاینت با استفاده از پروتکل FTP-DATA لیست فایل‌های موجود در دایرکتوری فعلی را برای او ارسال کرده‌است.

323	5.209358	127.0.0.1	127.0.0.1	FTP	50 Request: LIST
329	5.210505	127.0.0.1	127.0.0.1	FTP	69 Response: 150 Connection accepted
339	5.210682	127.0.0.1	127.0.0.1	FTP-DATA	3231 FTP Data: 3187 bytes (PASV) (LIST)

همچنین در قسمت زیر نام کاربری (TestUser) و گذرواژه (1234) کاربری که به فایل‌ها دسترسی پیدا کرده (و آن را به عنوان ادمین اضافه کرده بودیم) قابل مشاهده است.

220	5.206327	127.0.0.1	127.0.0.1	FTP	59 Request: USER TestUser
226	5.206592	127.0.0.1	127.0.0.1	FTP	80 Response: 331 Password required for testuser
229	5.206678	127.0.0.1	127.0.0.1	FTP	55 Request: PASS 1234
237	5.206907	127.0.0.1	127.0.0.1	FTP	59 Response: 230 Logged on

طبق اطلاعات زیر در رابطه با لایه transport، برای انتقال این بسته از پروتکل TCP با شماره پورت مبدا 54899 و شماره پورت مقصد 21 استفاده شده‌است.

```
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 54899, Dst Port: 21, Seq: 1, Ack: 149, Len: 15
▼ File Transfer Protocol (FTP)
```

۹. هدرهای استفاده شده در پروتکل HTTP

```
▼ Hypertext Transfer Protocol
  ▼ GET /connecttest.txt HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /connecttest.txt HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /connecttest.txt
      Request Version: HTTP/1.1
      Cache-Control: no-cache\r\n
      Connection: Close\r\n
      Pragma: no-cache\r\n
      User-Agent: Microsoft NCSI\r\n
      Host: www.msftconnecttest.com\r\n
```

با توجه به شکل بالا اتصال برقرار شده برای ارسال این بسته از نوع close می‌باشد، به این معنا که ارتباط برقرار شده ناپایا می‌باشد و تنها یک پیغام HTTP می‌تواند بر روی یک اتصال TCP منتقل شود. بنابراین پس از پاسخ سرور به کلاینت اتصال باید بسته شود.

همچنین درخواست داده شده از نوع GET بوده و برای دریافت داده از روی سایت مورد نظر فرستاده شده‌است. مقدار هدر User-Agent برای فرستادن اطلاعات مربوط به سیستم عامل و مرورگر استفاده شده به کار می‌رود. مقدار این هدر از آنجایی می‌تواند اهمیت داشته باشد که بعضی از قابلیت‌های وبسایت‌ها ممکن است برای یک مرورگر خاص قابل استفاده نباشد. در این صورت باید به کاربر پیغام خاصی نشان داده شود و یا از برنامه جایگزینی استفاده شود. مقدار این هدر برای بسته فرستاده شده برابر با Microsoft NCSI می‌باشد.

۱۰. مقدار هدر Flags در پروتکل TCP

برای اولین بسته TCP مقدار Flags برابر با SYN می‌باشد، بنابراین می‌توان گفت از این بسته برای شروع ارتباط از سمت کلاینت به سرور استفاده شده‌است.

```
Acknowledgment number (raw): 0
1000 .... = Header Length: 32 bytes (8)
> Flags: 0x002 (SYN)
Window: 64240
[Calculated window size: 64240]
```