۱- راه‌اندازی سرویس‌های Web و FTP

۱-۱- هدف آزمایش

هدف این آزمایش، آشنایی با تنظیمات مقدماتی مربوط به راه‌اندازی سرویس‌های Web و FTP و تحلیل بسته‌های HTTP و FTP است.

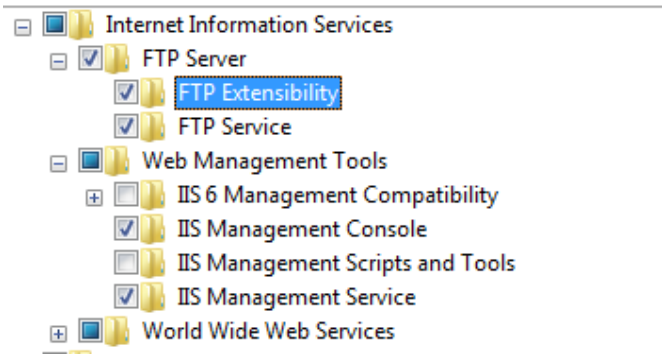
۱-۲- قطعات و ابزارهای موردنیاز

ابزارهای موردنیاز در این آزمایش عبارت‌اند از:

- کامپیوتر شخصی با سیستم‌عامل ویندوز 7 برای هر گروه
- برنامه Filezila نسخه ۳.۱۷.۰.۱

۱-۳- شرح آزمایش

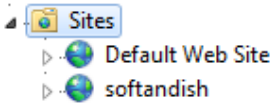
ابتدا تنظیمات مربوط به سرور Web را انجام می‌دهیم. سپس تنظیمات FTP Server را بررسی می‌کنیم. برای این منظور ابتدا عبارت Turn windows features on or off را در قسمت جستجوی ویندوز ۷، جستجو کنید. سپس بخش‌های زیر را از پنجره نمایش داده شده، انتخاب نمایید و بر روی OK کلیک کنید. دقت کنید هر سه بخش FTP Server، Web Management Tools و World Wide Web Services مانند شکل (۲-۱) تیک خورده باشند.



شکل (۱-۲) پیش تنظیمات

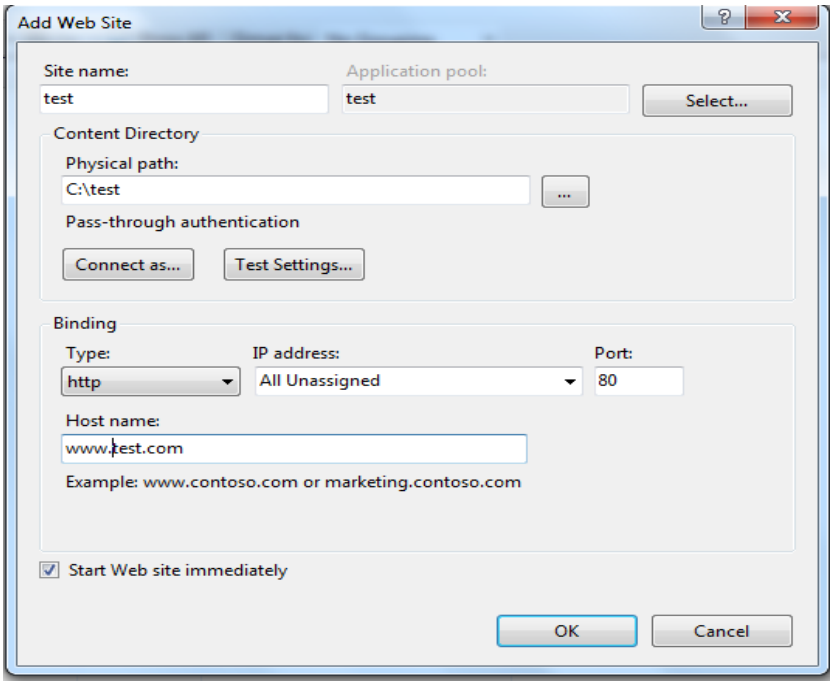
۱-۳-۱- تنظیمات سرور Web

۱. از بخش start عبارت iis را جستجو کرده و Internet information service manager را انتخاب کنید. در پنجره باز شده از ستون سمت چپ بر روی Sites کلیک راست کنید و Add Website را انتخاب کنید.



شکل (۲-۲) مرحله اول

۲. در پنجره باز شده، یک نام و یک Host name برای سایت انتخاب کنید. همچنین باید یک مسیر بر روی سیستم خود مشخص کنید که اطلاعات مربوط به سایت در آنجا نگهداری می‌شوند.



شکل (۳-۲) مرحله دوم

۳. مشاهده می‌کنید که به صورت پیش‌فرض سایت بر روی تمام آدرس‌های IP دستگاه و بر روی پورت ۸۰ bind می‌شود. با زدن دکمه OK سایت ایجاد می‌شود.

۴. یک صفحه ساده مانند شکل زیر ایجاد کنید و آن را در مسیر مشخص شده برای سایت قرار دهید. نام آن را index.html بگذارید.

شکل (۴-۲) مرحله سوم

۵. حال در مرورگر خود آدرس Host نوشته شده برای سایت را وارد کنید.

سوال ۱: سایتی که ایجاد کرده‌اید نمایش داده نمی‌شود، چرا؟

۶. به آدرس C:\Windows\System32\drivers\etc در سیستم بروید و فایل hosts را با یک ویرایشگر مانند Notepad++ باز کنید. خط زیر را به آن اضافه کنید. دقت کنید که Host name خود را به‌جای www.test.com قرار دهید.

```
127.0.0.1 www.test.com
```

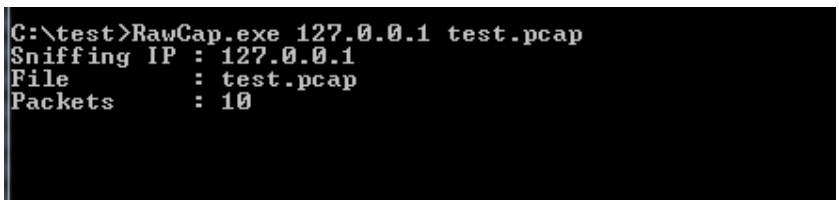
شکل (۵-۲) مرحله چهارم

۷. حال در cmd دستور زیر را وارد کنید. ipconfig /flushdns این دستور باعث پاک شدن کش DNS سیستم شما خواهد شد.

سوال ۲: آدرس سایت خود را در مرورگر وارد کنید و ارتباط خود را با استفاده از wireshark شنود کنید. آیا می‌توانید مشخص کنید کدام بسته مربوط به سایت شما است؟ چه اتفاقی افتاده است؟

۸. Wireshark نمی‌تواند ترافیک مربوط به آدرس‌های Loopback را شنود کند؛ بنابراین از برنامه Rawcap استفاده می‌کنیم. از آدرس http://www.netresec.com/?page=RawCap آن را دانلود کنید.

۹. در محیط cmd به محل فایل rawcap.exe بروید. آن را با دستور نشان داده شده در شکل (۶-۲) اجرا کنید



شکل (۶-۲) دستورات اجرایی در cmd

۱۰. حالا سایت را باز کنید. پس از اتمام باز شدن، با ctrl+c می‌توانید از rawcap خارج شوید. فایل در محل اجرای برنامه ذخیره می‌شود. دقت کنید قبل از باز کردن سایت، کش مرورگر خود را پاک کنید.

۱۱. فایل ذخیره‌شده را با wireshark باز کنید. بسته‌های مربوط به سایت را پیدا کنید. بر روی یکی از آن‌ها کلیک راست کرده و follow HTTP Stream را انتخاب کنید. شکلی مشابه شکل (۷-۲) نمایش داده خواهد شد.

No.	Time	Source	Destination	Protocol	Length	Info
58	5.996343	127.0.0.1	127.0.0.1	TCP	48	7391 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=65495 SACK_PERM=1
59	5.996343	127.0.0.1	127.0.0.1	TCP	48	80 → 7391 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=65495 SACK_PERM=1
60	5.996343	127.0.0.1	127.0.0.1	TCP	40	7391 → 80 [ACK] Seq=1 Ack=1 Win=8192 Len=0
61	5.996343	127.0.0.1	127.0.0.1	HTTP	580	GET / HTTP/1.1
62	5.996343	127.0.0.1	127.0.0.1	TCP	40	80 → 7391 [ACK] Seq=1 Ack=541 Win=7652 Len=0
63	5.998343	127.0.0.1	127.0.0.1	HTTP	337	HTTP/1.1 200 OK (text/html)
64	5.998343	127.0.0.1	127.0.0.1	TCP	40	7391 → 80 [ACK] Seq=541 Ack=298 Win=7895 Len=0

شکل (۷-۲) نمونه‌ای از خروجی Follow HTTP Stream

سوال ۳: آدرس پورت‌های مبدا و مقصد چیست؟ روند برقراری ارتباط در پروتکل HTTP چگونه است؟ وب سرور چگونه آدرس سایت درخواستی شما را تشخیص می‌دهد؟

۱۲. بر روی اولین بسته در پنجره باز شده کلیک کنید. بخش‌های مختلف پروتکل HTTP را مشاهده کنید.

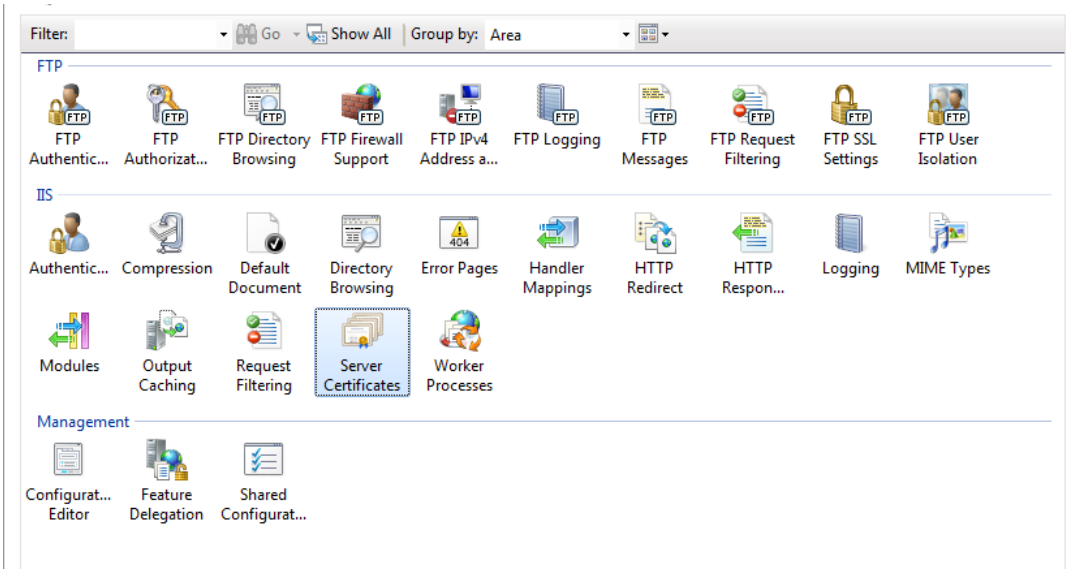
سوال ۴: مقدار بخش Connection چیست؟ درخواست HTTP از نوع GET بوده است یا از نوع POST؟ مقدار User Agent چیست؟ به نظر شما این مقدار بیانگر چه چیزی است؟

سوال ۵: 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؟

سوال ۶: یک سایت دیگر با نام دلخواه ایجاد کنید و بسته‌های مربوط به آن را شنود کنید. چه تفاوتی بین این دو سایت وجود دارد؟

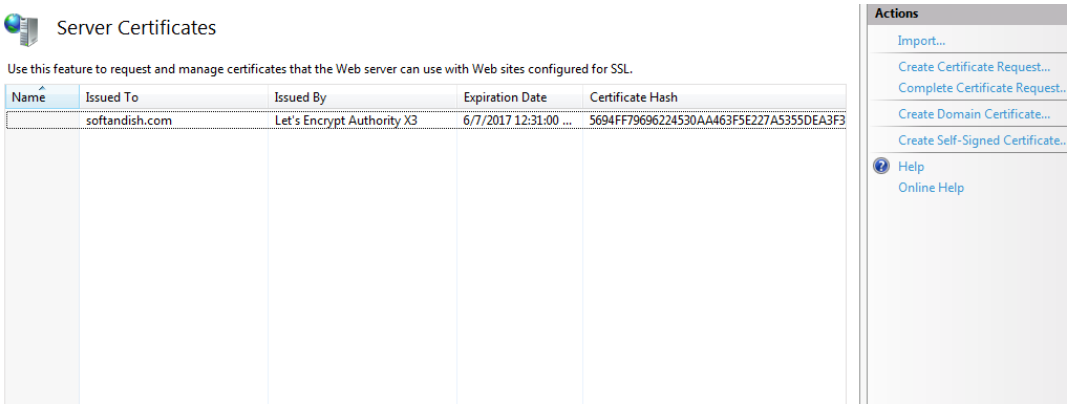
سوال ۷: در مرورگر آدرس 127.0.0.1 را تایپ کنید. چرا هیچ‌کدام از سایت‌ها نمایش داده نمی‌شوند؟

۱۳. دوباره به محیط IIS Manager بروید. این بار در ستون سمت چپ بر روی نام کامپیوتر کلیک کنید. صفحه نمایش داده شده در شکل (۲-۸) باز می‌شود.



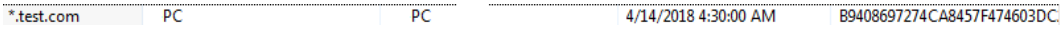
شکل (۸-۲) صفحه نمایش داده شده بعد از انتخاب نام کامپیوتر

۱۴. بر روی Server Certificate کلیک کنید. از ستون سمت راست بر روی Create Self-Signed Certificate کلیک کنید.



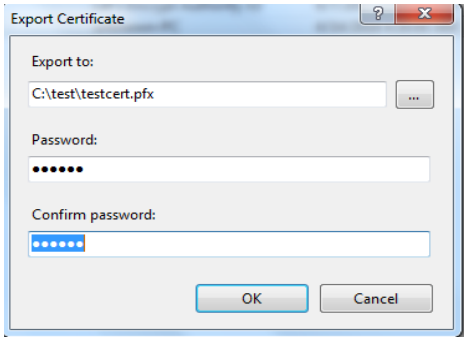
شکل (۹-۲) انتخاب Create Self-Signed Certificate

۱۵. یک نام برای آن انتخاب کنید و بر روی OK کلیک کنید. بهتر است نام انتخابی مطابق نام سایت باشد؛ مثلا test.com.* گواهی مطابق شکل (۲-۱۰) ساخته می‌شود.



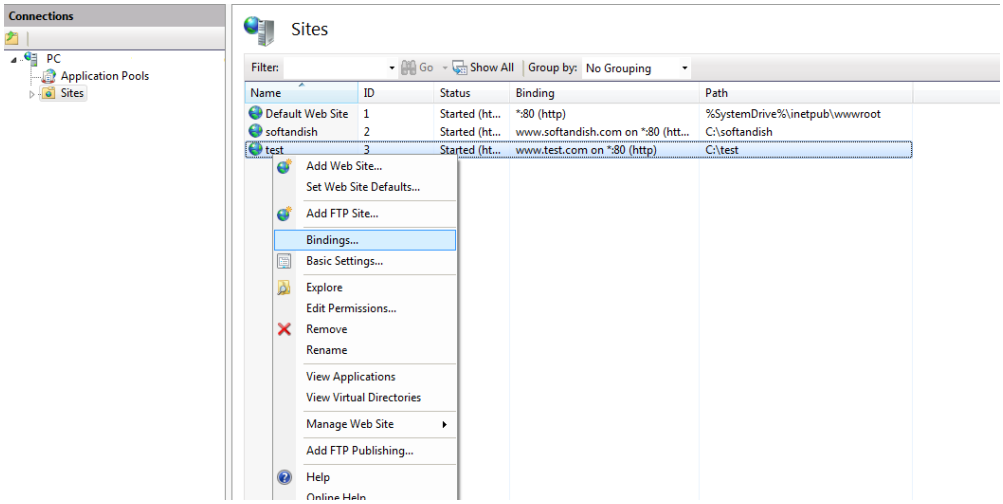
شکل (۱۰-۲) نمونه گواهی ساخته شده

۱۶. اگر بر روی گواهی ساخته شده کلیک راست کرده و export را کلیک کنید صفحه نشان داده شده در شکل (۲-۱۱) نمایش داده می‌شود. آن را کامل کرده و گواهی را export کنید. هر پسورد دلخواهی که می‌خواهید در بخش Password قرار دهید.



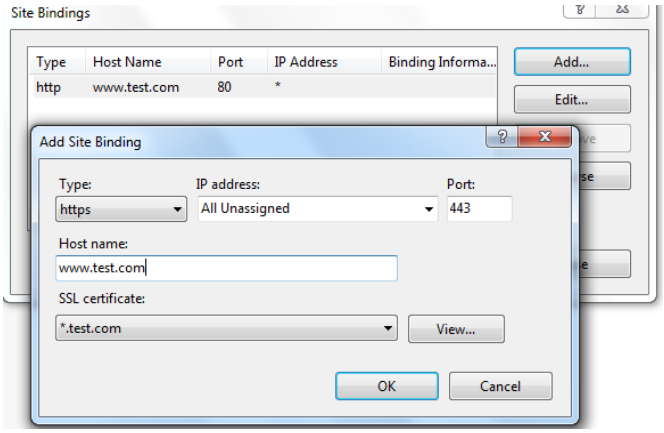
شکل (۱۱-۲) نحوه export گواهی

۱۷. حال دوباره از ستون سمت چپ بر روی Sites کلیک کنید. سپس سایت خود را انتخاب کرده و بر روی آن کلیک راست کرده و Binding را انتخاب کنید.



شکل (۱۲-۲) Binding- مرحله اول

۱۸. بر روی Add کلیک کنید و مطابق شکل (۲-۱۳) آن را تکمیل کنید. دقت کنید که گواهی که خودتان ایجاد کرده‌اید را باید انتخاب کنید.

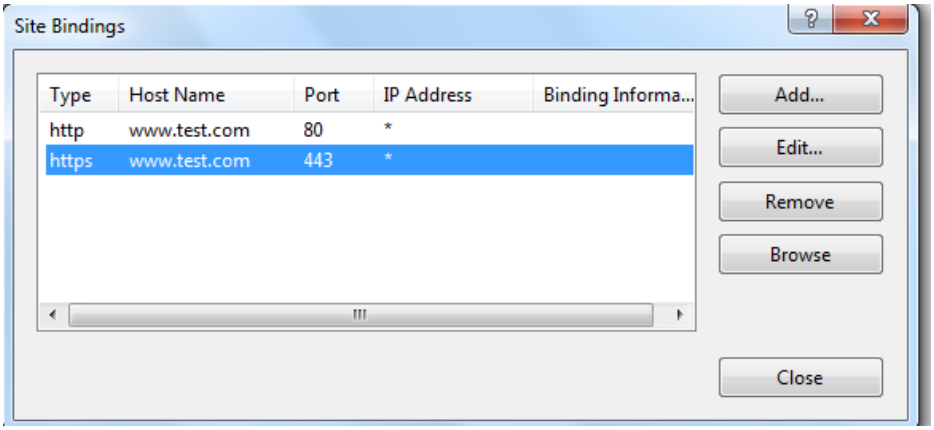


شکل (۱۳-۲) Binding- مرحله دوم

۱۹. بر روی OK کلیک کنید. حالا Binding های نشان داده شده در شکل (۲-۱۴) را دارید.

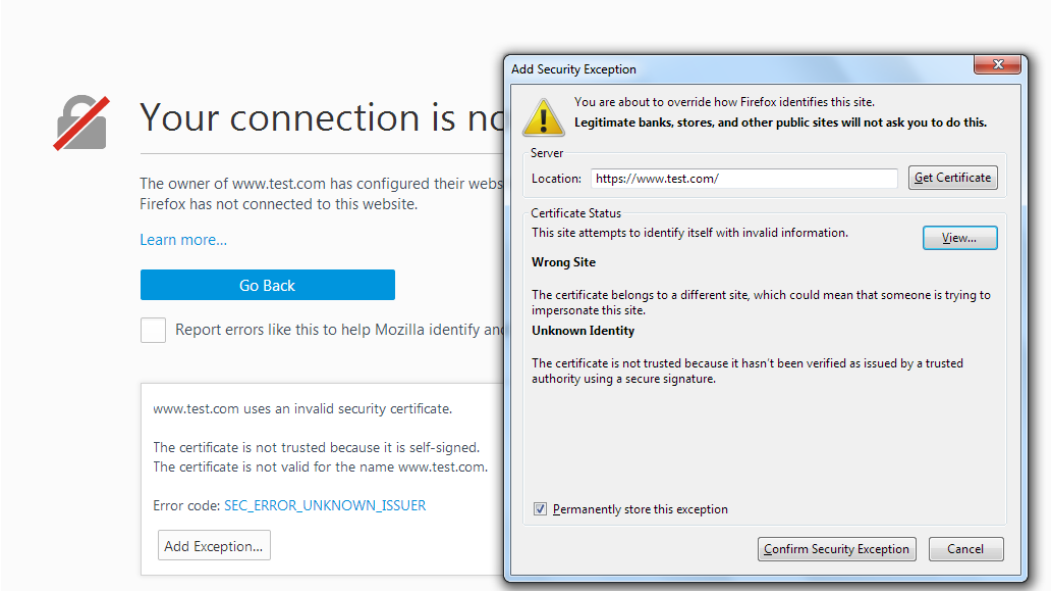
۲۰. حال آدرس https://www.test.com/ را در مرورگر خود باز کنید. دقت کنید که به‌جای test.com آدرس سایت خود را قرار دهید.

سوال ۸: آیا با مشکلی مواجه شدید؟ اگر با مشکل مواجه شده‌اید با استفاده از rawcap، مشخص کنید که چه مشکلی وجود دارد.



شکل (۲-۱۴) Binding- مرحله سوم

۲۱. سایت را در مرورگر باز کنید. خطای نشان داده شده در شکل (۲-۱۵) نمایش داده می‌شود.



شکل (۲-۱۵) خطای نمایش داده شده

۲۲. بر روی Add exception کلیک کرده و دکمه View را فشار دهید.

سوال ۹: مشخص کنید که گواهی را چه کسی برای چه کسی صادر کرده، مدت‌زمان اعتبار گواهی چقدر است، کلید عمومی صادرکننده چیست و امضای دیجیتال انجام شده با چه

الگوریتم‌هایی انجام شده است.

۲۳. حال ارتباط را با Rawcap شنود کنید. بر روی بسته TLS مربوط به این ارتباط کلیک راست کرده و Follow SSL Stream را انتخاب کنید. صفحه‌ای مطابق شکل (۲-۱۶) نمایش داده می‌شود.

سوال ۱۰: آیا می‌توانید متن ارتباط را بخوانید؟ چرا؟

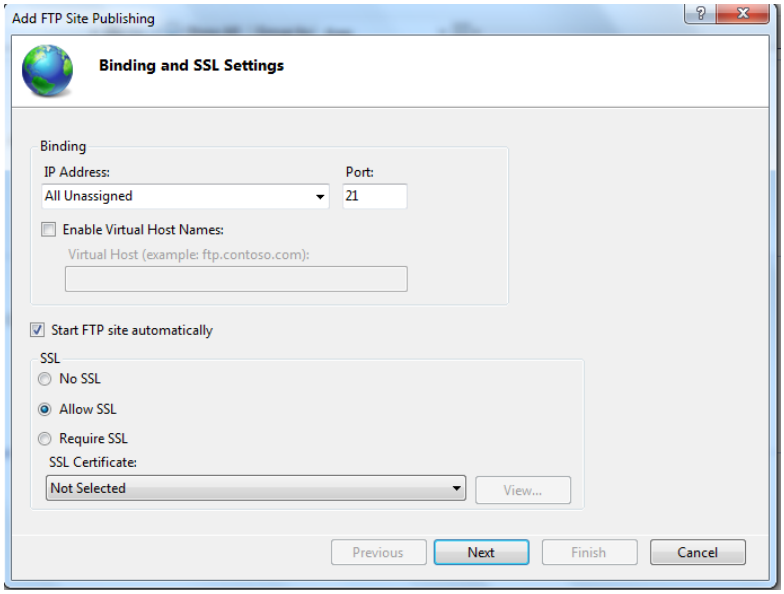
20	2.054118	127.0.0.1	127.0.0.1	TCP	48 1593 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=65495 SACK_PERM=1
21	2.054118	127.0.0.1	127.0.0.1	TCP	48 443 → 1593 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=65495 SACK_PERM=1
22	2.054118	127.0.0.1	127.0.0.1	TCP	40 1593 → 443 [ACK] Seq=1 Ack=1 Win=8192 Len=0
24	2.054118	127.0.0.1	127.0.0.1	TCP	40 443 → 1593 [ACK] Seq=1 Ack=230 Win=7963 Len=0
30	2.056118	127.0.0.1	127.0.0.1	TCP	40 1593 → 443 [ACK] Seq=230 Ack=146 Win=8047 Len=0
32	2.056118	127.0.0.1	127.0.0.1	TCP	40 443 → 1593 [ACK] Seq=146 Ack=289 Win=7904 Len=0
34	2.056118	127.0.0.1	127.0.0.1	TCP	40 443 → 1593 [ACK] Seq=146 Ack=971 Win=7222 Len=0
36	2.058118	127.0.0.1	127.0.0.1	TCP	40 1593 → 443 [ACK] Seq=971 Ack=375 Win=7818 Len=0
23	2.054118	127.0.0.1	127.0.0.1	TLSv1	269 Client Hello
29	2.055118	127.0.0.1	127.0.0.1	TLSv1	185 Server Hello, Change Cipher Spec, Encrypted Handshake Message
31	2.056118	127.0.0.1	127.0.0.1	TLSv1	99 Change Cipher Spec, Encrypted Handshake Message
33	2.056118	127.0.0.1	127.0.0.1	TLSv1	722 Application Data, Application Data
35	2.058118	127.0.0.1	127.0.0.1	TLSv1	269 Application Data

شکل (۲-۱۶) نمونه خروجی Follow SSL Stream

سوال ۱۱: به یک سایت مانند https://google.com وصل شده، گواهی آن را بررسی کنید. گواهی آن سایت با گواهی سایت شما چه تفاوت‌هایی دارد؟

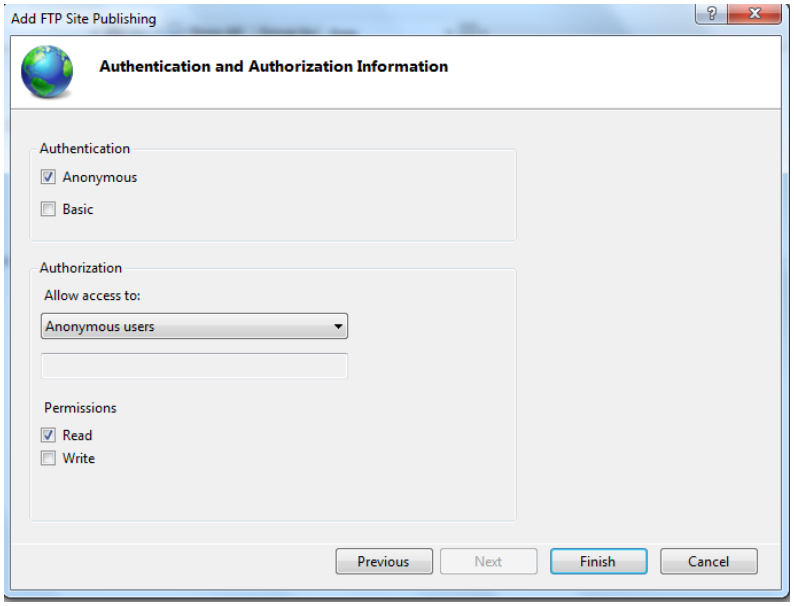
۲-۳-۱- تنظیمات سرور FTP

۱. دوباره به صفحه اصلی IIS Manager بروید. بر روی نام سایت ساخته شده خودتان در ستون سمت چپ کلیک راست کرده و Add FTP Publishing را انتخاب کنید. تنظیمات را مطابق شکل (۲-۱۷) انجام دهید. به‌جای Test.com اسم سایت خود را قرار دهید.



شکل (۲-۱۷) FTP Site Publishing

۲. دکمه Next را بزنید و صفحه بعد را مطابق شکل (۲-۱۸) کامل کنید.



شکل (۱۸-۲) تکمیل Binding

۳. بر روی دکمه Finish کلیک کنید. درنهایت Binding هم ساخته می‌شود.

۴. به آدرس ftp://www.test.com/ بروید. ارتباط را با Rawcap شنود کنید.

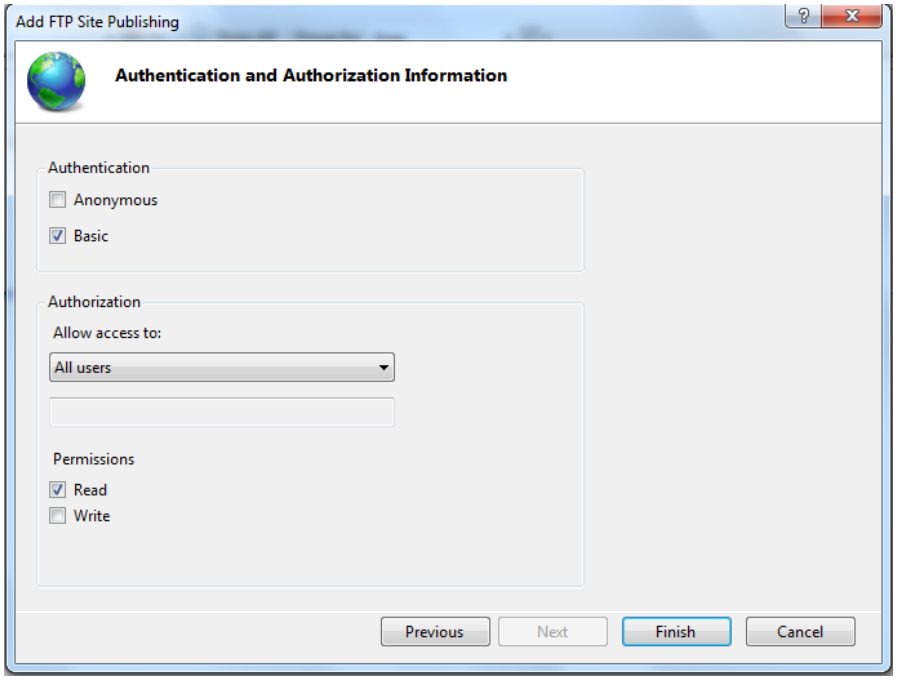
سوال ۱۲: مشخص کنید چه دستوری برای لیست کردن فایل‌های دایرکتوری استفاده شده است. مشخص کنید چه نام کاربری برای دسترسی به سایت استفاده شده است. پروتکل لایه Transport استفاده شده برای این بسته‌ها چیست؟ آدرس پورت مبدا و مقصد ارتباط را مشخص کنید.

۵. اکنون با کلیک راست کردن بر روی سایت خود و انتخاب گزینه Remove FTP Publishing، تنظیمات قبلی را حذف کنید. حال دوباره Binding جدیدی ایجاد کنید و این بار بخش Authentication را مطابق شکل (۲-۱۹) تکمیل کنید.

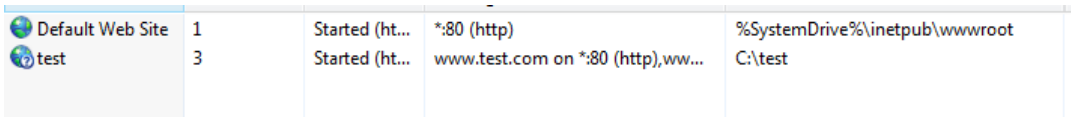
۶. دوباره به آدرس ftp://www.test.com/ بروید. این بار باید نام کاربری و پسورد سیستم خود را وارد کنید تا اجازه دسترسی به شما داده شود. ارتباط را با Raw cap شنود کنید.

سوال ۱۳: آیا نام کاربری و پسورد قابل خواندن است؟

۷. اگر از منوی سمت چپ، ابتدا بر روی Sites کلیک کنید، صفحه نشان داده شده در شکل (۲-۲۰) نمایش داده می‌شود.



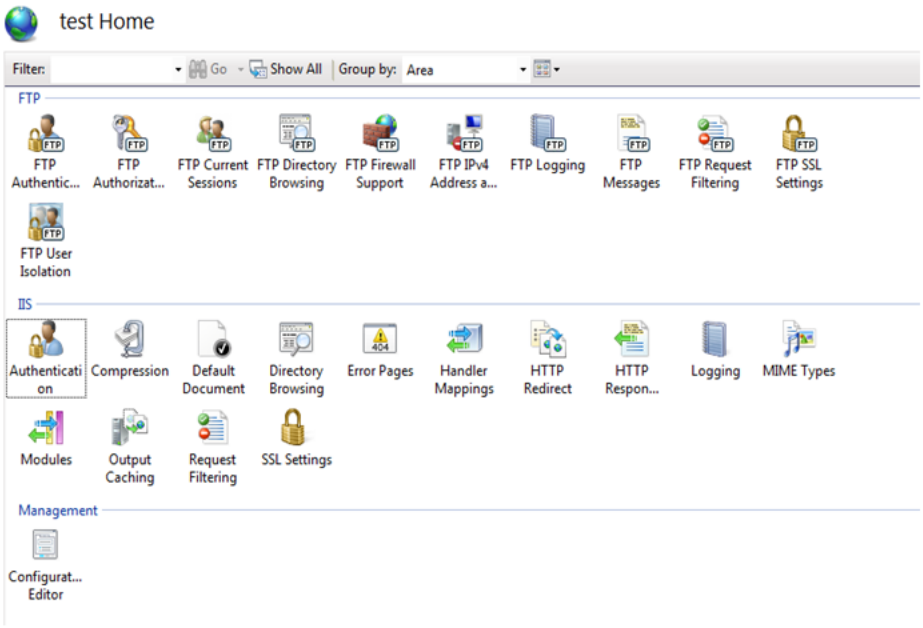
شکل (۱۹-۲) تنظیمات Authentication



شکل (۲۰-۲) صفحه نمایش داده شده بعد از انتخاب Sites

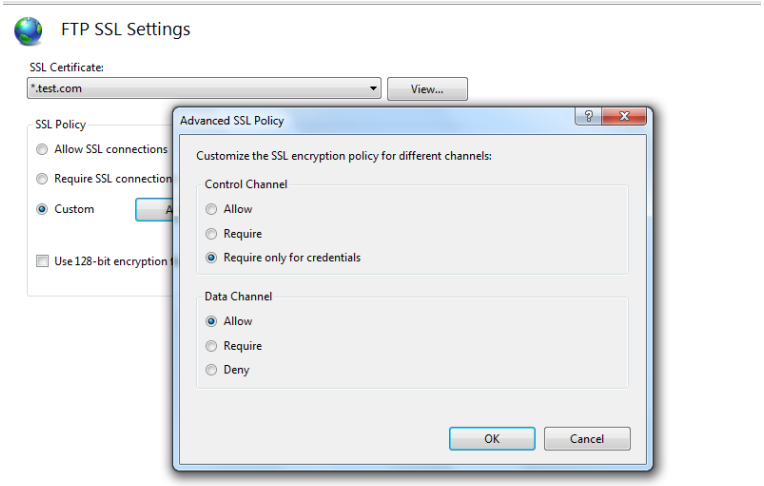
۸. با انتخاب سایت خود، صفحه نشان داده شده در شکل (۲-۲۱) نمایش داده می‌شود. تنظیمات نام‌های کاربری و دسترسی‌ها در این بخش مشخص است

سوال ۱۴: به FTP Authentication و FTP Authorization وارد شوید و مشخص کنید چه سطح دسترسی برای چه کاربرانی تعریف شده است.



شکل (۲-۲۱) صفحه نمایش داده شده بعد از انتخاب نام سایت خود

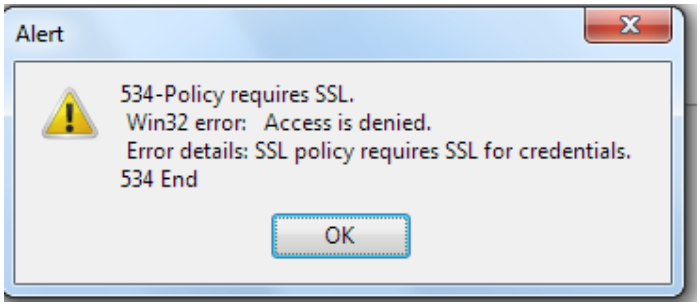
۹. دوباره از منوی سمت چپ، ابتدا بر روی Sites کلیک کنید و سپس سایت خود را انتخاب کنید. به بخش FTP SSL Settings بروید. یک گواهی انتخاب کنید. سپس بر روی Custom کلیک کنید و آن را مطابق شکل (۲-۲۲) تکمیل کنید. پس از آن دکمه Apply را فشار دهید.



شکل (۲-۲۲) تنظیمات SSL Policy

سوال ۱۵: سعی کنید دوباره سایت را از مرورگر باز کنید. آیا می‌توانید به سایت وارد شوید؟

سوال ۱۶: در مرورگر فایرفاکس خطای نمایش داده شده در شکل (۲-۲۳) نشان داده می‌شود. معنی این خطا چیست؟



شکل (۲۳-۲) خطای نمایش داده شده

۱۰. برنامه Filezilla را از آدرس https://filezilla-project.org/ دانلود کنید. پس از نصب، در قسمت Host، loopback را بنویسید. نام کاربری و پسورد ویندوز خود را وارد کنید و بر روی Quickconnect کلیک کنید. ارتباط را با Rawcap شنود کنید. آیا نام کاربری و پسورد قابل‌خواندن است؟

۳-۳-۱- پروتکل HTTP

۱. عمل شنود را آغاز کنید، مرورگر را باز کرده و به آدرس http://aut.ac.ir بروید. شنود را متوقف کرده و بسته‌ها را بررسی کنید:

۲. بر روی یکی از بسته‌های پروتکل HTTP کلیک راست کرده و Follow HTTP Stream را انتخاب کنید. اگر Wireshark شما این گزینه را ندارد آن را به روز کنید.

۳. بر روی اولین بسته در پنجره باز شده کلیک کنید. بخش های مختلف پروتکل HTTP را مشاهده کنید. مقدار بخش Connection چیست؟ درخواست HTTP از نوع GET بوده است یا از نوع POST؟ مقدار User Agent چیست؟ به نظر شما این مقدار بیانگر چه چیزی است؟

۴. در پنجره باز شده، بسته هایی با پروتکل TCP هم مشخص شده است. اولین بسته را انتخاب کنید. سپس مقدار Flags در پروتکل TCP را مشاهده کنید. چه مقادیری برای این بسته تنظیم شده است؟

۴-۳-۱- پروتکل FTP

۱. عمل شنود را آغاز کرده و مرورگر را باز کرده و به آدرس ftp://ftp.lip6.fr/ بروید. شنود را متوقف کنید. یک بسته مربوط به پروتکل FTP را انتخاب کرده، بر روی آن کلیک راست کنید و Follow TCP Stream را انتخاب کنید.

۲. پروتکل لایه Transport استفاده شده برای این بسته ها چیست؟ آدرس پورت مبدا و مقصد ارتباط را مشخص کنید.

۳. در یکی از بسته ها مقدار Username و در بسته دیگر مقدار Password به سمت سرور ارسال شده است. این مقادیر را مشخص کنید.