**نحوه نصب OpenSSL**

OpenSSL

OpenSSL یک بسته نرم افزاری از (Open Source Initiative(OSI است، به این معنی که می توانید از آن در اهداف تجاری یا غیر تجاری استفاده کنید. می توانید این نرم افزار را از وب سایت www.openssl.org دریافت کنید.

بر خلاف سایر بسته های نرم افزاری، این فایل حاوی تمام چیزهای مورد نیاز برای نصب OpenSSL بر روی پلات فرم های زیر است:

1. UNIX
2. LINUX
3. Open VMS
4. Windows
5. MacOS

اگر در حال استفاده از UNIX/LINUX هستید، می توانید با استفاده از دستورات زیر مبادرت به استخراج فایل ها و زیر شاخه ها بر روی سیستم خود کنید:

gzip –d openssl-0.9.6c.tar.gz

tar –xvf opens-0.9.6c.tar

این دو دستور مبادرت به استخراج تمام فایل ها و زیر شاخه های مرتبط در شاخه ای به نام openssl-0.9.6c می کند. گاهی اوقات می توانید از یک دستور استفاده کنید.

Tar –zxvf openssl-0.9.6c.tar.gz

کاربران ویندوز می توانند از winzip یا winrar برای استخراج تمام فایل ها به شاخه مقصد استفاده کنند.

برای استفاده از این بسته (پکیج)، نیاز به بسته های زیر دارید:

Perl5

کامپایلر ANSI C مانند gcc یا cc با محیط توسعه دهنده.

فرض کنید که در حال استفاده از سیستم UNIX/LINUX هستید و در درون شاخه OpenSSL می باشید. می توانید با استفاده از دو دستور زیر برای ایجاد و نصب موقت بسته بر روی سیستم خود استفاده کنی:

$./config

$make

عبارات فوق کتابخانه ها libcrypto.a و libssl.z و برنامه خط دستور openssl را ایجاد می کنند.

برنامه خط دستور در زیر شاخه apps ذخیره می گردد. پس از ایجاد بسته، باید قبل از نصب دایم آن بر روی سیستم، آن را تست کنید. می توان کتابخانه ها را توسط عبارات زیر تست کرد:

$make test

OpenSSL یک بسته نرم افزاری پیچیده است، حتی تست آن دو صفحه کامل را در بر می گیرد. تست را برای این انجام می دهیم که آیا کتابخانه ها قادر به ایجاد کلیدهای RSA و انجام تصدیق سرویس دهنده-سرویس گیرنده هستند یا خیر. اگر همه چیز مرتب باشد، پیغام “passed all test” در انتهای صفحه ظاهر خواهد شد. در این مورد، می توانیم از دستور زیر برای نصب بسته استفاده کنیم:

$make install

در کنار سایر موارد، این دستور زیر شاخه های زیر را تحت شاخه اصلی openssl-0.9.6c ایجاد می کند:

Certs در ابتدای کار تهی بوده و مکان پیش فرض برای فایل های گواهینامه است.

Private در ابتدای کار تهی بوده و مکان پیش فرض برای فایل های کلید خروجی است.

Bin حاوی openssl باینری و چند یوتیلیتی دیگر است.

Include/openssl حاوی فایل های سرآیند در صورت نیاز به کامپایل برنامه ها با libcrypto یا libssl.library است.

Lib حاوی خود فایل های کتابخانه OpenSSL است.

برای اکثر کاربران ، برنامه خط دستور openssl و گواهینامه ابزار های ضروری برای کار با SSL هستند. برای برنامه نویسان، فایل های سرآیند در شاخه include/openssl و کتابخانه ها ، کامپونت های مهمی در ایجاد برنامه های SSL هستند.

اگر از سیستم ویندوز استفاده می کنید، زیر شاخه یا پوشه پیش فرض ms تحت پوشه Openssl0.9.8r نام دارد. برای کامپایل OpenSSL تحت ویندوز، نیاز به بسته Perl برای Win32 است. چنین بسته ای در سایت www.activestate.com قرار داده شده است که آن را می توانید از لینک www.activestate.com/activeperl دریافت کنید. همچنین به یکی از کامپایلر های زیر نیاز دارید:

(++Visual C++ (VC

Borland C

(GNUC (Mingw32 or Cygwin32

در اینجا فقط به توضیح نحوه کامپایل OpenSSL با Visual C++ می پردازیم. ابتدا، برنامه Perl را برای پیکربندی OpenSSL با VC++ اجرا می کنیم:

Perl Configure vc-win32

گام بعدی ایجاد makefile اختصاصی Visual C++ توسط دستور زیر است:

Ms\do\_ms

این دستور فایل do\_ms.bat در شاخه ms را اجرا کرده و به دنبال آن تمام فایل های make برای Visual C++ ایجاد می شوند. اکنون می توانید نرم افزار را با استفاده از nmake کامپایل نمایید:

nmake –f ms\ntdll.mak

مجددا فرض می کنیم تمام دستورات در شاخه Openssl0.9.8r تایپ شده اند. اگر همه چیز به خوبی پیش برود، تمام (Dynamic Linked Libraries) DLL ها و فایل های اجرایی در شاخه out32dll ایجاد خواهند شد. حال می توانیم OpenSSL موجود در out32dll را اجرا کنیم. برای مثال، می توانید کتابخانه ها و نرم افزار را توسط

cd out32dll

..\ms\test

آزمایش کنید