Lab 2.4: Digital Certificates

1 Introduction

No	Description	Result
1	From: `http://asecuritysite.com/encryption/digitalcert` Open up certificate 1 and identify the following.	Serial number: Effective date: Name: Issuer: What is CN used for: What is ON used for: What is O used for: What is L used for:
2	Now open-up the ZIP file for the certificate, and view the CER file.	What other information can you gain from the certificate: What is the size of the public key: Which hashing method has been used: Is the certificate trusted on your system: [Yes][No]

3	For Example 2 to Example 6. Complete the following table:	

Cert	**Organisation (Issued to)**	**Date range when valid**	**Size of public key**	**Issuer**	**Root CA**	**Hash method**	**Is it trusted?**
1							
2							
3							
4							
5							
6							

2 PFX files

We have a root certificate authority of My Global Corp, which is based in Washington, US, and the administrator is admin@myglobalcorp.com and we are going to issue a certificate to My Little Corp, which is based in Glasgow, UK, and the administrator is admin@mylittlecorp.com.

No	Description	Result
1	We will now view some PFX certificate files, and which are protected with a password: `http://asecuritysite.com/encryption/digitalcert2`	For Certificate 1, can you open it in the Web browser with an incorrect password: Now enter “apples” as a password, and record some of the key details of the certificate: Now repeat for Certificate 2:
2	Now with the PFX files (contained in the ZIP files from the Web site), try and import them onto your computer. Try to enter an incorrect password first, and observe the message.	Was the import successful? If successful, outline some of the details of the certificates:

3 Creating certificates

Now we will create our own self-signed certificates.

No	Description	Result
1	Create your own certificate from: `http://asecuritysite.com/encryption/createcert` Add in your own details.	View the certificate, and verify some of the details on the certificate. Can you view the DER file?
2	Now download the certificate (CER) onto your Windows host, and see if you can import it.	Do you manage to import the certificate? If so, what are some of the details on the certificate:

4 Creating a self signed certificate

You will be assigned a folder in vCentre. Navigate to Production->crypto->netxx and then startup your Kali instance.

We have a root certificate authority of My Global Corp, which is based in Washington, US, and the administrator is admin@myglobalcorp.com and we are going to issue a certificate to My Little Corp, which is based in Glasgow, UK, and the administrator is admin@mylittlecorp.com.

No	Description	Result
1	On Kali, login and get an IP address using: `sudo dhclient eth0`	
2	Create your RSA key pair with: `openssl genrsa -out ca.key 2048`	How many years will the certificate be valid for?

	Next create a self-signed root CA certificate ca.crt for My Little Corp: `openssl req -new -x509 -days 1826 -key ca.key -out ca.crt`	Which details have you entered:
3	Next go to Places, and from your Home folder, open up ca.crt and view the details of the certificate.	Which Key Algorithm has been used: Which hashing methods have been used: When does the certificate expire: Who is it verified by: Who has it been issued to:

4	Next we will create a subordinate CA (My Little Corp), and which will be used for the signing of the certificate. First, generate the key:
	
	`openssl genrsa -out ia.key 2048`
	
	Next we will request a certificate for our newly created subordinate CA:
	
	`openssl req -new -key ia.key -out ia.csr`
		View the newly created certificate.
		
		When does it expire:
		
		Who is the subject of the certificate:
		
		Which is their country:
		
		Who signed the certificate:
		
		Which is their country:

	We can then create a **certificate from the subordinate CA** certificate and **signed by the root CA**. `openssl x509 -req -days 730 -in ia.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out ia.crt`	What is the serial number of the certificate: Check the serial number for the root certificate. What is its serial number:
5	If we want to use this certificate to digitally sign files and verify the signatures, we need to convert it to a PKCS12 file: `openssl pkcs12 -export -out ia.p12 -inkey ia.key -in ia.crt -chain -CAfile ca.crt`	Can you view ia.p12 in a text edit?

6	The crt format is in encoded in binary. If we want to export to a Base64 format, we can use DER:
	
	`openssl x509 -inform pem -outform pem -in ca.crt -out ca.cer`
	
	and for My Little Corp:
	
	`openssl x509 -inform pem -outform pem -in ia.crt -out ia.cer`
		View each of the output files in a text editor (ca.cer and then ia.cer). What can you observe from the format:
		
		Which are the standard headers and footers used: