# Security 1 Lab

## Installing Command-Line Hash Generators and Comparing Hashes

*In this project, you download different command-line hash generators to compare hash values.*

1. Use your Web browser to go to https://kevincurran.org/com320/labs/md5deep.zip

2. Download this zip archive.

3. Using Windows Explorer, navigate to the location of the downloaded file. Right-click the file and then click **Extract All** to extract the files.

4. **Create** a Microsoft Word document with the line below:

> *Now is the time for all good men to come to the aid of their country.*

5. Save the document as **Country1.docx** in the directory containing files and then close the document.

6. Start a command prompt by clicking **Start**, entering **cmd**, and then pressing **Enter**.

7. *Navigate* to the location of the downloaded files.

8. Enter **MD5DEEP64 Country1.docx to** start the application that creates an MD5 hash of Country1.docx and then press Enter. What is the length of this hash? *(note: If you are not working on a 64 bit machine, then simply run the MD5deep.exe 32 bit version).*

9. Now enter **MD5DEEP64 MD5DEEP.TXT** to start the application that creates an MD5 hash of the accompanying documentation file MD5DEEP.TXT and then press Enter. What is the length of this hash? Compare it to the hash of Country1.docx. What does this tell you about the strength of the MD5 hash?

10. Start Microsoft Word and then **open** Country1.docx.

11. Remove the period at the end of the sentence so it says *Now is the time for all good men to come to the aid of their country* and then **save** the document as **Country2.docx** in the directory that contains the files. Close the document.

12. At the command prompt, enter **MD5DEEP64 Country2.docx** to start the application that creates an MD5 hash of Country2.docx and then press Enter. What difference does removing the period make to the hash?

13. Return to the command prompt and perform the same comparisons of Country1.docx and Country2.docx using **sha1deep.exe** (SHA-1), **sha2S6deep.exe** (SI·IA—25 6), and **whirlpooldeep.exe** (Whirlpool). What observations can you make regarding the length of the hashes between Country1.docx and Country2.docx for each hash algorithm? What do you observe regarding the differences between hash algorithms (compare MD5 with SHA—1, SHA—256 with Whirlpool, and so on)? *(Note - you may need to run64 bit versions)*

14. Enter Exit at the command prompt.

## Installing GUI Hash Generators and Comparing Hashes

*In this project, you download a GUI hash generator and compare the results of various hashes.*

1. Download Hash Tab for Windows from here : https://kevincurran.org/com320/labs/hashtab.exe

2. Follow the default instructions to **install** Hash Tab.

3. Click the right mouse button on the Windows **Start** icon.

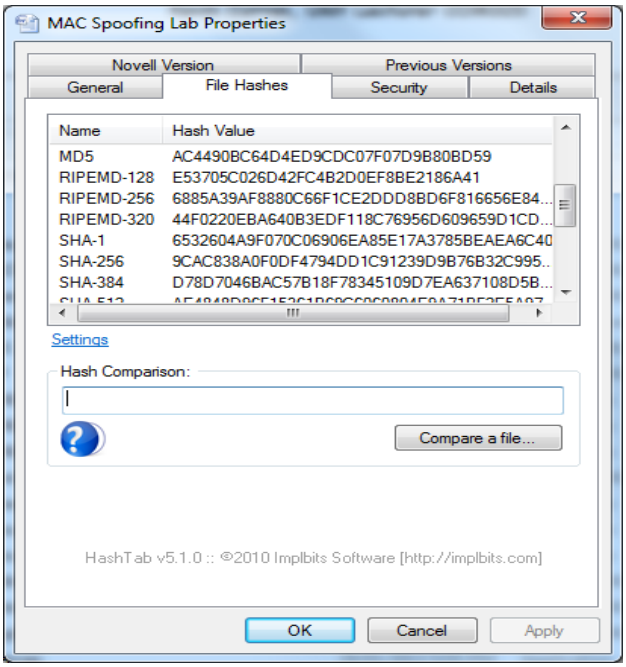
4. Click **Open Windows Explorer**.

5. Navigate to the document **Country1.docx**.

6. Click once on **Country1.docx** and then right-click.

7. Click **Properties**.

8. Notice that there is a new tab, File Hashes. **Click this tab** to display the hashes for this file, as shown below.




10. Right click and select **Click Settings.**

11. Click the **Select All** button.

12. Click **OK**.

13. Scroll through the different hash values generated.

14. Click **Compare a file**.

15. Navigate to the file **Country2.docx** and then click **OK**.

16. A hash is generated on this file. what tells you that the hashes are not the same?

17. Which program would you prefer to use?

18. Close all windows.

## Viewing Digital Certificates

1. Visit a site such as http://www.gs4.com/ in your Chrome browser

2. Note that there is **no padlock** in the browser address bar to left of URL. This indicates that no certificates are used for this site. To verify this, click Page and then Properties. The Protocol is HTTP and the connection is Not Encrypted. Why do you think digital certificates are not used here? Should they be?

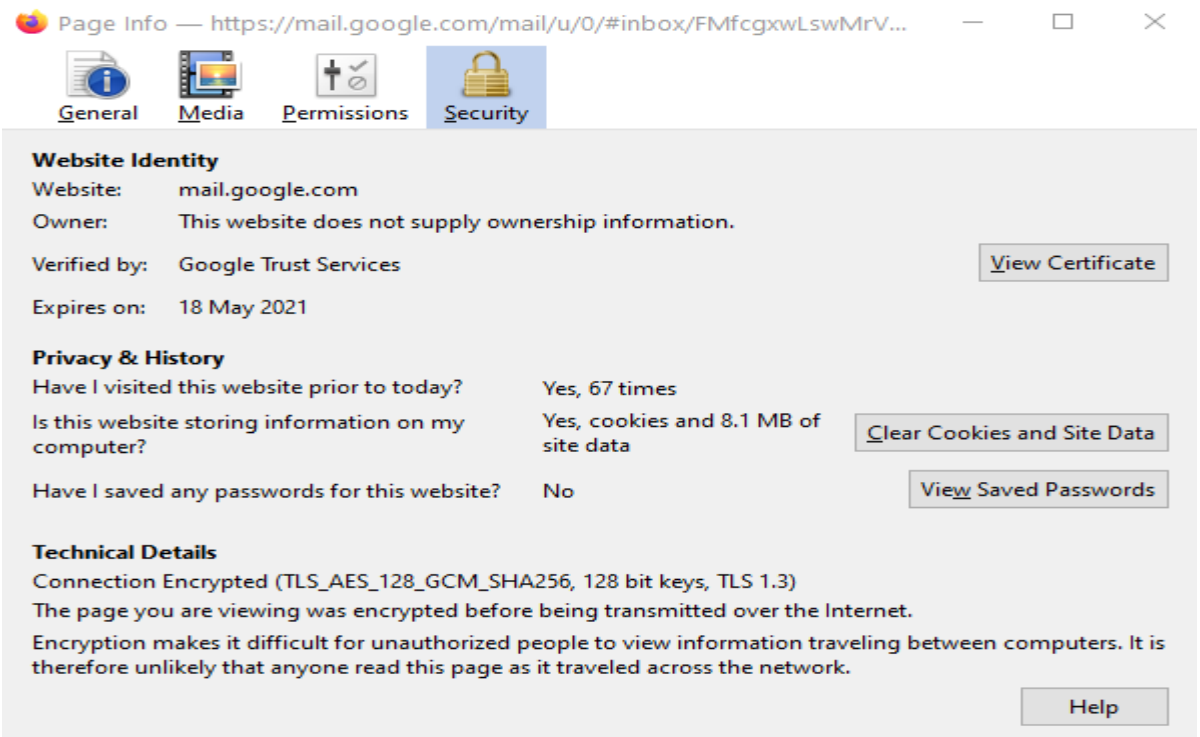
3. Click the **Certificates** button. What message appears? Click OK and then click OK in the Properties dialog box.

4. Now use your Web browser to go to **gmail.google.com**. This is the Web interface to the Google e-mail facility. What protocol is being used (notice what appears before the :// in the address)? Why did that automatically occur? What is different about the information exchanged through e-mail and through a search engine?

5 . Note the padlock icon in the browser address bar. Click the padlock icon to View the Website Identification window. In Chrome, then click the **Connection tab**, and select "Certificate Information" link. *(note, in other browsers you would simply click "**More Information**" in the dropdown).*

6. Click View **certificates**. Note the general information displayed under the General tab.

8. Now click **Connection Secure** and click the **More Information** tab. The fields are displayed for this X.509 digital certificate.



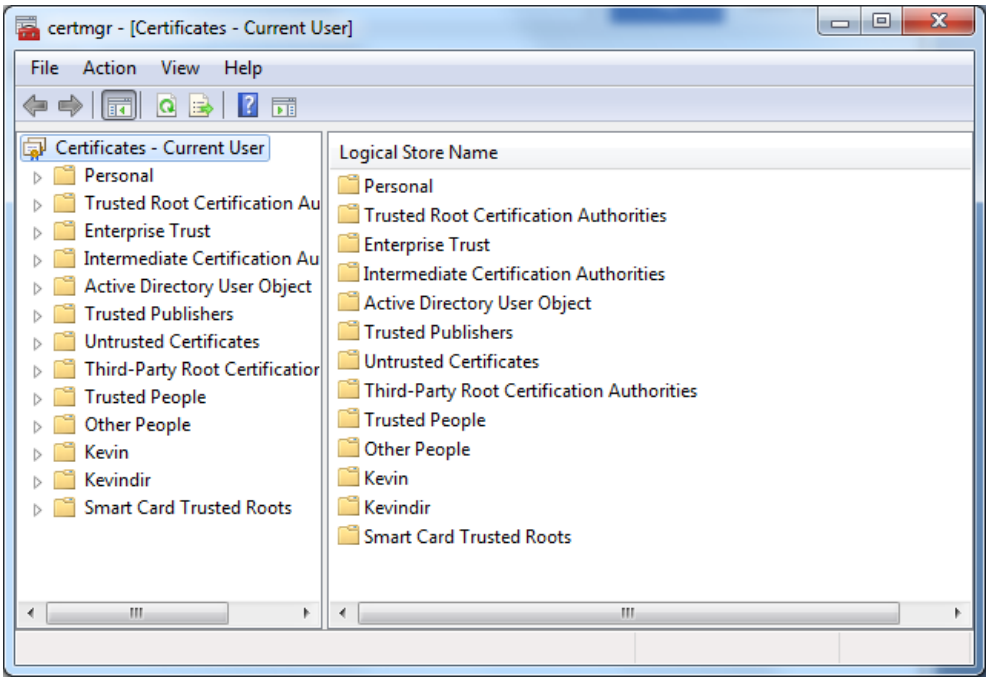

9. Explore the information there.

## Viewing Digital Certificate Revocation Lists (CRL) and Untrusted Certificates

*Revoked digital certificates are listed in a Certificate Revocation List (CRL), which can be accessed to check the certificate status of other users. Here you view the CRL and any untrusted certificates on your computer.*

1. Type the **Windows Key & R** to bring up the **Run Dialog**.

2. Type **CERTMGR.MSC** and then press Enter. You should see a popup similar to below:




3. In the left pane, expand **Trusted Root Certification Authorities**.

4. In the right pane, double-click **Certificates**. These are the CAs approved for this computer. »

5. In the left pane, expand **Intermediate Certification Authorities**.

6. Click Certificates to view the intermediate CAs.

7. Click **Certification Revocation List**.

8. In the right pane, all revoked certificates are displayed. Select a revoked certificate and double—click it.

9. Double-click one of the revoked certificates. Read the information about it and click fields for more detail if necessary. Why do you think this certificate has been revoked? Close the Certificate Revocation List by clicking the **OK** button.

10. In the left pane, expand Untrusted Certificates.

11. Click Certificates. The certificates that are no longer trusted are listed in the right pane.

12. Double-click one of the **untrusted certificates**. Read the information about it and click fields for more detail if necessary. Why do you think this certificate is no longer trusted?

13. Click **OK** to close the Certificate dialog box.

14. Close all windows.

## Downloading and Installing a Digital Certificate

In this project, you download and install a free e-mail digital certificate.

1. Go to https://www.comodo.com/home/email-security/free-email-certificate.php.
*(Note: It is not unusual for Web sites to change the location where files are stored. If the preceding URL no longer functions, then open a search engine and search for "Comodo Free Secure Email Certificate")*

2. Click **Sign Up Now**.

3. You will be taken to the Application for Secure Email Certificate.

4. Enter the requested information. Based on the information requested, how secure would you rate this certificate? Under which circumstances would you trust it? Why? Click **I accept** and then click **Next**.

5. If a Web Access Confirmation dialog box opens, click **Yes**.

6. Open your e-mail account that you entered in the application and **open the e-mail** from Comodo.

7. Click **Click & Install Comodo Email Certificate**.

8. Follow the instructions to install the certificate on the computer by **accepting all default settings**.

9. Verify that the certificate is installed. Click **Start**, type **Run,** and then press **Enter**.

10. Type **CERTMGR.MSC** and then press **Enter**.

11. In the left pane, expand **Personal**.

12. In the right pane, double-click **Certificates**. Your personal certificate should be displayed.

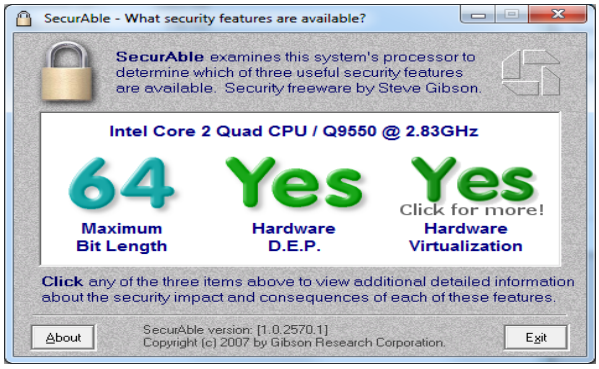
13. Close all windows.

# Configure Microsoft Windows Data Execution Prevention (DEP)

*Data Execution Prevention (DEP) is a Microsoft Windows feature that prevents attackers from using buffer overflow to execute malware. Most modern CPUs support an NX (No eXecute) bit to designate a part of memory for containing only data. An attacker who launches a buffer overflow attack to change the "return address" to point to his malware code stored in the data area of memory would be defeated because DEP will not allow code in the memory area to be executed. If an older computer processor does not support NX, then a weaker software-enforced DEP will be enabled by Windows. Software-enforced DEP protects only limited system binaries and is not the same as NX DEP. DEP provides an additional degree of protection that reduces the risk of buffer overflows. In this lab, you will determine if a Microsoft Windows system can run DEP. If it can, you learn how to configure DEP.*

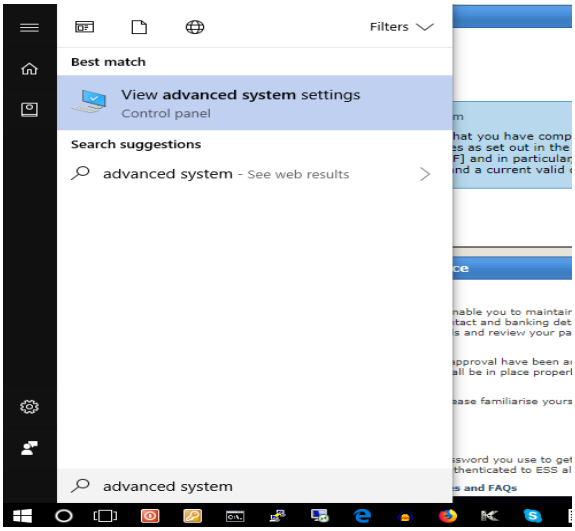
1. The first step is to determine if the computer supports NX. Use your Web browser to go to www.grc.com/securable. Click Download now and follow the default settings to install the application on your computer. (Note - *If you are no longer able to access the program through the preceding URL, then use a search engine to search for "GRC securable".)*

2. Double-click **SecurAble** to launch the program, as shown below.

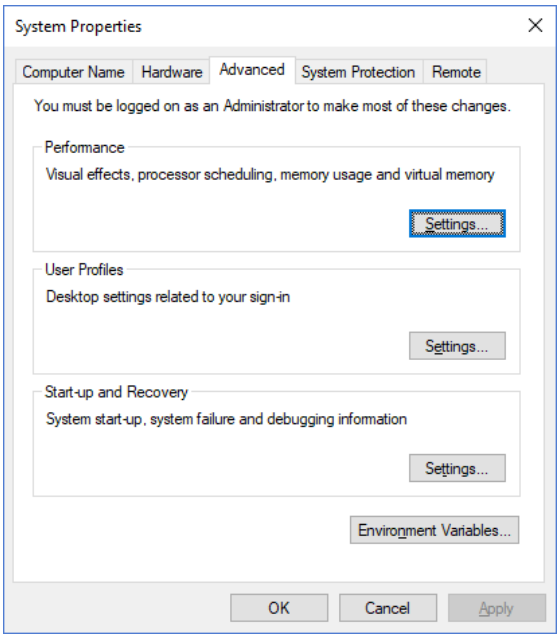



If it reports that Hardware D.E.P. is "No," then that computer's processor does not support NX. **Close the SecurAble application.**

3. The next step is to check the DEP settings in Microsoft Windows. Click **Windows Key** and type *Advanced Systems Settings.* (see below)



4. You should then see the Systems Property Window (see below).




6. Click **Advanced** tab & click **Settings** under **Performance**. Click the **Data Execution Prevention** tab.

8. Windows supports two levels of DEP controls: DEP enabled for only Windows programs and services and DEP enabled for Windows programs and services as well as all other application programs and services. If the configuration is set to *Turn on DEP for essential Windows programs and services only,* then click **Turn on DEP for all Windows programs and services except those I select**. This will provide full protection to all programs.

9. If an application does not function properly, it may be necessary to make an exception for that application and not have DEP protect it. If this is necessary, click the **Add** button and then search for the program. Click the program to add it to the exception list.