Unit 7 Lab

Secure Data Destruction

1. **In your own words, how did the "shred" function work, and why is it better than simply "deleting" a file? What is the advantage of the shred function over the other items on the list? What is its limitation over the more advanced methods listed in the article like the Wipe command?**

Shred is a program that will overwrite your files in a way that makes them very difficult to recover by a third-party program. Normally, when you delete a file, that portion of the disk is marked as being ready for another file to be written to it, but the data is still there. The wipe command securely erases files from magnetic memory and thereby making it impossible to recover deleted files or directory content. Wiping is better because it actually deletes the file, shredding gives you the option but doesn't always do it like how wiping does it.

What is a BIOS?

1. **In your own words, what is a BIOS? How could it be used to change the OS environment in a computer? (To practice the installation of environmental controls, contact your instructor.)**

BIOS is a program pre-installed on Windows-based computers (not on Macs) that the computer uses to start up. It allows you to choose which device to boot off of, change the boot priority, change hardware settings, etc.

Drive Encryption

1. **In what ways is encryption similar across all three operating systems? In which ways is it different? Provide at least one example each of a similarity and a difference.**

All three operating systems allow you to encrypt the **FULL** startup disk. However, the utility to do so is not pre-installed on every one of the three major operating systems. For example, you have to install it on Linux but in Windows it is already installed (you just have to enable it).

2. **Using your virtual OS from Unit 2's Activity and the instructions in the first link above, apply drive encryption to a USB flash drive. (You may want to use a blank drive or a drive that doesn't have a lot of important files on it.) Why did the instructions require you to back up the drive? What limitations do you encounter when using your newly encrypted USB drive? How might you "decrypt"/unencrypt the USB drive in the future if you wanted to use it for something else?**

The instructions required me to backup the drive, because if I didn't I would run the risk of losing my data if something were to go wrong. The limitation is that the encryption will only be able to be read by other Linux systems, not by another Windows or macOS system. If you wanted to decrypt the drive, you could install something called Dislocker which can decrypt the drive.

PGP Encryption

1. In terms of encryption and security, what are the two features of PGP?

PGP encryption uses a combination of two forms of encryption: *symmetric key encryption*, and *public-key encryption*.

2. Name at least one advantage and disadvantage each of using OpenPGP.

A disadvantage of PGP is compatibility issues. Both the sender and the receiver must have compatible versions of PGP software or the information either will not be decoded or will be decoded by only one party. An advantage is that you can be certain who the email is from and who it is for.

Application Security

1. Provide three distinct methods or approaches for improving application security for your chosen app. The method can be "high-level," dealing with your overall approach to app security, or it can focus on nitty-gritty details.

a. Ask professionals to "attack" your application (to test the security of the application)

b. Scan your website for vulnerabilities often

c. Keep everything up to date

d. Have a very strong password policy in place

PKI and Certificates

1. Discuss at least one "best practice" to consider when implementing a PKI, and why that practice makes sense.

- The operating system should be without Graphical Shell (Core).
- Make a hardening of your server.
- Use a specific administrator password.

2. What is a common use of PKI in business?

PKI can also be used for corporate databases, signatures of electronic documents and such forms protection as messaging protect, protect mobile devices, USB protection, Windows Server Update Services, Active Directory, etc.

3. What is the relationship between PKI and Certificates of Authority?

The purpose of a PKI is to securely associate a key with an entity. The trusted party signing the document associating the key with the device is called a certificate authority (CA).

4. **Using the provided links as a starting point, choose a program you have access to that allows you to create and view a CA (e.g., most Microsoft Office programs or Adobe's PDF reader). What are the steps required to create a CA for that file—specifically, what was one major "hurdle" that prevented you from just telling the program to encrypt the file?**

Microsoft Outlook 2016 supports two encryption options, which include **S/MIME encryption** and **Microsoft 365 Message Encryption**.

Send a Message with S/MIME:

a. On the tools Menu, click Accounts
b. Click the account that you want to send an encrypted message from and select **Advanced > Security**.
c. In Certificate, select the certificate that you want to use.
d. Click OK, and then close the Accounts dialog box.
e. In an email message, choose Options, select Encrypt and pack Encrypt with S/MIME option from the drop-down.
f. In an email message, select **Options > Security > Encrypt Message.**
g. Finish composing your message, and then click **Send**.

Send a Digitally Signed Message:

1. On the Tools menu, click Accounts
2. Click the account that you want to send a digitally signed message from, and select Advanced > Security
3. In Certificate, select the certificate that you want to use. You'll only see those certificates that you've added to the keychain for your Mac OSX user account and those certificates that are valid for digital signing or encryption
4. To make sure that your digitally signed messages can be opened by all recipients, even if they do not have an S/MIME mail application and can't verify the certificate, select Send digitally signed messages as clear text.

To allow your recipients to send encrypted messages to you, make sure that you've selected your signing and encryption certificates, and then select Include my certificates in signed messages.

5. Click OK, and then close the Accounts dialog box
6. In an email message, select **Options > Security > Digitally Sign Message**.
7. Finish composing your message, and then click **Send**.

Send a Message with Microsoft 365 Message Encryption:

1. In an email message, choose Options, select Encrypt and pick the encryption option that has the restrictions you'd like to enforce, such as Do Not Forward or Encrypt-Only.
2. In an email message, select Options > Permissions and pick the encryption option that has the restrictions you'd like to enforce, such as Do Not Forward.

3. **Why do you need to have the password for your "keyring" to be able to revoke a key? What solution does the site offer to this dilemma?**

   This is a verification step so that anyone can't just do this. "The way to avoid this dilemma is to create a key revocation certificate at the same time that you generate your key pair. Put the revocation certificate away in a safe place and you will have it available should the need arise."

4. **Which kind of key can be restored or backed up at any time? For the other kind of key, what are the two limited circumstances in which it can be backed up?**

   The Certificate Services private keys can be backed up or restored. There are only two cases in which a Certificate Services private key must be backed up. The first case is after the installation of Certificate Services. The second case is after any renewal operation of the Certificate Services certificate.