# *IT Security (420-F30-HR)*

# *Lab 03b – Risk Register, Data at Rest*

Date assigned: Friday, Feb 7

Date Due: Tuesday, Feb 11 – start of class

**Objectives:**

Learn:

1. Understand how to secure data at rest
2. Calculate effort required for brute force cracking
3. Practice the implementation of a Risk Register

# Data at Rest - Physical

## Read about Manning’s theft of US military secrets [here](https://www.theguardian.com/world/2010/nov/28/how-us-embassy-cables-leaked). How did she steal the information?

## By downloading classified files onto a CD labeled as “Lady Gaga”. She afterwards transferred the files and gave them to WikiLeaks

## What 4 steps do the US military have to mitigate this type of theft?

1. Restricting access
2. Monitoring systems
3. Blocking removable media
4. Increasing security training

## Research: definition of “data exfiltration”. Provide the definition and explain how it applies to this case.

Data exfiltration is the unauthorized transfer of data from a computer or network to an external location.

Chelsea Manning used data exfiltration by secretly copying military files onto a CD.

# Data at Rest - Encryption

## What is the purpose of BitLocker for Windows 10 or Windows 11 machines?

## BitLocker is used to encrypt the entire hard drive, protecting data from unauthorized access if the device is lost or stolen.

## Assuming your data is on an encrypted disk. Put brief justification for your answer in the appropriate Column

|  |  |  |
| --- | --- | --- |
| Scenario | Files Protected/Mitigated | Files Not protection |
| Whole PC is stolen, knows your login password |  | They can log in and access files |
| Hard drive is taken out and stolen. Rest of the PC is destroyed. | BitLocker prevents access without key | If not enabled, can be accessed by attaching drive to another PC. |
| User logged in and left the PC unlocked (from the OS point of view) |  | The attacker can use the unlocked session to access files |

## Assuming your data is on an encrypted NAS ([like Synology](https://linuxhint.com/setup-encryption-synology-nas/)). Put brief justification for your answer in the appropriate Column

|  |  |  |
| --- | --- | --- |
| Scenario | NAS Files Protected/Mitigated | NAS Files No protection |
| Whole NAS is stolen | If NAS encryption is enabled and the device is powered off, files are protected. | If not enabled, the attacker can access files by inserting the drives into another system. |
| PC (with key) and NAS stolen |  | The files are not protected since the key is available. |
| User logged in and left the PC unlocked (from the OS point of view). Encrypted folder is mounted. |  | Files are not protected since they are already decrypted and accessible. |

## Is a Windows 11 PC storage encrypted by default? (provide your sources).

It depends on the version of Windows 11 and the hardware.

* **Windows 11 Home:** Device encryption is enabled by default **only** if the PC meets specific hardware requirements (TPM 2.0, Secure Boot, and modern standby).
* **Windows 11 Pro & Enterprise:** BitLocker encryption is available but must be manually enabled.

**Sources:**

[Microsoft Support: Device Encryption](https://support.microsoft.com/en-us/windows/device-encryption-in-windows-10-58797a7b-5718-4e99-0bc7-f3c5a5f37c61)

[Microsoft Learn: BitLocker Overview](https://learn.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview)

## Is the PC you’re currently on have encryptions turned on? (provide your sources).

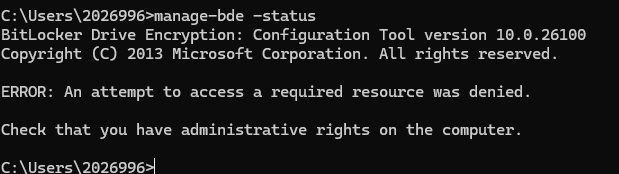
To check if your PC has encryption enabled:

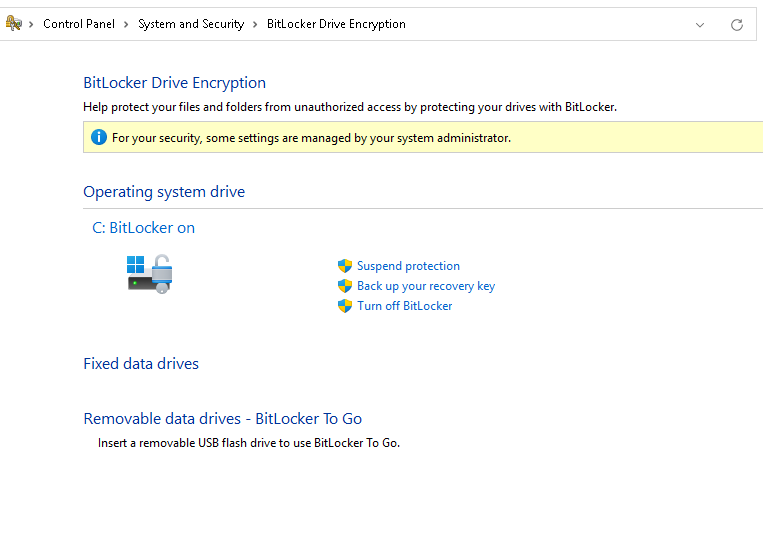
1. Open Settings, Privacy & Security, Device Encryption (for Windows Home).
2. Or, open Control Panel → BitLocker Drive Encryption (for Windows Pro & Enterprise).
3. Run the following command in Command Prompt:

manage-bde -status

1. Take a screenshot of the results and attach it to verify.

* ChatGPT





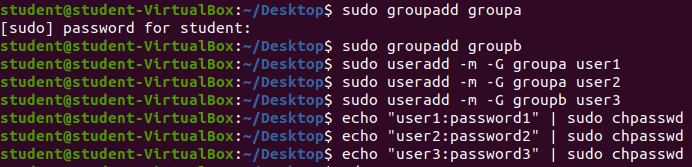
# Data at Rest – ACL/Permissions

## Log onto a linux machine (Kali, LinuxBox1 or LinuxBox2), create the following (show me the Linux commands, you must make groups and users):

user1 belongs to groupa

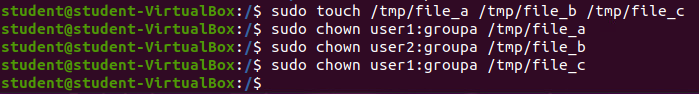
user2 belongs to groupa

user3 belongs to groupb



Create the following in /tmp/

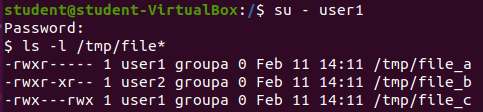
|  |  |  |  |
| --- | --- | --- | --- |
| File/Dir | user1 | user2 | user3 |
| file\_a | Can do anything | Read only | No permissions |
| file\_b | Read and execute | Can do anything | Read only |
| file\_c | Can do anything | No permissions | Can do anything |

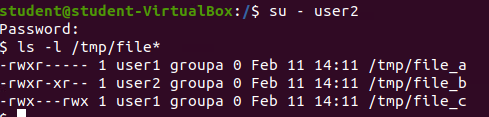


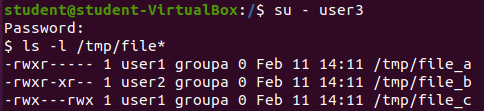


Login as each user to validate the permissions.

Hints: chown, chgroup, adduser, addgrp, chmod, sudo







# Data at Rest – Digital signatures

We will use the md5 hash to generate a digital signature. See [here](https://www.tutorialspoint.com/unix_commands/md5sum.htm) for details on the command.

## Log onto a linux box on your VDI setup, create a big file

cd /

ls -lR > ~/data.txt

This will leave a large file called data.txt in your home directory.

cd

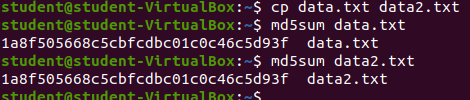
take a look at the contents of data.txt

cp data.txt data2.txt

how to tell both files are identical?

md5sum data.txt

md5sum data2.txt



1. challenge: can you change data2.txt so that the contents are different, but the md5 calculation is different? Change just one character and see what difference it makes to the md5 output.

After changing one letter:



1. Explain how would you use this feature to convince someone that the file you sent is untampered with?

You can user this feature to see if the hashes match, proving it has not been tampered with.

Before sending file -> calculate MD5 hash and share with recipient. Recipient downloads file and runs md5sum. If it matches, the file is safe

1. Which elements of the CIA triad do digital signatures address and how?

Integrity: Ensures data has not been altered. Even a single character change results in a completely different hash.

# Brute Force crack

Time for some math to understand the scale of brute force cracking and demonstrate your math skills:

|  |  |
| --- | --- |
| Scenario | Answer |
| Assuming a password of only 1 character [a-z] | 26 |
| Assuming a password of 2 characters [a-z] | 676 |
| Assuming a password of N characters [a-z] | 26^n |
| Password of 7 [a-z] | 26^7 8031810178 |
| Assuming 10M combinations can be brute forced every second, how long would it take to crack a Password of 7 [a-z], worst case, in minutes | 13 minutes |
| Assuming 10M combinations can be brute forced every second, how long would it take to crack a Password of 7 [a-zA-Z], worst case, in hours | 52^7 = 1.028071703e12/10000000/60/60 28 hours |

**Marking Scheme**

|  |  |  |
| --- | --- | --- |
|  | **Mark** | **Out of** |
| **Part A: Risk Register** |  |  |
| Completed |  | 8 |
| Analyze difference |  | 2 |
|  |  |  |
| **Part B: Data At Rest - Physical** |  |  |
| How stolen |  | 2 |
| 4 steps |  | 4 |
| Data exfiltration |  | 2 |
|  |  |  |
| **Part C: Disk encryption** |  |  |
| BitLocker |  | 6 |
| NAS |  | 6 |
|  |  |  |
| **Part D: ACL** |  |  |
| filea (1 pts per user) |  | 3 |
| fileb (1 pts per user) |  | 3 |
| filec (1 pts per user) |  | 3 |
| Commands and output |  | 4 |
|  |  |  |
| **Part E: Data signatures** |  |  |
| Generate files and sigs |  | 2 |
| Alter and compare sigs |  | 2 |
| Tamper detection |  | 2 |
| CIA |  | 2 |
|  |  |  |
| **Part F: Brute Force Crack** |  |  |
| 1 x [a-z] |  | 1 |
| 2 x [a-z] |  | 1 |
| N x [a-z] |  | 4 |
| 7 x [a-z] |  | 2 |
| Time for 7[a-z] |  | 2 |
| Time for 7[a-zA-Z] |  | 2 |
|  |  |  |
| Crossword |  | 10 |
| Handed in properly |  | 4 |
| **Total** |  | **87** |