Identify your role – incident has happened and u r an incident responder

Part A systematic guide, gives u the direction u has to look

Find the entry point of the attacker, the attacker leaves footprints – log files when they laterally move through the system

DC log, corrupted memory file

Use MS excel to filter logs –

Use a forensic tool to analyse the memory dump, to find easter eggs on which u would do the difficult question to do deep analysis

Report U findings to the manager,

Part C – literature review - current attackers, - literature review should be based on findings and how it relates with the current cyber security frameworks –

DC log has encrypted things, decipher it – Github – cyber chef

Investigate the hash scenarios and try to decrypt them and find out

Fstab directory – changes need to be made if it does not allow u to share folders

Forensic analysis tool

SIFT FOUNDATION

Sudo snap install volatility framework

What kind of profile we have, memory dump, get the image info – takes 20 mins to run

At the end will get an ID with windows64 bit profile

First start with log file, convert to excel and identify patterns

Look into the daemon processes and netscan processes

Attack train track / time line should be different, identify it using netscan

Find the easter egg from this to move forward, find malicious things that exist

Get idea for the technical analysis part from this – when u find the time line and easter eggs

There is a function to analyse strings as well