Assignment 1 : **Get To Know Your System** …10 Marks

Download a malware, analyse using sysinternal tools and show

Should be a full investigation on windows

Disk (where is residing, what is accessing, access rights, hidden or unusual files etc),
Registry (persistent? , what else ha it modified in registry?),
Memory (where is it residing) etc,
Processes (what processes impacted, how can we identify, who owns the process, access rights of the process, unusual process etc)
Network (who is it communicating with/ what is it communication, how is it communicationg , unusual open sockets, unusual requests? etc)
Backdoor?
Suspiscious accounts?
Resource Usage

Not necessarily limited to above. How else can we know the footprints of the malware? Creativity pays in marks.

Can be disk based malware/Memory based/ multi-vector or………
Can investigate multiple malwares also (priority is to see multiple impacts from same malware)
Can be a known malware but show the execution with investigation of impact vs original (spanning different impact areas)

Differentiator is the team being able to show impact at multiple levels of the system (complexity matters).

Note:
Should be a full investigation on windows
Two teams should not use same malware (so please keep your malware to yourself)
While taking snapshot of impact please have timestamp+ machine identity part of snapshot. Should be able to show the same on VM in case required.

Submission Guidelines
PDF with filename Team#Assn1.pdf
No Theory description please

Submission Date : 2nd March