**CyberShield Capstone Exercise**

July 2021

**Resources**

LODS Virtual Platform

Kali Linux – Attacker system

Windows 2012 server – Victim system

**Objective**

* To identify a vulnerability on the victim system
* To exploit the vulnerability successfully
* To create a .dll file for later injection (let’s call it evil.dll)
* Identify a process that is running in Windows (e.g. start Notepad.exe)
* Inject the .dll into Notepad.exe successfully.

**Questions**

* What are basic requirements for the attack to be successful?
* What are countermeasures or controls that should be implemented, at a minimum, to ensure that the attack would not succeed?
* Please fill out the Security Assessment Report!

**Hints**

* You may want to explore and use a combination of the following:
  + nmap
  + metasploit
  + msfvenom
  + powersploit