Instructions:

- Students required to have Kali Linux and Windows Server 2012/ Windows 10 to complete the assignment.
- Screenshots of all-important steps are to be captured where preparing the assignment.

---

1. Complete the following task on reconnaissance using Way-back machine https://archive.org/

   i. Show the archival history of following sites

      - Kali.org
      - hackthebox.eu

2. Obtain list of recent Sri Lankan compromised sited using (Minimum 10)

   i. Google Dorks

   ii. http://www.zone-h.org/

   iii. https://mirror-h.org/

3. Clone hackthebox.eu site to your local machine using 'HTTrack' (You may use either windows or Linux (Kali) version) and list out juicy information /materials.

4. Use the Nmap or Zenmap (Kali) and discover followings from 'hackthebox.eu' site,

   i. Open Ports Discovered

   ii. IP Address of the host

   iii. TRACEROUTE output

   iv. Operating System of the Server

5. Perform Zenmap or Nmap scan against windows 2012 server/ Windows 10 and demonstrate following

   i. Port 80 is open (hint: Web should be up and running)

   ii. Port 80 is Closed (hint: incoming traffic to port 80 is closed by firewall)

6. Use the Wireshark packet analyzer tool and illustrate **three-way hand shake** while assessing hackthebox.eu site.

7. Demonstrate (Step by step) Notepad content hiding using 'Snow' steganography tool.

8. Perform following clearing tracks activities on Windows Server 2012,

i. auditpol get

ii. auditpol backup

iii. auditpol clear

iv. auditpol restore

9. Demonstrate how to exploit client-side vulnerability by establishing a VNC session using Kali Linux as the attacker machine and windows Server 2012 as the victim machine.

   Hint: use windows/meterpreter/reverse_tcp

10. Demonstrate, Sniffing Facebook Credentials using Social Engineering Toolkit (SET)