**CT Revision Guide – Part 1**

**Topic 1 – Fundamentals of EH & Service Side Attack**

* Must know
  + **Professional Attributes (Professional Values/Professional Skills) – Lecture 0**
  + **Our Pen-Test Methodology**
  + **Limitations of Pen-Test**
  + **Legal Issues**
  + **Code of Ethics**
  + **Service Side Attack** 
    - **The attack is launched from the client to the listening server. This attack doesn’t need human help at the server end for the exploitation to work and the attack can be launched directly over the network**

**Topic 2 – Initial Pen-Test Project Engagement Activities & Client-Side Attack**

* Must Know
  + **Securing a Pen-Test Project**
  + **Planning Phase and Purpose of Planning**
  + **Main Planning Activities**
    - **Review Scope Document**
    - **Review Rules of Engagement Document**
    - **Create Penetration Test Plan**
    - **Examine Legal Issues**
  + **Client Side Attack**
    - **Exploits weakness found in various applications that are commonly used to penetrate into the target computer system or server**
  + **The difference between Service Side Attack and Client Side Attack.**
    - **Service side attack is attacking the service that runs on the server and client side is attacking the software that runs on the user machine.**

**Topic 3 – Reconnaissance**

* Must know
  + When do you need to do Reconnaissance?
    - To look for Ip addresses that is used by the target organization. Ip address leads to network addresses and host devices
  + Methods to obtain Network IDs
    - Using NSLOOKUP
  + subbrute – why you need it in network and host device penetration testing
    - Helps us to find out the internet domain and sub domain names that the organization use
  + How Shodan works and how to prevent being detected
    - **Shodan works** by requesting connections to every imaginable internet protocol (IP) address on the internet and indexing the information that it gets back from those connection requests. **Shodan** crawls the web for devices using a global network of computers and servers that are running 24/7
    - **Use a VPN when accessing things outside of the network**

**Topic 4 – Scanning and breaking into Network Perimeter Devices**

* Must Know
  + Use of Airgedon and its limitation
  + Alternate method to obtain WPA-PSK encrypt key
    - Evil Twin/Social Engineering
  + Wireless AP Configuration and Security Issues
  + Use of Palo Alto - VM50 VM
  + Brute Force for Credential on Devices providing **Remote Services**

**Topic 5 – Scanning for Internal Host Devices**

* Must know
  + How to obtain Network ID.. include sniffing using wireshark
  + How to make use of arp-scan
    - This is a very fast arp scanner that shows every active IPv4 device on the subnet, it shows all active devices even if they have firewall
    - Arp-scan --localnet
  + How to make use of fping
    - Fping is used to send a ping request to several hosts at once
  + How to make use of nmap
    - Nmap is used to map out the whole network
  + How to identify the function of the device based on the open ports found
  + How to use traceroute command and interpret traceroute output
  + How to map out the devices connected to the router found from the traceroute command output  
     nmap, fping

**Topic 6 – Vulnerabilities Scanning**

* Must Know
  + How to scan for vulnerabilities using NSE
  + How to scan for vulnerabilities using Nessus
  + Advantages of NSE modular approach and Nessus plug-in approach adopted in their software architecture