**KALI LINUX COMMANDS**

**Vulnerability management and scanning**

* Wordpress

Wpscan tool ( to scan wordpress websites)

Wpscan –url <target domain>

Nikto –h <target ip or domain>

**Vulnerability assessement steps**

* Spotting weakness
* Understanding risks
* Deciding priorities – what needs to be attended first
* Boosting security –take action –update /patch
* Regular checkups – va +pt
* Types of vulnerability assessment:

1. **White Box Vulnerability assessment** (pentester is given all info –ip address, codes, internal network details username & passwords)
2. **Black Box Vulnerabiltiy assessment** (pentester is given no info/ very little info about the target to be hacked – checking for outsider attacks).
3. **3rd party tools Vulnerability assessment**  (3rd party softwares, CRM…)
4. **In-house apps** ( in house developed apps)
5. **Network assessment –wifi/wired**

* **Vulnerability management Life Cycle.**

1. Pre engagement = what to do before VA
2. Engagement = actual VA/test happens
3. Post engagement – what to do after VA

* Pre-engagement

1. Understanding the clients\s business
2. Process
3. Landscape – security /missing / how they operate
4. Build of list apps, software –things to test
5. Paperwork + meetings with the client
6. Scheduling: we need written permission