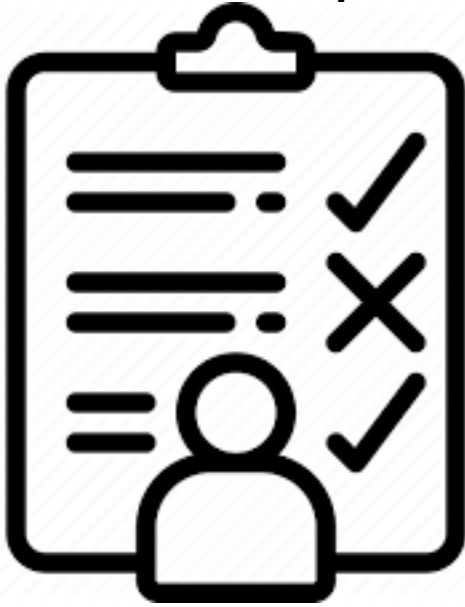


# ***Pentest questionnaire***

## **Pentest Questionnaire**

**This room contains questions related to penetration testing**



### ***[Task 1] Do you know all the answers?***

**Basic questions related to penetration testing**

---

**[# 1] A very popular port scanner used in assessments.**

`nmap`

**[# 2] Flag used to load a list of hosts.**

`-iL`

**[# 3] Command line vulnerability scanner**

`nikto`

**[# 4] Popular packet analyzer tool having a GUI.**

`wireshark`

**[# 5] Online platform to search for exploits.**

`exploit-db`

**[# 6] First phase of the penetration test.**

`reconnaissance`

**[# 7] Common penetration testing framework used across multiple platforms.**

`metasploit`

**[# 8] A vulnerability assessment framework developed by Tenable.**

`nessus`

**[# 9] Automated tool to exploit SQL Injections.**

sqlmap

**[#10] Vulnerability which when exploited can send commands to the operating system.**

os injection

**[#11] A vulnerability which pops an alert box**

xss

**[#12] You do it horizontally and laterally.**

privilege escalation

**[#13] Windows SMB exploit.**

eternal blue

**[#14] Vulnerability by which the attacker can include local files(short name)**

lfi

**[#15] Vulnerability by which the attacker can include remote files(short name)**

rfi