

The Ethical Hacker Methodology

FIVE STAGES:

1st **RECONNAISSANCE** #Information Gathering

- ACTIVE Vs PASSIVE

Passive means search items to google machine, you have just check the company logo or just picture not just visited the actual website not doing active against it

2nd **SCANNING & ENUMERATION** #We use tools such as NMap, Metasploit, NIKTO, etc.

(We are Scan actively that tools against it and looking for open port and vulnerability and different item

And results we are returning also called Enumeration)

3rd **GAINING ACCESS** ("EXPLOITATION")

we gain the access and run the exploit against their clients network and vulnerable service try to gain access the machine or the environment etc.

4th **MAINTAINING ACCESS**

for that required maintain all the access and items open or use

5th **COVERING TRACKS**

we want to delete any logs that you me forget or malware that you have uploaded or (Delete ACCOUNT, or any data you leave)