

FIVE STAGES OF ETHICAL HACKING

Monday, July 26, 2021

1:23 PM

1. RECONASSINCE

a. INFORMATION GATHERING

- i. Active and Passive
- ii. Passive- Going to Google to find employee's names and gaining information(Twitter page, etc)
- iii. Active- Scanning actively to the client (like open ports, seeing versions of the programs running, Finding exploits)

2. SCANNING AND ENUMERATION

- a. Active scanning- Nmap, Nessus, Nikto

3. Gaining Access

- a. Exploitation

4. MAINTAINING ACCESS

5. COVERING TRACKS