

Information Gathering (Reconnaissance)

Passive Recon

Types of Passive Recon

1. Physical/Social

- Location Information
 - Satellite images
 - Drone recon
 - Building layout (badge readers, break areas, security, fencing)
- Job Information
 - Employees (name, job title, phone number, manager, etc.)
 - Pictures (badge photos, desk photos, computer photos, etc.)

2. Web/Host Assessment

- Target Validation
 - WHOIS, nslookup, dnsrecon
 - Finding Subdomains
 - Google Fu, dig, Nmap, Sublist3r, Bluto, crt.sh, etc.
 - Fingerprinting
 - Nmap, Wappalyzer, WhatWeb, BuiltWith, Netcat
 - Data Breaches
 - HaveIBeenPwned, Breach-Parse, WeLeakInfo
-