**Passive Reconnaissance**

1. **Introduction**
2. **Passive Versus Active Recon:**

<https://www.unifiedkillchain.com/>

1. **Whois:**
   * Registrar: Via which registrar was the domain name registered?
   * Contact info of registrant: Name, organization, address, phone, among other things.
   * Creation, update, and expiration dates: When was the domain name first registered?
   * Name Server: Which server to ask to resolve the domain name?
2. **nslookup and dig:**

nslookup OPTIONS DOMAIN\_NAME SERVER

nslookup -type=A tryhackme.com 8.8.8.8

* A 🡪 IPv4 Addresses
* AAAA 🡪 IPv6 Addresses
* CNAME 🡪 Canonical Name
* MX 🡪 Mail Servers
* SOA 🡪 Start of Authority
* TXT 🡪 TXT Records Raw

dig @SERVER DOMAIN\_NAME TYPE

1. **DNSDumpster:**

<https://dnsdumpster.com/>

1. **Shodan.io:**

<https://www.shodan.io/>

<https://tryhackme.com/room/shodan>

1. **Summary:**

<https://tryhackme.com/room/dnsindetail>