Passive Reconnaissance

* **whois** to query WHOIS servers
* **nslookup** to query DNS servers
* **dig** to query DNS servers

Passive reconnaissance activities include many activities, for instance:

* Looking up DNS records of a domain from a public DNS server.
* Checking job ads related to the target website.
* Reading news articles about the target company.

ctive reconnaissance activities include:

Connecting to one of the company servers such as HTTP, FTP, and SMTP.

Calling the company in an attempt to get information (social engineering).

Entering company premises pretending to be a repairman.

| **Query type** | **Result** |
| --- | --- |
| A | IPv4 Addresses |
| AAAA | IPv6 Addresses |
| CNAME | Canonical Name |
| MX | Mail Servers |
| SOA | Start of Authority |
| TXT | TXT Records  A screen shot of a computer  Description automatically generatedA screen shot of a computer  Description automatically generated |

A screenshot of a computer

Description automatically generated

| **Purpose** | **Commandline Example** |
| --- | --- |
| Lookup WHOIS record | **whois tryhackme.com** |
| Lookup DNS A records | **nslookup -type=A tryhackme.com** |
| Lookup DNS MX records at DNS server | **nslookup -type=MX tryhackme.com 1.1.1.1** |
| Lookup DNS TXT records | **nslookup -type=TXT tryhackme.com** |
| Lookup DNS A records | **dig tryhackme.com A** |
| Lookup DNS MX records at DNS server | **dig @1.1.1.1 tryhackme.com MX** |
| Lookup DNS TXT records | **dig tryhackme.com TXT** |

A screenshot of a computer

Description automatically generated