Passive Reconnaissance

Farah Anany

# Introduction

Tools and their uses:

* **whois:** This tool is used to query WHOIS servers(look up WHOIS records)
* **nslookup:** This tool is used to query DNS servers – Database Records
* **dig:** This tool is also used to query DNS servers - database records. But you can retain more information with it than with nsloookup.

Examples of Online Services that you can use to get information about the target website:

* **DNSDumpster**
* **Shodan.io**

Defenders’ Objectives Vs Attackers’ Objectives

* The Defender: The defender must know what he/he will find out about your system and network and if there’s something that’s not supposed to be accessible to the public. One should see if there are any vulnerabilities.
* The Attacker: As an attacker, one should collect information about the target system.

# **Passive** Versus **Active** Recon

The writer, Sun TZU, says in his famous book, “The Art of War”,” If you know the enemy and know yourself, your victory will not stand in doubt.”

What exactly is **Passive** Recon?

It is an initial survey to gather information about a certain target.

What is **Active** Recon?

It is directly interacting with the target to get information.

ACTIVE

PASSIVE

|  |  |
| --- | --- |
| Passive Reconnaissance | Active Reconnaissance |
| You rely on **publicly available** knowledge. | It requires **direct engagement** with the target because there is some information that must be retrieved only through directly engaging with the adversary. |
| When you gather information from **publicly available resources** without directly interacting with the specific target. | Connecting to one of the company servers:  1)HTTP  2) FTP  3)SMTP |
|  | **Social engineering**: Calling the company via the phone to collect information |
|  | Entering the company and pretend to be a repairman to get information. |

# WHOIS

It is a request and response protocol which is considered a very helpful command-line utility.

It is extremely helpful for looking up information about a **domain**. The domain registrar is responsible for maintaining the whois records for the domain names it’s leasing. The whois server replies with different information related to the domain requested.

|  |  |
| --- | --- |
| **Registrar** | Via which entity/registrar was the domain registered? |
| **Contact information of registrant** | Name, organization, address, phone, among other things. (unless made hidden via a privacy service) (tryhackme.com) |
| **Name Server** | The server which is responsible for **resolving** the domain name. |
| **Important Dates** | Date of registration of the domain name  Date of expiration of the domain name  Data of last update of the domain name |

**A screenshot of a computer

Description automatically generated1.Using WHOIS: Syntax: whois tryhackme.com**

**A white and grey rectangular object

Description automatically generated with medium confidence**

# Nslookup & dig

SOA:

Start of authority

Options:

QUERY TYPES

A: IPV4

TXT:

Txt records

MX:

Mail Servers

CNAME:

Canonical name

AAAA:

IPV6

|  |  |
| --- | --- |
| Server | DNS server you want to query |
| Domain name | The name you are looking for |
| options | Information like: Is it IPV4 or IPV6? What are the canonical names for the domain name, if there are any. What mail server is the website using? |

* Dig has the same purpose as nslookup but offers more information. For example, the domain information groper can return information like TTL (Time To Live) by default.

Screenshots of the using dig and nslookup:

1)nslookup

2)cname

3)MX: mail server

4)IPV6

5)IPV4

6)TXT: text records

7) Mail servers: Using dig

A screenshot of a computer

Description automatically generated

A black background with white text

Description automatically generated

A black surface with white text

Description automatically generated with medium confidence

A blue background with white text

Description automatically generated

A screenshot of a computer

Description automatically generated

A black background with white text

Description automatically generated

A screenshot of a computer

Description automatically generated

# DNSDumpster

The DNSDumpster is an online service which used to find **subdomains.** Finding subdomains can be extremely useful. They can be used to exploit vulnerabilities. Also, the lack of updates and maintenance can lead to vulnerabilities. The DNSDumpster resolves the domain names to IP addresses.

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

# Shodan.io

Things that you can find out through Shodan.io:

* IP address
* hosting company
* geographic location
* server type and version

Looking up apache and ngix. A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated