Active Information Gathering.

6.3.1 Offsec

Type 1: DNS Enumeration

It’s a database used for translating domain name to IP address.

Types of DN records

NS: Nameserver record contain name of authoritative server hosting the DNS records for domain

A: Contains IPv4 address of hostname

AAAA: Contains IPv6 address of hostname.

MX: Mail exchange records contains name of the email server.

PTR: Pointer record used for reverse lookup translate IP address to domain name.

CNAME: Canonical name records – used to create aliases for host records

TXT: Text records contain arbitrary data.

Eg1: Find IP address from domain name

kali@kali:~$ **host www.megacorpone.com**

www.megacorpone.com has address 149.56.244.87

eg2: To find email server handling A screen shot of a computer screen

Description automatically generated

eg3:

A screen shot of a computer

Description automatically generated

Where cat list.txt has

kali@kali:~$ cat list.txt

www

ftp

mail

owa

proxy

router

Automate DNS enumeration – DNSrecon & DNSenum

DNSrecon

-d –domain name

-t –option

Std--- standard enumeration

A screenshot of a computer

Description automatically generated

DNSenum

A screenshot of a computer

Description automatically generated

Windows DNS enumeration – nslookup

A screen shot of a computer

Description automatically generated