


nslookup

```
C:\Users\PC-1>nslookup
Default Server: UnKnown
Address: 192.168.0.1

> set type=a
> www.cyberartspro.com
Server: UnKnown
Address: 192.168.0.1

Non-authoritative answer:
Name:    cyberartspro.com
Address: 94.73.146.29
Aliases: www.cyberartspro.com
```



Authoritative name server:

```
> set type=cname
> www.cyberartspro.com
Server: UnKnown
Address: 192.168.0.1

Non-authoritative answer:
www.cyberartspro.com    canonical name = cyberartspro.com
> cyberartspro.com
Server: UnKnown
Address: 192.168.0.1

cyberartspro.com
    primary name server = ns1.natrohost.com
    responsible mail addr = hostmaster.cyberartspro.com
    serial = 2022042801
    refresh = 10800 (3 hours)
    retry = 3600 (1 hour)
    expire = 777600 (9 days)
    default TTL = 3600 (1 hour)
```

```
cyberartspro.com
    primary name server = ns1.natrohost.com
    responsible mail addr = hostmaster.cyberartspro.com
    serial = 2022042801
    refresh = 10800 (3 hours)
    retry = 3600 (1 hour)
    expire = 777600 (9 days)
    default TTL = 3600 (1 hour)
> set type=a
> ns1.natrohost.com
Server: UnKnown
Address: 192.168.0.1

Non-authoritative answer:
Name:    ns1.natrohost.com
Addresses: 142.132.184.215
           85.159.64.2
```

The authoritative name server store the records associated with the domain. If you can determine the authoritative name server (primary name server) and obtain its associated IP address, you might attempt to exploit the server to perform attack such as DoS, DDoS, URL Redirection, etc.

