DNS enumeration :

SMTP , SNMP , FTP

Objective : to enumerate the information from open port .

There are many dns server in companies , for example a chekpoin maintains 4 dns server , other acts as a redundant and to make it absolute DNS zone transfer happens , one of the primary responsibility of DNS system adm is to configure zone transfer in such a way that it happens with concerned DNS server only .

If attacker comes to know that port 53 is opened he can extract data from that especially Records.

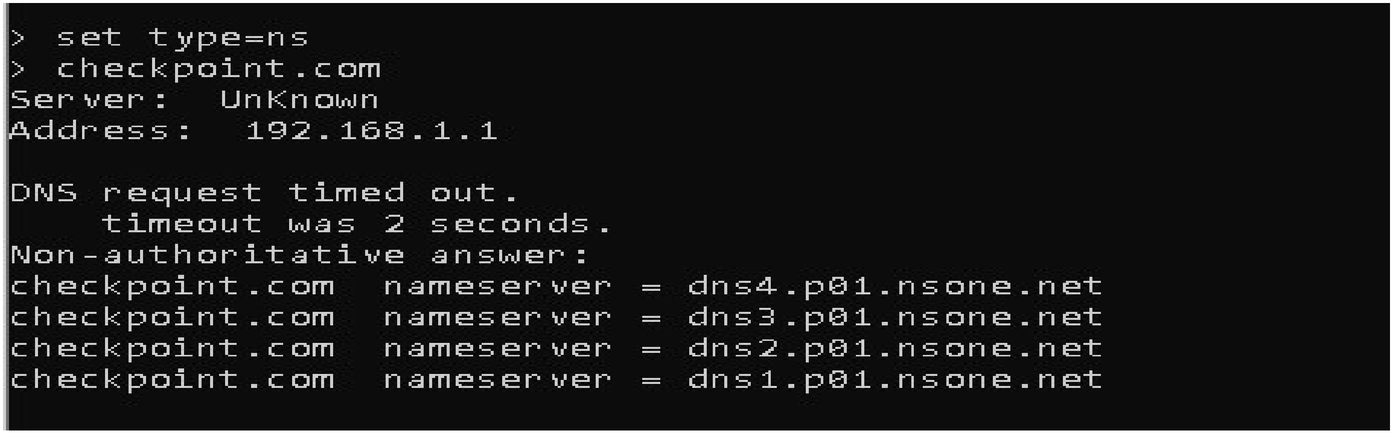
Enumeration : to explore .

Windows :

C:\>nslookup ***Nslookup by default gives all info from all dns record***

C:\>set type=ns

C:\>checkpoint.com

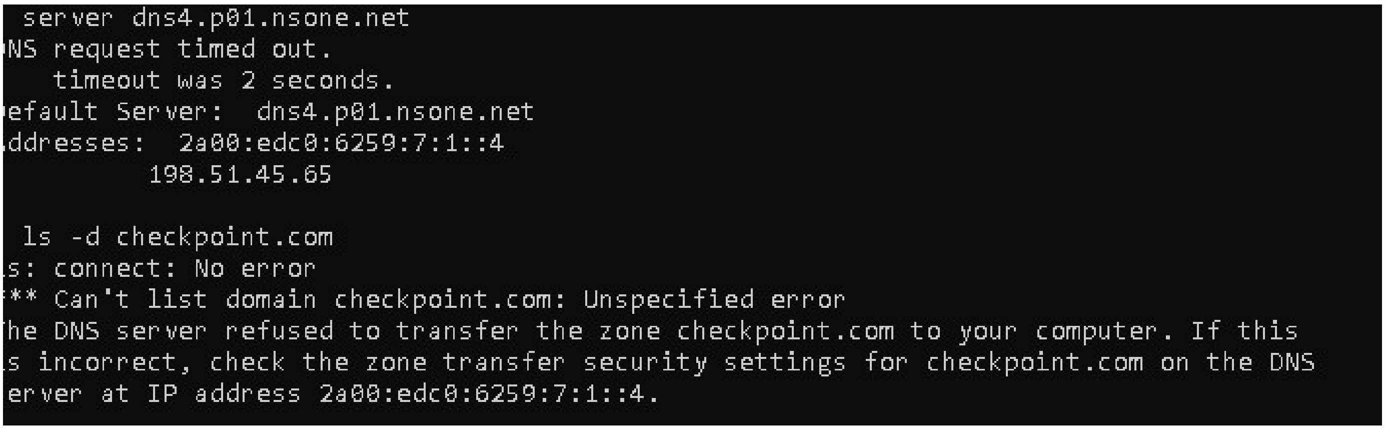


```
> set type=ns
> checkpoint.com
Server:  UnKnown
Address:  192.168.1.1

DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
checkpoint.com  nameserver = dns4.p01.nsone.net
checkpoint.com  nameserver = dns3.p01.nsone.net
checkpoint.com  nameserver = dns2.p01.nsone.net
checkpoint.com  nameserver = dns1.p01.nsone.net
```

>server dns1.p01……

>ls -d checkpoint.com

Refused :…………………

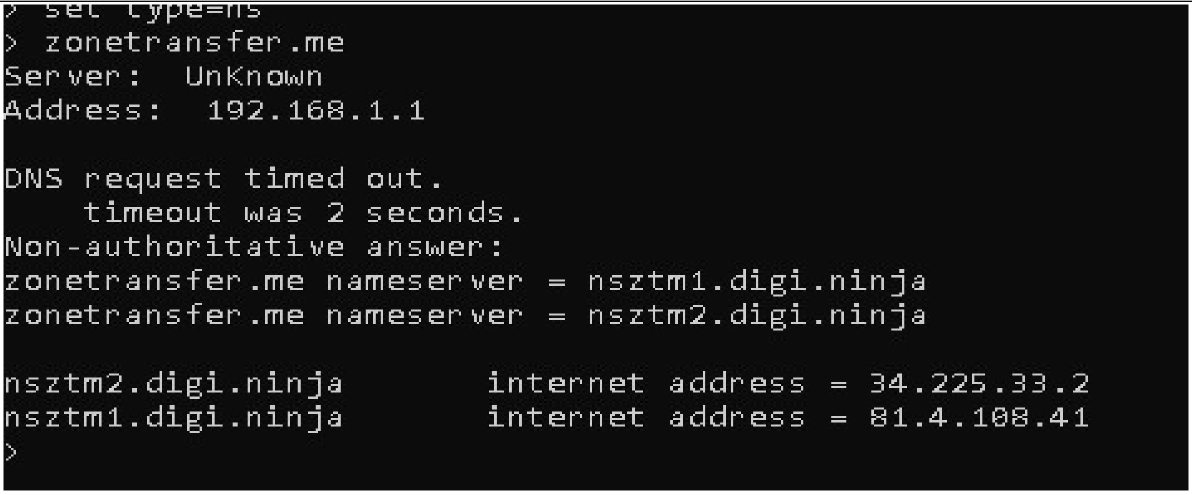


```
 server dns4.p01.nsone.net
NS request timed out.
   timeout was 2 seconds.
efault Server:  dns4.p01.nsone.net
ddresses:  2a00:edc0:6259:7:1::4
          198.51.45.65

 ls -d checkpoint.com
s: connect: No error
** Can't list domain checkpoint.com: Unspecified error
he DNS server refused to transfer the zone checkpoint.com to your computer. If this
s incorrect, check the zone transfer security settings for checkpoint.com on the DNS
erver at IP address 2a00:edc0:6259:7:1::4.
```

Fresh start :

C:\>nslookup

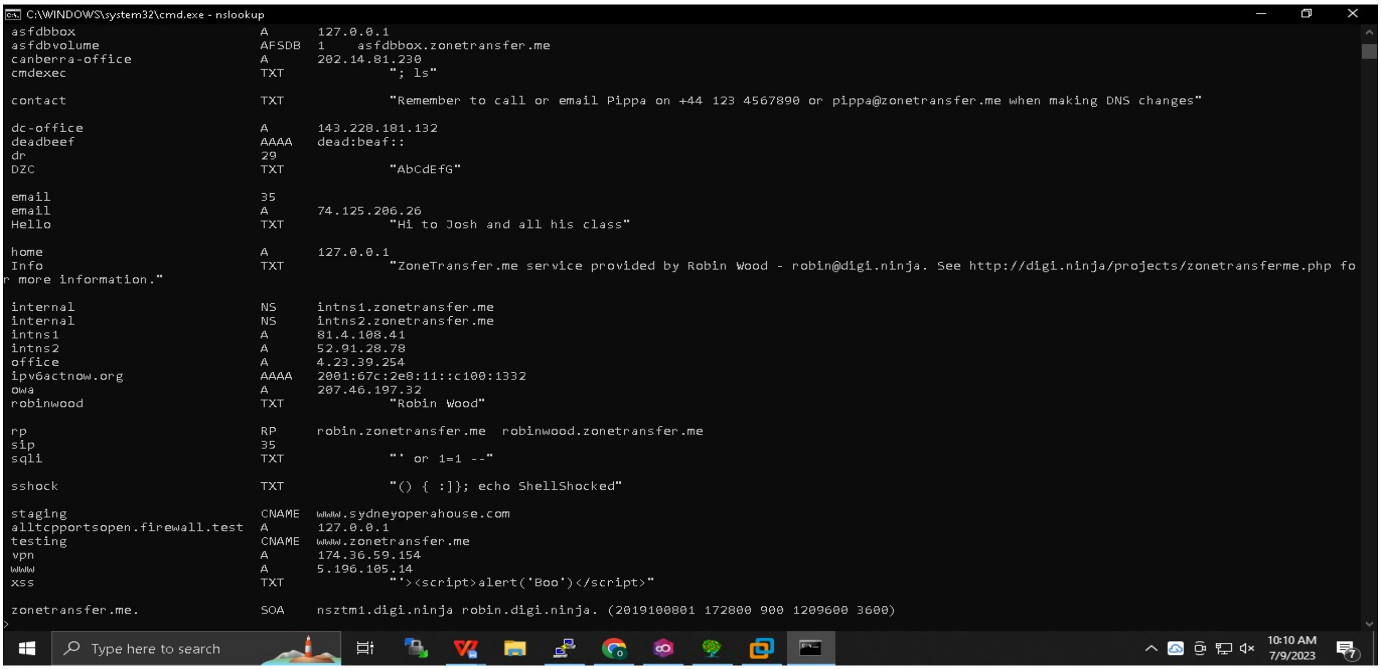
C:\>zonetransfer.me



```
> set type=ns
> zonetransfer.me
Server:  UnKnown
Address:  192.168.1.1

DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
zonetransfer.me nameserver = nsztm1.digi.ninja
zonetransfer.me nameserver = nsztm2.digi.ninja

nsztm2.digi.ninja       internet address = 34.225.33.2
nsztm1.digi.ninja       internet address = 81.4.108.41
>
```

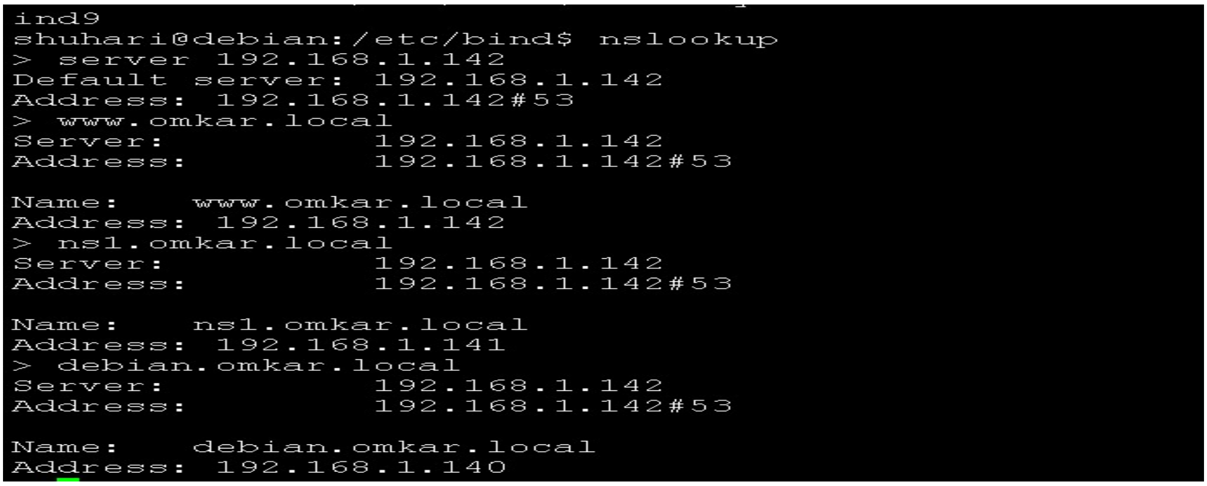
>server ……………….

>ls -d site

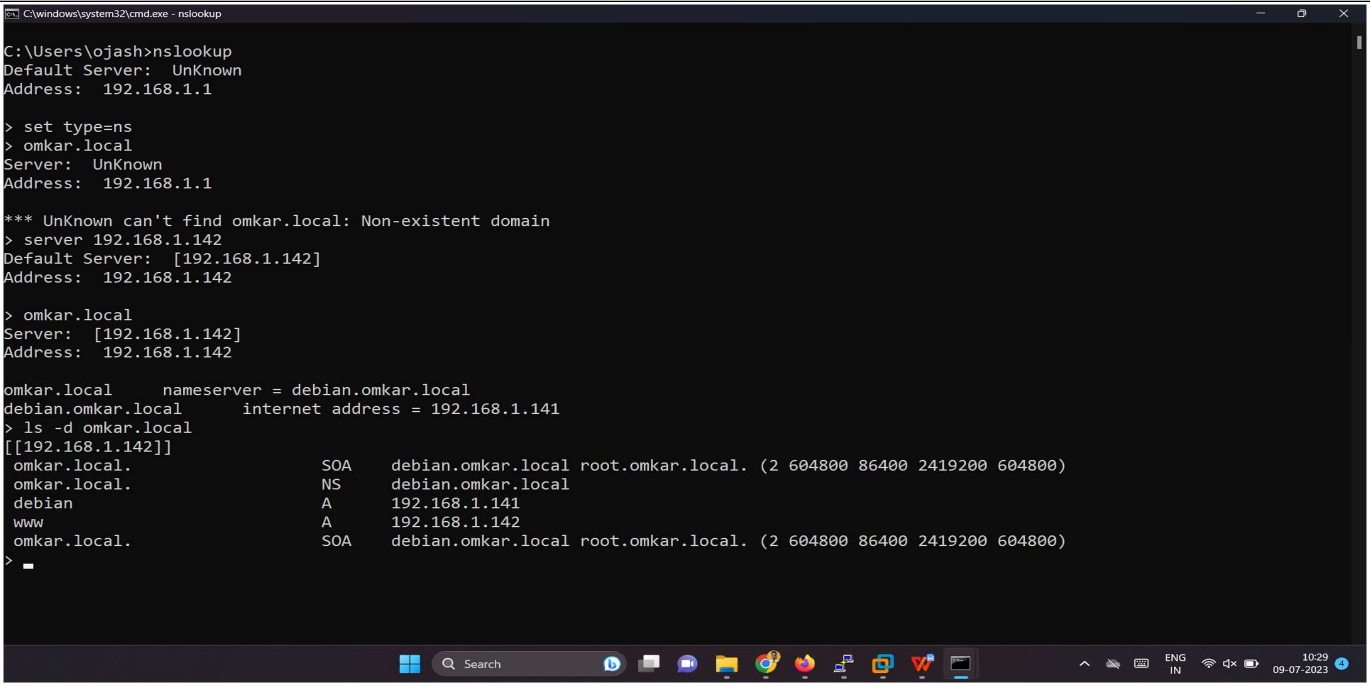


```
 asfdbbox                      A       127.0.0.1
 asfdbvolume                   AFSDB   1     asfdbbox.zonetransfer.me
 canberra-office               A       202.14.81.230
 cmdexec                       TXT              "; ls"

 contact                       TXT              "Remember to call or email Pippa on +44 123 4567890 or pippa@zonetransfer.me when making DNS changes"

 dc-office                     A       143.228.181.132
 deadbeef                      AAAA    dead:beaf::
 dr                            29
 DZC                           TXT              "AbCdEfG"

 email                         35
 email                         A       74.125.206.26
 Hello                         TXT              "Hi to Josh and all his class"

 home                          A       127.0.0.1
 Info                          TXT              "ZoneTransfer.me service provided by Robin Wood - robin@digi.ninja. See http://digi.ninja/projects/zonetransferme.php fo
r more information."

 internal                      NS      intns1.zonetransfer.me
 internal                      NS      intns2.zonetransfer.me
 intns1                        A       81.4.108.41
 intns2                        A       52.91.28.78
 office                        A       4.23.39.254
 ipv6actnow.org                AAAA    2001:67c:2e8:11::c100:1332
 owa                           A       207.46.197.32
 robinwood                     TXT              "Robin Wood"

 rp                            RP      robin.zonetransfer.me  robinwood.zonetransfer.me
 sip                           35
 sqli                          TXT              "' or 1=1 --"

 sshock                        TXT              "() { :]}; echo ShellShocked"

 staging                       CNAME   www.sydneyoperahouse.com
 alltcpportsopen.firewall.test A       127.0.0.1
 testing                       CNAME   www.zonetransfer.me
 vpn                           A       174.36.59.154
 www                           A       5.196.105.14
 xss                           TXT              "'><script>alert('Boo')</script>"

 zonetransfer.me.              SOA     nsztm1.digi.ninja robin.digi.ninja. (2019100801 172800 900 1209600 3600)
>
```

Set our own dns server -> put it in bridge and check whether info is getting revealed or not .



```
ind9
shuhari@debian:/etc/bind$ nslookup
> server 192.168.1.142
Default server: 192.168.1.142
Address: 192.168.1.142#53
> www.omkar.local
Server:         192.168.1.142
Address:        192.168.1.142#53

Name:   www.omkar.local
Address: 192.168.1.142
> ns1.omkar.local
Server:         192.168.1.142
Address:        192.168.1.142#53

Name:   ns1.omkar.local
Address: 192.168.1.141
> debian.omkar.local
Server:         192.168.1.142
Address:        192.168.1.142#53

Name:   debian.omkar.local
Address: 192.168.1.140
```



```
C:\Users\ojash>nslookup
Default Server:  UnKnown
Address:  192.168.1.1

> set type=ns
> omkar.local
Server:  UnKnown
Address:  192.168.1.1

*** UnKnown can't find omkar.local: Non-existent domain
> server 192.168.1.142
Default Server:  [192.168.1.142]
Address:  192.168.1.142

> omkar.local
Server:  [192.168.1.142]
Address:  192.168.1.142

omkar.local     nameserver = debian.omkar.local
debian.omkar.local      internet address = 192.168.1.141
> ls -d omkar.local
[[192.168.1.142]]
 omkar.local.                   SOA    debian.omkar.local root.omkar.local. (2 604800 86400 2419200 604800)
 omkar.local.                   NS     debian.omkar.local
 debian                         A      192.168.1.141
 www                            A      192.168.1.142
 omkar.local.                   SOA    debian.omkar.local root.omkar.local. (2 604800 86400 2419200 604800)
> 
```