

It is not a big attack but may lead to critical

→ DNS Zone transfer is used to copy a zone file from a master DNS to a slave DNS

If DNS server is misconfigured not only authorized slave DNS server can request a copy of the zone file but anyone asking for zone file will get a copy.

identifying

> dig @8.8.8.8 ns target
You get some DNS name

> dig @DNS_name target
You will get zone file of target

> dig @NS axfr target

```
Offensive-MacBook-Pro:~ offensivehunter$ dig @dns1.leapswitch.com axfr hackersera.com
; <<> DiG 9.10.6 <<> @dns1.leapswitch.com axfr hackersera.com
; (1 server found)
;; global options: +cmd
; Transfer failed.
Offensive-MacBook-Pro:~ offensivehunter$
```

→ secure results.

Reference

ZoneTransfer.me

*with host commands

> host -t ns target

> host -l target DNS_name