**LABO 19**

**DNS**

1. Zorg dat op je laptop geen VPN draait. (Geen van Howest, maar ook geen NordVPN of andere.)

Note: Zoniet lopen je DNS-requests over deze VPN wat vertekende resultaten kan opleveren en waar mogelijks het gebruik van een alternatieve nameserver niet lukt.

Note2: Merk op dat, wanneer je een VPN draait, de provider van die VPN dus kan zien welke sites je allemaal opvraagt!

1. Open op je laptop de Windows command prompt.

Zoals je weet, heb je een DNS-server nodig om te kunnen surfen. Met welk commando kan je het IPv4-adres opvragen van de DNS-servers die door je laptop gebruikt worden? (commando + optie)

ipconfig /all

Plak hieronder een screenshot van enkel die regels van de output van je commando waarin die adressen getoond worden voor je actieve NIC waarmee je verbinding met het internet maakt. (Voor sommigen is dit thuis bekabeld, bij anderen via Wi-Fi.)

Behalve de IP-adressen (IPv4 en mogelijks IPv6) die je NIC zelf toegewezen krijgt, zul je daar ook het IP-adres (of meerdere) van de DNS server zien. Plak hier een screenshot van deze output.

Bij welk(e) device(s) horen de IP-adressen van de DNS servers (m.a.w. waar staan die DNS servers)?

IP-adres hoort bij de DNS-server van je provider of de DNS-service van je thuisrouter

1. Vraag terug de IP-adressen op van de DNS-servers op die door je laptop gebruikt worden, maar ditmaal gebruikmakend van de GUI.

Plak hieronder een screenshot van het venster waarin je deze info gevonden hebt.

Rechtsklikken op hert draadloos netwerkicoontje (in de taakbalk) > Netwerk en Internetinstellingen openen > Netwerkcentrum > Draadloze netwerkverbinding > Details

Tip: je kan snel naar al je netwerkverbindingen gaan door ***ncpa.cpl*** (Network Control Panel Applet) in te tikken in je command prompt venster.

Hoe heeft je draadloze NIC dit IP-adres gekregen?

via de DHCP-service van je thuisrouter

1. Start je Linux-VM op en meld je erop aan met de account *mickey* en wachtwoord *mouse*.

Het IPv4-adres van de DNS-server die door (de NIC van) je Linux-VM gebruikt wordt, bevindt zich in de file ***/etc/resolv.conf***.

Met welk commando kan je bijgevolg dat IP-adres opvragen?

cat /etc/resolv.conf of more /etc/resolv.conf of less /etc/resolv.conf

Noteer hieronder het commando waarmee je de output van je vorig commando beperkt tot enkel die regel die het gevraagde adres bevat.

grep nameserver /etc/resolv.conf 🡪 192.168.X.2

1. In je Linux-VM zou je ook nslookup kunnen gebruiken, maar die is standaard niet geïnstalleerd bij een minimale Debian installatie. Je kan die makkelijk installeren, maar we zullen hier eens een andere tool gebruiken die even nuttig is en wel standaard aanwezig is: **host** .

Gebruik deze tool om google.be te resolven.

host google.be

Output:

google.be has address 108.177.119.94

google.be has IPv6 address 2a00:1450:400e:80d::2003

Plaats de lijn met de DNS-server in /etc/resolv.conf in commentaar en voeg een gelijkaardige lijn toe om DNS-server 8.8.8.8 te gebruiken

nameserver 8.8.8.8

Resolve nu nogmaals google.be met de **host** tool. Zijn IPv4/IPv6-adressen nu dezelfde?

google.be has address 172.217.17.35

google.be has IPv6 address 2a00:1450:400e:80a::2003

andere IP-adressen.

(Je mag nu /etc/resolv.conf terug aanpassen om de originele DNS-server weer te gebruiken.)

Note: je kon ook gewoon “host google.be 8.8.8.8” uitvoeren zonder /etc/resolv.conf aan te passen indien je maar 1-malig 8.8.8.8 wilt gebruiken. Maar zo zie je hou je permanent de name server kan aanpassen.

1. Zoals je wellicht weet, beschikt je laptop over een lokale DNS-cache waarin naam-naar-IP-adres-vertalingen tijdelijk bewaard worden. In deze opdracht leer je met deze cache werken.

Voer op je host onderstaande opdrachten uit mbv een legacy Windows-commando:

* Met welk ipconfig-commando (met extra optie) kan je de inhoud van de lokale DNS-cache wissen? Doen!

ipconfig /flushdns

* Met welk ipconfig-commando (met extra optie) kan je de inhoud van de lokale DNS-cache tonen? Doen!

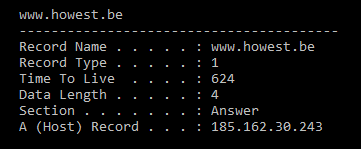
ipconfig /displaydns

Als je dit commando heel snel na het vorig commando ingetikt hebt, dan zal je DNS-cache wellicht leeg zijn (hangt ervan af of je andere netwerkapplicaties open staan hebt).

* Surf naar [www.howest.be](http://www.howest.be)

Toon opnieuw de inhoud van je lokale DNS-cache en plak hieronder een screenshot van dat deel van de lokale DNS-cache waarin gegevens over de website van Howest getoond worden (6 regels onder de stippellijn).

ipconfig /displaydns



Opmerking: om automatisch te zoeken in de output, kun je in Powershell volgende cmdlets combineren:

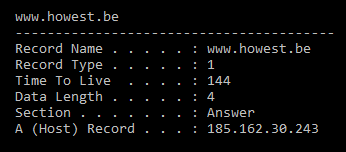
ipconfig /displaydns | Select-String -Pattern "www.howest.be" -Context 0,6

(dit betekent: zoeken in de uitvoer van ipconfig /displaydns op “www.howest.be” en 0 lijnen ervoor printen, maar wel 6 lijnen erna printen)

* In de TTL-regel zie je hoelang de naam-naar-adres vertaling nog in je lokale DNS-cache zal verblijven? Noteer deze waarde hieronder (getal + eenheid)

In mijn geval: 624s (dus nog een goede 10 minuten…)

* Toon opnieuw de inhoud van de lokale DNS-cache en plak hieronder opnieuw een screenshot van dat deel van de lokale DNS-cache waarin gegevens over de Howest-webserver getoond worden.

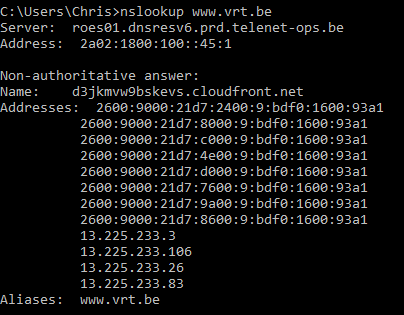


Welke regel is er gewijzigd tov het vorige screenshot? Leg uit waarom!

De TTL-waarde is verminderd omdat die record ondertussen een aantal seconden minder lang in de lokale DNS-cache zit.

1. Naam-naar-IP-adresvertalingen vertalingen kan je ook laten uitvoeren door gebruik te maken van het Windows ***nslookup***-commando. Dit commando kan zowel in de interactieve als in de niet-interactieve mode gebruikt worden.

Je gebruikt het NSLOOKUP-commando **in de niet-interactieve mode** door onmiddellijk na het commando een argument (bv een naam of een IP-adres) te gebruiken. Test deze niet-interactieve mode uit om de IP-adressen van de webserver van de VRT (www.vrt.be) te achterhalen. Plak hieronder een screenshot van je commando en zijn output.



Heb je hiervoor een forward of een reverse lookup-query gebruikt?

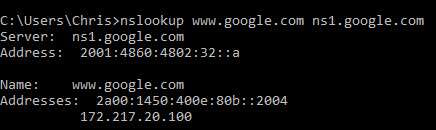
Forward lookup query

In de eerste 2 regels van de output van dit commando wordt de naam en het IP-adres van de DNS-server getoond die de gevraagde naam-naar-adres vertaling doet. Dit is standaard de DNS-server die in de IP-adresconfiguratie werd vastgelegd (zie opdracht 1).

In de volgende regel(s) word(t)(en) dan de IP-adressen getoond die met de opgezochte naam overeenkomen. Merk op dat zowel IPv4- als IPv6-adressen getoond worden.

Je kan ook een andere DNS-server gebruiker dan de default DNS-server. Deze moet je dan wel ook als extra argument in je nslookup-commando specifiëren. Test dit uit door de IP-adressen van de Google-website te achterhalen mbv ns1.google.com (dit is één van de DNS-servers van Google).

Plak hieronder een screenshot van je ingetikte commando en zijn output.



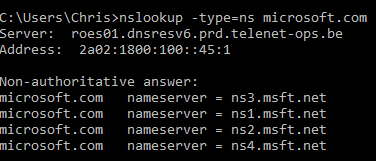
Vergelijk de output van je 2 ingetikte commando’s. Er is één opvallend verschil. Welk? Verklaar dit!

Bij 2de commando staat er geen regel “Non-authoritative answer” omdat je de opzoeking hebt laten doen door de DNS-server van Google zelf die uiteraard verantwoordelijk (authoritative) is voor de DNS van Google.

1. Vraag mbv het nslookup-commando alle DNS-servers op die verantwoordelijk zijn voor DNS van het microsoft.com domein.

Tip: maak hiervoor gebruik van de type-optie.

Plak hieronder een screenshot van je ingetikte commando en zijn output.



1. Gebruik de niet-interactieve mode van het nslookup-commando ook eens om de naam te achterhalen van de computer met als IP-adres 8.8.8.8 en vul deze hieronder in:

nslookup 8.8.8.8

**Naam server met IP-adres 8.8.8.8 =** dns.google

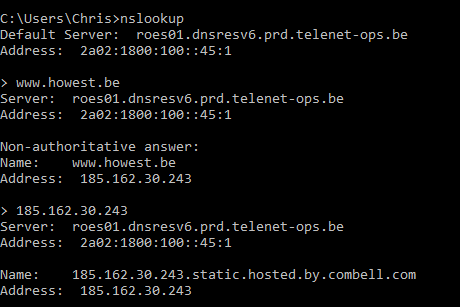
Heb je hiervoor een forward of een reverse lookup-query gebruikt?

Reverse lookup query

1. Je gebruikt het NSLOOKUP-commando **in de interactieve mode** door onmiddellijk na het *nslookup* commando op *Enter* te drukken. Je komt dan in de speciale nslookup-prompt terecht waar je speciale commando’s of gewoon DNS-namen of IP-adressen kan invoeren.

Test ook deze methode eens uit voor het uitvoeren van een forward en een reverse lookup voor de website van onze hogeschool.

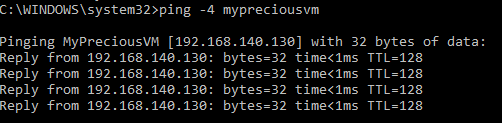
Verlaat daarna de interactieve nslookup-mode (mbv het exit-commando) en plak hieronder een screenshot van de hele interactieve nslookup-sessie.



1. Zorg ervoor dat je Windows 10 VM (of je Linux VM) bereikbaar is via de naam MyPreciousVM.

Als je dit correct ingesteld hebt, moet je vanaf je laptop kunnen pingen naar de naam MyPreciousVM. Test dit uit en plak hieronder een screenshot van je commando en de output.

Tip: voeg hiervoor op je laptop een regel aan de hosts-file toe, met daarin het IP-adres van je VM en de naam MyPreciousVM.

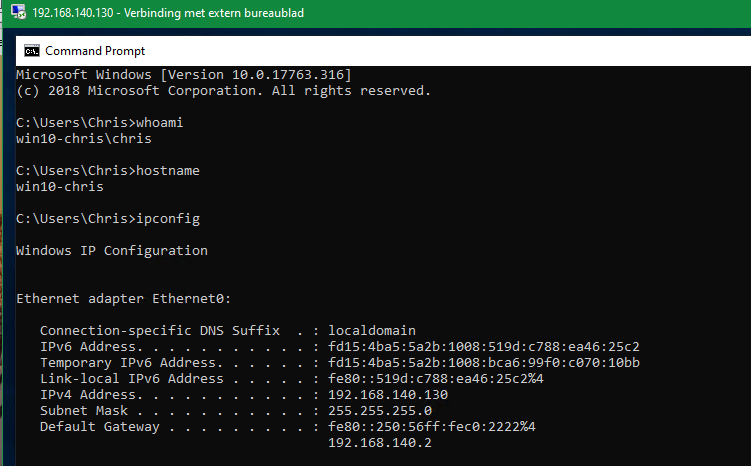


1. Pas de instellingen op je Windows 10 VM aan zodat je er vanop afstand op kan aanmelden. In Windows-terminologie: zorg ervoor dat de “Remote Desktop” instelling op je VM aan staat.

In je VM: Rechtsklik op Start-knop > System > Remote Desktop > Off 🡪 On

Maak daarna vanaf je laptop een Remote Desktop connectie (Nederlandse term: “Extern Bureaublad”) met je Win10-VM (op basis van zijn IP-adres).

Plak hieronder een screenshot van je eigen Remote Desktop (met dezelfde info in zoals op mijn screenshot hieronder; dus in de VM een cmd-prompt met daarin de door jou ingetikte commando’s).



Op je host (laptop): Start-knop > Verbinding met Extern Bureaublad

Bij problemen:

* Check firewall op VM
* Check of user account mag inloggen
* Check de naam van de user account (whoami)
* User account moet een wachtwoord hebben

Wat gebeurt er nadat de Remote Desktop verbinding tot stand gekomen is met de rechtstreekse verbinding (dus deze in VMware Workstation)?

Verbinding in VMware is verbroken

Wat kan je hieruit concluderen?

Er kan maximum 1 gebruiker op een Windows 10 aangemeld zijn.

1. Vraag mbv onderstaand legacy Windows-commando informatie op over alle TCP-connecties op je laptop.

***netstat -n***

Wil je nog meer info krijgen, dan maak je best gebruik van onderstaand commando. Hierdoor krijg je o.m. ook te zien welke processen (programma’s) de TCP-verbindingen opgestart hebben.

***netstat -nabo***

Pas dit commando aan zodat je enkel info te zien krijgt over de TCP-verbinding tussen je host en je VM. Plak hieronder een screenshot van dit commando en zijn output.

Tip: maak hiervoor gebruik van het commando ***findstr*** om in de output van het vorige commando naar een string te zoeken en noteer dit commando hieronder.



Of: netstat -nabo | Select-String -Pattern "192.168.140.128"

De Remote Desktop applicatie maakt gebruik van het **RDP-protocol**. Van welke poort wordt er volgens de output van je commando standaard door RDP gebruikgemaakt?

**Poortnumer RDP-server =** 3389

1. Open de capture file met als naam Labo18.pcapng. Deze file heb je al voor Labo18 moeten downloaden.

1. Zorg ervoor dat enkel DNS-pakketten getoond worden.

Fiterexpressie = dns

Je zal merken dat er 2 soorten DNS-messages getoond worden: DNS-requests en de bijhorende DNS-responses.

1. Bekijk het pakket nr 49 en vervang in onderstaande tabel de vraagtekens door gepaste protocolnamen. Vervang de vraagtekens onder de tabel door de grootte van de velden (in bytes).

Tip: als je alle groottes bij elkaar optelt, moet je de framegrootte uitkomen die in de eerste regel van het Details-venster getoond wordt!

|  |  |  |  |
| --- | --- | --- | --- |
| ????  HEADER | ???? HEADER | ???? HEADER | ???? MESSAGE |

?? B ?? B ?? B ?? B

|  |  |  |  |
| --- | --- | --- | --- |
| Ethernet  HEADER | IP HEADER | UDP HEADER | DNS MESSAGE |

14 B 20 B 8 B 31 B

1. In ons geval (pakket nr 16) is het pakket een DNS-request. Dit kan je zien door in de Info-kolom te kijken, maar je kan het ook zwart op wit zien in het Details-venster.

DNS-request want het woordje “respons” staat niet expliciet in de Info-kolom

Van welke hostnaam wordt er naar het bijhorende IP-adres gevraagd?

[www.google.be](http://www.google.be)

Wordt er hier naar een IPv4- of een IPv6-adres gevraagd? Ook deze vraag kan je beantwoorden door in de Info-kolom te kijken. Daarin staat er om welk soort DNS-record er verzocht wordt (zie ook dia nr 9 in hoofdstuk 15 – deel 2 van de theorie).

IPv4-adres (aangeduid met de letter A in de Info-kolom)



1. Onderaan in het Details-venster van het DNS-protocol zie je op welk nummer je de respons op deze request vindt. Door daarop te dubbelklikken, ga je automatisch naar dat nummer. Doen!

Welk IP-adres correspondeert er bijgevolg met de opgevraagde hostnaam? Ook deze vraag kan je beantwoorden door in de Info-kolom of in het Details-venster te kijken…



1. Keer even terug naar pakket nr 16. In het Details-venster kan je zien dat het verschil tussen een DNS-request en een DNS-response aangeduid wordt aan de hand van de response-vlag: als deze op 0 staat, is het een request, als deze op 1 staat, is het een response.

Maak van deze info gebruik om je filterexpressie zodanig aan te passen dat je enkel nog de DNS-responses te zien krijgt en noteer deze filterexpressie hieronder.

dns.flags.response eq 1

Hoeveel zo’n DNS-responses zijn er bijgevolg?

39

1. Toon enkel de pakketten die tot dezelfde UDP-stream behoren als pakket nr 16.

Rechtsklikken op pakket > Follow > UDP stream

Hoeveel zo’n pakketten zijn er?

2

Wordt zo’n stream geïnitialiseerd en gefinaliseerd? Waarom (niet)?

Neen want dit gebeurt nooit bij UDP