

# Hacker Highschool

## SECURITY AWARENESS FOR TEENS



### LES 2

## BASIS COMMANDO'S IN LINUX EN WINDOWS



## “License for Use” Information

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the Hacker Highschool web page at [www.hackerhighschool.org/license](http://www.hackerhighschool.org/license).

The HHS Project is a learning tool and as with any learning tool, the instruction is the influence of the instructor and not the tool. ISECOM cannot accept responsibility for how any information herein is applied or abused.

The HHS Project is an open community effort and if you find value in this project, we do ask you support us through the purchase of a license, a donation, or sponsorship.

All works copyright ISECOM, 2004.

## Informatie over de “Gebruiksvoorwaarden”

De lessen en werkboeken van het Hacker Highschool (HHS) project zijn beschikbaar onder de volgende door ISECOM gestelde voorwaarden:

Alle informatie uit het HHS-project mag, niet-commercieel, gebruikt worden voor en door basisschool-leerlingen en studenten van middelbaar en hoger onderwijs. Dit materiaal mag niet worden gereproduceerd voor (door-)verkoop in welke vorm dan ook. Gebruik van dit materiaal in een klas, cursus, training, kamp of andere georganiseerde vorm van kennisoverdracht waarvoor geld wordt gevraagd is expliciet verboden zonder een licentie. Om een licentie te regelen kunt u het onderdeel LICENSE bezoeken op de website van de Hacker Highschool, [www.hackerhighschool.org/license](http://www.hackerhighschool.org/license).

Het HHS-project is een leermiddel en, zoals met elk leermiddel, de docent/trainer bepaalt in grote mate het effect van het leermiddel. ISECOM kan geen aansprakelijkheid aanvaarden voor de positieve of negatieve gevolgen van het gebruik van dit materiaal en de daarin opgenomen informatie.

Het HHS-project is een initiatief van de open community, en wanneer u de resultaten van onze inspanning waardevol genoeg vindt om het te gebruiken, vragen we u uw steun te betuigen door:

- de aankoop van een licentie;
- een donatie
- ons te sponsoren.

Op al het werk berust copyright van ISECOM, 2004.



## Inhoudsopgave

“License for Use” Information.....	2
Informatie over de “Gebruiksvoorwaarden” .....	2
2.1. Introductie en Doelen.....	5
2.2. Benodigdheden en Opstelling .....	5
2.2.1 Benodigdheden.....	5
2.2.2 Opstelling.....	5
2.3. Systeem werking: WINDOWS.....	6
2.3.1 Hoe open je een MS-DOS scherm.....	6
2.3.2 Commando's en gereedschappen (Windows).....	6
2.4. Systeem werking: Linux.....	9
2.4.1 Hoe open je een console-scherm.....	9
2.4.2 Commando's en gereedschappen (Linux).....	9
2.5. Oefeningen.....	12
2.5.1 Oefeningen in Windows.....	12
2.5.2 Oefeningen in Linux.....	12
2.5.3 Oefening 3.....	13



## Auteurs

Daniel Fernández Bleda, Internet Security Auditors

Jairo Hernández, La Salle URL Barcelona

Jaume Abella, La Salle URL Barcelona - ISECOM

Kim Truett, ISECOM

Pete Herzog, ISECOM

Marta Barceló, ISECOM

## Vertaald door:

Raoul Teeuwen



**Universitat Ramon Llull**





## 2.1. Introductie en Doelen

Deze les introduceert commando's en basis gereedschappen voor zowel Windows- als Linux-besturingssystemen en maakt je er bekend mee. De commando's moet je weten om de oefeningen in de volgende lessen te kunnen doen

Na deze les zou je de volgende commando's moeten kennen en beheersen:

- Igemene Windows en Linux commando's
- Basis netwerk-commando's en gereedschappen
  - ping
  - tracert
  - netstat
  - ipconfig
  - route

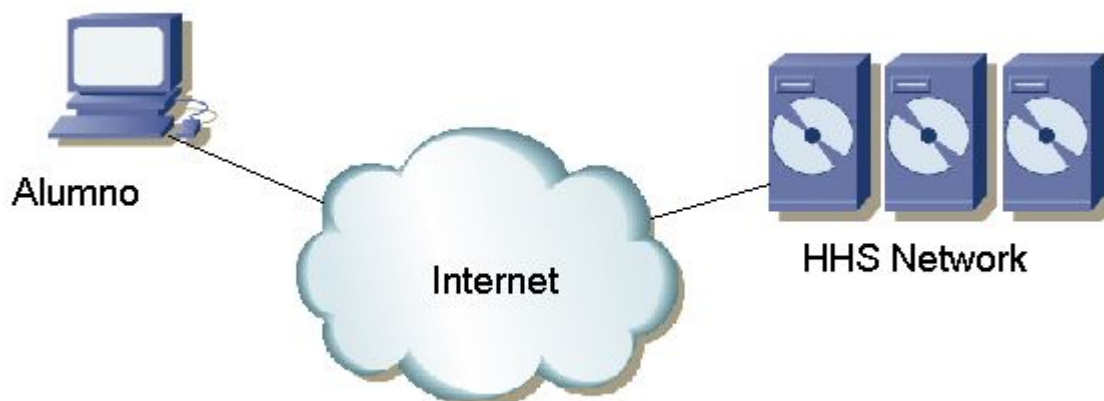
## 2.2. Benodigheden en Opstelling

### 2.2.1 Benodigheden

Voor de les heb je het volgende nodig:

- een PC met Windows 98/Me/2000/NT/XP/2003
- een PC met Linux Suse/Debian/Knoppix\
- toegang tot het Internet.

### 2.2.2 Opstelling







Dit beschrijft de configuratie waarmee je gaat werken. Hij bestaat uit je PC, met toegang tot het Internet, en het ISECOM Hacker Highschool netwerk, waartoe je via Internet toegang hebt. Tegen dat laatste netwerk ga je je oefeningen uitvoeren.

Merk op dat de toegang tot het ISECOM test netwerk afgeschermd is. Om toegang te krijgen dient je docent/instructeur contact op te nemen met de systeembeheerder, zoals beschreven op de [www.hackerhighschool.org](http://www.hackerhighschool.org) website.

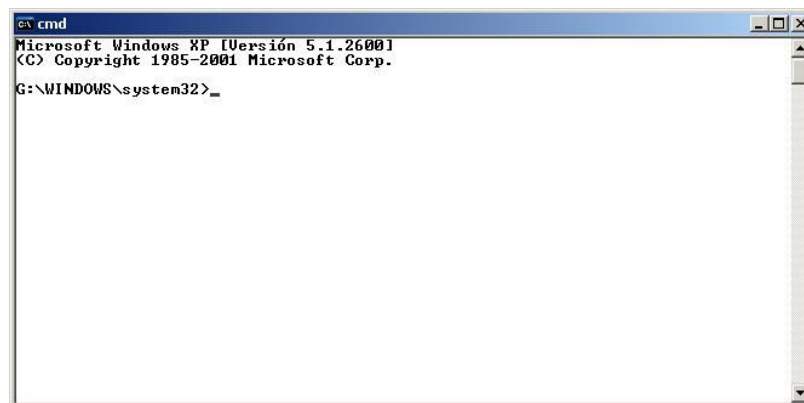
## 2.3. Systeem werking: WINDOWS

De meeste gereedschappen die je nodig hebt om netwerken te onderzoeken bestaan uit Windows-systeem-commando's. Daarom gaan we je leren een commando-prompt te openen als je werkt onder het Windows besturingssysteem.

### 2.3.1 Hoe open je een MS-DOS scherm

Om de volgende commando's uit te voeren, moet je een commando-prompt openen (een MS-DOS scherm). Dit gaat in alle versies van Windows op dezelfde manier.

- 1.- Klik op de START knop
- 2.- Kies RUN/UITVOEREN (afhankelijk van je taalversie)
- 3.- Typ "command" als je Windows 95/98 gebruikt of "cmd" voor alle andere versies van Windows en druk op Enter of klik OK.
- 4.- Er zal een scherm verschijnen dat lijkt op het volgende scherm:



```

cmd
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
G:\WINDOWS\system32>_
  
```

- 5.- Nu kunnende onderstaande commando's en gereedschappen worden ingevoerd en gebruikt.

### 2.3.2 Commando's en gereedschappen (Windows)

#### Commando's

date	Toon of wijzig de datum van het systeem
time	Toon of wijzig de tijd van het system
ver	Toon de MS-DOS versie die gebruikt wordt



date	Toon of wijzig de datum van het systeem
dir	Toon een lijst van submappen en bestanden in de huidige map (directory)
cls	Wis het scherm
mkdir, md mapnaam	Maak een map met de naam "mapnaam" Voorbeeld: md gereedschap
chdir, cd mapnaam	Toon de naam of wijzig de huidige map naar "mapnaam" Voorbeeld: cd gereedschap
rmdir, rd mapnaam	Verwijder de map met de naam "mapnaam" Voorbeeld: rd tools
tree mapnaam	Toon de structuur van mappen in een text-formaat Voorbeeld: tree c:\gereedschap
chkdsk	Controleer een disk en toon een status rapport
mem	Toon de hoeveelheid geheugen die in gebruik en vrij is binnen het systeem
rename,ren bron doel	Wijzig de naam van bestanden Voorbeeld: ren oudenaam nieuwenam
copy bron doel	Kopieer 1 of meer bestanden naar een andere plaats Voorbeeld: copy c:\gereedschap\mijnbestand.txt c:\tmp
move bron doel	Verplaats bestanden en wijzig de naam van bestanden en mappen Voorbeeld: move c:\gereedschap c:\tmp
type file	Toon de inhoud van 1 of meer tekst-bestanden Voorbeeld: type c:\gereedschap\ mijnbestand.txt
more file	Toon de informatie scherm voor scherm (stopt en wacht als er meer informatie is dan op 1 scherm getoond kan worden) Voorbeeld: more c:\gereedschap\ mijnbestand.txt
delete, del file	Verwijder 1 of meer bestanden Voorbeeld: del c:\gereedschap\ mijnbestand.txt

Noot: De *schuin* getoonde woorden zijn geen commando's; op die plaats dienen de juiste waarden ingevuld te worden. Sommige commando's zijn zowel via het korte als het lange commando te gebruiken; zo zijn "delete" en "del" hetzelfde commando/doen hetzelfde.

Gereedschappen



ping host	<p>Controleer verbinding met de machine "host"          Het commando ping zendt "packets" via het ICMP (Internet Control Message Protocol) naar een andere computer om te zien of hij via het netwerk benaderbaar is. Daarnaast toont het een statistische samenvatting van het percentage pakketjes waarop niet gereageerd is, en de reactiesnelheid (response time). Als naam voor de machine kan zowel de naam als een IP-adres gebruikt worden.</p> <p>Voorbeelden: ping www.google.com          ping 193.145.85.2          Enkele opties zijn:          - n N: zend N pakketjes          - t: ping de gespecificeerde host totdat CTRL+C gedrukt wordt          Om meer opties te zien tik je: ping /h</p>
tracert host	<p>Toon de route waarlangs de pakketjes naar de "host"-machine reizen.          Het commando tracert is de afkorting van trace route (volg de route), en je kunt het gebruiken om er achter te komen hoe pakketjes van jouw machine naar de doelmachine (host) reizen. Het kan je ook laten zien hoeveel tijd elke jump/hop/stap kost. Maximaal zullen 30 stappen getoond worden. Het is soms interessant om de namen van de machines te zien die het pakket op zijn reis passeert.</p> <p>Voorbeelden: tracert www.google.com          tracert 193.145.85.2          Enkele opties zijn:          - h N: reis maximaal N stappen.          - d: om de machinenamen niet te tonen.          Om meer opties te zien: tracert</p>
ipconfig	<p>Toon informatie over de actieve interfaces (ethernet, ppp, etc.) in de computer.          Enkele opties:          /all: om meer details te tonen          /renew naam: Haalt verse gegevens voor de verbinding "naam" op als DHCP op automatisch staat.          /release naam: Sluit alle verbindingen af als DHCP op automatisch staat.          Om meer opties te zien: ipconfig /?</p>
route print	<p>Toon de route tabel (routing table)          Met het commando route kunnen statische routes worden toegevoegd, routes worden gewist of gegevens over de routes worden getoond.          Enkele opties:          print: om de lijst van routes te tonen.          delete: om een route te wissen.          add: om een route toe te voegen.          Om meer opties te zien: route/?</p>
netstat	<p>Toon informatie over de status van het netwerk en de gemaakte verbindingen met machines op afstand.</p>

**Enkele opties:**

- a: Om alle verbindingen en ontvangende poorten te controleren
- n: om adressen en poortnummers in cijfervorm te tonen
- e: om Ethernet statistieken te verzamelen





Als voorbeeld: netstat - an  
 Om meer opties te zien: netstat /?

Voor aanvullende informatie over deze commando's en gereedschappen tik je "command / h" of

"command /?, " of "help command" achter de commando-prompt.

We hebben bijvoorbeeld 3 manieren om aanvullende informatie te krijgen over het gereedschap netstat:

- 1) netstat /h
- 2) netstat /?
- 3) help netstat

## 2.4. Systeem werking: Linux

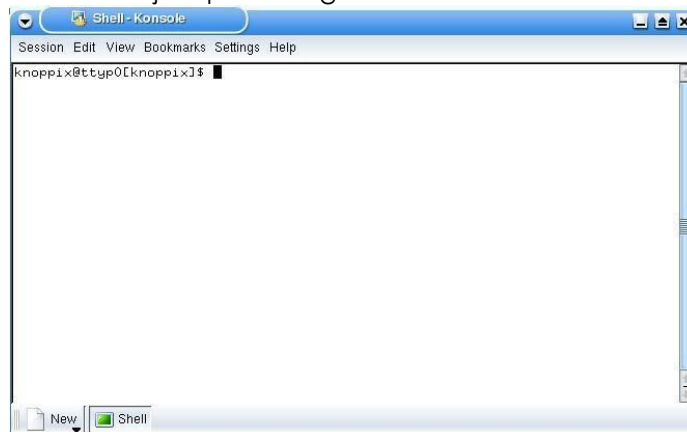


Net zoals in Windows wordt als je Linux gebruikt een groot deel van de commando's die je gaat gebruiken vanaf een console-scherm geactiveerd. Daarom leren we eerst hoe we een console-scherm oproepen onder Linux.

### 2.4.1 Hoe open je een console-scherm

Om de volgende commando's uit te kunnen voeren, dient een console-scherm geopend te worden:

1. - Ga naar de START APPLICATION knop
2. - Kies "Run Command"
3. - Tik "konsole" (ENTER)
4. - Er verschijnt een scherm dat lijkt op het volgende scherm:



5. - Nu kunnen de onderstaande commando's en gereedschappen gebruikt worden.

### 2.4.2 Commando's en gereedschappen (Linux)

Commando's

<b>hostname</b>	Toon de naam van de local host (de computer die je nu gebruikt)
<b>finger gebruiker</b>	Toon informatie over de gebruiker "gebruiker" Voorbeeld: finger root



<b>hostname</b>	Toon de naam van de local host (de computer die je nu gebruikt)
<b>ls</b>	Toon de inhoud van mappen Voorbeeld: ls -la
<b>cd map</b>	Ga van de huidige map naar "map". Wanneer er geen mapnaam aangegeven is, gaat u naar de home directory (hoogste mapniveau), Voorbeeld: Voor de login-naam "mijnlogin" zal het commando \$cd zorgen dat u in de map /home/mijnlogin komt te staan Voorbeeld: \$cd - ga naar de laatst bezochte map Voorbeeld: \$cd /tmp ga naar de "tmp" map
<b>cp bron doel</b>	Kopieer bestanden. Kopieer het bestand "bron" naar het bestand "doel". Voorbeeld: cp /etc/passwd /tmp
<b>rm file</b>	Wis bestanden. Alleen de eigenaar van het bestand (of root) kan de bestanden wissen. Voorbeeld: rm mijnbestand
<b>mv bron doel</b>	Verplaats of hernoem bestanden en mappen. Voorbeeld: mv oudenaam nieuwenaaam
<b>mkdir map</b>	Maak een map met de naam "map". Voorbeeld: mkdir gereedschap
<b>rmdir map</b>	Wis de map met de naam "map" als die map leeg is. Voorbeeld: rmdir gereedschap
<b>find / -name bestand</b> Vind	een bestand met de naam "bestand", en start de zoektocht van de root directory Voorbeeld: find / -name mijnbestand
<b>echo tekenreeks</b>	Schrijf de tekenreeks (string) "tekenreeks" naar het standaard uitvoerapparaat Voorbeeld: echo hallo
<b>commando &gt; bestand</b>	Leid de normale scherm-uitvoer van het commando "commando" naar het bestand "bestand" Voorbeeld: ls > mijnls
<b>command &gt;&gt; file naar het bestand</b>	Leid de normale scherm-uitvoer van het commando "commando" "bestand". Als het bestand al bestaat, voeg de gegevens dan achteraan het bestand toe. Voorbeeld: ls >> mijnls
<b>man commando</b>	Toon de online helppagina's over "commando" Voorbeeld: man ls

Noot: De *schuin* getoonde woorden zijn geen commando's; op die plaats dienen de gewenste waarden ingevuld te worden.



Voor aanvullende informatie over het gebruik van deze commando's en gereedschappen tik je "commando

-help" of "man commando" in het console-scherm.

Om bijvoorbeeld meer over het commando "ls" te weten te komen, tikt u 1 van de volgende 2 mogelijkheden in:

- 1) ls --help
- 2) man ls

Gereedschappen (Kijk alstublieft in het Windows-hoofdstuk voor uitgebreide informatie over deze gereedschappen.)

<b>ping host</b>	Controleer verbinding met de machine "host" Voorbeeld: ping www.google.com
<b>tracert host</b>	Toon de route waarlangs de pakketjes naar de "host"-machine reizen. Voorbeeld: tracert www.google.com
<b>ifconfig</b>	Toon informatie over de actieve interfaces (ethernet, ppp, etc.) in de computer
<b>route</b>	Toon de route tabel (routing table)
<b>netstat</b>	Toon informatie over de status van het netwerk en de gemaakte verbindingen met machines op afstand Voorbeeld: netstat -an

### Vergelijking van basis commando's tussen Windows en Linux

Deze tabel toont van de basis-commando's welke commando's een zelfde werking hebben. Commando's moeten uitgevoerd worden vanaf een console (in Linux) of vanaf een MS-DOS-scherm (in Windows).

Linux	Windows
command --help	command /h, command /?
man command	help command
cp	copy
rm	del
mv	move
mv	ren
more, less, cat	type
lpr	print
rm -R	deltree
ls	dir
cd	cd
mkdir	md
rmdir	rd
route	route print
tracert -l	tracert
ping	ping
ifconfig	ipconfig



## 2.5. Oefeningen

### 2.5.1 Oefeningen in Windows

1. Ga naar een MS-DOS-scherm.
2. Ga na met welke MS-DOS-versie je werkt. Noteer welke versie het is en met welk commando je er achter bent gekomen.
3. Ga na wat de systeem-datum en -tijd is. Wanneer dit fout is ingesteld, stel het dan goed in. Welk commando heb je gebruikt?
4. Ga na welke mappen en bestanden er bestaan in de map "c:\". Welk commando heb je gebruikt?
5. Maak de map c:\hhs\les0. Kopieer alle bestanden met de extensie ".sys" die zich in "[c:\](#)" bevinden naar deze map. Welke bestanden heb je gevonden? Welke commando's heb je gebruikt?
6. Stel het IP-adres van je host vast. Welk commando heb je gebruikt? Welk IP-adres heb je zelf?
7. Stel vast langs welke route je pakketjes naar "[www.google.com](#)" reizen. Noteer de IP-adressen van de tussenliggende stations.

### 2.5.2 Oefeningen in Linux



1. Stel vast wie de eigenaar is van het bestand "passwd". (Noot: eerst moet je vaststellen waar dat bestand zich bevindt). Welk commando heb je gebruikt?
2. Maak de map "werk" in je eigen home directory (dus als bijvoorbeeld je inlognaam "mijnlogin" is, maak je de map in "/home/mijnlogin"), en kopieer je het bestand "passwd" naar de map "werk" die je zojuist hebt gemaakt. Stel vast wie de eigenaar is van het bestand "passwd" dat zojuist gekopieerd is.
3. Maak de map ".hide" in de map "werk". Toon de inhoud van die map. Wat moest je doen om de inhoud van de map ".hide" te zien?
4. Maak het bestand "test1" met als inhoud "Dit is de inhoud van bestand test1" in de map "werk". Maak het bestand "test2" met de inhoud "Dit is de inhoud van bestand test2" in de map "werk". Kopieer de inhoud van de zojuist gemaakte bestanden naar een bestand met de naam "test". Welke commando's heb je gebruikt?
5. Stel de naam en het IP-adres van je eigen machine vast. Welke commando's heb je gebruikt?  
Wat is je IP-adres?
6. Volg de route naar "[www.google.com](#)". Noteerd de IP-nummers van de tussenliggende machines.



### 2.5.3 Oefening 3

Vul de volgende tabel in met overeenkomende commando's en gereedschappen in Windows en Linux. Bijvoorbeeld: het Linux commando "command -help" is vergelijkbaar met het Windows

commando "command /h". Een ander voorbeeld: "cp" in Linux doet hetzelfde als het commando "copy" onder Windows..

	
command --	command /h
help	h
cp	copy
	del
mv	
more	
	print
ls	deltree
cd	
	md
route	rd
	tracert
Ping	
	ipconfig





## Als je meer wil weten

Voor een uitgebreide verzameling termen kun je de volgende URLs bezoeken:

<http://www.matisse.net/files/glossary.html>

<http://www.uic.edu/depts/accc/inform/v106.html>

<http://www.catb.org/~esr/jargon/>

Windows – voor aanvullende informatie over commando's en gereedschap typ je "command /h" of

"command /?", of "help command" vanaf een MS-DOS-scherm.

Linux – voor aanvullende informatie over commando's en gereedschap typ je "command --help" of "man command" vanaf een console.