

25-9-2015 5:45 Leestijd 4 - 5 minuten

Als je andermans computer wilt binnengaan, moet je een ingang zien te vinden. In de tweede les over hacken gaan we informatie vergaren, poorten scannen en *fingerprints* van besturingssystemen verzamelen.

Eerste hulp bij hacken. Zo kom je iemand anders' computer binnen

Correspondent Hacken



[Dimitri Tokmetzis](#)



Illustratie: Rob van Barneveld (voor De Correspondent)

Je wilt onopgemerkt een kantoor binnenkomen. De hoofdingang sla je dus maar over. Om het gebouw heen lopend, zoek je naar deuren en ramen die niet goed afgesloten zijn. Je morrelt wat aan klinken, in de hoop dat iemand slordig is geweest.

Daar staat iemand een sigaretje te roken. Een werknemer? Hopelijk laat die je binnen. Dan zie je daar wel hoe je andere dichte deuren kunt omzeilen, of je mensen moet bedotten, toegangspasjes

afhandig dient te maken. Alles om tot de boardroom door te dringen, vanwaaruit je het bedrijf over kunt nemen.

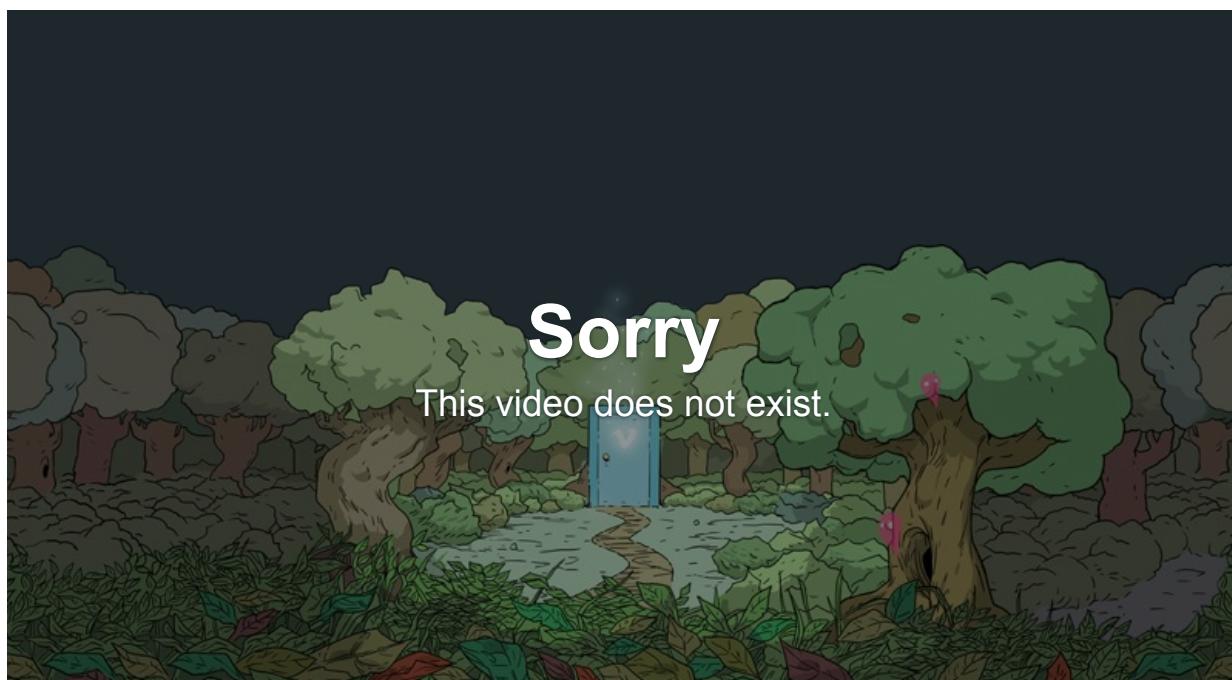
Als je een computer wilt binnendringen, doe je eigenlijk hetzelfde. Je morrelt aan de poorten en probeert de software zo gek te krijgen je erin te laten. Als dat eenmaal gelukt is, probeer je steeds meer macht te verzamelen. Totdat je de machine geheel onder controle krijgt.

Op zoek naar kwetsbaarheden

Met een hackgroep van twintig Correspondentlezers is de eerste stap al gezet. De groep kreeg een simpele opdracht: vind op de redactie van De Correspondent mijn server. Zoek uit

welke programma's op die server staan. Als je dat weet, kun je namelijk op zoek naar kwetsbaarheden.

We gebruiken [Kali Linux](#), een besturingssysteem voor hackers. *Ik heb enkele dagen geleden de ontwikkelaars van Kali Linux gesproken en zal daar binnenkort een verhaal over publiceren.* Kali Linux biedt mogelijkheden voor het scannen van andere computers, het vinden van kwetsbaarheden in software, het exploiteren van die kwetsbaarheden, het onderscheppen van netwerkverkeer en meer.



In deze teaser van de zojuist uitgebrachte tweede versie van Kali Linux krijg je een idee wat het besturingssysteem zoal kan.

Stap 1. De server vinden

Op ons netwerk zijn soms tientallen computers aangesloten - laptops, smartphones, de printer. Onze router geeft ieder apparaat een intern IP-adres, vaak iets in de trant van 192.168.178.xxx, waarbij de x het unieke nummer is op ons netwerk.

Maar hoe vinden we het IP-adres van ons doelwit? Daarvoor heb ik [een IP-scannerapp](#) op mijn smartphone die met één druk op de knop het hele netwerk

scant, rapporteert welke apparaten hij tegenkomt en hoe die heten.

Een stel onverlaten verandert ondertussen het wachtwoord, dat ik blijkbaar niet goed beveiligd had

Kali Linux heeft ook een aantal programma's dat we kunnen gebruiken. De belangrijkste is Nmap, een heel populair opensourceprogramma. Ik kom zo nog uitgebreid terug op wat dit wonderbaarlijke stuk software allemaal kan. Voor nu is het belangrijk dat we met een simpel commando ([in de command line](#)) het hele netwerk in kaart kunnen brengen:

```
nmap -sL 192.168.1.0/24 | grep "("
```

Waar die zin voor staat?

- nmap: Start het programma Nmap.
- -sL: Zoek de hostnames op het netwerk dat ik zo ga geven. Een hostname is de naam van een verbonden apparaat.
- 192.168.1.0/24: zoek alle adressen op ons netwerk.
- | grep "(": ik wil geen lijst met alle mogelijke IP-adressen (255 stuks) maar alleen van verbonden apparaten. Zoek daarom op zinnen waar een (in staat. Niet de meest charmante oplossing, maar wel effectief.

De *output* laat een aantal apparaten zien. Voornamelijk pc's en smartphones, maar ook de router (een stel onverlaten verandert ondertussen het wachtwoord, dat ik blijkbaar niet goed beveiligd had), de printer (en laten die meteen maar even wat prints met '*hello correspondent*' uitbreken) en mijn server genaamd

'corriepl.'

We hebben 'm gevonden.

Stap 2. Zoek uit welke software op de server draait

Maar hoe?

Ook hier biedt Nmap uitkomst. Maar dan moet je eerst weten wat een poortscanner doet.

IEDERE COMPUTER DIE DATA NAAR EEN ANDERE COMPUTER stuurt, gebruikt poorten.



IEDER SOORT DATAVERKEER GEBRUIKT EEN EIGEN POORT, ZODAT DATASTROMEN GE-SCHEIDEN BLIJVEN.



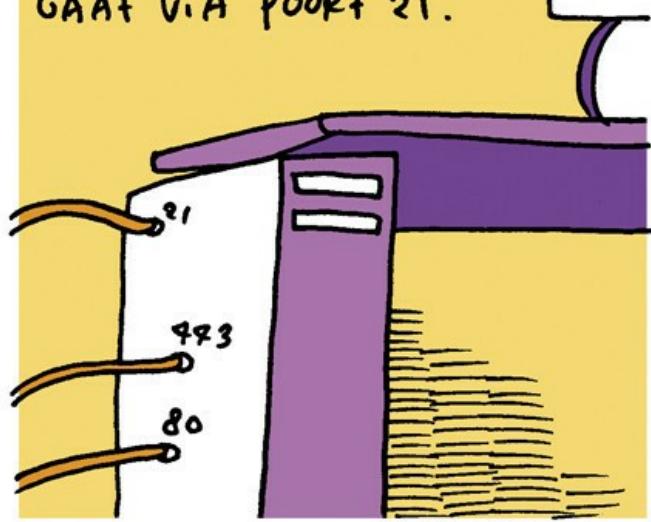
JE BROWSER VRAAGT WEB-PAGINA'S MEESTAL OP VIA POORT 80.



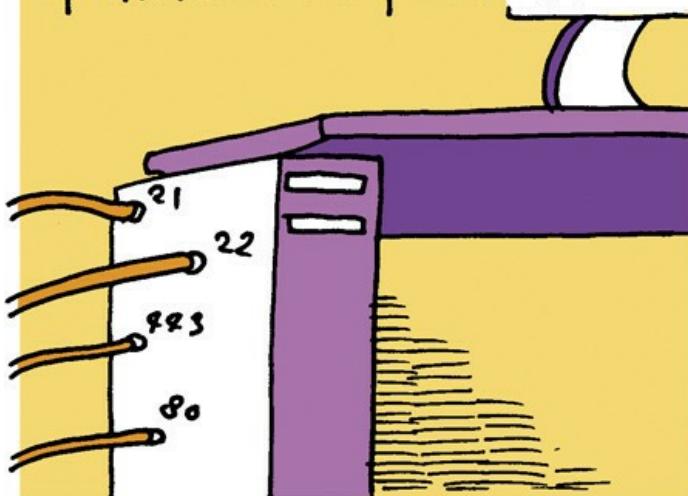
DE PAGINA WAAROP JE DIT VERHAAL LEEST, IS BEVEILIGD (HTTPS). DIE GEBRUIKT POORT 443.



FTP-VERKEER (VOOR HET
VERSTUREN VAN BESTANDEN)
GAAT VIA POORT 21.



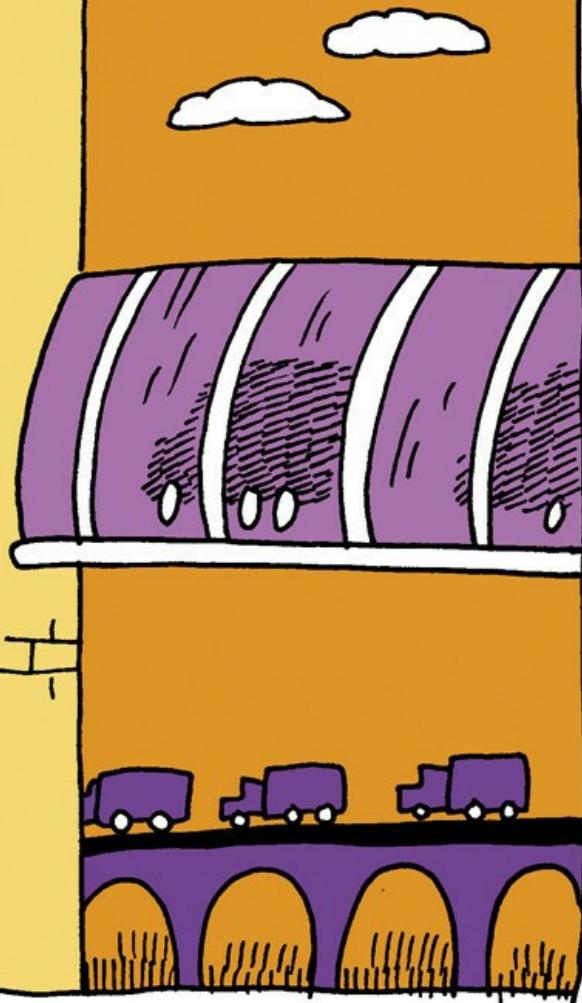
SSH (SECURE SHELL, TOEGANG
TOT EEN COMPUTER VOOR BEHEER
OP AFSTAND) VIA POORT 22.





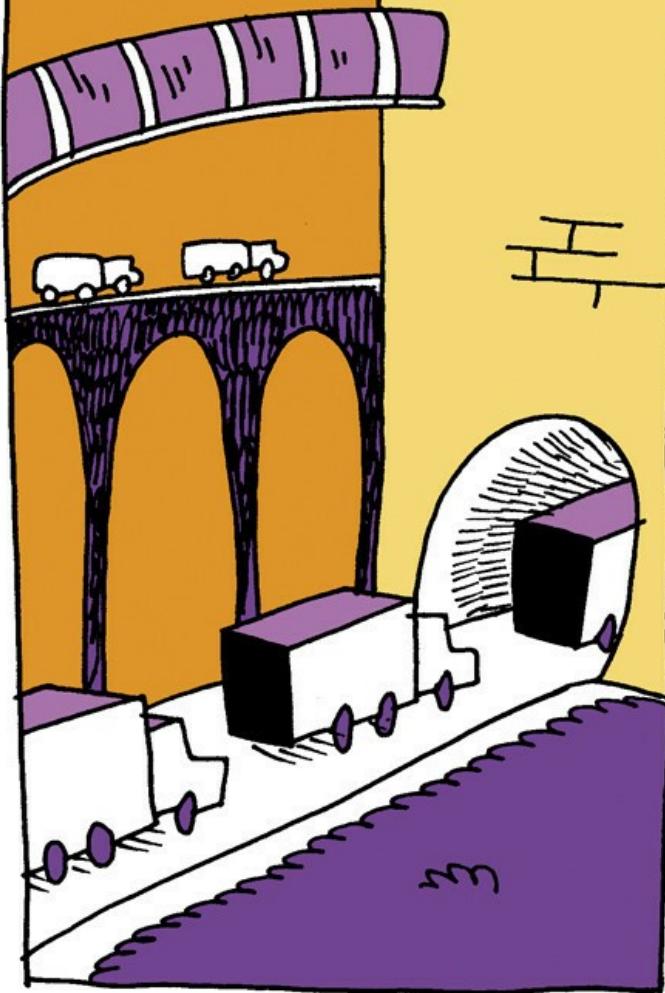
GEREGISTREERDE POORTNUMMERS
(1024-49152)

ZOALS EEN ANONIMISERINGS-
PROTOCOL OF EEN GAME-
PROGRAMMA



PRIVATE OF DYNAMICHE
POORTNUMMERS (49152-65535).

Iedereen kan deze
gebruiken.



Met Nmap kun je die poorten stuk voor stuk afgaan. Dat werkt zo.

MET NMAP KUN JE EEN
COMPUTER SCANNEN,
Bij VOORBEELD OP ZOEK NAAR
GATEN IN DE BEVEILIGING

HET IS EEN PROGRAMMA
DAT JE OP DE COMMAND
LINE GEBRUIKT



NMAP WERKT ALS VOLGT:
JE RICHT HET OP EEN
DOELWIT.



BIJVOORBEELD 95.211.235.78
(HET IP-ADRES VAN
DECORRESPONDENT.NL)

NMAP STUURT EEN AANTAL
VERSCHILLENDÉ PAKKETJES
DIE OP ALLE POORTEN BONKEN
EN IN VERSCHILLENDÉ TALEN
DINGEN VRAAGT





MAAR VAAK KRIJGT NMAP
WEL ANTWOORD. DAN ROEPT
EEN WEBSERVER BIJVOORBEELD:

JA HOOR, IK WIL JE
BEST EEN WEBPAGINA
STUREN

TROUWENS, IK
BEN APACHE VAN
VERSIE X

HET KAN ZIJN DAT ER EEN
FIREWALL IS GEINSTALLEERD.
DIE ZET DE POORTJES DICKT
DIE NIET GEBRUIKT WORDEN

EN ALS HET EEN GOEDE FIREWALL IS, KIJKT HIJ OOK NAAR WIE ER VOOR DE POORT STAAT.
ALS HIJ DE ONGENOODE GASTEN NIET VERTROUWT, GOOT HIJ ALLE POORTEN DICKT.



ALS JE WEET WELKE POORTEN OPEN STAAN EN WELKE SOFTWARE ER ACHTER ZIT, KUN JE OP ZOEK GAAN NAAR LEKKEN.



OP INTERNET IS HET VRIJ; MAKELIJK TE VINDEN WELKE ZWAKHEDEN IN WELKE SOFTWARE ZITTEN

MET EEN PROGRAMMA ALS
METASploit KUN JE EEN DATA-
BASE MET ZWAKHEDEN DOOR-
ZOEKEN EN AFVUREN OP DE
BETREFFENDE ZWAKKE POORT



Die software (een exploit)
is dan het breekijzer
waarmee je binnen kunt
komen



Ik test dit op mijn server.

Ik ga eerst op zoek naar het IP-adres van de server, dus:

```
nmap -sL 192.168.1.0/24
```

De server blijkt op 192.168.1.37 te zitten.
Dan ga ik wat commando's proberen,
maar eigenlijk is het meteen al raak.

Ik schrijf:

- nmap -sV -v 192.168.1.37 en zeg eigenlijk:
- nmap: start nmap op.
- -sV: als je een open poort vindt, zoek dan voor me uit wat voor software daarachter 'luistert'. *Met luisteren bedoel ik dat software actief is, in die zin dat hij wacht op inkomend verkeer, wat vrij logisch is bij een server die op het internet is aangesloten.*
- -v: staat voor verbose, dus vertel me stap voor stap wat je aan het doen bent.
- en dan het IP-adres.

Na 47 seconden krijg ik deze informatie terug:

```
1. dimitritokmetzis@MacBook-Pro: ~ (zsh)
→ ~ nmap -sV -v 192.168.1.37

Starting Nmap 6.49BETA3 ( https://nmap.org ) at 2015-09-24 15:44 CEST
NSE: Loaded 33 scripts for scanning.
Initiating Ping Scan at 15:44
Scanning 192.168.1.37 [2 ports]
Completed Ping Scan at 15:44, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:44
Completed Parallel DNS resolution of 1 host. at 15:44, 0.02s elapsed
Initiating Connect Scan at 15:44
Scanning 192.168.1.37 [1000 ports]
Discovered open port 22/tcp on 192.168.1.37
Discovered open port 80/tcp on 192.168.1.37
Discovered open port 443/tcp on 192.168.1.37
Discovered open port 9091/tcp on 192.168.1.37
Discovered open port 10000/tcp on 192.168.1.37
Completed Connect Scan at 15:44, 0.09s elapsed (1000 total ports)
Initiating Service scan at 15:44
Scanning 5 services on 192.168.1.37
Completed Service scan at 15:44, 16.04s elapsed (5 services on 1 host)
NSE: Script scanning 192.168.1.37.
Initiating NSE at 15:44
Completed NSE at 15:45, 30.60s elapsed
Nmap scan report for 192.168.1.37
Host is up (0.0051s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
80/tcp    open  http   Apache httpd 2.2.22 ((Debian))
443/tcp   open  ssl/http Apache httpd 2.2.22 ((Debian))
9091/tcp  open  http   Transmission BitTorrent management httpd (unauthorized)
10000/tcp open  http   MiniServ 1.760 (Webmin httpd)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/local/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 47.65 seconds
```

De uitvoer van mijn commando in Nmap.

Wat zien we hier?

Nmap wordt gestart en gaat op zoek naar hosts en vindt een aantal open poorten. Tegen het einde zien we een overzichtje met PORT, STATE, SERVICE en VERSION. Dit zijn de poorten die openstaan. De service die erachter draait

is vooral http (dus webverkeer), maar ook ssh (beveiligde toegang op afstand) en ssl/http (beveiligd webverkeer).

Ik zie ook een lijst met soorten software, zoals OpenSSH, versie 6.0p1. Mijn server is ook een webserver, gezien het gebruik van Apache. Er zit een torrentclient op poort 9091 en Webmin (ook beheer op afstand) op poort 10000.

Met deze informatie kan ik op zoek gaan in verschillende [exploitdatabases](#). Ik vul dan bijvoorbeeld Apache 2.2.22 in en zie of er bepaalde zwakheden bekend zijn waar ik gebruik van kan maken.

Mijn server geeft al snel zijn geheimen prijs. Ik heb er geen goede *firewall*. *Een firewall is software die ongewenst internetverkeer kan tegenhouden. Je kunt zelf de regels bepalen wat wel en wat niet door de firewall mag. Op zitten (er staan*

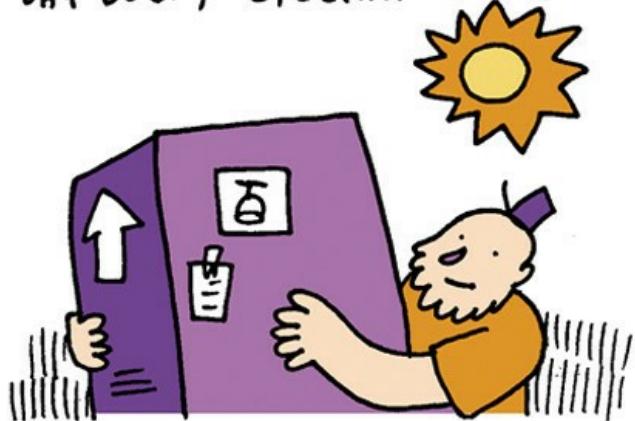
alleen twee torrentfiles *Torrentfiles zijn bestanden die je deelt met andere internetgebruikers. De bestanden in kwestie zijn de gelekte documenten van de Gamma International hack en de bestanden van Hacking Team die onlangs zijn gehacked.* op). Een beetje systeembeheerder beschermt zijn servers wel wat beter.

Maar hoe kom je daar dan binnen?

Je kunt bijvoorbeeld kiezen wat voor soort poorten je scant, UDP of TCP.



DEZE PROTOCOLLEN KUN JE
ZIEN ALS VERHUIZERS DIE
MET DOZEN VOL DATA SJOUWEN.
MAAR DE MANIER WAAROP ZE
DAT DOEN, VERSCHILT NOGAI.



TCP (TRANSMISSION Control
Protocol) IS EEN KEURIGE
MENEER



VOORDAT HIJ DATA VERZENDT,
MELOFT HIJ ZICH EERST NETJES
BIJ DE SERVER. HIJ ZEGT DAN:

SYN

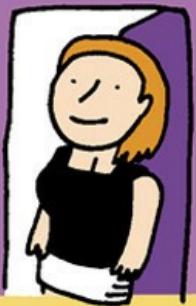
DE SERVER WEET DAN
DAT ER DATA GAAN KOMEN

DE SERVER STUURT DAAROP
EEN BERICHT TERUG:

Ack

WAT ZOVEEL WIL ZEGGEN ALS:
"IK HEB JE BOODSCHAP ONTVANGEN
EN BEN ER KLAAR VOOR".

HET KEURIGE TCP STUURT
VOOR DE ZEKERHEID DAN NOG
EEN BERICKTJE:



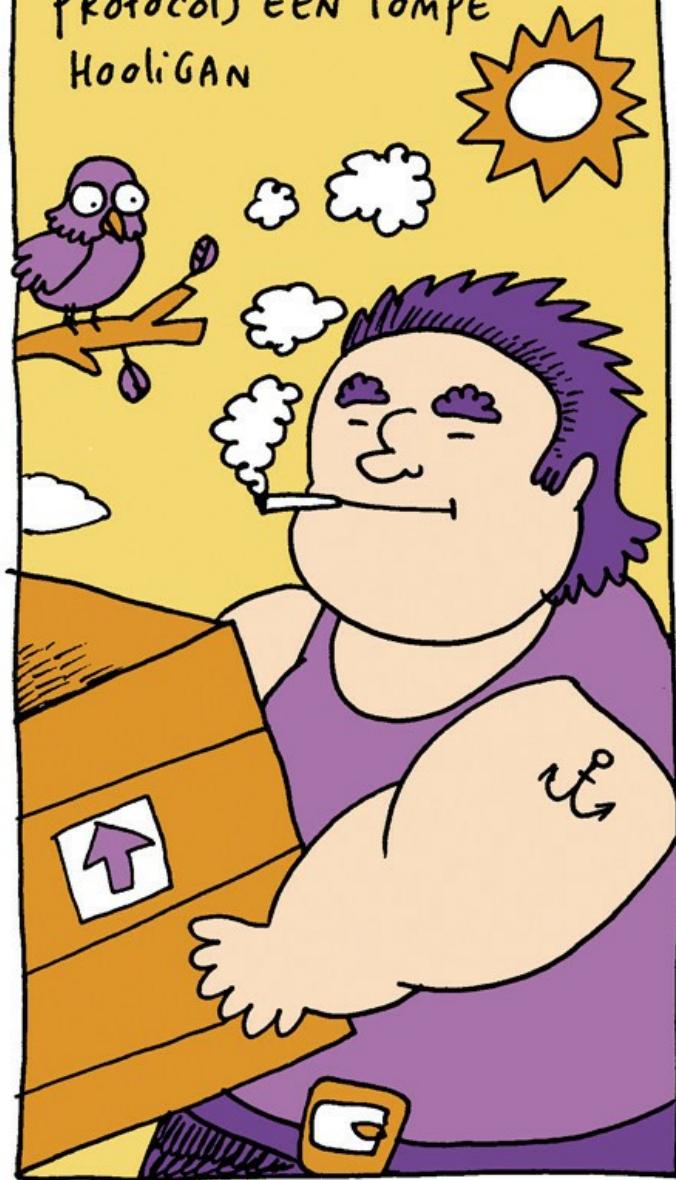
"IK HEB JE BEGREPEN". PAS
DAN KOMT DE DATATRANSFER
GOED tot STAND.

AF EN TOE STEMMEN ZE NOG
EVEN MET ELKAAR AF OF ALLE
DATA WEL ECHT IS AANGEKOMEN
EN VERGELIJKEN ZE HET AANTAL
VERZONDEN Bits.



AAN HET EINDE STUURT HIJ
NOG EEN BERICKTJE DAT HIJ
KLAAR IS; FIN.

VERGELEKEN MET TCP IS
UDP (USER DATAGRAM
Protocol) EEN lompe
HooliGAN



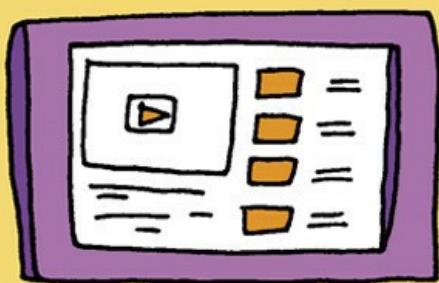
Hij introduceert zich
niet, maar smijt al
zijn data zo snel
mogelijk richting de
server.



HET KAN UDP NIETS SCHELEN
OF DE PAKKETJES WEL ZIJN
AAN GEKOMEN



TOCH BIEDT UCP EEN GROOT
VOORDEEL, NAMELIJK EFFICIËNTIE.
ERG HANDIG BIJ HET STREAMEN
VAN VIDEO'S.



DE NETTE TCP HEB JE DAN
HELEMAAL NIET NODIG.



Maar je kunt ook net doen alsof je vanaf een heel andere computer scant (IP-spoofing). Je kunt in plaats van een 'SYN'-bericht (zie strip hierboven) een

'ACK'-berichtje sturen, waardoor sommige *firewalls* denken dat de verbinding al is geaccepteerd. Je kunt ook heel specifiek op een poort scannen, bijvoorbeeld op poort 23 (telnet). Én je kunt complete scripts schrijven met wat er moet gebeuren als een bepaalde software wordt ontdekt. Nmap is zo krachtig dat het programma zelfs wordt gebruikt om het hele internet in kaart te brengen.

Voor de goede orde: het scannen van poorten en het achterhalen welke software er op een server draait, is maar een van de manieren om kwetsbaarheden te vinden. Je kunt ook de systeembeheerder bellen met een smoes, of een werknemer een phishingmail *Een phishingmail is een mail waarin je een document of link stuurt vanwaaruit kwaadaardige software wordt gedownload, of die het slachtoffer naar een nagemaakte*

site brengt. Op die manier kan er informatie worden gestolen, zoals bijvoorbeeld wachtwoorden. sturen. Waarbij ik even wil opmerken dat je dit dus niet moet doen, want illegaal, onethisch, etc.

Nu we de structuur van ons lokale netwerk in kaart hebben gebracht en mijn server zijn binnengekomen, wordt het tijd om de software te kraken. Zitten er kwetsbaarheden in? Daarover meer in de volgende aflevering van deze reeks.

Illustraties door [Rob van Barneveld](#). Met dank aan Bert van der Lingen en Stefan van der Wal voor hun nuttige adviezen.

Eerder in deze serie:

Oproep

Heb jij nog sterke verhalen over (poort)scannen? Welke tools gebruik jij het liefste? En voor de leken, heb je nog vragen over het scannen?