

**HO  
GENT**



# Cybersecurity

## 6. Het 5x9 principe



## **6. Het 5x9 principe**

6.1 Hoge beschikbaarheid

6.2 Maatregelen om de beschikbaarheid te verbeteren

6.3 Incident response

6.4 Disaster recovery

6.5 Verkenning en enumeratie

**HO  
GENT**

## **6.1 Hoge beschikbaarheid**

**HO  
GENT**

## Wat is het 5x9 principe?

- Wordt in het Engels **the Five Nines** genoemd
- Systemen en services kennen een uptime van 99,999%
- Ofwel: ze zijn beschikbaar in 99,999% van de tijd
- Concreet: downtime bedraagt minder dan 5,26 minuten per jaar

Availability	Downtime / Year	Downtime / Month	Downtime / Week	Downtime / Day
99.999%	5.256 Mins	0.438 Mins	0.101 Mins	0.014 Secs
99.995%	26.28 Mins	2.19 Mins	0.505 Mins	0.072 Secs
99.990%	52.56 Mins	4.38 Mins	1.011 Mins	0.144 Secs
99.950%	4.38 Hrs	21.9 Mins	5.054 Mins	0.72 Secs
99.900%	8.76 Hrs	43.8 Mins	10.108 Mins	1.44 Mins
99.500%	43.8 Hrs	3.65 Hrs	50.538 Mins	7.2 Mins
99.250%	65.7 Hrs	5.475 Hrs	75.808 Mins	10.8 Mins
99.000%	87.6 Hrs	7.3 Hrs	101.077 Mins	14.4 Mins

**HO  
GENT**

## Wat is het 5x9 principe?

- Hoge beschikbaarheid kan je bekomen door:
  - **Single points of failure** vermijden (zie ook H.2)
  - **Robuuste** systemen bouwen
  - **Monitoren** van de systemen
  - Failures / problemen **detecteren** wanneer ze zich voordoen.
  - **Redundancy** en **backups**.

**HO  
GENT**

Voorbeeld van monitoring: hoe goed zijn jouw SSD' s en HDD' s nog? Controleer het met CrystalDiskInfo ( <https://crystalmark.info/en/software/crystaldiskinfo/> ).

## 6.1 Hoge beschikbaarheid

### Omgevingen met hoge beschikbaarheid (cruciale sectoren).

- Financiële sector:
  - Trading, diensten beschikbaar voor klant, vertrouwen van de klant
- Gezondheidssector:
  - Patiëntenzorg de klok rond
- Industrie
  - Fabrieken, assemblage, ...
- Transportsector:
  - NMBS, luchtvaart, ...
- Openbare veiligheid:
  - Staat in voor de veiligheid van de gemeenschap (brandweer, politie, leger, ...)
- Nutvoorzieningen:
  - Energiecentrales, waterzuiveringsstations, ...
- Telecom sector:
  - Telefoon, internet, TV, ...
- Retail industrie:
  - Supply chains, leveren van producten, ...
  - Denk aan de eindejaarsperiode



## Bedreigingen van de beschikbaarheid

- Er zijn heel wat oorzaken van **verlies van beschikbaarheid**.  
Van het falen van systeem tot een natuurramp.
  - System failure
  - Niet-doelbewuste oorzaak
  - Doelbewuste aanval
  - Natuurramp



## Hoge beschikbaarheid

**Grote storing bij Telenet:  
enkele ziekenhuizen, politie  
van Antwerpen, veel  
bedrijven... tijdlang  
telefonisch niet bereikbaar**

17/09/2020 om 10:07 door Arthur De Meyer | Bron: BELGA - [Print](#) - [Citeer](#)



Het Universitair Ziekenhuis van Gent, een campus van de UZ Leuven en de ziekenhuizen van ZNA waren donderdagvoormiddag een tijdlang telefonisch niet bereikbaar. "De oorzaak is een probleem bij onze provider Telenet", klinkt het bij UZ Gent. Telenet bevestigt dat, maar omstreeks 10 uur was de storing van de baan. Ook de Blauwe Lijn van de Antwerpse politie en de Antwerpse brandweer waren een tijdlang onbeschikbaar.

"We hebben vannacht werken uitgevoerd aan ons netwerk", zegt de Telenet-woordvoerder. "Daarbij is een probleem opgetreden waardoor donderdag een heel deel van onze zakelijke klanten niet bereikbaar zijn." Onder meer UZ Gent, UZ Leuven en enkele Antwerpse ziekenhuizen waren getroffen, en ook de politie- en brandweerzone van Antwerpen.

Hoeveel bedrijven getroffen werden door de storing is niet geweten. "Het gaat om een groot deel, over heel Vlaanderen", aldus nog Geeraerts. "Exacte cijfers hebben we niet." Omstreeks 10 uur waren de problemen van de baan. "Alle getroffen bedrijven, waaronder ook een tiental ziekenhuizen, zijn weer bereikbaar", klinkt het.

**HO  
GENT**

Bron: [https://www.nieuwsblad.be/cnt/dmf20200917\\_92485312](https://www.nieuwsblad.be/cnt/dmf20200917_92485312)

## 6.1 Hoge beschikbaarheid

### Why Did the Tokyo Stock Exchange Halt Trading?

October 21, 2020 by Eugene Grygo

SHARE THIS STORY



JOIN THE DISCUSSION



In a bid to honor the fading art of the follow-up story, I have been rooting around to find out what has happened to the Tokyo Stock Exchange (TSE) since its systems outage earlier this month.

To remind you, the TSE had an unprecedented halt to trading for a full day on Oct. 1, but resumed trading on Friday, Oct. 2. It appears that hardware glitches and a series of mishaps forced the long stoppage, according to TSE officials. Officials at TSE and Fujitsu, a major IT supplier to the exchange, have acknowledged the IT problems and have apologized for them.



Grygo is chief content officer for FTF.

Officials have done more than apologize.

Last week, TSE's owner Japan Exchange Group sent an incident report to Japan's market regulator, the Financial Services Agency (FSA), according to the *Reuters* news agency and *Japan Times*. In addition, officials issued a report on the TSE website on Oct. 19 that provides more preliminary details.

What appears to be certain is that the glitch was not the result of a cyber-attack because the IT platforms involved did not have external connections, according to a report in *The Wall Street Journal*.

Initially, the blame is being put on magnetic-disk devices — used to warehouse trading information — that failed. In addition, a backup hardware system also malfunctioned, according to media reports and TSE statements.

For the moment, the TSE's report, "Cash Equity Trading System Failure on Oct. 1," is serving as the initial investigation.

For starters, the exchange has "a system requirement that operations should continue in the case of a NAS [Network Attached Storage] failure by switching over to another device within 30 seconds," according to the report.

"When we developed the current version of arrowhead [a hardware and software system developed by Fujitsu], we discussed with Fujitsu what NAS setting would be appropriate with reference to the Fujitsu product manual," according to the report.

"Since the product manual said the automatic switchover would function regardless of the NAS setting, we decided on the NAS setting taking into account the past performance of arrowhead with the same

Bron: <https://www.ftfnews.com/why-did-the-tokyo-stock-exchange-halt-trading/28027>

## 6.1 Hoge beschikbaarheid

### Venezuela power outage caused by US Cyber Attack

Posted by Naveen Goud



The populace in Venezuela is reigning under a power blackout which is suspected to have been caused by hackers backed by US Intelligence. Well, President Nicholas Maduro said so and added in his statement that his government has enough evidence to prove his claims.

However, a statement issued by the US official a few hours ago, says that last Thursday's blackout was not caused by any foreign interference, but occurred due to local corruption and mismanagement of the power corporation officials.

Going further into details, from Thursday last week, a glitch at the Guri Hydroelectric power station is said to have left the country reign under a power outage. Though the power was restored within 24 hours in some parts of the country, many of the regions were still in dark until Saturday.

Furthermore, few of the systems at the Sidor power plant were again knocked down at the grid on Saturday afternoon impacting the entire populace. FYI, Sidor power station has been sustaining the country's power supply until the Guri system was being repaired, which is supposed to supply 80% of the country's power.

"Till early Saturday, most of the systems i.e. around 70% of them were restored when we received info of another cyber incident at mid-day that disrupted the re-linking process impacting everything that had been restored before that hour. The news is out that infiltrators targeted the back-up systems in the second attack which led to major consequences in the electric company. It is a kind of electric war waged by the United States", said President Nicolas Maduro.

While Jorge Rodriguez blamed the outage a well-orchestrated incident of US Intelligence. 🇺🇸

**HO  
GENT**

Bron: <https://www.cybersecurity-insiders.com/venezuela-power-outage-caused-by-us-cyber-attack/>

## **6.2 Maatregelen om de beschikbaarheid te verhogen**

**HO  
GENT**

## Assets management

- Bedrijven moeten weten welke **hardware-** en **software assets** in het bedrijf aanwezig zijn. Deze assets moeten namelijk beveiligd worden.
- **Assets management:** omvat het **beheren** van al deze **assets**. Er dient een volledig overzicht (= inventaris) te zijn van alle hard- en software.
- Het bedrijf kan dan een **inschatting** maken welke **beveiligingsgevaaren** er zouden kunnen zijn.

**HO  
GENT**

## Assets management (cont.)

- Volgende zaken worden in beschouwing genomen:
  - Elk hardware systeem
  - Elk besturingssysteem
  - Elk hardware netwerk toestel
  - Elk network device operating system
  - Elke software applicatie
  - Elke firmware
  - Alle language runtime environments
- Sommige bedrijven kiezen voor een **automatische inventarisatie**: software die automatisch deze zaken bijhoudt.

## Assets management (cont.)

- **Asset classificatie:** groepeer alle resources van een organisatie op basis van gemeenschappelijke kenmerken. Organisaties moeten documenten, data records, bestanden, schijven, etc. gaan classificeren.
- **Identificatie van de bedreiging:** De United States Computer Emergency Readiness Team (US-CERT) en het U.S. Department of Homeland Security hebben een overzicht van vaak voorkomende kwetsbaarheden: common vulnerabilities and exposure (CVE). De CVE identificatie geeft meer informatie over deze kwetsbaarheden.

**HO  
GENT**

<https://cve.mitre.org/>

<https://twitter.com/CVEnew>

## Assets management (cont.)

- **Risk Analysis:** is het proces om een **inschatting** te maken van gevaren van zowel natuurlijke of menselijke invloeden.
- **Mitigation:** het **verminderen** van het **risico** of het verkleinen van de kans op een aanval. Een aantal technische zaken om het risico te verminderen zijn bvb. gebruiken van authenticatie, rechten op bestanden instellen, het gebruiken van een firewall, etc.



## Een diepe verdediging



- Een verdediging in **verschillende lagen** zorgt niet voor een scherm waar je niet kan binnendringen. Het zorgt wel dat je de cybercrimineel vaak een stap voor bent. Wanneer de verdediging op **verschillende niveaus** of in verschillende lagen plaatsvindt, vermijd je het risico op een geslaagde aanval.
- Een **gelaagde beveiliging** zorgt voor de meest omvangrijke beveiliging. Als cybercriminelen de eerste laag kunnen binnendringen, is er nog altijd een tweede (en evt. volgende) laag die ze moeten binnendringen. Beveiligen in lagen betekent dat je **meerdere barrières** gaat maken.
- Het **beperken van toegang** tot informatie vermindert de kans op een aanval. Een organisatie beperkt best de toegang om er voor te zorgen dat werknemers alleen toegang hebben tot de informatie die zij **nodig hebben** om hun job uit te voeren.

**HO  
GENT**

Vgl. Kasteel (LoR)

## Een diepe verdediging (cont.)

- **Diversiteit** : varieer in manieren van beveiliging. Wanneer men zich de toegang heeft verschaft tot de ene laag, mag dit niet de andere lagen in gevaar brengen. Zorg dus voor afwisseling: gebruik bijvoorbeeld in de andere lagen een ander encryptie algoritme.
- **Obscuring** of **verduisteren** van informatie kan deze ook beschermen. Een organisatie hoeft bijvoorbeeld niet prijs te geven welke OS versie of welk type firewall er gebruikt wordt.
- **Simplicity** of **eenvoud** leidt meestal tot een hogere beschikbaarheid. Als de beveiliging te complex wordt, wordt de kans op fouten ook alsmaar groter.



**HO  
GENT**

## Redundantie

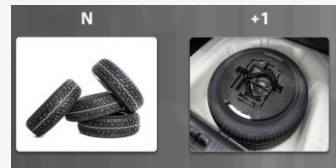


- Een **single point of failure** moet altijd vermeden worden. Dit kan zowel over hardware als data, processen, software, etc. gaan.
- Single points of failure zijn de **zwakke schakels** die ervoor kunnen zorgen dat het ganse systeem faalt.
- Een oplossing is dan dikwijls om ervoor te zorgen dat je niet op **één element** vertrouwt.
- De organisatie kan **redundantie** inbouwen om kritische processen over te nemen op de moment dat er eentje faalt. Er worden bijvoorbeeld meerdere load balancers voorzien (die eigenlijk allemaal hetzelfde doel hebben).

**HO  
GENT**

## Redundantie (cont.)

- **N+1 redundantie** is een algemeen principe. N+1 redundantie zorgt ervoor dat systemen **beschikbaar blijven** als er eentje faalt.
- Componenten (N) moeten steeds **minimum één backup** component hebben (+1)
- Voorbeeld: een auto heeft een reservewiel in de koffer voor als één van de vier wielen faalt.



## Weerstand van het systeem

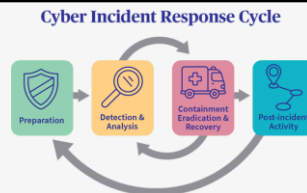
- De weerstand verwijst naar manieren en voor systemen om te zorgen dat deze systemen een **hoge tolerantie** hebben voor **falen**. Routing protocols zorgen bijvoorbeeld voor een verhoogde weerstand in een netwerk. Weerstand inbouwen is meer dan enkel redundantie voorzien.

**HO  
GENT**

## **6.3 Incident response**

**HO  
GENT**

## De incident response fase



- Incident response omvat een aantal procedures die bedrijven hanteren om te reageren wanneer een buitengewoon event plaatsvindt. Bedrijven moeten incident response plannen opstellen om **voorbereid** te zijn om het ergste. Incident response omvat **4 fasen**:
- Voorbereiding:** **planning** opstellen voor mogelijke gebeurtenissen.
  - Detectie en analyse:** het **ontdekken** van zo een gebeurtenis
  - Isoleren, uitdoven en herstellen:** inspanningen doen om de gebeurtenis te **isoleren**, eventueel te **stoppen** of **uit te doven** en dan ook de opgelopen schade trachten te **herstellen**.
  - Post-incident follow-up:** nagaan hoe dit is kunnen gebeuren, bekijken hoe dit in de toekomst kan worden **vermeden**

**HO  
GENT**

## Incident response | technologie

- Op technologisch vlak kunnen er rond incident reponse ook een aantal zaken gebeuren:
  - **Network Access Control (NAC)**: geeft toegang aan gebruikers tot een netwerk, indien zij volledig voldoen aan de **policy requirements** van de organisatie. Bijvoorbeeld, het NAC systeem eist als toestellen verbinden met het netwerk dat er een anti-virus is geïnstalleerd
  - **Intrusion Detection Systems (IDSs)**: monitort het netwerkverkeer. IDSs luisteren naar hackpogingen en ongeautoriseerde toegang. Het rapporteert, maar onderneemt geen actie.
  - **Intrusion Prevention Systems (IPSs)**: wordt op het pad tussen de bron en bestemming geplaatst. Het detecteert onmiddellijk een netwerkprobleem en pakt het ook aan. Dit wordt vaak meteen na de firewall geplaatst
  - **Advanced Threat Intelligence**: helpt organisaties om een cyberaanval te detecteren tijdens één van de fases (en soms zelfs voor de aanval plaatsvindt mits de juiste informatie).

**HO  
GENT**

NAC voorbeeld: When a computer connects to a computer network, it is not permitted to access anything unless it complies with a business defined policy; including anti-virus protection level, system update level and configuration. While the computer is being checked by a pre-installed software agent, it can only access resources that can remediate (resolve or update) any issues. Once the policy is met, the computer is able to access network resources and the Internet, within the policies defined by the NAC system. NAC is mainly used for endpoint health checks, but it is often tied to Role-based Access. Access to the network will be given according to the profile of the person and the results of a posture/health check. For example, in an enterprise the HR department could access only HR department files if both the role and the endpoint meets anti-virus minimums.

Een voorbeeld van een IDS: <https://www.snort.org/>

The IPS often sits directly behind the firewall and provides a complementary layer of analysis that negatively selects for dangerous content. Unlike its predecessor the Intrusion Detection System (IDS)—which is a passive system that scans traffic and reports back on threats—the IPS is placed inline (in the



direct communication path between source and destination), actively analyzing and taking automated actions on all traffic flows that enter the network.

## **6.4 Disaster recovery**

**HO  
GENT**

## Disaster Recovery Planning

- Soorten **rampen** – Het is nodig om een organisatie draaiende te houden wanneer er een ramp optreedt. Een ramp omvat zowel natuurlijke als menselijke acties die schade toebrengen aan assets en eigendom. Het kan de organisatie beletten om zijn activiteiten voort te zetten.
  - **Natuurramp** Natural Disasters – geologische rampen (bvb. aardbevingen), meteorologische rampen (denk aan bliksem, hagel, tornado, ...), gezondheidsramp (pandemieën, quarantaines) en overige rampen (waterlek → overstroming, brand, ...).
  - Ramp veroorzaakt **door mensen** – gebeurtenissen op het werk (staking, ontslag, en bewust trager werken), socio-politieke events (vandalisme, blokkades protesten, sabotage, terreur, ...) en onderbreking in nutsvoorzieningen (stroom, communicatie, ...)



**HO  
GENT**

## Disaster Recovery Planning (cont.)

- Er is nood aan **continuïteit** bij een onderneming. Organisaties kunnen heel wat doen om zich te wapenen tegen een (natuur)ramp. Helaas kan je niet op alles voorbereid zijn. Organisaties moeten plannen klaar hebben voor als het noodlot toeslaat.
- Men moet een aantal zaken gaan overwegen om continuïteit te garanderen. Het omvat veel meer dan te zorgen dat de **data** werd gebackupt en dat je redundantie inbouwt in de **hardware** systemen:
  - Documenteren van de configuraties
  - Zorgen voor alternatieve communicatiekanalen
  - Stroomvoorzieningen failsafe maken
  - Nagaan wat de impact voor de applicaties zijn
  - Nagaan hoe geautomatiseerde taken (tijdelijk) handmatig kunnen overgenomen worden

**HO  
GENT**

## Disaster Recovery Planning (cont.)

- Best practices:
  - Stel een **policy** op met richtlijnen om de continuïteit op verschillende vlakken te garanderen en maak een lijst met taken om deze richtlijnen uit te voeren.
  - Ga na welke **kritieke systemen** en **processen** er zijn binnen de organisatie. Prioriteer deze lijst op basis van noodzakelijkheid.
  - Identificeer de mogelijke **kwetsbaarheden**, **bedreigingen** en bereken de **risico's**
  - Identificeer en implementeer **controles** en **tegenmaatregelen** om deze risico's te beperken
  - Voorzie manieren om de kritieke systemen **terug up and running** te krijgen
  - Voorzie procedures om de organisatie ook **draaiende te houden** tijdens een chaotisch moment (bijvoorbeeld een ramp).
  - **Test** de plannen!
  - **Actualiseer** regelmatig deze plannen

## Ramp: brand



**Brand bij nucleaire faciliteit in Iran mogelijk gevolg van cyberaanval**

03 juli 2020 18:17

Laatste update: 03 juli 2020 18:54

40 NUjj-reacties



De brand die donderdagochtend (lokale tijd) plaatsvond bij de nucleaire faciliteit Natanz in Iran is mogelijk het gevolg van een cyberaanval. Drie Iraanse ambtenaren zijn daarvan overtuigd, zeggen zij anoniem tegen persbureau *Reuters*. Zij laten echter niet concreet weten waarom zij dat denken.

De atoomenergieorganisatie van Iran (AEOI) bracht donderdag een foto van het getroffen gebouw bij Natanz naar buiten. Daarop is te zien is dat de muren en het dak beschadigd zijn. Een uit haar scharnieren hangende deur suggereert dat er binnen een explosie heeft plaatsgevonden, maar dit is niet bevestigd.

Een van de bronnen van *Reuters* zegt dat een gebouw waar centrifuges in elkaar worden gezet het doelwit van de aanval was. Deze machines worden gebruikt om uranium te verrijken.

De AEOI plaatste donderdag ook een verklaring op haar - inmiddels ontoegankelijke - website. Bij het incident is "een van de technische niches beschadigd die in de open ruimte van het Natanz-terrein wordt gebouwd", aldus woordvoerder Behrouz Kamalvandi.

"Dit incident heeft niet geleid tot menselijke slachtoffers, noch heeft het de complexe routineactiviteiten in gevaar gebracht. Momenteel (donderdag rond 18.00 uur Nederlandse tijd, red.) zijn de deskundige teams van de organisatie aanwezig op de locatie en onderzoeken zij de kwestie."

Bron: <https://www.nu.nl/tech/6062246/brand-bij-nucleaire-faciliteit-in-iran-mogelijk-gevolg-van-cyberaanval.html>

Daarbij verwijst hij naar het in 2010 ontdekte computervirus Stuxnet, dat succesvol centrifuges in Natanz wist te saboteren. Nadat het virus in de nucleaire faciliteit binnen wist te komen, slaagde het erin om de centrifuges op hol te laten slaan.

## Ramp: bliksem



Bron: <https://time.com/4004192/google-data-lightning-belgium/>

Daarbij verwijst hij naar het in 2010 ontdekte computervirus Stuxnet, dat succesvol centrifuges in Natanz wist te saboteren. Nadat het virus in de nucleaire faciliteit binnen wist te komen, slaagde het erin om de centrifuges op hol te laten slaan.

## **6.5 Verkenning & enumeratie**

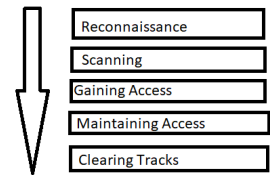
**HO  
GENT**



- In 6.2 hebben we al verwezen naar Assets management: bedrijven dienen een inventaris te maken van hun systemen. Zo kunnen ze inschatting maken naar kwetsbaarheid en stabiliteit toe.
- Diverse inventarissen worden door **hackers** ook opgemaakt en vormen de **beginfase** van het hacken.

[illegible]

## Hacking fasen



**HO  
GENT**

Hacking bestaat traditioneel uit 5 fases. De eerste 2 fases gaan over het inwinnen van allerlei informatie.

Eerst is het belangrijk om informatie in te winnen. Op basis van deze informatie kan de hacker dan proberen om zichzelf toegang te verschaffen tot een systeem. Vaak zal de hacker ook proberen om een deur open te houden: in de “toegang behouden” fase zal geprobeerd worden om zo’n deurtje open te zetten. Dit kan bereikt worden door een trojan horse of rootkit toe te voegen aan het systeem.

Hackers zullen dan achteraf alle sporen proberen uit te wissen (gemaakte accounts verwijderen, log files verwijderen, desinstalleren van programma’s, ...)

## Verkenningsfase



- EN: Reconnaissance
- **Passieve** verkenning (bvb. website bezoeken)
  - Geen directe interactie met het target
- **Actieve** verkenning (bvb. bedrijf opbellen, naamkaartje vragen, ...)
  - Directe interactie met het target
- Zonder authenticatie
- (Passieve) verkenning = niet illegaal
  - Vb. bezoeken van de webpagina van een bedrijf en kijken naar de vacatures.
- Technieken:
  - Social engineering
  - WHOIS db
  - nslookup
  - Dumpster diving

**HO  
GENT**

Verkenning is vaak niet illegaal. Het is niet verboden om een website te bezoeken en de vacatures bekijken. Er wordt meestal gebruik gemaakt van publieke informatie. Actieve verkenning (bvb. een server pingen) zou wel een spoor kunnen achter laten. Men zal eerst de voorkeur geven aan passieve verkenning.

## Verkenning

- Research doen
- Ook wel footprinting genoemd
- Zo veel mogelijk informatie inwinnen over het target, zonder dat men ontdekt wordt
- Elementaire informatie (website, welke webserver, fysieke locaties, management, branch offices, nieuwsartikels, ...)
- OS, Web servers & platformen (Windows versie, Apache, merken, ...)
- Queries uitvoeren om onderliggende infrastructuur te snappen (bvb. hosting, DB, ...).
- Nadenken over kwetsbaarheden (men kent nu de versies)

**HO  
GENT**

Hoe klein het stukje informatie ook is, soms is dat vak de sleutel die ontbreekt.

## Verkenning

- Target / organisatie begrijpen
- Beperken van aanvalsdomein (beperkte IP range, beperkt aantal toestellen, ...), op basis van ingewonnen informatie
- Vaak wordt een informatie DB opgesteld → verzamelen van ontdekte informatie
  - Wordt ook gebruikt om te prioriteren
- Layout van het netwerk maken (IP adres ranges, DMZ, firewalls, ...)

**HO  
GENT**

Aanvallers zullen voor de aanval plaatsvindt vaak al heel wat werk gedaan hebben gedurende de verkenningsfase. Bedrijven zijn zich vaak niet bewust van welke informatie publiek te vinden is. In deze fase ga je nl. op zoek welke informatie er (online) te vinden is.

## Types van verkenning

- Passief
  - Publieke informatie gebruiken (geen direct contact met target)
  - Zowel online als offline bronnen (bvb. nieuws artikels)
  - Bvb. bedrijfswebsite gebruiken, welke manier van inloggen, ...
- Actief
  - Direct contact met target (vaak social engineering)
  - Bvb. gebouw fysiek verkennen of solliciteren voor een job of het gebruiken van een nmap tool om het target te scannen
- Anoniem
  - Informatie vergaren van bronnen die niet kunnen achterhalen ie je bent
- Organisatie
  - Bvb. email van het bedrijf

## Doel

- Welke informatie zoekt men?
  - Netwerk informatie
    - Domeinnamen (incl. subdomeinen)
    - Interne domeinnamen (bvb. .com en .net)
    - IP adressen (website, range, ...)
    - TCP/UDP services
    - VPN informatie
    - Intrusion Detection System
    - Telefoonnummers / VOIP
  - OS informatie
    - Gebruikers- & groepsnamen
    - Routing table
    - SNMP
    - Systeem architectuur (laatste updates?)
    - Remote access?
    - BYOD?

## Doel

- Welke informatie zoekt men?
  - Organisatie
    - Website (incl. broncode)
    - Organigram
    - Details van werknemers (incl. publieke informatie op social media); evt. voor wachtwoorden
    - Locaties van branches
    - Recent verhuisd?
    - Security policies (werd het personeel getraind?)
    - Nieuwsartikels
    - ...



## Tools voor verkenning

- Zoekmachines (niet enkel de eerste 3 pagina's)
- Websites (incl. subdomeinen)
- Applicaties / built-in commando's
  - Nslookup
  - Powershell commands
  - ...



## 6.5 Verkenning & enumeratie

# WHOIS

- Domein naam informatie (IP adres, eigenaar, ...)

### Whois Record for HoGent.be

#### — Domain Profile

Registrar	BELNET IANA ID: — URL: <a href="https://domains.belnet.be">https://domains.belnet.be</a> Whois Server: —
Registrar Status	NOT
Dates	9,082 days old Created on 1995-12-14
Name Servers	ENS1.HOGENT.BE (193.190.172.1) (has 12 domains) ENS2.HOGENT.BE (193.190.172.4) (has 12 domains) NS1.BELNET.BE (has 3,273 domains) NS2.BELNET.BE (has 3,273 domains) NS3.BELNET.BE (has 3,273 domains)
Tech Contact	—
IP Address	193.190.173.132 - 12 other sites hosted on this server
IP Location	 - Oost-vlaanderen - Gent - Hogeschool Gent
ASN	 AS2611 BELNET, BE (registered Aug 27, 1993)

WHOIS SEARCH



**HO  
GENT**

## 6.5 Verkenning & enumeratie

# WHOIS

### Website

Website Title	<b>H</b> Home - Hogeschool&#x20;Gent	➡
Response Code	200	
Terms	555 (Unique: 272, Linked: 180)	
Images	8 (Alt tags missing: 0)	
Links	100 (Internal: 95, Outbound: 5)	

### Whois Record (last updated on 2020-10-25)

```
Domain:      hogent.be
Status:      NOT AVAILABLE
Registered:  Thu Dec 14 1995

Registrant:
  Not shown, please visit www.dnsbelgium.be for webbased whois.

Registrar Technical Contacts:
  Organisation:  BELNET
  Language:     en
  Phone:        +32.27903333
  Fax:          +32.27903332

Registrar:
  Name:         BELNET
  Website:      https://domains.belnet.be

Nameservers:
  ns3.belnet.be
  ns1.belnet.be
  ens1.hogent.be (193.190.172.1)
  ens2.hogent.be (193.190.172.4)
```

**HO  
GENT**

## Emailadressen vinden

The screenshot shows the Hunter.io web interface. At the top, there's a navigation bar with the Hunter logo, 'Product', 'Pricing', and a 'Sign in' link. The main search area has a text input field containing 'hogent.be' and an orange button labeled 'Find email addresses'. Below the input, it states 'Most common pattern: (first).(last)@hogent.be' and '1,137 email addresses'. A list of email addresses is displayed, each with a green dot indicating a verified email and a 'source' count. The list includes: 'e...michiels@hogent.be' (1 source), 'd...ler.reynaert@hogent.be' (1 source), 'c...line.mertens@hogent.be' (1 source), 'l...in.vanparys@hogent.be' (3 sources), and 'w...t.bosma@hogent.be' (6 sources). At the bottom, it says '1,132 more results for "hogent.be"'.

Email Address	Source Count
e...michiels@hogent.be	1 source
d...ler.reynaert@hogent.be	1 source
c...line.mertens@hogent.be	1 source
l...in.vanparys@hogent.be	3 sources
w...t.bosma@hogent.be	6 sources

**HO  
GENT**

De structuur van emailadressen is ook bijzonder Interessant voor aanvallers. Ze kunnen deze informatie bvb. gebruiken voor het spoofen van een emailbericht. hunter is een tool die je kan gebruiken om emailadressen te zoeken.

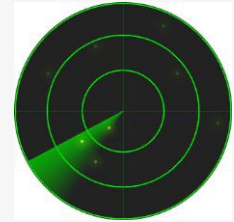
## Website analyseren

- Tools
  - Netcraft.com
  - builtwith.com
- Geeft informatie:
  - Frameworks,
  - DNS,
  - CDNs,
  - web stats,
  - hosting geschiedenis,
  - ...

**HO  
GENT**

In de verkenningfase is het ook zinvol om de website onder de motorkap te leren kennen.

## Scanningfase



- Actieve scanning (bvb. ping sweep)
- Passieve scanning (bvb. netwerk sniffer)
- Doel = informatie vergaren
  - OS versies van toestellen
  - Hardware toestellen (routers, firewalls, )
  - IP adres schema (bvb. printers, werknemer PC's, ...)
  - Kwetsbaarheden (bvb. versies – zero day attacks)
- Technieken:
  - Poort scanner
  - Vulnerability scanners
  - Trace route

**HO  
GENT**

Na de verkennings- en enumeratiefase heb je hopelijk genoeg informatie om de scanningsfase te beginnen. Zonder vorige fase zouden we nu niet weten wat te moeten scannen. Als je voor een opdrachtgever / klant werkt, kan het ook gebeuren dat hij/zij jou op voorhand heel wat informatie heeft en dat je in de verkennings- en enumeratiefase niet zo veel werk hebt. De verkennings- en enumeratiefase dient als voorbereiding op de scanningsfase.

Zo reageren Apple computers anders dan Windows computers.

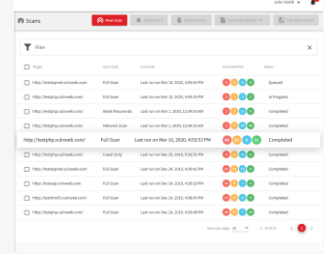
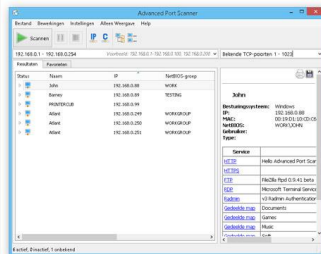
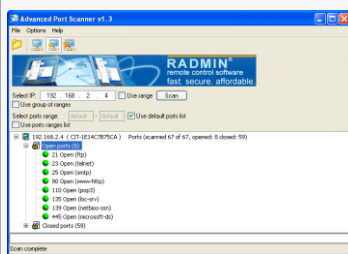
Netwerk sniffing: het netwerk afluisteren. Luisteren naar communicatie tussen toestellen die al op het netwerk zitten.

Deze tools zijn niet alleen voor hackers, maar zeker ook voor de netwerk experts belangrijk!

## Scanningfase



- Vaak voorkomende types scans:
  - Port Scanning – detecteren van open poorten en services die draaien op het target.
  - Network Scanning – IP addresses, Operating system details, Topology details, trusted routers information, etc
  - Vulnerability scanning – Gekende kwetsbaarheden of zwaktes scannen



Eén van de eerste zaken dat men wil doen is het uitvoeren van een port scan. Een port scan moet open poorten vinden in het target netwerk. Het is vaak het vertrekpunt om na te gaan welke services en applicaties er luisteren naar bepaalde poorten.

Het doel kan zijn het vinden van issues in het target netwerk opdat de klant/opdrachtgever zijn/haar netwerk kan verbeteren.

De open poorten en gebruikte services / applicaties kennen is vaak niet genoeg. Men wil ook de gekende kwetsbaarheden kunnen onderzoeken. Dit doet men dmv. een vulnerability scanner of kwetsbaarheden scanner. Het doel is het vinden van kwetsbaarheden voor de specifieke applicaties en services die op het netwerk aanwezig zijn.

## 6.5 Verkenning & enumeratie

# PING

- PING
  - IP adres
  - Pakketgrootte
  - Buffer

```
Select Command Prompt
Microsoft Windows [Version 10.0.19041.572]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\Joeri>ping www.hackthissite.org

Pinging www.hackthissite.org [137.74.187.101] with 32 bytes of data:
Reply from 137.74.187.101: bytes=32 time=23ms TTL=54
Reply from 137.74.187.101: bytes=32 time=23ms TTL=54
Reply from 137.74.187.101: bytes=32 time=31ms TTL=54
Reply from 137.74.187.101: bytes=32 time=27ms TTL=54

Ping statistics for 137.74.187.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 23ms, Maximum = 31ms, Average = 26ms

C:\Users\Joeri>ping www.hackthissite.org -f -l 2000

Pinging www.hackthissite.org [137.74.187.100] with 2000 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 137.74.187.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Joeri>
```

**HO  
GENT**

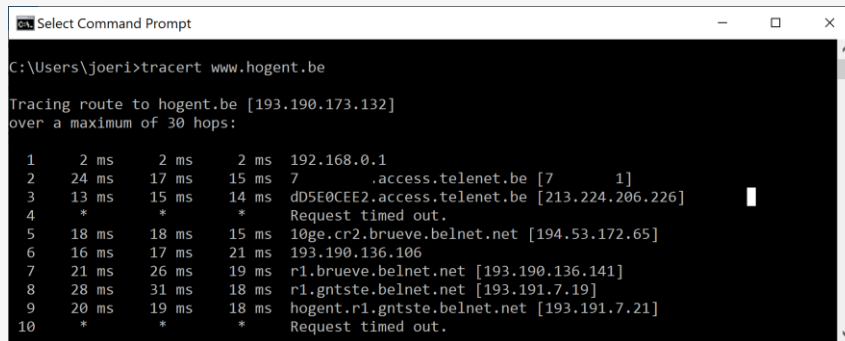
ICMP protocol. ICMP wordt soms geblokkeerd.

Pakketten hebben een maximumgrootte. Deze hangt af van de bestemming. PING kan gebruikt worden om deze threshold te achterhalen.



## Trace route

- Trace route (tracert op Windows)
  - Route die de request aflegt: van begin tot einde (target).



```
Select Command Prompt
C:\Users\joeri>tracert www.hogent.be

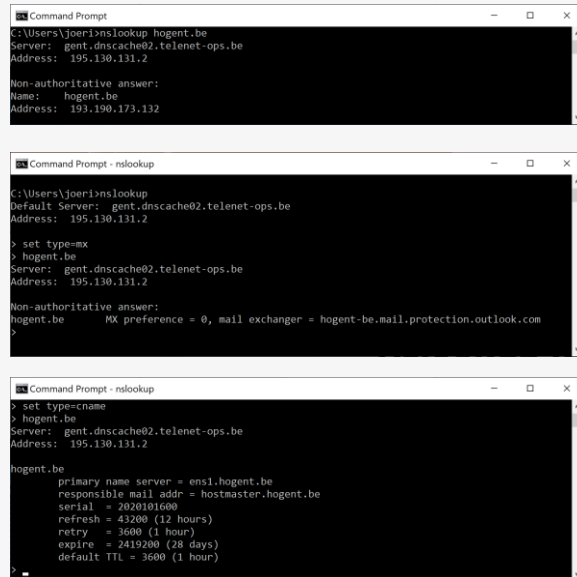
Tracing route to hogent.be [193.190.173.132]
over a maximum of 30 hops:
  0  0 ms  0 ms  0 ms  192.168.0.1
  1  2 ms  2 ms  2 ms  7.access.telenet.be [7.1]
  2  24 ms 17 ms 15 ms  dd5e0cee2.access.telenet.be [213.224.206.226]
  3  13 ms 15 ms 14 ms  Request timed out.
  4  *      *      *      Request timed out.
  5  18 ms 18 ms 15 ms  10ge.cr2.brueve.belnet.net [194.53.172.65]
  6  16 ms 17 ms 21 ms  193.190.136.106
  7  21 ms 26 ms 19 ms  r1.brueve.belnet.net [193.190.136.141]
  8  28 ms 31 ms 18 ms  r1.gntste.belnet.net [193.191.7.19]
  9  20 ms 19 ms 18 ms  hogent.r1.gntste.belnet.net [193.191.7.21]
 10  *      *      *      Request timed out.
```

**HO  
GENT**

Hops die men onderweg tegenkomt worden getoond. Soms worden ICMP requests geblokkeerd door een hop.

## Nslookup (DNS)

- Nslookup
  - Geassocieerde IP adressen
  - Verschillende gegevenstypes
    - MX (Mail eXchange records)
    - CNAME (canonical name record)
    - ...



```
Command Prompt
C:\Users\joeri>nslookup hogent.be
Server:      gent.dnscache02.telenet-ops.be
Address:     195.130.131.2

Non-authoritative answer:
Name:        hogent.be
Address:     193.190.173.132

Command Prompt - nslookup
C:\Users\joeri>nslookup
Default Server:  gent.dnscache02.telenet-ops.be
Address:         195.130.131.2

> set type=mx
> hogent.be
Server:      gent.dnscache02.telenet-ops.be
Address:     195.130.131.2

Non-authoritative answer:
hogent.be    MX preference = 0, mail exchanger = hogent-be.mail.protection.outlook.com
>

Command Prompt - nslookup
> set type=cname
> hogent.be
Server:      gent.dnscache02.telenet-ops.be
Address:     195.130.131.2

hogent.be
primary name server = ens1.hogent.be
responsible mail addr = hostmaster.hogent.be
serial = 2020101600
refresh = 43200 (12 hours)
retry = 3600 (1 hour)
expire = 2419200 (28 days)
default TTL = 3600 (1 hour)
>
```

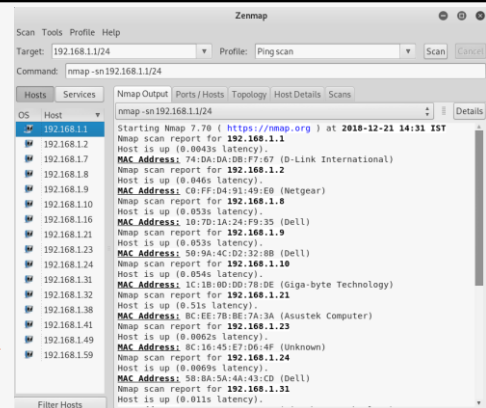
Via nslookup kunnen we achterhalen wat het IP adres van de server is, wat de domeinnaam is, wat de domeinnaam en IP-adres van de mailserver zijn, etc.

Terwijl je heel wat informatie publiek kan vinden, op een bepaald moment, moet je dieper graven. Dit betekent nog niet dat je volledig actief gaat scannen. Men gaat nu wel gaan communiceren met een IP adres. DNS (Domein Name System) Servers geven vaak heel wat informatie prijs. Dit gebeurt allemaal in het geniep. Heel wat informatie over domeinen en zelf IP-adres blocks wordt opgeslagen in de DNS Servers. DNS wordt o.a. gebruikt om een domeinnaam (bvb. Google.com) om te zetten naar een IP adres.

## 6.5 Verkenning & enumeratie

# nmap

- Bestaat al sinds 1997
- Voluit: network mapper
- Is een populaire **netwerkscanner**
- Wordt ook gebruikt als **port scanner**
- Wordt gebruikt om het **netwerk in kaart** te brengen en is enorm populair.
- Heeft ook een grafische user interface: Zenmap



**HO  
GENT**

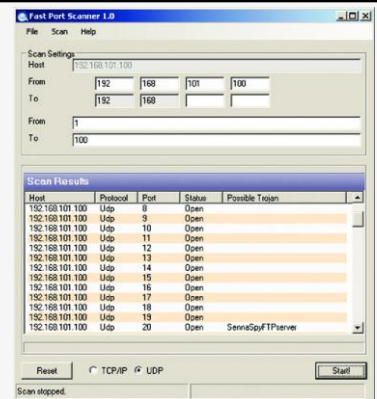
Nmap werd initieel opgezet als een generieke port scanner voor het Linux OS maar heeft in de loop der jaren veel bijkomende functionaliteit en ondersteuning voor andere besturingssystemen gekregen. Nmap is een standaard om het netwerk in kaart te brengen. De tool omvat héél veel verschillende features (bvb. UDP scanning, TCP scanning, SYN Scan, ...). Deze features vallen buiten de scope van deze cursus en komen aan bod in volgende jaren binnen onze opleiding. Er bestaat ook een GUI: Zenmap.

Een aantal features (buiten de scope van de cursus):

- Host-discovery: het ontdekken van op een netwerk aanwezige hosts. Dit kan onder meer gebeuren door zogenoemde ping- of arpscan
- Port-scanning: het ontdekken welke poorten op één of meerdere doelcomputers luisteren.
- Versiedetectie: het door ondervraging van het doelsysteem ontdekken welke services inclusief de versie daarvan het systeem aanbiedt
- OS (besturingssysteem)-detectie: het bepalen welk besturingssysteem de doelcomputer gebruikt.
- Nmap Scripting Engine (NSE)

## Poort scanner

- Een poort scanner kan gebruikt worden om het netwerk **onder de loep** te nemen en (binnen een bereik) te scannen naar open poorten.
- Een poort die open staat kan gezien worden als **toegangspoort**.



Poort	Service
20 en 21	FTP
22	SSH
23	telnet
25	SMTP

**HO  
GENT**

Wanneer een applicatie of service over het netwerk communiceert doet het dit via een poort. Een poort wordt geassocieerd met en gereserveerd voor die bepaalde service of applicatie. Communicatie dat langs die poort passeert, wordt dan doorgestuurd naar de applicatie of service. Wanneer een poort open staat, kan deze als een toegangspoort gebruikt om toegang te krijgen tot het netwerk en tot de applicatie of service.

Wat is nu een port scanner? Een port scanner moet open poorten vinden in het target netwerk. Het is vaak het vertrekpunt om na te gaan welke services en applicaties er luisteren naar bepaalde poorten. Nmap kan gebruikt worden, maar er zijn ook heel alternatieve tools beschikbaar.

De lijst met poorten en services is verre van compleet. Dit is louter illustratief en dien je niet vanbuiten te kennen. In andere opleidingsonderdelen komen deze poorten nog ter sprake.

<https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-en-4/ch-ports.html>

```
# nmap -sV -T4 -F insecure.org
```

```
Starting Nmap ( http://nmap.org )
Nmap scan report for insecure.org (74.207.254.18)
Host is up (0.016s latency).
rDNS record for 74.207.254.18: web.insecure.org
Not shown: 95 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.3 (protocol 2.0)
25/tcp    open  smtp     Postfix smtpd
80/tcp    open  http     Apache httpd 2.2.3 ((CentOS))
113/tcp   closed auth
443/tcp   open  ssl/http Apache httpd 2.2.3 ((CentOS))
Service Info: Host: web.insecure.org

Nmap done: 1 IP address (1 host up) scanned in 14.82 seconds
```

## Enumeratie

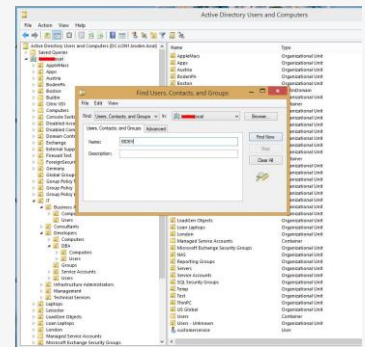
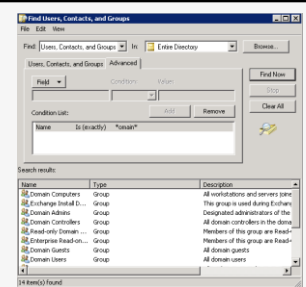
- Komt na het scannen
- Houdt er wel mee verband
- Enumeratie:
  - Welke services draaien er?
  - En ook: op welke versies draaien deze services?
  - Je vergaart meer informatie dan enkel IP-adressen en poorten: gebruikersnamen, netwerk shares, software en versie van de services, ...
  - Kan via `nmap` commando
  - Deze informatie kan men dan opnieuw gaan gebruiken in een latere fase.

**HO  
GENT**

Als er bvb. services zijn die authenticatie en autorisatie vereisen, kan je afleiden dat er met gebruikers wordt gewerkt.

# Enumeratie

- Informatie in deze stap:
  - Network resources en shares
  - Gebruikersnamen en groepen (denk aan Active Directory)
  - Routing tables (zie olod Computer Systems volgend semester)
  - Auditing en service settings
  - Namen van de toestellen
  - Applicaties
  - SNMP en DNS details



## Enumeratie

- Netwerk mappen kan bvb. via deze tools:
  - LanState pro:  
<https://www.dnsstuff.com/network-mapping-software>
  - PRTG Network Monitor
- Je moet wel eerst toegang hebben tot het netwerk.

**HO  
GENT**

**HO  
GENT**