Jaar 1

# Labo 2

Wanneer je iemand wilt hacken:

* Google
* Social skills
* Surfen naar de website()
* Dns lookups:
  + host + webname voor ip
  + host + webname + 8.8.8.8 voor extern ip
  + host -t mx + wabname voor mailrecords (met smtp kan iedere hacker fake mails sturen)
  + host -t txt + webnaam om uit te zoeken wie allemaal recht heeft om mail te sturen van het adres (via het DPF? protocol).
    - Dan weet je de infrastructuur
* Portscans gaan doen (m bv nvap):
  + nmap <opties> <doelwit>  
     -sP(simplePings = veel lawaai) ww.ap.be (niet gebruiken!)  
     -O(Operating system) 192.168.16.11  
     10.0.0.0/8 (range – te groot!)
  + Met gegeven ip range eerst ping scan om te zien wie er reageerd (als ncmp geblokkerd is kan je intense scan, no ping doen (maar gaat poorten in de range dan scannen, enkel doen als je weet dat het ip er is)
  + Dan een quickscan op de ip’s die reageren
  + Dan mogelijk een comprehensive scan (duurt zeer lang) om meer te leren over het systeem.

**Honeypot** = hacker lure

# The Dark Web

>Gebruik Tails (Vm gemaakt voor anonimiteit)!

## Stream cifers

=>Elke bit die door een incryptie/decryptie methode komt worden allemaal apart bewerkt.

## Block cifers

Het encryptie/decryprtie werkt op blocken van bits.

Jaar 2

# Les 1

## Tijdlijn

Security was rustige wereld. Virussen waren enkel “annoying”.

**2010** – **StuxNet**, Sec wereld in paniek tot 2015 – Veel uit geleerd zoals:

Airgap systemen bestaan niet. Elke systeem/netwerk is altijd op een manier te penetreren, zoals door social engeniering -> Usb stick op de grond laten liggen en mensen hun interesse aanspreken, voordoen als reparatie bedrijf, …

**2013** – Veil is lifted – **WikiLeaks** -> VS was actief mensen hun data aan het lezen en gebruiken.

Top10 snowden leaks:



* Gezonde dosis scepticisme

**2014** – **icloud leaked**, duizende private fotos van oa celebraties vrijgegewen aan het publiek. Gebeurt door mensen die hun security questions eerlijk hadden ingevuld en een **EPPB tool** van in de tijd.

Biometric security, still no liftoff. Beter is een combinatie van samenkomende secrity ellementen

In de security wereld is er een balans tussen security en mobiliteit van data.

2014 – Sony Pictures hacked by north korea. Twee journalisten waren naar Noord korea gegaan om daar de situatie de filmen en het staatshoofd te vermoorden(?). Het staatshoofd heeft dan een aanval gepleegd op sony pictures om die film te kunnen vernietigen.  
Grote vraag: Hoe kan je daar op reageren, welke counter acties kan je doen. Want cyber aanvallen kunnen onder vele situaties gebeuren, het kan uitgevoerd zijn door een land, door een groep, of een enkele terrorist.

2015 – Door rusland gesponsorde hackers hadden een powerplant gehacked en plat gelegd. (phantom mouse techniek)

2015 – Madison Ashley data breach – was een tinder maar voor mensen al met relaties. 25gb of company data (email, user dataà stolen. Resulted in suicides, divorses and public shaming.

GDPR – Zo goed mogelijk u best doen maar elk system is hackbaar.

2015 – Shellshock and Heartbleed – megaexploits – Heartbleed: major vulnerability in OpenSSL library. Shellshock: family of bugs in Linux Bash shell resulting in ability to execute any command whatsoever.

Verkaaltje: kabel leide naar afgezeilde kamer waar nog een oude server draaide en diende als exploit hub voor outside attackers. De security problemen van nu liggen altijd aan relieken van het verleden.

Social Engeniering: pentesting, de methode van te gaan kijken hoe gemakkelijk je in systemen binnengeraakt.

2016 – IOT begint – niet lang voordat deze begonnen gebruikt te worden om exploits te maken.  
Rise van de botnet attack – een aanval die duizende iot apparaten gebruikt die hun messaging system gebruiken om 1 doelwit te flooden met pings en zo plat te leggen.

Shodan – Search engine voor iot apparaten te vinden verbonden met het internet.

Mirai botnet –

2016 – Shadow brokers – Cyber war – NASA ANT Catalog publiek gezet

2017 – Going for the big bucks – Wannacry – Randsomware gebaseerd op te code van de NSA die de Shadowbrokers hadden publiek gezet

Shadow brokers ondekt als niet een simpele hacker groep maar als spionen van china

2016 – Americaanse verkiezingen – Putin – Nieuwe manier van mensen hun opinies te veranderen – subtiele propaganda, fake news, social influencing, facebook, twitter, memes, 9gag  
Alternatieve app voor whatsapp - Telegram

Israel launched airstrike in response to Hamas cyberattack – respons changing

2019 - EU elections also influenced trough misinformation on social media, ook vooral door de reacties van mensen in comments. Misinformations en bad behaviour in comment sections still a large social issue and should be tended too sooner than later.  
Extra Info on SLIDES

2018 – Haven van Antwerpen – cyberspecialist had drugsmaffia geholpen containers uit te haven te stelen. Had hacktools zoals raspberryPI etc in een stekkerdoos verstopt en gesmokkeld in de haven.

Tip voor penttesters: bedrijven zetten altijd heel duidelijk op papier de scope van de pentest en blijf daar altijd binnen, anders zijn er vaak grote consecuencies. Als je fysiek in het gebouw zou moeten krijg je ook altijd een get out of jail free card.

2020 – Attacking the big players – 5.2 miljoen hotel gests … meer op de slides

Maze Randsomware – slachtoffers: Cognizant, Canon allegedly, Xerox, and industries like healthcare -

Schooljaar tip: Hack niemand waar je geen toestemming voor hebt!

## Future

* Deepfakes & Sextortion Cases Will Rise
* Covid-phising – angst voor pandemie gebruiken voor phising
* Deepfake voice technology
* AI powered attacks (keeps being delayed) – possibly happening under our noses
* Social Media disinformation (#fakenews)
* Election security

## BE AN ETHICAL HACKER

In deze opleiding is het de bedoeling om een white hat hacker te zijn. Dit is hacking waar je toestemming voor hebt op toestellen waar de eigenaar goedkeuring heeft gegeven. Dit gaat in tegenstelling tot grey hat hacking (hacking met goede doelen maar zonder toestemming) en black hat hacking (hacking met slechte intesies of voor eigenbelang).

# Tips voor de opleiding

White hat hacking in vrije tijd: intigrity.com bug bounty platform

Tools: metasploit, kali OS