Informationssikkerhed

...

Din vej ned i kaninhullet

Agenda

- Hvem er vi som personer
- Hvad er Etik
- Hvad er Loyalitet (og tavshedspligt)
- Hvordan kommer vi igang
- Hvad er læring?
- Hvad kræver det
- Labs for hacking, reversing, OSINT og andet godt
- Hvor får jeg hjælp

Din vej til Info-Sec

Et gammelt mundheld

Du bliver ansat på dine færdigheder og fyret på din personlighed.

Din vej til Info-Sec

Vi skal starte allerede i dag

- Hvad er Integritet?
- Hvad er Etik?
- Hvad er Loyalitet (og tavshedspligt)?
- Hvad er Stabilitet
- Hvad er Troværdighed?

Du som person er forskellen

Du er den folk kommer til, når du arbejder med sikkerhed. Din person er forskellen og kulturen!

Agenda

Hvad er Integritet

Din vej til Info-Sec

Hvad er Integritet?

At gøre det rigtige, når andre ikke ser det!

Agenda

Hvad er Etik

Din vej til Info-Sec

Hvad er Etik?

- Etik drejer sig om, hvad vi bør gøre som enkeltindivider
- Etik er altså styrende for en del af vores handlinger.
- Vi deler ikke belastende viden om andre, hvis vi kender til den.
- Vi hjælper andre, når vi kan se de har brug for vores viden om Info-sec

Agenda

Hvad er Loyalitet

og tavshedspligt

Din vej til Info-Sec

Hvad er Loyalitet (og tavshedspligt)?

- Du er en god kollega (Tro mod virksomheden)
- Du er medarbejderen virksomheden kan betro sig til
- Du render ikke med sladder
- Du holder kortene tæt på kroppen om hvad virksomheden er / har været udsat for (med mindre andet aftalt, som et led i awareness)
- Du kan overholde tavshedspligten (ofte beskrevet af virksomheden og de krav der er)

Din vej til Info-Sec

Tavshedspligt og sikkerhedsgodkendelse

- Kan du sikkerhedsgodkendes ? = ren straffeattest
- Kan du bevist at du kan holde på hemmeligheder = ikke eksponere hvad du har oplevet
- Kan du håndtere klassificeret materiale og potentielt se nationens sikkerhed?

Link: https://da.wikipedia.org/wiki/Sikkerhedsgodkendelse

Din vej til Info-Sec

Hvad er Stabilitet

- Du er mødestabil
- Du holder folk informeret (Hvor du er til at fange og hvilke kanaler, opdateret kalenderen)
- Folk kan altid søge hjælp hos dig (Eller viden og guidance. HUSK, du skal ikke påtage dig alle opgaver)

Agenda

Hvad er Troværdighed

Din vej til Info-Sec

Hvad er Troværdighed

- Det du siger, er det du gør (Laver man en aftale, så holdes denne, ellers bliver der informeret i god tid)
- Det du siger er det du ved (ved du det ikke , så siger du det!)
- Det du siger er det din erfaring siger (baseret på det du har prøvet/ testet)
- Du holder andre informeret (Hvis der opstår uforudsete barriere, så informere du folk, så ikke de skal gætte. Den værste form er, når folk ikke holdes informeret)

Agenda

Hvad er Info-sec

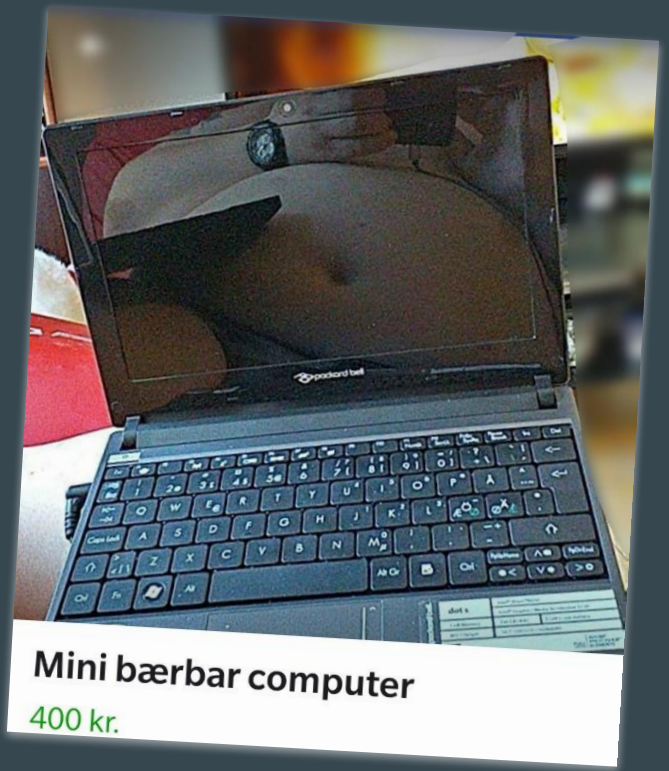
(Information security)

Din vej til Info-Sec

Spring cleaning på internettet.

Har du dumme billeder på internettet?
har du skrevet noget som er “uheldigt” på internettet?
har du indhold på internettet som er kontroversielt?
Har du været en “skid” på internettet overfor andre?

Ovenstående bliver set og læst af en arbejdsgiver. De danner deres meninger om dig baseret på dette, og det er med til at dømme dig! ... retfærdigt eller uretfærdigt!



Kig dig over skulderen

Det er nemlig hvad andre gør inden din jobsamtale.

Kig dig selv over skulderen

30 min

Hvad kan du finde om dig selv på nettet ?
evet udveksle information med sidemanden
(Husk etikken… finder i noget, så oplys og hjælp!)

- Dit navn
- Telefonnummer
- e-mail
- måske et billede ?

Formål

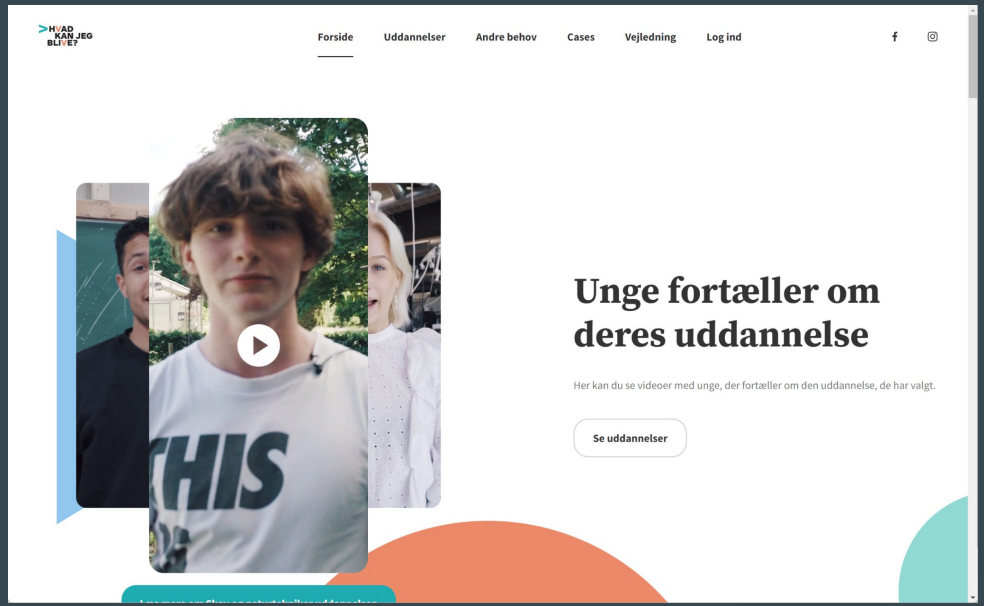
Husk, at når i skal søge job i informationssikkerheds branchen. Så bliver i med stor sandsynlighed udsat for det samme.

Agenda

Hvordan kommer jeg i gang?

Hvor starter man?

Kig hvad det kræver at komme ordentlig fra start



Kilde: https://hvadkanjegblive.dk/

Din vej til Info-Sec

Et par ord om læring

Alt ny viden skal efterprøves! om det er Dansk, Matematik, Biologi eller IT/Sikkerhed
Begrundet gyldig viden = Det du ved og har observeret / tested / efterprøvet
Læring kommer nemmere med interesse. Det der interessere dig, optager også mere af din tid!

Din vej til Info-Sec

FEJL

Fejl
Er
Justeret
Læring

Din vej til Info-Sec

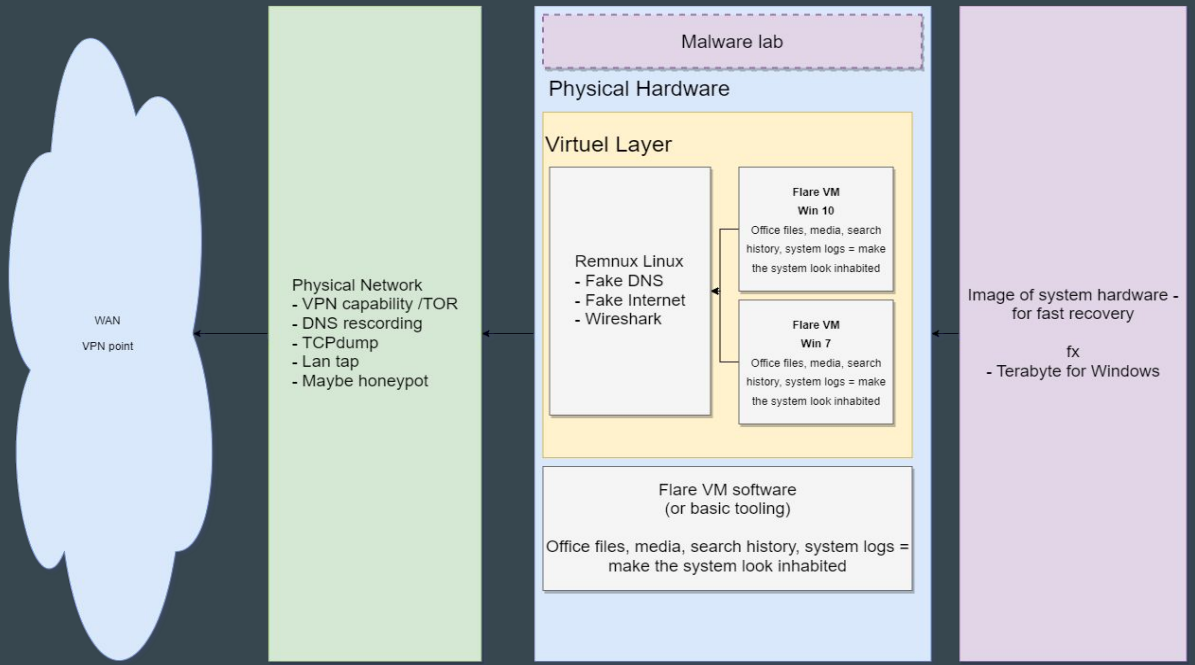
Skab dit eget rum for dette!

Alt ny viden skal efterprøves! om det er Dansk, Matematik, Biologi eller IT/Sikkerhed
Begrundet gyldig viden = Det du ved og har observeret / tested / efterprøvet
Læring kommer nemmere med interesse. Det der interessere dig, optager også mere af din tid!

Agenda

Hvad er et lab?

Hvad med fysisk labs ?



Kom ud og prøv tingene af

I kan starte i dag online

Fra bunden

- Tryhackme.com
- Hackthebox.com

De lidt øvede

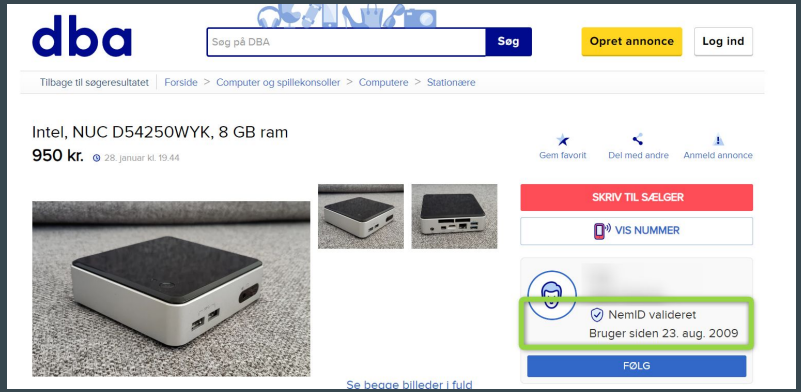
- blueteamlabs.online

Kasm hvad for et firben?

Hvad kan jeg bruge ?

Nyt udstyr

Køb det også brugt



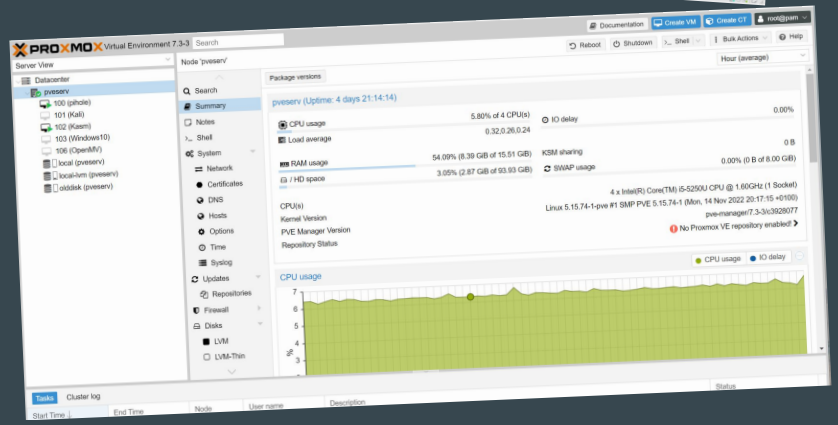
Hvad med fysisk labs ?

Fysisk hardware
(udstyr du har i skuffen)

Virtuelle maskiner

Proxmox hypervisor

- kali linux
- linux
- windows
- Kasm (streaming apps til browser)



ADVARSEL Hvis i vil rode med virus

Husk hvad du arbejder med

Stand alone - maskine og en mulighed for hurtig re-etablering (image backup af opsætning for hurtigt restore)

Opdeling - Anvend opdeling af eks browsere, netværk og hardware. Så man minimere fejl og spredning i tilfælde af fejl.

Container - kan man begrænse spredning som eks ved VM'er

Backup - gem altid en kopi af jeres tools offline / cold storage

Brug sikkert netværk når du selv roder med det

Online - Benyt en VPN ud af netværket

Offline - Lukket internt netværk

Hvad er hacking?

Så længe du ikke ændrer noget

Straffelovrådet lægger i vurderingen vægt på, at der er adgang til f.eks. en server fra det åbne internet, og at alle potentielt kan få adgang med en almindelig webbrowser.

Den form for adgang bør 'som et klart udgangspunkt ikke anses for uberettiget adgang til en andens oplysninger', skriver rådet, der består af otte advokater, dommere og offentlige chefer.

Hacking

Hacking handler i bund og grund om evnen til at kunne manipulere med noget digitalt. Det kan for eksempel være at overtage andres profiler og private billeder.

Når man talte om hackere for få siden, betød det blot en person, der var dygtig til at arbejde med software og computere. Men i dag bliver begrebet også brugt i en negativ forstand.

Hacking bruges eksempelvis brugt til at betegne den type IT-kriminelle, der via internettet bryder ind i andres computere. De hacker sig ind i andres computere og kan dermed stjæle personlige oplysninger, få adgang til en netbank, passwords og så videre.

Hacking kan foregå på flere forskellige måder. Hackeren kan for eksempel stjæle ens kodeord eller forsøge at få en til at åbne en e-mail, som giver hackeren adgang til computeren. Der er også tale om hacking, hvis man skaffer sig adgang til en anden brugers profil på sociale medier, eksempelvis Facebook.

Kilde: https://danskelove.dk/straffeloven
Kilde: https://redbarnet.dk/foraeldre/leksikon/hvad-er-hacking/
Kilde: https://da.wikipedia.org/wiki/Hacker
Kilde: https://vidensbasen.anklagemyndigheden.dk/

Offentligt påtale vs privat påtale

Almindeligvis betegnes de undersøgelser, der foretages i en sag, for at finde ud af, om der er grundlag for at pålægge nogen strafansvar eller anden strafferetlig retsfølge, som efterforskning50. Om efterforskningen generelt bestemmer

RPL § 108, stk.1, der almindeligvis kaldes politiets generalfuldmagt, at politiet har følgende opgaver:
at opretholde sikkerhed, fred og orden, at påse overholdelsen af love og vedtægter samt at foretage det fornødne til forhindring af forbrydelser og til efterforskning og forfølgning af sådanne. *

Privat påtalt
En mindre del, først og fremmest injuriedelen, er underlagt *privat påtale*, hvilket vil sige, at forurettede selv skal føre en sag.

Ophavsret som f.eks download ulovlig MP3 er en privat sag

Offentligt påtalt

Størstedelen af straffeloven er underlagt *offentlig påtale*, dvs. at Anklagemyndigheden rejser sager uden at forurettede tager initiativ til det.

Organiseret udbredelse af MP3 er offentlig påtale. da der er tale om særlige skærpende omstændigheder.

Kilde: https://danskelove.dk/straffeloven og https://da.wikipedia.org/wiki/Straffeloven
*Lånt herfra: https://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Prisopgaver/Bedste_opg_2003.pdf

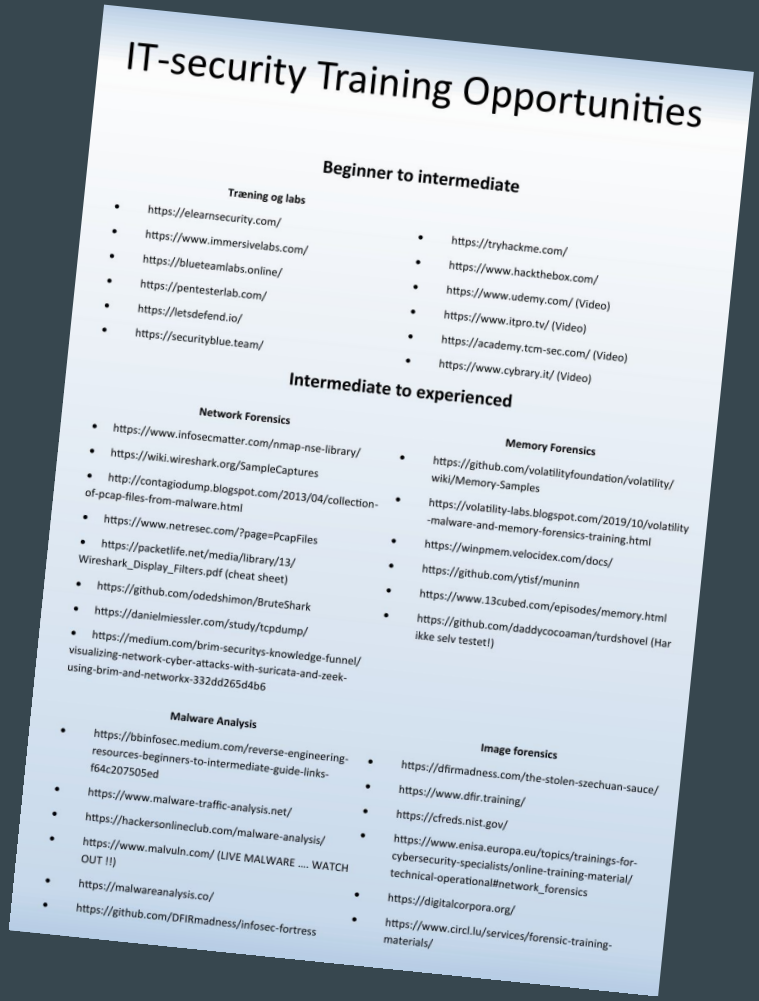
Agenda

Kom godt afsted

Hvor møder jeg andre ?

Kilde: https://codingpirates.dk/ (6 - 17 år)
Kilde: https://www.cyberskills.dk/community (15 år og op efter)

Links til træning



IT-security Training Opportunities

Beginner to intermediate

Træning og labs

- https://elearnsecurity.com/
- https://www.immersivelabs.com/
- https://blueteamlabs.online/
- https://pentesterlab.com/
- https://letsdefend.io/
- https://securityblue.team/
- https://tryhackme.com/
- https://www.hackthebox.com/
- https://www.udemy.com/ (Video)
- https://www.itpro.tv/ (Video)
- https://academy.tcm-sec.com/ (Video)
- https://www.cybrary.it/ (Video)

Intermediate to experienced

Network Forensics

- https://www.infosecmatter.com/nmap-nse-library/
- https://wiki.wireshark.org/SampleCaptures
- http://contagiodump.blogspot.com/2013/04/collection-of-pcap-files-from-malware.html
- https://www.netresec.com/?page=PcapFiles
- https://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf (cheat sheet)
- https://github.com/odedshimon/BruteShark
- https://danielmiessler.com/study/tcpdump/
- https://medium.com/brim-securitys-knowledge-funnel/visualizing-network-cyber-attacks-with-suricata-and-zeek-using-brim-and-networkx-332dd265d4b6

Memory Forensics

- https://github.com/volatilityfoundation/volatility/wiki/Memory-Samples
- https://volatility-labs.blogspot.com/2019/10/volatility-malware-and-memory-forensics-training.html
- https://winpmem.velocidex.com/docs/
- https://github.com/ytisf/muninn
- https://www.13cubed.com/episodes/memory.html
- https://github.com/daddycocoaman/turdshovel (Har ikke selv testet!)

Malware Analysis

- https://bbinfosec.medium.com/reverse-engineering-resources-beginners-to-intermediate-guide-links-f64c207505ed
- https://www.malware-traffic-analysis.net/
- https://hackersonlineclub.com/malware-analysis/
- https://www.malvuln.com/ (LIVE MALWARE .... WATCH OUT !!)
- https://malwareanalysis.co/
- https://github.com/DFIRmadness/infosec-fortress

Image forensics

- https://dfirmadness.com/the-stolen-szechuan-sauce/
- https://www.dfir.training/
- https://cfreds.nist.gov/
- https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational#network_forensics
- https://digitalcorpora.org/
- https://www.circl.lu/services/forensic-training-materials/

Hvad skal jeg sigte efter ?

Det som er DU syntes er sjovt og motivere dig!

Hold øje med hvad “industrien” har brug for

Vær nysgerrig og prøv tingene af

Hvis ikke du fejler lærer du ikke

Hvad kræves ?

Hvad kræves?

Du skal have lysten!

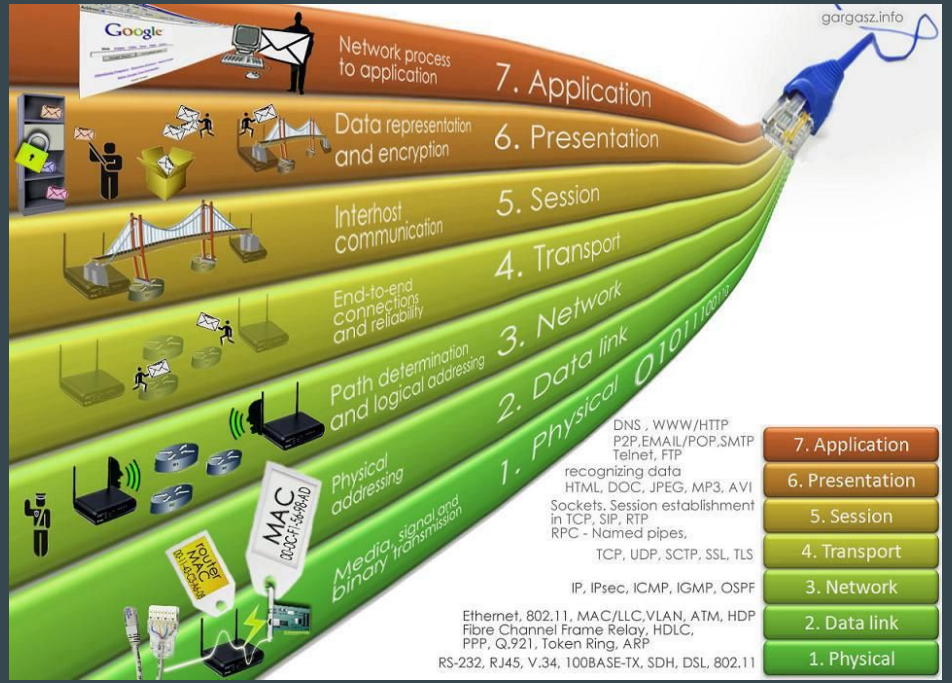
Du skal have basis viden

Du skal kunne lide at samarbejde - Alt IT-sikkerhedsarbejde er teamwork

Kunne kommunikere det du laver

Bare være dig selv og kom som du er!

Virksomheden skal nok klæde dig på



Billede lånt af : https://networkel.com/osi-model-7-layer-network-communication/

Fremtidig job ?

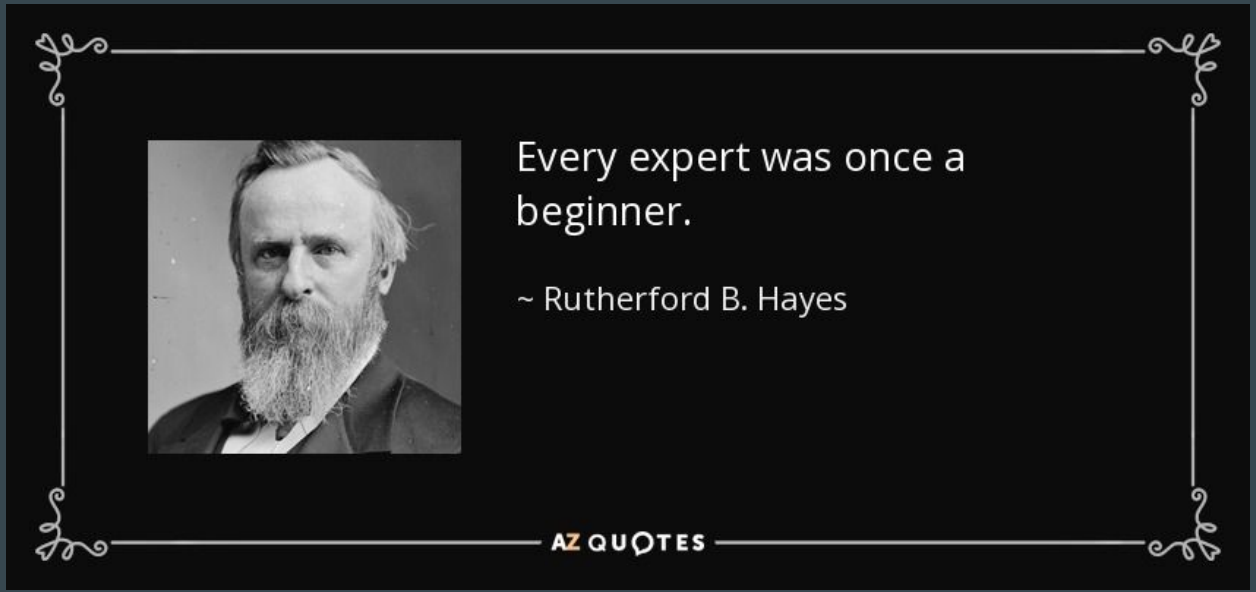
Et par ord om jobbet, når du kommer på jobmarkedet

- Spørg til hvordan virksomheden støtter din læring - hvad bliver sat af for det?
- Hvordan bliver du holdt ved lige ?
- Hvad er balancen mellem fritid og arbejde - har du vagter og bliver du en del af driften (kræver ofte at du bliver brugt i din fritid)
- Hvad bliver dit ansvarsområde og får du en mentor?
- **Med andre ord fokusér på din læring mere end løn!**

Lønnen kommer med alderen og min anbefaling er, at det må aldrig blive en motivationsfaktor

Du skal være glad for jobbet, så kommer resten af sig selv!

Hvad kræves ?



Amerikansk præsident 1877 - 1881
https://da.wikipedia.org/wiki/Rutherford_B._Hayes