Tilkoblingsguide til virtuelle labmaskiner for obliger

IN2120 - høst 2023

Hvis du bare vil rett til enkleste metode for å koble deg til, og har satt opp 2FA autentiseringsappen for UiO-innlogging, trykk her.

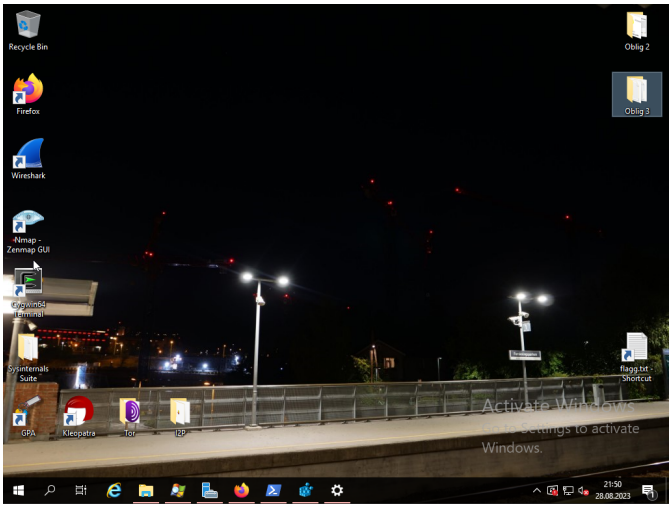
Hvorfor labmaskin?

For å gjøre obligene i dette emnet har du fått din egen virtulle labmaskin. Det er to grunner til dette:

1. Labmaskinen er en **"sandbox" (lekekasse)**, noe som betyr at her kan du herje fritt uten å bekymre deg. For eksempel kan du installere akkurat hva du vil på den, programmere på den, eller teste ut skadevare (virus og sånne ting). Faktisk blir en av oppgavene i kurset å kjøre skadevare og analysere hva skadevaren gjør, og det skal du selvfølgelig slippe å gjøre på din personlige maskin. Du kan fritt kjøre "ekte" virus og sånne ting på labmaskinen din - hvis du vil se nærmere på dem også - men det er fint hvis vi slipper å gjenopprette så mange labmaskiner til utgangspunktet, så prøv å ikke skade den virtuelle maskinen på en måte som gjør at den ikke virker.
2. Labmaskinen har de aller fleste av programmene som trengs til obligoppgavene ferdiginstallert, pluss noen filer og innstillinger vi skal se nærmere på. Tanken er at du skal slippe å installere ting på din personlige maskin.

Selv om du kan "gjøre hva du vil" på labmaskinen ber vi om at du ikke bruker den til å for eksempel sende ut spam eller kjøre skadevare som angriper andre maskiner. Det er rett og slett fordi UiO er redd for at våre IP-adresser kan bli "svartelistet", slik at for eksempel mail fra UiO ikke kommer frem.

Som operativsystem på labmaskinen din har vi valgt **Windows**. Hensikten med å velge Windows er at alle skal kjenne seg igjen, fordi dette er rett og slett en vanlig Windows-maskin.
Det du skal se på i obligene er for det meste ting som foregår på din egen PC hele tiden, men som du kanskje ikke har visst om. For den saks skyld kunne vi også brukt Mac, men det er enklere å få tak i verktøy for Windows.



For å koble seg til har vi valgt **RDP** *(Windows sin Remote Desktop -Protokoll)*. Igjen: Ikke en generell anbefaling, men bare fordi dette er det enkleste å komme igang med i Windows og fordi det finnes mange ulike programmer som støtter det. Det har vært mange alvorlige sårbarheter i RDP opp gjennom årene, både som lot angripere spionere[1][2] og som lot dem ta kontroll på sårbare maskiner[1]. På den annen side: Det har vært minst like alvorlige sårbarheter i Zoom[1][2][3]. Sårbarheter i både Zoom og RDP fikses kontinuerlig, så du behøver ikke være spesielt nervøs for å bruke RDP.

2FA (tofaktor-autentisering) for å nå nettet som har virtuelle maskiner

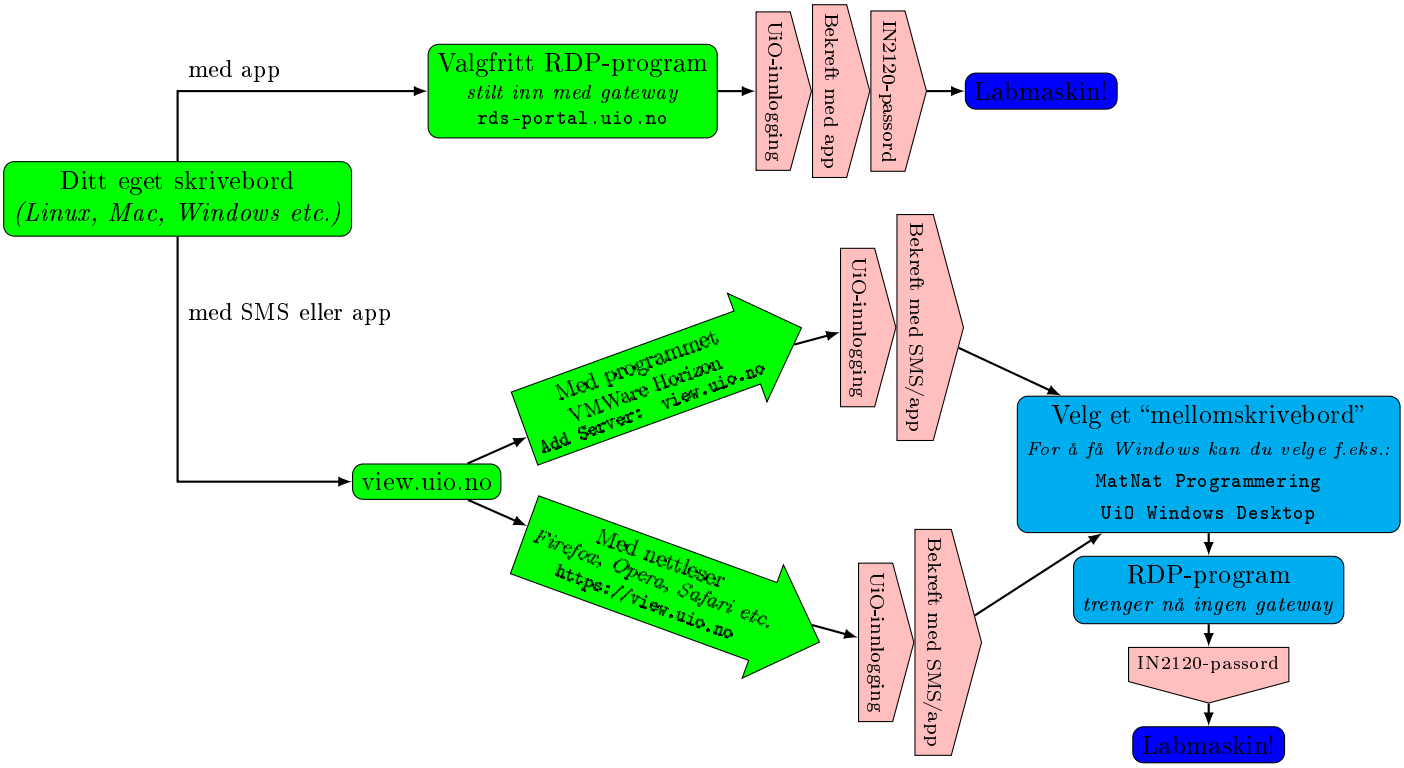
Vi skulle veldig gjerne gitt dere muligheten til å koble til direkte, med bare lab-passordet dere får i kurset og intet annet. Dessverre har vi rett og slett ikke nok IPv4-adresser til at alle kan få sin egen IP, og IPv6 er ikke engang støttet på Eduroam eller UiOs egne terminaler enda, så vi må gå omveien via en "mer tilgjengelig" UiO-maskin for tilgang til området der de virtuelle labmaskinene er installert.

Derfor blir det to påloggінger: Først til en "offentlig tilgjengelig" UiO-maskin med UiO-brukernavnet og UiO-passordet ditt, og derfra videre til selve labmaskinen som sitter på UiO sitt nett.

So far so good. Men:

UiO har innført 2FA (tofaktor-autentisering fra Microsoft) slik at man trenger mobiltelefon-app eller SMS for å logge seg inn med UiO-brukernavnet og UiO-passordet *(generelt, ikke bare i dette kurset)*.

Derfor må man sette opp 2FA etter sentral UiO-modell først, og vi gå via `view.uio.no` for å få 2FA til å fungere til vårt formål.[1]



[1] Dette likner faktisk på det som heter "lateral movement" i hacker-sjargong:
Å bruke tilgang ett sted til å bevege seg sideveis et sted man ikke kom inn direkte.

Hvilke måter du kan logge inn på, kommer altså an på hvilken variant av 2FA du bruker:

- De aller fleste har **Microsoft sin "app" for 2FA (Microsoft Authenticator)** på mobilen. Detaljer om installasjon og oppsett av dette finner du på UiO sine nettsider. For dere vil vi anbefale å bruke et RDP-program direkte, stilt inn til å gå via gateway, fordi dette er det desidert raskeste og enkleste. Instruksjoner for dette finner du her.
- Dersom du bruker **SMS-bekreftelse som 2FA**, fungerer ikke Microsoft sin løsning med gateway (dette er en svakhet i deres system), slik at du må gå via et "mellomskrivebord" på view.uio.no isteden. Fra mellomskrivebordet kan du da koble deg til med RDP-program på samme måte som i forrige punkt, men UTEN at du behøver å fylle inn noen gateway (for da er du allerede på UiO sitt nett).
  - Vi anbefaler at du bruker VMWare Horizon-programmet hvis du skal koble deg til `view.uio.no`. Dette er ferdiginstallert på termstuene til UiO, og kan ellers lastes ned gratis for både Windows, Linux og Mac ved å klikke på denne lenken.
  - Hvis du ikke kan/vil installere VMWare Horizon, kan du åpne `view.uio.no` ved å skrive inn adressen i nettleseren din isteden, selv om dette går litt tregere.

RDP-program (klienter)

Det finnes mange ulike klient-programmer[2] for å bruke RDP og vi vil ikke tvinge deg til å installere noe bestemt program på din egen maskin. Prøv deg gjerne frem hvis du vil!

Men de fleste vil bare ha noe som funker, så her kommer en liten guide for å gjøre dette enklest mulig, på Linux, Windows og Mac.

Oppsett i andre programmer, dersom du vil bruke det, er tilsvarende.

Husk: **Du må ha 2FA-appen klar for å koble deg til direkte via gateway, ellers må du bruke 2FA-SMS inn på view.uio.no og finne en maskin der så du kan droppe gateway.**

Linux

Dette er det desidert enkleste hvis du skal koble deg til direkte via gateway (forutsetter altså 2FA-appen):

De fleste Linux-maskiner, inkludert Linux-terminalene på UiO, har **FreeRDP** installert allerede. Da behøver du bare å åpne en kommandolinje og skrive inn følgende linje:

```
xfreerdp /cert:ignore /size:1280x1024 /kbd:Norwegian /gu:<ditt_uio-brukernavn> /g:rds-portal.uio.no
/gt:rpc /u:Admin /v:<ditt_labmaskinnummer>.in2120.uiocloud.no /p:'<ditt_labmaskinpassord>' /f
```

FreeRDP spør da om "GatewayPassord", som er UiO-passordet ditt, så må du godta innlogging i "2FA-appen", og så er du inne.

Kommandovinduet skal se ut noe sånt som dette:

```
→  ~ xfreerdp /cert:ignore /size:1280x1024 /kbd:Norwegian /gu:bjornask /g:rds-portal.uio.no /gt:rpc /u:Admin /v:[redacted].in2120.uiocloud.n
o /p:'[redacted]' /f
[18:06:14:703] [1241:1242] [INFO][com.freerdp.core] - freerdp_connect:freerdp_set_last_error_ex resetting error state
[18:06:14:703] [1241:1242] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpdr
[18:06:14:703] [1241:1242] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpsnd
[18:06:14:704] [1241:1242] [INFO][com.freerdp.client.common.cmdline] - loading channelEx cliprdr
[18:06:14:708] [1241:1242] [INFO][com.freerdp.client.x11] - Property 307 does not exist
[18:06:15:038] [1241:1242] [INFO][com.freerdp.primitives] - primitives autodetect, using optimized
[18:06:15:388] [1241:1242] [INFO][com.freerdp.core] - transport_connect:freerdp_set_last_error_ex resetting error state
[18:06:15:424] [1241:1242] [INFO][com.freerdp.core] - freerdp_tcp_connect:freerdp_set_last_error_ex resetting error state
[18:06:15:535] [1241:1242] [INFO][com.freerdp.crypto] - creating directory /home/bjornar/.config/freerdp
[18:06:15:536] [1241:1242] [INFO][com.freerdp.crypto] - creating directory [/home/bjornar/.config/freerdp/certs]
[18:06:15:536] [1241:1242] [INFO][com.freerdp.crypto] - created directory [/home/bjornar/.config/freerdp/server]
GatewayPassword:
[18:06:23:113] [1241:1242] [INFO][com.freerdp.core] - freerdp_tcp_connect:freerdp_set_last_error_ex resetting error state
[18:06:33:343] [1241:1242] [INFO][com.freerdp.core.gateway.tsg] - TS Gateway Connection Success
[18:06:35:163] [1241:1242] [INFO][com.freerdp.gdi] - Local framebuffer format  PIXEL_FORMAT_BGRX32
[18:06:35:163] [1241:1242] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_RGB16
[18:06:35:245] [1241:1242] [INFO][com.winpr.clipboard] - initialized POSIX local file subsystem
[18:06:35:255] [1241:1242] [INFO][com.freerdp.channels.rdpsnd.client] - [static] Loaded fake backend for rdpsnd
[18:06:39:260] [1241:1242] [INFO][com.freerdp.core] - rdp_set_error_info:freerdp_set_last_error_ex resetting error state
```

Om du ikke vil ha det i fullskjerm fjerner du bare "/f" på slutten, og du kan justere "/size" isteden. Forøvrig kan du gå inn og ut av fullskjerm med CTRL+ALT+ENTER (alle tre knapper samtidig).

Det finnes også en versjon av FreeRDP tilgjengelig til Mac, men denne har vi ikke testet ut (burde fungere).

Ønsker man isteden en "pek og klikk"-løsning til Linux kan man bruke Remmina, som finnes på mange maskiner og ellers er lett å få tak i. Hvordan man stiller inn at Remmina skal gå via en gateway ser man her. Dette har vi ikke testet, men hvis du vil prøve må du bytte ut "Name" med <**ditt_labmaskinnummer**>.in2120.uiocloud.no og "Group" skal antagelig være tom/blank.

[2] *En "klient" er et program for å bruke en tjeneste, som i det engelske "client — server"*

Windows

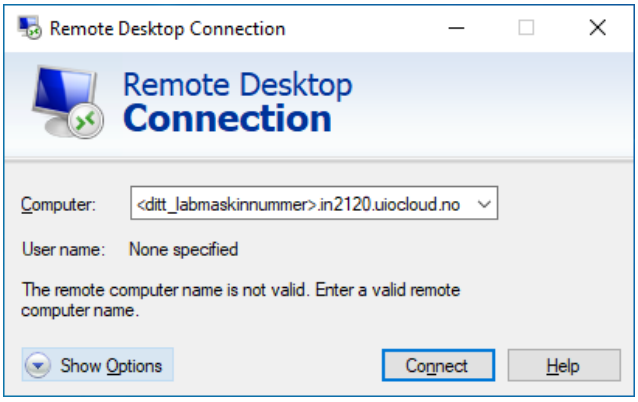
Programmet **Remote Desktop Connection** følger med Windows. Du finner det på startmenyen, under: *Windows Accessories* → *Remote Desktop Connection* (eller *Windows Tilbehør* på norsk)

Alternativt kan du trykke [*windowsknapp* + *R*] på tastaturet (begge knapper samtidig), skrive inn `mstsc.exe` og trykke *Run*/*Kjør*.

Først får man som regel opp en forenklet meny.

For å si det som en programmerer:

```
if {allerede inne på view.uio.no}
then {goto 2.}
else {trykk på "Show Options" og goto (a)}
```

1. 

Dette er samme felt som vi fyller inn i punkt 2.
Ikke bli forvirret av at vi har trykket "Show options" der.

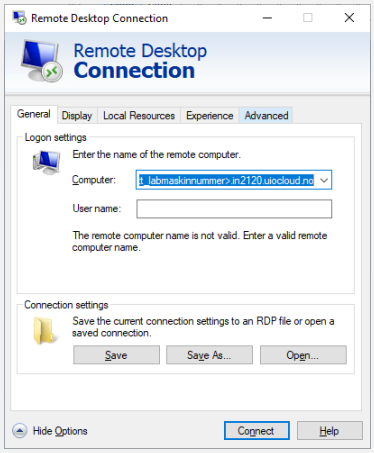
(Altså: Hopp over de følgende (a) til (f) hvis du gjør dette inne på en maskin på `view.uio.no`*.)*

(a)

Du skal få opp menyen på bildet.

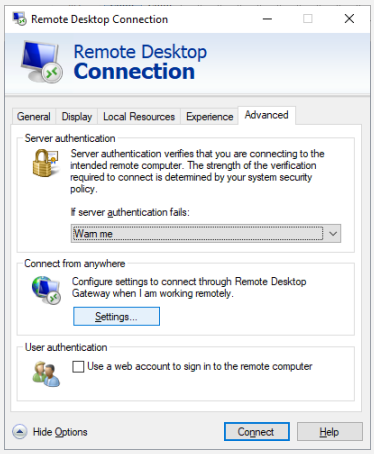
Nå må vi stille inn en "gateway", som er en slags portvokter-maskin vi skal kommunisere gjennom.

Trykk derfor på *"Advanced"*-fliken.



(b)

Trykk deg videre inn på "Settings..." (under "Connect from anywhere").



(c)

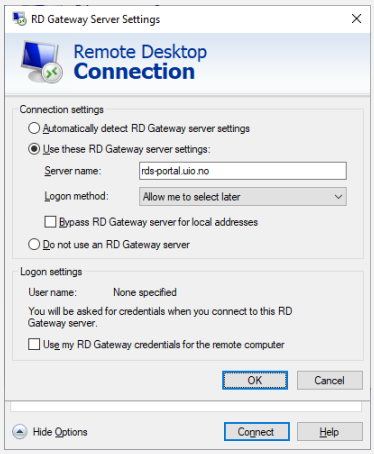
Velg "Use these RD Gateway server settings:" og fyll inn:

`rds-portal.uio.no`

Hvis noe annet er huket av og du vil unngå krøll kan du fjerne det for sikkerhets skyld.

Trykk "Ok".

I norsk Windows heter det "ES Portal", for "Eksternt Skrivebord".

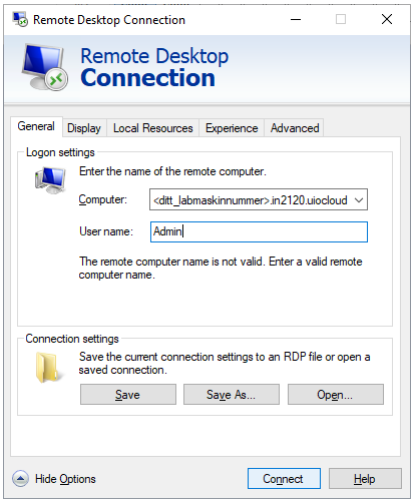


2.

Nå gjenstår det bare å fylle inn adressen til din labmaskin (noe sånt som 123.in2120.uiocloud.no) og brukernavnet "Admin" (for du skal være administrator på labmaskinen).

Computer: `<ditt_labmaskinnummer>.in2120.uiocloud.no`
User name: `Admin`

Så trykker du "Connect".

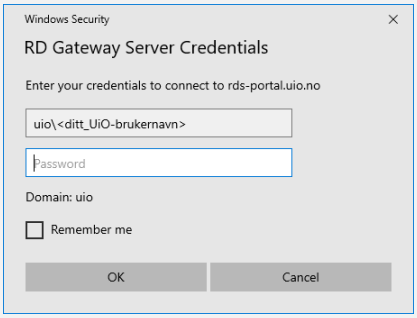


(d)

Hvis du måtte fylle inn en gateway (fordi du altså ikke allerede er inne på `view.uio.no`) får du opp denne dialogen for å logge deg inn på `rds-portal.uio.no` først.

Det er her du må fylle inn ditt **UiO-brukernavn og UiO-passord**, altså det samme som du bruker på UiO-mailen, Studentweb og generelt Feide.

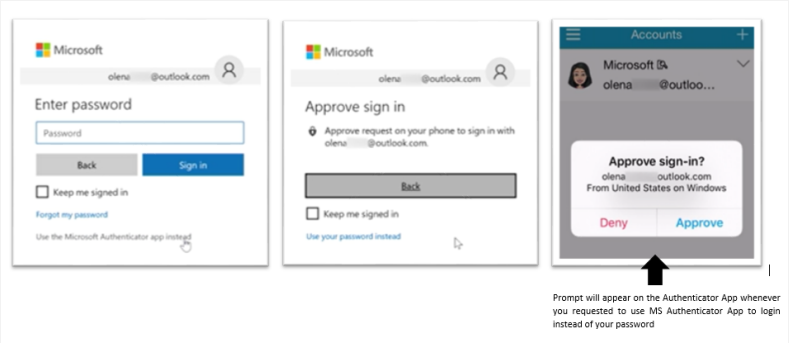
Merk at du må skrive `uio\` rett foran brukernavnet ditt.



(e)

Det er nå du må bruke 2FA-appen for tilgang til UiO sin gateway.

Når du trykker "Ok" til innloggingen i (d) skal det nemlig sprette opp en melding om å godkjenne innlogging, som du må godta.



Bildet er generelt og viser ikke hvordan det ser ut akkurat for oss.

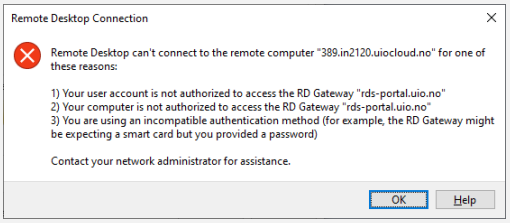
(f)

Hvis du isteden fikk opp dette bildet, er det fordi du ikke har noen fungerende 2FA-app.

Hvis du ikke ønsker å bruke 2FA-appen:

Forsøk å logge inn på view.uio.no i enten VMWare Horizon (raskest) eller i en web browser, med SMS som 2FA istedet. Gå inn på en Windows-maskin der inne, og dropp å stille inn gateway (når du altså er på en Windows-maskin på `view.uio.no`*).*

For UiO sine instruksjoner om å koble seg til `view.uio.no`*, klikk her.*
For mer om vår bruk av 2FA, klikk her.



3. Hvis du har kommet deg hit, blir du omsider spurt om passord til labmaskinen din. Fyll inn passordet (**ikke** ditt UiO-passord), trykk ok, og så skal alt funke.

Mac

Du kan laste ned Microsoft Remote Desktop i Apple sin "Mac App Store".

Oppsett er tilsvarende som for Windows, noe liknende dette (men med UiO sine maskinnavn).

Alternativt (kanskje enklest?) kan du prøve Mac-porten av FreeRDP og bruke kommandolinja, som beskrevet her.

Noen tips

- Du kan kopiere og lime inn tekst (for eksempel kommandolinja til FreeRDP) med [*ctrl* + *c*] og [*ctrl* + *v*]. I Linux-kommandolinjer må du samtidig holde inne [*shift*], for at tastetrykkene ikke skal tolkes som noe annet.
- Dersom du har problemer med å få kopiering og innliming til å fungere inne i et fjernstyrt skrivebord, kan det hende det fungerer å høyreklikke og velge "Kopier"/"Copy" eller "Lim inn"/"Paste".
- Labmaskin-passordet begynner med labmaskin-nummeret ditt, og slutter på "_". Husk at det er forskjell mellom stor og liten bokstav i passord.
- Dersom du skriver passordet inn i en kommandolinje (for eksempel til FreeRDP) må du putte enkle sitat-tegn rundt (altså `'`), for at ikke deler av passordet skal bli tolket som symboler for noe annet.
- For å slippe å skrive inn FreeRDP-kommandoen hver gang, holder det å trykke på opp-pila for å hente frem forrige kommando. Du kan også lage et alias.
- Et par artige ting å teste ut på labmaskinen, hvis du vil:
  - Foruten at Cygwin har gcc og gdb til programmering, kan du installere flere linux-programmer ved å kjøre Cygwin-installeren, som ligger under `Downloads -> program downloads -> setup-x86_64.exe`
  - I tillegg til å portscanne og sånne ting, kan du teste ut Tor og I2P som gjør surfing litt mer anonym.

Til slutt: Hvis du ikke får opp din virtuelle labmaskin

Hvis du ikke klarer å få opp din virtuelle maskin for laboppgavene kan du jobbe med en annen student på dens maskin for å finne svar på oblig-oppgavene. Det er ingen krise hvis din egen virtuelle maskin ikke virker. Å samarbeide med andre studenter på deres maskin er ikke juks.