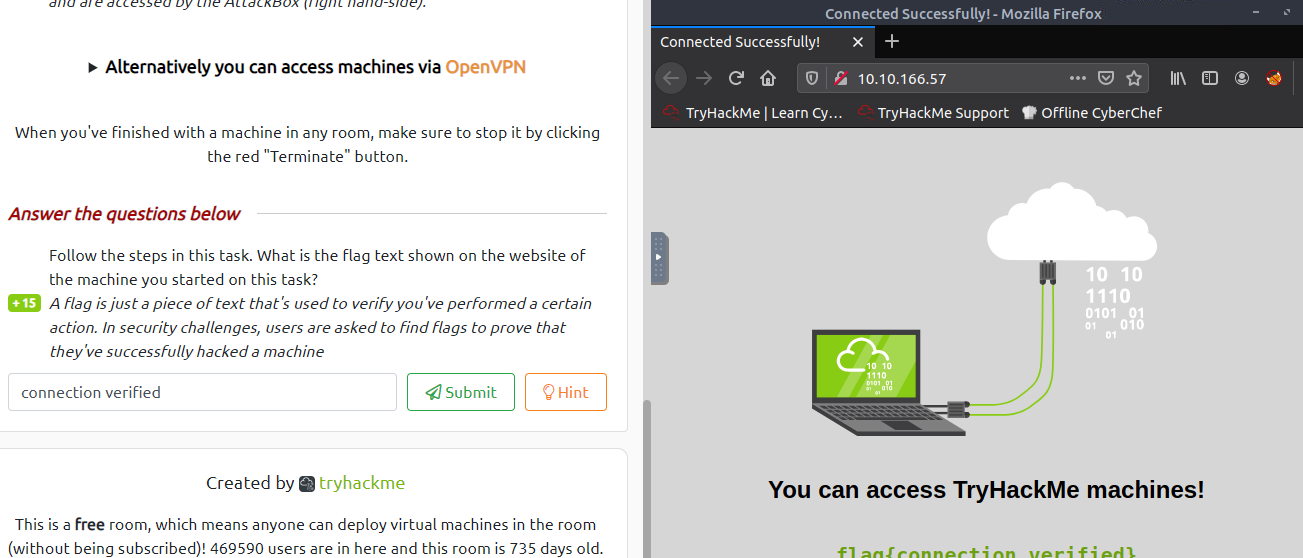
Lab 1 Del 1-

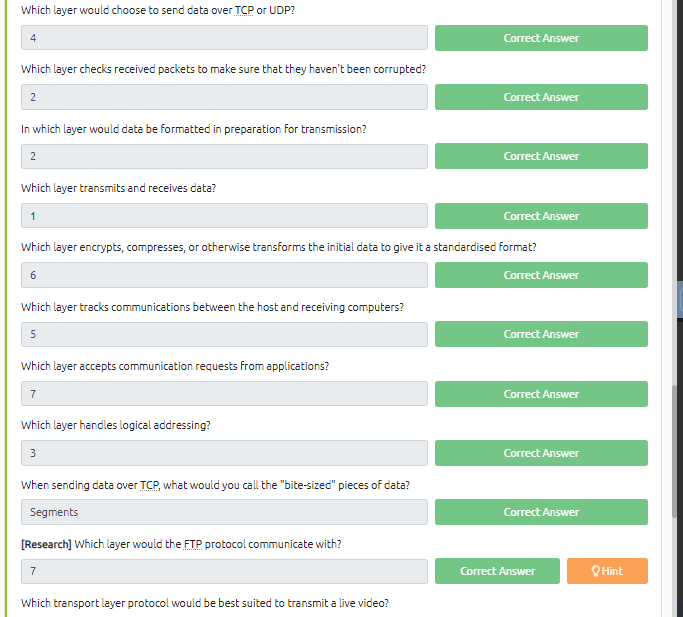
Starter attack machine og skriver inn ip adressen 10.10.166.57

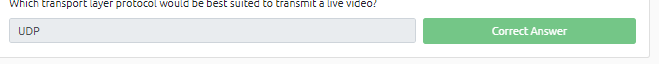


Task 1 :

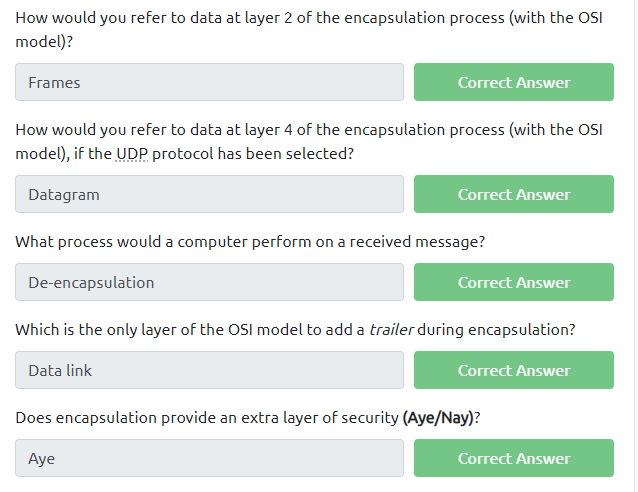
flag{connection\_verified}

Task2:

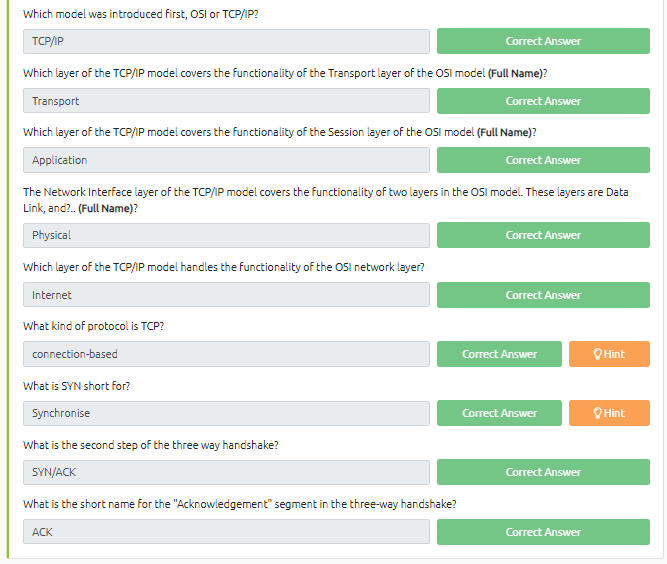




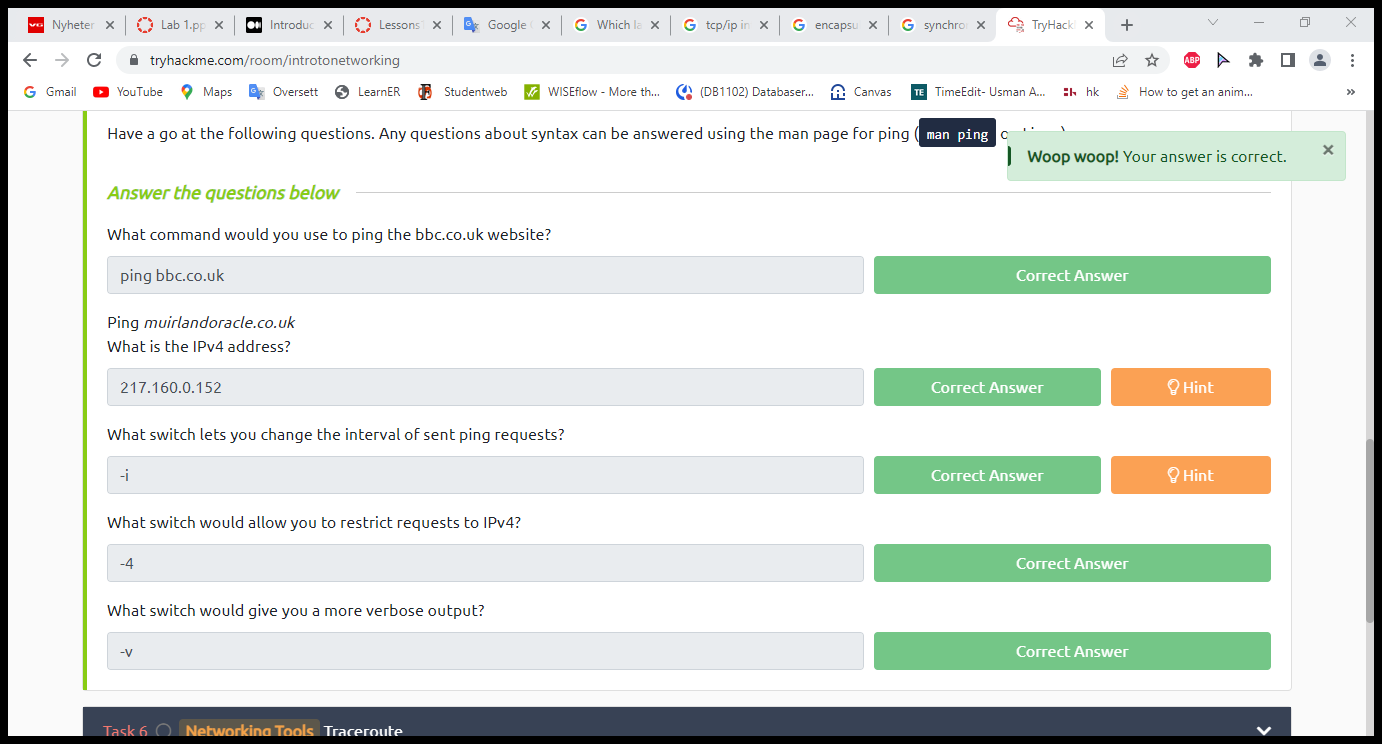
Task 3 :



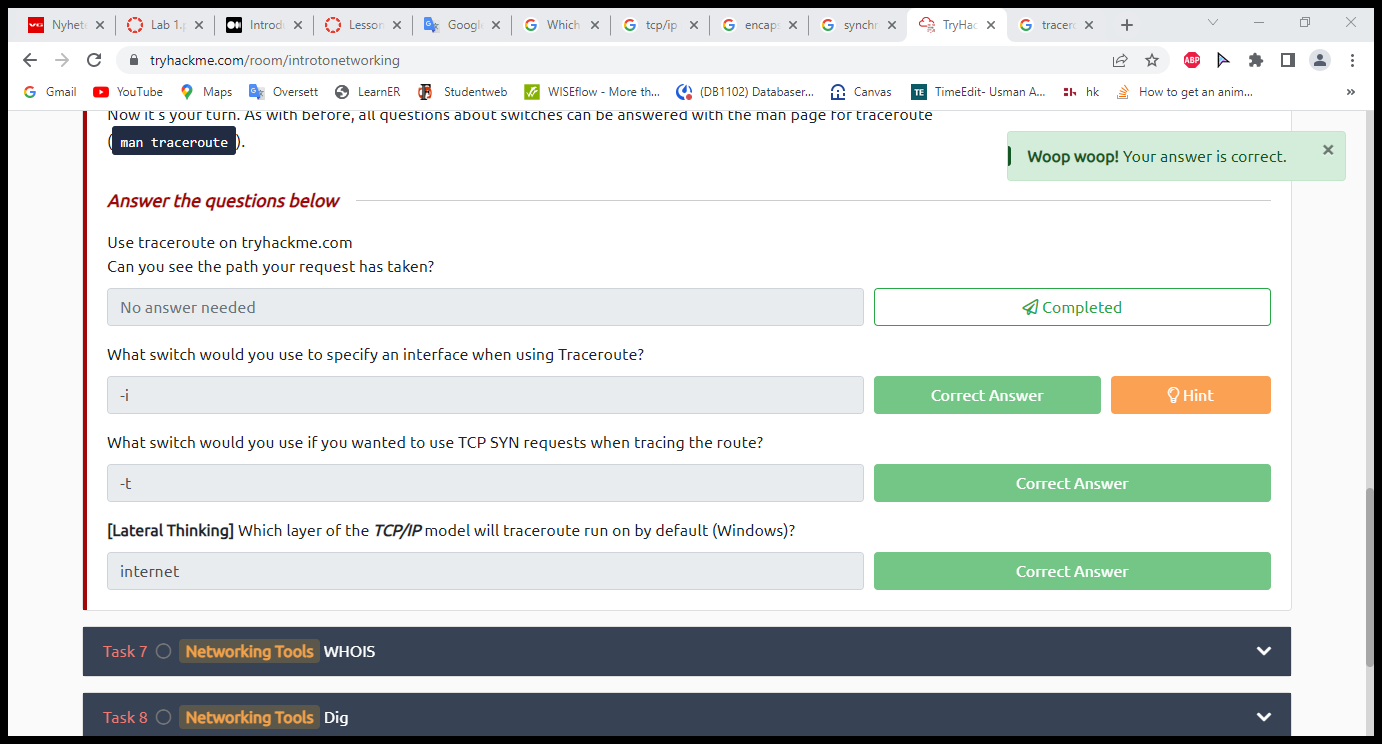
Task 4:



Task 5:

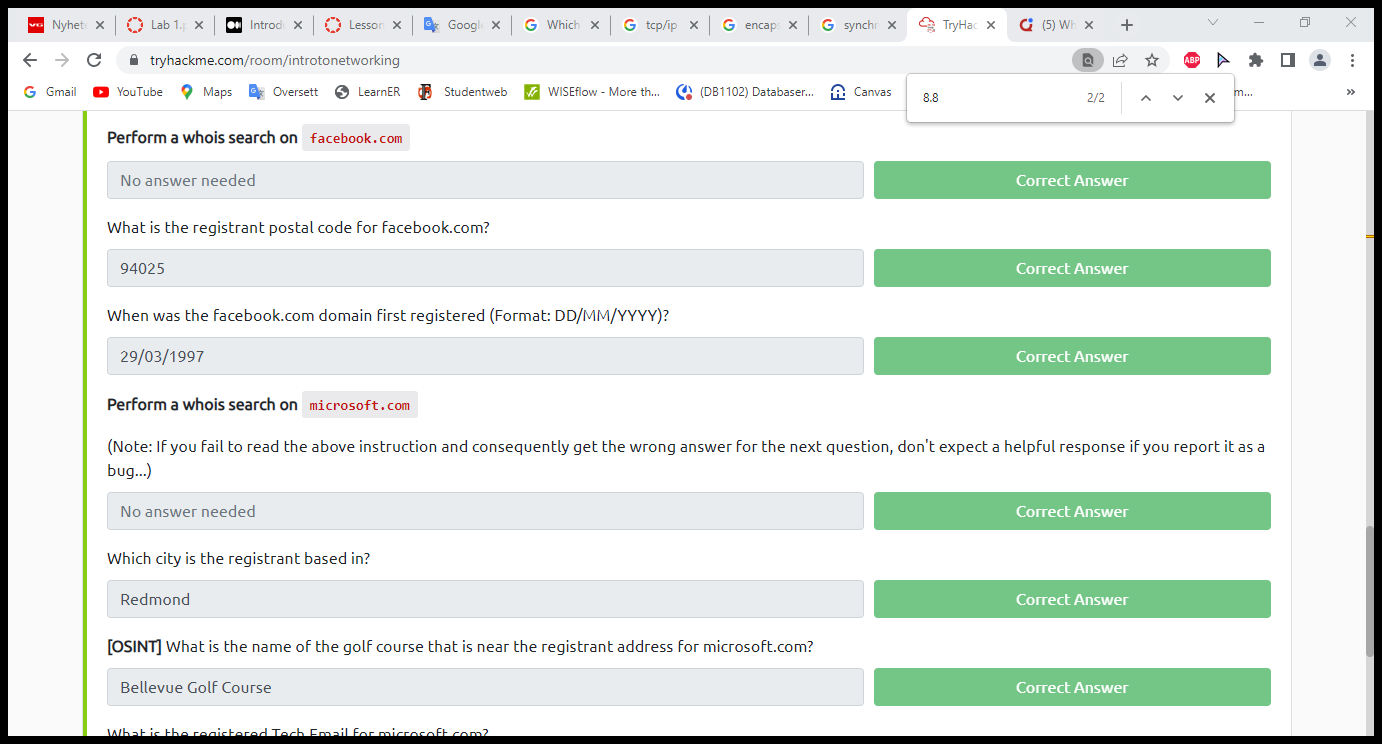


Task 6 :



Task 7:

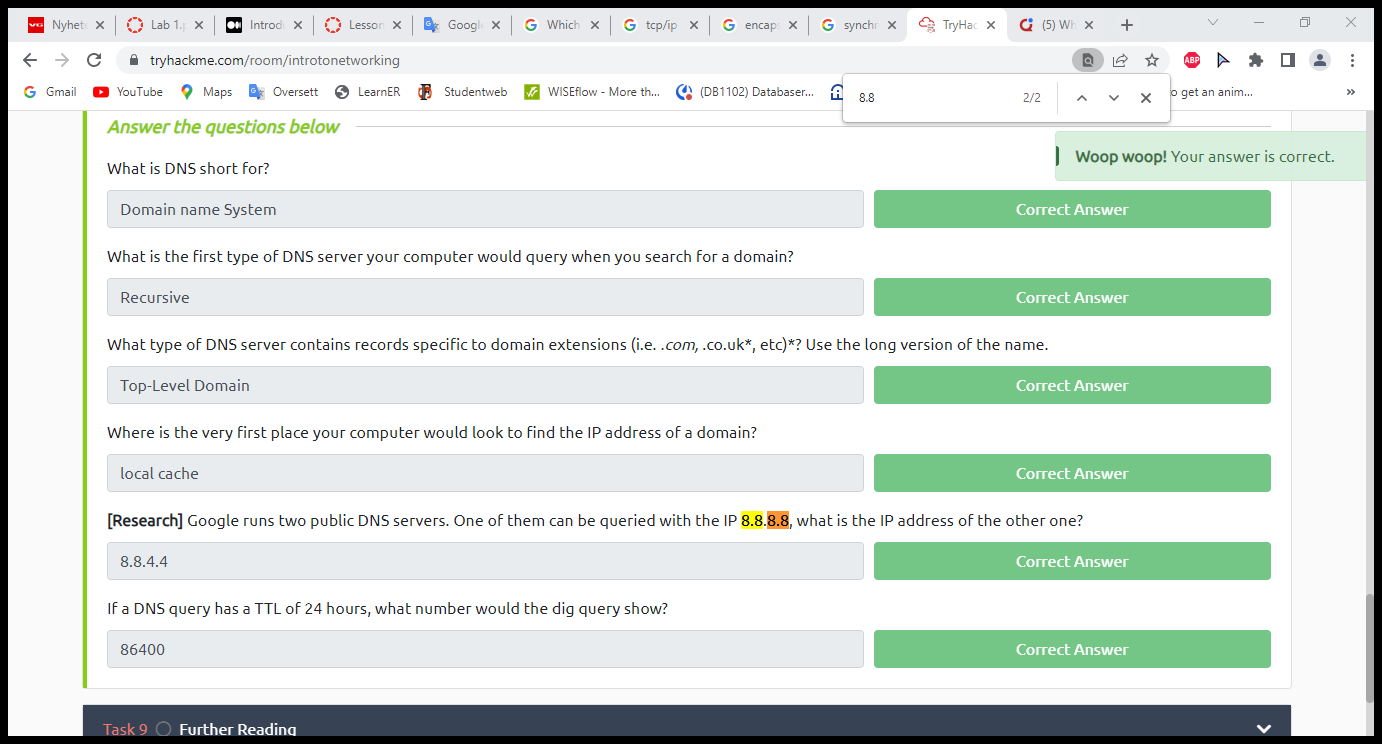
Søk whois facebook på google:



What is the registered Tech Email for microsoft.com?

msnhst@microsoft.com

Task 8:

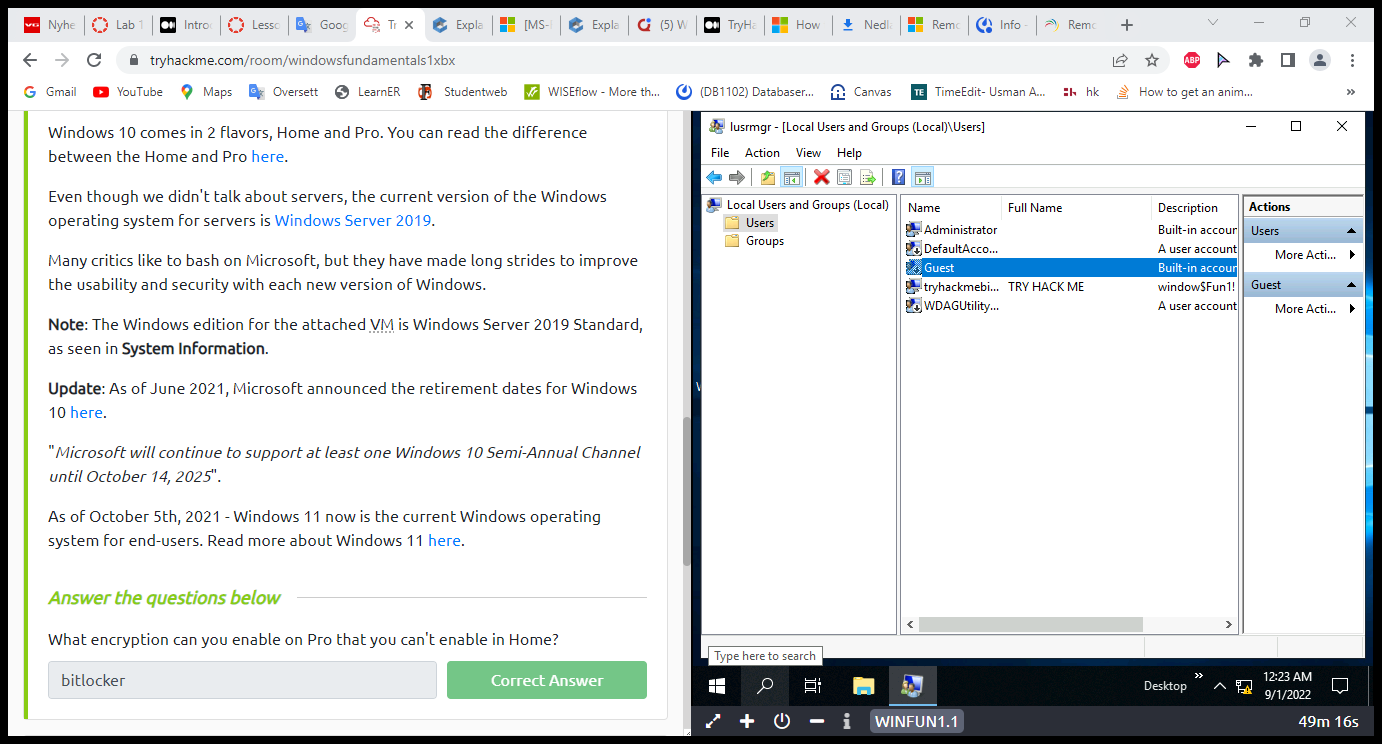


Task 9

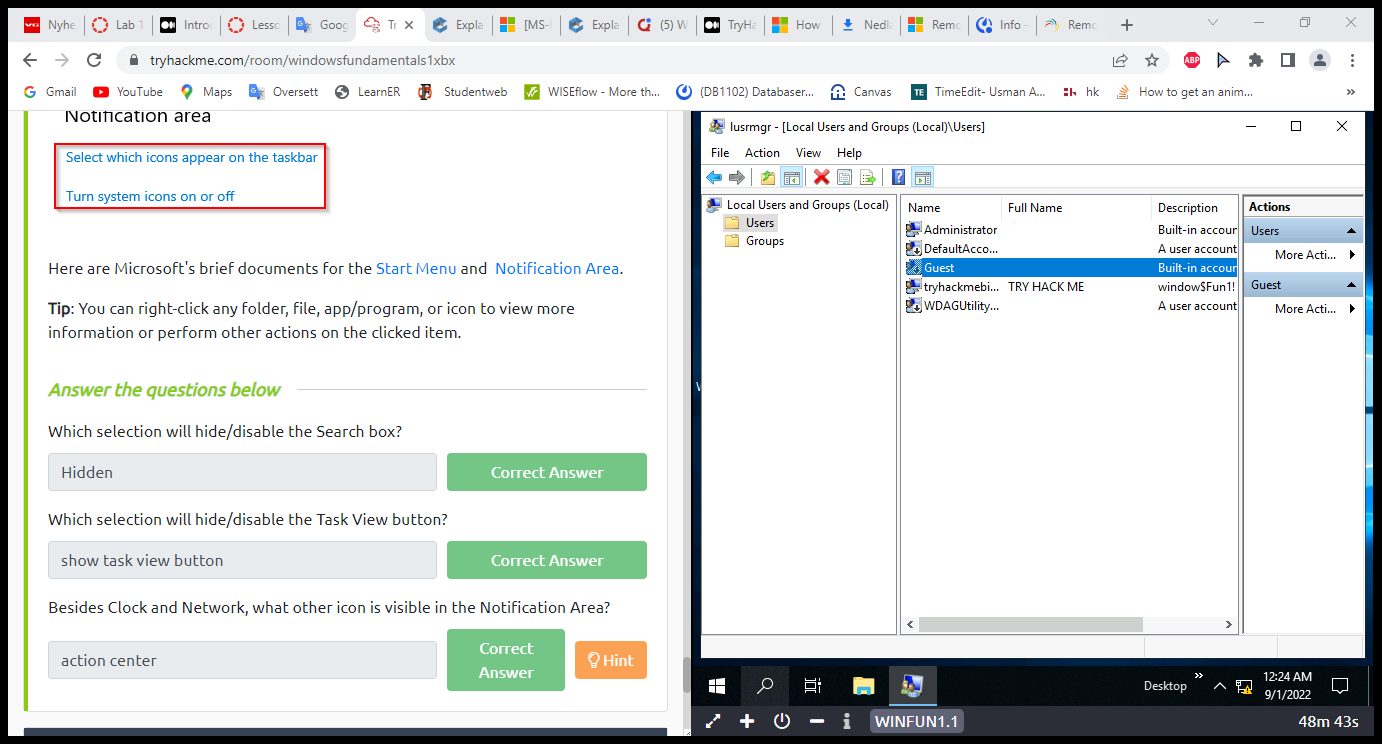
Windows fundamentals 1 :

Task 1 Start maskinen på tryhackme.com

Task 2 :



Task 3 :



Task 4 :

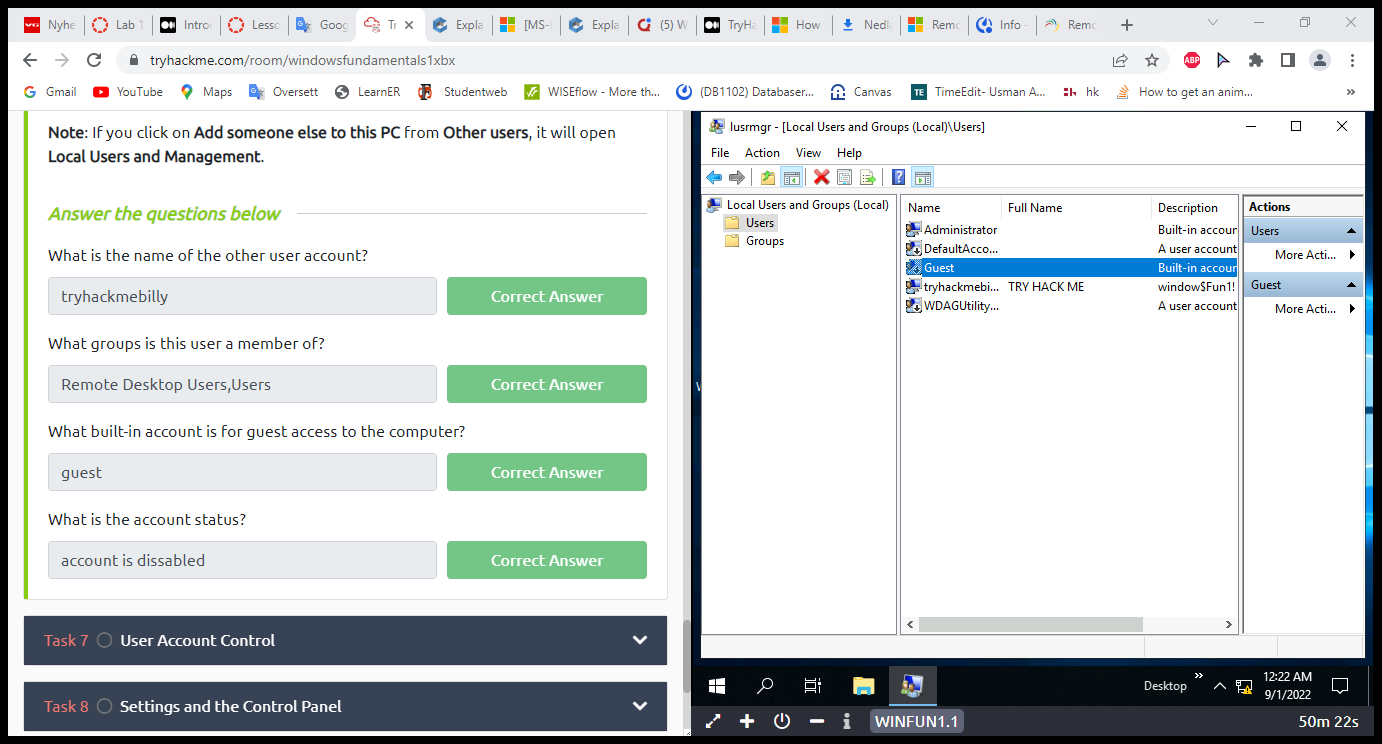
New Technology File System er svaret.

Task 5 :

%windir%

Task 6:

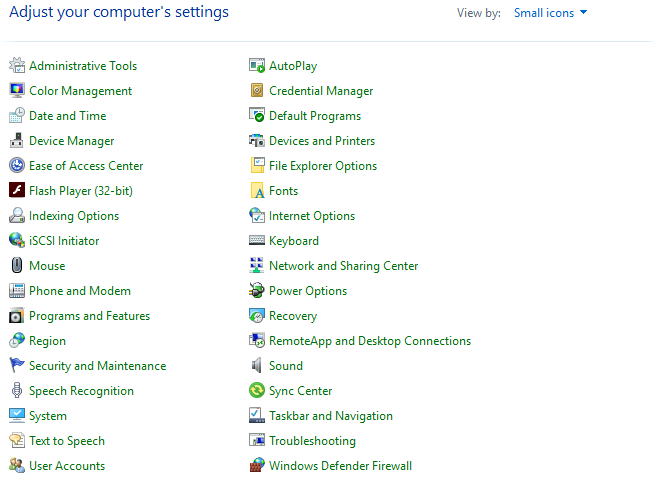
Høyre klikk på windows ikonet på menyen kjør og skriv inn lusrmgr.msc for å få en oversikt over brukere og grupper på maskinen.



Task 7:

User Account Control er svaret (UAC)

Task 8 :



Ser at siste innstillingsvalget er Windows Defender Firewall

Task 9 :

Task manager shortcut er : Ctrl+Shift+Esc. På tastaturet

Task 10 :

Trykk completed

Del 2

1. **Hva er NSMs grunnprinsipper for IKT-sikkerhet? Utforsk de fire kategoriene og se på de tilhørende kontrollene. Hvilke kontroller syns de virker spesielt viktig? Hva er sammen hengen mellom kategori, prinsipp og tiltak.**

NSM grunnprinsipper for IKT-sikkerhet er et sett med tiltak og prinsipper for å kunne sikre informasjonssystemer best mulig mot uønskede tilgang , skade eller sabotasje av systemet. Disse prinsippene vil være relevant for de store virksomhetene , i mens mindre må prioritere

De 4 NSM grunnprinsipper er : 1 )Identifisere og kartlegge , 2) Beskytte og opprettholde , 3) Oppdage , 4) Håndtere og gjenopprette. (1)Jeg mener det er spesielt viktig å kunne kartlegge systemet i virksomheten slik at man har en helhetlig og oversiktlig forståelse av styringsstrukturen, IKT -systemer og brukere i virksomheten . (3) Deretter kontrollere hvilke sårbarheter virksomheten står ovenfor for å kunne etablere en sikring mot virksomheten. (4) Videre kan man forberede virksomheten for kontrollering og håndtering av hendelsene. (2) Også kan man starte med å beskytte IKT-systemene mot sårbarheter og opprettholde en forsvarlig tilstand for å sikre systemene best mulig.

**Sammenhengen mellom kategori , tiltak og prinsipper.**

NSM har delt prinsippene inn i 4 kategorier. Og hver kategori har sine egne tiltak og prinsipper . Prinsippene og tiltakene skal bidra med å sikre Virksomhetene mot uautoriserte tilgang og misbruk. Hver prinsipp tilhører sikkerhetstiltak som beskriver en fremgangsmåte for sikring. Hver prinsipp er en aktivitet og må derfor vurderes i hele infosystemets levetid , det kan være fra planlegging og etablering til endring i systemet (avhending). De fleste grunnprinsippene bygger på hverandre selv om de er fordelt i de ulike kategoriene. Et tiltak skal kunne bidra med at de andre tiltakene skal kunne implementeres effektivt

1. **Hvilke andre grunnprinsipper har NSM utgitt? Reflekter rundt hvordan disse brukes for å etablere en helhetlig tilnærming til sikkerhet. Hvordan påvirker de hverandre? Er det mulig å ha god IKT-sikkerhet uten å ha god dekning på de andre områdene?**

NSM har utgitt andre grunnprinnsipper for fysisk sikring , personell sikring , sikkerhetsstyring .

Med disse tre bidrar dette til en solid tilnærming av sikkerhet . Den fysiske delen legger hovedfokuset på det med å sikre verdiene i en virksomhet og deretter forebygge , oppdage og håndtere en virksomhet som er utsatt for trusler . Det kan være inntrengelser eller ødeleggelse av verdiene til virksomheten . Det er også laget tiltak for sikkerhetsstyring som går ut på hvilke tiltak virksomheten må utføre for å kunne oppnå og opprettholdte et ønskelig sikkerhetsnivå.

En annen ting er personellsikring . mange aktører i dag kan sette inn personen i andre virksomheter for å kunne utføre ondsinnede handlinger , det kan være å få tilgang til verdiene virksomheten har og disse personene kan ha en sårbarhet som trussel aktører kan utnytte for å skade en virksomhet. Som kan medføre en stor konsekvens for virksomhetene . Derfor er det viktig for en virksomhet å implementere tiltak som kan forhindre dette og dermed minimere risikoen for en innside virksomhet. Dette er når en tildligere medarbeider misbruker sin tilgang for å utføre handlinger som kan sabotere eller skade systemet. Dette er lederens ansvar å ivare ta personellsikringen ved å ta i bruk slike tiltak som NSM har laget.

Personell sikkerhet sees ofte i sammenheng med fysisk sikkerhet . For virksomheten har et sett med tiltak for å kunne bidra med økt sikkerhet og gi en akseptabel sikkerhetsnivå for å kunne forsvare det fysiske aspektet. Og uten et fullstendig perspektiv vil det være tungvint for virksomheten å sikre sine verdier .

Nei det er ikke mulig å ha en god IKT – sikring uten de andre to prinsippene som fysisk er i sammenheng med sikkerhetsstyring. Virksomheten vil kunne oppnå et akseptabelt sikkerhetsnivå når de utnytter tiltakene som ivaretar de fysiske verdiene.

Og det er det samme med personell sikring er avhengig av fysisk sikring for å gi en optimal sikring.

**3. Hvilke andre rammeverk finnes for cybersikring? Hvilken standard syns du ligner mest på NSM sine grunnprinsipper? Utforsk likheter og forskjeller i de ulike standardene**

NIST (National Institute of Standards and Technology) har også sin egen sikkerhetsmodell bestående av 5 kategorier med hver sine prinsipper og tiltak for sikring av virksomhetene.

Identify , protect, detect , respond and recover (oppdag og håndter) kategorien er lik i NSM

NSM har 4 og forskjellen på kategoriene er at respond og recover er satt i separate kategorier . forskjellen er at de består av forskjellige prinsipper i de ulike kategoriene . Formålet derimot er lik for begge sikkerhets standardene det å beskytte it systemer mot uønskede handlinger og skade på virksomhetene.

**4. Du har akkurat blitt ansatt som CISO i en middels stor norsk virksomhet. Virksomheten har en del sensetiv informasjon og er avhengig av internet som en kjernefunksjon i daglig drift. Du oppdager tidlig at det er store avvik i alle de fire kategoriene i NSMs grunnprinsipper for IKT-sikkerhet. Du må utvikle en strategi for å styrke virksomhetens sikkerhet basert på grunnprinsippene. Hvordan ville du begynt?**

Siden dette er en middelsstor virksomhet kan jeg selv prioritere hvilke tiltak jeg må implementere for å sikre virksomheten best mulig , men velger å implementere de fleste prinsippene i kategoriene for å få en optimal beskyttelse av systemene .

Først ville jeg ha startet med å kartlegge styringsstrukturen for identifisering av struktur og prosesser for sikkerhetsstyring . Dette gjør jeg for å kunne styre arbeidet med IKT systemene. Dette er viktig for å få en helhetsoversikt over styringsstrukturen som bidrar med at jeg får informasjon som kan bidra med å prioritere og styre sikkerhetsarbeidet på virksomheten. Deretter ville jeg ha jobbet med å ivareta sikringen får å kunne sikre tilstanden over lengere tid og ha en full overvåkning av systemene. Dette gjør jeg for å forhindre mot fremtidige datatrusler som kan gi en konsekvens for IKT systemene. Hvis det blir oppdaget en trussel ville jeg ha sørget for at denne sårbarheten fjernes så fort som mulig . og hvis det er noen sikkerhetshull ville jeg ha tettet dem. Dette fører videre til det med å forberede seg på fremtidige trusler. Derfor er det viktig å ta en vurdering , kontrollere og håndtere dersom en slik hendelse inntar.

**5) I hvilke av de fire kategoriene ville du fokusert? Finnes det noen ”quick wins”? Er det noen områder som egner seg bedre for tjenesteutsetting enn andre? Drøft og diskuter gjerne med andre og lag virksomhetens strategi et tekstdokument.**

Jeg hadde fokusert mest å beskytte og opprettholde systemene og dersom en sårbarhet oppdages ville jeg ha jobbet med å få den ut av systemet og håndtere den sikkert . Da hadde jeg videre satt en overvåkning på systemet slik at jeg kan opprettholde sikkerheten i systemet .