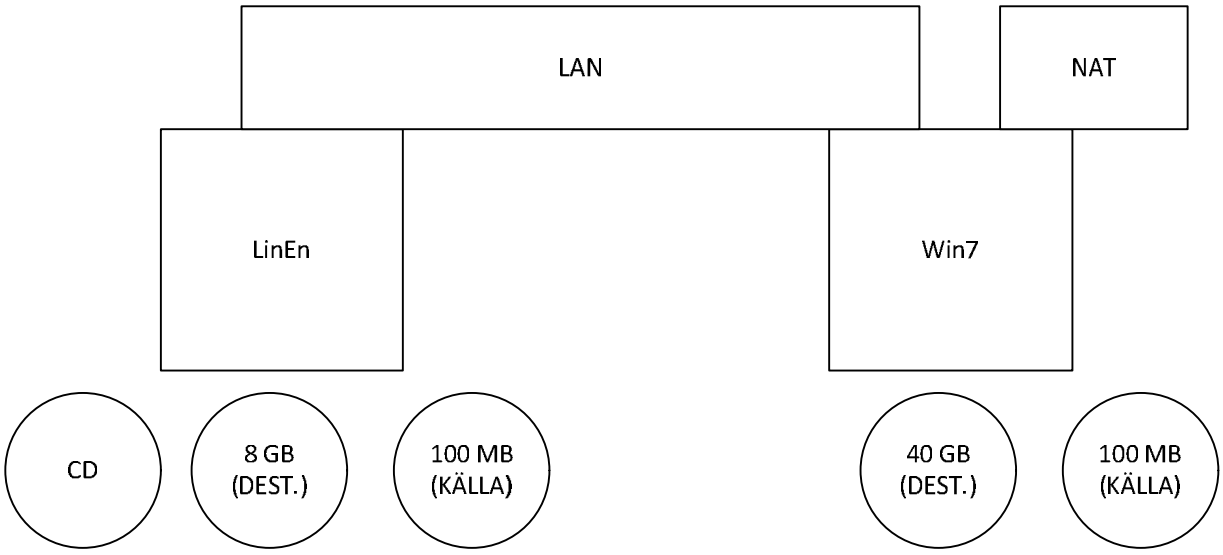
DT2005-2012
Avancerade forensiska verktyg I

Laboration 1

Syfte/mål
Laborationens syfte är att öva färdigheten att skapa korrekta forensiska avbilder med hjälp av olika verktyg, i huvudsak EnCase. Laborationen omfattar även att göra en korrekt wipe, hur man gör en nätverks utvinning samt hur HPA/DCO påverkar vårt arbete.

Förberedelse
Anslut till nätdisken \\idefs-03virt.hhnet\mawe (sal D513) alternativt \\idefs-03\mawe (övriga salar). Kopiera foldern DT2005-2012-Lab1 till disk D: . Starta de två kopierade VM från D: .

Systemöversikt



Systemet består av två virtuella maskiner sammankopplade med ett LAN. De har en stor och en liten hårddisk. Den lilla disken ska användas som källa i de olika övningarna. Windowsmaskinen är dessutom kopplad till Internet via NAT.

Uppgifter

- Genomför en lokal utvinning av käll-disken i EnCase. Se övning 4.1 och sidorna 130-137. Du jobbar endast i Windows.
- Genomför en lokal utvinning av källdisken i FTK Imager Lite. Använd format E01. Du jobbar endast i Windows.
- Genomför en lokal utvinning av källdisken i LinEn. Se sidorna 156-160 i boken. Du jobbar endast i Linux. Destinationsdisken är inte formatterad. Slå upp på Internet hur man partionerar och formaterar en oallokerad disk i Linux.
- Genomför en wipe av källdisken i EnCase. Se sidorna 542-545 i boken. Du jobbar endast i Windows.
- Extra uppgift. Genomför en nätverksutvinning mellan LinEn och EnCase. Se sidan 161 i boken. Du jobbar i Windows och Linux. Du måste ställa in statiska IP för båda maskinerna. Windowsmaskinens interface som kopplar mot NAT kan stängas av helt. Brandväggen i Windowsmaskinen kan stängas av helt.

Demonstration

- Tablau write blocker/TIM
- NetCat
- HPA/DCO