System Engineering Project 2023-2024 (EP3)

Inhoudsopgave

1 De context

In de derde examenperiode geven we jullie de keuze tussen een groepsopdracht of een individuele opdracht. In beide gevallen valt de opdracht rond de offerte weg. De opdrachten zijn hier onder uitgeschreven en zijn zo goed als identiek aan EP1 met hier en daar een kleine aanpassing. Lees het stuk “organisatie” zeker door zodat je weet hoe je jouw keuze bekend moet maken.

2 Individuele opdracht

Wanneer je kiest om de opdracht individueel aan te pakken dan laten we toe om de gehele setup uit te werken in VirtualBox op één laptop. Het is toegelaten dat alle machines zich bevinden in 1 subnetwerk, zonder VLANs – dit laat je toe alle servers te testen op je eigen laptop. **De opdracht blijft, op het netwerkgedeelte na, ongewijzigd.** Jouw skills in het configureren van netwerkapparatuur toon je enerzijds aan door een packet tracer setup voor te bereiden (cfr. paragraaf 2.1), anderzijds sluit je jouw opstelling aan op het klasnetwerk tijdens je demo-moment (cfr. paragraaf 2.2).

2.1 Netwerkopdracht (+ voorbereiding in packet tracer)

Tijdens je demo configureer je zelf NAT op een uplink router; je sluit je laptop aan op een switch die verbindt naar de LAN kant van jouw router. De WAN kant gebruikt het klasnetwerk (de default gateway in het klasnetwerk is 172.22.255.254; de DNS server is 172.22.128.1.).

Je werkt eveneens een packet tracer voorbereiding uit die deze ‘basic NAT’ opstelling bevat. Je kan starten vanaf het bestand ‘SEP-EP3-simulatie'. De client moet kunnen surfen naar (het gesimuleerde) www.hogent.internal.

2.2 Flat network

Opdelen in subnets vervalt – je sluit al jouw VMs aan op één en hetzelfde netwerk, binnen de range 192.168.149.0/24. Hoe je dit netwerk op je laptop in Virtualbox, is een keuze: het staat je vrij om in VirtualBox te experimenteren en een voorstel in te dienen. Zorg er dan echter voor dat je dit goed argumenteert. Probeer geen onnodige netwerkkaarten aan je virtuele machines toe te voegen! Speel je liever op safe dan staat hieronder een werkbare VirtualBox netwerk setup beschreven waarmee je aan de slag kan gaan.

Tijdens je demo-moment switch je alle VMs naar **bridged mode** als je ze aansluit op de switch van je eigen netwerk.

2.3 Addendum: Virtualbox Host-only suggestie

Merk op dat dit equivalent is aan de setup die gebruikt wordt in het olod Cybersecurity en Virtualisation; je kan en mag de bestaande Debian router dus hergebruiken.

Setup – host-only netwerk voorzien van internet (deze beschrijving is ook te vinden in het leerpad van cybersecurity en virtualisatie, puntje 2.2.3):

1. Maak een host-only netwerk aan in VirtualBox via VBoxManager (CLI) of in de GUI via “File” > “Tools” > “Network Manager” met volgende eigenschappen.
    a. Adapter: “Configure Adapter Manually” en kies een IPv4 Adres (bijvoorbeeld 192.168.50.1) en IPv4 Network Mask (bijvoorbeeld 255.255.255.0).
    b. Zorg ervoor dat bij de tab DHCP Server er geen Server draait, met andere woorden, Enable Server heeft **geen** vinkje.
2. Maak een Linux router machine. De setup is het vaakst getest op debian, we raden dus aan om een Debian machine op te zetten. Dit kan via vagrant, osboxes maar een clean install gaat ook vlot vanaf de iso. Zorg ervoor dat dit geen grafische interface heeft.
3. Zorg ervoor dat deze machine 2 NIC’s heeft. De eerste is verbonden met de default NAT van VirtualBox. De tweede verbind je met het host-only netwerk dat je gemaakt hebt in de eerste stap.
4. Voer onderstaande commando’s uit, of kopieer het als script. Zorg ervoor dat je root rechten hebt. Het is mogelijk dat je dit script meermaals moet uitvoeren om alles in orde te krijgen. Probeer na te gaan wat je doet en te troubleshooten waar nodig. Controleer opnieuw de interface namen.
5. Elke virtuele machine die nu op dit host-only netwerk verbindt, zal via DHCP een IP-adres krijgen. Wil je dit niet dan moet je het statisch instellen. Wijzig de DHCP range indien gewenst.

Router script

```
#!/bin/bash

apt update && apt upgrade -y
apt install vim bind9 isc-dhcp-server -y

# Enable routing
echo "net.ipv4.ip_forward = 1" >> /etc/sysctl.conf
/usr/sbin/sysctl -p

# Setup static IP
/usr/bin/cat << EOF >> /etc/network/interfaces.d/enp0s8
allow-hotplug enp0s8
iface enp0s8 inet static
    address 192.168.50.10
    netmask 255.255.255.0
EOF
```

```
# Setup Bind/DNS

/usr/bin/cat << EOF > /etc/bind/named.conf.options
  options {
      directory "/var/cache/bind";

      listen-on port 53 { any; };
      allow-query { any; };
      recursion yes;
      dnssec-validation no;
      forwarders {
              1.1.1.1;
      };
      forward only;
  };
EOF

systemctl enable named
systemctl start named

# Enable NAT'ing
systemctl enable nftables
systemctl start nftables



/usr/bin/cat << EOF > /etc/nftables.conf
#!/usr/sbin/nft -f

# Flush the rule set
flush ruleset

# Create a nat table
add table nat
add chain nat prerouting { type nat hook prerouting priority -100 ; }
add chain nat postrouting { type nat hook postrouting priority 100 ; }
add rule nat postrouting oifname "enp0s3" masquerade
EOF
```

```
# Configure and enable DHCP
/usr/bin/cat << EOF > /etc/default/isc-dhcp-server
INTERFACESv4="enp0s8"
EOF

/usr/bin/cat << EOF > /etc/dhcp/dhcpd.conf
# dhcpd.conf
option domain-name "hogent.local";
option domain-name-servers 192.168.50.10;

default-lease-time 600;
max-lease-time 7200;

ddns-update-style none;

subnet 192.168.100.0 netmask 255.255.255.0 {
    range 192.168.50.11 192.168.50.100;
    option routers 192.168.50.10;
    option subnet-mask 255.255.255.0;
}
EOF

reboot
```

3 Groepsopdracht

De groepsopdracht is identiek aan de opdracht uit EP1, behalve de offerte. Je moet dus nog altijd minstens een volledig werkende basisopstelling hebben met 2 extra's om te kunnen slagen.

3.1 Basisopdracht

3.1.1 Algemeen

Voor de basisomgeving gebruik je een domeinnaam met volgende structuur: <groepsafkorting>-<vestigingsnaam>.internal

❗ **Let op**: Als voorbeeld wordt er in dit document telkens gebruikt gemaakt van l01-thematrix.internal (de l van "lectoren"). Vervang dit steeds door jullie eigen domeinnaam (bv. g03-syndus.internal voor groep 3 uit Gent of a02-aralis.internal voor groep 2 uit Aalst).

- Leg eerst en vooral een IP-adrestabel vast voor alle componenten in het netwerk die dit nodig hebben. De specificaties voor de adressen vind je hieronder.
- De serverinfrastructuur bestaat uit virtuele machines (VMs) gebaseerd op een evenredige mengeling van Windows Server en de laatste versie van AlmaLinux. Servers bestaan enkel uit CLI gebaseerde VMs, een GUI is hier immers overbodig.
- Installatie en configuratie van de Windows systemen gebeurt deels in de GUI en deels aan de hand van PowerShell scripts. Op de Linux-systemen gebeurt dit **volledig** met Vagrant en bash-scripting. Wil je dit anders aanpakken, dan moet je dit eerst overleggen met de technische coaches.
- Containertechnieken zoals docker, docker compose, podman, LXC, ... zijn niet toegelaten. Tools zoals Puppet, Ansible, ... zijn ook niet toegelaten. Het doel is dat je zelf de scripts uitwerkt.
- Zorg ervoor dat alle scripts herbruikbaar zijn. Hiermee bedoelen we dat je "hard-coded" waarden vermijdt, maar in plaats daarvan overal variabelen gebruikt. De systeembeheerder kan de gewenste waarden invullen in een configuratiebestand dat ingelezen wordt door je scripts, of (in het geval van een PowerShell-script) via een dialoogvenster bij de uitvoering van het script.
- Schrijf testplannen met exacte procedures die toelaten te valideren of een deeltaak is uitgevoerd volgens de specificaties.
- Een ander teamlid volgt de instructies van de testplannen en schrijft een testrapport over het resultaat. Indien er tests falen, wordt een ticket aangemaakt in het kanban bord (met een link naar het rapport) zodat de verantwoordelijke de fout kan oplossen.

3.1.2 Netwerk

Het netwerk en alle servers worden uitgewerkt met IPv4; IPv6 is een challenge. Plan vooraf de nodige subnetten en verspil geen IP-adressen. Alle subnetten kies je binnen de vastgelegde range 192.168.10**X**.0/24, waarbij 10**X** staat voor jullie groepsnummer vermeerderd met 100. De default gateway die de ISP (zie onder) bij iteratie 1 zal gebruiken is 192.168.10**X**.254/30, en komt dus uit jouw eigen range van adressen! Jouw uplink interface gebruikt 192.168.10**X**.253/30.

Basisnetwerk - iteratie 1

Alle servers die je opzet maken gebruik van dit netwerk. Je simuleert dit netwerk in Packet Tracer, en test de (deels geautomatiseerde) uitrol op de netwerkapparatuur in het leslokaal. In een eerste iteratie baseer je jou op de kennis verworven in 'Computer Networks 2'.

- Voorzie VLANs voor servers, employees en DMZ:
    - VLAN 42 Interne servers
        - Vaste, private IP-adressen
        - De IP-adressen corresponderen met de adressering van de servers.
    - VLAN 11 Werkstations employees
        - Dynamische, private IP-adressen (via DHCP)
        - Kunnen interne servers en Internet bereiken
    - VLAN 13 DMZ
        - Vaste, private IP-adressen
        - Is bereikbaar vanop Internet; is ook bereikbaar vanuit de VLAN van de employees
        - Kan zelf ook de nodige servers binnen de VLAN van de Interne servers bereiken - maar enkel de nodige!
    - VLAN 1 Network Management
        - Vaste, private IP-adressen voor de netwerktoestellen (switch, router, TFTP-server (zie onder))
        - Enkel toegankelijk voor de TFTP-server - hoe ga je dit beveiligen (zie *1)?
- Inter-VLAN routing wordt uitgevoerd met een **router-on-a-stick** configuration.
- Simuleer de netwerkinfrastructuur met Packet Tracer. Na succesvolle simulatie worden dezelfde configuraties **geïmporteerd** op de apparatuur in het netwerklokaal, en worden de (virtuele) servers aangesloten tot één werkend geheel.
    - De configuraties van de netwerktoestellen worden vanaf een **TFTP-server** (zie Linux) opgeladen [1] - manuele aanpassingen nadien zijn te vermijden en stel je bij in de configs op deze TFTP-server!
    - In de eerste iteratie van jouw set-up stuur je het verkeer door naar een default ISP-router, opgezet door de lectoren. De **static routes** die de ISP moet configureren naar jouw router worden doorgeven aan de netwerk-lector.
- De gehele opstelling wordt lokaal uitgevoerd met VMs en de aanwezige apparatuur in het netwerklokaal.
    - De VMs draaien op de laptops van de studenten - je switcht de VM naar **bridged mode** als je hem aansluit op je eigen netwerk. Als er meerdere VM's op een enkele laptop moeten draaien: denk goed op voorhand na over deze verdeling (CPUs, RAM) om performantiebottlenecks en andere problemen te vermijden.

Basisnetwerk - iteratie 2

In een tweede iteratie baseer je jou op de kennis verworven in 'Computer Networks 3'. Deze zaken zal je pas kunnen implementeren nadat in dit vak de relevante lessen gegeven zijn.

- Configureer zelf NAT op je uplink router, die als publiek adres een IP-adres uit de netwerk-range van het leslokaal gebruikt (automatisch ingesteld via DHCP, de router wordt hier client!). Het subnetwerk (.252/30) naar de ISP-router uit iteratie 1 verdwijnt dan uit de set-up. Alternatief gebruik je een statisch IP 172.22.200.X/16,

waarbij X staat voor jullie groepsnummer. Default gateway in het klasnetwerk is 172.22.255.254; de DNS server is 172.22.128.1.

- (*1) Werk de Cisco router bij met de nodige Access Control Lists (ACLs) om het netwerk te beperken. Bouw deze firewall regels op vanuit het 'principle of least privilege': enkel de gekende communicatie tussen de drie netwerken wordt toegelaten; andere subnets en poorten worden by default geweigerd.
- Blijf (vanzelfsprekend) werken met configuraties die, na het booten van de netwerktoestellen, opgeladen worden vanaf de TFTP-server - je kan jezelf vermeien met deze semi-geautomatiseerde manier van werken!

3.1.3 Windows servers

Windows Servers bestaan enkel uit **CLI** gebaseerde VMs, een GUI is hier immers overbodig. De VMs zijn te benaderen via RSAT vanop een Windows GUI **client** VM.

3.1.4 Domain Controller

- Binnen jullie organisatie moeten al jullie systemen centraal beheerd worden. Hiervoor moeten jullie een Active Directory Domain opzetten, gecontroleerd door een Domain Controller (DC). Elk Windows toestel moet deel uitmaken van dit domain.
- Op deze DC draait Windows Server 2022 Standard als OS. Er is dus geen grafische interface aanwezig, enkel een CLI. Zorg er wel voor dat je een Windows Client (Windows 10/11) hebt binnen je domain met daarop de nodige RSAT-tools zodat je toch een grafisch overzicht hebt van de serverconfiguratie.
- Gebruik ad.l01-thematrix.internal als root domain voor Active Directory. Zo vermijd je conflicten met de webserver (zie verder).
- Stel een logische domainstructuur voor jullie organisatie op waarbinnen alle toestellen en gebruikers zijn ondergebracht. Gebruik dus niet de standaard containers die automatisch worden aangemaakt door Windows Server.
- Zorg ervoor dat de PC's en servers geen lokale gebruikers hebben, maar dat de authenticatie gebeurt via de DC. Verdeel de gebruikers in groepen met verschillende rechten. Denk hier zorgvuldig over na en zorg ervoor dat je bij minstens één gebruikersgroep afdwingt dat ze op bepaalde toestellen niet kunnen inloggen. Doe dit aan de hand van een Group Policy.
- Voorzie voor elke gebruiker een shared folder op deze DC.
- De Domain Controller is ook de DNS-server van het domain. Zorg ervoor dat deze alle DNS-queries binnen het domain kan beantwoorden. Voorzie dus de nodige A-records, PTR-records en CNAME-records voor de verschillende servers en clients. Queries voor andere domainen moet de DC doorsturen naar een forwarder naar keuze.
- Automatiseer dit alles zoveel mogelijk. Gebruik hiervoor scripts met VboxManage om de VM's aan te maken in Virtualbox, en PowerShell-commando's om de VM's nadien te configureren.

3.1.5 Linux servers

- Gebruik voor alle Linux VM's de laatste versie van AlmaLinux op dit moment. Installeer geen GUI. Alle servers mogen **enkel over een CLI** beschikken.
- Schakel SELinux niet uit.

- Linux VMs zijn benaderbaar via SSH. Zorg ervoor dat je **nooit** met het root account kan inloggen en dat je **enkel** door middel van SSH keys kan inloggen (dus niet door een gebruikersnaam en wachtwoord in te geven).

3.1.6 Databank

- Installeer een databank naar keuze (bv. MariaDB, PostgreSQL, ...). Deze zal gebruikt worden voor de CMS (zie verder).
- Enkel poorten nodig voor de databank en SSH mogen open staan in de firewall.
- Configureer de databank zodat deze enkel connecties aanvaardt van (het IP-adres van) de webserver. M.a.w. enkel de webserver kan connecteren op de databankpoort. Databank clients op andere devices worden sowieso geweigerd.

3.1.7 Webserver

- Installeer een webserver naar keuze (bv. Nginx, Apache, ...)
- Installeer op deze server een CMS (content management system) naar keuze (bv. Drupal, Wordpress, ...). De CMS moet gebruik maken van de databank op de databankserver.
- Zorg ervoor dat je kan inloggen en een post kan aanmaken.

3.1.8 Reverse proxy

- Plaats in de DMZ een reverse proxy naar keuze (Nginx, Apache, ...).
- HTTP**S** gaan we niet instellen op de webserver. In dit netwerk wordt dit de taak van de reverse proxy. De webserver is dus niet rechtstreeks van buitenaf bereikbaar, maar enkel via de reverse proxy. Maak gebruik van self-signed certificates voor HTTPS zodat je vanop elk werkstation naar deze webserver surfen zowel met of zonder het "www" voorvoegsel (https://www.l01-thematrix.internal/ en https://l01-thematrix.internal/). Bekijk onderstaande figuur: er is dus enkel een HTTPS-verbinding tussen client en reverse proxy. Tussen de reverse proxy en de webserver is er enkel een HTTP-verbinding.
- Zorg ervoor dat de reverse proxy HTTP/**2** over TLS gebruikt.
- Zorg ervoor dat, als de webserver gescand wordt met nmap, deze geen informatie geeft over de versie van de server.

3.1.9 TFTP-server

- Installeer een TFTP-server naar keuze.
- Netwerktoestellen worden via deze TFTP-server geconfigureerd (zie boven).
- De automatische installatie kopieert de netwerkconfiguraties naar de juiste map op deze server.

3.2 Uitbreidingen

In deze paragraaf worden uitbreidingen voor de basisomgeving omschreven. Hier kan je als team uit 'cherry picken': wat van deze zaken wil je implementeren? Bespreek met het team en overleg met de begeleider.

3.2.1 NAT port forwarding

- Breid de NAT-configuratie (zie basisopdracht) met port forwarding: externe vragen op poort 80 worden afgeleverd aan de reverse proxy in DMZ. Als extern IP-adres werk je niet met DHCP, maar met een statisch IP 172.22.200.**X**/16, waarbij **X** staat voor jullie groepsnummer (zie iteratie 2).
- Dit IP-adres resolved naar sepgroup**0X**.hogent.be (zonder leading zero als je groepsnummer groter is dan 9). Test door te surfen vanuit het klasnetwerk: is je website bereikbaar op https://sepgroup0X.hogent.be?

3.2.2 Redundante router

- Ontdubbel je router: werk een redundante (passive) router uit die een kabelbreuk naar de switch, een kabelbreuk naar de ISP, of een falen van de eerste router, kan opvangen. Let wel: dit opzetten is enkel mogelijk vanaf iteratie 2! Als extern IP-adres werk je niet met DHCP, maar met een statisch IP (zie NAT port forwarding). De tweede router ken je 172.22.200.**10X**/16 toe, waarbij **X** staat voor jullie groepsnummer.
- In een testplan test je ook de drie verschillende scenario's.
- Beide routers worden geconfigureerd vanaf de TFTP-server.

3.2.3 Trunk naar bridged (TFTP) VM

- Een aparte server voor TFTP is misschien overkill: deze wordt immers enkel gebruikt om éénmalig de netwerkapparatuur in te stellen. Merge de configuratie van de TFTP-server met één van de Linux-servers die je extra opstelt - en beperk dit tot één extra VM.
- De twee services zijn weliswaar op dezelfde VM actief, maar worden op IP-adressen uit verschillende VLANs aangeboden. Scheid beide netwerken door het éne op een native interface aan te sluiten (geen VLAN tags), en het andere via een VLAN-tag toegang te geven tot de gewenste VLAN.
- Pas de switch aan zodat de VLANs toegelaten worden (native en tagged).
- Let wel: initieel wordt de TFTP-server nog steeds gebruikt om de netwerktoestellen te configureren!
- Beperk de toegang voor TFTP tot het IP-adres, gebruikt in de Management VLAN. Beperk de toegang tot de andere service tot het IP-adres, gebruikt in de VLAN 'Interne servers'.

3.2.4 Intern IPv6

- Bereid jouw netwerk voor zodat het reeds (intern) dual stack werkt: zowel IPv4 als IPv6 werken in het eigen netwerk.
- IPv6 routing wordt enabled voor elke VLAN (behalve Management).
- Zowel DHCP als (interne) DNS worden uitgebreid met IPv6
- Verkeer tussen de eigen servers gaat bij voorkeur over IPv6 (werk dus de servers bij).

3.2.5 CA installeren en certificaten uitrollen op Windows

- Rol een Certificate Authority (CA) uit op een Windows Server. Dit kan door de bestaande Domain Controller van het domain te gebruiken of door een afzonderlijke, nieuwe, Windows server machine toe te voegen. Je gebruikt hiervoor best de Active Directory Certificate Services feature.
- Genereer een webserver certificaat om een webserver naar keuze te laten werken met HTTPS (i.p.v. HTTP/poort 80).
- Distribueer het CA-certificaat naar client toestellen via een GPO.

3.2.6 Redundante Windows server set-up

- Zorg voor een redundante Windows server set-up zodanig dat de functionaliteit van het domain gegarandeerd blijft wanneer de DC onbeschikbaar zou worden.

3.2.7 Matrix.org linux server

- Installeer Synapse. Dit is een server voor het matrix.org protocol dat in de open source community steeds meer IRC en andere chatsystemen vervangt. Je kan er makkelijk bots op programmeren en bridges installeren naar andere chatplatformen zoals Discord, Messenger, ... Daarnaast zijn chats default geëncrypteerd en onleesbaar voor admins.
- Matrix ondersteunt federatie (wat is dit?). Meestal is dit gewenst, maar hier hoef je dit niet op te zetten.
- Maak minstens 2 accounts en voer een geëncrypteerd gesprek.
- Maak een bash script op de webserver dat een bericht stuurt naar een matrix.org room als de webserver afsluit. Installeer dit script met een systemd unit en systemd timer.
- Installeer een bridge naar een extern chatplatform zoals Discord / IRC / Messenger / WhatsApp/ ... en zorg ervoor dat de Matrix.org accounts met gebruikers van dat extern platform kunnen communiceren en omgekeerd.

3.2.8 Nextcloud linux server

- Installeer Nextcloud. Dit is een self hosted Google Suite / OneDrive kloon. Het biedt een platform aan om bestanden te delen of te synchroniseren (= Google Drive), kalenders aan te maken en te delen (= Google Calendar), contacten bij te houden en te beheren (Google Contacts) en nog veel meer. Dankzij Nextcloud heb je de functionaliteit gelijkaardig aan Google Suite of OneDrive, maar blijf je baas over je eigen data.
- Maak naast een admin account ook minstens 1 user account aan. Zorg ervoor dat een Windows 10 client (of Linux client) de Nextcloud server kan bereiken via https://nextcloud.l01-thematrix.internal dankzij de reverse proxy.
- Installeer op de client de Nextcloud software voor clients en zorg ervoor dat je bestanden kan synchroniseren met de server en/of andere clients.
- Maak een kalender aan en zorg ervoor dat je deze kan importeren/synchroniseren met Thunderbird op een client.
- Installeer een plugin om forms te maken en deel een link naar form met iemand anders zodat die de form kan invullen.

3.2.9 Extra website

- Implementeer een tweede website naar keuze op de webserver. Zorg ervoor dat je naar deze website kan surfen via https://zelfgekozennaam.l01-thematrix.internal dankzij de reverse proxy. Werk je DNS-server bij zodat ook deze nieuwe URL gekend is.
- Implementeer load balancing voor deze website. Veel reverse proxies hebben hiervoor build-in support. Je zal wel de website (en eventueel databank) redundant moeten opzetten en ontdubbelen op een extra linux server.
- Host deze server op dezelfde webserver VM (zie basisopdracht). Beide webservers worden weliswaar gehost op hetzelfde IP-adres, maar worden op basis van URL gescheiden.
- Indien je met Apache werkt, kan deze scheiding door het opzetten van vhosts.
- Indien je met Nginx werkt, kan deze scheiding door het opzetten van server blocks.

3.2.10 Reverse proxy hardening

- Wat moeilijker dan het verbergen van de versie van de reverse proxy, is het verbergen van het type / gebruikte software pakket. Zoek uit hoe nmap geen of het verkeerde type reverse proxy weergeeft.

4 Organisatie

- Deze taak is **individueel** of in **groep (max. 5 studenten)**
- Als je in groep wil werken geef je ten laatste tijdens het feedbackmoment van EP2 door met wie je in de groep wil samenwerken aan dhr. Labijn (via e-mail of fysiek campus). De groep moet niet noodzakelijk dezelfde zijn als EP1, je mag die opnieuw samenstellen.
  Geef je geen (groeps)namen door, dan voer je de individuele opdracht uit!
- Je maakt een nieuwe repo aan (individueel of 1 per groep). Jouw repo uit EP2 kan als inspiratie dienen maar daar worden zelf geen nieuwe commits op uitgevoerd! Zorg ervoor dat je nieuwe repo alles bevat en "self-contained" is.
- Er wordt tijdens het zomerreces **GEEN feedback** verschaft over de opracht, inhoudelijk noch technisch. **Heb je vragen dan worden deze tijdens het feedbackmoment van EP2 gesteld of via e-mail ten laatste VOOR donderdag 27/6 om 18u00.**
- Het netwerklokaal zal geopend worden om je opstelling te testen op onderstaande momenten. Hou er wel rekening mee dat er GEEN technische ondersteuning is van onze kant uit.
  - Woensdag 21/8 08:30 - 12:00
  - Vrijdag 30/8 09:00 - 16:30
  - Woensdag 4/9 11:00 - 16:00

  Wens je tijdens één van deze momenten gebruik te maken van het lokaal, maak je hiervoor een afspraak met dhr. Van Maele.

5 Opleveringsdatum van de opdracht

Je dient op Chamilo onder Opdrachten => EP3, ten laatste op **woensdag 4/9/24 VOOR 13u00**, een link in naar je repo met de code. Deze datum is dan ook uiterste datum om commits op je repo uit te voeren.

Indien groepsopdracht: zorg dat er een document op de repo staat waarin een taakverdeling is opgenomen en dus duidelijk vermeld is wie welk stuk heeft gemaakt!

6 Evaluatie

De technische evaluatie (70%) gaat door op **donderdag 5/9/24**.
Het rooster wordt via Chamilo gepubliceerd na verstrijken deadline indienen repo.

Je score voor proces (30%) wordt mee overgenomen uit EP2. Die score kan je ENKEL tijdens het feedbackmoment verkrijgen. **Een afwezigheid op proces uit EP2 wordt dus automatisch ook een AFW in EP3 voor het volledige OLOD, ongeacht je technische score!**