Plan van Aanpak

Zie trello voor uitgebreide opdrachtverdeling

https://trello.com/b/fHIZMPoZ/p2sb2021g02

Risico analyse: Zie extra Excel bestand Risico_G02.xlsx

Opdracht 1

Opdrachtomschrijving

Als ict-dienstverlener is het nuttig om in bepaalde aspecten van ons aanbod te standaardiseren op één bepaald merk. Dat laat de medewerkers toe zich verregaand te specialiseren in de werking van die apparatuur en zo de klanten een betere dienstverlening te kunnen aanbieden. Voor netwerkapparatuur is de keuze in de context van dit project voor de hand liggend, ondanks de soms niet geringe kostprijs: Cisco.

Het is belangrijk om de apparatuur beter te leren kennen, zodat we die later doelmatig kunnen toepassen in complexere situaties. Dit gaan we doen aan de hand van enkele eenvoudige proefopstellingen met routers en switches. Voordat je hiermee van start gaat, vragen we je om eerst om de packettracer te maken die de commando's in verband met de basisconfiguratie van een switch herhaalt uit Computernetwerken 1. Deze packettracer-oefening en de labo's met betrekking tot de eenvoudige proefopstellingen kan in bijlage vinden.

- `opdracht-01-Packettracer - basisconfiguratie Switch.pka`: Basisconfiguratie Switch
- `opdracht-01-lab1.pdf`: consolesessie met een switch
- `opdracht-01-lab2.pdf`: eenvoudig netwerk met 2 switches
- `opdracht-01-lab3.pdf`: eenvoudig netwerk met router en switch
- `opdracht-01-lab4.pdf`: complexer netwerk met statische routering

Ook in netwerkbeheer raakt het automatiseren van de configuratie meer en meer ingeburgerd. Om hier ervaring mee op te doen doorlopen jullie zelfstandig de workshop Model-Driven Programmability, voeren de bijhorende labo's uite n leggen het final exam af. Nadere instructies en toegang tot het studiemateriaal volgen.

Deliverables

Tijdens de demo:

- De opstellingen van de 4 labo's in Packettracer

Op Github:

- PacketTracer-bestanden met een simulatie van de gegeven opstellingen
- Gedetailleerd verslag van realisatie van de proefopstellingen
- Cheat sheet met basiscommando's IOS
- Checklist: hoe reset je eventuele achtergebleven instellingen op een Cisco router/switch?

(Zie Trello voor uitgebreide uitleg over de deeltaak) https://trello.com/b/fHIZMPoZ/p2sb2021g02

Deeltaken

1. Switch configureren met basis instellingen
   Verantwoordelijke: Vic Rottiers
   Tester: Pieter Van Keer
   Deadline: 01/03/2021

2. Lab 1 - Console sessie met switch opzetten
   Verantwoordelijke: Vic Rottiers
   Tester: Pieter Van Keer
   Deadline:

3. Lab 2 - Een simpel netwerk opzetten
   Verantwoordelijke: Ruby Verhoye
   Tester: Maurits Monteyne
   Deadline: 01/03/2021

4. Lab 3 - Router - switch netwerk opzetten
   Verantwoordelijke: Pieter Van Keer
   Tester: Vic Rottiers
   Deadline: 01/03/2021

5. Lab 4 - Groter router - switch netwerk opzetten
   Verantwoordelijke: Maurits Monteyne
   Tester: Vic Rottiers
   Deadline: 01/03/2021

6. Checklist: Hoe verwijder je achtergebleven instellingen?
   Verantwoordelijke: Pieter Van Keer
   Tester: /
   Deadline: 01/03/2021

7. Workshop: Model-Driven Programmability
   Verantwoordelijken: Pieter Van Keer, Vic Rottiers, Ruby Verhoye, Maurits Monteyne
   Tester: /
   Deadline: 01/03/2021

8. Cheat sheet met basiscommando’s IOS
   Verantwoordelijke: Maurits Monteyne
   Tester: /
   Deadline: 01/03/2021

Opdracht 2

Opdrachtomschrijving: Linux-Webapplicatieservers

Verschillende klanten vragen ons om hun **webapplicatie** te hosten. Tot nu toe hebben we altijd manueel een server opgezet waarbij de nodige software geïnstalleerd en geconfigureerd werd. Door de groeiende vraag is dit niet houdbaar. De bedoeling is een soort "sjabloon" uit te werken zodat we veel sneller een nieuwe server kunnen opzetten die meteen geconfigureerd is om een applicatie op te draaien. Om het voor webapplicatie-ontwikkelaars eenvoudiger te maken om op hun eigen laptop een **testomgeving** op te zetten, is de eerste stap het creëren van VirtualBox VMs. Uiteindelijk is het de bedoeling om deze in de **cloud** te reproduceren.

We splitsen deze opdracht op in verschillende mijlpalen

Deliverables

M1: lokale testomgeving opzetten

Geschatte tijdsregistratie: 12u

- Vagrant-omgeving met 1 VM
- Installatie-script webserver + database
- Installatie-script webapplicatie
- Technische documentatie:
    - Hoe kan een teamlid (of de begeleider) de opstelling reproduceren zonder hulp?
    - Cheat sheet: wat zijn de belangrijkste commando's om de VM te beheren en om problemen op te lossen?
- Gebruikersdocumentatie: hoe kan een PHP-developer zonder hulp de VM configureren opstarten?
- Testplan en -rapport

Deadline (uitbouw, testing en rapport): 08/03/2021

Verantwoordelijke: Maurits Monteyne, Pieter Van Keer

Tester: Vic Rottiers, Pieter Van Keer

M2: Monitoring van de lokale testomgeving

Geschatte tijdsregistratie: 5u

- Aangepast installatiescript
- Aangepaste technische documentatie
- Testplan en -rapport van de load tests

Deadline (uitbouw, testing en rapport): 22/03/2021

Verantwoordelijke: Ruby Verhoye

Tester: Maurits Mon

M3: Productie-omgeving opzetten

Geschatte tijdsregistratie: -

- Aangepaste installatie-scripts zodat ze zowel lokaal als in de gekozen cloud-omgeving bruikbaar zijn
- Technische documentatie: hoe kan een teamlid de opstelling reproduceren?
- Gebruikersdocumentatie: hoe kan een klant een webapplicatieserver in een productie-omgeving opzetten?
- Testplan- en rapport

Deadline (uitbouw, testing en rapport): 22/03/2021

Verantwoordelijke: Pieter Van Keer

Tester:

M4: Containervirtualisatie

Geschatte tijdsregistratie: 8u

- Installatiescripts VM, containers
- Technische documentatie:
    - Hoe kan een teamlid de opstelling reproduceren?
    - Aangevuld cheat sheet: belangrijkste commando's om met Docker/Podman te werken
- Testplan en -rapport opstelling + load tests

Stappenplan:

1. Installatie Server
2. Installatie Docker
3. Installatie Cockpit
    1. Installatie Container 1 en 2

Deadline (uitbouw, testing en rapport): 22/03/2021

Verantwoordelijke: Vic Rottiers

Tester: Pieter Van Keer

Opdracht 3

Deliverables

Opdrachtomschrijving

Voor een kantoornetwerk (Windows omgeving) wens je de uitrol van software op de werkstations (clients) te automatiseren. Je wenst ook om de webserver van het bedrijf te automatiseren. Binnen een Windows omgeving kan je dit met "Microsoft Deployment Toolkit (MDT)" op een efficiënte manier uitvoeren.

Gebruik Virtualbox om deze installaties te doen. Maak geen gebruik van Vagrant. Dit gaat u redelijk veel problemen geven om dit op te zetten. Gebruik de toolkit MDT, en daar waar nodig gebruik je PowerShell om bepaalde roll-outs te doen van de server en eventueel ook de clients. Elke installatie moet gebeuren via PXE boot.

1: Installatie Windows VMs

Manuele installatie van de Windows Virtuele Machines.

Installeer volgende opstelling, alle installaties zijn met Windows Server 2019, en voor de client Windows 10. Vooraleer tot configuratie over te gaan, voer alle updates uit op de verschillende toestellen.

- 1 Domain Controller
  - naam domein is `CoronaPrj.local`
  - hostnaam: `GroepxxDC` met `xx` je groepnummer
- 1 Member Server lid van bovenstaand domein.
  - hostnaam: `GroepxxAut`
- Clientsystemen (toegevoegd aan bovenstaand domein)
  - hostnamen `GroepxxCly` met `y` een oplopend nummer

Deadline (uitbouw, testing en rapport): 26/04/2021

Verantwoordelijke: Vic Rottiers & Pieter Van Keer

Tester: Maurits Monteyne & Ruby Verhoye

2: Installatie van Rollen op Windows Server

Installeer binnen het domein volgende zaken:

- Rollen AD – DNS – DHCP (op latere DC)
- Rollen WSUS op latere Member Server
- Software: MDT op latere Member Server

Deadline (uitbouw, testing en rapport): 26/04/2021

Verantwoordelijke: Vic Rottiers & Pieter Van Keer

Tester: Maurits Monteyne & Ruby Verhoye

3: WSUS Windows Server Update Services uitbouwen

- Systeemupdates voor Clients voorzien
  - Voor clientupdates voorzie de Nederlandstalige updates en de Engelstalige update
- Systeemupdates voor Servers
  - Voor serverupdates voorzie je enkel de Engelstalige updates

Deadline (uitbouw, testing en rapport): 26/04/2021

Verantwoordelijke: nog niet verdeeld

Tester: nog niet verdeeld

4: Microsoft Deployement Toolkit leren gebruiken

We gebruiken MDT, terug te vinden op https://www.microsoft.com/en-us/download/details.aspx?id=54259 om volgende software pakketten automatisch op de clients te installeren:

Client Image:

- Windows 10
  - Clean installatie voor nieuwe toestellen
- Adobe Reader
  - Moet geïnstalleerd worden op nieuwe en bestaande toestellen, die de software nog niet hebben
  - Bij nieuwe installaties kan je het integreren in uw image van de Windows Client
- Java
  - Moet geïnstalleerd worden op nieuwe en bestaande toestellen.
  - Bij nieuwe installaties kan je het integreren in uw image van de Windows Client
- Officesuite (bv. LibreOffice)

Server Image:

We installeren een Windows Server 2019 automatisch a.d.h.v MDT. We voorzien ook verschillende tasksequences.

Zorg dat je een Windows Server 2019 automatisch kan installeren aan de hand van MDT. Voorzie in uw MDT verschillende tasksequences, dit wil zeggen dat je verschillende versies kan deployen. Hieronder enkele voorbeelden

- Tasksequence 1:
  - Windows 2019 clean install
- Tasksequence 2:
  - Windows 2019 met volgende onderdelen
    - ASP.NET
    - IIS
- Tasksequence 3:
  - Microsoft SQL Server.

Meeer info beschikbaar op deze link: https://docs.microsoft.com/nl-be/configmgr/mdt/index

Deadline (uitbouw, testing en rapport): 26/04/2021

Verantwoordelijke: nog niet verdeeld

Tester: nog niet verdeeld

Opdracht 4

Cybersecurity attack demo

Als jong team beslissen jullie om jullie ook te richten op de (groeiende) markt van **Cybersecurity**. De diensten die je wil gaan aanbienden zijn een Security Audit d.m.v. Penetration Testing. Gezien het onmogelijk is om zonder inkomsten of contract al deze activiteiten al te gaan ontplooien, beslissen jullie om slechts één demo aan de klant te laten zien om hen te overtuigen van jullie expertise - in de hoop zo een contract te kunnen binnenrijven.

Je werkt een demo uit die een bestaande, gekende aanval volledig nabootst. Je zoekt een demo die je relevant vindt, en die je ook haalbaar acht naar de kunde van je eigen team. Indruk maken mag.

Praktisch zet je dit volledig op in een virtuele omgeving, waar e.g. één VM de attacker is, en één VM de computer die je probeert binnen te dringen. Extra toestellen (routers, servers, ...) kunnen in je omgeving geplaatst worden al naar gelang je dit nodig hebt om je demo te kunnen geven. Je voorziet de nodige documentatie zodat je enerzijds de demo gemakkelijk kan geven, anderzijds de klant conceptueel begrijpt wat de demo precies doet (zonder alle praktische commando's).

Mogelijke bronnen:

- Hacking exposed 7: network security secrets & solutions
- Black Hat Python: Python Programming for Hackers and Pentesters
- The Kali Linux project
- VulnHub: "materials that allows anyone to gain practical 'hands-on' experience in digital security, computer software & network administration."
- Hack The Box: pen-testing labs
- IppSec Youtube-kanaal met walkthroughs van Hack The Box-uitdagingen
- The Cyber Mentor: Youtube-kanaal van een Ethical Hacker/Penetration tester
- Damn Vulnerable Web Application: PHP/MySQL-applicatie met beveiligingsproblemen
- Portswigger Web Security Academy: Gratis online web security training van de auteurs van de Burp suite
- Je eigen Internet research (hoewel je hier vaak door de bomen het bos niet ziet)

Deliverables

- **Werkende cybersecurity attack demo**
  We werken een demo uit waar we een cybersecurity attack simuleren, we tonen hierbij het effect dat dit heeft op het doelwit.
  Ook tonen we aan wat we van informatie kunnen te weten komen over het doelwit, en hoe er zo dagelijks duizenden gebruikers hun gegevens verliezen. **Verantwoordelijke: Maurits Monteyne**
  Tester: Niet van toepassing

- **De (virtuele) omgeving waarin alles voorbereid is**
  Dit is de omgeving waar we in gaan testen, en waar uiteindelijk ook de demo in gegeven zal worden.
  Verantwoordelijke: Pieter Van Keer & Maurits Monteyne
  Tester: Vic Rottiers

- **Technische documentatie**
  Over deze demo en de testomgeving moet er documentatie worden geschreven, zodat dit kan gereproduceerd worden door de andere teamleden. Zo kan er worden samengewerkt aan de andere deelopdrachten zoals het testen, en maken van de White Paper.
  Verantwoordelijke: Vic Rottiers
  Tester: Ruby Verhoye

- **White paper (uitleg exploit + oplossing)**
  Dit is de uitleg van hoe de demo werkt, en hoe de attack specifiek werkt.
  Verantwoordelijke: Vic Rottiers
  Tester: Maurits Monteyne
