5 Network en security – Windows

5.1 Netwerk en Windows

5.1.1 Opdrachten 'the basics'

- Geef 2 voorbeelden van een peer-to-peer netwerk en twee van een client-server netwerk
  Client-server voorbeelden: FTP, Email
  Peer to peer voorbeelden: Ubuntu, Manjaro

- Verklaar volgende begrippen
  - On-premises
    alle services die vanuit een cloud service model zouden kunnen worden geregeld, zijn eigen beheer, of on-premise
  - Azure-services
    Azure services : windows based cloud services
  - Hybride scenario's
    Hybrid clouds
  - Host (node on a TCP/IP network)
    A **network host** is a computer or other device connected to a computer network.
  - VPN
    VPN is a Virtual Private Network, IP-masking, IP address is hosted at another location, hiding your actual IP address
  - Proxy
    A proxy server acts as a gateway between you and the internet. It's an intermediary server separating end users from the websites they browse.

5.1.1.1 Extra: Verklaar volgende netwerktoestellen in eigen woorden.

  - Switch
    A switch is networking hardware that connects devices on a network by using packet switching to receive and forward data to the destination device
  - Wireless access point
    It is a wireless networking device that allows other wifi devices to connect to a wired network.
  - Router
    A router is the piece of hardware that allows communication between your home network and the internet
  - Firewall
    A security measure that monitors incoming foreign traffic and permits or blocks data based on a set of rules

- Repeaters
  Repeaters are network devices operating at physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it.

5.1.2 Opdrachten netwerkinstellingen in Windows

- Test je netwerkconnectie in de VM en zorg dat je netwerk in de VM in orde is.
- Waar zie je in Windows de netwerkkaart(en)?
  Netwerk kaarten zijn te vinden in System Information > Components > Network > Adapter
  - Controleer de status van de netwerkkaart(en).
    click Device manager. Look where it says "**Network adapters**". If there's an exclamation or question mark there, you have an ethernet problem; if not you're OK.
  - Vergelijk de netwerkkaarten van de VM met je eigen toestel.
    - Wat zijn de verschillende netwerkkaarten? vergelijk details & eigenschappen.
      De VM mist twee Netwerk kaarten: Vmware Virtual Ethernet for VmNet1 En VmNet8
  - Verander de naam van één van de verbindingen.
    Regedit **>** HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Network > ctrl + F search for adapter > double click Name > edit
    - Zie je deze naam ook terug komen in ipconfig en in devicemanager?
      Ja
- Zorg ervoor dat je netwerkkaart niet in een 'sleep modus' kan gaan.
  Device Manager > Nework Adapters > Network Card double click > Advanced tab > Sleepmode
  - Disable de netwerkkaart van de VM. Toon dit aan in network connections en device manager.
    Device manager > Select Card > Up top Disable
- Zoek uit (gebruik GUI en CLI) op je virtuele machine en/of je host machine en verklaar het begrip in je eigen woorden:

Adressering	Actuele waarde in VM	Verklaring (in eigen woorden)
Ipv4	192.168.1.10	Internet Protocol Version 4 (IPv4) is the fourth revision of the Internet Protocol and a widely used protocol in data communication over different kinds of networks.
Subnetmask	255.255.255.0	A subnet mask is a 32-bit number created by setting host bits to all 0s and setting network bits to all 1s. In this way, the subnet mask separates the IP address into the network and host addresses.
Default gateway	192.168.1.1	A default gateway is the node in a computer network using the Internet protocol suite that serves as the forwarding host (router) to other networks when no other route specification matches the destination IP address of a packet.
Link-local IPv6 address	117443625	The Dynamic Host Configuration Protocol version 6 (DHCPv6) is a network protocol for configuring Internet Protocol version 6 (IPv6) hosts with IP addresses, IP prefixes, default route, local segment MTU, and other configuration data required to operate in an IPv6 network. It is the IPv6 equivalent of the Dynamic Host Configuration Protocol for IPv4. DHCPv6 is defined by RFC 8415.
MAC address	00-0C-29-2C-61-B3	A media access control address (MAC address) is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment.
DHCP server	00-01-00-01-29-52-6B-9C-00-0C-29-2C-61-B3	Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

DNS server	192.168.1.1	The Domain Name System (DNS) is the phonebook of the Internet. When users type domain names such as 'google.com' or 'nytimes.com' into web browsers, DNS is responsible for finding the correct IP address for those sites.

- Adressen <-> talstelsels.

	IPv4	Ipv6	MAC
Gebruikt talstelsel voor de weergave	Dec	Hexadecimal	Hexadecimal
Aantal bits	32	128	32
Aantal mogelijkheden	S^32	2^128	281.5 biljoen
Waarde in de VM	192.168.1.10	117443625	00-0C-29-2C-61-B3
Binaire waarde	11000000.10101000.0001.1010	0b11100000000000000110000101001	00000000-00001100-00101001-00101100-01100001-10110011

- Verander je netwerk setting van dynamisch naar statisch. Geef een manueel een IP adres in. Bijvoorbeeld: Ip adres 10.0.0.1 – subnetmask 255.0.0.0
- Wat is het verschil tussen een dynamsiche en statische IP adressering?
  When a device is assigned a *static* IP address, the address does not change. Most devices use *dynamic* IP addresses, which are assigned by the network when they connect and change over time.
  - Kan je een getal ingeven hoger dan 255 bij een IPv4 adres? Verklaar je antwoord.
    An IPv4 address is made up of four octets -- an octet being an eight-bit value. When you have eight bits, the number of possible combinations is 2^8
  - Welk van volgende waarde kan je ingeven bij subnetmask zonder een foutmelding te krijgen over een 'invalid subnetmaks'
    In the class-based method, each of these four numbers can only have a maximum value of 255 or a minimum value of 0
  - Als je de waarden omzet naar de binaire vorm. Wat kan je dan concluderen als je de geldige subnetmaks vergelijkt met de ongeldige?
    Since the '1' bits need to be contiguous, the octets of **the subnet mask can only have the following values:** 128, 192, 224, 240, 248, 252, 254,

Waarde 255.255.255. …	Geldig?	Binaire waarde
• 255	Ja	11111111

• 254 • 250 • 200 • 128 • 192 • 100 • 10 • 5 • 0	Ja Nee Nee Ja Ja Nee Nee Nee Ja	11111110 11111010 11001000 10000000 11000000 01100100 00001010 00000101 00000000

- Test de connectie met het manueel ingegeven IP adres.
- Geef manueel de IPv4 gegeven in die je eerder hebt opgevraagd via dynamische settings en test connectivity.
- Restore de settings (terug naar dynamische adressering)

5.1.3 Netwerkconnectie en commands

- Ping naar 8.8.8.8 en Traceroute naar 8.8.8.8
    - Wat doet het commando ping?
      Stuurt en ontvangt test packages naar gegeven locatie
    - Wat doet het commando tracert?
      The TRACERT diagnostic utility determines the route to a destination by sending Internet Control Message Protocol (ICMP) echo packets to the destination.
    - Wat is het ip address 8.8.8.8
      Google
- Zoek van volgende dns namen het ip adres op. (maak gebruik van het juiste cmd).
    - bb.pxl.be
      ping bb.pxl.be
      ipv4: 193.190.154.242
    - www.pxl.be
      193.190.154.242
    - www.google.be
      2a00:1450:400e:80f::2003
    - www.google.com
      2a00:1450:400e:810::2004
- Herhaal bovenstaande via https://dnsmap.io

5.1.4 Extra: scan je thuisnetwerk

- Installeer Zenmap (GUI) of Nmap (CLI) en scan je thuisnetwerk. zie https://nmap.org/. Vind je de besproken IP adressen terug?
- Netwerkkaart in Virtualisatie
    - Bekijk, experementeer en onderzoek de opties bij de Virutalisatie software voor het gebruik van de netwerkkaart. (NAT, Bridged,…)

5.2 Beveiliging

5.2.1.1 Windows Firewall

- Open windows Firewall en verken de mogelijkheden.
- Wat is de werkwijze om een applicatie toegang te geven (zonder de firewall helemaal uit te zetten)?
  "Allow an app to or feature through FireWall"

Blokkeer FTP verkeer

- Ga naar ftp://speedtest.tele2.net/ en test een FTP download.
- Blokkeer via Windows Firewall de TCP poort gebruikt voor het FTP protocol.
- Test opnieuw de ftp download. (Probeer een ander bestand dat tijdens de eerste test.)

Blokkeer een applicatie

- Download en installeer de browser 'Vivivaldi'
- Test de applicatie.
- Zorg dat de applicatie geen toegang heeft tot het netwerk door een nieuwe rule in de firewall.

5.2.1.2 Windows defender

- Is Windows Defender voldoende als virusscanner?
- Open Windows defender en onderzoek de verschillende instellingen.
- Laat Windows Defender een snelle scan uitvoeren in je vm.
  Bespreek het resultaat.
- Zijn er bedreigingen gevonden? Hoeveel files zijn gescand.
- Virusscanner test

- Download de testfile van blackboard en importeer deze in de VM.
  - Hoe reageert de virusscanner?
  - Zorg dat de file kan geopend worden in de VM
  - Open de file en bekijk de inhoud ervan
  - Wat zou deze file kunnen zijn?

5.3 Gegevens beveiligen

5.3.1 Backup

5.3.2 Encryptie

5.3.2.1 EFS (Encyrpting file system)

- Maak een bestand encrypted.txt in een map '\EFS_Ecryptie'.
  Zet hier tekst in: dit bestand bevat secrets en wordt daarom versleuteld.

- Versleutel dit bestand met EFS.
  RM > Properties > General > Encrypt
- Exporteer de key. (-> via popup of via certmgr.msc)
  Certificates Manager > Select certificat > Export
- Verplaats naar een gedeelde schijf in VM. Verklaar! -> de encryptie wordt niet ondersteund door het bestandsyteem.
- Deel het document met een andere computer. (Stuur door via E-mail of plaats op een usb stick.) Wat gebeurt er met de EFS encryptie?
- Zip het beveiligd bestaan naar een gecomprimeerde folder. Wat gebeurt er?

5.3.2.2 Bitlocker

- Versleutel een usb-key met bitlocker en test de werking van bitlocker!
  - Versleutel een usb key op een Windows host
    - Wat is de recovery key en kan je hem opslaan?
    - Wat is het verschil tussen 'encrypt using disk space only' en 'encrypt entire drive'
    - Wat is het verschil tussen 'new encryption mode' en 'compatible mode'.
    - Zorg dat het jouw USB stick niet verwijderd gedurende het encryption proces! Anders is deze niet meer bruikbaar!
  - Probeer de data op de USB key te lezen vanuit een andere host.

5.3.2.3 Gegeven beveiligen

Ken je nog andere manieren om je gegevens te beschermen?

- Voor op een 'overdraagbaar medium zoals een USB key -> Test het uit!
- Lokaal opgeslagen bestanden
- Bestanden in een cloud omgeving

5.3.3 Hashing

<u>Berekenen van hashes in Windows</u>
Een tools om een hash te berekenen (zie bijlage in Blackboard):

- http://code.kliu.org/hashcheck/ (makkelijk om één file te bekijken)

Via powershell kan je een hash berekenen zonder extra te installeren tools. Powershell komt in latere hoofdstukken van deze cursus uitgebreid aan bod. Maar probeer na al om de hashes te berekenen m.b.v. PS.

Bijvoorbeeld voor de MD5 te berekenen van de file test.txt:

```
Get-filehash -path .\test.txt -algorithm md5
```

- Open paint, schrijf je handtekening in een blanco document en sla op als signature1.png.
  Copier dit bestand en hernoem het naar signature2.png.
  Bereken de MD5, SHA1, SHA-256 en SHA-512 en vervolledig onderstaande tabel. Wat valt er op voor de hash waarde van de 2 files?

Hash	hash file 1	Hash file 2	Aantal symbolen Hex	Aantal bit
MD5	'idem'	'idem'	32	128 bits
SHA1	--	--	40	160 bits
SHA-256	--	--	64	256 bits
SHA-512	--	--	128	512 bits

- Wanneer verandert een hash? Vergelijk de hashwaarde en verklaar.
    - Verander de inhoud van signature1.png en herbereken de hashes.
    - Verander de naam van de file en herbereken de MD5.
    - Verander de metadata (genomen op) en herbereken de MD5.
    - Open de file met een andere applicatie, verander niets en sla de file op.
    - Plaats de file in een zip en vergelijk de hash van de zip.
    - Zie je een patroon in de hash en de gemaakte verandering? → nee, het algoritme van een hash functie hoort zo te zijn dat je de hash niet kan voorspellen op basis van wijzigingen gemaakt in een file (of wachtwoord).

    → Wat kan je concluderen uit deze oefening? Wanneer verandert een hash van waarde?
- Vervolledig de tabel met een kolom aantal mogelijke hashes. (te bepaken aan de hand van de lengte in bit.)
- Tijdens de praktische examens op PXL-Digital wordt er gevraagd om een hash te bereken van je oplossing. Deze hash wordt genoteerd op het examencopy.
    - Kan je aan de hand van bovenstaande test achterhalen waarom dit belangrijk is?

5.3.3.1 Paswoorden

- Wat hebben paswoorden te maken met hashing?
- https://www.youtube.com/watch?v=phLcILslhbQ
  Paswoorden zijn niet van deze tijd… Wat is het alternatief?
- Wat is MFA en hoeveel manier kan je gebruiken als autenticatie?
    - Geef van elke een voorbeeld.

5.3.3.2 Extra opdracht: password manager

- Wat is een password manager
- Installeer een paswoord manager op de VM en verken de werking.
- Onderzoek wat voor jouw situatie de meest geschikte password manager is.