Labo 5: Protecting Devices and Networks

Inhoudsopgave

Inhoudsopgave

TIJDSBESTEDING

	Aleyna	Rasmus	Stef	Tomas	TOTAAL
1.1 Vakjargon	1 uur				1 uur
1.2 Basic Commands				1 uur	1 uur
2.1 PT – Router and Switch Configuration			3 uur		3 uur
2.2 PT - VLAN	3 uur				3 uur
2.3 PT – Security in a Network		4.5 uur			4.5 uur
3.1 THM – Active Reconnaisance				45 min	45 min
2.1 TLS-handshake in Wireshark	40 minuten				40 min
Layout + Eindcontrole	3 uur				3 uur
Totaal	7 uur 40 min	4.5 uur	3 uur	1 u 45 m	

1 Vakjargon

1.1 Vakjargon

ip=Connectionless: verwijst naar de communicatie tussen twee netwerkeindpunten zonder een voorafgaande afspraak waarbij het ene netwerkeindpunt een bericht naar het andere stuurt.

ip=Best effort: de benadering van servicekwaliteit waarbij het netwerk zelf niet actief differentieert in de behandeling van services die door het netwerk worden verzonden.

Address Spoofing Attacks: het vervalsen van de inhoud in de source IP-header. Meestal met willekeurige getallen, om de identiteit van de afzender te maskeren.

Echo Packets: een speciaal type netwerkpakket dat een icmp-pakket wordt genoemd.

ICMP: Internet Control Message Protocol, een protocol dat apparaten binnen een netwerk gebruiken om problemen met gegevensoverdracht te communiceren.

ACL: Access Control List, bevat regels die toegang verlenen tot bepaalde digitale omgevingen.

ARP: Address Resolution Protocol, een protocol of procedure die een steeds veranderend IP-adres verbindt met een vast fysiek mac-adres.

Gratuitous ARP: is een ARP-response die niet werd gevraagd door een ARP request.

AMP: Advanced Malware Protection, maakt gebruik van meerlagige benadering die AI en machine learning en gedragsdetectie omvat.

NGFW: Next Generation Firewall, oftewel een deep-packet inspectie-firewall die verder gaat dan poort-/protocolinspectie en blokkering om inspectie op applicatieniveau, inbraakpreventie van buiten de firewall toe te voegen.

WSA: Web Security Appliances, een vorm van serverapparaten dat is ontworpen om computer-netwerken te beschermen tegen ongewenst verkeer.

Honeypot: een cybersecurity mechanisme dat gebruik maakt van een gefabriceerd aanvalsdoel om cybercriminelen weg te lokken van legitieme doelen.

DNS: Domain Name System zet domeinnamen om in IP-adressen, die browsers gebruiken om internetpagina's te laden.

DHCP: Domain Host Configuration Protocol, is een netwerkserver die automatisch IP-adressen, standaardgateways en andere netwerkparameters levert en toewijst aan clientapparaten.

Amplification & Reflection: een techniek waarmee aanvallers zowel de hoeveelheid kwaadaardig verkeer die ze kunnen genereren, kunnen vergroten als de bronnen van het aanvalsverkeer kunnen verdoezelen.

TCP Syn Flood Attack: vindt plaats wanneer de aanvaller het systeem overspoelt met SYN-pakketten om het doelwit te overweldigen en het net in staat te stellen te reageren op nieuwe echte verbindingsverzoeken.

ARP Poisoning: is een type cyberaanval die wordt uitgevoerd via een LAN waarbij kwaad-aardige ARP-pakketten worden verzonden om de koppelingen in het IP naar het MAC-adres te wijzigen.

DHCP Starvation Attack: een aanval die zich richt op DHCP-servers waarbij valse dhcp-verzoeken worden gemaakt door een aanvaller met de bedoeling alle beschikbare ipadressen die door de dhcp-server kunnen worden toegewezen, uit te putten.

DHCP Spoofing Attack: treedt op wanneer een aanvaller probeert te reageren op dhcp verzoeken en zichzelf probeert op te sommen als de standaard gateway of dns-server.

DNS Tunneling: een methode voor cyberaanvallen die de gegevens van andere programma's of protocollen codeert in DNS-query's en reacties.

UDP Flood Attack: een vorm van volumetrische DoS aanval waarbij de aanvaller willekeurige poorten op de host aanvalt en overweldigt met ip-pakketten die udp-pakketten bevatten.

SNMP: Simple Network Management Protocol, een netwerkprotocol dat wordt gebruikt voor het beheer en de bewaking van op het netwerk aangesloten apparaten in IP-netwerken.

NTP: Network Time Protocol, is een internet protocol dat wordt gebruikt om te synchroniseren met computerkloktijdbronnen in een netwerk.

1.2 Basic Commands

- **Traceroute**: met dit commando kunnen we gaan kijken welk route of pad onze pakketjes gaan nemen naar een bepaalde host, hoeveel tussenstappen deze eigenlijk ondergaat. Hierbij hebben we een bepaalde parameter genaamd de "time to live" dit is het maximumaantal tussenstappen ons pakketje gaat nemen. Dus bij elke tussenstap gaat dit met 1 omlaag, dus bij een ttl van 64 gaat deze maximum 64 tussenstappen nemen. Een voorbeeld hiervan kan zijn **"`tracert 8.8.8.8`"** in onze terminal.

- **Ipconfig:** met het commando ipconfig kunnen we gaan kijken welke informatie we hebben over de verschillende netwerk interfaces. Gelijk onze wifi-adapter of onze ethernet adapter. We kunnen in nog meer detail gaan door verschillende flags te gebruiken bij ons commando. Zoals **"`ipconfig /all`"** met deze combinatie van commando en flag krijgen we alle informatie in detail van elke interface, inclusief de IPv6 of dergelijke.

- **Netstat:** met netstat kunnen we gaan kijken naar bepaalde connecties in ons netwerk, en troubleshooten waar het nodig is. Met andere woorden gaan we ons netwerk monitoren, hier zijn verschillende flags bij die het ons het leven een beetje gemakkelijker maken, bijvoorbeeld bij **"`netstat -n`"** krijgen we als resultaat, de verschillende IP-adressen waarmee we een actieve verbinding hebben, maar in plaats van de naam krijgen we het IP met de poort te zien.

- **Ping:** het ping commando is 1 van de meest voorkomende en meestgebruikte commando's die ik al heb gezien, met het ping commando gaan we eigenlijk zien of er wel connectie mogelijk is met het IP-adres, doormiddel van een ICMP-pakketje, als deze verstuurd wordt, gaat deze een antwoord teruggeven met als antwoord gelukt, en anders als hij geen antwoord krijgt is het mislukt. We kunnen oneindig veel keer pingen naar een IP-adres. En doormiddel van bijvoorbeeld het commando **"`ping 8.8.8.8`"** krijgen we in windows standaard 4 responses.

- **Pathping:** dit commando heeft als doel om bepaalde latencies en losses op een bepaalde connectie te bekijken en te achterhalen. Deze stuurt verschillende echo requests naar de routers. Je kan dit vergelijken als een uitgebreide Traceroute, met de loss en veel meer informatie. Hier zijn terug verschillende flags die we kunnen gebruiken. Met de flag -n gaan we bijvoorbeeld ervoor zorgen dat onze requests niet gaan proberen om een naam te achterhalen bij een IP-adres. Dus het commando zou er als volgt uitzien: **"`pathping -n 8.8.8.8`"**

- **Nslookup:** Dit is 1 van de meer gecompliceerde commandos uit onze lijst. NSlookup heeft te maken met de DNS van bepaalde ip adressen en om deze bijvoorbeeld te achterhalen. Deze commando heeft zelfs 2 verschillende modes, interactive en non interactive. Voor 1 stuk data raden ze aan om noninteractive te gebruiken, en voor meerder stukken data gaan we interactive gebruiken. Deze heeft verschillende flags die erbij komen kijken, zoals om deze in noninteractive te zetten moeten we eerst "-" voor de eerste parameter typen. Een voorbeeld van deze commando is **"`nslookup 8.8.8.8`"**

- **Netsh:** dit is een zeer merkwaardig commando. Met dit commando kunnen we in onze terminal, de netwerk configuratie van een computer veranderen, met als enige voorwaarde dat deze aanstaat. Dit commando kan gebruikt worden in de gewone terminal, of in PowerShell, aangezien dit een soort shell script is. Deze heeft dan terug flags om het commando uit te breiden. Bijvoorbeeld "-r" gaat aangeven welke computer we willen configureren.

- **Route:** met deze commando kunnen we de routing tabellen gaan manipuleren. Doormiddel van dit commando in combinatie met verschillende flags gaan we tabellen leegmaken, aanvullen of dergelijke. Een voorbeeld van een flag is bijvoorbeeld **"-f"** gaat alle tabellen leegmaken van de gateway entries.

2 Packet Tracer Oefeningen

2.1 PT - oefening 1 - Router and Switch Configuration

1. Configure SSH and Passwords

Step 1: Configure Basic Security on the Router

- Configure IP addressing on PCA according to the Addressing Table.

  Voor het IP-adres van PCA in te stellen dubbelklik je op de pc, bovenaan het menu op desktop en dan IP Configuration. Hier kunnen we het IP-adres ingeven.

- Console into RTA from the Terminal on PCA.

  Via de terminal van de pc kunnen we naar de routerconsole gaan.

- Configure the hostname as RTA.

  Om de hostname aan te passen geven we het volgende in: **`enable, configure terminal, hostname RTA`**

- Configure IP addressing on RTA and enable the interface.

  Voor het IP-adres in te stellen van de router doen we terug **`enable`** en **`configure terminal`**. Hierna geven we het volgende in: **`interface vlan1, ip address 172.16.1.1 255.255.255.0, no shutdown`**.

- Encrypt all plaintext passwords

  Om de paswoorden te encrypteren geven we het commando **`service password-encryption`** in.

- Set the minimum password length to 10.

  De minimale passwordlength kunnen we instellen met **`security passwordt min-length 10`**.

- Set a strong secret password of your choosing. Note: Choose a password that you will remember, or you will need to reset the activity if you are locked out of the device.

  Om het paswoord in te stellen geven we het volgende in: **`line console 0, password ***, login, end`**.

- Disable DNS lookup.

  Bij disable DNS lookup geven we **`no ip domain lookup`** in.

- Set the domain name to CCNA.com (case-sensitive for scoring in PT).

  Om de domain name aan te passen gebruiken we het commando **`ip domain-name CCNA.com`**.

- Create a user of your choosing with a strong encrypted password.

  Om een user aan te maken gebruik ik het commando dat is aangegeven in de opgave: **`username any_user secret any_password`**.

- Generate 1024-bit RSA keys.

  Het instellen van de RSA key staat ook in de opgave, **`crypto key generate rsa`**, hierna wordt gevraagd hoeveel bits de key moet zijn, hier typen we **`1024`**.

- Block anyone for three minutes who fails to log in after four attempts within a two-minute period.

  Om iemand te blokkeren na 4 pogingen inloggen in 2 minuten geven we dit in: **`login block-for 180 attempts 4 within 120`**.

- Configure all VTY lines for SSH access and use the local user profiles for authentication.

  Voor het volgende staan de commando's ook in de opgave: **`line vty 0 4, transport input ssh, login local`**.

- Set the EXEC mode timeout to 6 minutes on the VTY lines.

  Voor te timeout in te stellen op 6 minuten geven we **`exec-timeout 6`** in.

- Save the configuration to NVRAM.

  Om de configuratie op te slaan naar NVRAM geven we het volgende in: **`show running-config`** en **`reload`** om de configuratie te herladen.

- Access the command prompt on the desktop of PCA to establish an SSH connection to RTA.

  Als laatste gaan we naar de command prompt. Hier geven we **`ssh /?`** in om de verbinding te maken met de router RTA.

Step 2: Configure Basic Security on the Switch

- Click on SW1 and select the CLI tab.

  Selecteer het CLI-tabblad

- Configure the hostname as SW1.

  Als eerste configureren we de hostname, dit is hetzelfde als bij de router: **`enable, configure terminal, hostname SW1`**.

- Configure IP addressing on SW1 VLAN1 and enable the interface.

  Het ip adres instellen doen we ook zoals de router. **`Interface vlan 1, ip 172.16.1.2 255.255.255.0, no shutdown`**.

- Configure the default gateway address.

  De default gateway kunnen we configureren met het commando **`ip default gateway 172.16.1.1`**.

- Disable all unused switch ports.

  Om de ongebruikte poorten uit te schakelen gebruiken we terug de commando's die in de opgave staan: **`interface range F0/2-24, G0/2`** en **`shutdown`**.

- Encrypt all plaintext passwords.

  De plaintext passwords encrypteren gaat opnieuw met **`service password-encryption`**.

- Set a strong secret password of your choosing.

  Om het paswoord in te stellen geven we het volgende in: **`line console 0, password ***, login, end`**.

- Disable DNS lookup.

  Bij disable DNS lookup geven we **`no ip domain lookup`** in.

- Set the domain name to CCNA.com (case-sensitive for scoring in PT).

  Om de domain name aan te passen gebruiken we het commando **`ip domain-name CCNA.com`**.

- Create a user of your choosing with a strong encrypted password.

  Om een user aan te maken gebruik ik het commando dat is aangegeven in de opgave: **`username any_user secret any_password`**.

- Generate 1024-bit RSA keys.

  Het instellen van de RSA key staat ook in de opgave, **`crypto key generate rsa`**, hierna wordt gevraagd hoeveel bits de key moet zijn, hier typen we **`1024`**.

- Configure all VTY lines for SSH access and use the local user profiles for authentication.

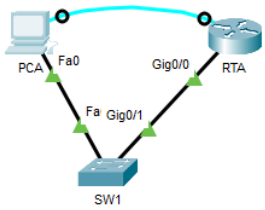
  Voor het volgende staan de commando's ook in de opgave: **`line vty 0 4, transport input ssh, login local`**.

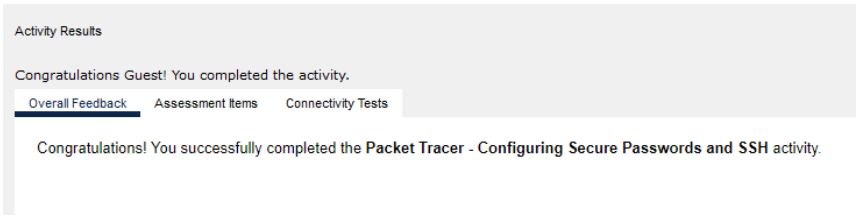
- Set the EXEC mode timeout to 6 minutes on all VTY lines.

  Voor te timeout in te stellen op 6 minuten geven we **`exec-timeout 6`** in.

- Save the configuration to NVRAM.

  Om de configuratie op te slaan naar NVRAM geven we het volgende in: **`show running-config`** en **`reload`** om de configuratie te herladen.





2. Secure Network Devices

Step 1: Document the Network

Device	Interface	Address	Mask	Gateway
RTR-A	G0/0/0	192.168.1.1	255.255.255.0	N/A
	G0/0/1	192.168.2.1	255.255.255.0	N/A
SW-1	SVI	192.168.1.254	255.255.255.0	192.168.1.1
PC	NIC	192.168.1.2	255.255.255.0	192.168.1.1
Laptop	NIC	192.168.1.10	255.255.255.0	192.168.1.1
Remote PC	NIC	192.168.2.10	255.255.255.0	192.168.1.1

Step 2: Router configuration requirements:

- Prevent IOS from attempting to resolve mistyped commands to domain names.

```
No ip domain-lookup
```

- Hostnames that match the values in the addressing table.

```
Hostname RTR-A
```

- Require that newly created passwords be at least 10 characters in length.

```
Security passwords min-length 10
```

- A strong ten-character password for the console line. Use @Cons1234!

```
Enable secret @Cons1234!
```

- Ensure that console and VTY sessions close after 7 minutes exactly.

```
Line con 0
exec-timeout 7 0
```

- A strong, encrypted ten-character password for the privileged EXEC mode. For this activity, it is permissible to use the same password as the console line.

```
password @Cons1234!
Login
```

- A MOTD banner that warns about unauthorized access to the devices.

```
Banner motd ^C
Unauthorized access prohibited. ^C
```

- Password encryption for all passwords.

  ```
  Service password-encryption
  ```

- A username of NETadmin with encrypted password LogAdmin!9.

  ```
  Username NETadmin password LogAdmin!9
  ```

- Enable SSH.
- Use security.com as the domain name.

  ```
  ip domain-name security.com
  ```

- Use a modulus of 1024.

  ```
  Crypto key generate rsa, 1024
  ```

- The VTY lines should use SSH for incoming connections.

  ```
  Transport input ssh
  ```

- The VTY lines should use the username and password that were configured to authenticate logins.

  ```
  Login local
  ```

- Impede brute force login attempts by using a command that blocks login attempts for 45 seconds if someone fails three attempts within 100 seconds.

  ```
  Login block-for 45 attempts 3 within 100
  ```

Step 3: Switch configuration requirements:

- All unused switch ports are administratively down.

  ```
  interface range fastEthernet0/1, fastEthernet0/3 – 24, GigabitEthernet0/2
  shutdown
  ```

- The SW-1 default management interface should accept connections over the network. Use the information shown in the addressing table. The switch should be reachable from remote networks.

  ```
  ip default-gateway 192.168.1.1
  ```

- Use @Cons1234! as the password for the privileged EXEC mode.

  ```
  enable secret @Cons1234!
  ```

- Configure SSH as was done for the router.

```
line vty 0 4
login local
transport input ssh
```

- Create a username of NETadmin with encrypted secret password LogAdmin!9

```
Username NETadmin password LogAdmin!9
```

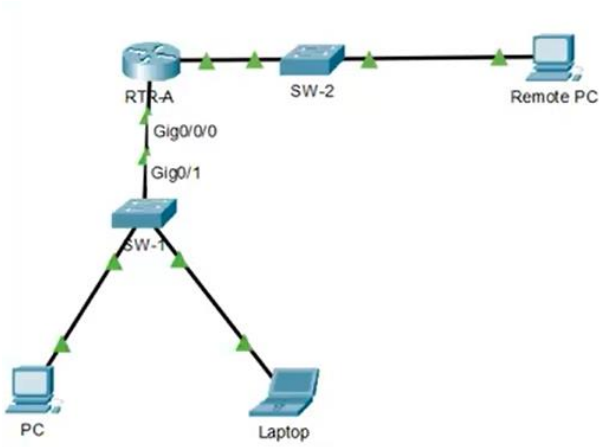
- The VTY lines should only accept connections over SSH.

```
line vty 0 4
transport input ssh
```

- The VTY lines should only allow the network administrator account to access the switch management interface.

```
line vty 0 4
login local
```

- Hosts on both LANs should be able to ping the switch management interface.



Packet Tracer - Secure Network Devices

Addressing Table

Device	Interface	Address	Mask	Gateway
RTR-A	G0/0/0	192.168.1.1	255.255.255.0	N/A
	G0/0/1	192.168.2.1	255.255.255.0	N/A
SW-1	SVI	192.168.1.254	255.255.255.0	
PC	NIC	192.168.1.2	255.255.255.0	
Laptop	NIC	192.168.1.10	255.255.255.0	
Remote PC	NIC	192.168.2.10	255.255.255.0	

Requirements

Note: To keep this activity brief and easy to manage, some security configuration settings have not been made. In other cases, security best practices have not been followed.

In this activity you will configure a router and a switch based on a list of requirements.

Instructions

Step 1: Document the Network

Complete the addressing table with the missing information.

Step 2: Router configuration requirements:

- Prevent IOS from attempting to resolve mistyped commands to domain names.
- Hostnames that match the values in the addressing table.
- Require that newly created passwords be at least 10 characters in length.
- A strong ten-character password for the console line. Use **@Cons1234!**
- Ensure that console and VTY sessions close after 7 minutes exactly.
- A strong, encrypted ten-character password for the privileged EXEC mode. For this activity, it is permissible to use the same password as the console line.
- A MOTD banner that warns about unauthorized access to the devices.
- Password encryption for all passwords.
- A user name of **NETadmin** with encrypted password **LogAdmin!9**.

Time Elapsed: 00:56:43 Completion: 100%

Dock | Check Results | Back | 1/1 | Next

2.2 PT - oefening 2 - VLAN

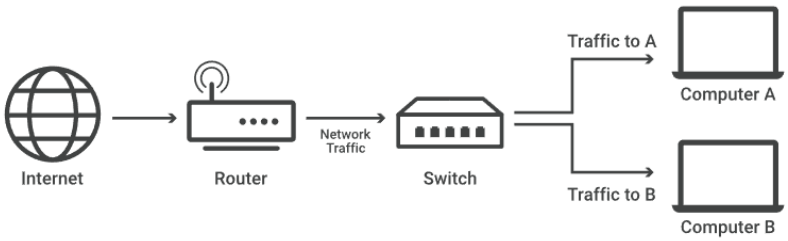
Step 1: voorbereiding

1. Wat is het netwerkadres en broadcast van:

   a. Netwerk lectoren (NoVLAN): netw = **10.10.10.128/25**; brcst = **10.10.10.255**
   b. Netwerk studenten (NoVLAN): netw = **10.10.10.0/25**; brcst = **10.10.10.127**
   c. Netwerk lectoren (VLAN): netw = **10.10.1.128/25**; brcst = **10.10.1.255**
   d. Netwerk studenten (VLAN): netw = **10.10.1.0/25**; brcst = **10.10.1.127**

2. Omschrijf in eigen woorden zonder rekening te houden met een VLAN wat de switch doet in het netwerk.

Een netwerkswitch verbindt apparaten in een netwerk met elkaar en laat ze communiceren door datapakketten uit te wisselen.



3. Genereer traffic over de verschillende netwerken (gebruik ping) en bekijk de mac-adress-table van de swichtes. Wat zijn de verschillen tussen in de mac-adres-table van SW-VLAN en SW-NOVLAN?

SW-NOVLAN

```
C:\>ping 10.10.10.5

Pinging 10.10.10.5 with 32 bytes of data:

Request timed out.
Reply from 10.10.10.5: bytes=32 time=7ms TTL=127
Reply from 10.10.10.5: bytes=32 time<1ms TTL=127
Reply from 10.10.10.5: bytes=32 time<1ms TTL=127

Ping statistics for 10.10.10.5:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 7ms, Average = 2ms
```

I. Genereer traffiek door een ping-request te versturen vanuit PC_LECTOR1 naar het IP-adres (10.10.10.5) van PC_STUD4.

II. Open de CLI van SW-NOVLAN en voer volgende commando's uit:

   a. **enable**
   b. **show mac address-table**

```
Switch(config)#do show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0003.e4c0.d677    DYNAMIC     Fa0/5
   1    0050.0f89.d801    DYNAMIC     Gig0/1
   1    0050.0f89.d802    DYNAMIC     Gig0/2
   1    00d0.bc10.6ad9    DYNAMIC     Fa0/12
```

Uit deze screenshot kunnen we afleiden dat er enkel VLAN 1 aanwezig is in het netwerk, dat wil dus zeggen dat het in geen geval afgesloten kan worden en dat het ook het verkeer controleert.

SW-VLAN

```
C:\>ping 10.10.1.3

Pinging 10.10.1.3 with 32 bytes of data:

Request timed out.
Reply from 10.10.1.3: bytes=32 time<1ms TTL=127
Reply from 10.10.1.3: bytes=32 time<1ms TTL=127
Reply from 10.10.1.3: bytes=32 time<1ms TTL=127

Ping statistics for 10.10.1.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

I. Genereer traffiek door een ping-request te versturen vanuit LECTOR1 naar het IP-adres (10.10.1.3) van STUD2.

II. Open de CLI van SW-VLAN en voer volgende commando's uit:

   a. **enable**
   b. **show mac address-table**

```
Switch#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

  10    0001.976a.25c5    DYNAMIC     Fa0/2
  10    0002.1608.4801    DYNAMIC     Gig0/1
  20    0001.96d8.a4a1    DYNAMIC     Fa0/11
  20    0002.1608.4801    DYNAMIC     Gig0/1
```

In dit scenario gebruikt het netwerk VLAN 10 en 20. Terwijl VLAN 10 is toegekend aan het studenten netwerk, is VLAN 20 toegekend aan het lectoren netwerk. De poorten in deze VLAN bevinden zich in één broadcast-domein.

Step 2: netwerken zonder VLAN

1. Ping naar het broadcast adres van 10.10.10.0/24. Welke IP-adressen zie je in de reacties?

   Het is een /24 netwerk, dus er zijn 254 bruikbare IP-adressen. Het broadcast adres is altijd het laatste niet bruikbare IP-adres binnen een subnet.

   De gevonden IP-adressen zijn:

```
C:\>ping 10.10.10.255

Pinging 10.10.10.255 with 32 bytes of data:

Reply from 10.10.10.136: bytes=32 time<1ms TTL=128
Reply from 10.10.10.129: bytes=32 time<1ms TTL=255
Reply from 10.10.10.129: bytes=32 time<1ms TTL=255
Reply from 10.10.10.7: bytes=32 time=1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.5: bytes=32 time=1ms TTL=127
Reply from 10.10.10.4: bytes=32 time<1ms TTL=127
Reply from 10.10.10.3: bytes=32 time=1ms TTL=127

Ping statistics for 10.10.10.255:
    Packets: Sent = 1, Received = 8, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

- **10.10.10.136**
- **10.10.10.129**
- **10.10.10.7**
- **10.10.10.2**
- **10.10.10.5**
- **10.10.10.4**
- **10.10.10.3**

2. Broadcastdomain:

   a. Voer het commando arp -d uit op één van de studenten toestellen.

```
C:\>arp -d
```

   b. Plaats PT in simulation mode.

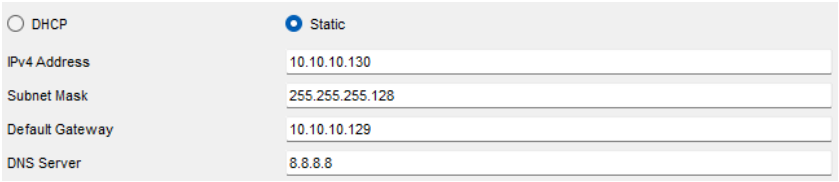
   c. Ping van dit toestel naar een andere student in simulation mode.

```
C:\>ping 10.10.10.7

Pinging 10.10.10.7 with 32 bytes of data:

Reply from 10.10.10.7: bytes=32 time=16ms TTL=127
Reply from 10.10.10.7: bytes=32 time=8ms TTL=127
Reply from 10.10.10.7: bytes=32 time=8ms TTL=127
```

   d. Welke toestellen ontvangen de broadcast?

   De ping is vertrokken vanuit PC_STUD1 naar Switch0 en dan naar Router1. De router stuurt het pakket terug door naar Switch0 en naar PC_STUD2. En zo gaat de reply in omgekeerde richting terug naar PC_STUD1.

3. Geef PC_STUD1 via manuele IP-settings de settings voor een toestel uit het lectoren netwerk. Is PC_STUD1 een volwaardige deelnemer van het subnet? Is er netwerkconnectie mogelijk?



Via volgende settings op PC_STUD1, heb ik een een ping verzoek gestuurd naar het IP-adres van PC_STUD2.

Daaruit blijkt dat PC_STUD1 nog altijd een volwaardige deelnemer is van het subnet aangezien het ping-request succesvol replies vertoond. Dit komt doordat het netwerk is opgedeeld in 2 subnetten maar nog altijd in hetzelfde fysieke netwerk zit.

```
C:\>ping 10.10.10.7

Pinging 10.10.10.7 with 32 bytes of data:

Reply from 10.10.10.7: bytes=32 time=1ms TTL=127
Reply from 10.10.10.7: bytes=32 time<1ms TTL=127
Reply from 10.10.10.7: bytes=32 time<1ms TTL=127

Ping statistics for 10.10.10.7:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Step 3: netwerk met VLAN

1. Ping naar het broadcast adres van 10.10.10.0/24. Welke IP-adressen zie je in de reacties?

```
C:\>ping 10.10.10.255

Pinging 10.10.10.255 with 32 bytes of data:

Reply from 172.16.0.1: bytes=32 time=14ms TTL=254
Reply from 172.16.0.1: bytes=32 time=1ms TTL=254
Reply from 172.16.0.1: bytes=32 time=15ms TTL=254
Reply from 172.16.0.1: bytes=32 time=10ms TTL=254

Ping statistics for 10.10.10.255:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 15ms, Average = 10ms
```

Omdat er hier weer sprake is van een /24, zijn er in totaal 254 bruikbare IP-adressen en is het broadcast adres waar we naar moeten pingen **10.10.10.255**. We zien maar één IP-adres in de reacties en dat is **172.16.0.1.**

2. Broadcastdomain: ☑

a. Voer het commando arp -d uit op één van de studenten toestellen. ☑

b. Plaats PT in simulation mode. ☑

c. Ping van dit toestel naar een andere student in simulation mode.

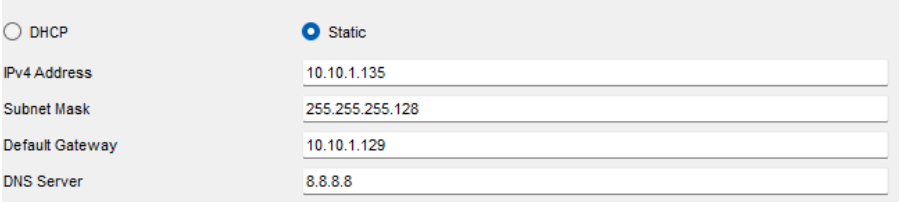
```
C:\>ping 10.10.1.3

Pinging 10.10.1.3 with 32 bytes of data:

Reply from 10.10.1.3: bytes=32 time=8ms TTL=128
Reply from 10.10.1.3: bytes=32 time=4ms TTL=128
Reply from 10.10.1.3: bytes=32 time=4ms TTL=128
Reply from 10.10.1.3: bytes=32 time=4ms TTL=128

Ping statistics for 10.10.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 8ms, Average = 5ms
```

d. Welke toestellen ontvangen de broadcast?

De ping is vertrokken vanuit STUD1 naar Switch1 en dan naar Router0 en STUD2. Vervolgens stuurt STUD2 het pakket terug naar Switch1 en verstuurd Switch1 het pakket verder door naar STUD1.

3. Geef PC_STUD1 via manuele IP-settings de settings voor een toestel uit het lectoren netwerk. Is PC_STUD1 een volwaardige deelnemer van het subnet? Is er netwerkconnectie mogelijk?

Met volgende settings is STUD1 geen volwaardige deelnemer van het netwerk, gezien er niet gepingt kan worden naar andere devices.



Step 4: VLAN!

1. Voer het commando "show VLAN" uit op de twee switchen. Wat is het verschil tussen de switchen?

SW-NOVLAN

```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
```

Wanneer dit commando wordt uitgevoerd op SW-NOVLAN, merk je dat er een default VLAN is en dat is VLAN 1 met volgende poorten: Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gig0/1 en Gig0/2.

SW-VLAN

Op deze switch hebben we VLAN 10 voor studenten en VLAN 20 voor de lectoren. Dat wil dus zeggen dat het netwerk is verdeeld in 2 subnetwerken. Waarvan 1 bedoeld is voor enkel de studenten, dus daarom ook beperkte privileges heeft, en het tweede bedoeld is voor de lectoren.

```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
10   studenten                        active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9
20   lectoren                         active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19
666  Blackhole                        active    Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
666  enet  100666     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
```

2. Welke poorten zijn op SW_VLAN bestemd voor de studenten, welke voor de lectoren?

Lectoren: Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gig0/1 en Gig0/2

Studenten: Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9

Concludeer op basis van de oefening wat een VLAN betekent voor security? M.a.w. wat is het verschil tussen de netwerken 'VLAN' en 'NOVLAN'?

VLAN's hebben het voordeel dat ze het netwerkverkeer en botsingen kunnen verminderen. Wanneer apparaten opgedeeld zijn in meerdere VLAN's, vaak per afdeling, is het gemakkelijker om te voorkomen dat een geïnfecteerde computer het gehele netwerk infecteert.

2.3 PT - oefening 3 – Security in a Network

2 Enumeration

1. Wat is het IP-adres 10.10.10.31?

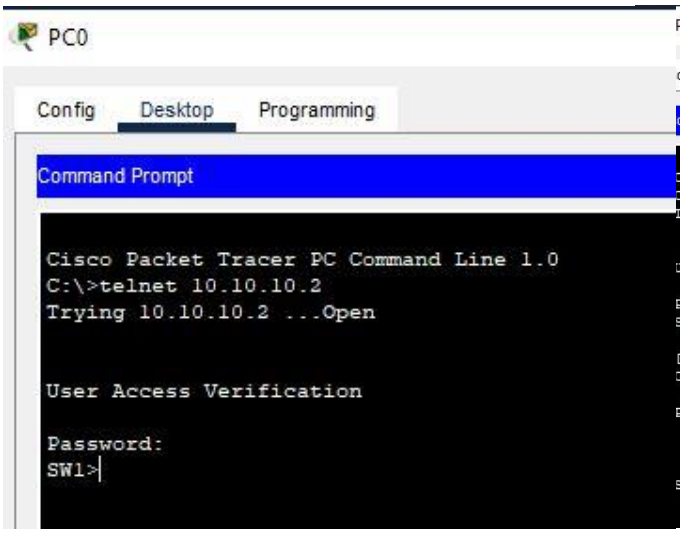
   Het IP-adres 10.10.10.31 is het laatste adres binnen het netwerk met de (SM) subnetmask /27. Door de SM van /27 zijn er 30 mogelijk geldige hosts, die de IP-adressen van 10.10.10.2 tot 10.10.10.30 zouden kunnen hebben (als er verder geen interfaces waren). 10.10.10.1 is het netwerkadres van dit netwerk, en 10.10.10.31 is het broadcast adres.

2. Bespreek het resultaat en maak een link naar Nmap

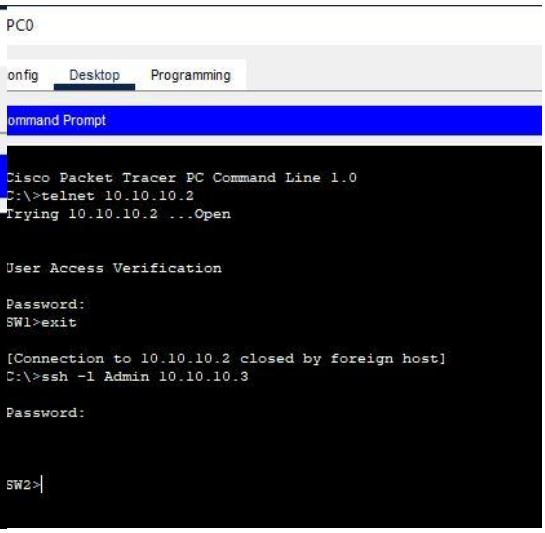
   Een van de basis-functionaliteiten van Nmap is network mapping, waarbij door een simpele scan het aantal aangesloten hosts van een netwerk zichtbaar wordt. Als een netwerk 'pings' van buitenaf zou toelaten, dan zou het mogelijk moeten zijn om dezelfde basale taak uit te voeren door een ping naar het broadcast adres te sturen vanuit een ander netwerk (bijvoorbeeld netwerk B).

3.3 Vragen: remote config

1. Wat is het verschil tussen de Telnet en SSH-connectie vanuit PC0?



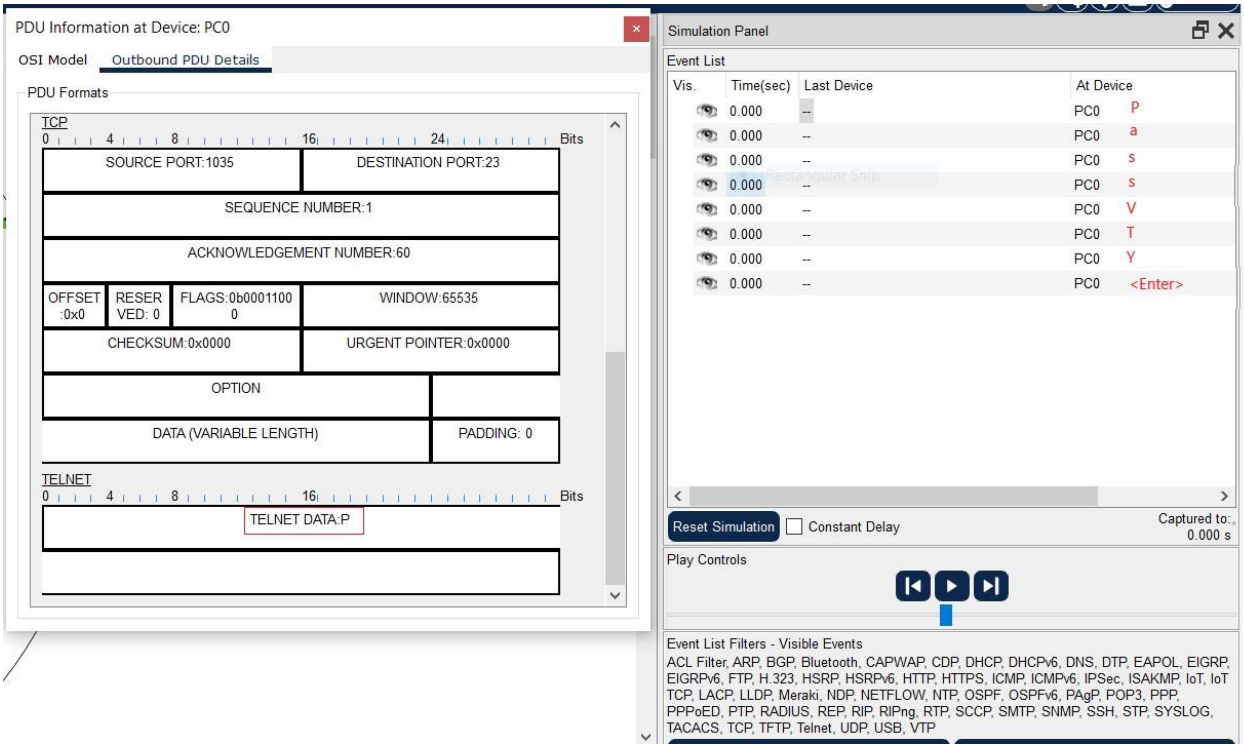
Screenshot 1: Telnet



Screenshot 2: SSH

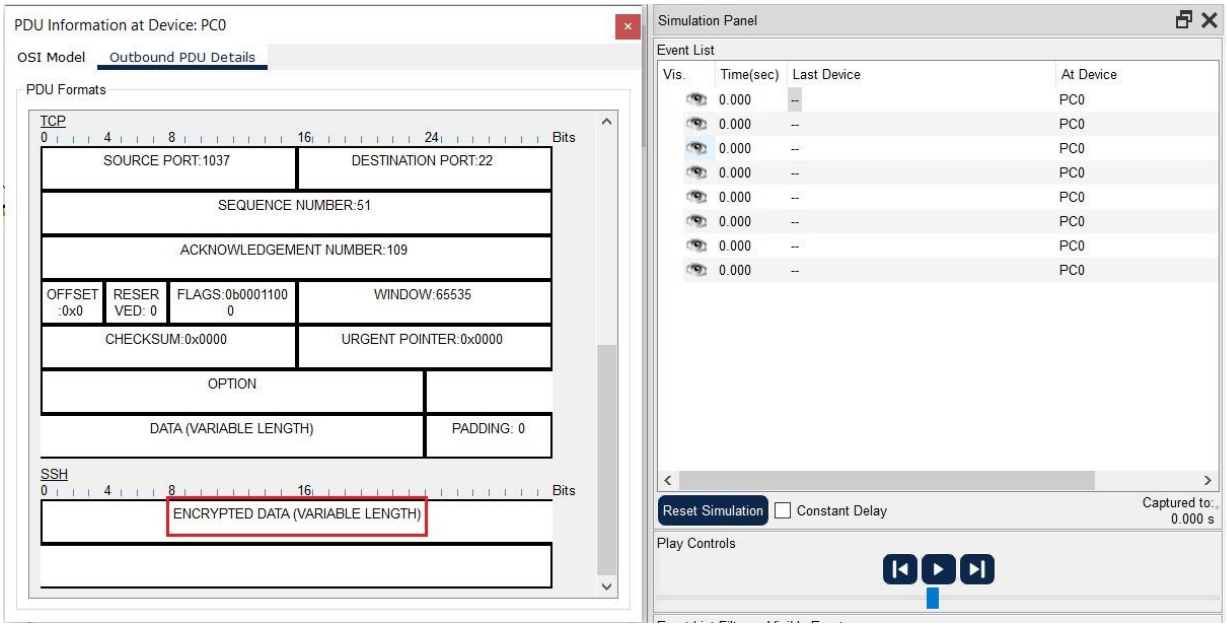
Het belangrijkste verschil tussen Telnet en SSH is versleuteling. Data die over Telnet verstuurd wordt is niet versleuteld, terwijl dat wel het geval is bij SSH. De data die met Telnet verstuurd wordt is dus zichtbaar voor iedereen die de mogelijkheid heeft om de packet transfer te bekijken.

Dit is ook duidelijk aan de hand van de inspectie op de volgende screenshots:



Screenshot 3: Telnet inspectie in simulation mode

Tijdens het versturen van het passwoord 'PassVTY' naar de Switch, om de Telnet verbinding te leggen, was het mogelijk om de packet data te inspecteren. Per key-down event wordt data aangemaakt, en verstuurd. Net zoals het in Wireshark mogelijk was om deze data te vervolgen met behulp van: Follow Telnet Stream, is het hier ook mogelijk om aan de hand van de 'Outbound PDU Details' te zien welke informatie verstuurd wordt. Op de screenshot boven links is de letter 'P' te zien in het Telnet protocol. Elke packet op de rechterkant bevat de volgende key-down event, waardoor het wachtwoord uiteindelijk 'vervolgbaar' is. Bij SSH is de data versleuteld en niet te zien:



4.1 Disable unused ports (SW2)

1. Wat is het nut van het shutdown commando?

Het shutdown commando geeft de mogelijkheid om bepaalde interfaces af te sluiten. Dit zou voor een gehele interface kunnen werken, zoals een router of switch, maar ook voor bepaalde ingangen van devices, bijvoorbeeld interface GigabitEthernet 0/0/0.

4.2 Port Security (SW1)

1. Is het mogelijk om PCXX te verbinden met het netwerk?

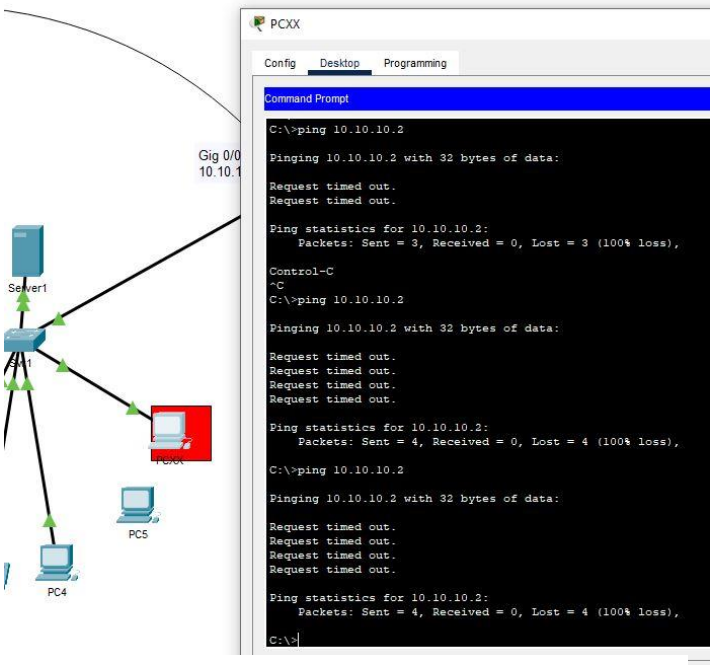
Screenshot 5: Reeds afgesloten poorten op SW1

```
interface FastEthernet0/6
 shutdown
!
interface FastEthernet0/7
 shutdown
!
interface FastEthernet0/8
 shutdown
!
interface FastEthernet0/9
 shutdown
!
interface FastEthernet0/10
 shutdown
!
interface FastEthernet0/11
 shutdown
!
interface FastEthernet0/12
 shutdown
!
interface FastEthernet0/13
 shutdown
!
interface FastEthernet0/14
 shutdown
!
interface FastEthernet0/15
 shutdown
!
interface FastEthernet0/16
 shutdown
!
interface FastEthernet0/17
 shutdown
!
interface FastEthernet0/18
 shutdown
!
interface FastEthernet0/19
 shutdown
!
interface FastEthernet0/20
 shutdown
!
interface FastEthernet0/21
 shutdown
!
interface FastEthernet0/22
 shutdown
!
interface FastEthernet0/23
 shutdown
!
interface FastEthernet0/24
 shutdown
```

Op de linker kant zijn de reeds afgesloten poorten te zien van SW1. Dit betekent dus dat alle poorten vanaf en inclusief interface FastEthernet 0/6 afgesloten zijn. Het was dus niet mogelijk om PCXX met het netwerk te verbinden.

2. Waarom is port security belangrijk bij een switch? Welke attacks kan je hiermee voorkomen?

De meest voorkomende attacks op een switch zijn meestal ARP Spoofing, Mac Flooding, Mac Spoofing en DHCP Spoofing. Door poort security in te stellen is het mogelijk om het aantal adressen te beperken per open poort. Door in te stellen dat maar 1 Mac adres tegelijk aangesloten mag worden is het mogelijk om een attack zoals Mac Flooding te voorkomen. In het volgende screenshot is zichtbaar dat PCXX geen verbinding kan maken met SW1; alle ping requests staan op timed out.



Screenshot 6: Port Security

5 ACL

1. Welke melding krijg je naar een ping?

```
C:\>ping 10.10.10.18

Pinging 10.10.10.18 with 32 bytes of data:

Reply from 10.10.10.65: Destination host unreachable.
Reply from 10.10.10.65: Destination host unreachable.
Reply from 10.10.10.65: Destination host unreachable.
Reply from 10.10.10.65: Destination host unreachable.

Ping statistics for 10.10.10.18:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

2. Kan een interface van netwerk B:

   a) pingen naar een interface binnen het netwerk? **Ja**

```
C:\>ping 10.10.10.68

Pinging 10.10.10.68 with 32 bytes of data:

Reply from 10.10.10.68: bytes=32 time=13ms TTL=128
Reply from 10.10.10.68: bytes=32 time<1ms TTL=128
Reply from 10.10.10.68: bytes=32 time=1ms TTL=128
Reply from 10.10.10.68: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.10.68:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 3ms

C:\>
```

   b) pingen naar 8.8.8.8? **Nee**

```
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Reply from 10.10.10.65: Destination host unreachable.
Reply from 10.10.10.65: Destination host unreachable.
Reply from 10.10.10.65: Destination host unreachable.
Reply from 10.10.10.65: Destination host unreachable.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

   c) een DNS query verzenden naar 8.8.8.8? **Nee**

```
C:\>nslookup 8.8.8.8

Server: [8.8.8.8]
Address:  8.8.8.8
DNS request timed out.
          timeout was 15000 milli seconds.

Server: [8.8.8.8]
Address:  8.8.8.8
*** UnKnown can't find 8.8.8.8: Non-existent domain.

C:\>
```

3. Waarvoor dient ACL en welke attacks kan je hiermee voorkomen?

   ACL's zijn de pakketfilters van een netwerk. Ze kunnen verkeer dat essentieel is voor de veiligheid beperken, toestaan of weigeren. Met een ACL is het mogelijk de stroom van pakketten te regelen voor een enkel IP-adres of een groep IP-adressen of voor andere protocollen, zoals TCP, UDP, ICMP, etc.

6 DNS & DHCP

1. Wat is het DNS adres gebruikt door PC0?

   8.8.8.8

2. Welke interface verdeeld deze informatie (DHCP)?

   Server 1: Click → Services → DHCP

3. Wat is het DNS adres gebruikt door PC8?

   8.8.8.8

4. Welke interface verdeeld deze informatie (DHCP)?

   Server 1

5. Op welk IP-adres bevindt zich de website pxl.be?

   8.8.8.10

   Rogue DNS Server → Services → DNS

7 Wi-Fi

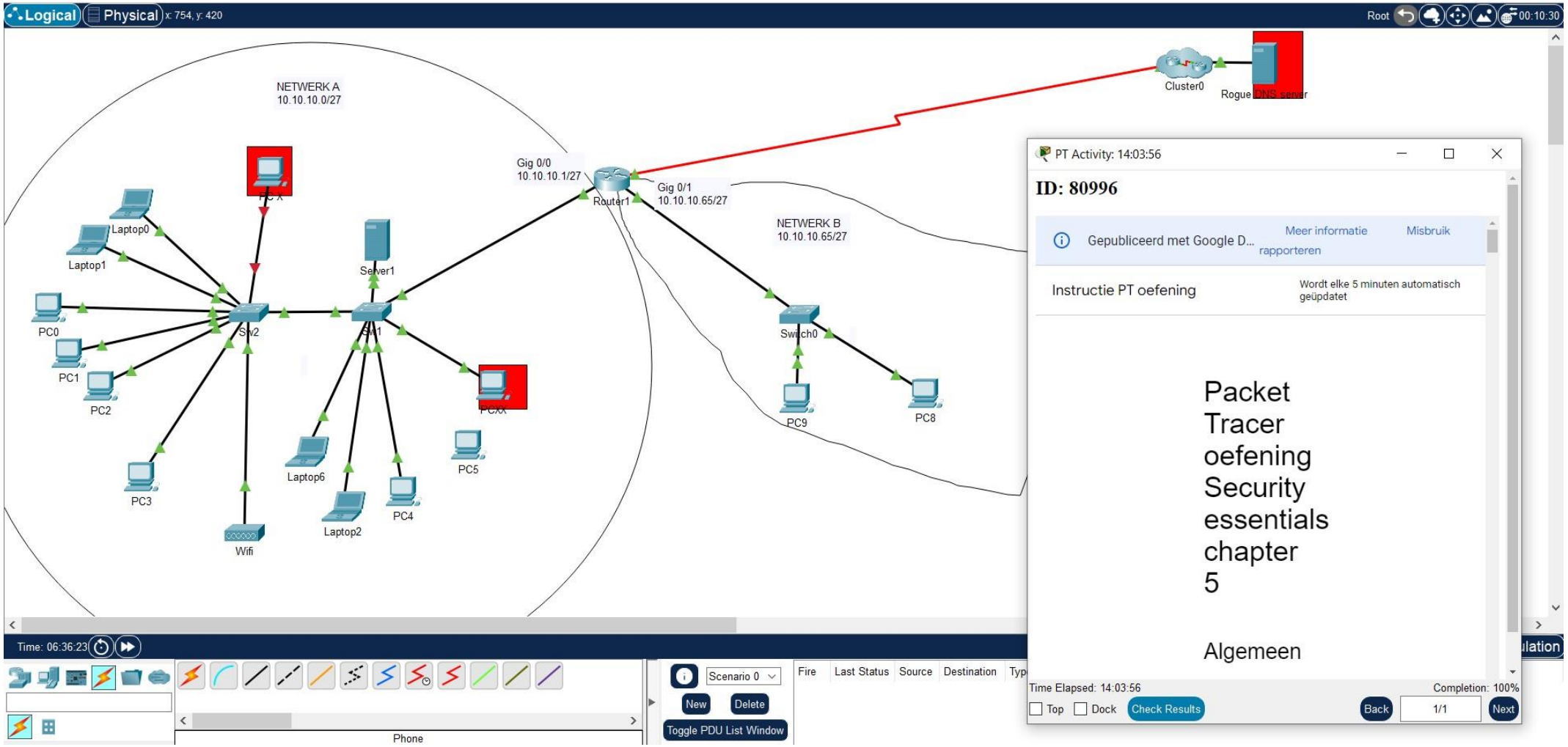
1. Welke encryptieprotocol wordt hier toegepast?

   AES is het encryptie protocol wat hier van toepassing is. Uit Labo 2 weten wij: AES is de eerste en enige encryptiemethode die is goedgekeurd door de National Security Agency (NSA) voor de bescherming van topgeheime (confidentiële) informatie. Het AES-algoritme gebruikt 3 sleutellengtes: 128, 192 en 256-bit.

2. Wat betekent SSID?

   De afkorting SSID staat voor Service Set Identifier. Dit is de unieke naam die een draadloos netwerk identificeert. Het staat in de pakketheader wanneer een datapakket wordt verzonden. De apparaten op het wifi-netwerk gebruiken deze identifier voor communicatie via het netwerk. De naam is maximaal 32 alfanumerieke tekens lang en hoofdlettergevoelig. Op de volgende pagina is het laatste screenshot te zien van de voltooide PT oefening met ID.

Screenshot 9: De voltooide oefening



3 THM Rooms

3.1 THM Active Reconnaissance

In deze THM wordt er besproken wat het verschil is tussen passive en active reconnaissance.

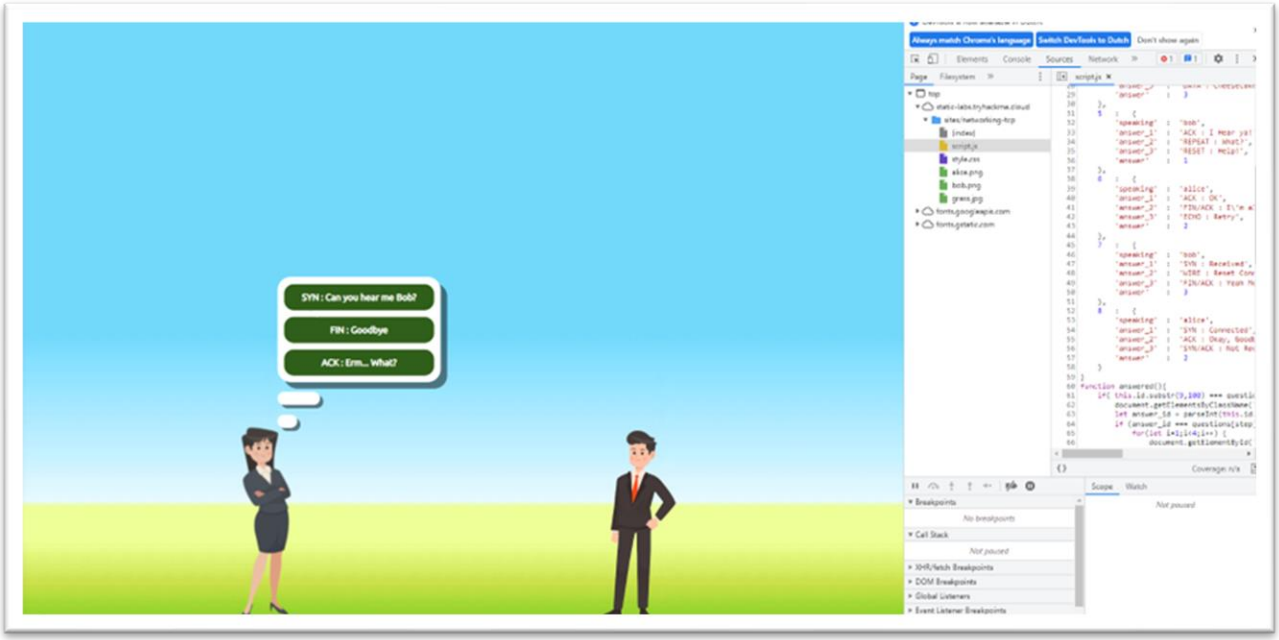
Passive Reconnaissance is waar we informatie gaan opzoeken over de target zonder interactie met de target zelf, zoals opzoekwerk op het internet of dergelijke.

Active Reconnaissance is waar we effectief een connectie gaan leggen tussen ons en de target. Bijvoorbeeld via een ping, of telnet, of door gewoon simpel te connecteren met hun webbrowser.

Eerst gingen we kijken hoe handig een webbrowser kan zijn. In de opzoekbalk kunnen we bijvoorbeeld bij een IP-adres een specifieke poort meegeven om te zoeken of er een webpagina op deze poort draait.

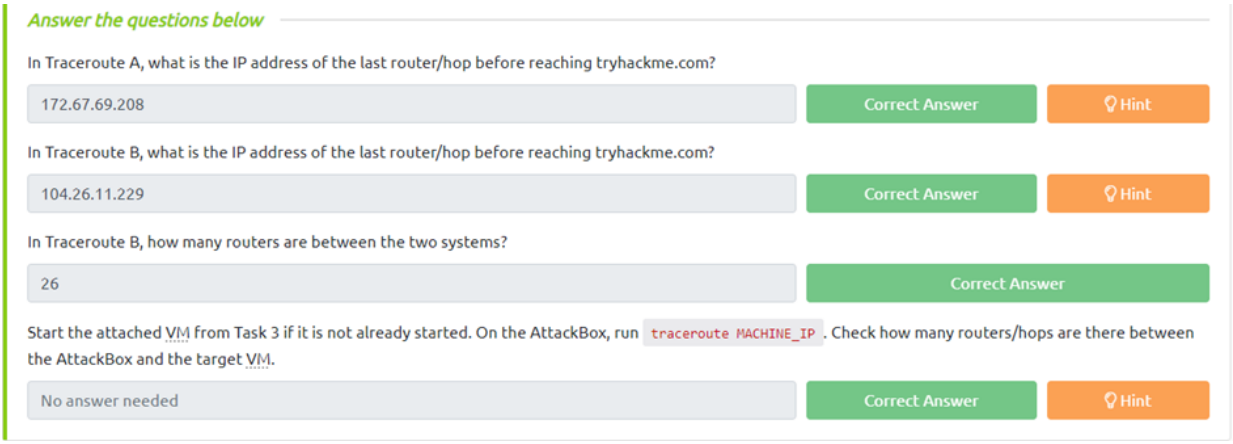
Hierna kunnen we dan opzoek gaan naar info via de “developer tools” hierin kunnen we knoeien met de JavaScript, of de cookies bekijken van ons systeem.

Bij deze kregen we de vraag om op te zoeken hoeveel vragen er waren op een bepaalde web-site, deze konden we vinden door in de Dev-tools te gaan kijken bij de source en de javascript file, hier stonden de vragen mooi opgelijst.

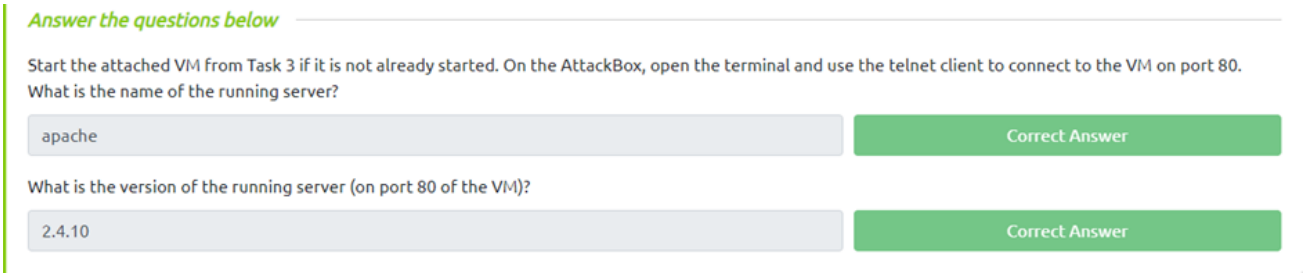


Hierna gingen we tewerk met het simpele ping commando, met de verschillende flags van deze ping commando, iedereen heeft wel al eens gewerkt met het ping commando.

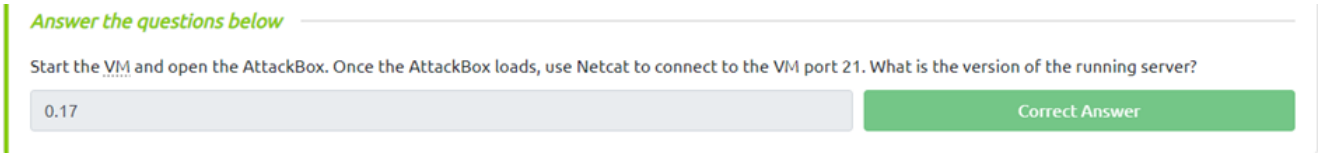
Hierna gingen we met de gelijkaardige maar toch heel verschillende commando "traceroute" te-werk, zoals de naam zelf suggereert, gaan we na welke stappen de packet doorgaat tot hij aan onze eindlocatie komt, hier gaan we kijken welke routers, en dergelijke hij passeert.



Telnet is daarnaast ook een geweldig commando, waarmee we remote control acces hebben via een CLI. Het security aspect is misschien niet zo geweldig, aangezien dat TELNET de informatie in cleartext verstuurd. Hierbij gingen we kijken naar de bepaalde server en kijken welke info we konden vinden met een ip adres en een poort



Dan tenslotte gingen we tewerk met Netcat of nc. Netcat heeft support voor TCP en UDP, en kan dus functioneren als een client of als een server. Die bijde gaan luisteren of connecteren aan een bepaalde poort. We gingen kijken welke versie van de server bekijken die aan het runnen was op de poort 21. Dit kunnen we doen met het commando **“nc -v MACHINE_IP 21”**



Conclusie

Dit zijn allemaal zeer handige tools voor een pen tester, met verschillende doeleinden om active reconnaissance uit te voeren. Dit maakt het heel interessant om te zien dat zo simpele tools toch gevaarlijk uit de hoek kunnen komen

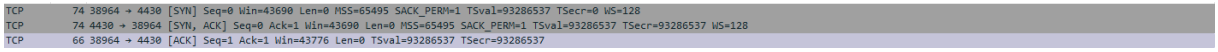
4 Extra

4.1 TLS Handshake in Wireshark

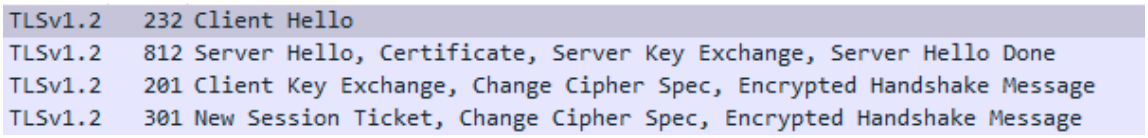
1. Vervangt een TLS handshake de TCP handshake? Toon aan via de pcap file.

Nee, een TLS handshake vervangt de TCP handshake niet.

TCP handshake:



TLS handshake:



2. Wat is het verschil tussen een TCP handshake en een TLS handshake?

Het verschil tussen een TCP en TLS handshake is makkelijk te onderscheiden.

Een TCP-handshake ziet eruit als volgt:

> Client -> Server **[** SYN X **]**
> Client <- Server **[** SYN Y, ACK X+1 **]**
> Client -> Server **[** ACK Y+1 **]**

- De eerste host (Client) stuurt de tweede host (Server) een "synchroniseer" (SYN)-bericht met zijn eigen volgnummer x, dat de Server ontvangt.
- De server antwoordt met een synchroon-bevestigingsbericht (SYN-ACK) met zijn eigen volgnummer y en bevestigingsnummer x+1, dat de klant ontvangt.
- Client antwoordt met een bevestigingsbericht (ACK) met bevestigingsnummer y+1, dat de server ontvangt en waarop hij niet hoeft te antwoorden.

Terwijl een TLS handshake er zo uitziet:

> Client -> Server **[**Client Hello**]**
> Client <- Server **[**Server Hello**]**
> Client <- Server **[**Certificate**]**
> Client <- Server **[**ServerKeyExchange**]**
> Client <- Server **[**ServerHelloDone**]**
> Client -> Server **[**ClientKeyExchange**]**
>
> Client -> Server **[**ChangeCipherSpec**]**
>
> Client <- Server **[**ChangeCipherSpec**]**
> Client <-> Server **[**Application**]**

- **Client Hello:** de Client-Hello is de informatie die de server nodig heeft om met de Client te communiceren via SSL/TLS. Dit omvat het SSL-versienummer, coderingsinstellingen, sessiespecifieke gegevens.

- **Server Hello:** de Server-Hello is informatie die de server nodig heeft om met de client te communiceren via SSL. Dit omvat het SSL-versienummer, coderingsinstellingen, sessiespecifieke gegevens.

- **Authentication and Pre-Master Secret:** Client verifieert het servercertificaat. De Client maakt het pre-mastergeheim voor de sessie, versleutelt met de openbare sleutel van de server en stuurt het versleutelde pre-mastergeheim naar de server.

- **Decryption and Master Secret:** de server gebruikt zijn privésleutel om het pre-mastergeheim te ontsleutelen. Zowel Server als Client voeren stappen uit om het hoofdgeheim te genereren met de overeengekomen code.

- **Encryption with Session Key:** zowel de client als de server wisselen berichten uit om te informeren dat toekomstige berichten versleuteld zullen worden.

3. Welke random bytes worden meegegeven tijdens de eerste client-hello?

```
Transport Layer Security
▾ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 161
  ▾ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 157
      Version: TLS 1.2 (0x0303)
    ▾ Random: 52362c1012cf23628256e745e903cea696e9f62a60ba0ae8311d70dea5e41949
        GMT Unix Time: Sep 15, 2013 23:52:16.000000000 West-Europa (zomertijd)
        Random Bytes: 12cf23628256e745e903cea696e9f62a60ba0ae8311d70dea5e41949
```

4. Welke cyphersuite wordt gebruikt door de server

```
Transport Layer Security
▾ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 66
  ▾ Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 62
      Version: TLS 1.2 (0x0303)
    ▾ Random: 52362c10a2665e323a2adb4b9da0c10d4a8823719272f8b4c97af24f92784812
        GMT Unix Time: Sep 15, 2013 23:52:16.000000000 West-Europa (zomertijd)
        Random Bytes: a2665e323a2adb4b9da0c10d4a8823719272f8b4c97af24f92784812
      Session ID Length: 0
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
```

5. Wat is de public key van het certificaat?

```
Handshake Protocol: Certificate
    Handshake Type: Certificate (11)
    Length: 447
    Certificates Length: 444
  Certificates (444 bytes)
      Certificate Length: 441
    Certificate: 308201b53082011e020900f4a72fd3e8fc37c4300d06092a864886f70d0101050500301f… (id-at-commonName=Test Certificate RSA)
      signedCertificate
          serialNumber: 0x00f4a72fd3e8fc37c4
        signature (sha1WithRSAEncryption)
            Algorithm Id: 1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
        issuer: rdnSequence (0)
          rdnSequence: 1 item (id-at-commonName=Test Certificate RSA)
        validity
          notBefore: utcTime (0)
          notAfter: utcTime (0)
        subject: rdnSequence (0)
          rdnSequence: 1 item (id-at-commonName=Test Certificate RSA)
        subjectPublicKeyInfo
          algorithm (rsaEncryption)
              Algorithm Id: 1.2.840.113549.1.1.1 (rsaEncryption)
          subjectPublicKey: 30818902818100ac352a937fc54f1898b29fa0fb34e6e28b9ed7469107d8488aa8438bfa…
              modulus: 0x00ac352a937fc54f1898b29fa0fb34e6e28b9ed7469107d8488aa8438bfac0ffb7cad55f…
              publicExponent: 65537
```

6. Wat is de public key van het Diffie-Hellman protocol?

```
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 70
    Handshake Protocol: Client Key Exchange
        Handshake Type: Client Key Exchange (16)
        Length: 66
      EC Diffie-Hellman Client Params
          Pubkey Length: 65
          Pubkey: 04cb2685d43bf72245dc2f496f5d78f3a48edf7b29ae7c51c68e2ed1fb12a286e06b3a3a…
```

7. Omschrijf de stappen van een TCP handshake op basis van de pcap file.

In de PCAP-file stuurt de Client een SYN-pakket naar de Server gevolgd met het volgnummer 0. Vervolgens reageert de Server hierop met een SYN-ACK-pakket om te bevestigen dat hij er is, gevolgd met sequence number 1. Om te bevestigen dat de Client het antwoord van de Server ontvangen heeft reageert hij met een ACK gevolgd met sequence number 1.