Security Audit - Audit

Getting ready

→ Understand the scope of the exercise

→ Retrieve and execute the VM on your lab system

Conduct the audit

Organisation of ISMS

→ What is the purpose of this VM ?

```
netdiscover -r 192.168.142.0/24
```

→ What services does it provide ?

```
nmap -sV 192.168.142.69
nmap -sV 127.0.0.1
```

→ who's responsable for configuring and setting this up ?

```
cat /etc/password
cat /home/admin/.ssh/authorized
```

→ what are the security measures provided ?

```
iptables -L -v -n
iptables -L
```

-n → désactive la resolution des hôtes

-v → mode "verbeux"

Network Architecture (Access Control, Filtering, containment, reliability)

→ Describe the Network topology

```
ip addr / ip a
```

→ Check network filtering from/to the VM by using port scanning (nmap)

```
nmap -sV 192.168.142.69
```

→ check filtering rules

```
iptables -L -v -n
ip6tables -L -v -n
```

Confidentiality and integrity of communication

→ Capture and analysis of traffic between the server and a client (tcpdump)

```
sudo tcpdump -i eth1 -s0 -w /opt/VM/SNS-lab/moodle.pcap
```

↳ analyse it with wireshark. ← use wireshark to open it

Access control to logical level (host system, VM, apps and data)

Operating system Audit

→ List of running services and configuration

```
systemctl list-units --type=service --state=running
```

→ Filtering (netfilter, tcp wrappers)

↳ base d'iptables

Vulnerability Scan (from the network or on the system)

→ debsecan on the system

```
sudo debsecan
```

→ list vulnerabilités connues pour les paquets scannés

lynis audit system

→ openvas/nuclei from the network

→ vulnerabilities scan of services (nikto/wikto, w3af, ...)

```
nikto -h 192.168.142.49 -p 443
nikto -h http://example.com
```

Evaluate Strength of passwords (using johntheripper or hashcat or...)

```
hashcat /opt/VM/SNS-LAB1/password.txt
hashcat /opt/VM/SNS-LAB1/password.txt -a 0 -m 3200 /usr/share/wordlists/john.lst
```

Data Security - Encryption ? Wiping ? Residual Data (cache, tmp files, logs) ?

Operational and management procedures

→ Backup and Recovery Planning

SSH ?

ipv6 actif ?

un nmap sur le loopback

avoir son adresse IP → ifconfig

:443 ← Open HTTP ← firefox 192.168.142.71:80
↳ HTTPS

wget 127.0.0.1 : 12321

(need password) // to connect in ssh ← ssh root@192.168.142.78

nmap en localhost ← nmap -sV 127.0.0.1

voir si des défenses sont prévues au niveau du firewall pour ipv6 ← ip6tables -L -v -n

fichier ordinaire

permissions du propriétaire

permission du groupe

proprio du fichier

```
-rw-r----- 1 root shadow
```

permission pour les autres

groupe proprio

vérifier les permissions des fichiers critiques / ls -l /etc/passwd
ls -l /etc/shadow

Vérifier si le système est mis à jour : apt list --upgradable

inventaire des fichiers installés : dpkg -l

Récupérer des infos sur le système : uname -a

lister les utilisateurs : cat /etc/passwd
vérifier les groupes et privilèges : sudo -l
vérifier les routes : route -n

Tester la configuration SSL : ./testssl.sh sur un serveur web

Vérifier les services en cours d'exécution : ps aux

crée un fichier avec les hash de /etc/shadow.
vim hash.txt → CTR + SHIFT + V → echap :x
fichier sauvegardé ←→

MD5	-m 500
SHA-256	-m 1400
SHA-512	-m 1800
bcrypt (Blowfish)	-m 3200

john --wordlist=/usr/share/john/password.lst --format=bcrypt hashes.txt
--format=auto ← déterminer automatiquement le format

hashcat -m 3200 -a 0 hashes.txt rockyou.txt

mv
mv fichier_source fichier_destination
cp fichier_source fichier_destination