



UNIVERSITÉ SORBONNE PARIS NORD
DÉPARTEMENT RÉSEAUX ET TÉLÉCOMMUNICATIONS

PARCOURS: CYBERSÉCURITÉ

SAE: ASSURER LA SÉCURISATION ET LA
SUPERVISION AVANCEES D'UN SYSTÈME
D'INFORMATION

BUT3 CYBERSÉCURITÉ

SUPERVISEUR:

DR. MOHAMED AMINE OUAMRI
UNIVERSITÉ SORBONNE PARIS NORD

UNIVERSITÉ
SORBONNE
PARIS NORD

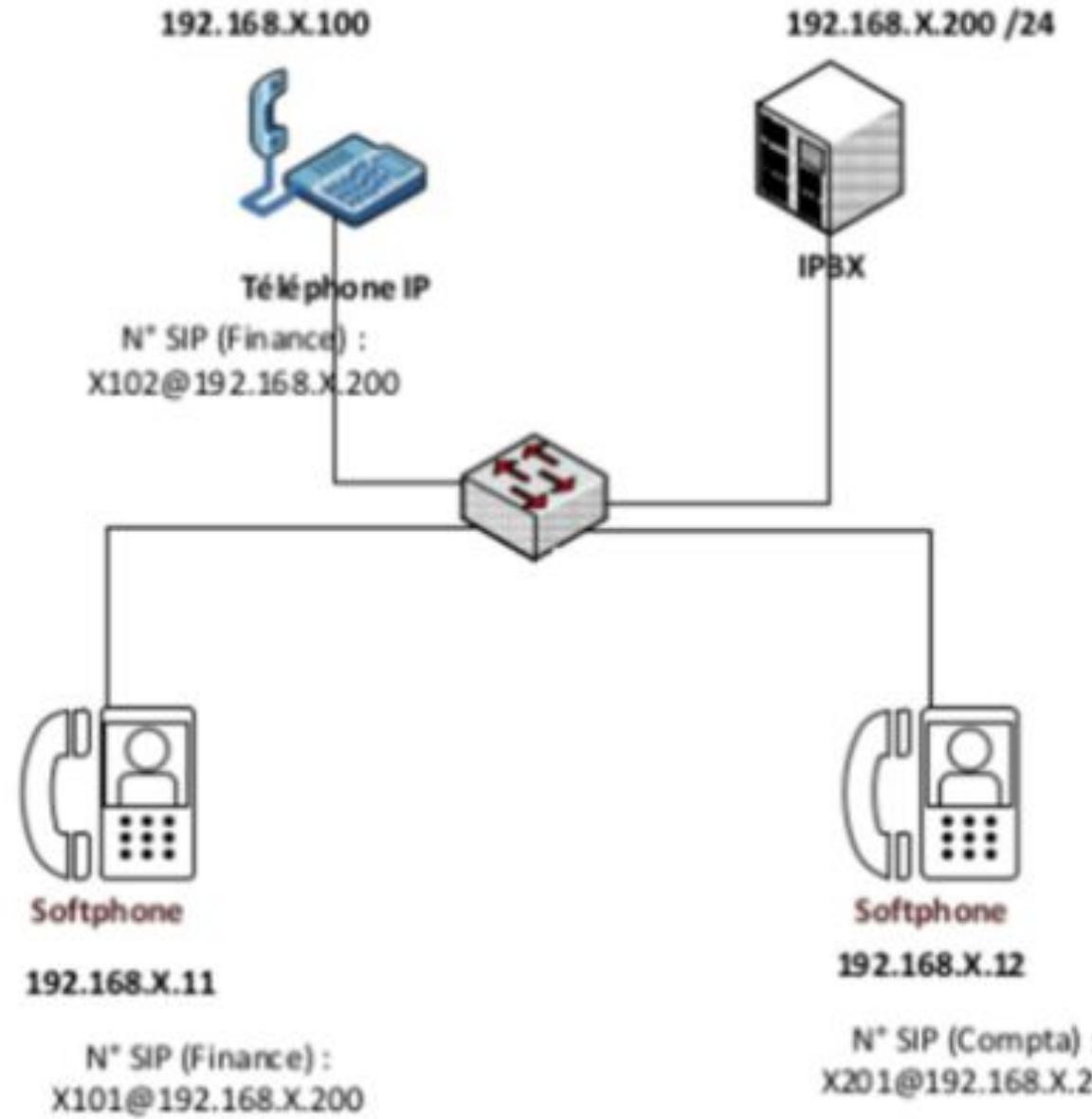


Présentation de la SAE Assurer la sécurisation et la supervision avancées d'un système d'information

- **Partie 1:Mise en place d'une attaque de type eavesdropping**
- **Partie 2 :Création et Analyse avec un SIEM Wazuh**

Projet réalisé et présenté par :

- Elodie Jourdain
- Salima Zribi



Partie 1 : Mise en place d'une attaque de type eavesdropping

Cette présentation explore une attaque de type "**eavesdropping**" sur une infrastructure **VoIP** basée sur **Asterisk**. Notre objectif est d'intercepter une communication téléphonique interne entre deux contextes clés : **Finance** et **Compta**.

Infrastructure VoIP

Basée sur **Asterisk**

Contextes Ciblés

Finance & Compta

Objectif Principal

Intercepter communication

Architecture Réseau VoIP

Notre architecture VoIP est composée de **trois éléments clés**, tous situés sur le **même sous-réseau** pour simplifier la démonstration de l'attaque.

- ❑ **Serveur IPBX Asterisk** : 192.168.1.200
- ❑ **Softphone victime** : 192.168.1.11
- ❑ **Téléphone IP** : 192.168.1.100
- ❑ **Machine attaquante** : 192.168.1.10

| Machine | @ip |
|---------------------|------------------|
| attaquant softphone | 192.168.1.11/24 |
| serveur | 192.168.1.200/24 |
| tel ip | 192.168.1.100/24 |

Installation et vérification d'Asterisk

- ❑ L'installation du serveur Asterisk est la **première étape cruciale**. Une fois installé, nous vérifions que le **service fonctionne correctement** pour assurer la base de notre **infrastructure VoIP**.

```
root@p20320:/home/toto# apt-get install asterisk
Lecture des listes de paquets... Fait
```

```
root@p20320:/home/toto# systemctl status asterisk
● asterisk.service - Asterisk PBX
  Loaded: loaded (/lib/systemd/system/asterisk.ser
  Active: active (running) since Thu 2025-12-04 15
    Docs: man:asterisk(8)
Main PID: 4002 (asterisk)
```

Comptes SIP et messagerie vocale

Nous avons configuré les utilisateurs SIP pour les contextes **Finance** et **Compta**, ainsi que leurs **boîtes vocales** respectives. Cela permet des communications internes structurées et la gestion des messages.

Utilisateurs SIP

Création des comptes pour Finance et Compta.

```
GNU nano 5.4                               users.conf
[general]
hasvoicemail = yes
hassip = yes

[template](!)
type = friend
host = dynamic
dtmfmode = rfc2833
disallow = all
allow = ulaw
allow = alaw

[1101](template)
fullname = Finance
username = 1101
secret = password
mailbox = 1101
context = finance

[1201](template)
fullname = compta
username = 1201
secret = password
mailbox = 1201
context = compta
```

Vérification de la création des comptes.

```
p20320*CLI> sip show users
Username          Secret      Accountcode  Def.Context  AC
L_Forceport
1101              password    finance      No
No
1201              password    compta      No
No
p20320*CLI>
```

Boîtes vocales

Création des boîtes vocales.

```
GNU nano 5.4                               voicemail.conf
[general]
maxmsg = 100 ;nombre maximum de messages de la boite vocale.
maxsecs = 0 ;durée maximum d'un message. Le 0 indique l'absence de limite.
minsecs = 0 ;durée minimum d'un message.
maxlogins = 3 ;nombre maximum d'erreur de login.
review = no ;permet à l'appelant de réécouter son message avant de le laisser sur la boite vocale.
saycid = no ;dicte le numéro de l'appelant avant l'écoute du message.

[finance]
1101 => 1234, finance
[compta]
1201 => 1234, compta
```

Vérification de la création des boîtes vocales.

```
p20320*CLI> voicemail show users
Context   Mbox  User           Zone     NewMsg
default   1101  Finance        0
default   1201  compta         0
finance   1101  finance        0
compta    1201  compta         0
4 voicemail users configured.
p20320*CLI>
```

DialPlan Asterisk

Le **DialPlan d'Asterisk** a été créé pour gérer le **routage des appels**. Il autorise les **communications inter-contextes**, permettant aux utilisateurs de **Finance** et de **Compta** de s'appeler mutuellement.

DialPlan Finance

Règles de **routage spécifiques** au département **Finance**.

```
p20320*CLI> dialplan show finance
[ Context 'finance' created by 'pbx_config' ]
  '1199' =>
    1. Answer()                                [extensions.conf:1]
    2. VoiceMailMain(${CALLERID(num)}@finance)  [extensions.conf:1]
    3. Hangup()                                 [extensions.conf:1]
  '_11XX' =>
    1. DIAL(SIP/${EXTEN},20)                   [extensions.conf:7]
    2. Voicemail(${EXTEN}@finance)             [extensions.conf:8]
    3. Hangup()                                 [extensions.conf:9]
  '_12XX' =>
    1. Goto(compta,${EXTEN},1)                 [extensions.conf:1]
                                         
-= 3 extensions (7 priorities) in 1 context. =-
p20320*CLI>
```

DialPlan Compta

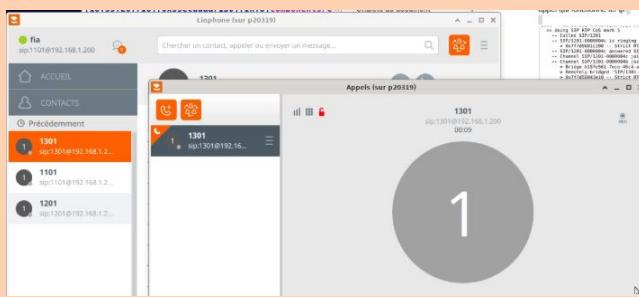
Règles de **routage spécifiques** au département **Compta**.

```
p20320*CLI> dialplan show compta
[ Context 'compta' created by 'pbx_config' ]
  '1199' =>
    3. Hangup()                                [extensions.conf:2]
  '1299' =>
    1. Answer()                                [extensions.conf:2]
    2. VoiceMailMain(${CALLERID(num)}@compta)  [extensions.conf:2]
  '_11XX' =>
    1. Goto(finance,${EXTEN},1)                [extensions.conf:3]
    3. Hangup()                                 [extensions.conf:2]
  '_12XX' =>
    1. DIAL(SIP/${EXTEN},20)                   [extensions.conf:2]
    2. Voicemail(${EXTEN}@compta)              [extensions.conf:2]
                                         
-= 4 extensions (7 priorities) in 1 context. =-
p20320*CLI>
```

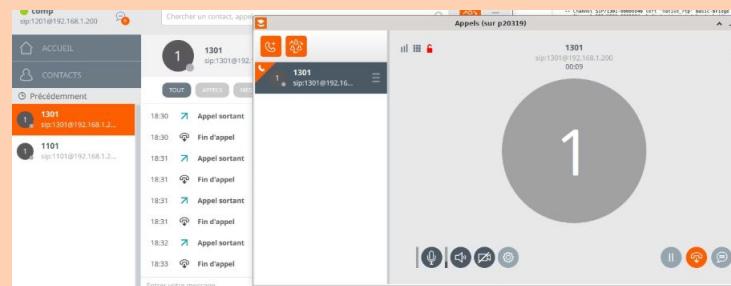
Appels VoIP fonctionnels

Avant l'attaque, nous avons vérifié la **fonctionnalité des appels VoIP**. Les communications entre **softphones**, entre **téléphone IP et softphone**, et entre les **contextes Finance et Compta** sont toutes **opérationnelles**.

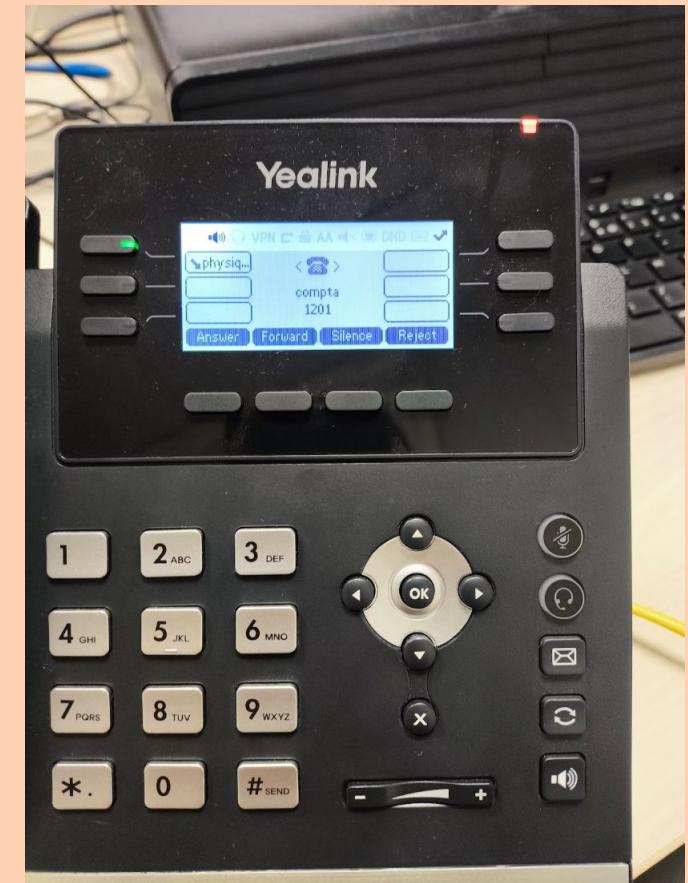
- ☐ **Appel entre 1101 et 1301**
(même contexte)



- ☐ **Appel entre 1201 et 1301 (contextes différents)**



- ☐ **Appel depuis Compta vers le téléphone physique**



Analyse Wireshark sans attaque

Une capture réseau initiale avec **Wireshark**, côté client, montre le **trafic SIP et RTP normal** d'une **communication VoIP**. Cela sert de **référence** pour identifier les **anomalies** lors de l'attaque.



Avant décroché

Trafic SIP initial.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|-------------------|------------------------|----------|--------|-----------------|
| 2 | 0.000041800 | 192.168.1.11 | 192.168.1.100 | UDP | 46 | 5060 → 5060 Len |
| 3 | 0.234955612 | 6c:4e:f6:6b:dc:90 | Spanning-tree-(for...) | STP | 60 | RST. Root = 327 |
| 4 | 2.239017816 | 6c:4e:f6:6b:dc:90 | Spanning-tree-(for...) | STP | 60 | RST. Root = 327 |
| 5 | 3.438156891 | 192.168.1.200 | 192.168.1.11 | SIP/SDP | 946 | Request: INVITE |
| 6 | 3.444227457 | 192.168.1.11 | 192.168.1.200 | SIP | 305 | Status: 100 Try |
| 7 | 3.465130702 | 192.168.1.11 | 192.168.1.200 | SIP | 450 | Status: 180 Rin |
| 8 | 4.238763772 | 6c:4e:f6:6b:dc:90 | Spanning-tree-(for...) | STP | 60 | RST. Root = 327 |
| 9 | 4.335600863 | 6c:4e:f6:6b:dc:90 | 6c:4e:f6:6b:dc:90 | LOOP | 60 | Reply |
| 10 | 4.857424419 | 6c:4e:f6:6b:dc:90 | CDP/VTP/DTP/PAgP/UD... | CDP | 462 | Device ID: Swit |
| 11 | 6.238676127 | 6c:4e:f6:6b:dc:90 | Spanning-tree-(for...) | STP | 60 | RST. Root = 327 |
| 12 | 8.243095527 | 6c:4e:f6:6b:dc:90 | Spanning-tree-(for...) | STP | 60 | RST. Root = 327 |
| 13 | 10.009729184 | 192.168.1.11 | 192.168.1.200 | UDP | 46 | 5060 → 5060 Len |
| 14 | 10.009773836 | 192.168.1.11 | 192.168.1.100 | UDP | 46 | 5060 → 5060 Len |
| 15 | 10.242782471 | 6c:4e:f6:6b:dc:90 | Spanning-tree-(for...) | STP | 60 | RST. Root = 327 |
| 16 | 12.246918216 | 6c:4e:f6:6b:dc:90 | Spanning-tree-(for...) | STP | 60 | RST. Root = 327 |
| 17 | 14.251177556 | 6c:4e:f6:6b:dc:90 | Spanning-tree-(for...) | STP | 60 | RST. Root = 327 |
| 18 | 14.336110400 | 6c:4e:f6:6b:dc:90 | 6c:4e:f6:6b:dc:90 | LOOP | 60 | Reply |
| 19 | 16.251061307 | 6c:4e:f6:6b:dc:90 | Spanning-tree-(for...) | STP | 60 | RST. Root = 327 |
| 20 | 18.255260534 | 6c:4e:f6:6b:dc:90 | Spanning-tree-(for...) | STP | 60 | RST. Root = 327 |
| 21 | 20.009851828 | 192.168.1.11 | 192.168.1.200 | UDP | 46 | 5060 → 5060 Len |
| 22 | 20.009871185 | 192.168.1.11 | 192.168.1.100 | UDP | 46 | 5060 → 5060 Len |
| 23 | 20.259580757 | 6c:4e:f6:6b:dc:90 | Spanning-tree-(for...) | STP | 60 | RST. Root = 327 |
| 24 | 22.259600391 | 6c:4e:f6:6b:dc:90 | Spanning-tree-(for...) | STP | 60 | RST. Root = 327 |



Après décroché

Flux RTP de la conversation.

| | | | |
|----------------------------------|---------------|-----|---|
| 2909 143.310658600 192.168.1.100 | 192.168.1.11 | RTP | 214 PT=ITU-T G.711 PCMU, SSRC=0x4B23294E, Seq=11100, Time=217600 |
| 2910 143.323271459 192.168.1.11 | 192.168.1.100 | RTP | 214 PT=ITU-T G.711 PCMU, SSRC=0x4BA9017D, Seq=1353, Time=3692360718 |
| 2911 143.334640129 192.168.1.100 | 192.168.1.11 | RTP | 214 PT=ITU-T G.711 PCMU, SSRC=0x4B23294E, Seq=11101, Time=217760 |
| 2912 143.350557781 192.168.1.100 | 192.168.1.11 | RTP | 214 PT=ITU-T G.711 PCMU, SSRC=0x4B23294E, Seq=11102, Time=217920 |
| 2913 143.352742761 192.168.1.11 | 192.168.1.100 | RTP | 214 PT=ITU-T G.711 PCMU, SSRC=0x4BA9017D, Seq=1354, Time=3692360878 |
| 2914 143.373379766 192.168.1.11 | 192.168.1.100 | RTP | 214 PT=ITU-T G.711 PCMU, SSRC=0x4BA9017D, Seq=1355, Time=3692361038 |
| 2915 143.374654482 192.168.1.100 | 192.168.1.11 | RTP | 214 PT=ITU-T G.711 PCMU, SSRC=0x4B23294E, Seq=11103, Time=218080 |
| 2916 143.390627634 192.168.1.100 | 192.168.1.11 | RTP | 214 PT=ITU-T G.711 PCMU, SSRC=0x4B23294E, Seq=11104, Time=218240 |
| 2917 143.393672374 192.168.1.11 | 192.168.1.100 | RTP | 214 PT=ITU-T G.711 PCMU, SSRC=0x4BA9017D, Seq=1356, Time=3692361198 |
| 2918 143.413234885 192.168.1.11 | 192.168.1.100 | RTP | 214 PT=ITU-T G.711 PCMU, SSRC=0x4BA9017D, Seq=1357, Time=3692361358 |
| 2919 143.414642913 192.168.1.100 | 192.168.1.11 | RTP | 214 PT=ITU-T G.711 PCMU, SSRC=0x4B23294E, Seq=11105, Time=218400 |
| 2920 143.430598867 192.168.1.100 | 192.168.1.11 | RTP | 214 PT=ITU-T G.711 PCMU, SSRC=0x4B23294E, Seq=11106, Time=218560 |
| 2921 143.434209163 192.168.1.11 | 192.168.1.100 | RTP | 214 PT=ITU-T G.711 PCMU, SSRC=0x4BA9017D, Seq=1358, Time=3692361518 |
| 2922 143.434220937 192.168.1.11 | 192.168.1.100 | RTP | 214 PT=ITU-T G.711 PCMU, SSRC=0x4BA9017D, Seq=1359, Time=3692361678 |
| 2923 143.454585651 192.168.1.100 | 192.168.1.11 | RTP | 214 PT=ITU-T G.711 PCMU, SSRC=0x4B23294E, Seq=11107, Time=218720 |
| 2924 143.470566337 192.168.1.100 | 192.168.1.11 | RTP | 214 PT=ITU-T G.711 PCMU, SSRC=0x4B23294E, Seq=11108, Time=218880 |
| 2925 143.473535590 192.168.1.11 | 192.168.1.100 | RTP | 214 PT=ITU-T G.711 PCMU, SSRC=0x4BA9017D, Seq=1360, Time=3692361838 |
| 2926 143.494613816 192.168.1.100 | 192.168.1.11 | RTP | 214 PT=ITU-T G.711 PCMU, SSRC=0x4B23294E, Seq=11109, Time=219040 |
| 2927 143.503050337 192.168.1.11 | 192.168.1.100 | RTP | 214 PT=ITU-T G.711 PCMU, SSRC=0x4BA9017D, Seq=1361, Time=3692361998 |
| 2928 143.510842602 192.168.1.100 | 192.168.1.11 | RTP | 214 PT=ITU-T G.711 PCMU, SSRC=0x4B23294E, Seq=11110, Time=219200 |
| 2929 143.523772665 192.168.1.11 | 192.168.1.100 | RTP | 214 PT=ITU-T G.711 PCMU, SSRC=0x4BA9017D, Seq=1362, Time=3692362158 |
| 2930 143.523787601 192.168.1.11 | 192.168.1.100 | RTP | 214 PT=ITU-T G.711 PCMU, SSRC=0x4BA9017D, Seq=1363, Time=3692362318 |
| 2931 143.534628314 192.168.1.100 | 192.168.1.11 | RTP | 214 PT=ITU-T G.711 PCMU, SSRC=0x4B23294E, Seq=11111, Time=219360 |
| 2932 143.550570746 192.168.1.100 | 192.168.1.11 | RTP | 214 PT=ITU-T G.711 PCMU, SSRC=0x4B23294E, Seq=11112, Time=219520 |

rame 105: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0

0 01 80 c2 00 00 00 6c 4e f6 6b dc 90 00 27 42 42IN .k...BB

eth0: alias capture in progress

Demandé le 2023 - Affiché le 2023 / 100 00%

Profile Default

Préparation de la machine attaquante

Pour l'attaque "**Man In The Middle**", la machine attaquante est préparée avec les outils nécessaires (**Wireshark**, **dsniff**) et une adresse IP configurée pour intercepter le trafic.

```
toto@p20321:~$ echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward  
1
```

■ Outils d'attaque

Installation de **Wireshark** et **dsniff**.

```
attaque@p20325:~$ sudo apt-get install dsniff -y  
Lecture des listes de paquets... Fait  
Construction de l'arbre des dépendances... Fait  
Lecture des informations d'état... Fait  
Les paquets supplémentaires suivants seront installés :  
  libnet1 libnids1.21  
Les NOUVEAUX paquets suivants seront installés :  
  dsniff libnet1 libnids1.21  
0 mis à jour, 3 nouvellement installés, 0 à enlever et 404 non  
Il est nécessaire de prendre 192 ko dans les archives.  
Après cette opération, 665 ko d'espace disque supplémentaires s  
Réception de :1 http://deb.debian.org/debian bullseye/main amd6  
  1.1.6+dfsg-3.1 [60.4 kB]
```

```
toto@p20321:~$ sudo su  
root@p20321:/home/toto# sysctl -p /etc/sysctl.conf
```

■ Configuration IP

Adresse IP de l'attaquant : **192.168.1.10**.

■ Objectif

Mettre en place une attaque **Man In The Middle**.

Mise en place de l'attaque ARP Spoofing

L'attaque **ARP Spoofing** empoisonne les **tables ARP** des victimes, faisant de l'attaquant la passerelle. Cela permet de **détourner tout le trafic VoIP** à travers la machine de l'attaquant.

Lancement de l'attaque

Utilisation d'**outils** pour empoisonner l'ARP

ARPspoof pour positionner la machine attaquante entre le **softphone** et le **serveur asterisk**.

Empoisonnement de la table ARP

→ L'attaquant devient **passerelle**

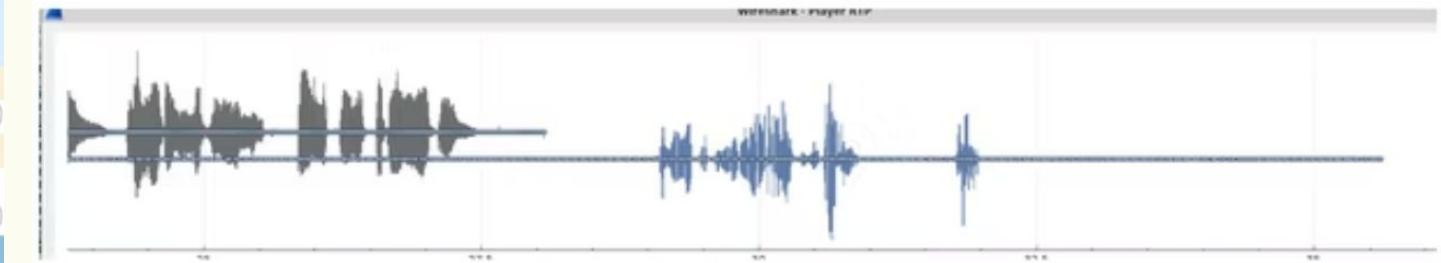
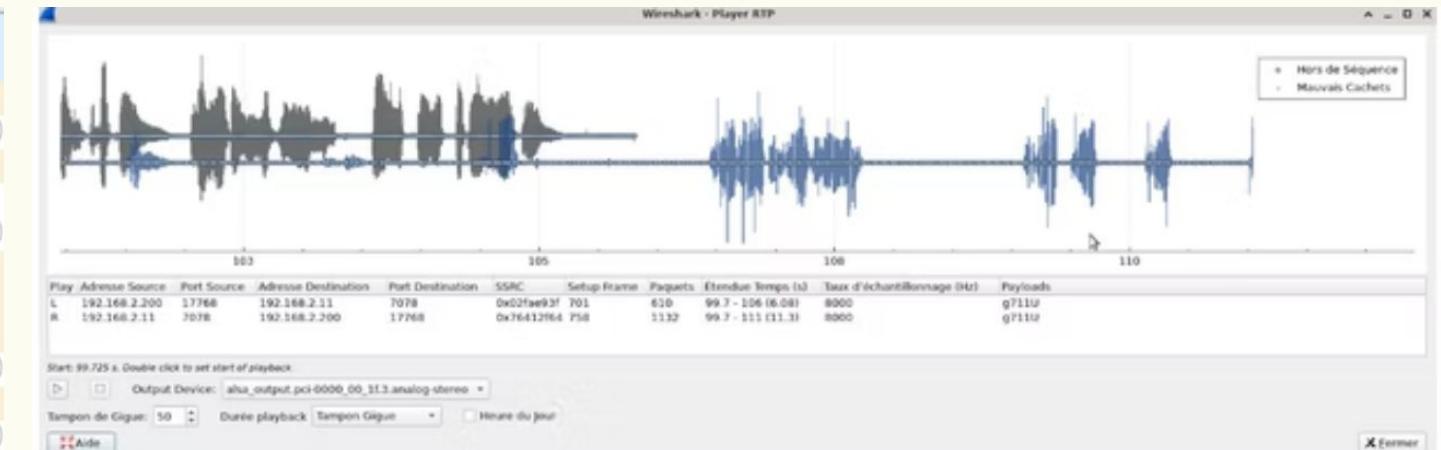
→ Détournement du trafic VoIP

```
toto@p20321:~$ sudo arp -a
[sudo] Mot de passe de toto :
? (192.168.1.100) at 24:9a:d8:1e:43:10 [ether] on eth0
? (192.168.1.200) at 40:a6:b7:81:ad:39 [ether] on eth0
? (192.168.53.254) at 00:15:17:ef:57:42 [ether] on eth1
? (192.168.1.20) at <incomplete> on eth0
? (192.168.1.11) at 40:a6:b7:81:a8:8b [ether] on eth0
```

Interception et écoute des appels

- ❑ Avec l'attaque en place, **Wireshark** sur la machine attaquante capture les **flux SIP et RTP**. Le décodage des **flux RTP** permet ensuite d'écouter le **message vocal intercepté**.

| | | | | | |
|------|--------------|-------------------|-----------------------|------|---|
| 3829 | 47.797495012 | 192.168.1.11 | 192.168.1.200 | UDP | 46 5060 → 5060 Len=4 |
| 3830 | 47.797518174 | 192.168.1.11 | 192.168.1.100 | UDP | 46 5060 → 5060 Len=4 |
| 3831 | 48.100958321 | IntelCor_81:ad:38 | IntelCor_81:a8:8b | ARP | 60 192.168.1.200 is at 40:a6:b7:81:ad:38 |
| 3832 | 49.641901815 | 6c:4e:f6:6b:dc:90 | Spanning-tree-(for... | STP | 60 RST, Root = 32768/1/6c:4e:f6:6b:dc:80 Cost = 0 |
| 3833 | 50.101117579 | IntelCor_81:ad:38 | IntelCor_81:a8:8b | ARP | 60 192.168.1.200 is at 40:a6:b7:81:ad:38 |
| 3834 | 51.554740627 | 6c:4e:f6:6b:dc:90 | 6c:4e:f6:6b:dc:90 | LOOP | 60 Reply |
| 3835 | 51.649055972 | 6c:4e:f6:6b:dc:90 | Spanning-tree-(for... | STP | 60 RST, Root = 32768/1/6c:4e:f6:6b:dc:80 Cost = 0 |
| 3836 | 52.101262144 | IntelCor_81:ad:38 | IntelCor_81:a8:8b | ARP | 60 192.168.1.200 is at 40:a6:b7:81:ad:38 |
| 3837 | 52.901815116 | IntelCor_81:a8:8b | YealinkX_1e:43:10 | ARP | 42 Who has 192.168.1.100? Tell 192.168.1.11 |
| 3838 | 52.902797280 | YealinkX_1e:43:10 | IntelCor_81:a8:8b | ARP | 60 192.168.1.100 is at 24:9a:d8:1e:43:10 |
| 3839 | 53.650361522 | 6c:4e:f6:6b:dc:90 | Spanning-tree-(for... | STP | 60 RST, Root = 32768/1/6c:4e:f6:6b:dc:80 Cost = 0 |
| 3840 | 54.101443579 | IntelCor_81:ad:38 | IntelCor_81:a8:8b | ARP | 60 192.168.1.200 is at 40:a6:b7:81:ad:38 |
| 3841 | 55.650246616 | 6c:4e:f6:6b:dc:90 | Spanning-tree-(for... | STP | 60 RST, Root = 32768/1/6c:4e:f6:6b:dc:80 Cost = 0 |
| 3842 | 56.101595367 | IntelCor_81:ad:38 | IntelCor_81:a8:8b | ARP | 60 192.168.1.200 is at 40:a6:b7:81:ad:38 |
| 3843 | 57.654277764 | 6c:4e:f6:6b:dc:90 | Spanning-tree-(for... | STP | 60 RST, Root = 32768/1/6c:4e:f6:6b:dc:80 Cost = 0 |
| 3844 | 57.797450853 | 192.168.1.11 | 192.168.1.200 | UDP | 46 5060 → 5060 Len=4 |
| 3845 | 57.797469485 | 192.168.1.11 | 192.168.1.100 | UDP | 46 5060 → 5060 Len=4 |
| 3846 | 58.101648135 | IntelCor_81:ad:38 | IntelCor_81:a8:8b | ARP | 60 192.168.1.200 is at 40:a6:b7:81:ad:38 |
| 3847 | 59.658539113 | 6c:4e:f6:6b:dc:90 | Spanning-tree-(for... | STP | 60 RST, Root = 32768/1/6c:4e:f6:6b:dc:80 Cost = 0 |
| 3848 | 60.101778392 | IntelCor_81:ad:38 | IntelCor_81:a8:8b | ARP | 60 192.168.1.200 is at 40:a6:b7:81:ad:38 |
| 3849 | 61.555210581 | 6c:4e:f6:6b:dc:90 | 6c:4e:f6:6b:dc:90 | LOOP | 60 Reply |
| 3850 | 61.658470571 | 6c:4e:f6:6b:dc:90 | Spanning-tree-(for... | STP | 60 RST, Root = 32768/1/6c:4e:f6:6b:dc:80 Cost = 0 |
| 3851 | 62.101933148 | IntelCor_81:ad:38 | IntelCor_81:a8:8b | ARP | 60 192.168.1.200 is at 40:a6:b7:81:ad:38 |



Protection contre l'interception des appels

VoIP

Chiffrement des communications

Utiliser le protocole **SRTP (Secure Real-time Transport Protocol)** pour chiffrer les flux et rendre les données inintelligibles en cas d'interception.

Authentification forte

Mettre en place des authentification robustes pour les utilisateurs et les appareils, tels que l'**authentification mutuelle TLS**, afin d'éviter les accès non autorisés.

Segmentation réseau

Isoler le trafic VoIP sur un **VLAN** pour limiter l'exposition et la portée des attaques au sein du réseau.

Surveillance et détection d'intrusion

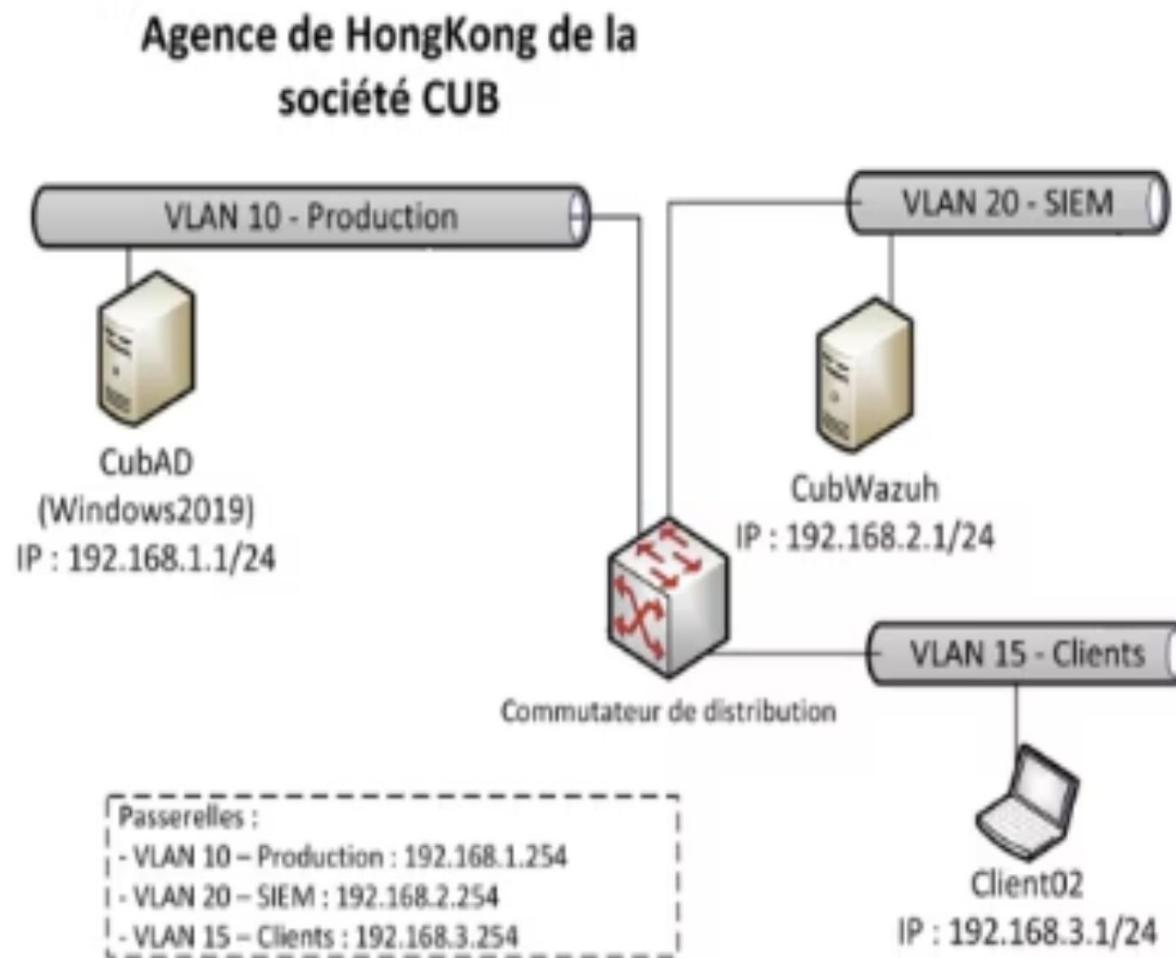
Déployer des **IDS** pour surveiller le trafic réseau et alerter en cas de tentatives d'interception.

Difficultés rencontrés lors de cette SAE :

- Problème de connexion entre les machines
- on avait soit internet soit les machines connectés à travers eth0 du coup ça nous a freinés durant les trois premières séances et on n'a pas pu avancer
- on a finalement réussi à résoudre le problème et à terminer la SAE

Partie 2 :Création et Analyse avec un SIEM Wazuh

Déploiement, Audit de Conformité et Gestion des Vulnérabilités



L'objectif est d'identifier les vulnérabilités de chaque machine (windows et linux) , de les observer sur le SIEM et de les corriger

Architecture Réseau et Connectivité

Infrastructure de Routage

- Switch Cisco de niveau 3 inter-VLAN activé.
- Segmentation par VLANs : 10 (Production), 15 (Client), 20 (SIEM).
- Routage inter-VLAN activé.



```
/dev/ttyUSB0 - PuTTY (sur p20329) ^ _ □ x

Gi1/0/13, Gi1/0/14, Gi1/0/15
Gi1/0/16, Gi1/0/17, Gi1/0/18
Gi1/0/19, Gi1/0/20, Gi1/0/21
Gi1/0/22, Gi1/0/23, Gi1/0/24
Gi1/0/25, Gi1/0/26, Gi1/0/27
Gi1/0/28

10  vlan_AD
15  CLIENTS
20  vlan_WAZUH
1002 fddi-default
1003 token-ring-default
1004 fddinet-default
1005 trnet-default
Switch#sh ip int br
Interface          IP-Address      OK? Method Status      Protocol
Vlan1              unassigned     YES NVRAM  up        down
Vlan10             192.168.1.254  YES NVRAM  up        up
Vlan15             192.168.3.254  YES NVRAM  up        up
Vlan20             192.168.2.254  YES NVRAM  up        up
GigabitEthernet1/0/1 unassigned    YES unset   up        up
```

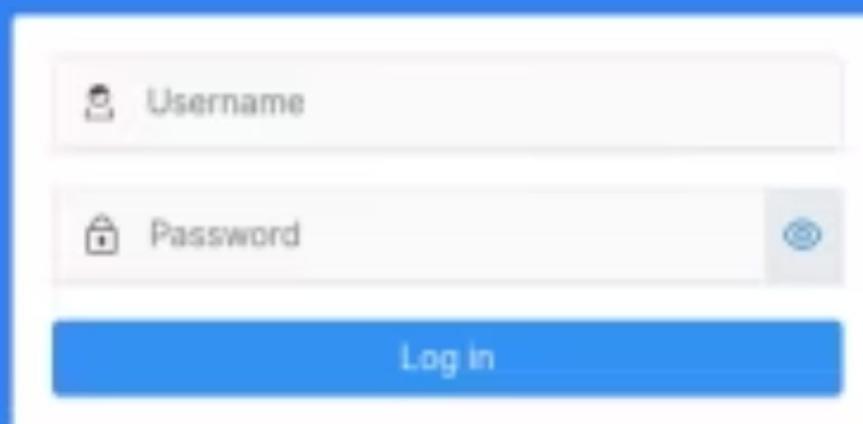
Configuration des VMs

- Adaptateurs réseau en mode Bridge ou Accès.
- Adresses IP statiques pour une liaison Manager constante.

| Machine | VLAN | @ physique | Masque | Passerelle(Gateway) |
|-----------------|------|-------------|--------|---------------------|
| CubAD | 10 | 192.168.1.2 | /24 | 192.168.1.254 |
| Client02 | 15 | 192.168.3.2 | /24 | 192.168.3.254 |
| CubWazuh | 20 | 192.168.2.3 | /24 | 192.168.2.254 |

Speech Dispatcher library is missing. [Learn more](#)[Don't show again](#)The Wazuh logo, featuring the word "wazuh." in a large, white, sans-serif font with a black dot on the "h".

The Open Source Security Platform



A screenshot of the Wazuh login interface. It features a blue header with the Wazuh logo and text. Below is a white login form with two input fields: "Username" and "Password", each with a corresponding icon (user and lock). A "Log In" button is at the bottom.

Déploiement de la Solution Wazuh

Méthode d'installation sur Ubuntu Server 22.04 (VLAN 20).

Rôle des Composants

Manager : Analyse des logs et application des règles.

Indexer : Stockage et recherche des événements.

Dashboard : Visualisation et interface de gestion.

Agents Déployés

- Windows Server 2019 (VLAN 10 - CubAD).
- Ubuntu Client (VLAN 15 - Poste utilisateur).

Déploiement et Configuration des Agents Wazuh



Installation Manuelle

Déploiement manuel des agents sur les systèmes cibles.

Ubuntu (VLAN 15) : paquet .deb.

Windows (VLAN 10) : exécutable .msi.



Configuration ossec.conf

Modifier le fichier `ossec.conf` sur l' agent Ubuntu.

Action : Renseigner l'IP du Manager (192.168.2.1) pour l'enregistrement et la remontée des journaux.



Validation sur le Dashboard

Résultat :

| Agents (2) | | | | | | | |
|---------------|---------------------|------------------------|--------------------|--|--------------------|----------|--------------|
| | | Show only outdated (1) | + Deploy new agent | ⟳ Refresh | 💾 Export formatted | More ▾ | ⚙️ |
| status=active | | | | | | | |
| ID ↑ | Name | IP address | Group(s) | Operating system | Cluster node | Version | Status |
| 004 | WIN-2I1AIV O6ADI | 192.168.1. 1 | default | Microsoft Windows Server 2019 Standard Evaluation 10.0.17763.3650 | node01 | v4.7.2 ● | active ⓘ ⓘ ⓘ |
| 005 | client15-VirtualBox | 192.168.3. 1 | default | Ubuntu 22.04.3 LTS | node01 | v4.11.2 | active ⓘ ⓘ ⓘ |

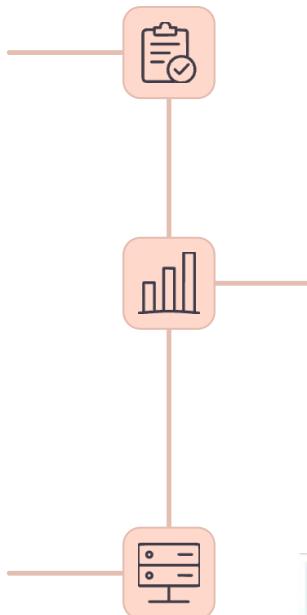
```
: GNU nano 6.2 /var/ossec/etc/ossec.conf
<!--
Wazuh - Agent - Default configuration for ubuntu 22.04
More info at: https://documentation.wazuh.com
Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>
  <client>
    <server>
      <address>192.168.2.1</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>ubuntu, ubuntu22, ubuntu22.04</config-profile>
    <notify_time>20</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
    <crypto_method>aes</crypto_method>
  </client>
[ 201 lignes écrits ]
^G Aide ^O Écrire ^W Chercher ^K Couper ^T Exécuter ^C Emplacement
^X Quitter ^R Lire fich. ^Y Remplacer ^U Coller ^J Justifier ^/ Aller ligne
```

Audit de Conformité (SCA)

Vérifier le durcissement des systèmes selon les benchmarks

Objectif



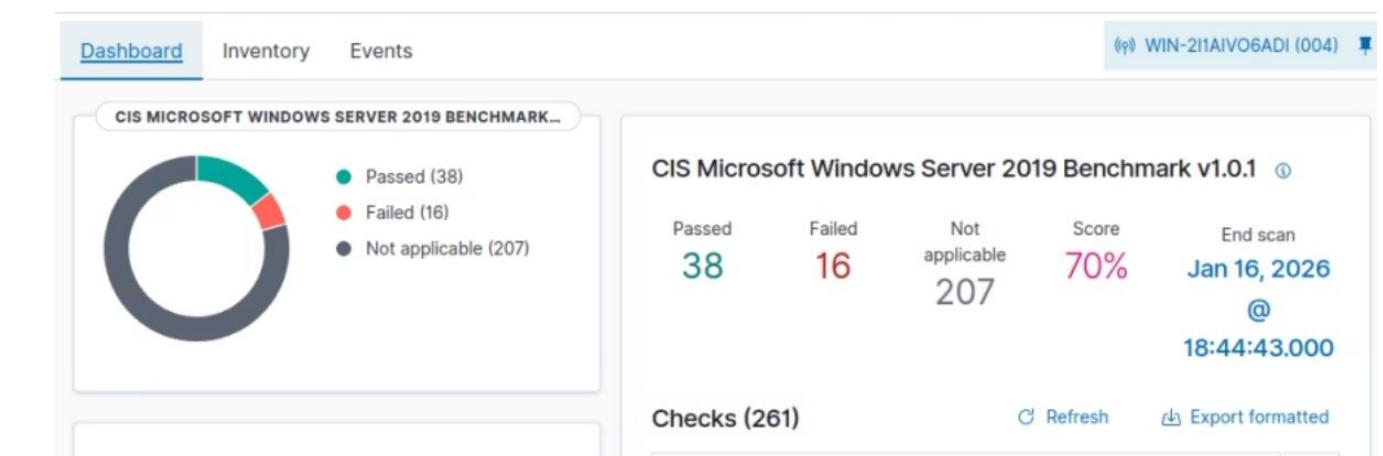
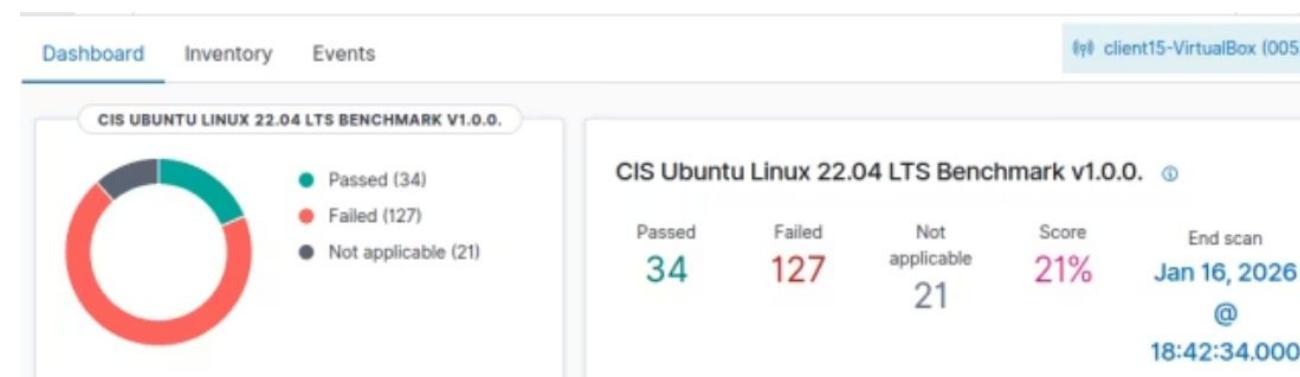
Analyse des scores

(Tests réussis vs fails).

Moins de failles=politiques de sécurité proches des recommandations

Difference Windows/Linux

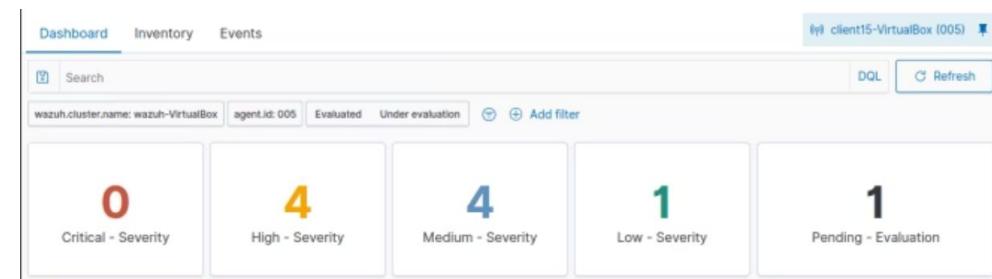
- Complexité supérieure de Windows Server.
- Politiques de sécurité spécifiques à chaque noyau.
 - Wazuh adapte ses tests : il cherche des clés de registre sur Windows et des lignes de commande sur Linux.



Gestion des Vulnérabilités

Vulnérabilités

Relevées : Failles logiciel sur policykit-1 et libpoppler.

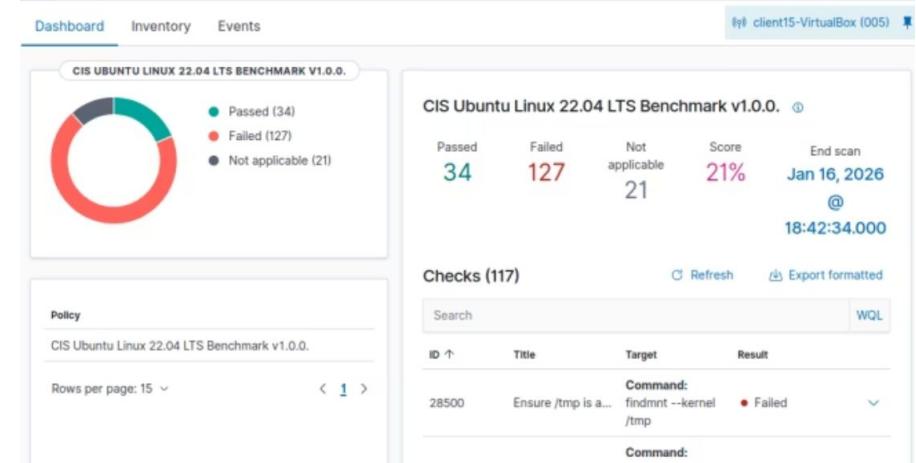


Windows : Failles d'élévation de priviléges (ex: CVE-2025-21419).



Analyse

Distinction entre vulnérabilités logicielles (failles connues) et de configuration système (mdp trop simple).



Remédiation et Résultats

Actions Correctives

Ubuntu : Succès via `sudo pro fix CVE-2020-25686.` (méthode proposée par le SIEM)

The screenshot shows the Canonical Ubuntu Security interface. On the left, there's a sidebar with 'Vulnerability details' containing fields like 'vulnerability.enumeration' (CVE), 'vulnerability.id' (CVE-2024-56431), 'vulnerability.published_at' (Dec 25, 2024 @ 18:15:05.000), and 'vulnerability.reference' (links to https://ubuntu.com/security/CVE-2024-56431 and https://www.cve.org/CVERecord?id=CVE-2024-56431). The main content area displays 'CVE-2024-56431' with publication date (Dec 25, 2024), last updated (26 August 2025), Ubuntu priority (Medium), and CVSS 3 Severity Score (9.8 - Critical). It also includes a 'Description' section with a note about a bug in libtheora.

This screenshot shows the 'Fix a specific CVE with the Ubuntu Pro Client' documentation. It explains how to use the 'Ubuntu Pro Client installed, updated and set up.' to run the command `sudo pro fix CVE-YYYY-XXXX`. A note states that if the update is already installed, it will be skipped.

```
client15@client15-VirtualBox:~$ sudo pro fix CVE-2020-25686
CVE-2020-25686: Dnsmasq vulnerabilities
- https://ubuntu.com/security/CVE-2020-25686
1 affected source package is installed: dnsmasq
(1/1) dnsmasq:
A fix is available in Ubuntu standard updates.
The update is already installed.

✓ CVE-2020-25686 is resolved.
client15@client15-VirtualBox:~$ sudo pro fix CVE-2022-3219
CVE-2022-3219:
```

Windows : Patchs identifiés (MSRC).

Vérification Finale

Baisse du nombre de vulnérabilités sur le Dashboard.

Validation de l'efficacité des mises à jour.

The dashboard shows a summary of vulnerabilities: Critical - Severity (0), High - Severity (4), Medium - Severity (0), Low - Severity (0), and Pending - Evaluation (0). The search bar shows 'wazuh.cluster.name: wazuh-VirtualBox agent.id: 005'. The top navigation bar includes 'Dashboard', 'Inventory', 'Events', and a search bar.

CVE d'une vulnérabilité critique : ces vulnérabilités font partie des TOP 5 vulnérabilités comme mentionné dans le dashboard du SIEM

The dashboard displays the 'Top 5 vulnerabilities' and 'Top 5 OS'. The 'Top 5 vulnerabilities' table shows CVE-2024-56431 (Count 1), CVE-2022-26923, and CVE-2023-36025 (Count 1). The 'Top 5 OS' table shows Microsoft Windows Server 2019 Standard, Ubuntu 22.04.3 LTS (Jammy), and Ubuntu 20.04.6 LTS (Focal Fossa). Both tables include 'Filter for value' and 'Filter out value' buttons.

Remédiation de la parties windows

Quelques captures décrivant le processus qu'on a suivi

Identification de la vulnérabilité à partir du dashboard du SIEM

| Vulnerability details | |
|----------------------------------|---|
| t vulnerability.description | Windows Setup Files Cleanup Elevation of Privilege Vulnerability |
| ▀ vulnerability.detected_at | Jan 16, 2026 @ 18:39:33.052 |
| t vulnerability.enumeration | CVE |
| t vulnerability.id | CVE-2025-21419 |
| ▀ vulnerability.published_at | Feb 11, 2025 @ 19:15:40.000 |
| t vulnerability.reference | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21419 |
| t vulnerability.scanner.source | National Vulnerability Database |
| t vulnerability.scanner.vendor | Wazuh |
| # vulnerability.score.base | 7.1 |
| t vulnerability.score.version | 3.1 |
| t vulnerability.severity | High |
| ⌚ vulnerability.under_evaluation | false |
| t wazuh.cluster.name | wazuh-VirtualBox |
| t wazuh.schema.version | 1.0.0 |

En cliquant sur le lien de la section “vulnerability reference” ça nous ramène à la page de remédiation de la vulnérabilité windows

| Vulnérabilité d’élévation de privilèges dans le nettoyage de fichiers de l’installation de Windows | |
|--|-------------------------|
| CVE-2025-21419 | Security Vulnerability |
| Date de publication : Feb 11, 2025 | |
| Assigning CNA: Microsoft | |
| CVE.org link: CVE-2025-21419 | |
| Impact: Élévation de privilèges | Gravité max.: Important |
| Weakness: CWE-59: Improper Link Resolution Before File Access ('Link Following') | |
| CVSS Source: Microsoft | |
| Chaîne vectorielle: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H/E:F/RL:O/RC:C | |
| Metrics: CVSS:3.1 7.1 / 6.6 | |
| Metric | Value |
| ▼ Métriques de score de base (8) | |
| ► Vecteur d’attaque | ► Locale |
| ► Complexité d’attaque | ► Faible |
| ► Priviléges requis | ► Faible |
| ► Intervention de l’utilisateur | ► Aucune |

| | | | | | | | | | |
|--------------|--|---|------------------------|-----------|-------------------------|---------------------------------|-----------------|-----------|----------|
| Feb 11, 2025 | Windows Server 2019 (Server Core installation) | - | Elevation of Privilege | Important | 5052000 | Security Update | 10.0.17763.6893 | Microsoft | Required |
| Feb 11, 2025 | Windows Server 2019 | - | Elevation of Privilege | Important | 5052000 | Security Update | 10.0.17763.6893 | Microsoft | Required |

| Titre | |
|---|---------------------|
| 2025-02 Mise à jour cumulative pour Windows 10 Version 1809 pour les systèmes x86 (KB5052000) | Windows 10 LTSB |
| 2025-02 Mise à jour cumulative pour Windows Server 2019 pour les systèmes x64 (KB5052000) | Windows Server 2019 |
| 2025-02 Mise à jour cumulative pour Windows 10 Version 1809 pour les systèmes x64 (KB5052000) | Windows 10 LTSB |

Problèmes rencontrés et Adaptation (Kali)



Incapacité matérielle

Le réseau IUT possédant un FW cela a rendu la machine Kali inexploitable.

Rôle initial

Threat Hunting : attaques simulées et scans offensifs.

Décision

Abandon de la partie offensive pour se concentrer sur le **Blue Teaming** (Défense et Audit de conformité).



Conclusion de la Partie 3

Bilan Technique

Maîtrise du flux de supervision dans un environnement segmenté par VLANs.

Analyse Critique

Le SIEM a permis de transformer une visibilité floue en une liste d'actions prioritaires.