Ce cours

Commencé le	mardi 11 avril 2023, 19:15
État	Terminé
Terminé le	vendredi 21 avril 2023, 14:02
Temps mis	9 jours 18 heures
Note	20,50 sur 23,00 (89,13%)

QUESTION 1

Terminé

Non noté

Prénom et nom des étudiants ayant contribué au labo :

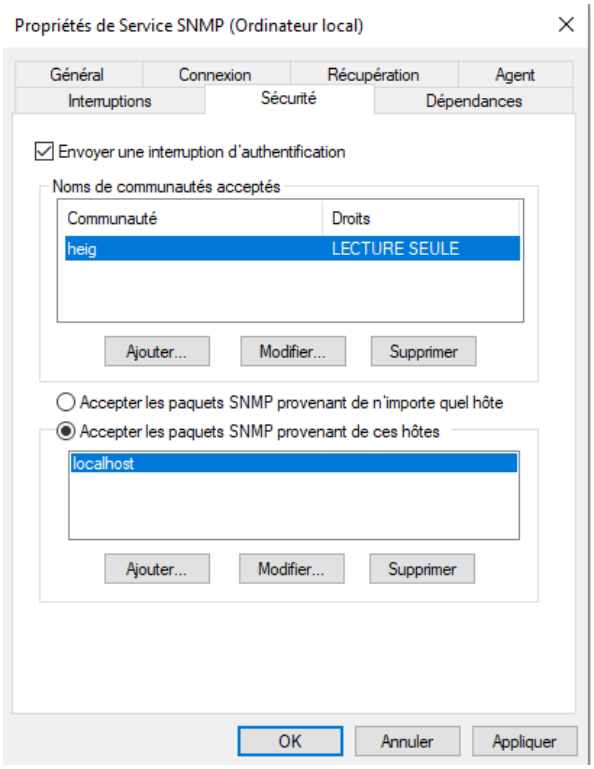
Alexis Martins

QUESTION 2

Terminé

Note de 1,00 sur 1,00

Montrez à l'aide de captures d'écran les changements de configuration que vous avez réalisés



Commentaire :

QUESTION 3

Terminé

Note de 0,50 sur 1,00

Montrez les valeurs retournées par les 5 objets SysDescr, SysName, SysUpTime, ifNumber, et l'adresse IP de votre cible.

```
-----SNMP query started-----
1: sysDescr.0 Hardware: Intel64 Family 6 Model 140 Stepping 1 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 19045 M
2: sysObjectID.0 enterprises.311.1.1.3.1.1
3: sysUpTime.0 0:24:49.00
4: sysContact.0
5: sysName.0 win10-GRS-A
6: sysLocation.0
7: sysServices.0 76
-----SNMP query finished-----
Total # of Requests = 1
Total # of Objects = 8
```


```
-----SNMP query started-----
1: ipAdEntAddr.127.0.0.1 127.0.0.1
2: ipAdEntAddr.192.168.81.10 192.168.81.10
-----SNMP query finished-----
Total # of Requests = 1
Total # of Objects = 3
```

Commentaire :

Ces valeurs sont-elles correctes par rapport à la "réalité" ?

QUESTION 4

Terminé

Note de 1,00 sur 1,00

Montrez la configuration du routeur cisco de manière à ce qu'il puisse être géré via SNMPv2 (choisissez cisco pour community string RO et ciscorw pour community string RW). Configurez également le routeur pour qu'il envoie ses traps snmp au manager SNMPb sur Windows A. Prévoyez la synchro temps et l'affichage des événements en ms.

```
ntp server ch.pool.ntp.org
service timestamps debug datetime msec
snmp-server community ciscoRO RO 1
snmp-server community ciscoRW RW 1
snmp-server enable traps
snmp-server host 192.168.81.10 version 2c ciscoRO
```

Commentaire :
A quoi sert le string ciscoRO de la dernière ligne ?

QUESTION 5

Terminé

Note de 1,00 sur 1,00

Montrez les valeurs retournées par les 5 objets SysDescr, SysName, SysUpTime, sysObjectID, et l'adresse IP de votre cible.

```
-----SNMP query started-----
1: sysDescr.0 Cisco IOS Software [Amsterdam], Virtual XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 17.3.2, RELEAS
2: sysObjectID.0 enterprises.9.1.1537
3: sysUpTime.0 0:06:08.53
4: sysContact.0
5: sysName.0 GRS_rtr
6: sysLocation.0
7: sysServices.0 78
8: sysORLastChange.0 0:00:00.00
-----SNMP query finished-----
Total # of Requests = 1
Total # of Objects = 9
```

```
-----SNMP query started-----
1: ifNumber.0 5
-----SNMP query finished-----
Total # of Requests = 1
Total # of Objects = 1
```

```
-----SNMP query started-----
1: ipAdEntAddr.192.168.81.1 192.168.81.1
-----SNMP query finished-----
Total # of Requests = 1
Total # of Objects = 2
```

Commentaire :

QUESTION 6

Terminé

Note de 0,50 sur 1,00

A quoi sert/correspond la valeur retournée par sysObjectID ? Que vous manque-t-il pour l'interpréter correctement ?

La valeur retournée par `sysObjectID` est un identifiant unique représentant le type et le fabricant d'un équipement réseau dans le cadre du protocole SNMP. Pour l'interpréter correctement, il est nécessaire de disposer d'une base de données ou d'un dictionnaire d'OIDs associant ces identifiants aux équipements et fabricants correspondants.

Commentaire :
-> MIB

QUESTION 7

Terminé

Note de 1,00 sur 1,00

A l'aide de Wireshark, capturez et présentez de manière lisible les trames lorsque la machine Windows 10 interroge le routeur Cisco pour obtenir le nom de l'équipement (les champs concernant SNMP doivent être visibles et commentés).

No.	Time	Source	Destination	Protocol	Lengtr	Info
18	16.862386377	192.168.81.10	192.168.81.1	SNMP	84	get-request 1.3.6.1.2.1.1.5.0
19	16.864717736	192.168.81.1	192.168.81.10	SNMP	91	get-response 1.3.6.1.2.1.1.5.0

```
> Frame 18: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface vmnet8, id 0
> Ethernet II, Src: VMware_ad:89:b0 (00:0c:29:ad:89:b0), Dst: VMware_73:47:23 (00:0c:29:73:47:23)
> Internet Protocol Version 4, Src: 192.168.81.10, Dst: 192.168.81.1
> User Datagram Protocol, Src Port: 53470, Dst Port: 161
v Simple Network Management Protocol
    version: v2c (1)
    community: ciscoRO
  v data: get-request (0)
    v get-request
        request-id: 1055
        error-status: noError (0)
        error-index: 0
      v variable-bindings: 1 item
        v 1.3.6.1.2.1.1.5.0: Value (Null)
            Object Name: 1.3.6.1.2.1.1.5.0 (iso.3.6.1.2.1.1.5.0)
            Value (Null)
    [Response In: 19]
```

```
> Frame 19: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface vmnet8, id 0
> Ethernet II, Src: VMware_73:47:23 (00:0c:29:73:47:23), Dst: VMware_ad:89:b0 (00:0c:29:ad:89:b0)
> Internet Protocol Version 4, Src: 192.168.81.1, Dst: 192.168.81.10
> User Datagram Protocol, Src Port: 161, Dst Port: 53470
v Simple Network Management Protocol
    version: v2c (1)
    community: ciscoRO
  v data: get-response (2)
    v get-response
        request-id: 1055
        error-status: noError (0)
        error-index: 0
      v variable-bindings: 1 item
        v 1.3.6.1.2.1.1.5.0: "GRS_rtr"
            Object Name: 1.3.6.1.2.1.1.5.0 (iso.3.6.1.2.1.1.5.0)
          > Value (OctetString): "GRS_rtr"
    [Response To: 18]
    [Time: 0.002331359 seconds]
```

On remarque pour le get la version du protocole utilisée, ainsi que le community string utilisée. On remarque aussi l'OID qui est cherché par le get.

Dans ce cas, on voit l'OID qui correspond au nom de l'appreil, ainsi que la valeur de cette attribut.

Pour la réponse, c'est presque similaire sauf que l'on retrouve la valeur de réponse.

Commentaire :
+request-id

QUESTION 8

Terminé

Note de 1,00 sur 1,00

Montrez et analysez l'échange de messages capturés par Wireshark lors du changement de nom (*hostname*) de votre routeur,

```
> Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface vmnet8, id 0
> Ethernet II, Src: VMware_ad:89:b0 (00:0c:29:ad:89:b0), Dst: VMware_73:47:23 (00:0c:29:73:47:23)
> Internet Protocol Version 4, Src: 192.168.81.10, Dst: 192.168.81.1
> User Datagram Protocol, Src Port: 53470, Dst Port: 161
v Simple Network Management Protocol
    version: v2c (1)
    community: ciscoRW
  v data: set-request (3)
    v set-request
        request-id: 1059
        error-status: noError (0)
        error-index: 0
      v variable-bindings: 1 item
        v 1.3.6.1.2.1.1.5.0: "router-martins"
            Object Name: 1.3.6.1.2.1.1.5.0 (iso.3.6.1.2.1.1.5.0)
          > Value (OctetString): "router-martins"
    [Response In: 21]
```

```
> Frame 21: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface vmnet8, id 0
> Ethernet II, Src: VMware_73:47:23 (00:0c:29:73:47:23), Dst: VMware_ad:89:b0 (00:0c:29:ad:89:b0)
> Internet Protocol Version 4, Src: 192.168.81.1, Dst: 192.168.81.10
> User Datagram Protocol, Src Port: 161, Dst Port: 53470
v Simple Network Management Protocol
    version: v2c (1)
    community: ciscoRW
  v data: get-response (2)
    v get-response
        request-id: 1059
        error-status: noError (0)
        error-index: 0
      v variable-bindings: 1 item
        v 1.3.6.1.2.1.1.5.0: "router-martins"
            Object Name: 1.3.6.1.2.1.1.5.0 (iso.3.6.1.2.1.1.5.0)
          > Value (OctetString): "router-martins"
    [Response To: 8]
    [Time: 6.206439996 seconds]
```

La première capture concerne le set. On voit l'objet qui doit être modifiée, ainsi que la nouvelle valeur qu'on lui associe.

Dans la seconde capture, c'est la réponse du routeur qui nous "confirme" que la valeur a bien été attribuée.

Commentaire :

QUESTION 9

Terminé

Note de 1,00 sur 1,00

Montrez les messages (traps) reçus par l'application SNMPb.

Commentaire :
Quel événement source ?

QUESTION 10

Terminé

Note de 1,00 sur 1,00

Analysez les trames de la capture précédente et décodez la signification des différents messages SNMP en recherchant la signification du « OID code » à l'aide du SNMP Object Navigator Cisc

1.3.6.1.2.1.1.3.0 : sysUpTimeInstance

1.3.6.1.4.1.9.9.43.2.0.1 : ciscoConfigManEvent

Le reste des OID affichés n'avaient pas d'informations dans leur base de données.

Commentaire :
1.3.6.1.4.1.9.9.43.1.1.6.1.3.**1** = **2** (**.1** = index d'événement **2** = via snmp)

QUESTION 11

Terminé

Note de 0,50 sur 1,00

Montrez la configuration de votre routeur de manière à ce qu'il n'accepte des requêtes SNMP que de la part de votre machine Windows 10 uniquement.

acces-list 1 permit 192.168.81.10

Commentaire :

il faut appliquer cette acl à votre agent snmp ->

snmp-server community ciscoRO ro 1

QUESTION 12

Terminé

Note de 1,00 sur 1,00

Montrez le(s) fichier(s) de configuration nécessaires à la configuration de SNMP sur votre nœud Linux

Premièrement, il faut installer le service :

sudo apt install snmpd

Ensuite, il fallait modifier le fichier de configuration ci-dessous snmpd.conf

sudo vi /etc/snmp/snmpd.conf

Dans le fichier il fallait ajouter

rocommunity heig

agentAddress udp:161

Il ne fallait pas oublier aussi de commenter la ligne :
agentAddress udp:127.0.0.1:161

Finalement on exécute la commande pour redémarrer le service :

service snmpd restart

Commentaire :

QUESTION 13

Terminé

Note de 0,50 sur 1,00

Montrez le résultat dans SNMPb d'une requête permettant de connaître la durée de fonctionnement de votre nœud Linux.

```
-----SNMP query started-----
1: sysUpTime.0 0:04:11.85
-----SNMP query finished-----
Total # of Requests = 1
Total # of Objects = 1
```

Commentaire :
Est-ce bien le noeud Linux ?

QUESTION 14

Terminé

Note de 1,00 sur 1,00

Montrez la commande (cmdlet) utilisée depuis Windows pour récupérer le nom de votre routeur.

Voici le petit script PowerShell pour récupérer ces informations :

```
$SNMP = New-Object -ComObject olePrn.OleSNMP
$SNMP.open('192.168.81.1','ciscoRO',2,1000)
$RESULT = $SNMP.get('.1.3.6.1.2.1.1.5.0')
$SNMP.Close()
$RESULT
```

Le résultat ci-dessous :

Commentaire :
OK, mais plus simple avec une seule cmdlet

QUESTION 15

Terminé

Note de 1,00 sur 1,00

Montrez la commande (*cmdlet*) ou le script utilisé pour récupérer toutes les minutes la liste des processus/programmes actifs sur votre machine Windows.

J'ai trouvé deux méthodes pour faire cela donc je les mets les deux (même si la première est plus simple et suffisante).

La première utilise la cmdlet classique de PowerShell pour récupérer les processus. (Méthode validée par l'assistant)

```
While ($true)
{
   Get-Process
   Start-Sleep -Seconds 60
}
```

La seconde manière permet d'utiliser SNMP pour récupérer cette information :

```
while($true) {
   snmptable -Version 2c -Community heig -ComputerName 127.0.0.1 HOST-RESOURCES-MIB::hrSWRunTable | Select-Object -Property "hrSWRunName"
   Start-Sleep -Seconds 60
}
```

Commentaire :

QUESTION 16

Terminé

Note de 1,00 sur 1,00

Donnez la liste des fichiers MIBs que vous avez chargé et expliquez comment vous avez déterminé ce choix.

En cherchant sur Internet, je suis tombé sur un lien sur le forum Cisco (https://community.cisco.com/t5/other-network-architecture-subjects/how-to-get-dram-flash-memory-size-via-snmp/td-p/352874) qui indiquait ce qui était nécessaire et comme les télécharger via ce lien : https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2&mibName=CISCO-FLASH-MIB

J'ai donc voulu télécharger le fichier CISCO-FLASH-MIB qui semblait être celui qui me fallait, mais j'ai vu qu'il avait des dépendances avec d'autres fichiers. J'ai donc téléchargé aussi les deux dépendances qu'il me manquait CISCO-SMI et CISCO-QOS-PIB-MIB.

Résumé des téléchargements :
- CISCO-SMI (Dépendance pour flash)
- CISCO-QOS-PIB-MIB (Dépendance pour flash)
- CISCO-FLASH-MIB

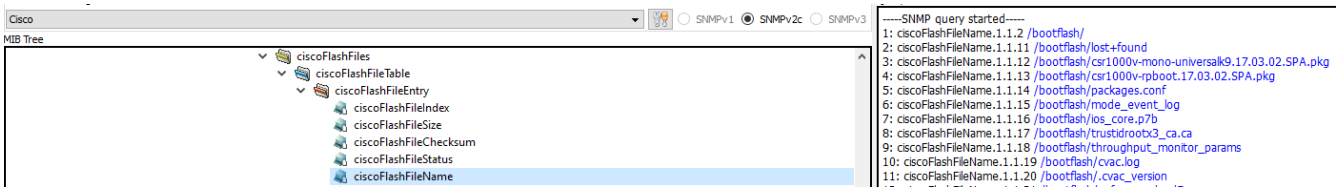
Commentaire :
CISCO-QOS-PIB-MIB : je ne suis pas certain

QUESTION 17

Terminé

Note de 1,00 sur 1,00

Montrez, via une requête SNMPb, le nom des 10 premiers fichiers stockés sur la mémoire flash de votre routeur Cisco.



Commentaire :

QUESTION 18

Terminé

Note de 1,00 sur 1,00

Montrez la configuration de votre router afin qu'il n'accepte plus que des requêtes SNMPv3 en mode authentifié et chiffré.

Dans un premier, il faut désactiver SNMPv2 sur le routeur :

no snmp-server community ciscoRO RO 1

no snmp-server community ciscoRW RW 1

no snmp-server host 192.168.81.10 version 2c ciscoRO

Ensuite, on peut activer SNMPv3 :

snmp-server group group3 v3 priv

snmp-server user user3 group3 v3 auth sha mypassword1 priv aes 128 privpassword1

snmp-server host 192.168.81.10 version 3 priv user3

Commentaire :
3ème commande pas nécessaire pour répondre à cette question.

QUESTION 19

Terminé

Note de 1,00 sur 1,00

Montrez la configuration en mode SNMPv3 de votre application SNMPb et montrer le résultat d'une requête sur la valeur SysUpTime (MIB-2) en SNMPv3.

D'abord, il faut aller dans "Options > Manage SNMPv3 USM Profiles" pour configurer le profil SNMPv3

Ensuite, on peut aller dans "Options > Manage Agent Profiles" et activer pour notre routeur CISCO SNMPv3 en cochant la case. On fini par cliquer (comme sur le screen) sur les propriétés de SNMPv3 pour finir de configurer.

Résultat final :

Commentaire :

QUESTION 20

Terminé

Note de 1,00 sur 1,00

Capturez/analysez les messages lors d'une requête SNMP v3.

Q2

Déjà on remarque que la structure des échanges est bien plus complexes. Surtout, on voit que les messages sont en effet complètement illisibles cela est dû grâce au chiffrement proposé par SNMPv3.

Commentaire :

QUESTION 21

Terminé

Note de 0,50 sur 1,00

Quelle(s) bonne(s) pratique(s) supplémentaires suggérez-vous pour sécuriser votre trafic SNMP v3 ?

En plus des configurations de bases avec SNMPv3, il est aussi possible de limiter les adresses sources de requêtes.

Il est possible de définir des vues qui sont des sous-arbres de MIB. Le but étant de restreindre l'accès à toutes les MIBs et de ne laisser aux utilisateurs que celles que ceux-ci devraient voir.

Les utilisateurs sont mis dans des groupes de sécurité et on donne accès aux vues voulues à ces groupes.

On peut aussi indiquer qu'il faut avoir des mots de passes forts.

Commentaire :
out-of-band management / VLAN

QUESTION 22

Terminé

Note de 1,00 sur 1,00

A l'aide de WMI explorer, retrouver les caractéristiques du processeur de votre VM Windows ainsi que le SID de l'utilisateur *grs.*

Montrez le résultat avec des captures d'écran.

Commentaire :

QUESTION 23

Terminé

Note de 1,00 sur 1,00

Ecrivez un script PowerShell permettant de lister, à l'aide de WMI, les partitions de la VM Windows avec leur lettre de lecteur et de retourner le pourcentage d'espace vide.

En cas d'espace insuffisant, une alarme Syslog est générée et récupérée sur votre serveur Syslog

Montrez votre script

```
# Configuration de la connexion Syslog
$syslogServer = "192.168.81.10"
$syslogPort = 514
$syslogFacility = "Local7"
$syslogPriority = "Critical"

# Seuil d'espace libre minimum en pourcentage
$freeSpaceThreshold = 70

# Récupération des partitions avec leur lettre de lecteur et leur espace libre
$partitions = Get-WmiObject Win32_Volume | Where-Object { $_.DriveLetter -ne $null -and $_.FreeSpace -ne $null -and $_.Capacity -ne $null } | Select-Object DriveLetter,FreeSpace,Capacity

# Vérification de l'espace libre pour chaque partition
foreach ($partition in $partitions) {
    $driveLetter = $partition.DriveLetter
    $freeSpace = $partition.FreeSpace
    $totalSize = $partition.Capacity
    $freeSpacePercent = [math]::Round(($freeSpace / $totalSize) * 100, 2)

    Write-Host "Partition $driveLetter : $freeSpacePercent% libre"

    # Génération d'une alarme Syslog si l'espace libre est inférieur au seuil
    if ($freeSpacePercent -lt $freeSpaceThreshold) {
        $message = "$($env:COMPUTERNAME): Espace libre insuffisant sur la partition $driveLetter : $freeSpacePercent% libre"
        Send-SyslogMessage -Server $syslogServer -Port $syslogPort -Severity $syslogPriority -Facility $syslogFacility -Message $message
    }
}
```

NB : Le Threshold est fixé assez haut, car j'avais besoin de testé. Sinon j'aurai mis un seuil plus bas.

Commentaire :

QUESTION 24

Terminé

Note de 1,00 sur 1,00

Ecrivez un script PowerShell permettant de lister, à l'aide de WMI, les partitions de la VM Windows avec leur lettre de lecteur et de retourner le pourcentage d'espace vide.

En cas d'espace insuffisant, une alarme Syslog est générée et récupérée sur votre serveur Syslog

Montrez le résultat (valeurs obtenues et message Syslog reçu)

Commentaire :

◄ LABO 2 - SNMP-WMI

Aller à...

LABO 3 - YAML NETCONF/RESTCONF ►