UNIVERSITÉ DE NANTES

IUT NANTES

LYCÉE EUGÈNE LIVET NANTES

Lycée Nicolas Appert
Enseignement général, hôtellerie, STI depuis 1989

Licence Professionnelle SEICOM

Nom : Prénom :

M3-7 - Supervision Réseau

TP N°3

Table des matières

1 - Objectifs du TP N°3

- Apprendre à utiliser des outils d'analyse réseau
- Aborder la supervision réseau via Cacti

Préparation préalable au TP : aucune

Condition de réalisation :

- Travail par binôme
- Pour chaque binôme :
    - Une station de travail par étudiant
    - Toutes les machines se branchent sur le même réseau
- Chaque binôme dispose d'un range de 3 adresses utilisables :
  Groupe 1 : 10.0.119.66 à 10.0.119.68 (/27)
  Groupe 2 : 10.0.119.70 à 10.0.119.72 (/27)
  Groupe 3 : 10.0.119.74 à 10.0.119.76 (/27)
  Groupe 4 : 10.0.119.78 à 10.0.119.80 (/27)
  Groupe 5 : 10.0.119.82 à 10.0.119.84 (/27)
  Groupe 6 : 10.0.119.86 à 10.0.119.88 (/27)

2 - Présentation générale

Le thème proposé comme support pour les TP de ce module est la mise en place d'une maquette d'infrastructure sécurité qui doit offrir les services suivants :

- Connectivité d'une filiale au SI d'une entreprise
- Connectivité Wi-Fi pour différentes populations (invités & personnel)
- Analyse et supervision réseau

3 - Fonctionnement du système

- La filiale est connectée à l'entreprise via la technologie VPN IPsec au travers d'un réseau externe.
- Les points d'accès Wi-Fi (AP) permettent à différentes populations d'utilisateurs de se connecter, chacun ayant des autorisations spécifiques une fois connecté.
- Une solution d'analyse réseau doit permettre de visualiser les flux réseaux à différents points et d'offrir des données de métrologie.

4 - Objectifs des 3 séances de travaux pratiques

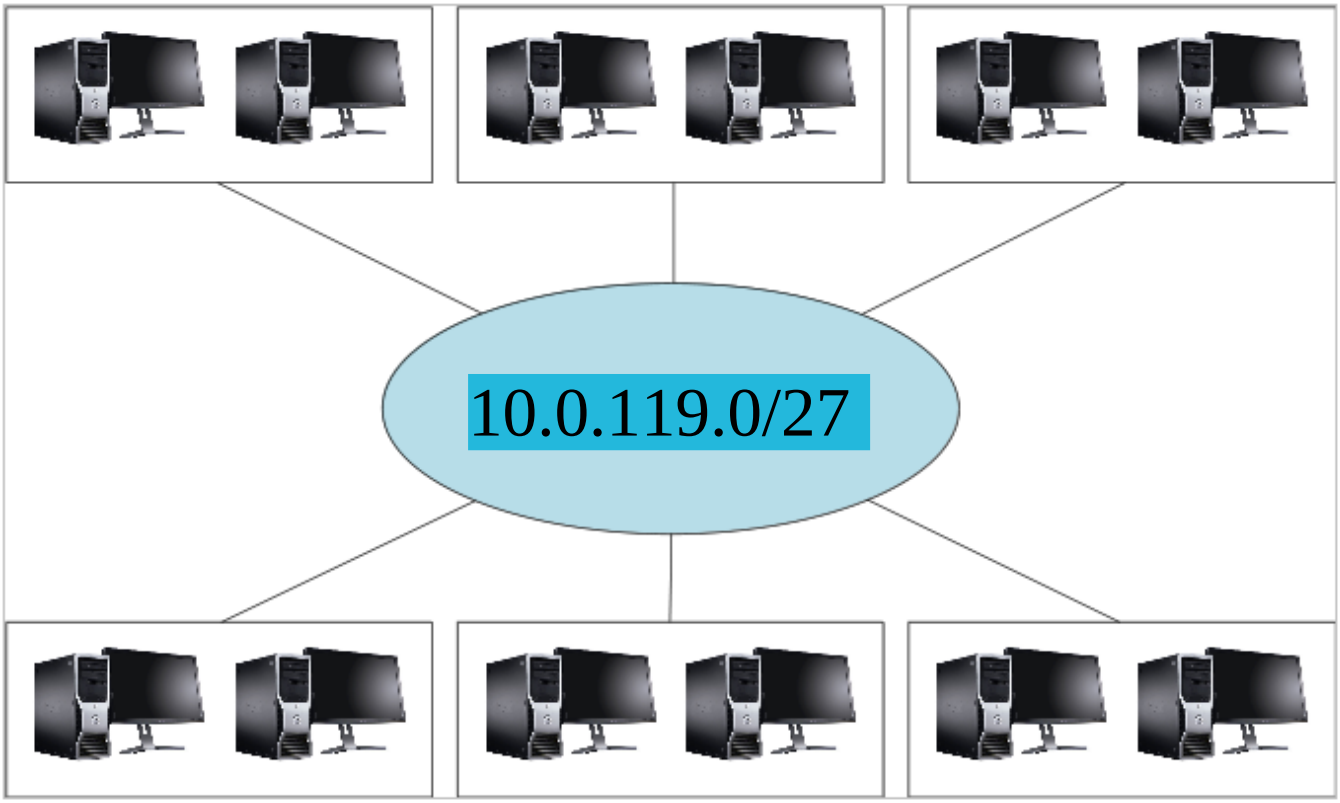
- Connaître les principaux éléments de sécurité sur un réseau informatique et leur mise en œuvre
- Comprendre les concepts de base de sécurisation d'un système d'information
- Maîtriser les méthodologies de mise en œuvre et de maintenance d'une architecture sécurité

5 - Installation des applications complémentaires

$ sudo apt-get install ntopng cacti mz nmap telnetd dsniff snmpd nuttcp iftop

1. Nouveau mot de passe du superutilisateur de MySQL : root
2. Mot de passe de l'administrateur : root
3. Type de serveur web : Apache2
4. Faut-il configurer la base de données de cacti avec dbconfig-common ? oui
5. Mot de passe de l'administrateur de la base de données : root

6 - L'architecture du TP N°3



La passerelle est en 10.0.119.65

7 - Aborder la supervision réseau via Cacti

7.1 - Configurer SNMP

Editer le fichier /etc/snmp/snmpd.conf.

- Commentez la ligne : "agentAddress udp :127.0.0.1:161"
- Décommentez la ligne : "rocommunity public localhost"
- En dessous, ajoutez la ligne : "rocommunity public 10.0.119.64/27"
- Redémarrez le service SNMP (sudo /etc/init.d/snmpd restart)

7.2 - Tester la connectivité en SNMP

Executer la commande suivante en renseignant vos paramètres :

$ snmpwalk –v 2c –c xxxxxx adresse_ip 1.3.6.1.2.1.1

- -v : version
- -c : communauté SNMP

■ Q9 : Quelles informations pouvez-vous recueillir ?

……
……

7.3 - Configurer Cacti

Pour Illustrer la capacité de création de graphes et de stockage des données de Cacti, pour ce TP nous allons collecter les informations pour les paramètres suivants de la machine de TP : charge, bande passante sur les interfaces réseaux, taux d'occupation d'un point de montage.
Cacti se configure via le navigateur : http://localhost/cacti

La première étape de configuration consiste à déclarer la machine à Cacti. Ceci se fait dans la section 'devices', ou l'on choisit 'add'. L'écran nous demande de remplir certains champs, ceux qui nous intéressent sont :

– Description : 'machine de tp'
– Hostname : addresse IP ou nom d'hôte de la machine
– Host template : Cacti possède des modèles tout faits pour certains type d'équipements, voir la liste déroulante, dans notre cas ou dans le cas d'un équipement qui n'aurait pas de modèle prêt on sélectionne 'Generic SNMP-enabled host'
– SNMP community : communauté SNMP que nous avons défini dans le snmpd.conf.
– SNMP Version : 2

On peut alors utiliser le bouton 'create' qui va créer en arrière-plan la configuration de Cacti pour cet hôte. Si vous retournez dans la console globale, dans 'Devices', vous devriez voir la machine que vous venez de déclarer.

Maintenant il faut dire à Cacti quoi monitorer sur cette machine. Toujours dans 'Devices', sélectionner la machine en cliquant sur son nom.

Première information, si votre agent SNMP est bien configuré, vous devriez voir le descriptif de la machine dans le coin supérieur gauche.

Plus bas sur cet écran nous allons configurer ce qui doit être monitoré dans les sections : 'associated graphs templates' et 'associated data queries'. Les graphes templates vous permettront en choisissant simplement dans la liste et en faisant 'add' un type de graphique prédéfini. Le nom des templates est suffisamment explicite. Choisissez certains templates judicieux pour monitorer votre machine.

Les data queries comportent des modèles de requêtes que Cacti va effectuer, mais il n'en exploitera que la partie spécifiée dans la configuration. Un exemple : la requête 'SNMP get mounted partitions' récupérera toutes les partitions montées, à nous ensuite

de choisir lesquelles ont souhaite grapher. Parmi les data queries intéressantes que l'on va sélectionner : 'SNMP get mounted partitions' ; 'SNMP Interface statistics' . Sauvez votre configuration avec 'Save'.

Pour l'instant Cacti collecte des informations sur les paramètres que nous lui avons précisé, par contre il ne nous les affiche pas encore sous forme de graphiques. Toujours dans l'écran d'un hôte, dans le coin supérieur droit utilisez 'Create graphs for this host'.

Vous obtenez un écran qui synthétise tout ce que Cacti collecte, il suffit de sélectionner les lignes adéquates et de faire 'create' pour qu'il construise les bons graphes.

Enfin dernière étape, ranger les données. Cacti permet de classer les vues de graphiques en arbre, dans la console sous 'graphs tree', l'utilisation est très intuitive.

Ajoutez ainsi les machines de chaque binôme et organisez les graphiques.

NOTE : Cacti met parfois du temps avant de pouvoir afficher les graphes (le temps de la collecte – soit parfois plus de 30 minutes). Si c'est le cas, passez à la suite et revenez commenter les résultats sur Cacti après.

Q10 : Que pouvez-vous conclure quant à l'utilisation de ce type d'outil ?

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

8 - Apprendre à utiliser des outils d'analyse réseau

8.1 - Analyse du « bruit de fond »

Connectez-vous à votre sonde NTOP : http://localhost:3000
Note : Il est également possible d'utiliser *DarkStat*.

En allant dans la partie Dashboard :

- Q1 : Quel est le top 5 des ports présents dans les communications :
  ……
- Q2 : Quel est le top 5 des applications présentes :
  ……

8.2 - Générer du trafic HTTP

Avec l'application MZ, générer du trafic avec les caractéristiques suivantes :

- Adresse IP source : 10.0.119.X
- Adresse IP destination : 10.0.119.X
- Port destination : tcp / 80
- Nombre de paquets : 1000000

- Q3 : Complétez la ligne de commande suivante (Aide : sudo mz –h)
  sudo mz ……

Visualiser le trafic généré via NTOP

8.3 - Lancer une découverte de votre environnement

Avec l'application NMAP, vous pouvez analyser votre environnement IP. La commande suivante va permettre d'analyser l'ensemble du réseau 10.0.119.0/27 :

$ sudo nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 10.0.119.64/27
- T4 : rapidité du scan (0 à 5)
- A : Détection des OS et versions
- v : mode bavard
- PE : découverte par ICMP
- PS et PA: analyse de ports donnés

- Q4 : Quelles machines avez-vous découvertes ?
  ……
  ……
  ……
- Q5 : Quelles informations peut-on recueillir ?
  ……
  ……
  ……

8.4 - Exemple de capture de mot de passe FTP

Lancer l'outil de capture des mots de passe :
$ sudo dsniff -c -i eth0

Demander à votre binôme de se connecter à votre station en FTP et réciproquement.

Note : vous pouvez utiliser netwag et/ou netwox pour créer le serveur FTP
ou suivre les indications ici : https://guide.ubuntu-fr.org/server/ftp-server.html

8.5 - Mesure de débit réseau

La mesure d'un débit réseau se réalise entre deux équipements qui disposent de l'application nuttcp (un en mode serveur, un en mode client).

Lancement du mode serveur
$ sudo nuttcp –S --nofork

Le transfert consiste à envoyer (mode –t) ou recevoir (mode –r) des données du client vers le serveur sur les ports de communication suivants :

- ☐ Tcp/5000 (contrôle)
- ☐ Tcp/5001 (données)

Lancement du mode client (tcp)
$ sudo nuttcp –b –t IP_du_serveur

- Q6 : Quel est le débit (upload) mesuré ? ……

$ sudo nuttcp –r –t IP_du_serveur

- Q6 : Quel est le débit (download) mesuré ? ……

Lancement du mode client (udp)
En mode udp il faut spécifier le débit que l'on souhaite tester. On le précise avec –R 80000 qui correspond au débit en kbps, sinon par défaut il teste pour 1000 kbps.

$ sudo nuttcp –b –u –R 80000 –t IP_du_serveur

- Q7 : Quel est le débit mesuré ? ……
- Q8 : Que se passe-t-il si la valeur –R est supérieure à celle de l'interface réseau ?
  ……
  ……

8.6 - Questions complémentaires

- Q11 : Quelle est l'adresse IP de la station enseignant ?
  ……
  ……
- Q12 : Quels services réseaux sont accessibles ?
  ……
  ……
- Q13 : Quelles informations avez-vous pu recueillir sur les caractéristiques de cette machine ?
  ……
  ……
  ……
  ……
  ……
  ……
  ……
  ……

8.7 - Attaque Brute Force

Pour trouver un mot de passe, une solution consiste a utiliser un dictionnaire de mot et tester les connexions de façon systématique. Une application comme hydra cela.

Installer hydra :

```
sudo apt-get install hydra-gtk
```

A l'aide du tutoriel présent ici : https://linuxtrack.net/viewtopic.php?id=842

Essayez de craquer le mot de passe « ssh » d'une station du réseau.

(des dictionnaires peuvent être disponibles ici :http://www.kali-linux.fr/forum/index.php?topic=2476.0 , attention à la taille de certains)

8.8 - Pour aller plus loin

- Tester d'autres outils en vous inspirant de ce qui existe sur le cd de Kali Linux (airCrack par exemple).

  https://www.kali.org/

- Intégrer votre serveur de supervision à l'architecture déployée depuis le début :
  - Parefeu pfsense
  - Point d'accès WLAN
  - Station d'administration