Laboratoire de gestion des réseaux informatiques (GRX)

Syslog

Auteur : Sébastien Henrioud, (modifié par Bastian Gardel)

Professeur : Stephan Robert

Version : 3.0/5.10.2016

Groupe No : \_\_\_\_\_\_\_\_\_

Etudiants : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Contenu

[Délai 3](#_Toc463513504)

[1 Introduction 3](#_Toc463513505)

[2 Matériel 3](#_Toc463513506)

[3 Topologie 4](#_Toc463513507)

[4 Table d’adressage 4](#_Toc463513508)

[5 Laboratoire 5](#_Toc463513509)

[Objectif 1 : Construire le réseau et réaliser la configuration de base des équipements. 5](#_Toc463513510)

[Objectif 2 : Configurer un serveur et deux clients Syslog 5](#_Toc463513511)

[Objectif 3 : Configurer syslog sur des composants du réseau 6](#_Toc463513512)

[Objectif 4 : (Optionnel) Rediriger les événements windows sur un serveur Syslog 7](#_Toc463513513)

**Objectifs**

1. Construire le réseau et réaliser la configuration de base des équipements.
2. Configurer un serveur et des clients Syslog
3. Configurer syslog sur des composants du réseau
4. (Optionnel) Rediriger les événements windows sur un serveur syslog

## Délai

Le fichier PDF du rapport contenant les réponses aux questions et la configuration des équipements doit être envoyé au professeur et à l’assistant avant le début du prochain laboratoire. Le rapport doit être rédigé de telle sorte à ce qu'un ingénieur qui ne connait pas la gestion des réseaux puisse refaire les expériences que vous avez menées sans autre documentation que celle de votre rapport.

# Introduction

Dans ce laboratoire, vous allez découvrir un premier protocole standard utilisé dans la gestion des réseaux, Syslog, supporté une grande majorité des équipements (réseau, imprimantes, PCs) dont le but est que chaque client envoie un message sur un serveur central. Ce protocole est utilisé dans la gestion des systèmes informatiques mais aussi pour des audits de sécurité, ainsi que pour l’analyse et le debogage dans un cadre plus général.

# Matériel

Chaque poste de travail est composé des éléments suivants :

* 1 poste de travail Dell 9010 avec :
	+ Win7 + Wireshark
	+ VM Kali (Disponible sur la clé usb)
* 1 Poste de travail Dell 9020 avec :
	+ Win 7
* 1 routeur Cisco (Dans l’armoire du fond)
* 1 switch Cisco (En Place sur les tables)

# Topologie



# Table d’adressage

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Equipement | OS | Interface | Adresse IP | Masque de sous-réseau | Passerelle par défaut |
| R1 |  |  |  |  |  |
|  |  |  |  |  |  |
| S1 |  |  |  |  |  |
|  |  |  |  |  |  |
| Dell 9010 | Win7 | NIC |  |  |  |
|  | Kali (VM) | NIC |  |  |  |
| Dell 9020 | Win7 | NIC |  |  |  |

# Laboratoire

## Objectif 1 : Construire le réseau et réaliser la configuration de base des équipements.

* Câbler le réseau comme noté selon la topologie ci-dessus.
* Configurer les PCs.
	1. Dell 9010
		1. Interface en DHCP connectée au réseau de l’école
		2. Interface en statique connectée selon le schéma
		3. VM Kali. (Demander la vm préparée par l’assistant)
			1. Configurer l’interface de la VM avec l’adresse IP 192.168.1.4 en statique.
			2. Configurer Virtual Box en « Bridged Networking »
	2. Dell 9020
		1. Interface en statique connectée selon le schéma
* Réinitialiser le switch et le routeur si nécessaire
	1. !! Attention !! Ne pas lancer l’installation initiale sur le routeur (Initial configuration dialog)
* Réaliser la configuration par défaut pour le routeur et le switch de sorte à ce que chaque équipement puisse « pinguer » n’importe quel autre élément (vérification de la connectivité). On peut relier le Dell 9010 à Internet avec une carte réseau libre.
* Installer les programmes suivants sur le Dell 9010. Installez-les dans le même dossier. Vous pouvez garder celui proposé par défaut. (Utilisez la carte réseau libre de votre PC pour vous connecter à Internet et déconnectez-vous ensuite).
	1. <http://sourceforge.net/projects/syslog-server/>
	2. <http://sourceforge.net/projects/syslog-win32/files/syslog-win32/0.3/>
* (2 pts) Remplir la table d’adressage (à joindre au rapport). Vérification de la connectivité.

## Objectif 2 : Configurer un serveur et deux clients Syslog

* Sur le Dell 9010, aller dans le dossier dans lequel vous avez installé les programmes.
* Dans le même dossier, ouvrez ensuite la console syslog. Vous pouvez ensuite lancer logger.exe, taper un message, puis cliquer sur « enter ».
* Sur la console, vous faites un Refresh et vous devriez voir apparaitre les messages générés par « logger ».
* Depuis la VM linux, configurer syslog, en modifiant le fichier /etc/rsyslog.conf, pour qu’il redirige les messages sur le serveur situé sur le Dell 9010 (Port 514 UDP).
* Générez des messages (reboot, ...) et affichez-les sur la console du serveur syslog distant (Dell 9010). Capturez le trafic syslog à l’aide de Wireshark.
* (1 pt) Quels sont les types de messages générés par Syslog? Donnez plusieurs exemples qui vous semblent utiles dans la gestion des réseaux. A la fin de la manipulation essayez-en quelques-uns non demandés dans la donnée.
* (1 pt) Que pouvez-vous dire sur la sécurité des échanges de messages Syslog ?
* (1 pt) Présentez et expliquer 3 captures de messages Syslog différents.
* Installez WhatsUp Gold free Syslog Server: ftp://ftp.ipswitch.com/ipswitch/Product\_Downloads/IpswitchSyslogServer1.0.0.59.exe
* Après l’installation, essayer de l’éxécuter. Utiliser la fonction “envoie de message” pour en tester le fonctionnement. La question, qui suit, devrait vous aider à résoudre le problème.
* (1 pt) Pourquoi n’est-il pas possible de faire tourner en même temps syslog-server de sourceforge.net et le serveur syslog de WhatsUp Gold ?
* Une fois le problème corrigé, vous pouvez utiliser logger.exe comme précedemment.
* (1 pt) Est-ce que ces deux programmes sont vraiment différents ? Expliquez!
* (1 pt) Quelles possibilités offrent ces deux serveurs pour alerter l’administrateur du serveur Syslog à distance?
* (1 pt) Présentez et expliquer 3 captures de messages Syslog différents.

## Objectif 3 : Configurer syslog sur des composants du réseau

* Configurez les équipements Cisco de manière à récupérer leurs messages sur votre serveur Syslog.
* (2 pt) Quelle est la différence de configuration entre un switch et un routeur (pour pouvoir récupérer ses messages Syslog) ? Expliquez et illustrez.

## Objectif 4 : (Optionnel) Rediriger les événements windows sur un serveur Syslog

* Installez le programme <http://sourceforge.net/projects/el2sl> sur le Dell 9020 à l’aide d’une clé usb.
* Effectuer les configurations nécessaires
* Montrez le bon fonctionnement de la redirection à l’aide de screenshot.