Projets LPRS 2023

Petit rappel : les projets sont à réaliser par petits groupes de **2 ou 3 étudiants** (ni plus, ni moins). Une fois le groupe constitué, vous faites une liste **décroissante** de vos 4 sujets préférés[1] et vous l'envoyez par mail à laroque@u-cergy.fr. Les choix sont gérés en mode « premier arrivé, premier servi ».

Sujet 1 : Wifi

Tutrice : Tuyet-Trâm Dang-Ngoc

Nous utilisons quasi constamment le Wifi, tant dans le cadre privé, que sur les lieux de travail ou dans certains lieux publics.
Il y a toutefois plusieurs types de chiffrement utilisés et utilisables : aucun, WEP, WPA1, WPA2,… ainsi que plusieurs mode d'authentification/autorisation : simple association, Pre Shared Key, architecture PKI, Portail captif...
Vous aurez à déployer chacun des cas d'utilisation, expliquer leur fonctionnement, en décrivant pour chacun des cas :

- le principe de fonctionnement global
- le type de chiffrement utilisé, son principe et les échanges qui y sont effectués dans ce cadre
- les contraintes, installation que cela entraine du côté utilisateur et du côté administrateur
- une réflexion critique sur ce type de cas (avantage, inconvénient, coût matériel, coût humain, disponibilité, SÉCURITÉ, ...

Vous devrez accorder une attention particulière à la vulgarisation (la description de chaque cas identifié doit être synthétique et compréhensible par tous) et sur les références et annexes (qui doivent être précises et montrer qu'il y a un travail approfondi derrière)

Sujet 2 : Mise en place d'un système de monitoring & gestion des logs (Multi système avec poller)

Tuteur : Arnaud Mesguen

Objectif :

- Apprendre les différentes façons de gérer le monitoring SNMP, Scripting, WMI, Trap, Ping, OID
- Installation/configuration d'un système de monitoring open source
- Installation/configuration d'un système de Syslog
- Prise en compte de contrainte d'entreprise (coût, portabilité, évolutivité)

Contexte :
Le département informatique chercher à accroître sa réactivité lors d'incident de production, c'est

1 Vous pouvez également proposer un sujet, sous réserve qu'il soit validé par l'un des enseignants de la LPRS.

pourquoi il a décidé de s'appuyer sur le monitoring et la gestion de logs afin de gérer de façon centrale la remontée d'incident.
La solution de monitoring devra permettre de voir d'un point central tous les incidents des équipements à travers les différents réseaux ; de plus un système de gestion de logs devra être présent afin d'analyser de manière centralisée les causes des différents incidents.
Les solutions devront être open-source afin de répondre à des contraintes budgétaires et virtualisées pour assurer leur portabilité.
Le parc à gérer est hétérogène (Linux, Windows, switches, routeurs, firewalls de marques différentes)

Matériel :
Les équipements seront mis à disposition dans une potence en salle 478.

Sujet 3 : Mise en place d'une architecture réseau sécurisé (hardening "physique" & "logique" / redondance)

Tuteur : Arnaud Mesguen

Objectif :

- Sécurisation au niveau réseau
- Sécurisation au niveau système
- Sécurisation au niveau physique

Contexte :
Devant l'augmentation des attaques informatiques, le département informatique cherche à sécuriser son architecture. Cela passe par différents biais, avoir une architecture solide et redondante en se basant sur les solutions souhaitées. Les points abordés pourront être divers, passant de l'agrégation de ports à la mise en place d'anneau ou la mise de mots de passe forts, la double authentification, la mise en place de WSUS, LGPO, bloqueurs de ports, etc ...
Certains points devront être abordés comme la mise en place de règles de pare feu pertinentes, redondance des équipements pour répondre à une haute disponibilité (réseau/système)...
Chaque choix devra être expliqué afin d'assurer la pertinence de la solution mise en place.

Le matériel :
Les équipements pourront être mis en place en salle 478 et pourront s'accorder avec l'équipe Monitoring pour faire un projet sur des équipements commun pour plus de pertinence.

Sujet 4 : l'IoT aujourd'hui, le temps de la démocratisation : quelle(s) technologie(s) avec quel niveau de sécurité pour quel(s) impact(s) ?

Tuteur : Jean-Luc BOURDON (jean-luc.bourdon@u-cergy.fr)
Objectif : Définir un benchmark des technologies actuelles utilisées dans les objets de l'IoT et de leur niveau de sécurité
Contexte : Le développement de l'IoT depuis quelques années va croître encore de manière exponentielle pour les 20 prochaines années...

1. Qu'en est-il des technologies utilisées ? De leur sécurité ?
2. Quid des normes américaines *vs* les normes européennes ?
3. Quid de leur impact environnemental ?
4. Quid de leur impact économique ?
5. Quid de leur impact sur la vie citoyenne ?

Ce projet a pour objectif un état de l'art de la situation actuelle et des prévisions à court, moyen et long terme.

Sujet 5 : Build a cloud-based Hadoop cluster

Tuteur : Dimitris Kotzinos <Dimitrios.Kotzinos@cyu.fr>
Objectif :

- To setup a networked cluster of Virtual Machines (on the same and/or multiple computers)
- To setup a Hadoop cluster based on the Virtual Machines
- To add the ability to manage resources on the Hadoop cluster
- To demonstrate how to add/remove machines in the cluster
- To run basic computations based on Hadoop

Contexte :
Modern demanding computations take place in cloud environments where we can support elasticity (easy adding/removing of resources), availability (99,9% uptime, easy substitution of faulty resources) and fast distributed computations. Cloud systems are based on the use of Virtual Machines (VM) that allow flexible configurations and easy substitution in case of a problem.
The main goal of this project is to setup such an environment based on VMs that would be able to run a Hadoop (https://hadoop.apache.org/) cluster. Hadoop is a framework for distributed computations that includes different aspects like a distributed file system, a distributed database and a resource manager. The emphasis of the project is on the setup of the Hadoop cluster, the proper configuration of the different elements and the showcase that everything works properly together; distributed computations will be used only as a demonstrator of the actual functionality. The main idea would be to setup a cluster of VMs that would allow the configuration of a Hadoop cluster on top of them with all the elements functioning properly.

After completing this project students will be able

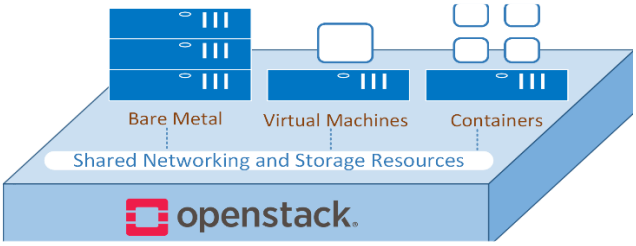
- To develop hands-on skills on configuring virtual machines
- To deploy and configure a Hadoop cluster on top of those VMs
- To deploy and configure different elements of the Hadoop ecosystem (e.g. HDFS, YARN, etc.)

Sujet 6 : OpenStack Installation and Deployment

Tutrice : Iryna Andriyanova

Le texte est en anglais mais les échanges avec le tuteur sont en français !

Motivation



OpenStack is a great open source cloud management software also known as data center operating system. OpenStack controls large pools of storage, networking and compute resources. These resources altogether are managed through APIs or dashboard. OpenStack orchestrates bare metal servers to form data center that provides Infrastructure as a Service (IaaS) functionality. Moreover, additional components of OpenStack provides orchestration, fault management and service management to ensure high availability of user applications.

OpenStack is a free open source data center operating system, no compulsion of vendor lock-in, and advantage of wide community support are the key factors driving the growth of OpenStack across the globe. Thus creating huge job opportunities in IT sector.

The purpose of this project is to learn and deploy various methods of OpenStack installation and managing OpenStack through dashboard or command line interface (CLI).

Project Objectives

Unlike other applications, OpenStack has no standard way of installation but has many deployment methods. Each deployment method comes with its own requirements and challenges. This makes OpenStack more complex for IT professionals and requires relevant knowledge to install and manage.

In this project you will learn and implement practically the following deployment methods of OpenStack:

i. Developer deployment (devstack)
ii. Manual installation (VM, bare metal)
iii. Community deployment (Kolla-Ansible, OpenStack-Ansible)

Project requirements

- Experience with Linux
- Experience with virtualization
- Good understanding of networking, cloud services and storage concepts

Available equipment

We have three physical machines, manageable CISCO switch and networking cables available for this project at St. Martin campus.

After completing this project you will be able to

1. install and manage OpenStack in production environment
2. decide the right choice of OpenStack deployment method along with hardware requirements
3. prepare for the OpenStack Administrator Certification Exam to become certified OpenStack administrator

Sujet 7 : Système de détection des intrusions dans les réseaux

Les progrès rapides dans les domaines de l'internet et de la communication ont entraîné une augmentation considérable de la taille des réseaux et des données correspondantes. En conséquence, de nombreuses nouvelles attaques sont générées et posent des défis à la sécurité des réseaux pour détecter avec précision les intrusions.

Malgré les efforts considérables déployés par les chercheurs et les ingénieurs, les systèmes de détection d'intrusion doivent encore relever des défis pour améliorer la précision de la détection tout en réduisant les taux de fausses alarmes et pour détecter les nouvelles intrusions. Récemment, des systèmes de détection d'intrusion basés sur l'apprentissage automatique et l'apprentissage profond ont été déployés comme solutions potentielles pour détecter les intrusions sur le réseau de manière efficace.

La figure 1 illustre un système de détection d'intrusions qui contient plusieurs étapes :

1. La collecte de données de chaque canal du réseau à l'aide de statistiques et l'extraction de caractéristiques pour chaque paquet. Le vecteur de données capture le contexte temporel du canal et de l'expéditeur du paquet.
2. La transformation de données
3. La projection de données
4. L'utilisation d'un ensemble d'autoencodeurs
5. La validation des résultats

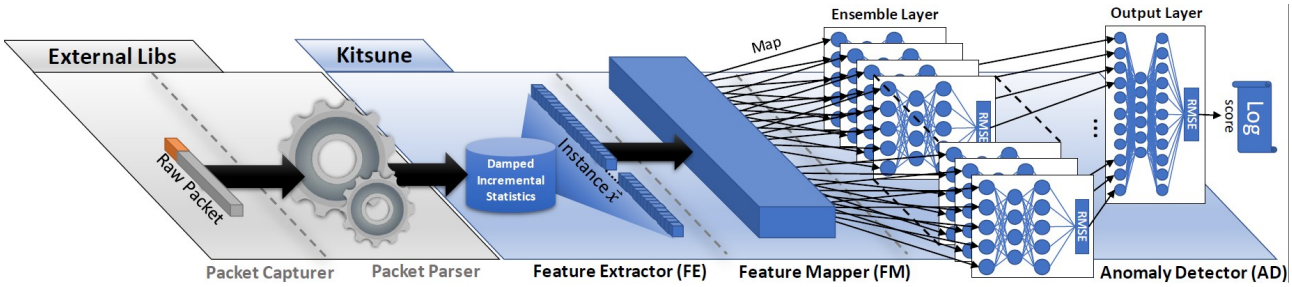


Figure 1 : Le système de détection d'intrusions Kitsune

Dans ce dépôt, vous trouverez une implémentation Python de Kitsune, un système de détection d'intrusion en ligne, basé sur un ensemble d'autoencodeurs :
https://github.com/ymirsky/Kitsune-py

L’objectif de ce projet est de tester les modèles d’apprentissage artificiel pour la détection d’intrusions en utilisant les données disponibles sur :
https://www.unb.ca/cic/datasets/index.html

Résultats attendus
Tests de plusieurs modèles d’apprentissage artificiel pour la détection d’intrusions sur un réseaux informatique, comparer les modèles et les résultats obtenus.
Compétences souhaitées
- Réseaux informatiques et Traitement de données
- Connaissances générales du langage Python ou la possibilité de monter en compétence en Python (utilisation des librairies numpy, pandas, scikit-learn)
Contact
Nistor GROZAVU : nistor.grozavu@cyu.fr

Sujet 8 : stratégie de création de comptes

Tuteur : N. Ouassini
Une école a vu son le nombre d’étudiants augmenter par rapport aux années précédentes.
l’administrateur a voulu changer sa méthode pour la création des comptes utilisateurs.
L’administrateur veut mettre en place une stratégie de création de comptes

- Il faut que les etudiants aient un espace de stockage sur le réseau
- Il faut que chaque utilisateur reçoive par mail son login généré automatiquement à partir d’un AD ou LDAP avec Mot de passe
- Une stratégie pour que tous les utilisateurs aient leurs identifiants et mot de passe directement sur leur boite mail perso (publipostage)

Le matériel

- switch CISCO
- un routeur
- Des unités centrales
- compte sur la boite sur le domaine epmistes.net
- Distribution linux
- Système d’exploitation Windows 10 et serveur 2019
- Serveurs

Sujet 9 : architecture multi-sites

Tuteur : N. Ouassini
ECAM-EPMI s’agrandit et ouvre 2 autres écoles, une dans le sud et une sur paris.
Le site de CERGY représente 1170 étudiants et administrateurs, celui de paris 700 utilisateurs et administrateurs et l’école dans le sud 160 utilisateurs.
Quelle architecture préconisez-vous pour avoir une stratégie identique pour les 3 sites ?
L’école dispose de 200 licences flottante SolidWorks, 5 licences ANSYSYS et une vingtaine de licences Matlab sur le site de Cergy
L’idée est de mettre à disposition des 3 écoles les mêmes licences sans qu’il n’y ait aucun impact sur le site Cergy et les 3 écoles, sachant que l’école n’a pas les moyens d’acheter une licence pour

chaque école.

Le travail

- Mise en place de machines virtuelles, un RDP, un VPN ……. Ou même une proposition de votre part pour que toutes les licences soient accessibles partout où les utilisateurs travaillent.
- Mise en place d'une architecture avec Visio
- Mise en place de la plateforme
- Sécurisation des données
- Continuité de service

Le matériel

- 2 switch Cisco 2960
- 2 routeurs Cisco série 800
- Des UC (unités centrales).

Sujet 10 : Haute disponibilité de VM

Tuteur : N. Ouassini

Je cherche à résoudre la problématique suivante sur mon réseau: mettre en place un SAN hautement disponible afin d'y stocker les machines virtuelles gérées par un cluster de virtualisation.
Je sollicite votre aide pour mettre en place 2 serveurs de virtualisation (PROXMOX) et virtualisation de 2 serveurs : 2008 R2, 1 Ubuntu.
Sur un des 2 serveurs

- Mise en place de DRBD
- Mise en place heartbeat entre les deux serveurs
- Mise en place et configuration du NFS.

Sujet 11 : Domotique

Tuteur : N. Ouassini

Une entreprise spécialisée dans le domaine de la domotique a mis en place un serveur de gestion de IOT (matériels connectés)
Vous êtes chargés de :

- La mise en place du serveur domotique comme par exemple Openhab, Jeedom ou Home assistant
- La supervision du firewall PFSENSE sur le serveur avec mise en place d'un contrôleur multimédia Plex
- L'automatisation des notifications
- Owntrack
- La supervision du matériel CISCO
- La mise en place de remontées de notification sur téléphone

Sujet 12 : Communication inter-VLAN

Tuteur : N. Ouassini

Le but de ce projet est de mettre en place une communication inter-vlan à l'aide de switch reliés entre eux par des liens Trunks et de les configurer avec le protocole de redondance, qui permet d'avoir une tolérance aux pannes, de façon à assurer la communication entre les switch, lorsqu' un des liens les reliant tombe, en empruntant un autre lien.
Vos tâches concernent la mise en place de la plateforme avec les commandes explicatives nécessaires à la configuration de l'ensemble des éléments du réseau (switch, pc et routeur).

Architecture matérielle

Tuteur : N. Ouassini
Mise en place de 3 vlan avec un serveur DHCP pour chaque sous-réseau, uniquement sur des routeurs

- Schéma représentatif de l'architecture réseau à réaliser sous packet tracer
- Suppression des configurations de périphériques existantes
- Configurations de la sécurité de base des périphériques
- Configuration d'un mot de passe pour les connexions de consoles.
- Configuration d'un mot de passe pour les connexions de terminaux virtuels (vty).
- Limitation du protocole STP sur les interfaces comportant des postes/serveurs.
- Configuration de l'interface VLAN de gestion sur Comm1, Comm2 et Comm3
- Choix et configuration du commutateur « comm X » pour qu'il soit toujours pont racine et de « comm Y » comme pont de secours.
- Vérification du routage entre réseaux locaux virtuels

Sujet 13 : Pare-feu et VPN

Tuteur : N. Ouassini

Dans le cadre d'une création d'un réseau d'entreprise vous devrez mettre en place un pare-feu « IPFIRE » et le configurer. Vous devrez en outre trouver un moyen de bloquer le site « Facebook » en http/https.

Travail demandé

- Mise en place des règles de filtrage ainsi que des redirections de port.
- Mise en place d'un VPN
- Mise en place d'un routage inter vlan.
- Mise en place d'une authentification radius à partir de Ipfire

Votre mission est intéressante d'un point de vue professionnel où la sécurité est une clef de voûte de l'informatique.

Matériel

- des UC
- des switchs Cisco ou 3com
- Routeurs Cisco ou 3 Com
- 1 serveur.